

# СЗИ «Страж NT»

Руководство администратора



© ЗАО НПЦ «МОДУЛЬ». Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ является частью эксплуатационной документации и входит в комплект поставки программного обеспечения. На него распространяются все условия лицензионного соглашения. Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ЗАО НПЦ «Модуль».

Все торговые марки и названия программ являются собственностью их владельцев.

## ЗАО НПЦ «Модуль»

Телефон/факс: +7 (495) 955-9029

E-mail: [info@guardnt.ru](mailto:info@guardnt.ru)

Web: <http://www.guardnt.ru>

# Оглавление

---

Введение .....	6
Структура документа .....	6
Условные обозначения .....	7
Обозначения .....	7
Перекрестные ссылки .....	7
Примечания .....	8
Соглашения о терминах .....	8
Общие сведения .....	9
Назначение программы .....	9
Условия применения .....	9
Механизмы системы защиты .....	10
Установка и снятие системы защиты .....	14
Подготовка к установке системы защиты .....	14
Тестирование подсистемы идентификации .....	14
Установка системы защиты .....	16
Вход в систему .....	25
Снятие системы защиты .....	27
Ситуации, возникающие при входе в систему .....	29
Рекомендации при возникновении внештатных ситуаций .....	30
При установке и снятии системы защиты .....	30
При загрузке операционной системы .....	32
Аварийное снятие системы защиты .....	34
Настройка системы защиты .....	36
Общие настройки .....	37
Метки конфиденциальности .....	38
Ярлыки .....	38
Замкнутая программная среда .....	39
Шаблоны настроек .....	41
Менеджер пользователей .....	43
Дополнительный аудит .....	43
Преобразование информации .....	44
Монитор системы защиты .....	45
Для администратора .....	45

Для пользователей .....	47
Маркировка документов .....	47
Угловой штамп .....	48
Нижний штамп .....	49
Последний лист .....	50
Дополнительные поля .....	51
Дополнительно .....	52
Управление носителями информации .....	54
Редактирование свойств для групп носителей .....	56
Добавление и удаление зарегистрированных носителей информации .....	58
Редактирование свойств носителей .....	60
Экспорт настроек .....	61
Управление пользователями .....	63
Создание, удаление и переименование пользователей .....	65
Просмотр пароля и списка идентификаторов пользователя .....	66
Смена пароля пользователя .....	67
Просмотр и редактирование свойств пользователя .....	68
Общие свойства .....	69
Свойства безопасности .....	69
Членство в группах .....	70
Формирование персональных идентификаторов .....	71
Чтение и очистка идентификаторов .....	73
Дополнительно .....	74
Работа с ресурсами .....	75
Общие сведения .....	75
Представление файлов и папок .....	78
Выбор столбцов .....	78
Файловые операции .....	79
Работа с файловыми ресурсами .....	79
Редактирование разрешений .....	80
Изменение владельца .....	82
Редактирование параметров системного аудита .....	83
Назначение грифа .....	84
Установка режима запуска и допуска .....	84
Редактирование параметров дополнительного аудита .....	85

Дополнительные параметры для папок.....	85
Установка параметров целостности .....	86
Проверка целостности .....	87
Работа с принтерами.....	88
Редактирование разрешений и смена владельца .....	88
Назначение грифа.....	89
Контроль устройств .....	92
Редактирование свойств для групп устройств .....	93
Экспорт настроек.....	94
Журнал событий .....	96
Открытие и сохранение журнала событий.....	99
Группы событий.....	100
Фильтрация и поиск .....	102
Дополнительно.....	104
Редактор шаблонов настроек.....	106
Работа с шаблонами.....	107
Работа с ресурсами .....	108
Импорт разрешений.....	110
Тестирование системы защиты .....	111
Дополнительные функции.....	115
Режим автозапуска .....	115
Блокировка компьютера.....	116
Разблокировка компьютера .....	117
Повторная идентификация пользователей.....	118
Термины и определения .....	119

# Введение

---

Документ предназначен для администратора системы защиты информации от несанкционированного доступа «Страж NT» (версия 3.0) (далее в документе СЗИ «Страж NT»). В документе приведены сведения о назначении и вариантах применения системы защиты, об архитектуре и общих принципах функционирования программного обеспечения, а также сведения об используемых механизмах и средствах защиты.

Представленные в документе элементы графических интерфейсов программ и операционной системы соответствуют работе системы защиты в среде операционной системы Microsoft Windows 7.

## Структура документа

Материал руководства организован следующим образом:

- В главе **Общие сведения** приводятся сведения о назначении системы защиты информации, условия и варианты ее применения. Также в этой главе кратко описаны механизмы и компоненты системы защиты информации.
- В главе **Установка и снятие системы защиты** описаны процедуры установки и снятия системы защиты информации, а также порядок входа пользователей в систему. Дополнительно в этой главе рассматриваются действия администратора системы защиты при возникновении внештатных ситуаций.
- В главе **Настройка системы защиты** приводятся сведения о назначении и применении программы **Настройка системы защиты**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при настройке замкнутой программной среды и применении шаблонов настроек.
- В главе **Управление носителями информации** приводятся сведения о назначении и применении программы **Учет носителей**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при учете носителей информации.
- В главе **Управление пользователями** приводятся сведения о назначении и применении программы **Менеджер пользователей**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при работе с учетными записями пользователей и персональными идентификаторами.
- В главе **Работа с ресурсами** приводятся сведения о назначении программы **Менеджер файлов**, ее экранные формы и параметры. Также описаны типовые

действия администратора системы защиты при работе с ресурсами и их защитными атрибутами.

- В главе [Контроль устройств](#) приводятся сведения о назначении программы **Контроль устройств**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты.
- В главе [Журнал событий](#) приводятся сведения о механизмах подсистемы регистрации, а также о назначении программы **Журнал событий**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при работе с журналом событий.
- В главе [Редактор шаблонов настроек](#) приводятся сведения о назначении программы **Редактор шаблонов настроек**, ее экранные формы и параметры. Также описан порядок создания шаблонов настроек и работы с ними.
- В главе [Тестирование системы защиты](#) приводятся сведения о назначении программы **Тестирование системы защиты**, ее экранные формы и параметры. Также описаны типовые действия администратора при тестировании механизмов системы защиты.
- В главе [Дополнительные функции](#) приводится описание дополнительных механизмов и функций системы защиты.
- В главе [Термины и определения](#) приведены основные понятия и термины, встречающиеся в данном руководстве.

## Условные обозначения

### Обозначения

В тексте документа могут встречаться следующие обозначения:

- Названия элементов интерфейса Windows набраны строчными буквами **полужирного** начертания.
- Имена файлов и каталогов, программ набраны строчными буквами **полужирного** начертания.

### Перекрестные ссылки

В тексте документа могут встречаться ссылки на другие части данного документа или другие источники информации. Внутренние ссылки содержат указание на номер страницы с необходимыми сведениями, таблицу, рисунок или раздел. Например, ссылка на Рисунок 1 данного документа выглядит следующим образом: (см. Рис. 1).

## Примечания

Информация, требующая особого внимания, оформлена в виде примечаний со значками, отражающими степень ее важности:



Так отмечается важная информация, которую необходимо принять во внимание.



Так отмечаются сведения, не принятие во внимание которых может привести к критическим последствиям.



Так отмечаются ссылки на источники дополнительной информации.

## Соглашения о терминах

Некоторые термины, содержащиеся в тексте руководства, уникальны для системы защиты информации «Страж NT», другие являются общепринятыми определениями. Смысл основной части терминов излагается в главе [Термины и определения](#), которая находится в конце этого документа.



# Общие сведения

---

В данной главе рассматриваются назначение системы защиты информации, условия и варианты ее применения. Также в этой главе кратко описаны механизмы и компоненты системы защиты информации.

## Назначение программы

Система защиты информации от несанкционированного доступа «Страж NT» (версия 3.0) представляет собой комплекс средств защиты информации в автоматизированных системах на базе персональных компьютеров.

СЗИ «Страж NT» предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах на базе персональных ЭВМ. СЗИ «Страж NT» может использоваться при разработке систем защиты информации для автоматизированных систем до классов защищенности 3А, 2А и 1Б включительно в соответствии с требованиями Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», а также для создания информационных систем обработки персональных данных до 1 класса включительно.

## Условия применения

СЗИ «Страж NT» может устанавливаться на автономных рабочих станциях, рабочих станциях в составе рабочей группы или домена, серверах, в том числе в составе кластера. СЗИ «Страж NT» может функционировать на одно- и многопроцессорных компьютерных системах под управлением операционных систем Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 и Windows Server 2008 R2. Компьютер, на котором устанавливается СЗИ «Страж NT», должен удовлетворять требованиям, необходимым для загрузки операционной системы.

В силу особенностей реализации защитных механизмов СЗИ «Страж NT» существуют дополнительные требования к аппаратному обеспечению компьютера:

- загрузочный жесткий диск должен иметь не менее 63 секторов перед началом первого раздела (32 256 байтов);
- при использовании USB-клавиатуры и USB-идентификаторов пользователей в некоторых случаях требуется наличие не менее 2 контроллеров USB;

- в случае применения в качестве идентификаторов пользователей USB флэш-накопителей в BIOS компьютера должна быть включена поддержка таких устройств.

Тип файловой системы на жестких дисках компьютера не имеет значения, это может быть FAT 16, FAT 32 или NTFS. Жесткий диск компьютера, на котором установлена операционная система, должен иметь свободное пространство объемом не менее 30 Мб.

Перед началом установки СЗИ «Страж NT» рекомендуется установить все системное и прикладное программное обеспечение, предусмотренное на данном рабочем месте. Установка дополнительного программного обеспечения в процессе функционирования СЗИ «Страж NT» является нежелательной.



*После установки системы защиты изменение логической структуры загрузочного жесткого диска будет невозможно. Вследствие этого функционирование программ, выполняющих данные операции, например оснастки **Управление дисками**, будет непредсказуемым.*

Для установки, настройки и управления функционированием СЗИ «Страж NT» должен быть назначен администратор системы защиты. Пользователь, выполняющий функции администратора системы защиты, должен быть создан перед началом установки системы защиты стандартными средствами операционной системы. При установке системы защиты на локальный компьютер администратор системы защиты должен быть включен в группу локальных администраторов. В случае установки системы защиты на компьютер, входящий в домен, администратор системы защиты должен входить в группу локальных администраторов компьютера, а также в группу администраторов домена. Администратор системы защиты должен иметь одинаковое имя и пароль для входа на всех компьютерах, на которых планируется установка СЗИ «Страж NT».

Администратор системы защиты должен быть подготовленным пользователем, знающим принципы функционирования и имеющим навыки работы с операционной системой и СЗИ «Страж NT».

### **Механизмы системы защиты**

В СЗИ «Страж NT» реализована смешанная разрешительно-запретительная модель защиты информации с жестким администрированием. Система защиты представляет собой совокупность следующих основных подсистем:

- идентификации и аутентификации;
- разграничения доступа;

- контроля потоков информации;
- управление запуском программ;
- управления защитой;
- регистрации событий;
- маркировки документов;
- контроля целостности;
- стирания памяти;
- учета носителей информации;
- преобразования информации на отчуждаемых носителях;
- контроля устройств;
- тестирования системы защиты.

Подсистема идентификации и аутентификации обеспечивает опознание пользователей при входе в компьютер по персональному идентификатору и подтверждение подлинности путем запроса с клавиатуры личного пароля. Данная подсистема также обеспечивает блокировку экрана компьютера и идентификацию пользователя после такой блокировки.

Подсистема разграничения доступа реализует дискреционный и мандатный принципы контроля доступа пользователей к защищаемым ресурсам. Функционирование данной подсистемы основано на присвоении защищаемым объектам атрибутов защиты. К атрибутам защиты ресурса, имеющим отношение к разграничению доступа, относятся:

- идентификатор безопасности владельца ресурса;
- список контроля доступа;
- режим запуска (для исполняемых файлов);
- метка конфиденциальности (гриф для неисполняемого файла или допуск для исполняемого файла).

Дискреционный принцип основан на сопоставлении полномочий пользователей и списков контроля доступа ресурсов (логических дисков, папок, файлов, принтеров).

Мандатный принцип контроля доступа реализован путем сопоставления при запросе на доступ к ресурсу меток конфиденциальности пользователя, прикладной программы и защищаемого ресурса.

Подсистема контроля потоков информации предназначена для управления операциями над ресурсами, имеющими различные метки конфиденциальности.

Подсистема запуска программ предназначена для обеспечения целостности и замкнутости программной среды и реализована путем разрешения для исполняемых файлов режима запуска. Если режим запуска программы не разрешен, то файл не является исполняемым и не может быть запущен пользователем ни при каких условиях.

Подсистема управления защитой включает в себя следующие программы администрирования системы защиты:

Программа	Назначение
<b>Установка и снятие системы защиты</b>	Загрузка всех компонентов системы защиты информации, выполнение необходимых настроек в операционной системе, удаление всех компонентов при снятии системы защиты.
<b>Настройка системы защиты</b>	Установка параметров системы защиты информации, а также создание замкнутой программной среды, применение шаблонов настроек и другие сервисные функции.
<b>Учет носителей</b>	Настройка параметров работы системы защиты с носителями информации.
<b>Менеджер пользователей</b>	Управление пользователями системы защиты информации, их свойствами и персональными идентификаторами.
<b>Менеджер файлов</b>	Управление ресурсами, а также их защитными атрибутами.
<b>Контроль устройств</b>	Настройка правил работы системы защиты с устройствами компьютера.
<b>Журнал событий</b>	Работа с журналом событий системы защиты.
<b>Редактор шаблонов настроек</b>	Автоматизированное создание шаблонов настроек системы защиты.
<b>Монитор системы защиты</b>	Отображение состояния системы защиты, а также быстрый вызов функций управления системой защиты.

Подсистема регистрации обеспечивает регистрацию запросов на доступ к ресурсам компьютера и возможность выборочного ознакомления с регистрационной информацией и ее распечатки.

Подсистема маркировки документов обеспечивает автоматическое проставление учетных признаков в документах, выдаваемых на печать, а также регистрации фактов печати документов.

Подсистема контроля целостности предназначена для настройки и периодической проверки параметров целостности системы защиты, программного обеспечения и постоянных информационных массивов.

Подсистема стирания памяти реализует механизм заполнения нулями выделяемых программам областей оперативной памяти и стирания файлов на диске по команде удаления. В рамках данной подсистемы также реализовано стирание файла подкачки страниц по завершении сеанса работы.

Подсистема учета носителей информации позволяет управлять доступом к носителям информации в соответствии с разрешениями и параметрами, прописанными в журнале учета носителей.

Подсистема преобразования информации на отчуждаемых носителях позволяет включить дополнительную защиту для съемных носителей с помощью режима прозрачного преобразования всей информации на носителе.

Подсистема контроля устройств позволяет формировать необходимую конфигурацию устройств для пользователей в соответствии с установленными разрешениями.

Подсистема тестирования системы защиты предназначена для комплексного тестирования основных механизмов системы защиты, как на локальном компьютере, так и на удаленном, с использованием локальной вычислительной сети.



*Более подробные сведения о механизмах и компонентах системы защиты можно найти в документе МАНУ.00030-01 з1. Система защиты информации от несанкционированного доступа «Страж NT». Версия 3.0. Описание применения.*

# Установка и снятие системы защиты

---

В данной главе описаны процедуры установки и снятия системы защиты информации, а также порядок входа пользователей в систему. Дополнительно в этой главе рассматриваются действия администратора системы защиты при возникновении внештатных ситуаций.

## Подготовка к установке системы защиты

Перед установкой СЗИ «Страж NT» на компьютер следует провести ряд обязательных процедур:

- проверить оперативную память компьютера, а также его жесткий диск на отсутствие вирусов;
- убедиться в наличии на жестком диске свободного места, достаточного для установки и функционирования системы защиты;
- убедиться, что на компьютере в данный момент не запущены какие-либо программы, препятствующие работе с системным реестром, выполняющие функции защиты от шпионского программного обеспечения и так далее.
- убедиться в наличии исправного персонального идентификатора (в случае использования ГМД он должен быть отформатирован) и в возможности его чтения подсистемой идентификации (см. раздел [Тестирование подсистемы идентификации](#));
- убедиться, что пароль пользователя, устанавливающего систему защиты, не содержит символов кириллицы и специальных знаков, а его длина не превышает 15 символов.

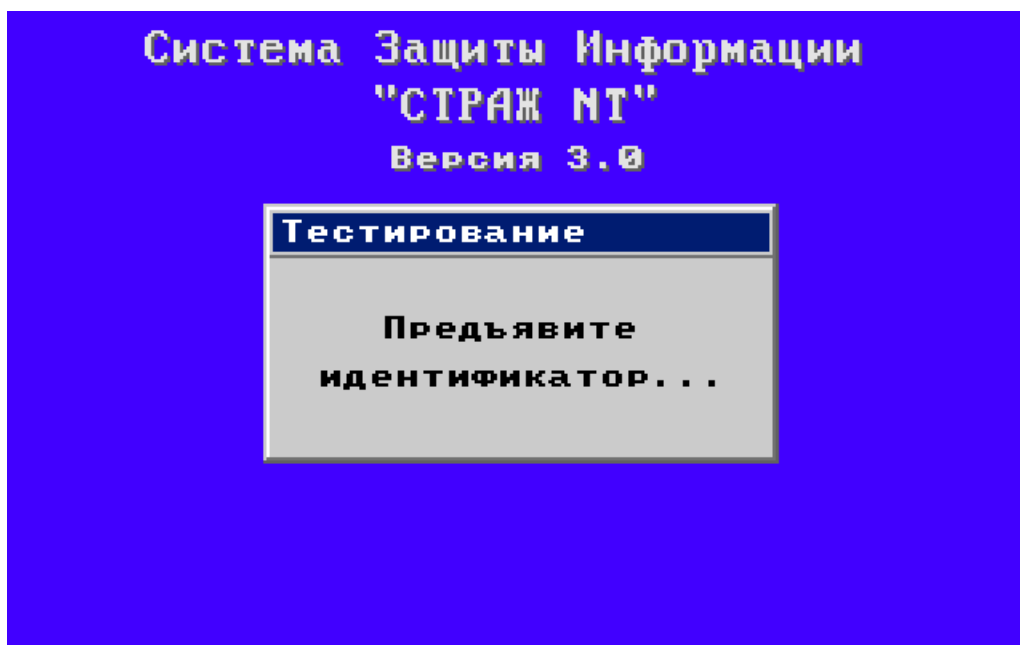


*Недопустимо наличие установленных на компьютере других операционных систем и программ-мультизагрузчиков, так как наличие первых снижает защищенность системы, а наличие вторых может привести к некорректной установке системы защиты.*

## Тестирование подсистемы идентификации

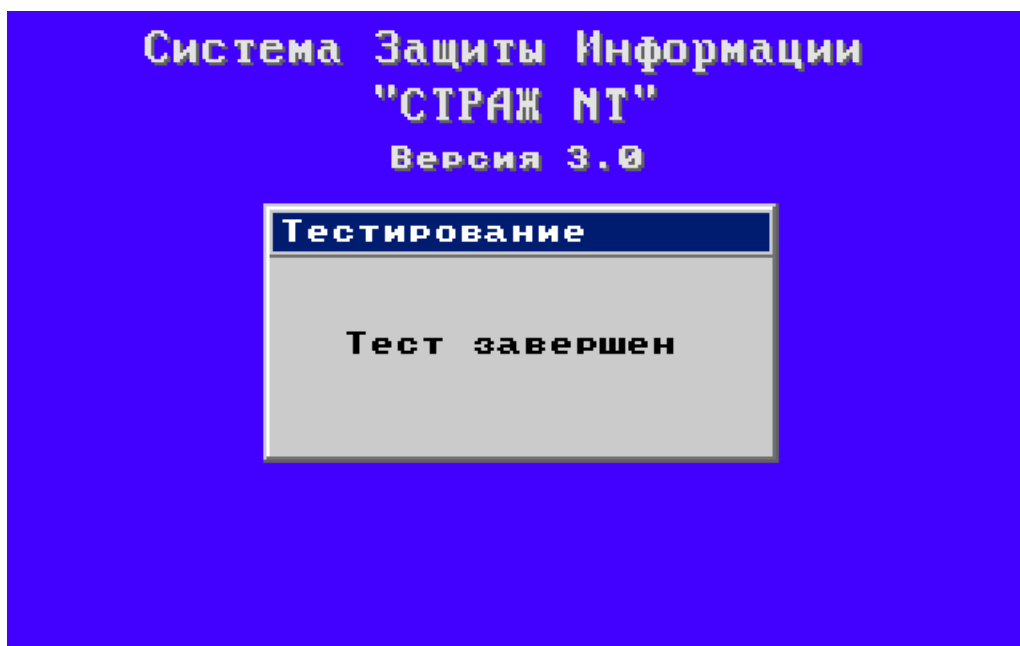
Тестирование подсистемы идентификации предназначено для определения возможности чтения персональных идентификаторов в подсистеме идентификации до загрузки операционной системы. Тестирование подсистемы идентификации проводится до установки системы защиты информации.

Для запуска тестирования необходимо в BIOS Setup компьютера установить принудительную загрузку с носителя информации, на котором поставляется установочный комплект системы защиты. После появления диалога, приведенного на Рис. 1, необходимо предъявить необходимый персональный идентификатор.



*Рис. 1. Тестирование подсистемы идентификации.*

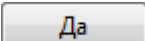
Тестирование считается успешным, если на экране появится сообщение, как на Рис. 2.



*Рис. 2. Результат тестирования подсистемы идентификации.*

После появления сообщения о результатах тестирования следует перезагрузить компьютер.

## Установка системы защиты

Для начала процесса установки СЗИ «Страж NT» необходимо установить компакт-диск в привод CD-ROM. При этом операционная система самостоятельно запустит **Мастер установки**. Если окно **Мастера установки** не появляется, необходимо запустить его самостоятельно, открыв в программе **Проводник** содержимое компакт-диска и запустив программу **GInstall.exe**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей (UAC), при запуске программы на экране появится окно, как показано на Рис. 3. Для продолжения необходимо нажать кнопку .

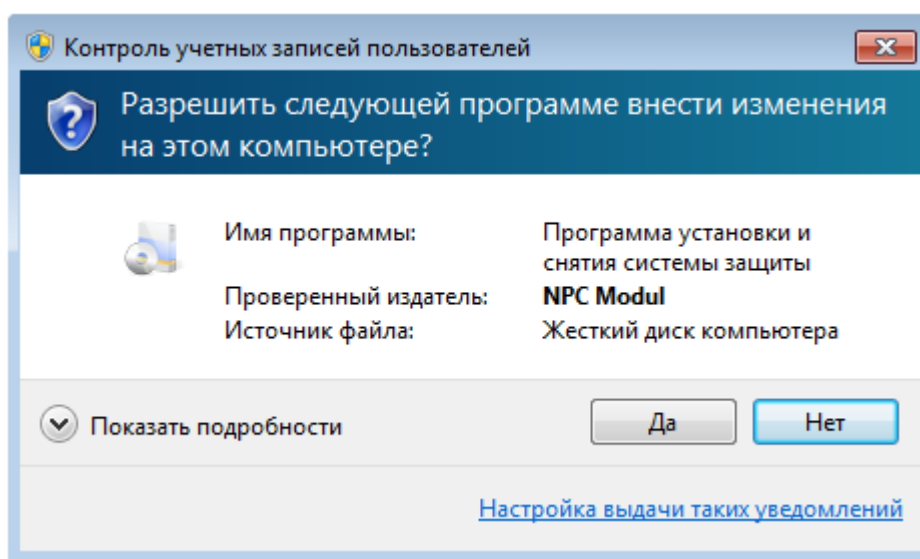
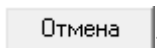


Рис. 3. Сообщение подсистемы контроля учетных записей пользователей.

Если система защиты уже установлена на данном компьютере, **Мастер установки** проинформирует об этом и предложит снять систему защиты, иначе на экране появится окно, как показано на Рис. 4. Из **Мастера установки** можно выйти, нажав кнопку

.



*При возникновении ситуаций, не описанных в данном разделе, следует обратиться к разделу **Рекомендации при возникновении внештатных ситуаций**.*



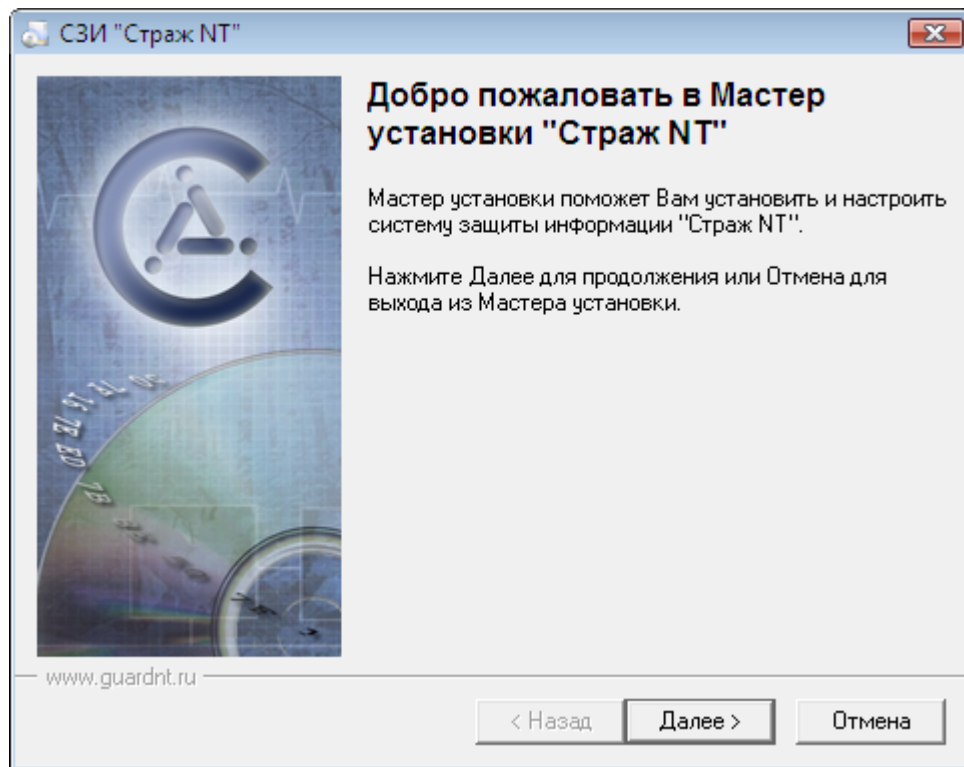


Рис. 4. Начальная страница Мастера установки.

После нажатия кнопки  на экране появится окно с текстом лицензионного соглашения (см. Рис. 5). Внимательно прочитайте его. Для продолжения установки системы защиты необходимо нажать кнопку **Я принимаю условия лицензионного соглашения.**

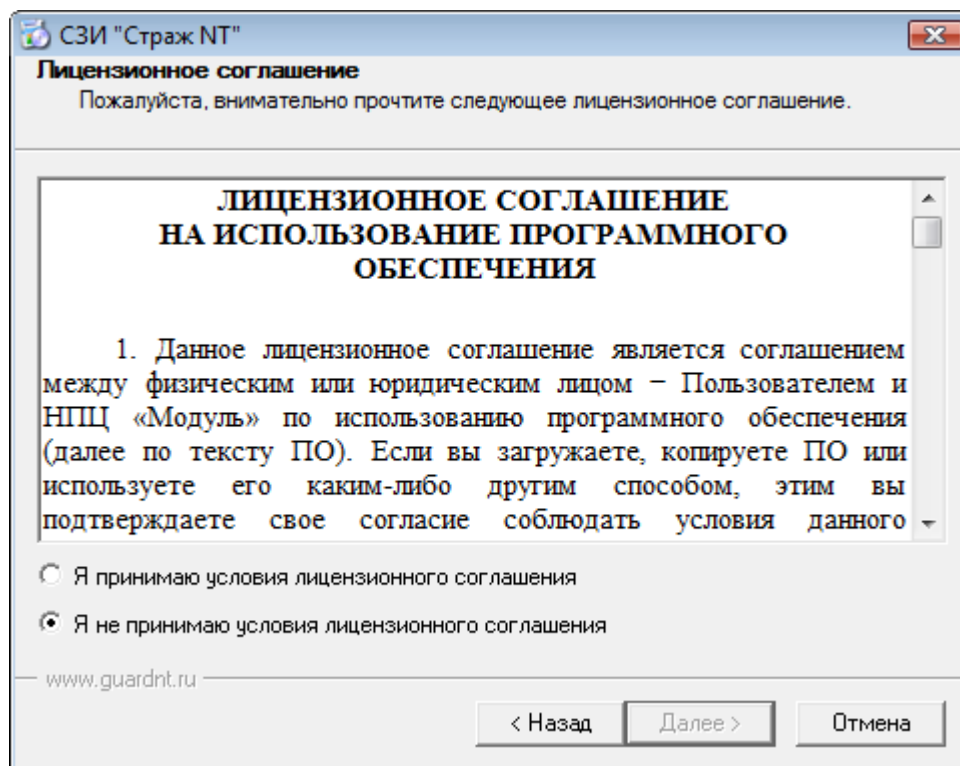


Рис. 5. Лицензионное соглашение.

После этого необходимо нажать кнопку . При этом на экране появится диалог, требующий ввода лицензионного номера установочного комплекта (см. Рис. 6).

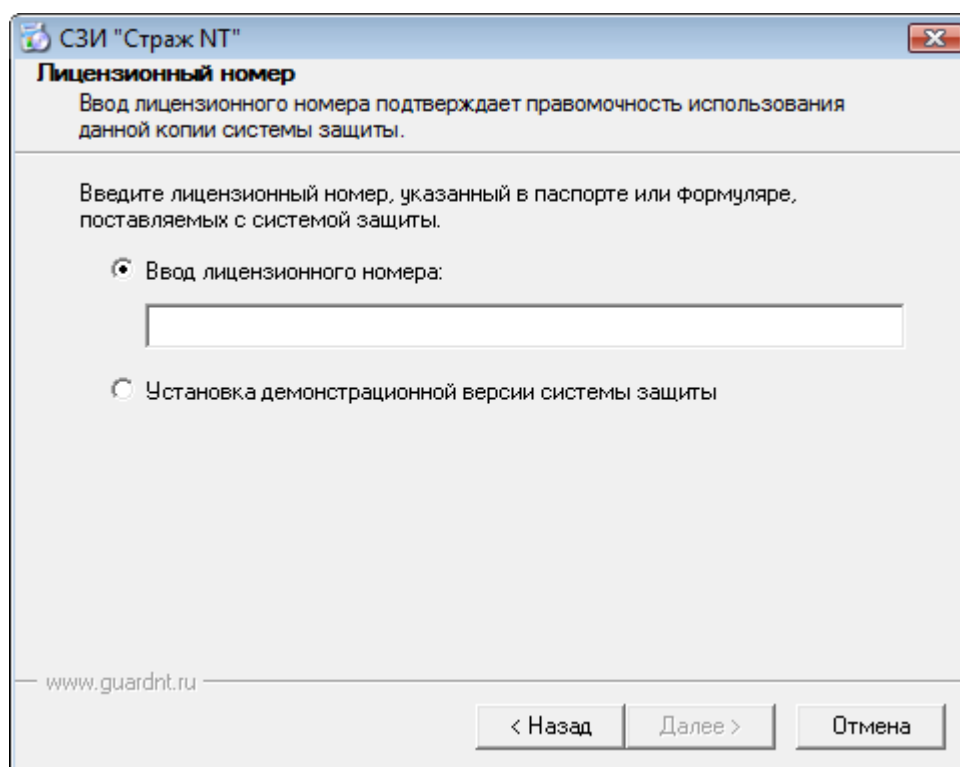
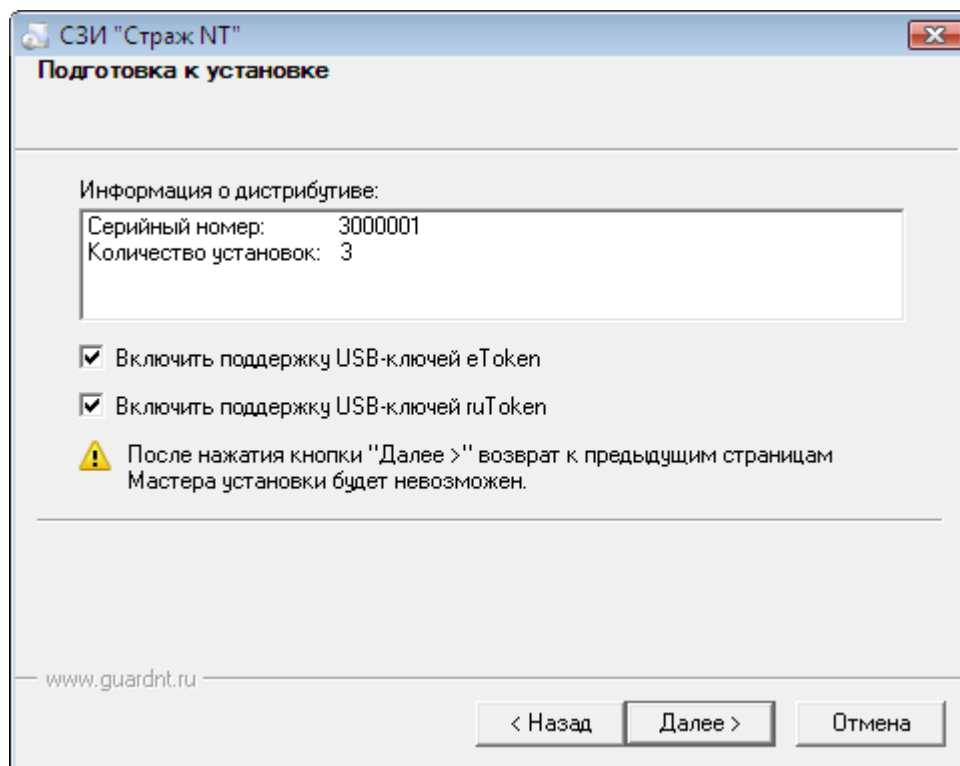


Рис. 6. Ввод лицензионного номера.

Лицензионный номер определяет количество компьютеров, на которые возможна установка системы защиты с данного установочного комплекта, а также срок действия лицензии, если она ограничена. Лицензионный номер указывается в формуляре (паспорте) на систему защиты. Если в текущей папке отсутствует файл лицензии или срок ее действия истек, а также по требованию пользователя, устанавливающего систему защиты, возможна установка демонстрационной версии системы защиты. Демонстрационная версия обладает теми же характеристиками и функциями, что и лицензионная, за следующими исключениями.

- Отсутствует подсистема идентификации пользователей до загрузки операционной системы. Идентификация пользователей будет проходить стандартными для операционной системы средствами с помощью их имени и пароля. При этом при установке СЗИ не формируется персональный идентификатор администратора и, соответственно, не работает механизм формирования персональных идентификаторов пользователей.
- Отключены механизмы подсистемы маркировки документов, выдаваемых на печать. Документы, выдаваемые на печать, маркироваться не будут, факты печати документов в журнал печати заноситься не будут.
- Отключена подсистема преобразования носителей информации.

Кнопка будет активизирована только в случае ввода правильного лицензионного номера. После нажатия кнопки появится диалог, содержащий информацию об установочном комплекте (см. Рис. 7). Если в процессе эксплуатации системы защиты в качестве персональных идентификаторов будут использоваться USB-ключи eToken или ruToken, необходимо установить для них драйвера. Для этого необходимо, чтобы флажки **Установить драйверы для USB-ключей eToken** или **Установить драйверы для USB-ключей ruToken** были установлены. По умолчанию указанные флажки установлены, если в системе соответствующие драйвера не были найдены. В противном случае указанные флажки будут сняты. Если в системе уже установлены драйвера eToken или ruToken, устанавливать их необязательно. Для продолжения установки необходимо нажать кнопку .



*Рис. 7. Информация о комплекте.*

На данном этапе начинается копирование файлов, регистрация необходимых служб системы защиты и настройка параметров компьютера. Установка драйверов USB-ключей eToken и ruToken в зависимости от системы может занять до нескольких минут. Следует обратить внимание, что после выполнения данной процедуры возврат к предыдущим страницам **Мастера установки** будет невозможен. После выполнения необходимых действий на экране появится диалоговое окно формирования персонального идентификатора администратора (см. Рис. 8).

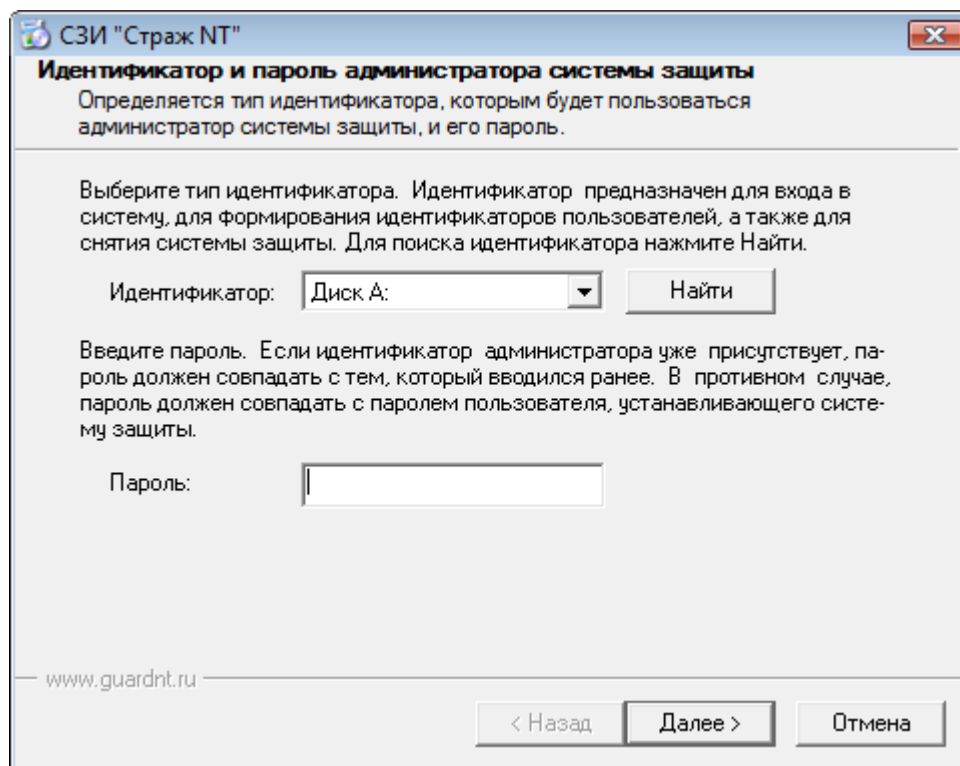


Рис. 8. Формирование идентификатора администратора.

В указанном окне необходимо выбрать тип идентификатора, которым будет пользоваться администратор. Для формирования первого ключа администратора поддерживаются следующие типы идентификаторов: дискеты 3,5", устройства типа iButton, USB-ключи Guardant ID, ruToken и eToken Pro.



*Устройства типа iButton отличаются объемом памяти. Так, iButton DS-1990 памяти не содержит, поэтому не может быть использовано в качестве идентификатора. iButton DS-1992 способно хранить всего 256 байтов информации, поэтому также не может быть использовано в качестве персонального идентификатора администратора.*

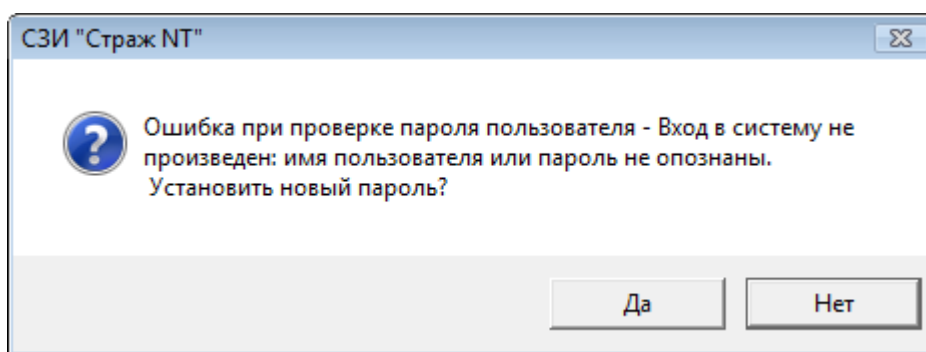
Для автоматического поиска установленного идентификатора необходимо нажать кнопку **Найти**. В этом случае **Мастер установки** последовательно будет опрашивать все устройства, в которые может быть установлен персональный идентификатор (приводы ГМД, СОМ и USB-порты), и при наличии в них исправного персонального идентификатора определит его тип и отобразит в окне.



*В окне отображается первый найденный персональный идентификатор.*

После определения типа идентификатора администратора необходимо ввести его пароль и нажать кнопку . Введенный пароль должен совпадать с паролем пользователя, устанавливающего систему защиты. Введенный пароль проверяется и, в случае его корректности, начинается формирование персонального идентификатора администратора.

Если система защиты устанавливается на нескольких компьютерах с одним администратором, и его персональный идентификатор уже сформирован, необходимо использовать его повторно. Если пароль пользователя, устанавливающего систему защиты, будет отличаться от пароля, который использовался при создании персонального идентификатора администратора на других компьютерах, следует ввести последний. В этом случае, **Мастер установки** выдаст сообщение о некорректности пароля и предложит установить его (см. Рис. 9).



*Рис. 9. Некорректный пароль.*

На данное предложение необходимо ответить утвердительно. При этом пользователю, устанавливающему СЗИ, будет предложено подтвердить новый пароль (см. Рис. 10).

Если на предъявленном идентификаторе уже записана информация о данном компьютере, созданная другим комплектом системы защиты, на экран будет выведено соответствующее предупреждение с предложением перезаписать данную информацию. При положительном ответе информация о данном компьютере будет перезаписана с учетом нового номера инсталляционного комплекта. При отказе вновь появится диалог, как показано на Рис. 8.

Если на предъявленном идентификаторе уже записана какая-то информация, которую **Мастер установки** не сможет распознать, на экран будет выдано предупреждение об этом. Если информация, записанная на идентификаторе, не нужна, необходимо ответить положительно. При этом информация, записанная на идентификаторе, будет утеряна. При нажатии кнопки  вновь появится диалог, как показано на Рис. 8.

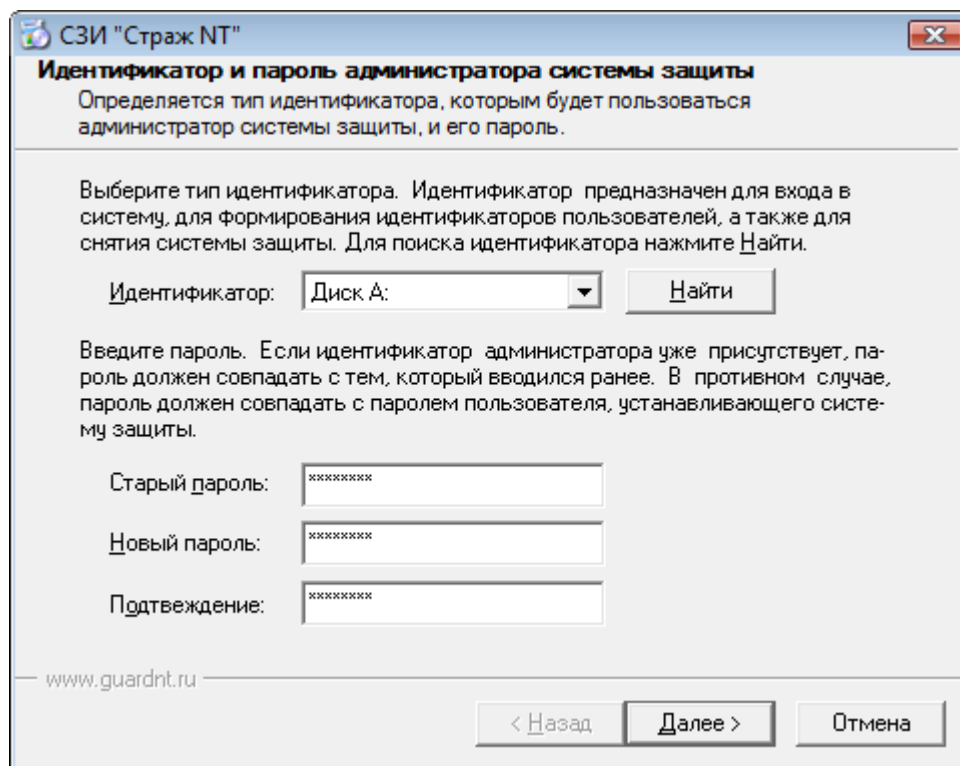


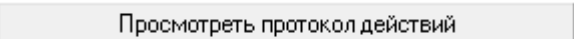
Рис. 10. Подтверждение пароля.

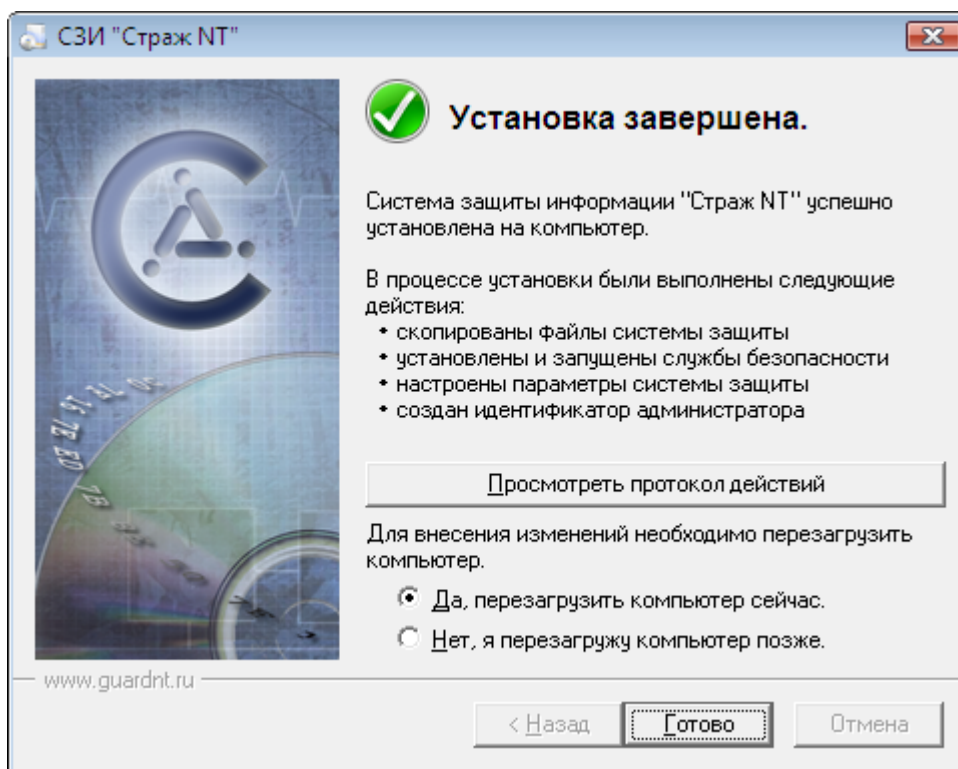
Систему защиты можно устанавливать на такое количество компьютеров, которое указано в формуляре (паспорте). Если количество установок превышает, **Мастер установки** предупредит об этом, и установка системы защиты будет прекращена. В противном случае, программа считывает записанную информацию и добавит к ней информацию о данном компьютере. Если же информация о данном компьютере уже присутствует на предъявленном идентификаторе, **Мастер установки** автоматически определит это и сравнит имена доменов: текущего и записанного на идентификаторе. При их совпадении персональный идентификатор не перезаписывается. В противном случае информация о домене корректируется для данного компьютера и идентификатор перезаписывается.



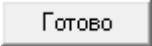
*Если система защиты была ранее установлена на данном компьютере, и после ее снятия имя компьютера было изменено, то при использовании ранее сформированного персонального идентификатора администратора системы защиты количество установок системы защиты уменьшится на одну.*

После формирования персонального идентификатора **Мастер установки** завершается кратким отчетом о произведенных действиях (см. Рис. 11). В случае обнаружения ошибок при установке системы защиты, программа проинформирует об этом с указанием этапа установки, на котором произошла ошибка. В протоколе действий **Мастера установки** содержатся подробные сведения о выполненных в ходе установки действиях, информация о

возникших ошибках, а также их причина. Для просмотра протокола действий необходимо нажать кнопку 



*Рис. 11. Завершение установки.*

Для перехода к этапу первоначальной загрузки операционной системы необходимо перезагрузить компьютер. Компьютер автоматически перегружается, если при нажатии кнопки  была установлена опция перезагрузки. В противном случае необходимо перезагрузить компьютер самостоятельно.



## Вход в систему

Загрузка компьютера с установленной системой защиты информации начинается диалогом, представленным на Рис. 12.

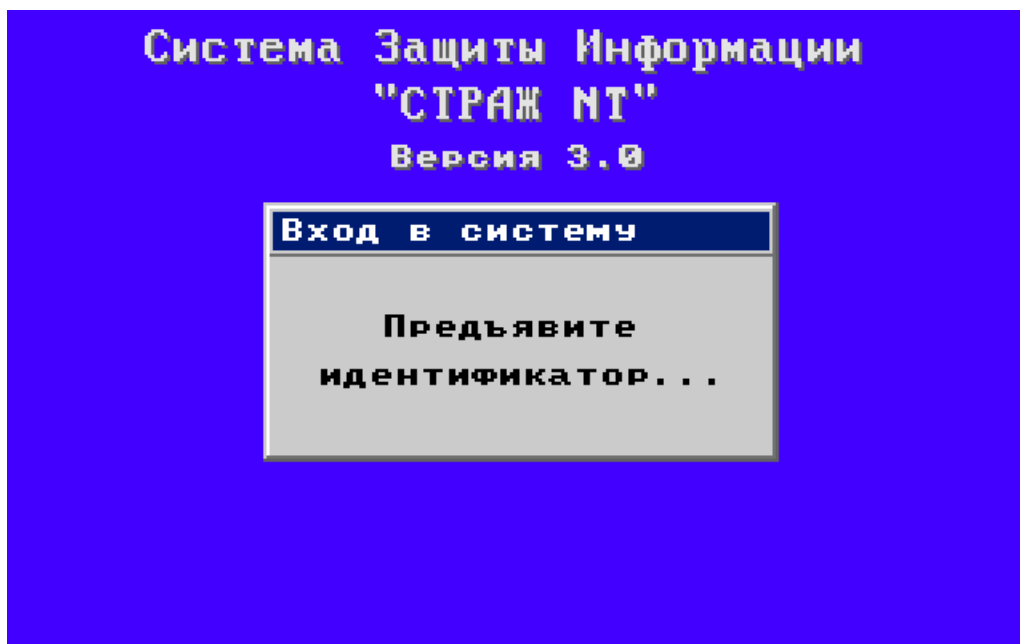


Рис. 12. Окно входа в систему.

Если в BIOS Setup установлена загрузка компьютера с гибкого магнитного диска и в указанном дисководе находится дискета, являющаяся персональным идентификатором, то на экране появляется сообщение, представленное на Рис. 13.

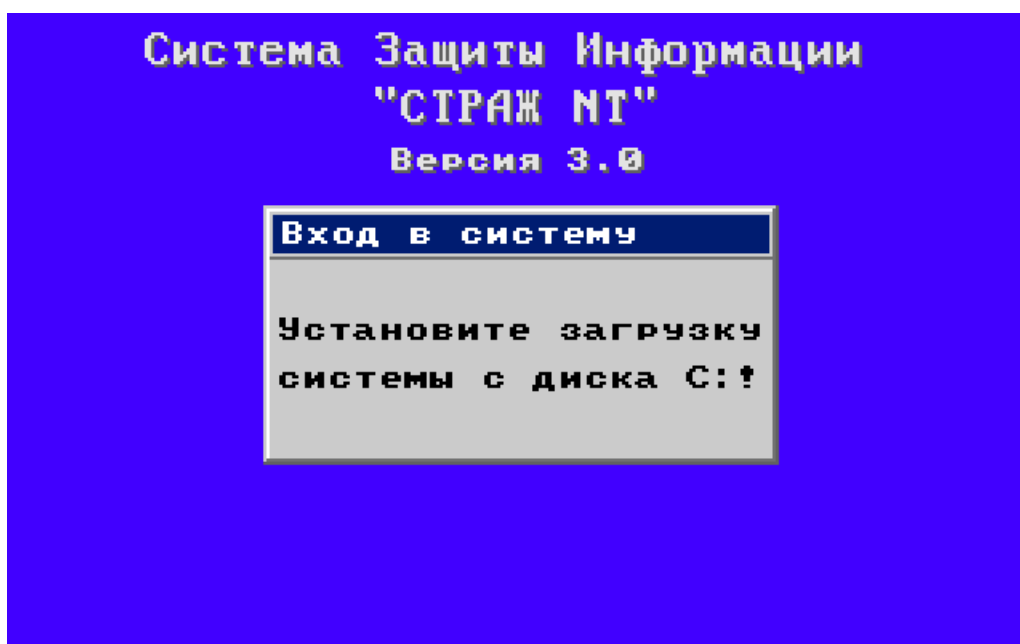
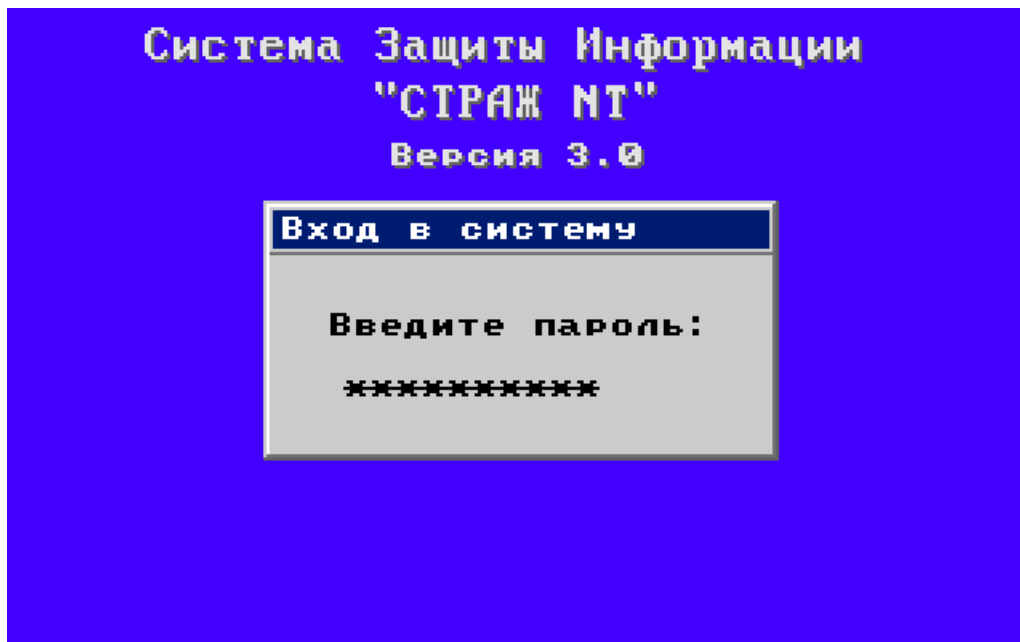


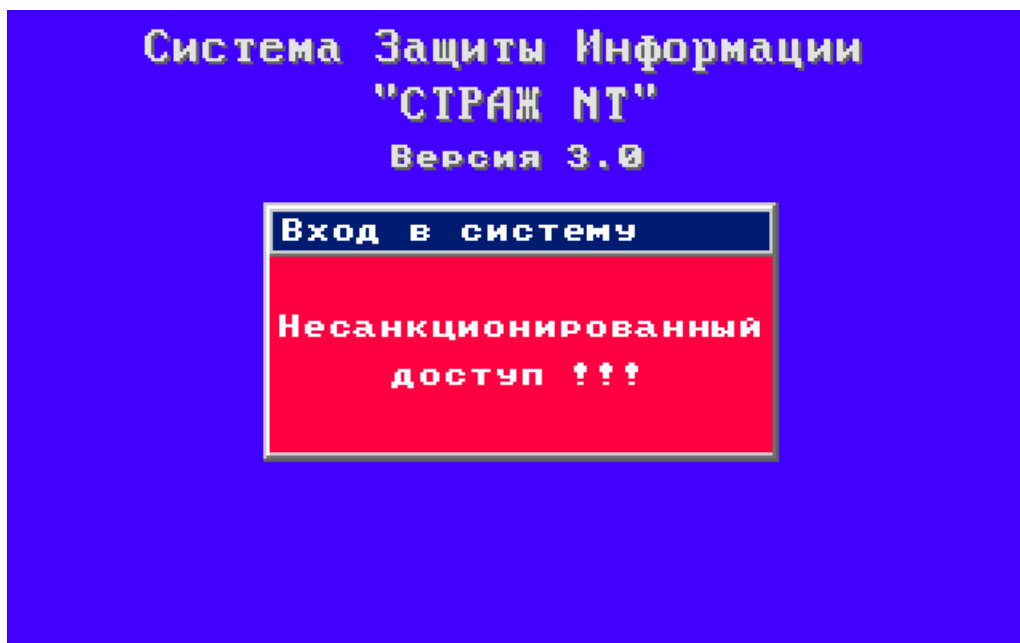
Рис. 13. Предупреждение.

В таком случае необходимо настроить BIOS Setup таким образом, чтобы загрузка компьютера осуществлялась с жесткого диска. Для продолжения загрузки необходимо вставить персональный идентификатор администратора системы защиты и ввести пароль (см. Рис. 14), завершив ввод нажатием клавиши <Enter>.



*Рис. 14. Окно ввода пароля.*

При вводе правильного пароля загрузка компьютера продолжается обычным образом. В противном случае после трех попыток ввода неправильного пароля компьютер блокируется, и на экране появляется сообщение, представленное на Рис. 15.



*Рис. 15. Попытка несанкционированного входа.*

Сообщение сопровождается звуковыми сигналами. При этом происходит регистрация данного события с сохранением значения последнего вводимого пароля. Подробнее о регистрации событий можно узнать в главе [Журнал событий](#). В процессе загрузки вход в систему осуществляется автоматически, используя информацию, записанную в памяти персонального идентификатора входящего пользователя, в данном случае, администратора системы защиты.

### Снятие системы защиты

Снятие СЗИ «Страж NT» может выполнить только пользователь, имеющий привилегии администратора системы защиты. Снятие СЗИ «Страж NT» осуществляется выбором в программном меню пункта **Программы | Страж NT | Снятие системы защиты**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей, при запуске программы на экране появится окно, как показано на Рис. 3. Для продолжения необходимо нажать кнопку . При этом на экране появится диалоговое окно, представленное на Рис. 16.

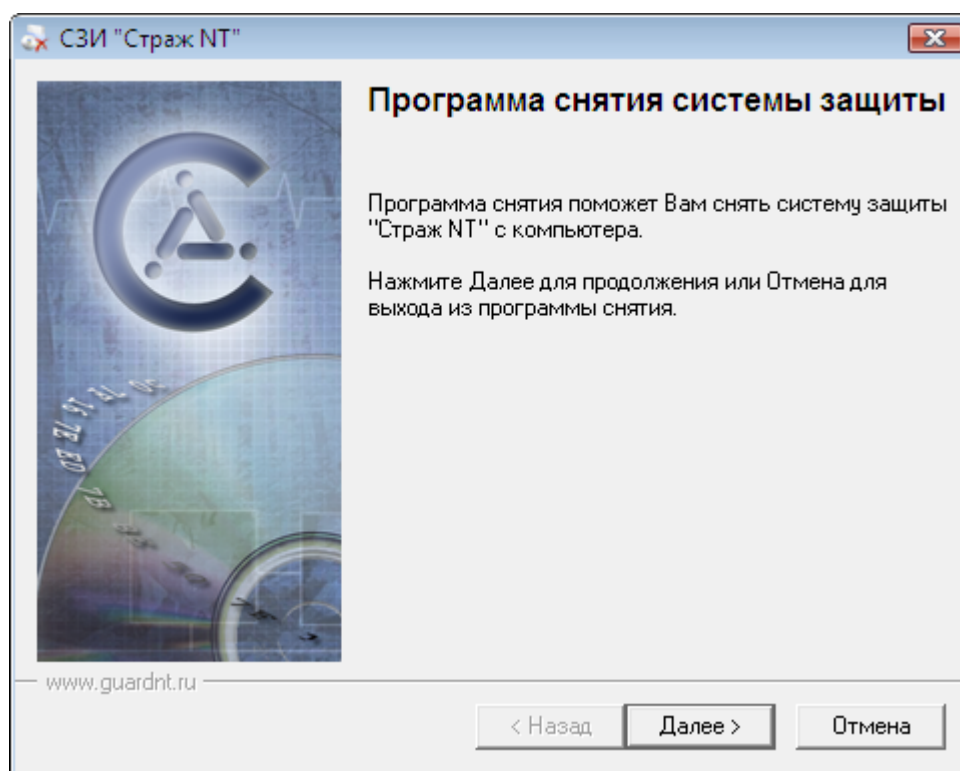
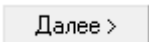
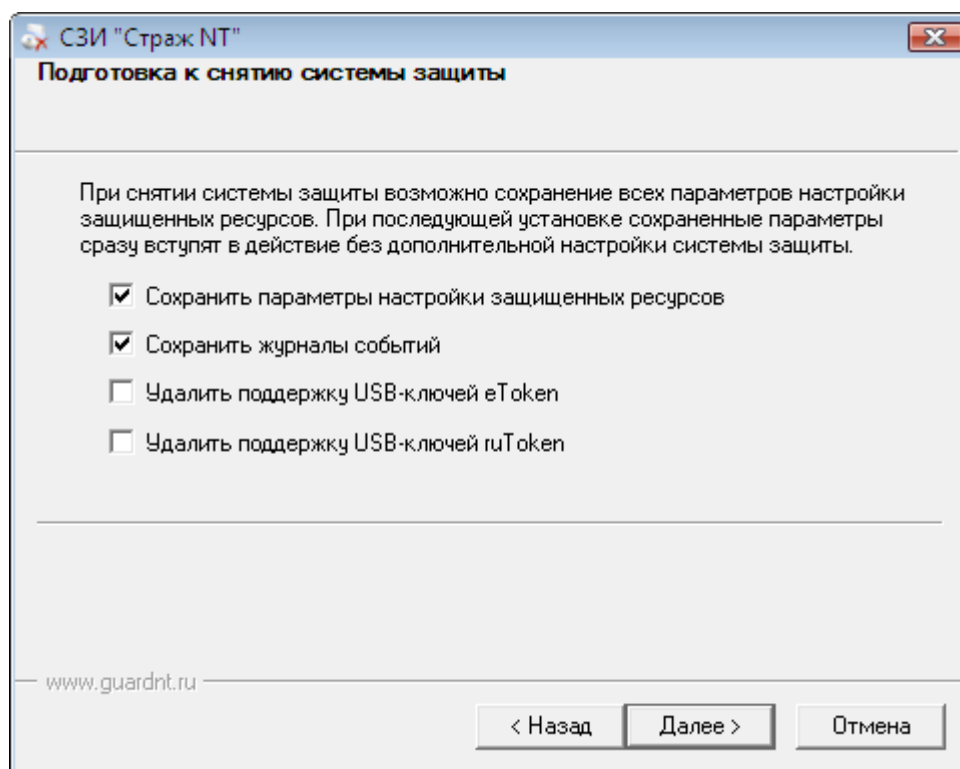


Рис. 16. Начальный диалог Программы снятия системы защиты.

Чтобы прервать выполнение **Программы снятия** необходимо нажать кнопку . Для продолжения снятия системы защиты необходимо нажать кнопку . Если предполагается последующая установка системы защиты на данный компьютер, имеется возможность сохранения всех настроек системы защиты. Для этого необходимо, чтобы

флажок **Сохранить параметры настройки защищенных ресурсов** был установлен, как показано на Рис. 17. В противном случае его необходимо снять. При этом все настройки системы защиты будут удалены. Если необходимо сохранить журналы событий, в том числе и находящиеся в архиве, надо установить флажок **Сохранить журналы событий**. Также, если в дальнейшем на данном компьютере использование USB-ключей eToken и ruToken не предполагается, необходимо удалить их драйвера из системы. Для этого нужно установить флажки **Удалить драйвера USB-ключей eToken** и **Удалить драйвера USB-ключей ruToken**. Для продолжения снятия системы защиты необходимо нажать кнопку .

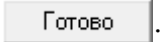


*Рис. 17. Подготовка к снятию системы защиты.*

После снятия системы защиты, если был выбран режим сохранения настроек, некоторые файлы системы защиты, а также специальные локальные группы удалены не будут. Если система защиты использовалась на компьютере, который входит в домен, специальные глобальные группы при снятии системы защиты удалены не будут. После снятия СЗИ со всех компьютеров, входящих в домен, в том числе и с контроллера домена, при необходимости глобальные группы GAdmins, GLevel1, GLevel2 удаляются самостоятельно штатными средствами операционной системы.



Если при снятии системы защиты был выбран режим сохранения настроек, самостоятельно не удаляйте специальную локальную группу GAdmins. Это может привести к некорректной работе системы защиты при последующей установке.

После снятия СЗИ «Страж NT» рекомендуется перезагрузить компьютер (см. Рис. 18). Для этого необходимо выбрать соответствующий флажок и нажать кнопку .

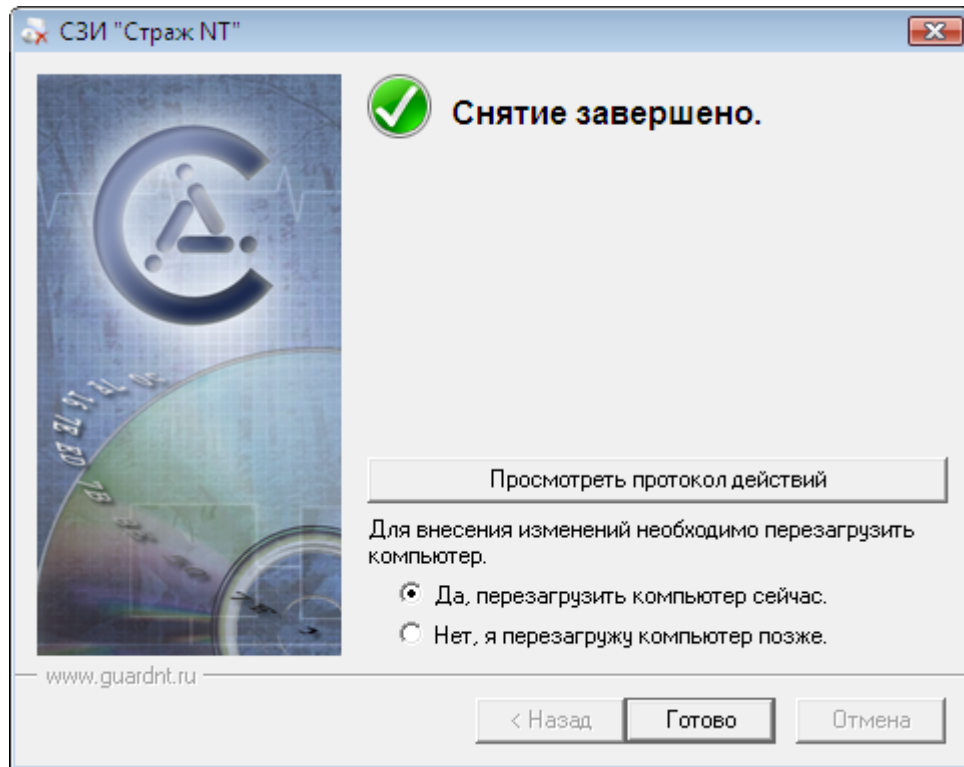


Рис. 18. Завершение Программы снятия.

### Ситуации, возникающие при входе в систему

Ниже описаны ситуации, которые могут возникнуть при входе в систему. Рассматриваются как причины возникших ситуаций, так и необходимые действия для их преодоления. В случае возникновения ситуаций, не описанных ниже, следует обратиться к разделу [Рекомендации при возникновении внештатных ситуаций](#).

При включении компьютера сразу появляется надпись «Введите пароль:»

<b>Причина</b>	В дисковод ГМД вставлена дискета, являющаяся персональным идентификатором, которая уже была считана.
<b>Действия</b>	Вам следует продолжить вход в систему, т. е. ввести пароль.

*При включении компьютера сразу появляется надпись «Установите загрузку системы с диска С:»*

<b>Причина</b>	Компьютер пытается загрузить систему с дискеты, вставленной в один из дисководов ГМД.
<b>Действия</b>	Необходимо предъявлять идентификатор после запроса, показанного на Рис. 12. Рекомендуется изменить порядок загрузки операционной системы таким образом, чтобы первым загрузочным устройством должен быть жесткий диск.

*Надпись «Предъявите идентификатор...» не мигает или отсутствует на экране*

<b>Причина</b>	Одно из устройств, подключенное к USB-порту, не отвечает на запрос.
<b>Действия</b>	Необходимо либо выключить устройство, либо предъявлять идентификатор до появления запроса, показанного на Рис. 12.

### **Рекомендации при возникновении внештатных ситуаций**

В данном разделе описаны действия администратора системы защиты в случае возникновения внештатных ситуаций. Также описан механизм аварийного снятия системы защиты. При возникновении ситуаций, не описанных в данном разделе, рекомендуется обратиться в службу технической поддержки.

#### **При установке и снятии системы защиты**

В процессе установки и снятия системы защиты ведется подробный протокол действий, выполняемых программой, который находится в папке временных файлов текущего пользователя %Temp% и называется **GInstall.log**. Если данный файл уже существует, записи дописываются в его конец. Запись в протоколе действия содержит дату, время и описание выполняемого действия. Если при выполнении какого-либо действия произошла ошибка, в протокол действий будет добавлена соответствующая запись с описанием ошибки. Пример протокола действий с записью об ошибке приведен на Рис. 19.

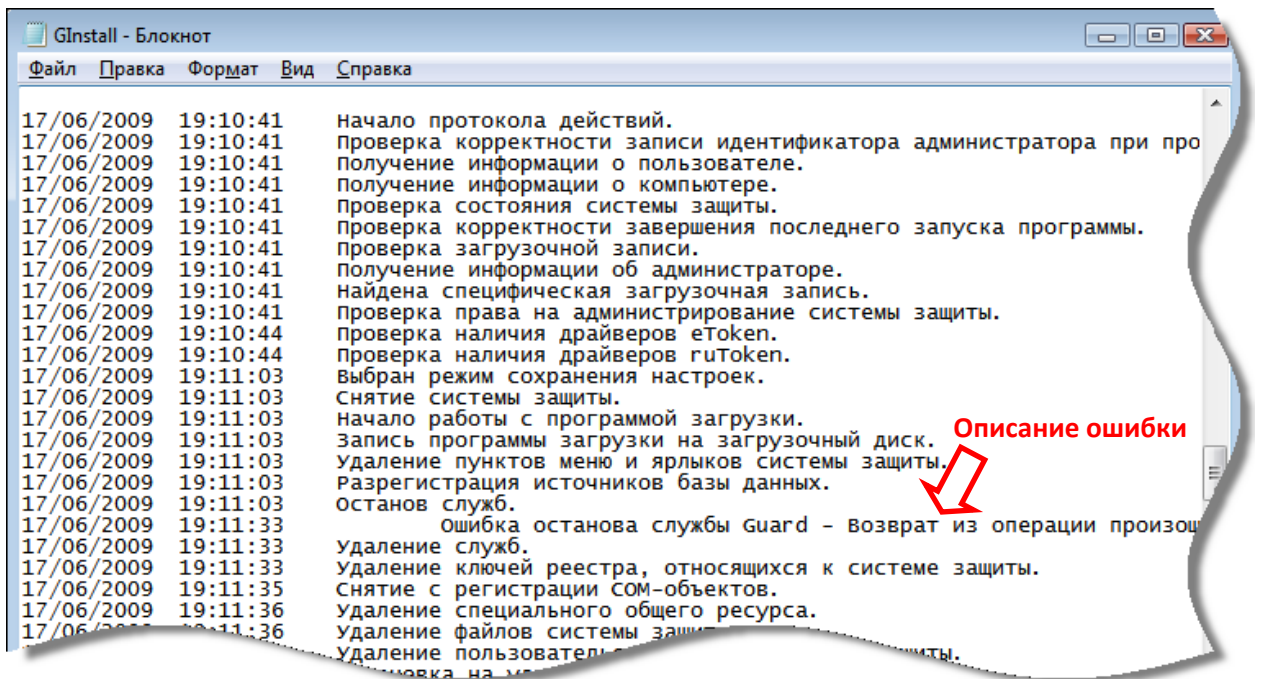
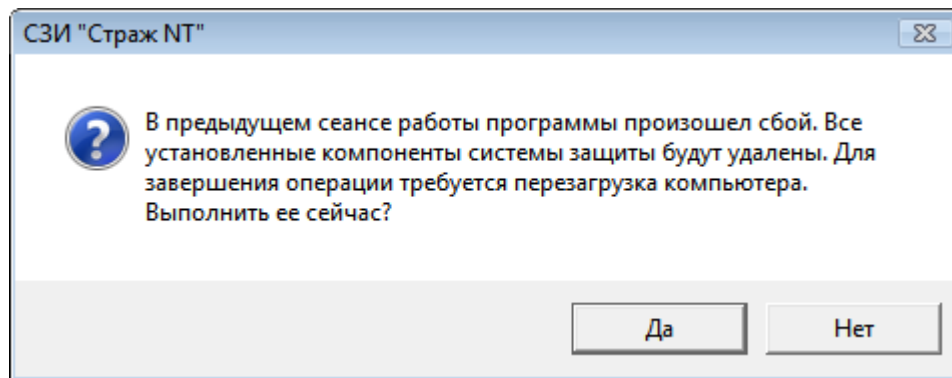


Рис. 19. Пример протокола действий.

Анализ протокола действий в большинстве случаев позволяет администратору системы защиты самостоятельно устранить причину, из-за которой возникает ошибка. В случае невозможности самостоятельного решения проблемы рекомендуется обратиться в службу технической поддержки, с указанием действия, при выполнении которого произошла ошибка и ее описания.

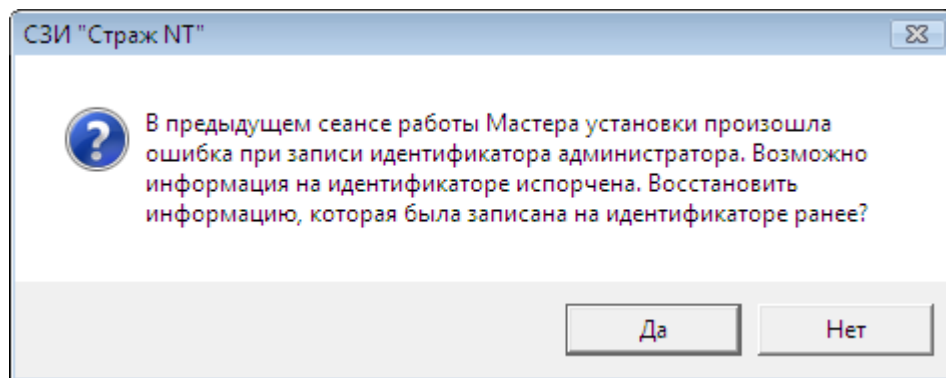
В процессе установки и снятия системы защиты возможно возникновение внештатных ситуаций, таких, например, как внезапное отключение электропитания. При этом выполняемые процессы останутся незавершенными. Некоторые из них, например, регистрация служб системы защиты или установка подсистемы идентификации, весьма критичны для работоспособности всей системы.

При возникновении сбоя необходимо осуществить попытку загрузки операционной системы компьютера. После загрузки ОС необходимо заново запустить **Мастер установки**, который определит, что во время прошлого запуска произошел сбой, последовательно удалит все компоненты системы защиты и выдаст запрос на перезагрузку (см. Рис. 20). То же самое произойдет при сбое выполнения **Программы снятия**.



*Рис. 20. Сбой при установке/снятии системы защиты.*

Существует вероятность аппаратного отказа при формировании персонального идентификатора администратора системы защиты. Если на нем была записана информация о других компьютерах, существует риск для этих компьютеров потерять персональный идентификатор администратора системы защиты. Поэтому до формирования персонального идентификатора администратора информация с него резервируется. В случае успешного формирования, резервная информация уничтожается, в случае же сбоя – остается на компьютере. Для восстановления персонального идентификатора администратора системы защиты необходимо заново запустить **Мастер установки**, который обнаружит резервную информацию и предложит записать ее на идентификатор (см. Рис. 21).



*Рис. 21. Процедура восстановления персонального идентификатора.*

Если же на предъявленном идентификаторе уже записана какая-то информация, **Мастер установки** предупредит об этом. После этого программа последовательно удалит все компоненты системы защиты и выдаст запрос на перезагрузку (см. Рис. 20).

#### **При загрузке операционной системы**

В редких случаях загрузка операционной системы приводит к отказу с отображением экрана стоп-ошибки или так называемого «синего экрана смерти» (BSOD), пример которого показан на Рис. 22.



```
A problem has been detected and windows has been shut down to prevent damage to your computer.
```

```
If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:
```

```
Check for viruses on your computer. Remove any newly installed hard drives or hard drive controllers. Check your hard drive to make sure it is properly configured and terminated. Run CHKDSK /F to check for hard drive corruption, and then restart your computer.
```

```
Technical information:
```

```
*** STOP: 0x0000007B (0x80399BB0, 0xC0000034, 0x00000000, 0x00000000)
```

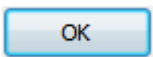


Код ошибки

Рис. 22. Пример «синего экрана смерти».

При возникновении подобной ситуации необходимо сделать еще одну попытку загрузить операционную систему. В случае очередной неудачи необходимо запомнить или записать код ошибки (см. Рис. 22) и произвести аварийное снятие системы защиты, как описано в следующем разделе. Код ошибки и, возможно, дампы памяти необходимы специалистам службы технической поддержки для локализации и устранения причин, приводящих к отказу операционной системы.

Если в процессе загрузки операционной системы происходит автоматическая перезагрузка или экран стоп-ошибки отображается очень короткое время, необходимо выполнить следующие действия:

- Выполнить аварийное снятие системы защиты.
- Загрузить операционную систему под администратором системы защиты.
- Вызвать окно свойств системы, выбрать вкладку **Дополнительно** и нажать кнопку **Параметры...** в группе **Загрузка и восстановление**.
- Снять флажок **Выполнить автоматическую перезагрузку** (см. Рис. 23) и нажать кнопку .
- Восстановить подсистему идентификации системы защиты и осуществить попытку загрузки операционной системы.

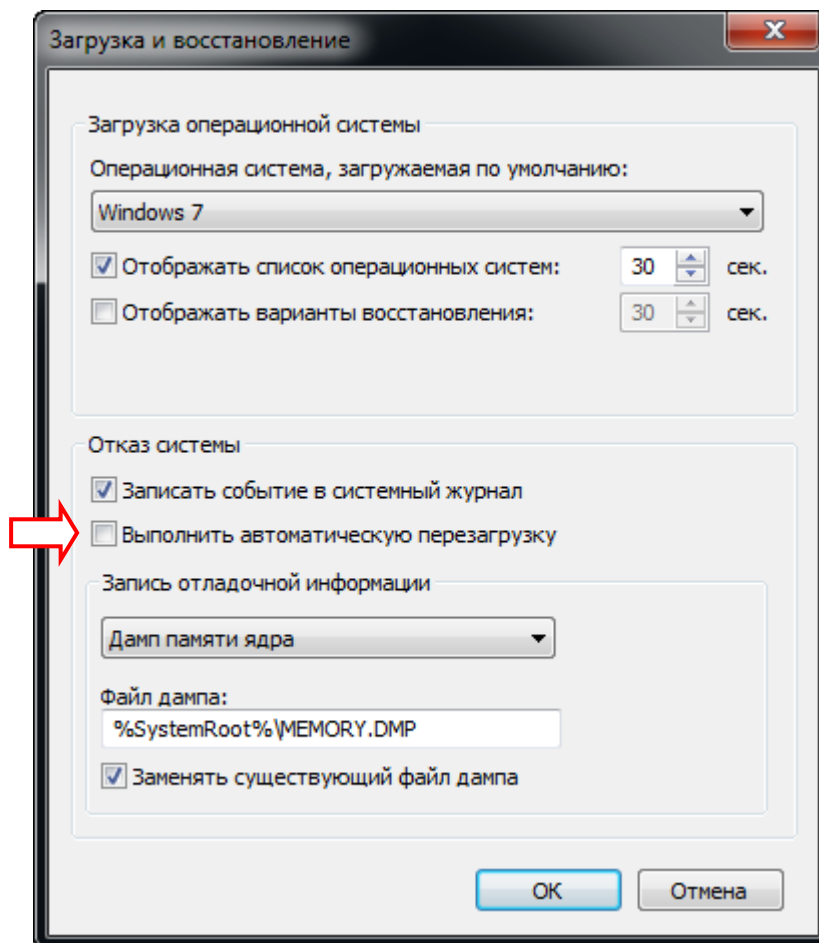


Рис. 23. Параметры загрузки и восстановления системы.

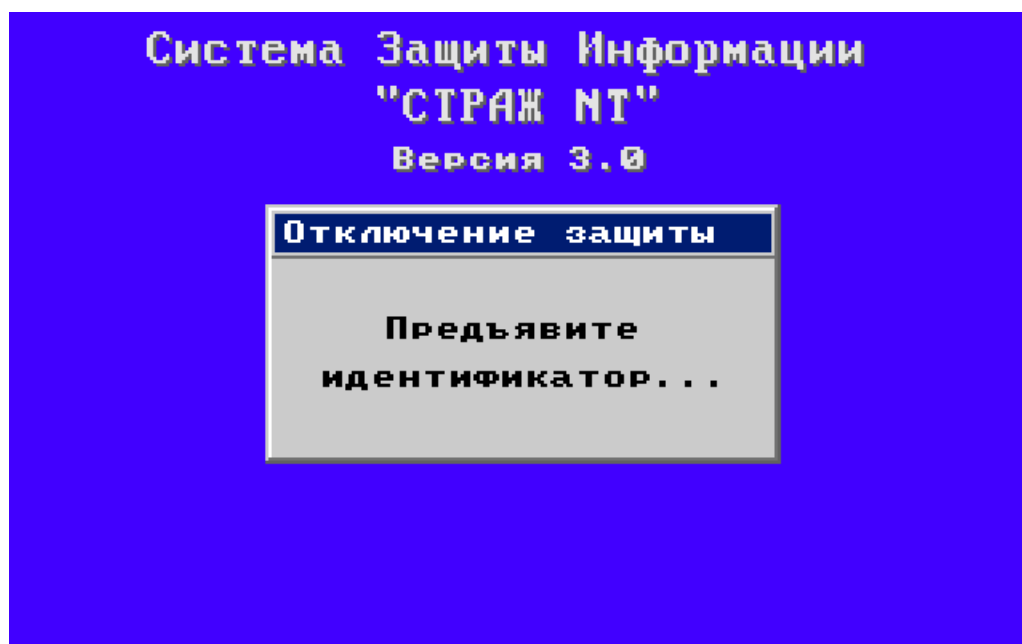
После выполнения вышеуказанных действий при отказе система не будет автоматически перезагружаться и даст возможность зафиксировать код ошибки.

#### Аварийное снятие системы защиты

Механизмы аварийного снятия системы защиты предназначены для отключения подсистемы идентификации и основных служб СЗИ. Для выполнения аварийного снятия системы защиты необходимо в BIOS Setup компьютера установить принудительную загрузку с носителя информации, на котором поставляется установочный комплект системы защиты. После появления диалога, приведенного на Рис. 24, необходимо предъявить персональный идентификатор администратора системы защиты и ввести его пароль. После появления сообщения об отключении системы защиты следует перезагрузить компьютер. Загрузка операционной системы будет выполняться в обычном режиме без процедуры идентификации.

После загрузки операционной системы и выяснения причины отказа необходимо либо снять систему защиты штатным образом, как описано в разделе [Снятие системы защиты](#), либо восстановить подсистему идентификации и работоспособность основных служб

системы защиты, повторно загрузившись с носителя информации, на котором поставляется установочный комплект системы защиты.



*Рис. 24. Аварийное снятие системы защиты информации.*

# Настройка системы защиты

В данной главе приводятся сведения о назначении и применении программы **Настройка системы защиты**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при настройке замкнутой программной среды и применении шаблонов настроек.

Программа **Настройка системы защиты** предназначена для установки параметров системы защиты информации, а также для создания замкнутой программной среды, применения шаблонов настроек и других сервисных функций.

Программа **Настройка системы защиты** запускается при выборе администратором системы защиты в программном меню пункта **Программы | Страж NT | Настройка системы защиты**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей, при запуске программы на экране появится окно, как показано на Рис. 25. Для продолжения необходимо нажать кнопку

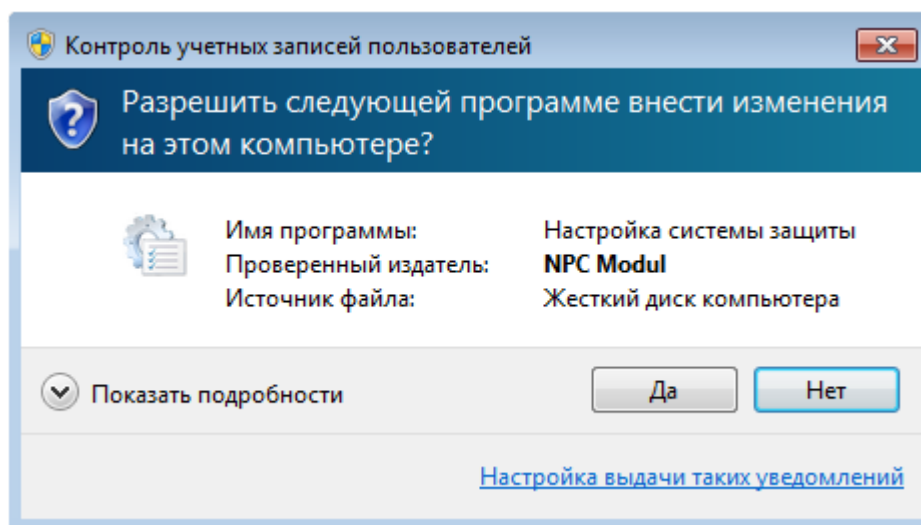


Рис. 25. Сообщение подсистемы контроля учетных записей пользователей.

При этом на экране появляется диалоговое окно, как показано на Рис. 26. При выборе пунктов, представленных в виде дерева в левой части окна, в правой части появляется диалог, содержащий соответствующие группы настроек системы защиты. Все настройки применяются при нажатии кнопки  или , за исключением групп **Замкнутая программная среда** и **Шаблоны настроек**. Подробные сведения об этих группах приводятся далее в соответствующих разделах.

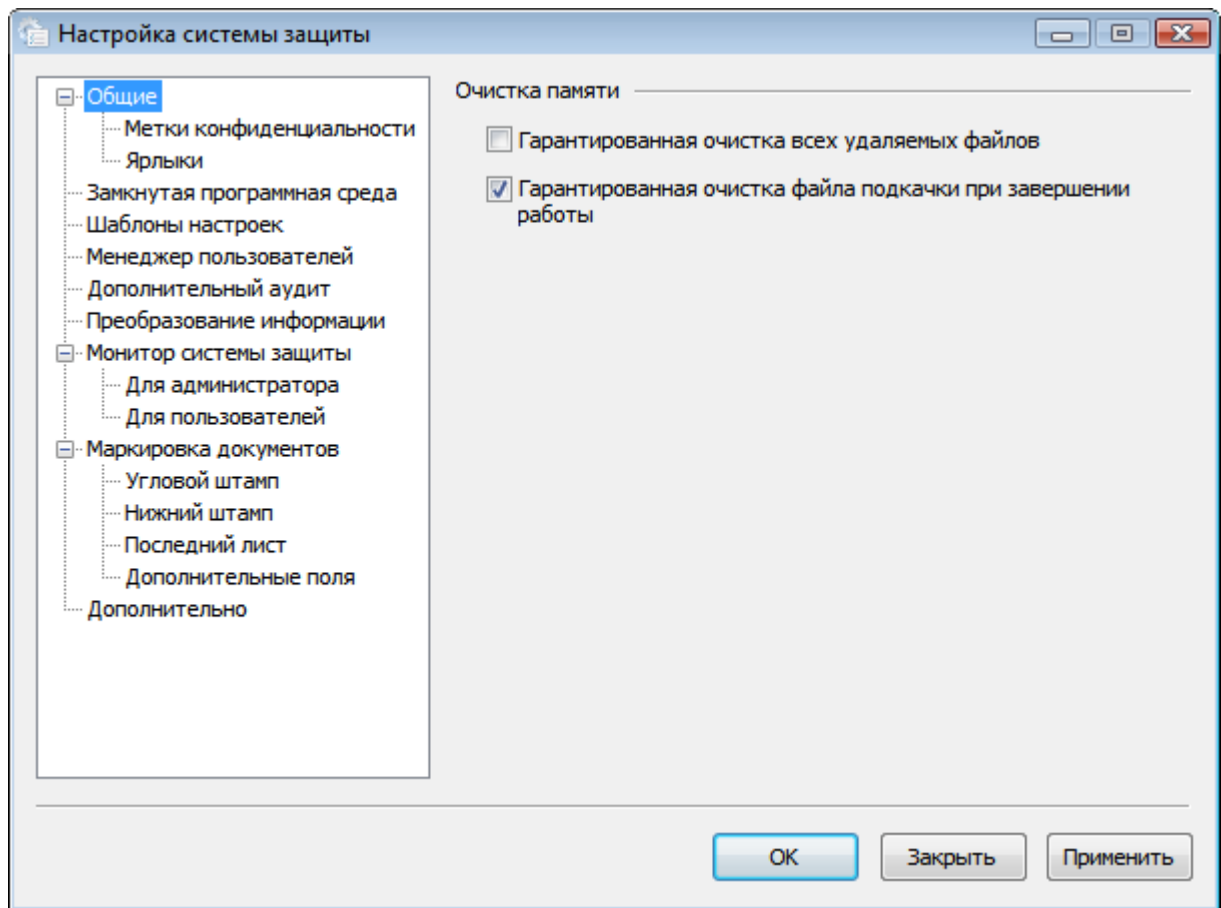


Рис. 26. Общий вид окна программы Настройка системы защиты.

### Общие настройки

Установка флажка **Гарантированная очистка всех удаляемых файлов** означает, что все удаляемые файлы в системе перед удалением будут заполняться случайной последовательностью байтов. По умолчанию данный режим действует только при удалении файлов, имеющих гриф выше «Несекретно».



*Установка флажка **Гарантированная очистка всех удаляемых файлов** может привести к снижению производительности системы при выполнении большого количества файловых операций.*

Установка флажка **Гарантированная очистка файла подкачки при завершении работы** означает, что при выключении (перезагрузке) компьютера файл подкачки **pagefile.sys**, а также **hyperfil.sys** будет заполняться случайной последовательностью байтов.



*Установка флажка **Гарантированная очистка файла подкачки при завершении работы** увеличивает период времени выключения (перезагрузки) компьютера из-за достаточно большого объема указанных файлов.*

## Метки конфиденциальности

Названия меток конфиденциальности используются для обозначения уровней конфиденциальности (грифов) защищаемых ресурсов, а также для обозначения уровней допуска программ и пользователей. По умолчанию названия меток конфиденциальности имеют следующие значения: «Несекретно», «Секретно» и «Сов.секретно».

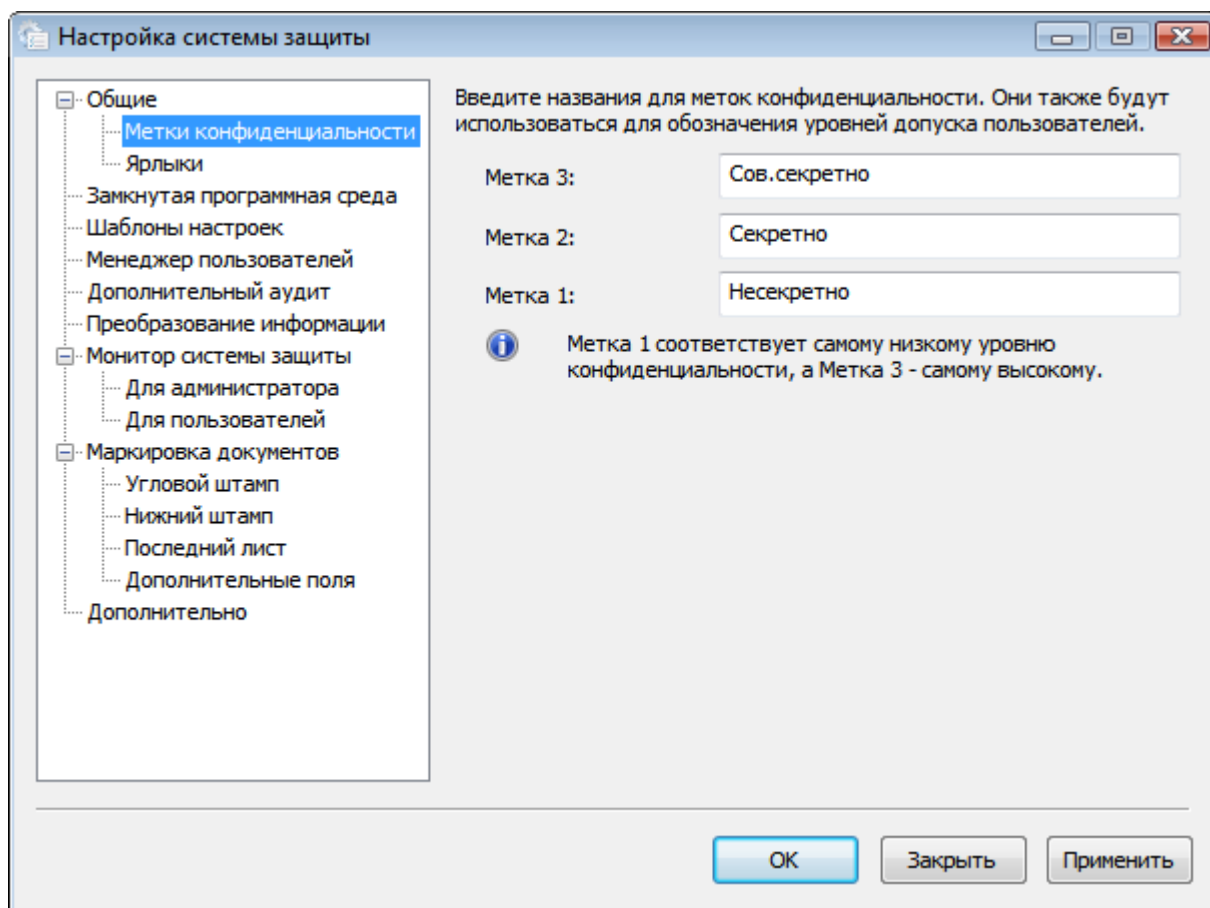


Рис. 27. Настройка названий меток конфиденциальности.



Метка 1 соответствует самому низкому уровню конфиденциальности в иерархической классификации, а Метка 3 – самому высокому.

## Ярлыки

Для создания на рабочем столе администратора ярлыков программ, входящих в состав системы защиты, необходимо установить необходимые флажки. Для программы **Менеджер файлов** существует возможность создания ярлыка на общем рабочем столе всех пользователей. Для этого необходимо установить флажок **Для всех пользователей**. Для одновременной установки всех флажков необходимо нажать кнопку

При отображении данной группы настроек наличие установленных флажков программ означает, что для данных программ ярлыки на рабочем столе уже существуют. Для удаления этих ярлыков необходимо снять соответствующие флажки.

Если группа ярлыков в программном меню или отдельные ее элементы по какой-то причине отсутствуют, для ее восстановления необходимо установить флажок **Восстановить группу ярлыков в программном меню**.

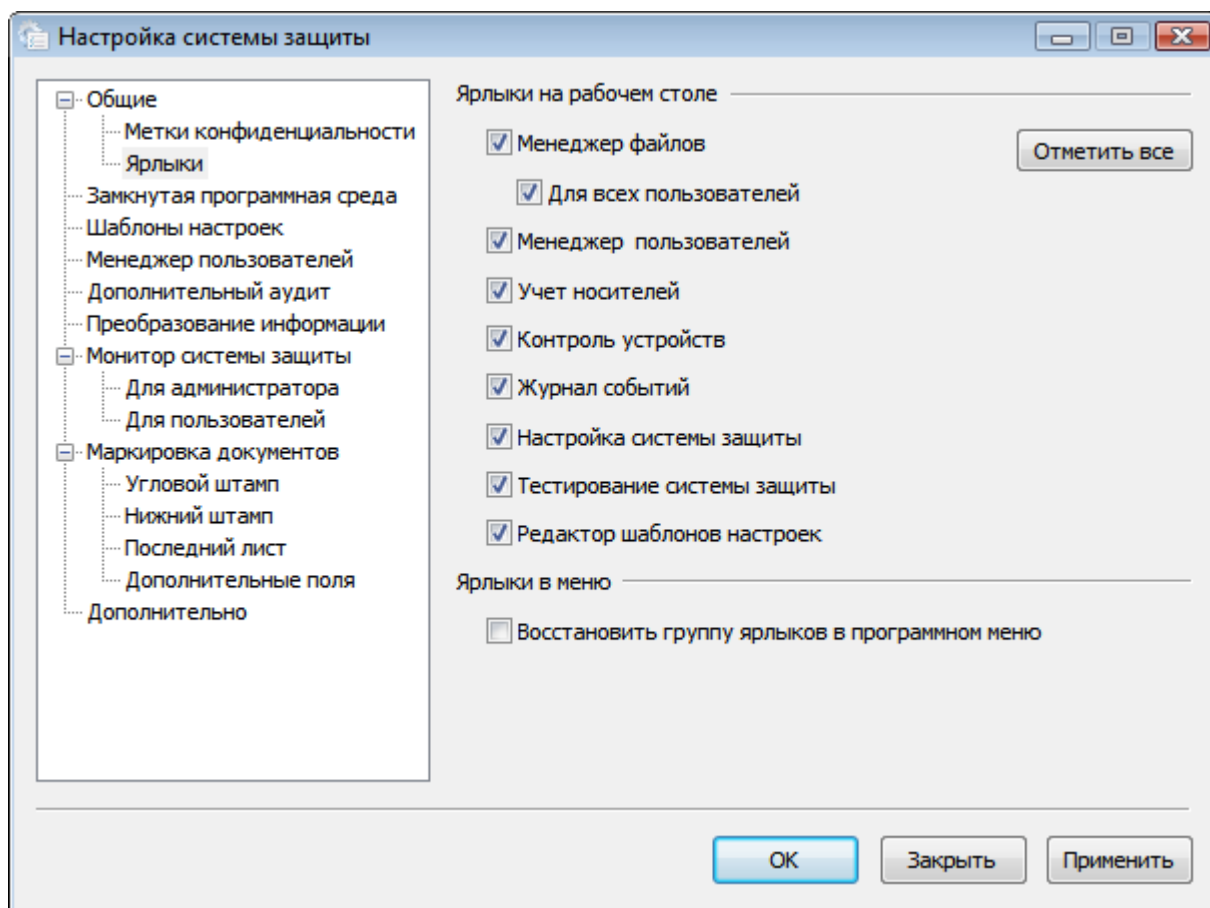


Рис. 28. Настройка ярлыков программ системы защиты.

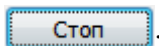
### Замкнутая программная среда

Для запуска механизмов настройки замкнутой программной среды необходимо выбрать папки (или весь компьютер), где будет проводиться поиск и настройка исполняемых файлов, и нажать кнопку **Настроить**. При этом первым шагом анализируются все файлы в выбранных папках на возможность их выполнения в системе. Вторым шагом на все найденные исполняемые файлы, кроме нижеследующих исключений, устанавливается режим запуска «Приложение». Исключениями являются:

- исполняемые файлы в папке `%SystemRoot%\Installer`;

- файл `%SystemRoot%\system32\msiexec.exe` – на него устанавливается режим запуска «Инсталлятор»;
- все файлы с расширениями `msi` и `msp` – на них устанавливается режим запуска «Инсталлятор».

Процесс создания замкнутой программной среды можно остановить, нажав кнопку



В некоторых случаях в 32-х разрядных ОС стандартные механизмы анализа исполняемых файлов не распознают исполняемый файл. Это происходит в случаях, если программа написана для работы под управлением операционной системы MS-DOS или имеет нестандартный PE-заголовок. Чтобы на такие файлы устанавливался режим запуска, необходимо перед нажатием кнопки **Настроить** установить флажок **Поддержка старых форматов**.

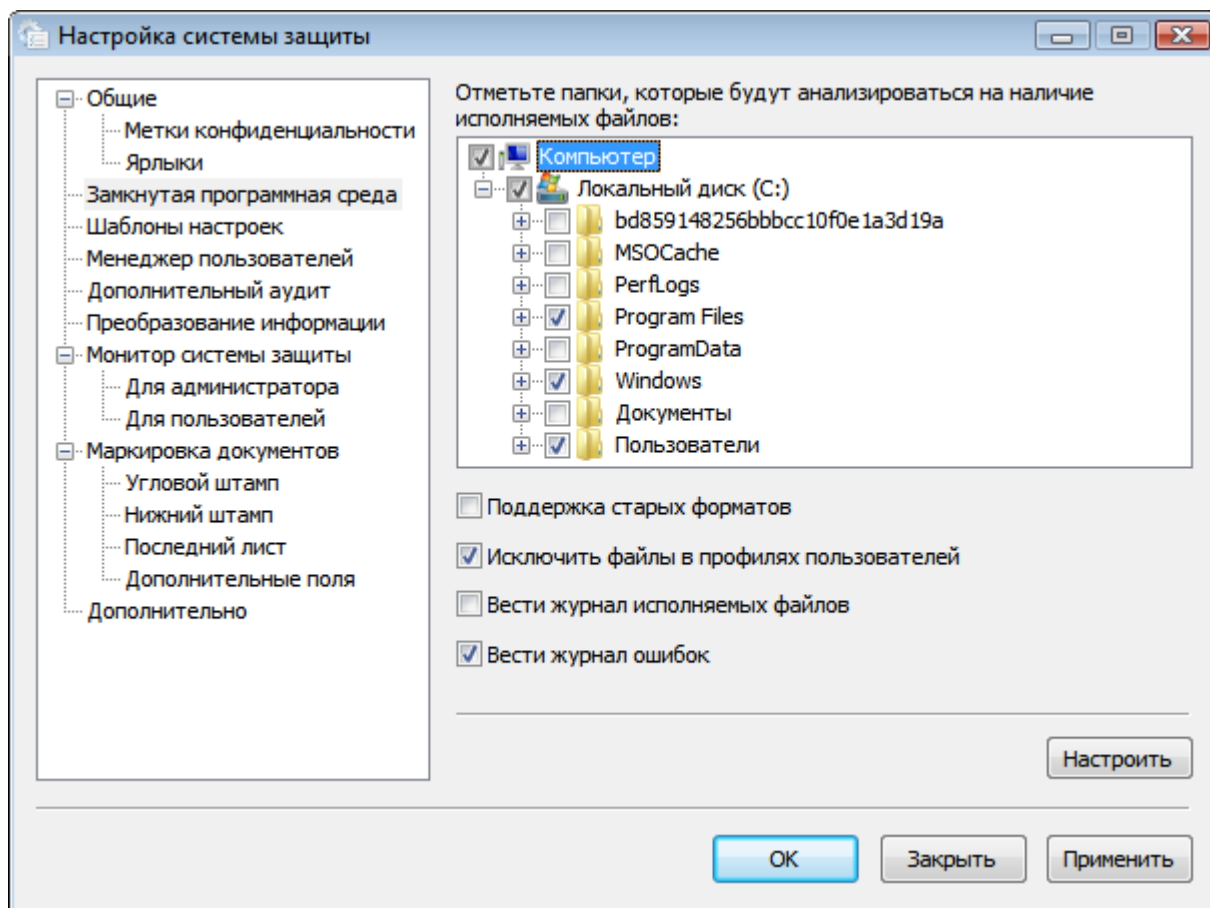
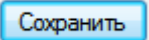


Рис. 29. Настройка замкнутой программной среды.

Установка флажка **Исключить файлы в профилях пользователей** означает, что на исполняемые файлы, находящиеся в папках профилей пользователей (например, папки `Desktop`, `%Temp%`), не будет устанавливаться режим запуска.

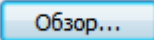
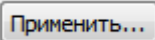
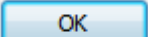


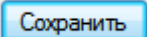
Установка флажка **Вести журнал исполняемых файлов** означает, после настройки замкнутой программной среды администратору будет предложено сохранить список файлов, на которые был установлен режим запуска. Список исполняемых файлов сохраняется в обычный текстовый документ.

Установка флажка **Вести журнал ошибок** означает, что если в процессе настройки замкнутой программной среды возникали ошибки доступа к файлам, после его окончания на экране появится диалог со списком файлов, при настройке которых произошла ошибка с ее описанием. Для сохранения списка ошибок необходимо нажать кнопку . Список ошибок сохраняется в обычный текстовый документ.

### Шаблоны настроек

В связи с тем, что современные пакеты прикладных программ имеют сложную структуру, их настройка, особенно для обработки конфиденциальной информации, занимает много времени, если выполнять ее вручную. Также много времени уходит на анализ работы таких пакетов программ. Для автоматизации этого процесса используются шаблоны настроек. Шаблон настроек представляет собой набор правил и защитных атрибутов для папок и файлов, входящих в состав пакета прикладных программ (см. главу [Редактор шаблонов настроек](#)).

Для получения списка доступных шаблонов необходимо выбрать папку, в которой находятся содержащие их файлы, нажав кнопку . Для применения шаблона необходимо его выбрать в списке и нажать кнопку . При этом на экране может появиться диалог (см. Рис. 31) со списком пользователей, для которых уже сформированы профили. Необходимо выбрать пользователей, для которых будет применен профиль, и нажать кнопку .

Если в процессе применения шаблона возникали ошибки доступа к файлам, после его окончания на экране появится диалог со списком файлов, при доступе к которым произошла ошибка с ее описанием. Для сохранения списка ошибок необходимо нажать кнопку . Список ошибок сохраняется в обычный текстовый документ.

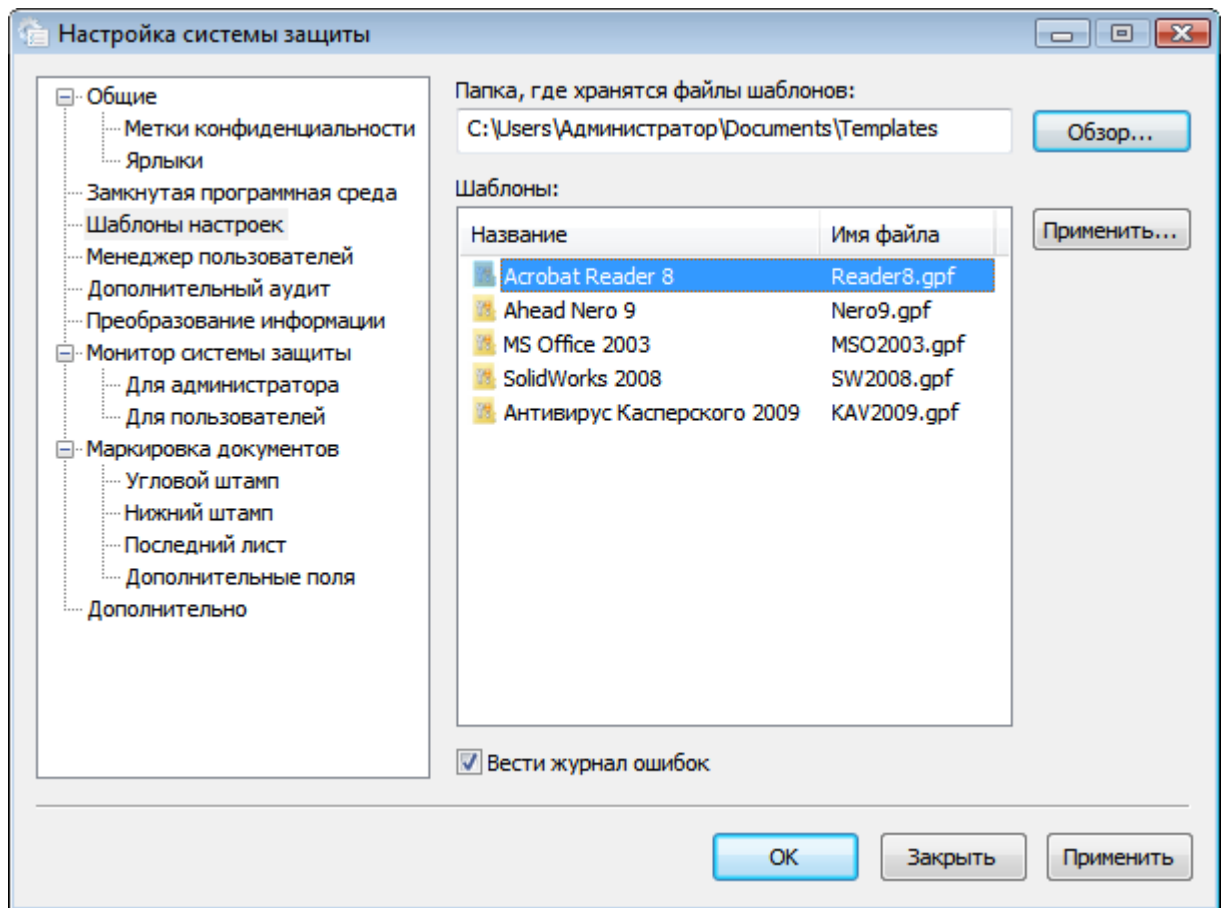


Рис. 30. Применение шаблонов.

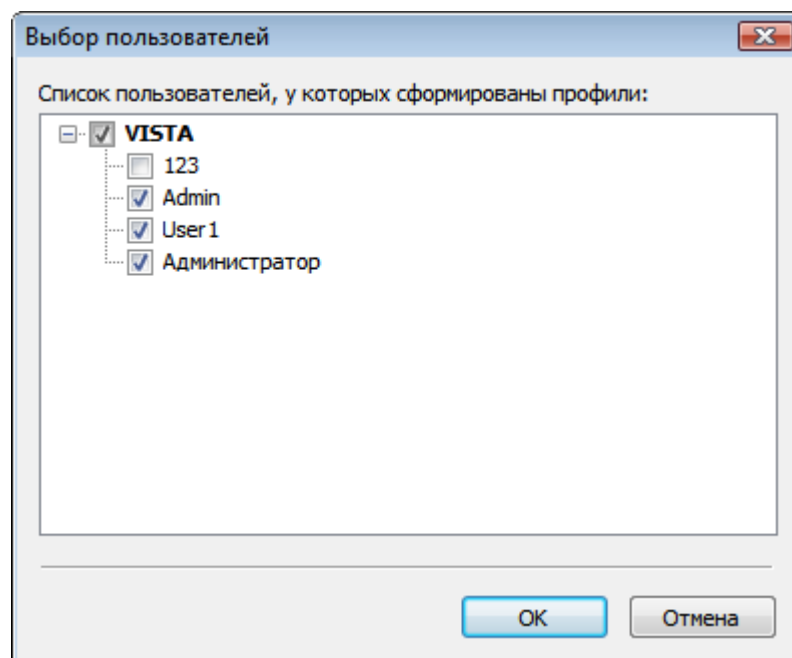


Рис. 31. Выбор пользователей для применения шаблона.

## Менеджер пользователей

По умолчанию база данных локальных пользователей компьютера находится в папке %SystemRoot%\Guard данного компьютера, а база данных доменных пользователей – в папке %SystemRoot%\Guard контроллера домена. При необходимости, например, для централизованного хранения баз, можно изменить место расположения баз данных пользователей. Для этого необходимо нажать кнопку **Задается пользователем** и ввести полный путь к папке, где будут располагаться файлы баз данных пользователей либо выбрать ее, нажав кнопку **Обзор...**.



*Папка расположения файлов баз данных пользователей должна существовать на момент запуска программы **Менеджер пользователей**.*

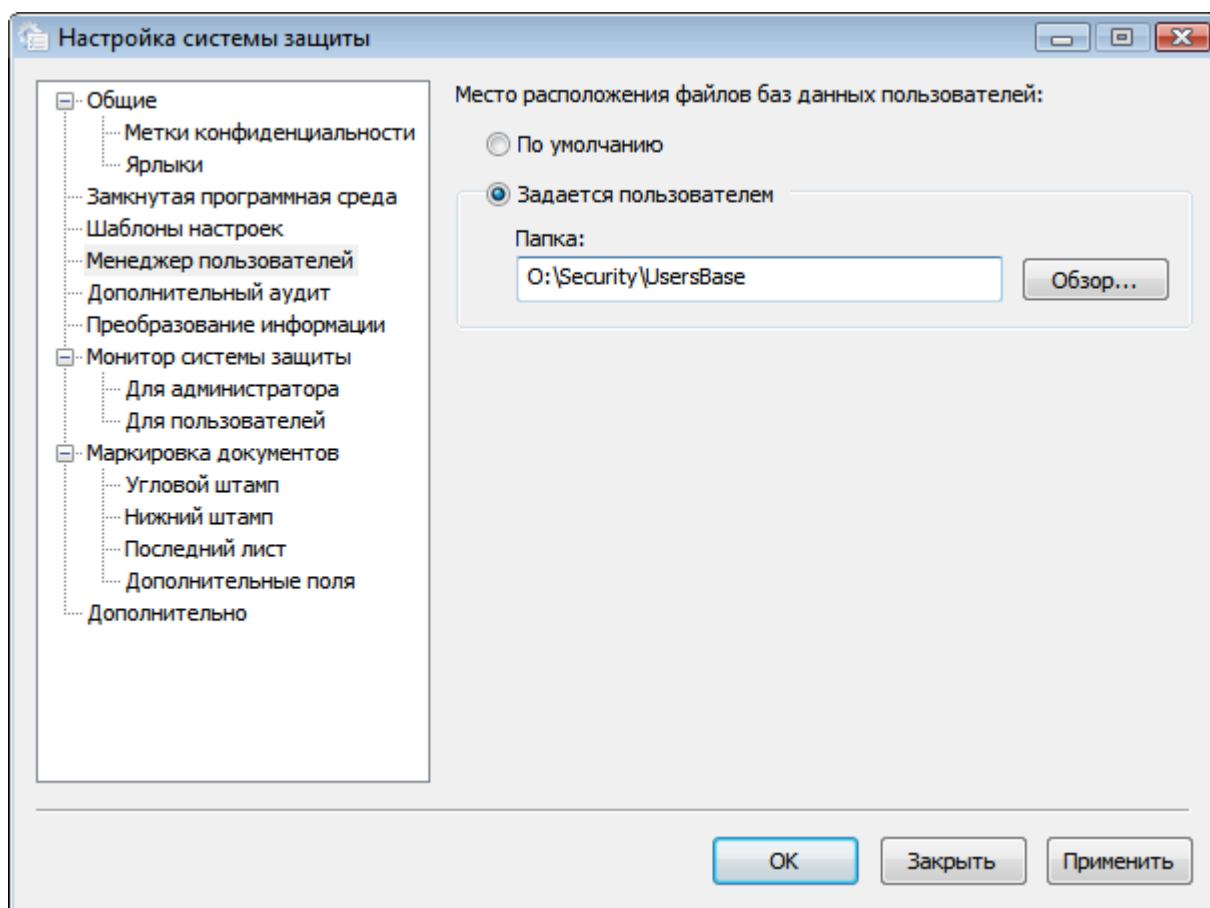


Рис. 32. Настройка параметров программы Менеджер пользователей.

## Дополнительный аудит

Параметры дополнительного аудита определяют события, которые будут регистрироваться в журнале событий для ресурсов, у которых включен дополнительный аудит, а также для всех конфиденциальных ресурсов. Могут регистрироваться как успешные события, так и

события отказа. Чтобы событие регистрировалось необходимо, чтобы флажок, соответствующий данному событию, был установлен.

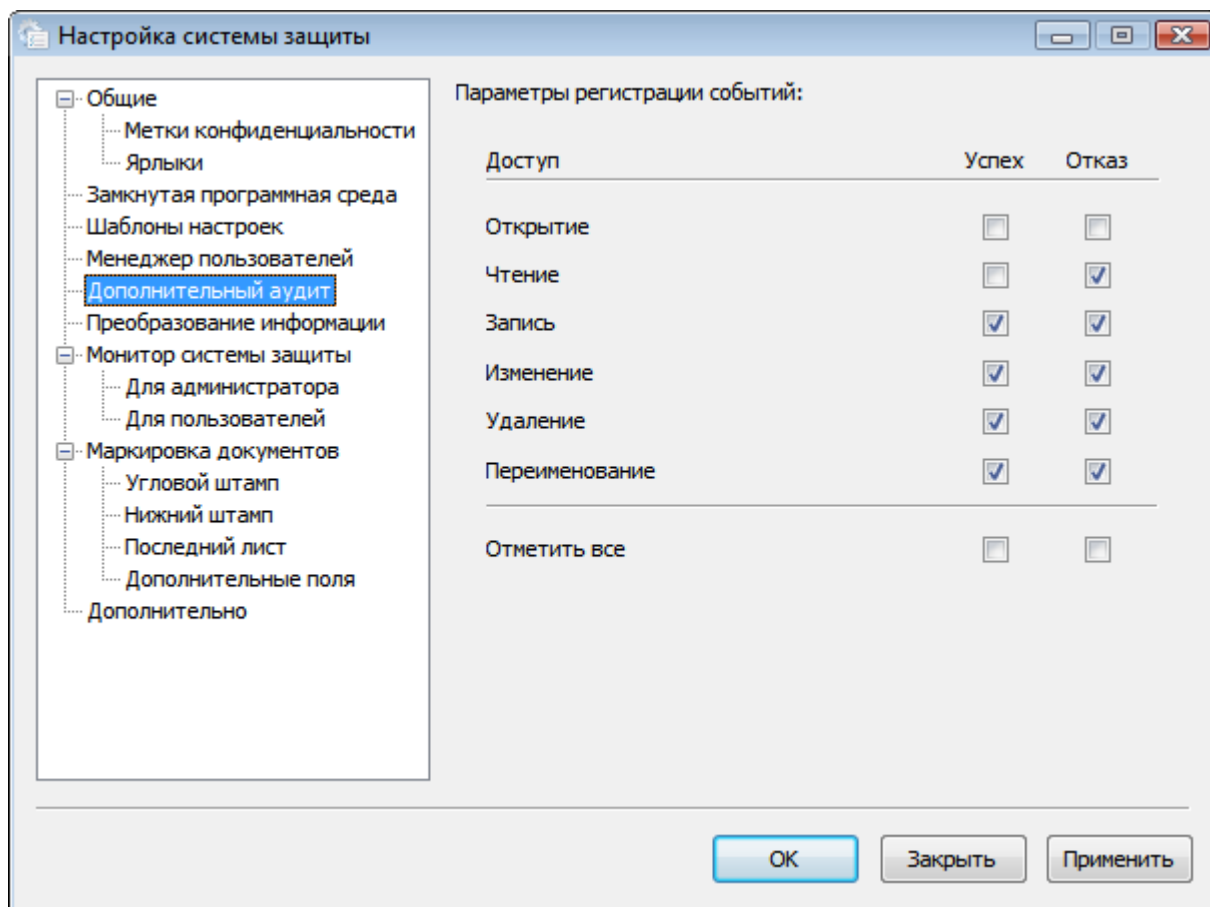


Рис. 33. Настройка параметров дополнительного аудита.

### Преобразование информации

Информация, записываемая на отчуждаемые носители информации, при необходимости, может быть преобразована. При включении режима преобразования, информация, записываемая на отчуждаемые носители, преобразуется на рабочем ключе компьютера либо на главном ключе. При считывании информации с отчуждаемых носителей информация восстанавливается с использованием соответствующих ключей. При попытке прочитать открытую информацию с отчуждаемого носителя при включенном режиме преобразования, пользователю будет выдана ошибка.

Если информация преобразована на рабочем ключе компьютера, она не сможет быть прочитана нигде, кроме этого компьютера. При преобразовании информации на главном ключе, данная информации может быть прочитана на компьютерах с одинаковым главным ключом. Главный ключ одинаков у тех компьютеров, система защиты на которых устанавливалась с использованием одного и того же персонального ключа администратора системы защиты.

При изменении параметра преобразования информации на отчуждаемых носителях необходимо перезагрузить компьютер, чтобы изменения вступили в силу.

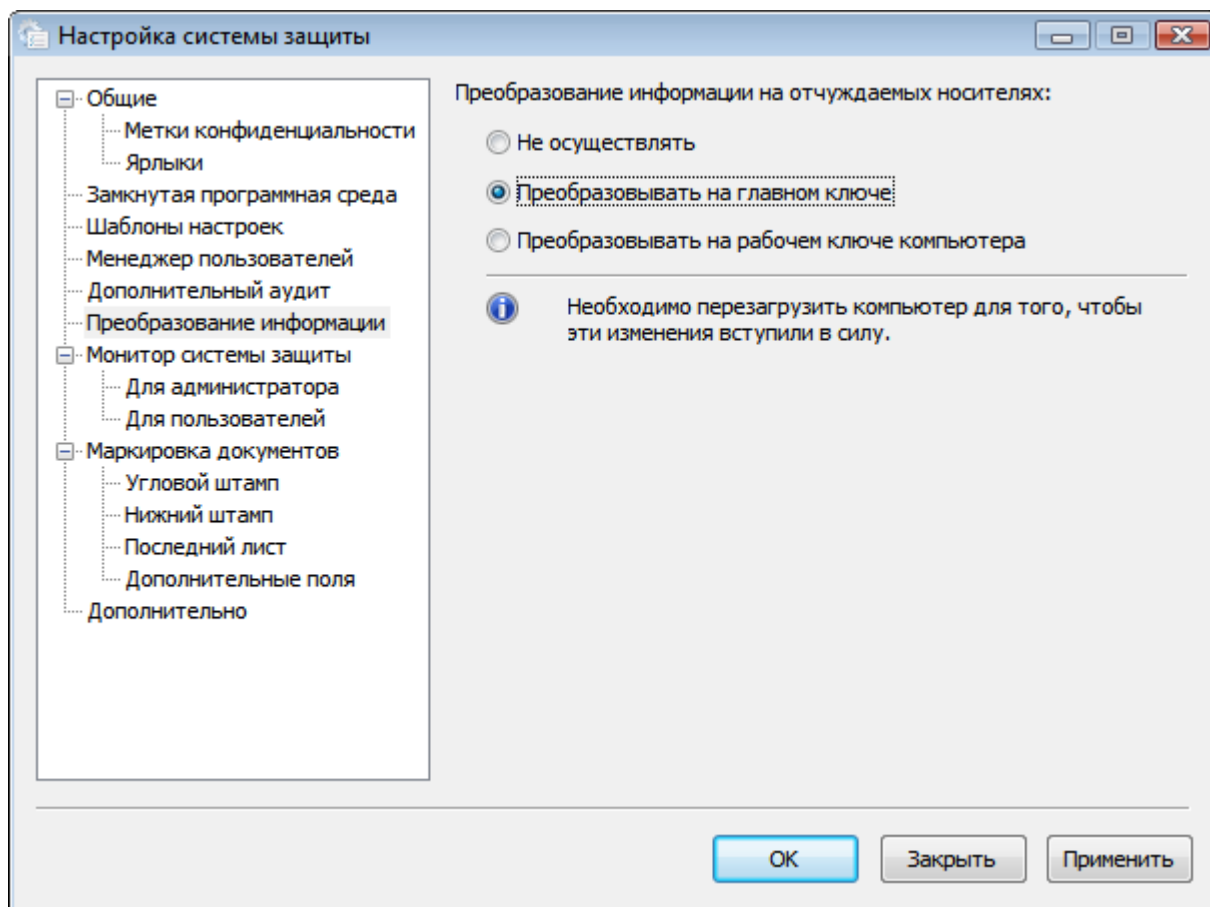


Рис. 34. Настройка параметров преобразования информации.

### Монитор системы защиты

Единственным параметром программы **Монитор системы защиты** является необходимость загрузки данной программы при старте операционной системы. Если флажок **Загружать при старте Windows** установлен, у каждого пользователя при загрузке операционной системы данная программа будет запущена.

### Для администратора

В данном диалоге настроек (см. Рис. 35) определяется контекстное меню программы **Монитор системы защиты** для текущего администратора системы защиты. Таким образом, каждый администратор может иметь свое контекстное меню в данной программе.

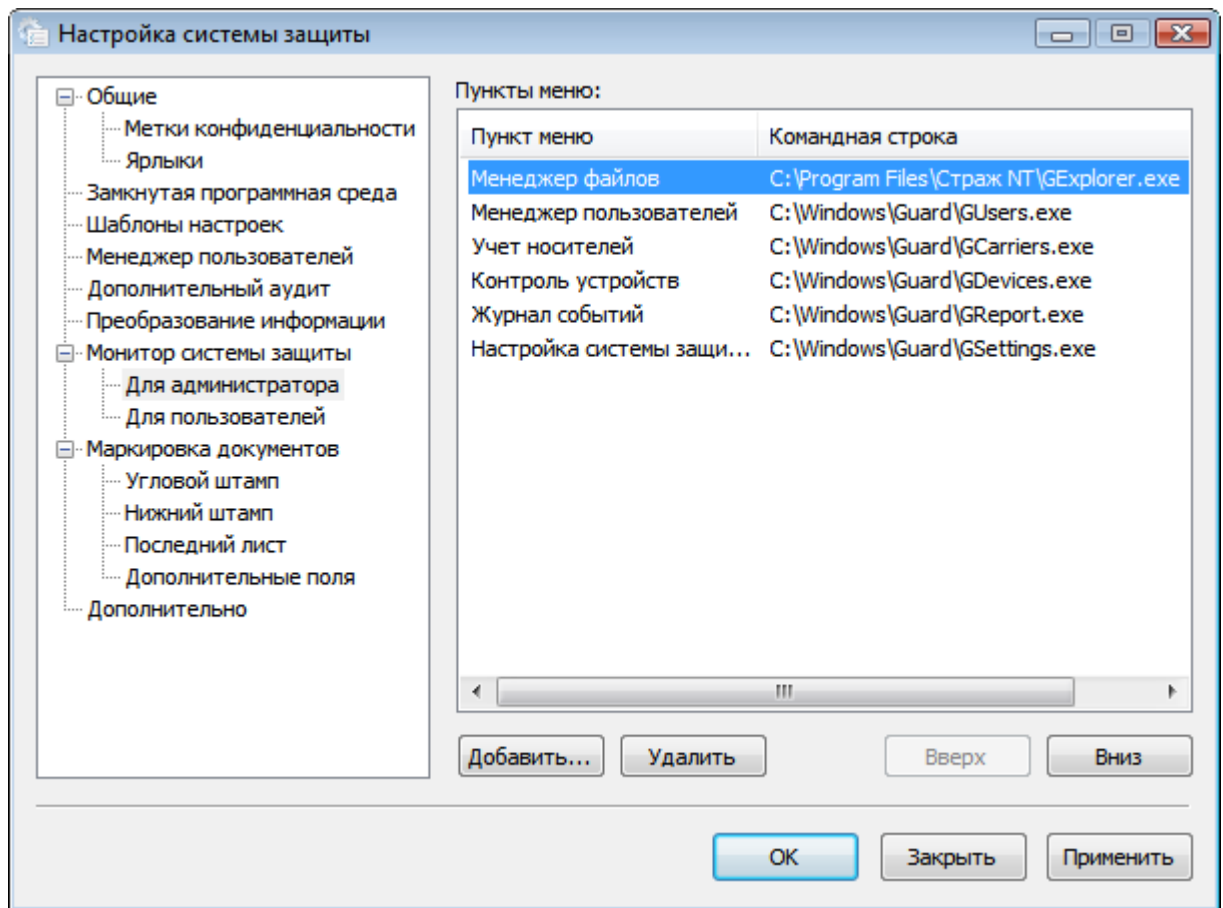


Рис. 35. Настойка параметров программы Монитор системы защиты.

Для добавления пункта меню необходимо нажать кнопку **Добавить...** при этом на экране появится диалог (см. Рис. 36), в котором необходимо ввести наименование пункта меню, ввести и выбрать название программы, а также ввести параметры командной строки, которые будут применяться при запуске программы.

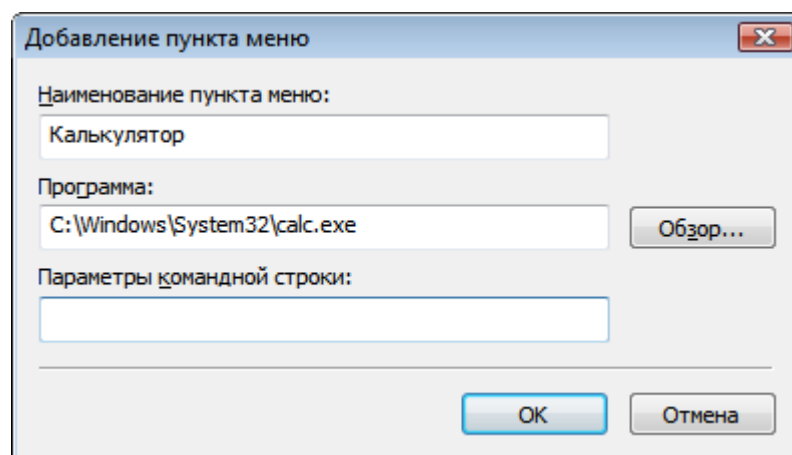


Рис. 36. Добавление пункта меню.

Для сохранения пункта меню необходимо нажать кнопку . Для удаления пункта меню необходимо выбрать его в списке и нажать кнопку . Также кнопками  и  можно управлять положением выбранного пункта в контекстном меню.

### Для пользователей

В данном диалоге настроек определяется контекстное меню программы **Монитор системы защиты** для всех пользователей. Таким образом, у всех пользователей одно и то же контекстное меню. Его настройка происходит аналогично настройке меню для администратора. Дополнительно, установка флажка **Разрешить отключение режима блокировки** разрешает пользователям управлять режимом блокировки системы защиты.

### Маркировка документов

Параметры маркировки документов определяют общие правила для всех маркируемых страниц (см. Рис. 37).

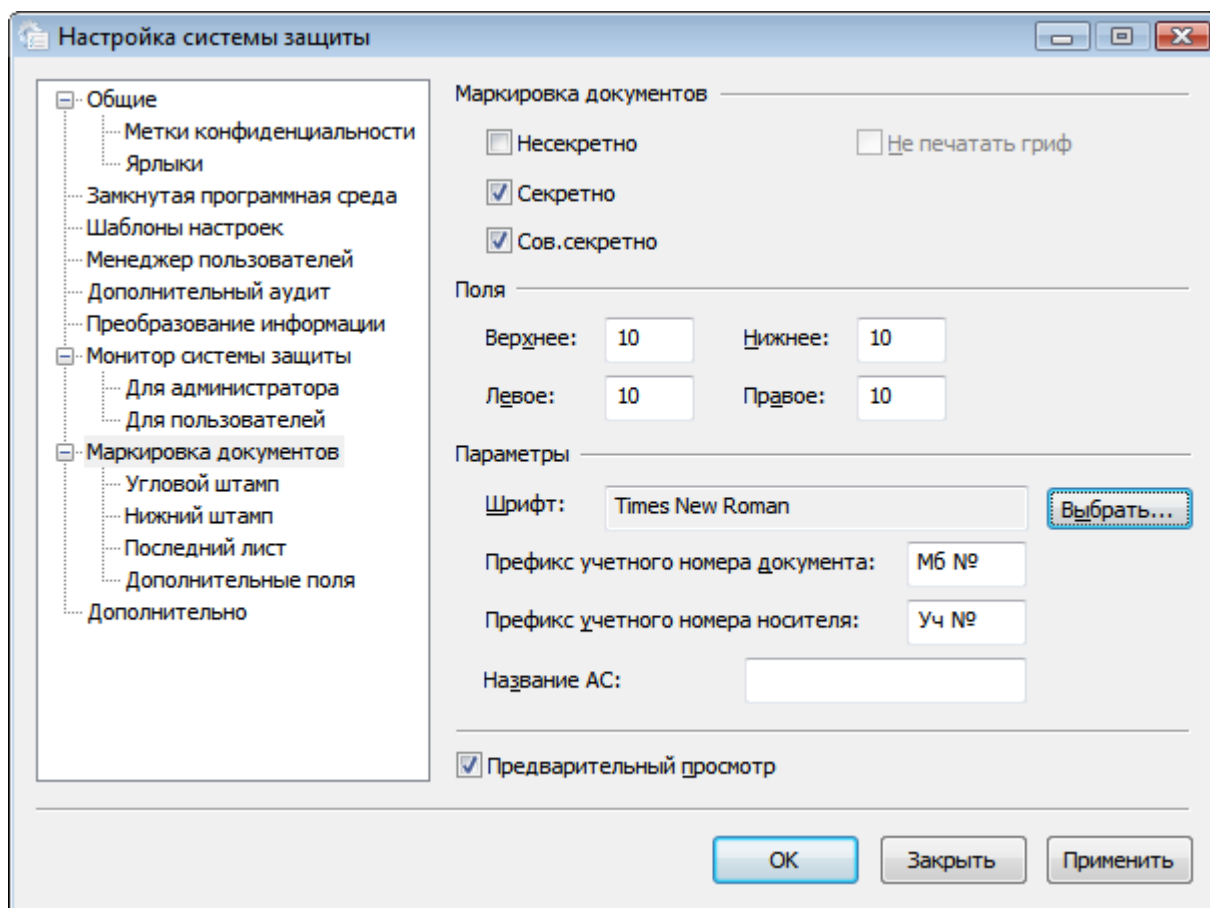


Рис. 37. Общие настройки маркировки документов.

В области **Маркировка документов** присутствуют три поля с названиями меток конфиденциальности. Установка этих флажков означает, что документы, имеющие

соответствующую метку, буду маркироваться согласно установленным правилам. Существует возможность не выводить значение метки конфиденциальности для документов самого нижнего уровня. Для этого необходимо установить флажок **Не печатать гриф**. В области **Поля** необходимо ввести значения отступов от границ листа. В области **Параметры** поле **Шрифт** определяет параметры шрифта, которым будет выводиться весь текст за исключением метки конфиденциальности. Изменить шрифт можно, нажав кнопку . Поле **Префикс учетного номера документов** определяет значение, которое идет перед номером документа (например, «Мб»). Поле **Префикс учетного номера носителя** определяет значение, которое идет перед номером носителя информации, с которого печатается документ. Если флажок **Предварительный просмотр** установлен, справа от основного окна программы отображается диалоговое окно предварительного просмотра маркировки документа (см. Рис. 38).

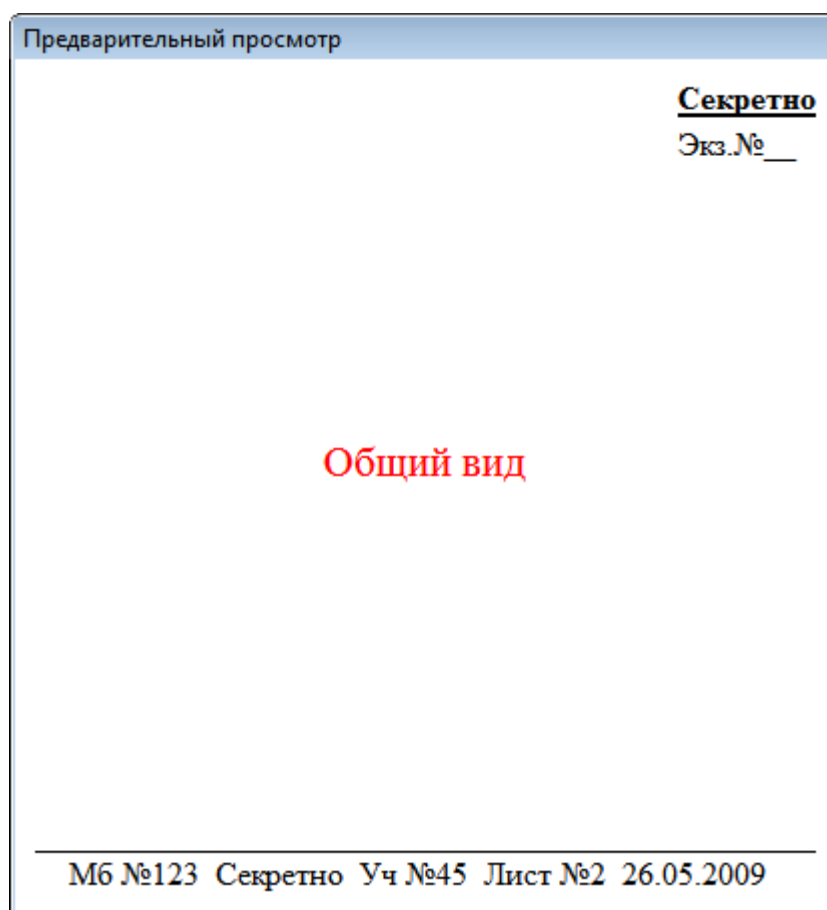


Рис. 38. Окно предварительного просмотра.

#### Угловой штамп

Данные параметры определяют вид углового штампа, который печатается на первой странице маркируемого документа. В списке перечислены поля, которые могут быть выведены на печать в угловом штампе. Если флажок в первом столбце будет установлен,



поле будет напечатано. Порядок печати полей можно изменить, нажимая кнопки **Вверх** и **Вниз**. Поле **Шрифт грифа** определяет параметры шрифта, которым будет выводиться метка конфиденциальности документа. Изменить шрифт можно, нажав кнопку **Выбрать...**. Если флажок **Предварительный просмотр** установлен, справа от основного окна программы отображается диалоговое окно предварительного просмотра маркировки документа.

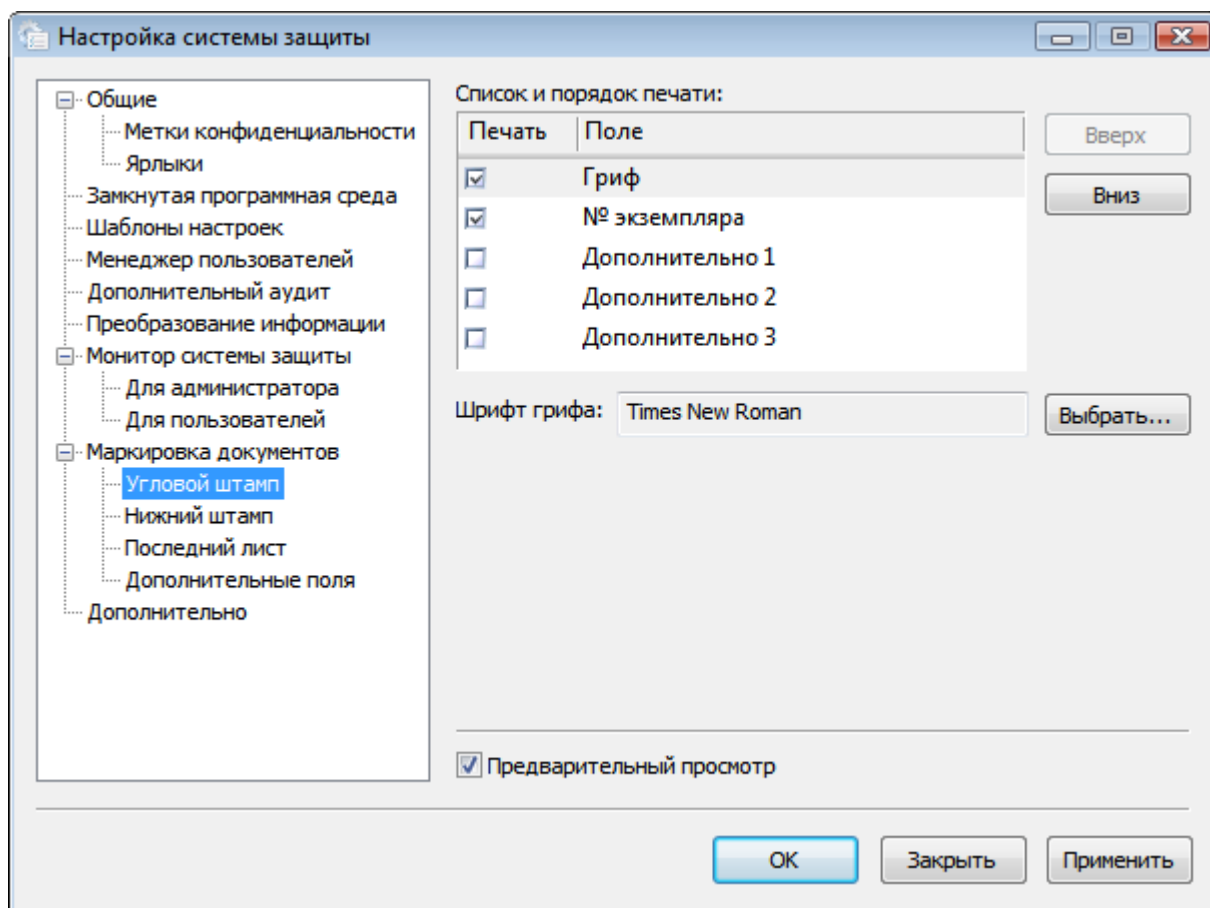


Рис. 39. Настройки маркировки углового штампа документов.

### Нижний штамп

Данные параметры определяют вид нижнего штампа, который печатаются на каждой странице маркируемого документа. В списке перечислены поля, которые могут быть выведены на печать в угловом штампе. Если флажок в первом столбце будет установлен, поле будет напечатано. Порядок печати полей можно изменить, нажимая кнопки **Вверх** и **Вниз**.

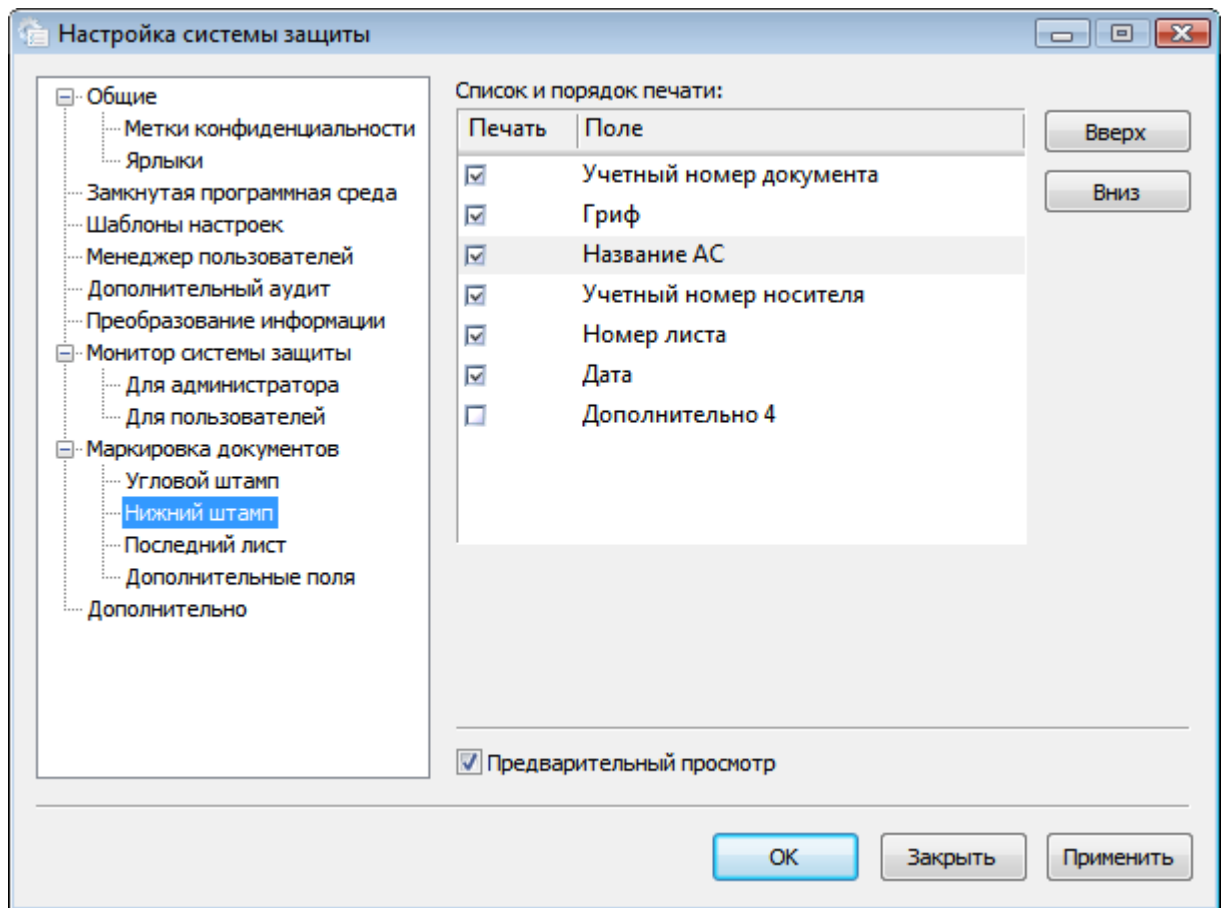


Рис. 40. Настройки маркировки нижнего штампа документов.

### Последний лист

Данные параметры определяют вид нижнего штампа последнего листа маркируемого документа. В списке перечислены поля, которые могут быть выведены на печать в угловом штампе. Если флажок в первом столбце будет установлен, поле будет напечатано. Порядок печати полей можно изменить, нажимая кнопки  и . Если в области **Исполнитель** установлена кнопка **Задается пользователем**, во время печати документа пользователь самостоятельно должен ввести имя исполнителя документа. В противном случае имя исполнителя берется из текущей учетной записи. Если в области **Кто отпечатал** установлена кнопка **Задается пользователем**, во время печати документа пользователь самостоятельно должен ввести свое имя. В противном случае имя пользователя, отпечатавшего документ, берется из текущей учетной записи.

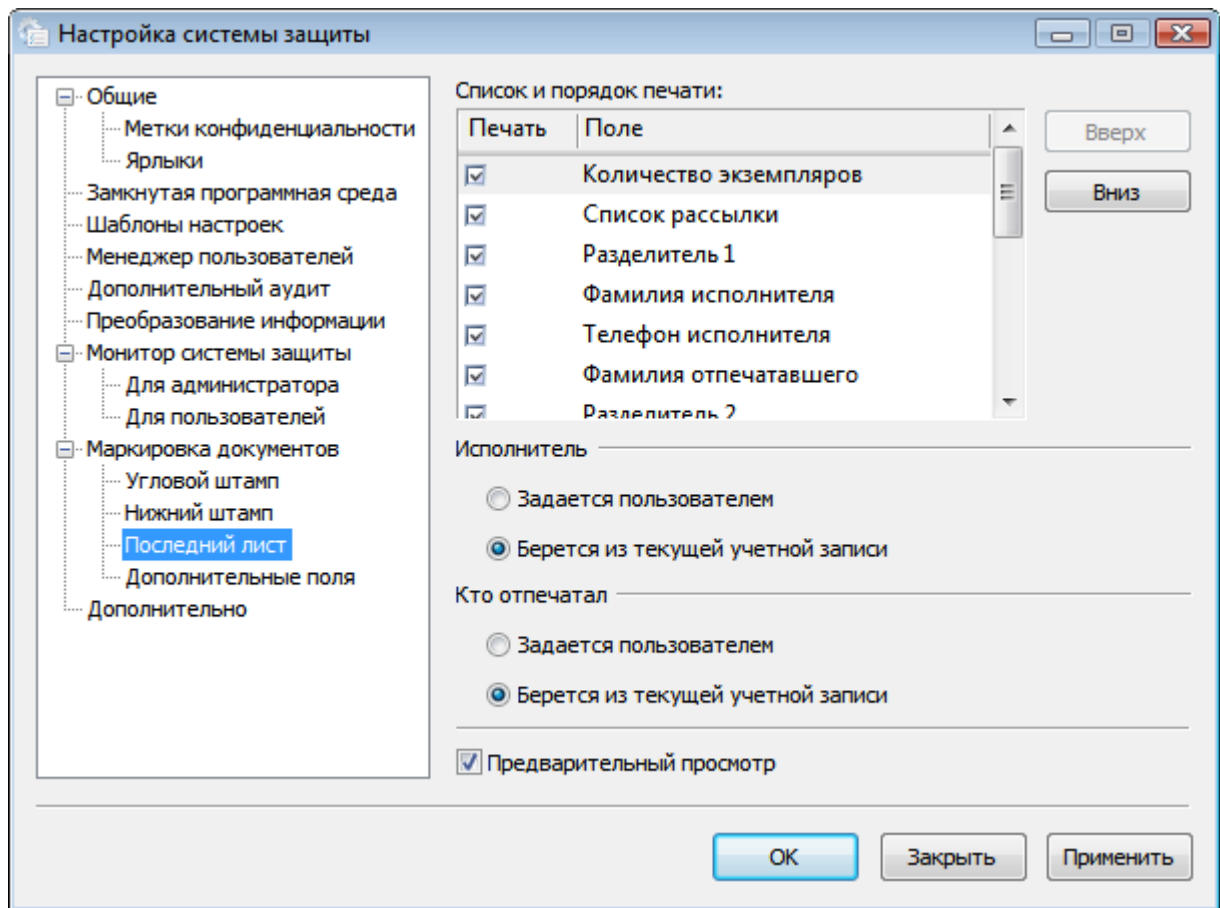


Рис. 41. Настройки маркировки последнего листа документов.

### Дополнительные поля

В данных параметрах определяются названия дополнительных полей, которые задаются пользователем во время печати документа, если их вывод предусмотрен настройками маркировки.

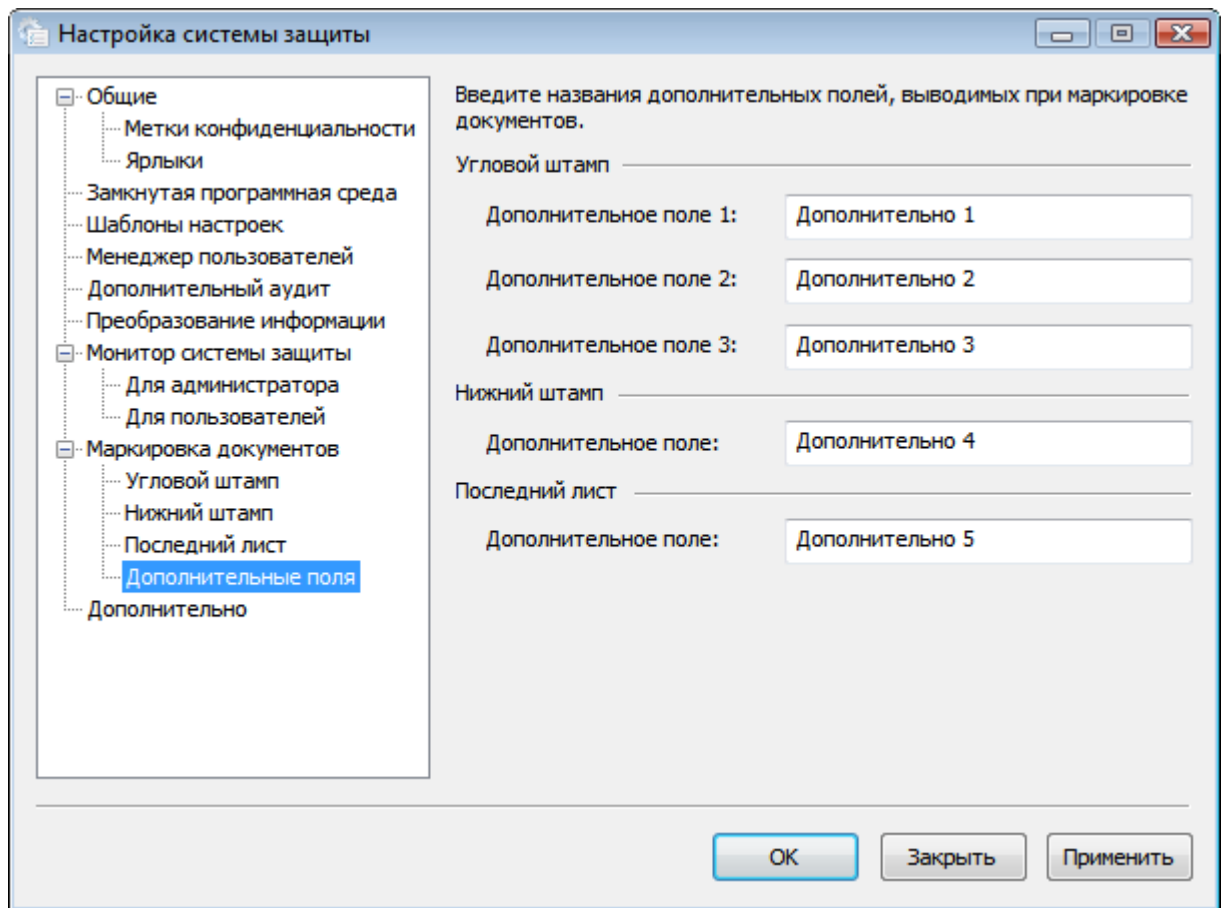
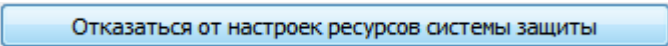


Рис. 42. Дополнительные настройки маркировки документов.

### Дополнительно

При нажатии кнопки  система защиты останавливается, файл настроек удаляется, и система запускается вновь с включенным режимом автоматической расстановки режима запуска на этот и следующий сеанс. После удаления настроек системы защиты настоятельно рекомендуется выполнить перезагрузку компьютера.

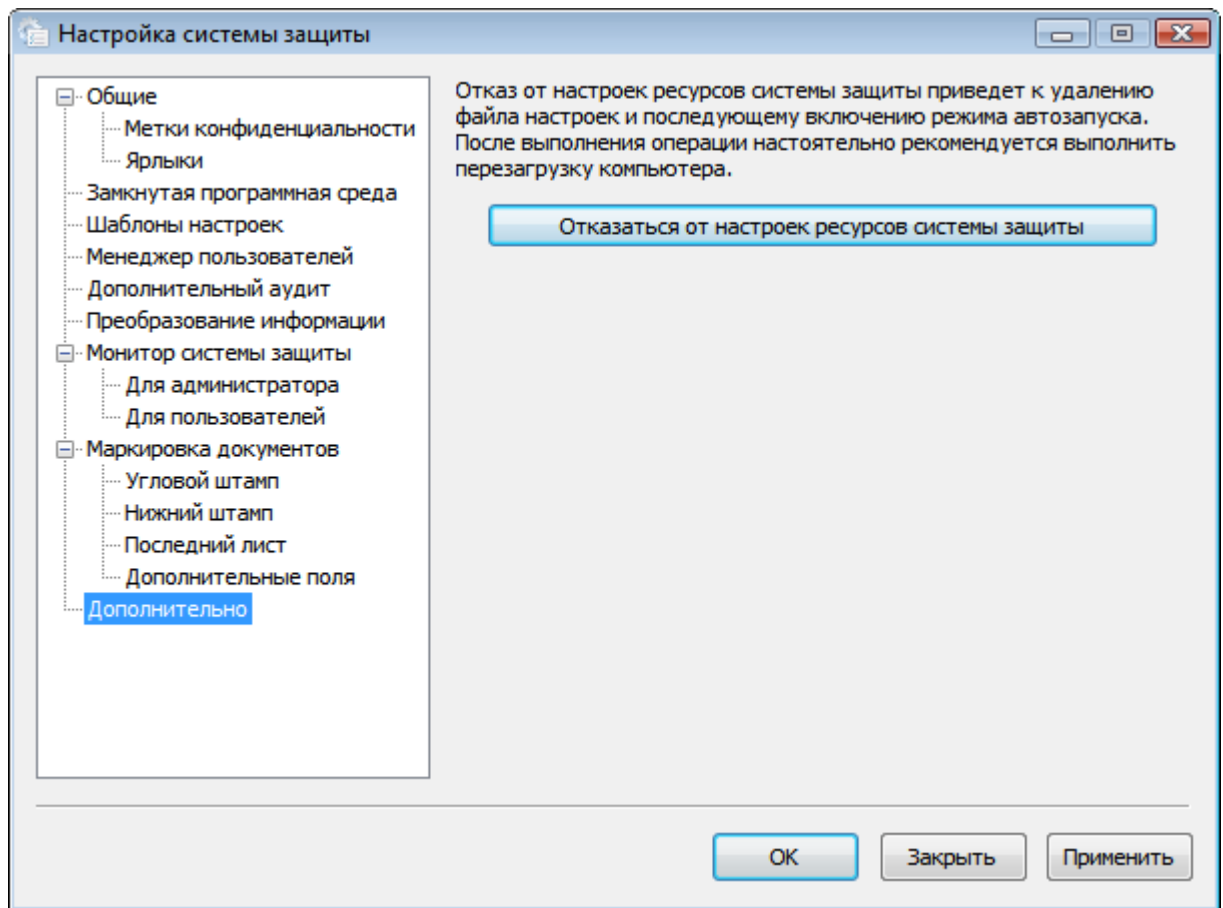


Рис. 43. Дополнительные настройки.

# Управление носителями информации

В данной главе приводятся сведения о назначении и применении программы **Учет носителей**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при учете носителей информации.

СЗИ «Страж NT» контролирует доступ ко всем носителям информации, используемым в процессе работы. Программа **Учет носителей** предназначена для настройки параметров работы системы защиты с носителями информации.

Программа **Учет носителей** запускается при выборе администратором системы защиты в программном меню пункта **Программы | Страж NT | Учет носителей**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей, при запуске программы на экране появится окно, как показано на Рис. 44. Для продолжения необходимо нажать кнопку .

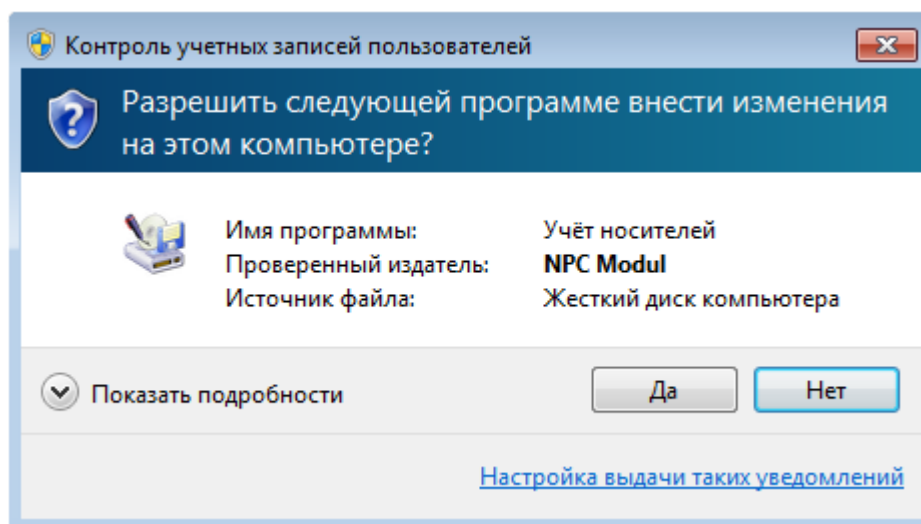


Рис. 44. Сообщение подсистемы контроля учетных записей пользователей.

При этом на экране появляется диалоговое окно, пример которого показан на Рис. 45. Слева вверху отображён список групп носителей, каждая из которых соответствует определенному типу. Слева внизу расположена область списка компьютеров, входящих в рабочую группу или домен. Справа представлен список зарегистрированных на выбранном компьютере носителей информации с их свойствами:

Свойство	Описание
Учётный номер	Определяет номер, который задаёт пользователь при регистрации носителя.
Имя диска	Определяет букву тома, с которой носитель определился в системе. Если в этом поле ничего нет, значит носитель в данный момент отсутствует в системе.
Гриф	Определяет метку конфиденциальности носителя.
Пользователь	Определяет фамилию должностного лица, за которым закреплён данный носитель.
Дата учёта	Определяет дату и время добавления носителя в список.
Серийный номер	Определяет серийный номер носителя.
Тип доступа	Определяет тип доступа к носителю. Если установлен тип доступа «простой», то правила разграничения доступа к носителю будут распространяться на все ресурсы, находящиеся на данном носителе. В противном случае, разграничение доступа к ресурсам на данном носителе будет осуществляться согласно правилам доступа к объектам файловой системы NTFS.

При подключении зарегистрированного носителя информации к нему будут применяться те правила безопасности, которые ему задал администратор системы защиты. Если носитель не зарегистрирован, к нему будут применяться правила, заданные для группы носителей, к которой он принадлежит. Для группы носителей администратор системы защиты имеет возможность задать только разрешения и параметры дополнительного аудита. При этом заданные разрешения будут распространяться на все ресурсы, находящиеся на подключенном незарегистрированном носителе.

В процессе установки системы защиты в список зарегистрированных носителей будут добавлены все присутствующие на момент установки носители типа «Жёсткий диск». При этом для них устанавливаются следующие разрешения: системе, группе локальных администраторов и группе «Все» – полный доступ. Также для них устанавливается самая низкая метка конфиденциальности, отключен дополнительный аудит, тип доступа – обычный. В дальнейшем администратор системы защиты может менять свойства зарегистрированных носителей.

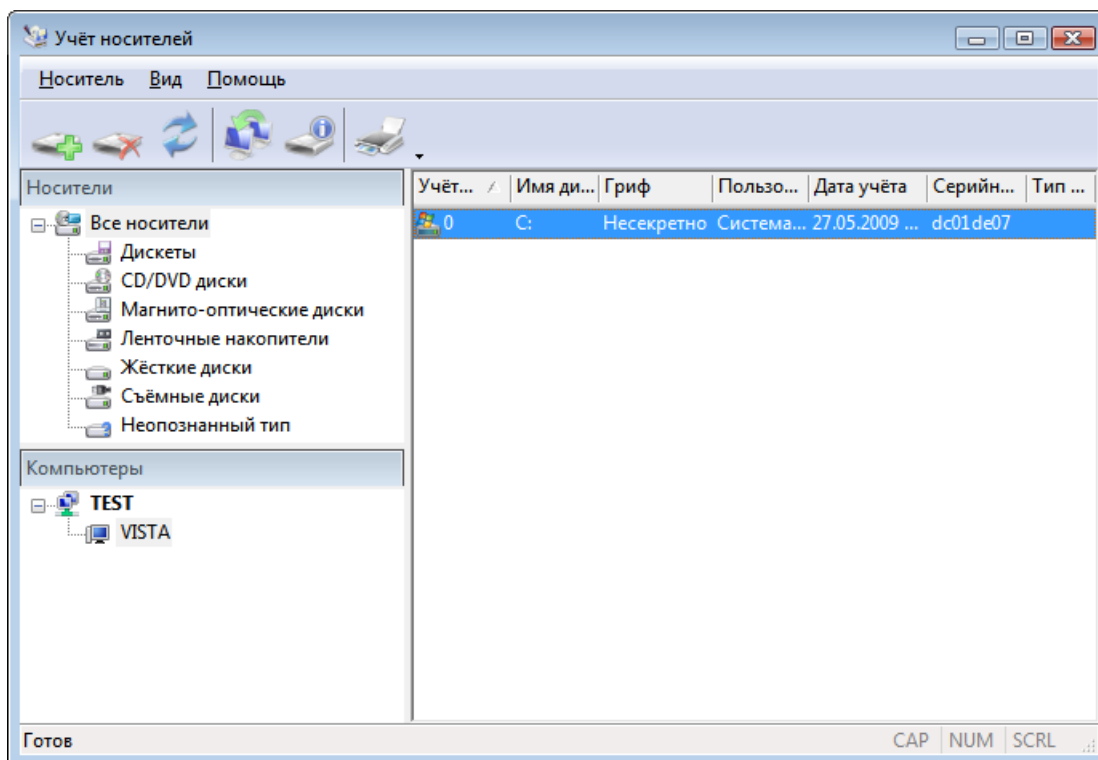


Рис. 45. Общий вид окна программы Учёт носителей.

### Редактирование свойств для групп носителей

При установке системы защиты для всех групп носителей устанавливаются разрешения по умолчанию: системе, группе локальных администраторов и группе администраторов системы защиты – полный доступ. Также для групп носителей устанавливается самая низкая метка конфиденциальности и отключен дополнительный аудит. Для просмотра и редактирования свойств выбранной группы носителей необходимо выбрать пункт меню **Носитель | Свойства** и в появившемся диалоговом окне, пример которого показан на Рис. 46, выбрать вкладку **Свойства**.

Для просмотра и редактирования разрешений для выбранной группы носителей необходимо выбрать пункт меню **Носитель | Свойства** и в появившемся диалоговом окне, пример которого показан на Рис. 46, выбрать вкладку **Безопасность**. При этом выводится окно редактора списка контроля доступа, в котором отображается дискреционный список контроля доступа для выбранной группы.



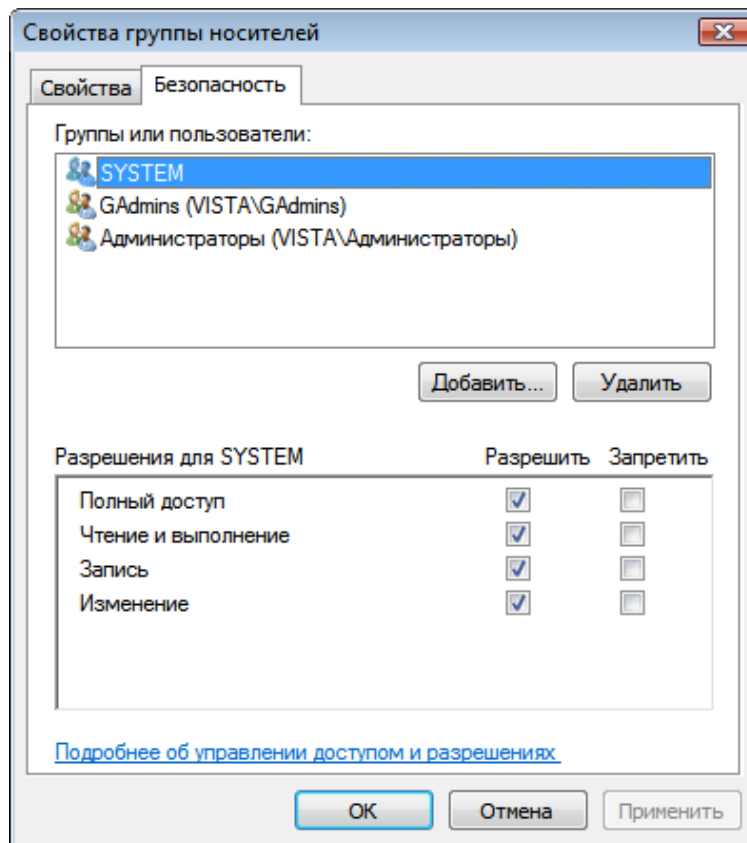
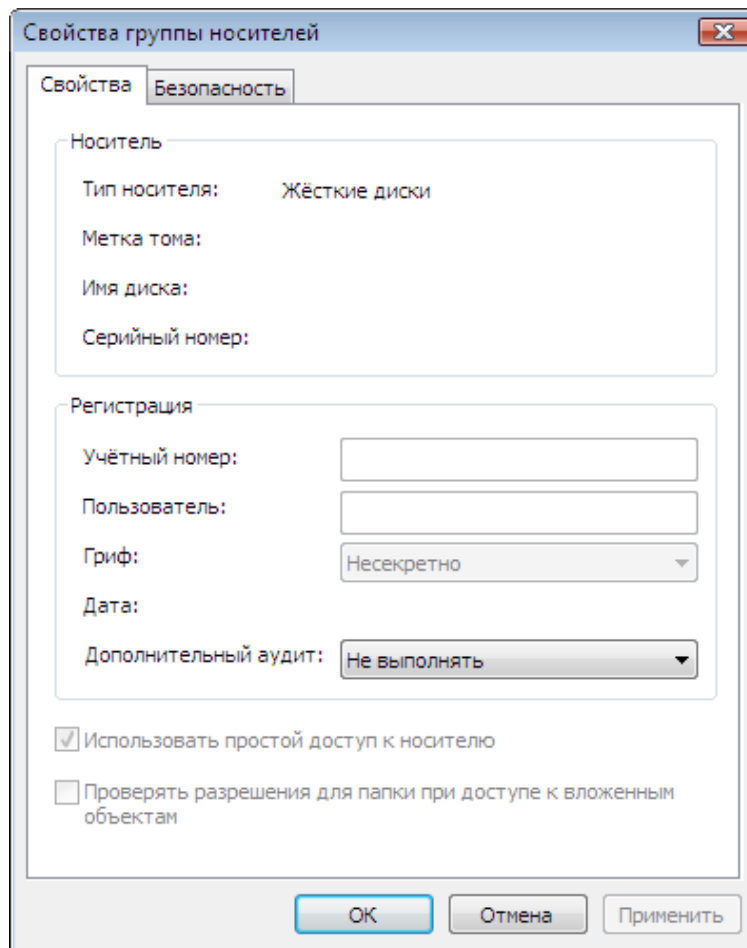
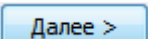


Рис. 46. Свойства для группы носителей.

## Добавление и удаление зарегистрированных носителей информации

Для разграничения доступа к конкретным носителям информации, администратор системы защиты может зарегистрировать каждый носитель в отдельности. Если носитель присутствует в списке зарегистрированных носителей, к нему не будут применяться правила разграничения доступа для группы носителей, к которой он принадлежит.

Для добавления носителя в список зарегистрированных необходимо выбрать пункт меню **Носитель | Добавить носитель...** либо вызвать контекстное меню в области списка пользователей и выбрать пункт **Добавить носитель...**. При этом на экране появится мастер добавления носителя (см. Рис. 47), в котором необходимо выбрать один из носителей и нажать кнопку .

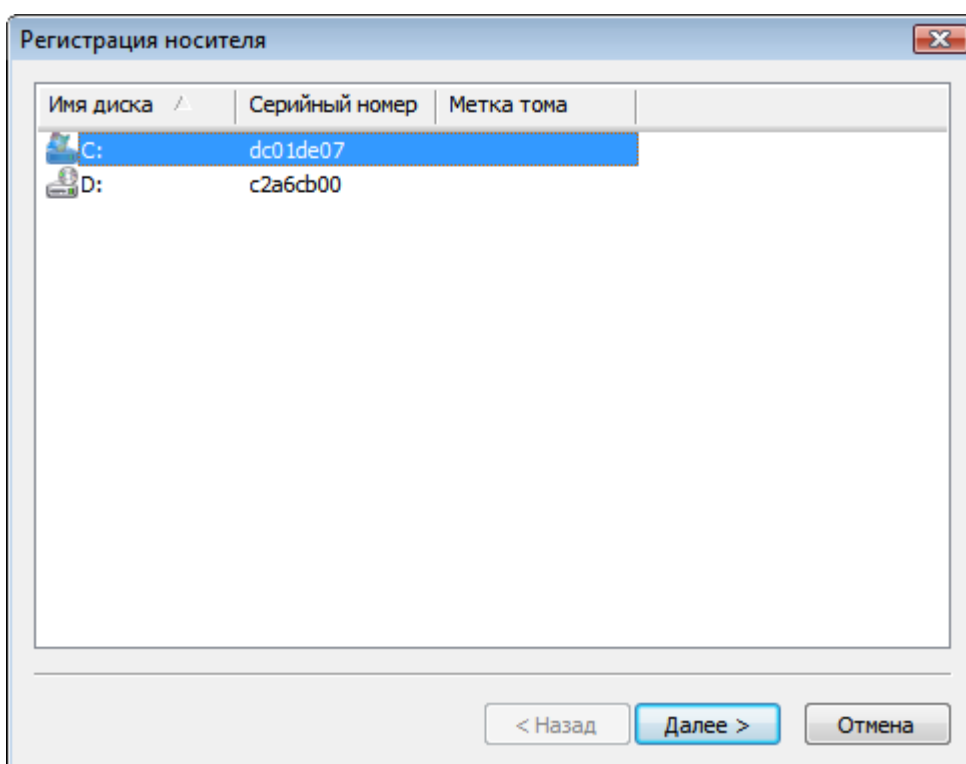


Рис. 47. Регистрация носителя информации.

При этом появится диалог, в котором необходимо задать регистрационные данные выбранного носителя (см. Рис. 48).

Регистрация носителя

Учётный номер носителя: 012

Имя ответственного пользователя: Administrator

Гриф носителя: Секретно

Использовать простой доступ к носителю

< Назад Готово Отмена

Рис. 48. Регистрационные данные носителя.

После нажатия кнопки **Готово** носитель будет зарегистрирован. Если носитель с таким серийным номером уже присутствует в списке, на экран будет выдано предложение, перезаписать параметры зарегистрированного носителя (см. Рис. 49). При положительном ответе новые параметры заменят уже существующие.

Учёт носителей

⚠ Носитель с таким серийным номером уже существует, заменить?

Да Нет

Рис. 49. Предложение о перезаписи параметров носителя.

Для удаления носителя из списка необходимо выбрать его в списке и выбрать пункт меню **Носитель | Удалить носитель** либо выбрать пункт **Удалить носитель** контекстного меню.



Для нормального функционирования компьютера системный диск должен присутствовать в списке зарегистрированных носителей. Удаление системного диска из списка невозможно.

## Редактирование свойств носителей

Для просмотра и редактирования свойств и разрешений для выбранного носителя необходимо выбрать пункт меню **Носитель | Свойства** или пункт **Свойства** контекстного меню и в появившемся диалоговом окне выбрать соответствующую вкладку. При этом в зависимости от выбранной вкладки выводится окно свойств носителя (см. Рис. 50) или окно редактора списка контроля доступа, в котором отображается дискреционный список контроля доступа для выбранного носителя.

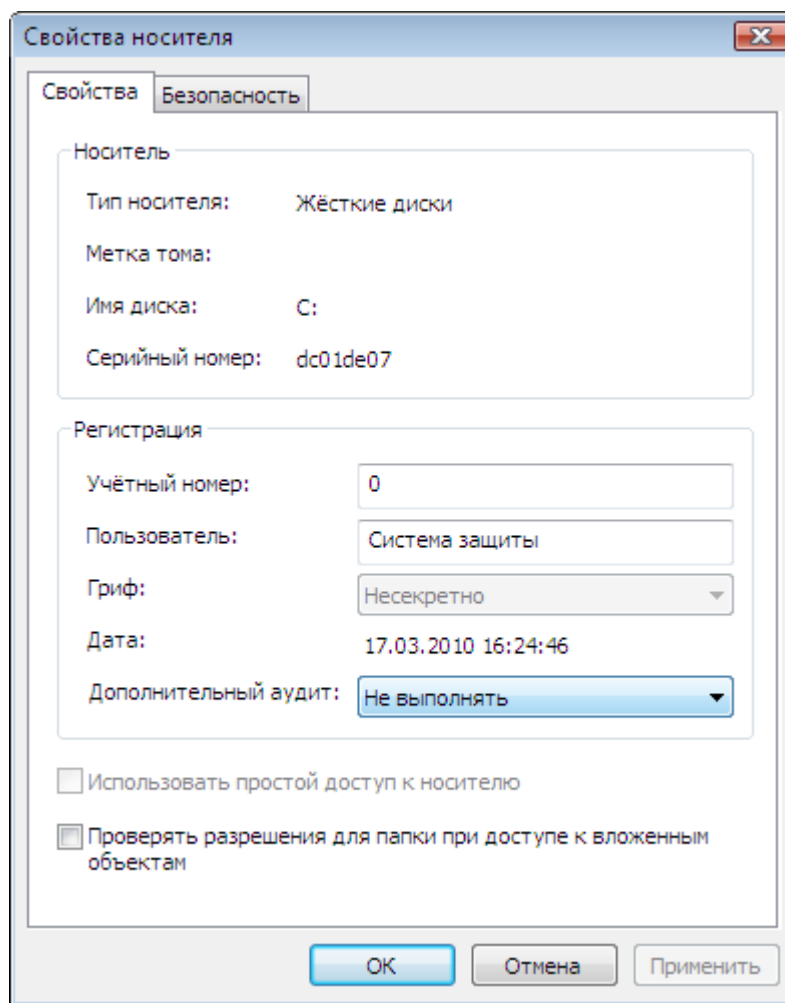


Рис. 50. Свойства зарегистрированного носителя информации.

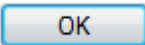
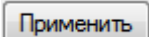
Для изменения параметров дополнительного аудита выбранного носителя необходимо выбрать соответствующее значение из раскрывающегося списка в поле **Дополнительный аудит** .

При установке флажка **Проверять разрешения для папки при доступе к вложенным объектам** при попытках доступа к ресурсам носителя будут проверяться и учитываться установленные для выбранного носителя разрешения.

Для установки использования простого типа доступа к выбранному носителю необходимо установить флажок **Использовать простой доступ к носителю**.

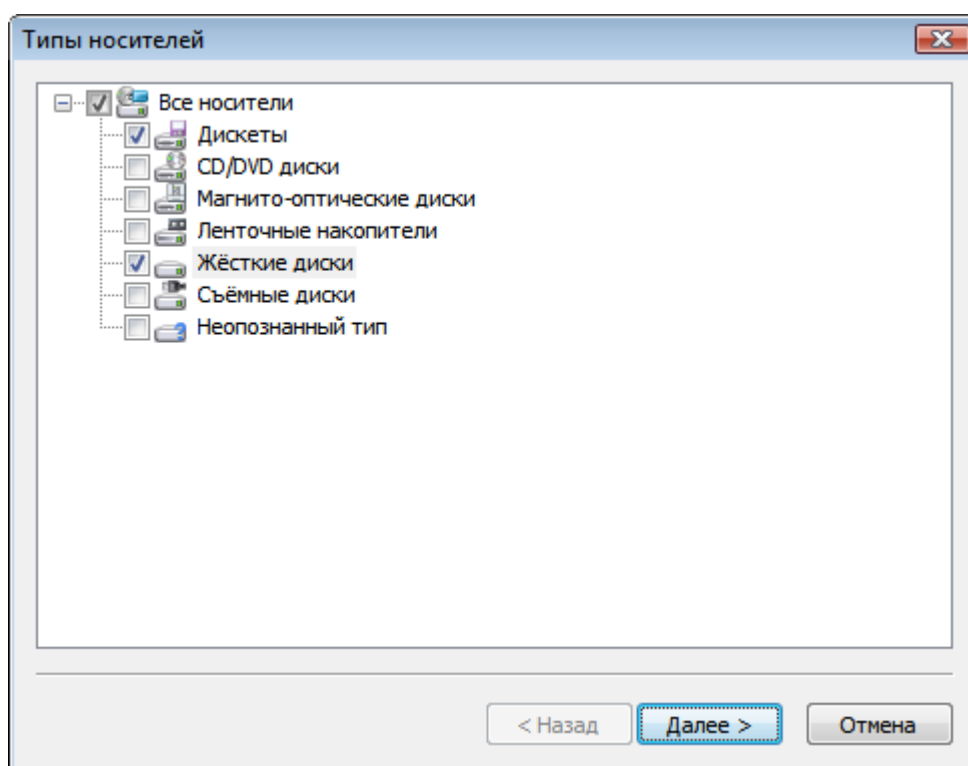


*Для системного диска нельзя установить использование простого типа доступа.  
Данное поле будет неактивно.*

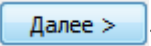
Для сохранения сделанных изменений необходимо нажать кнопку  или .

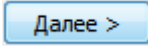
## Экспорт настроек

Для экспорта настроек на другие компьютеры необходимо выбрать пункт меню **Носитель | Экспорт настроек**. После этого на экране появится мастер экспорта настроек (см. Рис. 51).



*Рис. 51. Мастер экспорта настроек – выбор параметров групп носителей.*

В данном окне необходимо выбрать группы носителей, параметры которых будут экспортироваться, и нажать кнопку . На экране появится окно экспорта списка зарегистрированных носителей (см. Рис. 52). В данном окне необходимо выбрать носители, настройки которых будут экспортироваться на другие компьютеры. Если на компьютере, куда экспортируются настройки, уже присутствует зарегистрированный носитель с таким серийным номером и установлен флажок **Требовать подтверждение изменения параметров носителей**, программа предложит заменить настройки. В противном случае, замена на новые настройки будет выполнена автоматически.

После нажатия кнопки  на экране появится окно выбора компьютеров (см. Рис. 53).

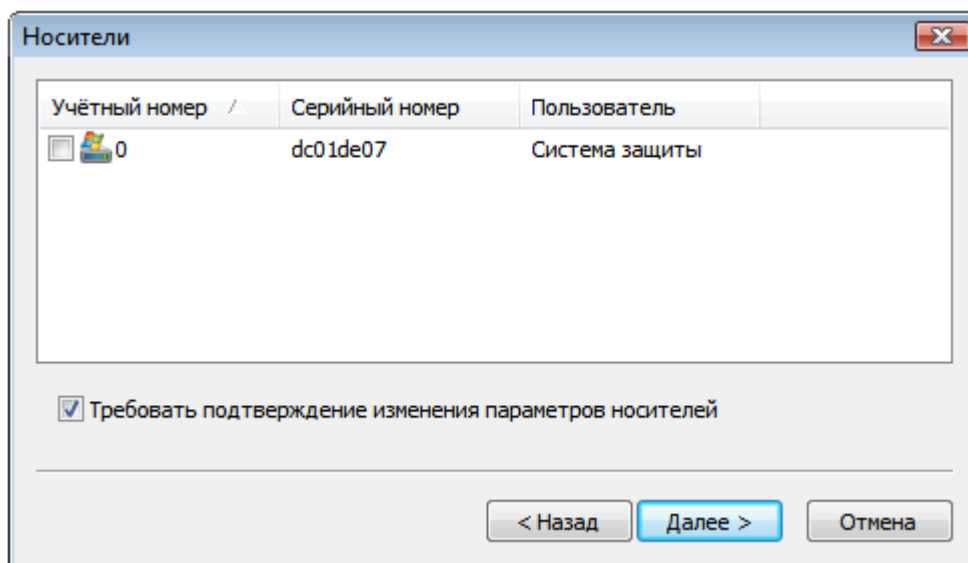


Рис. 52. Мастер экспорта настроек – выбор носителей.

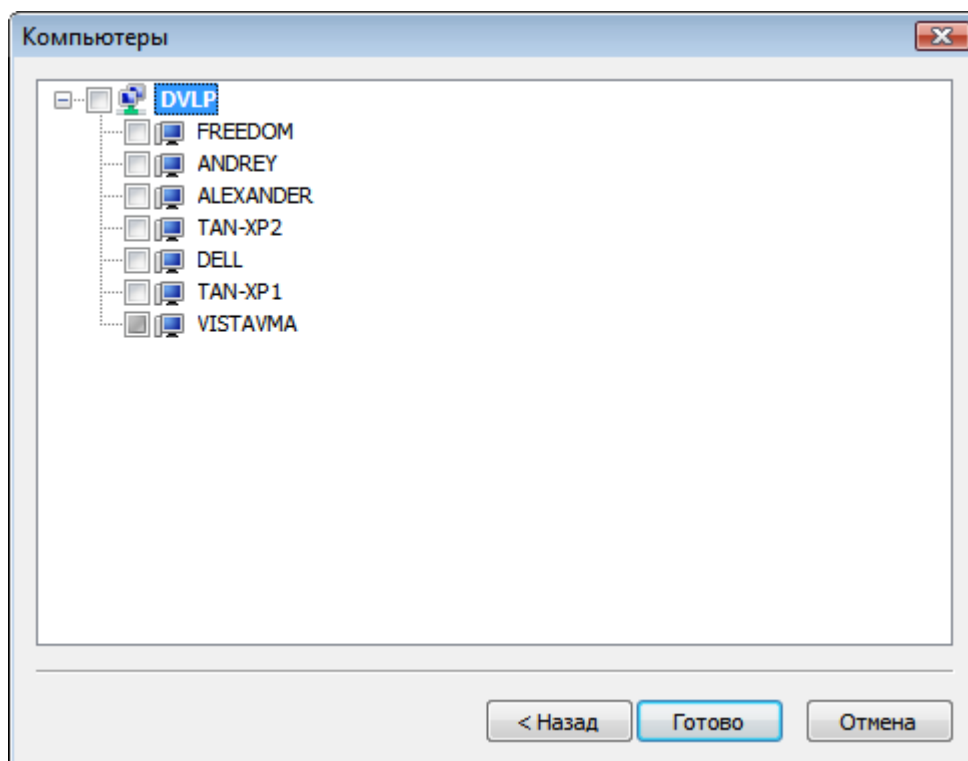
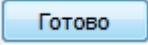


Рис. 53. Мастер экспорта настроек – выбор компьютеров.

После нажатия кнопки  настройки будут перенесены на отмеченные компьютеры.

# Управление пользователями

В данной главе приводятся сведения о назначении и применении программы **Менеджер пользователей**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при работе с учетными записями пользователей и персональными идентификаторами.

Программа **Менеджер пользователей** предназначена для управления пользователями системы защиты информации, их свойствами и персональными идентификаторами и позволяет выполнять следующие функции:

- создание, удаление и переименование пользователей;
- просмотр пароля и списка идентификаторов пользователя;
- смена пароля пользователя;
- просмотр и редактирование свойств пользователя;
- формирование персональных идентификаторов;
- чтение и очистка идентификаторов.

Программа **Менеджер пользователей** запускается при выборе администратором системы защиты в программном меню пункта **Программы | Страж NT | Менеджер пользователей**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей, при запуске программы на экране появится окно, как показано на Рис. 54. Для продолжения необходимо нажать кнопку

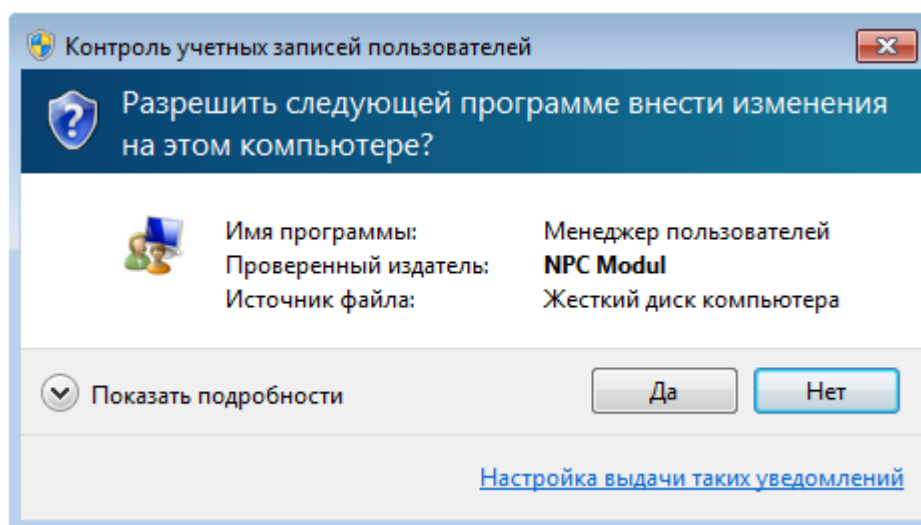


Рис. 54. Сообщение подсистемы контроля учетных записей пользователей.

При этом на экране появляется диалоговое окно, пример которого показан на Рис. 55.

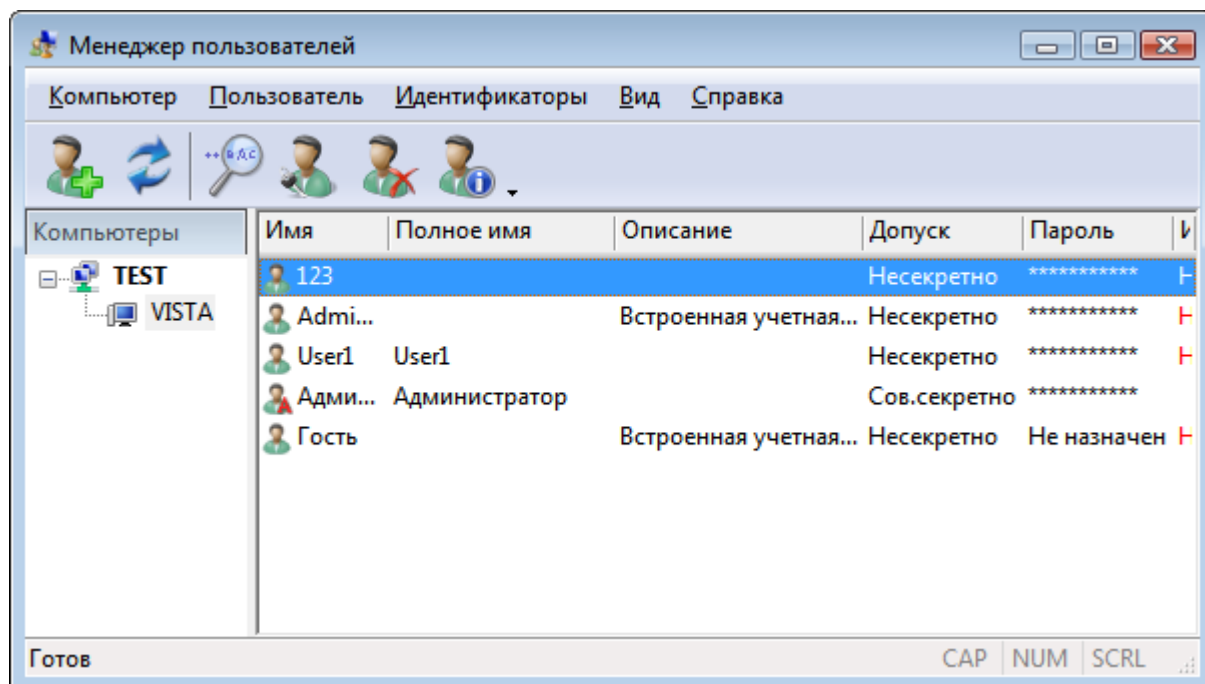



Рис. 55. Общий вид окна программы Менеджер пользователей.

Слева отображается список компьютеров, входящих в рабочую группу или домен. Справа представлен список пользователей выбранного компьютера или домена с их основными свойствами:

Свойство	Описание
Имя	<p>Определяет название учетной записи пользователя в системе.</p> <p> <i>Имя пользователя не должно превышать 15 символов.</i></p>
Полное имя	Определяет полное имя пользователя.
Описание	Определяет дополнительную информацию о пользователе.
Допуск	Определяет допуск пользователя к защищаемым ресурсам системы.
Пароль	<p>Определяет пароль пользователя и его текущее состояние. Звездочки в колонке <b>Пароль</b> означают, что значение пароля сохранено в базе системы защиты. Значение «Не назначен» в колонке <b>Пароль</b> означает, что пароль данного пользователя неизвестен системе защиты. Такому пользователю невозможно сформировать персональный идентификатор.</p>






*Пароль пользователя не должен превышать 15 символов и может содержать символы только латинского алфавита, цифры, а также специальные символы.*

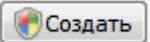

---

**Идентификатор** Определяет текущее состояние персонального идентификатора пользователя. Значение «Не сформирован» в колонке **Идентификатор** означает, что у данного пользователя нет ни одного сформированного идентификатора. Такой пользователь не сможет войти в систему. Значение «Не актуален» означает, что после формирования персонального идентификатора у пользователя был изменен пароль.

---

Пользователи, являющиеся администраторами системы защиты, отмечаются специальным значком .

### **Создание, удаление и переименование пользователей**

Для создания пользователя необходимо выбрать пункт меню **Компьютер | Новый пользователь** или **Домен | Новый пользователь** либо вызвать контекстное меню в пустой области списка пользователей и выбрать пункт **Новый пользователь...**. При этом на экране появится диалог (см. Рис. 56), в котором необходимо ввести имя пользователя, полное имя, описание, а также его пароль и допуск. Для создания пользователя необходимо нажать кнопку . Если создается пользователь в домене, существует возможность размещения его учетной записи в контейнере Active Directory, отличном от контейнера «по умолчанию». Для этого в диалоге (см. Рис. 56) необходимо нажать кнопку  и в появившемся окне выбрать необходимый контейнер AD. При установке флажка **Создать профиль пользователя на этом компьютере** после удачного создания пользователя на данном компьютере формируется его локальный профиль.

Новый пользователь

Пользователь: abukov

Создать профиль пользователя на этом компьютере

Расположение: По умолчанию

Полное имя: Буков Александр Денисович

Описание: Начальник сертификационной лаборатории

Допуск: Секретно

Пароль: \*\*\*\*\*

Подтверждение: \*\*\*\*\*

Показать пароль

Рис. 56. Создание нового пользователя.

Для удаления пользователя необходимо выбрать его в списке пользователей и выбрать пункт меню **Пользователь | Удалить** либо выбрать пункт **Удалить** контекстного меню.

Для переименования пользователя необходимо выбрать его в списке пользователей и выбрать пункт меню **Пользователь | Переименовать** либо выбрать пункт **Переименовать** контекстного меню. После этого необходимо ввести новое имя пользователя и нажать клавишу «Enter».

### Просмотр пароля и списка идентификаторов пользователя

Для просмотра пароля пользователя необходимо выбрать его в списке пользователей и выбрать пункт меню **Пользователь | Показать пароль...** либо выбрать пункт **Показать пароль...** контекстного меню. При этом в столбце **Пароль** вместо звездочек появится значение пароля пользователя, которое при изменении фокуса снова будет скрыто. Если пароль пользователя неизвестен системе защиты, указанные пункты меню будут недоступны.

Для просмотра списка персональных идентификаторов пользователя необходимо выбрать его в списке пользователей и выбрать пункт меню **Пользователь | Показать список идентификаторов...** либо выбрать пункт **Показать список идентификаторов...** контекстного меню. При этом на экране появится диалог, как показано на Рис. 57. В списке

идентификаторов указаны тип идентификатора и время его создания. При необходимости из списка можно удалить выбранные идентификаторы. Для этого необходимо нажать кнопку **Удалить**. Для удаления всех зарегистрированных идентификаторов пользователя необходимо нажать кнопку **Удалить все**. Для сохранения изменений необходимо нажать кнопку **ОК**.

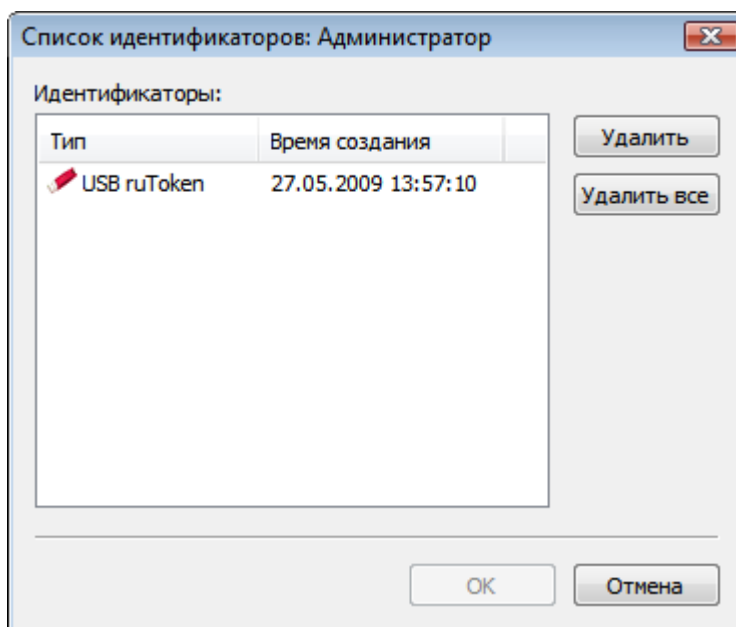
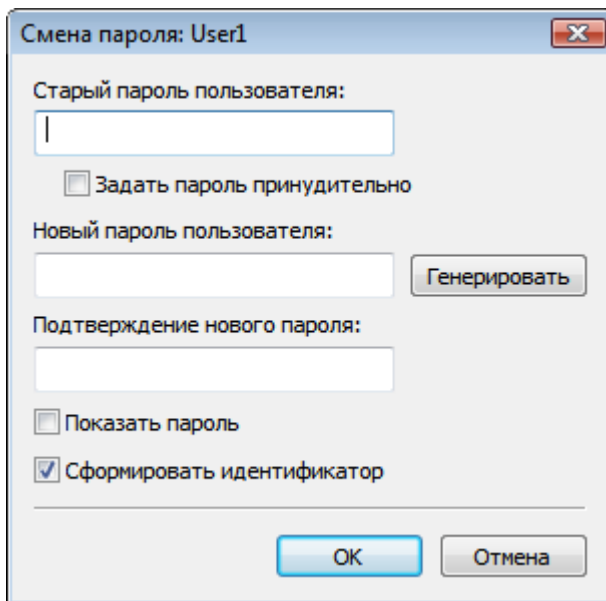


Рис. 57. Список персональных идентификаторов пользователя.

### Смена пароля пользователя

Для смены пароля пользователя необходимо выбрать его в списке пользователей и выбрать пункт меню **Пользователь | Изменить пароль...** либо выбрать пункт **Изменить пароль...** контекстного меню. При этом на экране появится диалог изменения пароля пользователя (см. Рис. 58). Если значение текущего пароля сохранено в базе системы защиты, поле **Старый пароль пользователя** будет автоматически заполнено и недоступно для редактирования. В противном случае для корректной смены пароля пользователя необходимо ввести в указанное поле значение текущего пароля. В поле **Новый пароль пользователя** необходимо ввести значение нового пароля, а в поле **Подтверждение нового пароля** ввести значение нового пароля еще раз. Смена пароля пользователя возможна только в случае совпадения введенных значений. Для автоматической генерации нового пароля пользователя необходимо нажать кнопку **Генерировать**. При этом в оба поля будет автоматически введен пароль, состоящий из восьми буквенно-цифровых латинских символов. Если значение старого пароля пользователя неизвестно, можно принудительно назначить ему новый пароль, установив флажок **Задать пароль принудительно**. Если

выбранному пользователю запрещена смена пароля, флажок **Задать пароль принудительно** будет установлен автоматически.



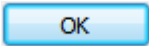
The image shows a Windows-style dialog box titled "Смена пароля: User1". It contains the following elements:

- A text label "Старый пароль пользователя:" followed by an empty text input field.
- A checkbox labeled "Задать пароль принудительно" which is currently unchecked.
- A text label "Новый пароль пользователя:" followed by an empty text input field and a "Генерировать" button to its right.
- A text label "Подтверждение нового пароля:" followed by an empty text input field.
- A checkbox labeled "Показать пароль" which is unchecked.
- A checked checkbox labeled "Сформировать идентификатор".
- At the bottom, there are "OK" and "Отмена" buttons.

Рис. 58. Смена пароля пользователя.




*Принудительная смена пароля пользователя может привести к необратимым потерям информации для этого пользователя. В целях безопасности операционная система защищает некоторую информацию, запрещая доступ к ней при принудительной смене пароля пользователя.*

Для смены пароля пользователя необходимо нажать кнопку . При этом если флажок **Сформировать идентификатор** будет установлен, то после смены пароля на экране появится диалог формирования персонального идентификатора. Если смена пароля с использованием старого значения пароля пользователя завершилась неудачно, администратору будет предложено задать пароль принудительно.

## Просмотр и редактирование свойств пользователя

Для редактирования свойств пользователя необходимо выбрать его в списке пользователей и выбрать пункт меню **Пользователь | Свойства** либо выбрать пункт **Свойства** контекстного меню. Также диалог свойств пользователя открывается при двойном нажатии на пользователе левой клавиши мыши. Диалог свойств пользователя представляет собой несколько вкладок.

## Общие свойства

Во вкладке **Общие** отображаются такие свойства как полное имя пользователя и его описание (см. Рис. 59). Также в этой вкладке отображается путь к профилю пользователя или текст ошибки, по которой он не может быть считан. Если профиль пользователя отсутствует, его можно сформировать, установив флажок **Создать профиль пользователя на этом компьютере**. Для сохранения изменений необходимо нажать кнопку .

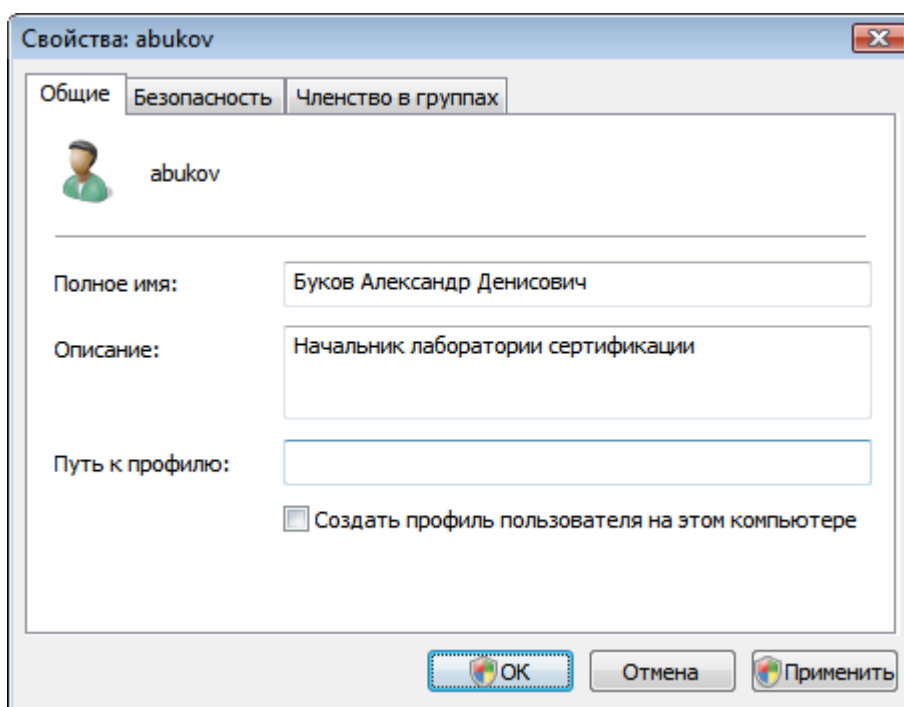
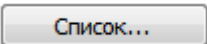



Рис. 59. Свойства пользователя – Общие.

## Свойства безопасности

Во вкладке **Безопасность** отображаются свойства пользователя, относящиеся к системе защиты. Допуск пользователя определяет максимальный гриф ресурса, доступный пользователю для чтения. Если пользователь является администратором системы защиты, флажок **Пользователь является администратором системы защиты** будет установлен. В поле **Идентификатор** отображается тип персонального идентификатора по умолчанию, а в поле **Состояние** – текущее состояние персонального идентификатора (см. Рис. 60). Нажав кнопку  можно просмотреть и отредактировать список созданных персональных идентификаторов пользователя (см. Рис. 57). Если список персональных идентификаторов пользователя пуст, состояние идентификатора будет иметь значение «Не сформирован». Если пользователю был изменен пароль, значение состояния идентификатора будет изменено на «Неактуален». Для сохранения изменений необходимо нажать кнопку .

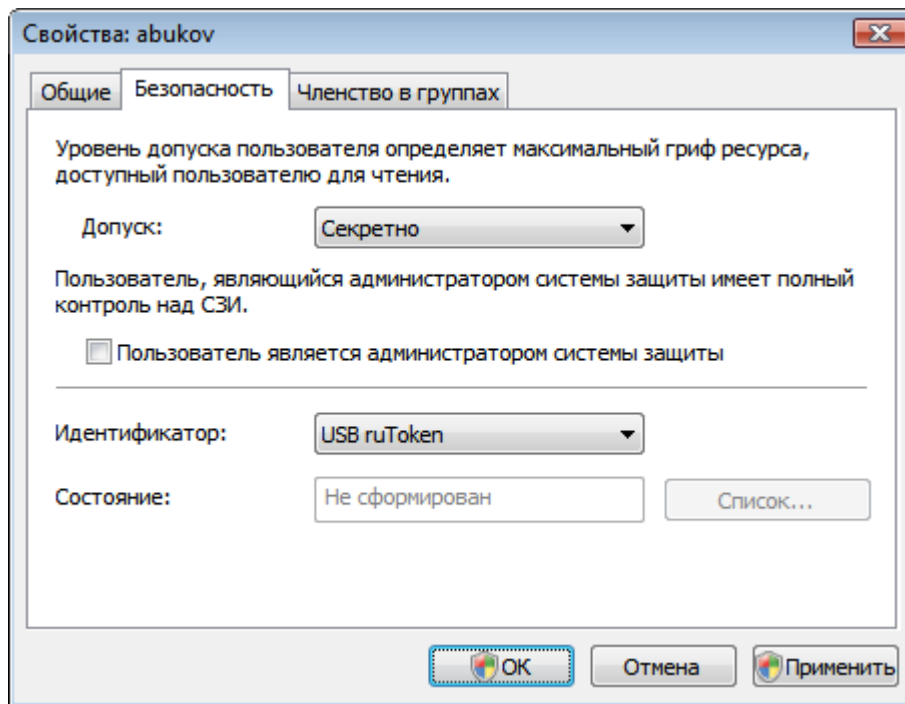


Рис. 60. Свойства пользователя – Безопасность.

### Членство в группах

Вкладка **Членство в группах** позволяет добавить пользователя в группы и удалить его из групп (см. Рис. 61).

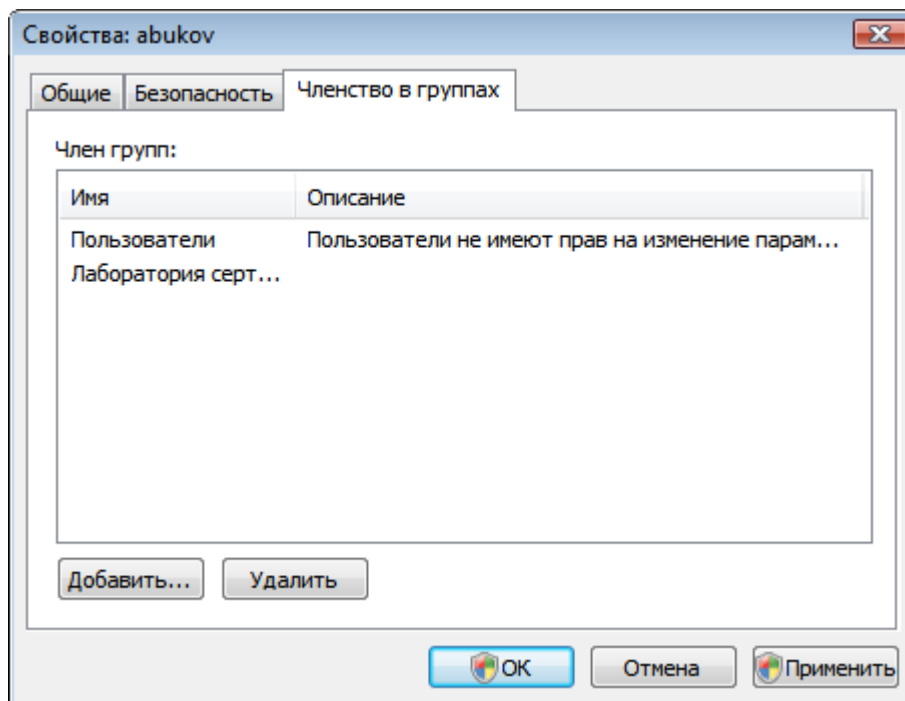


Рис. 61. Свойства пользователя – Членство в группах.

Для добавления пользователя в группу необходимо нажать кнопку **Добавить...** и ввести имя или выбрать необходимую группу. Для удаления пользователя из группы необходимо выбрать ее в списке и нажать кнопку **Удалить**. Для сохранения изменений необходимо нажать кнопку **ОК**.

## Формирование персональных идентификаторов

Для формирования персонального идентификатора пользователя необходимо выбрать его в списке пользователей и выбрать пункт меню **Пользователь | Сформировать идентификатор...** либо выбрать пункт **Сформировать идентификатор...** контекстного меню. Сформировать идентификатор пользователя можно, если в базе системы защиты сохранен его пароль. В противном случае соответствующие пункты меню будут недоступны. Формирование персонального идентификатора начинается с предъявления персонального идентификатора администратора системы защиты, с помощью которого был произведен вход в систему, как показано на Рис. 62.

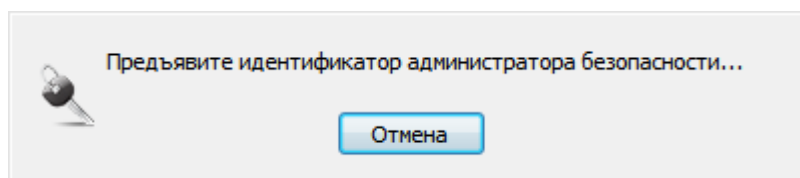


Рис. 62. Ожидание предъявления идентификатора администратора.

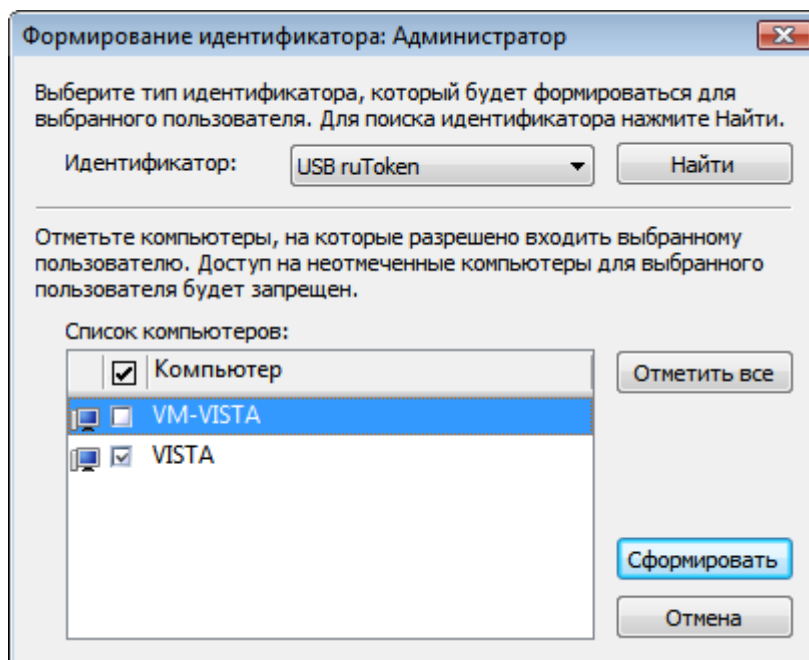
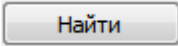


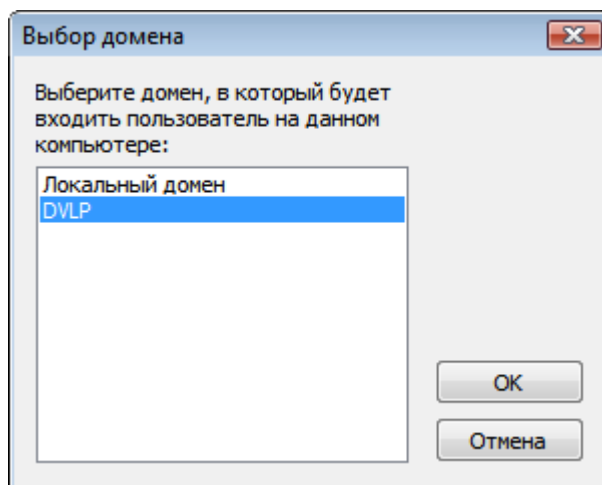
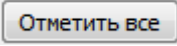
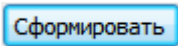


Рис. 63. Формирование идентификатора пользователя.

Персональный идентификатор администратора системы защиты предъявляется только один раз за сеанс работы программы. После успешного считывания предъявленного идентификатора на экране появляется диалог, как показано на Рис. 63. В поле **Идентификатор** отображается тип идентификатора, который будет формироваться. При отображении диалога в этом поле выводится тип идентификатора по умолчанию. Его можно изменить вручную или найти первый попавшийся идентификатор, нажав кнопку . В поле **Список компьютеров** отображен список компьютеров, который был считан с персонального идентификатора администратора. Если напротив имени компьютера изображена иконка , вход на этот компьютер осуществляется в локальный домен, если  - в сетевой. При необходимости можно заменить домен входа. Для этого необходимо выбрать компьютер, нажать правую клавишу мыши и выбрать пункт меню **Изменить домен входа...**. При этом на экране появится диалог, пример которого показан на Рис. 64.



*Рис. 64. Смена домена входа для компьютера.*

Перед формированием персонального идентификатора пользователя необходимо отметить компьютеры, вход на которые будет ему разрешен. Чтобы выбрать все компьютеры необходимо нажать кнопку . Для начала процедуры формирования персонального идентификатора необходимо нажать кнопку . При этом на экране появится диалог, предлагающий предъявить идентификатор пользователя выбранного типа (см. Рис. 65).



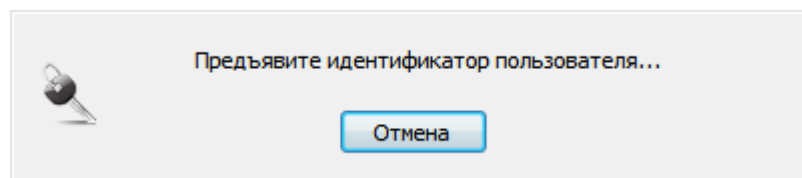


Рис. 65. Ожидание предъявления идентификатора пользователя.

После выполнения процедуры записи идентификатора на экране появится соответствующее сообщение.

### Чтение и очистка идентификаторов

Для чтения информации с персональных идентификаторов необходимо выбрать пункт меню **Идентификаторы | Считать** и далее пункт меню, соответствующий типу идентификатора, который необходимо считать. При этом появится диалог, предлагающий предъявить идентификатор выбранного типа. При выборе пункта меню **Первый найденный** считается первый идентификатор, который нашла система защиты. Если предъявленный идентификатор зарегистрирован в системе защиты и к нему подойдет сохраненный в базу пароль, он автоматически расшифруется, и на экран (см. Рис. 66) будет выведена следующая информация о считанном идентификаторе: имя пользователя, доступ пользователя, флаг администратора СЗИ, тип идентификатора и список компьютеров, на которые указанный пользователь может войти.

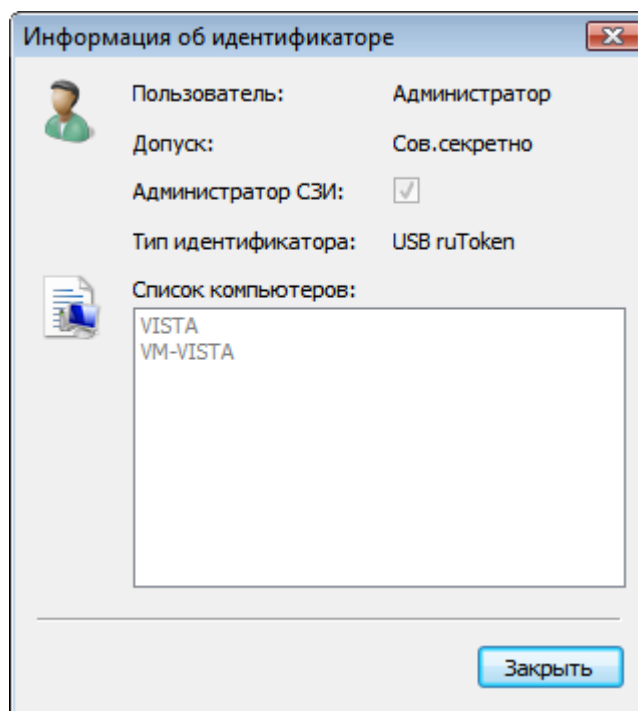
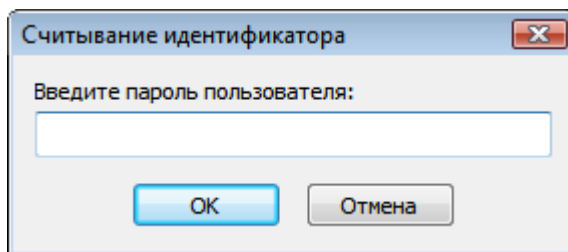


Рис. 66. Информация об идентификаторе.

Если предъявленный идентификатор не зарегистрирован в системе защиты, администратору будет предложено ввести пароль пользователя – владельца предъявленного идентификатора самостоятельно. В случае положительного ответа на экране появится запрос ввода пароля (см. Рис. 67). После ввода правильного пароля на экране вышеуказанная информация об идентификаторе.



*Рис. 67. Запрос ввода пароля пользователя – владельца идентификатора.*

Для очистки персонального идентификатора необходимо выбрать пункт меню **Идентификаторы | Очистить** и далее пункт меню, соответствующий типу идентификатора, который необходимо очистить. При этом появится диалог, предлагающий предъявить идентификатор выбранного типа. После выполнения процедуры очистки идентификатора на экране появится соответствующее сообщение.

### **Дополнительно**

При запуске программы считывание списка компьютеров и списка пользователей происходит автоматически. При необходимости их можно обновить. Для обновления списка компьютеров необходимо выбрать пункт меню **Компьютер | Обновить список компьютеров** или **Домен | Обновить список компьютеров**. Для обновления списка пользователей необходимо выбрать пункт меню **Компьютер | Обновить список пользователей** или **Домен | Обновить список пользователей** либо выбрать пункт **Обновить список пользователей** контекстного меню в пустой области списка пользователей.

Пункты меню **Вид** предназначены для управления внешним видом программы, например, видом и составом панелей инструментов.

# Работа с ресурсами

В данной главе приводятся сведения о назначении и применении программы **Менеджер файлов**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при работе с защищаемыми ресурсами.

Управление ресурсами, а также их защитными атрибутами, осуществляется с помощью программы **Менеджер файлов**, которая позволяет выполнять следующие операции:

- выполнение файловых операций над ресурсами;
- установка защитных атрибутов ресурсов;
- проверка целостности защищаемых ресурсов.

Для запуска программы **Менеджер файлов** необходимо выбрать пункт меню **Программы | Страж NT | Менеджер файлов**. При этом на экране появится окно, пример которого показан на Рис. 68.

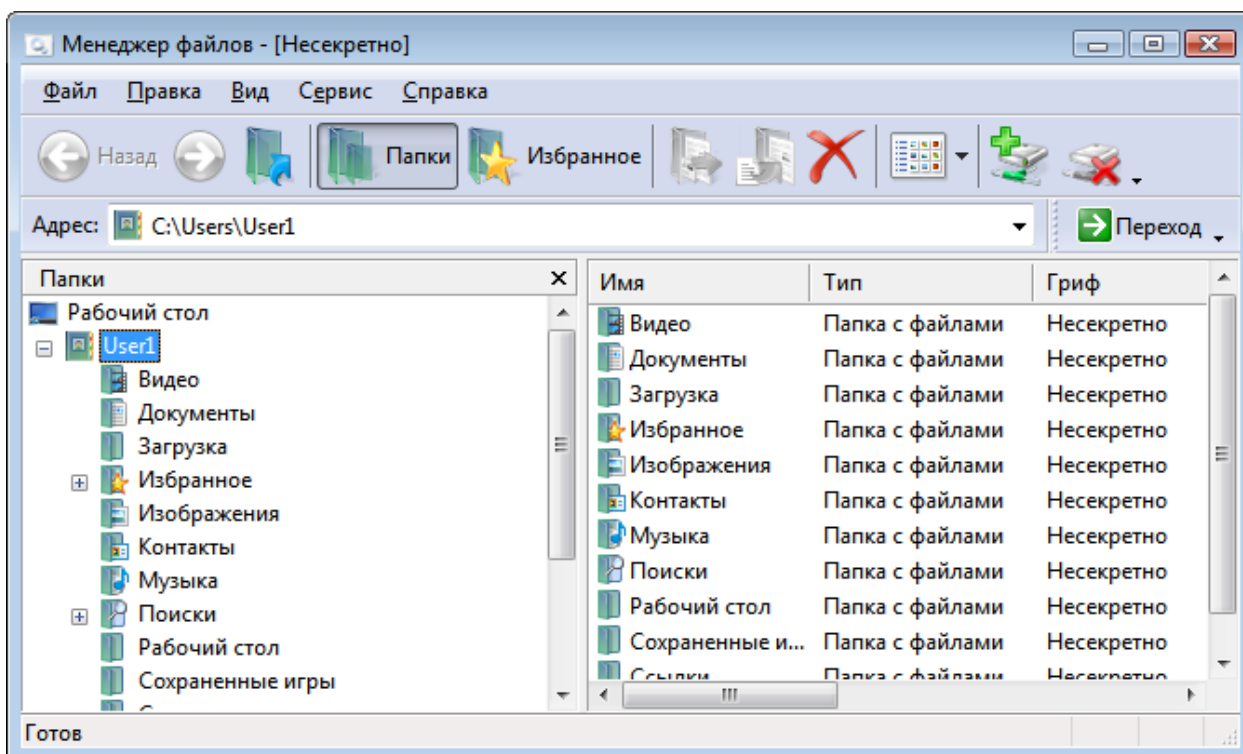







Рис. 68. Общий вид программы Менеджер файлов.



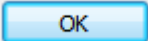
## Общие сведения

Интерфейс программы **Менеджер файлов** приближен к интерфейсу стандартной программы операционной системы **Проводник**. В левой части главного окна может располагаться панель папок (по умолчанию), отображающая дерево папок, либо панель

избранных папок. Правую часть главного окна занимает представление содержимого папки, выбранной в левой панели. Для отображения содержимого папки необходимо выбрать ее в левой панели либо ввести ее полный путь в панели инструментов **Адрес:** и нажать кнопку .

 Для папок, имена которых являются текстовыми представлениями идентификаторов безопасности (например, S-1-5-21-...), дополнительно в круглых скобках выводится соответствующее идентификатору безопасности имя. Примером таких папок являются дочерние папки Корзины (RECYCLER).

При перемещении по папкам сохраняется история выбранных папок. Перемещение по истории выбранных папок осуществляется нажатием на панели инструментов кнопок  и , а также путем выбора из выпадающего списка адресной строки в панели инструментов. Для перемещения в родительскую папку необходимо на панели инструментов нажать кнопку . Все вышеуказанные действия можно выполнить, выбирая пункты меню **Вид | Переход**.

Для отображения в левой части панели папок необходимо выбрать пункт меню **Вид | Панели обозревателя | Папки** либо в панели управления нажать кнопку . Для отображения в левой части панели избранных папок необходимо выбрать пункт меню **Вид | Панели обозревателя | Избранное** либо в панели управления нажать кнопку . Для добавления ссылки на папку в панель избранных папок необходимо выбрать папку в панели папок и выбрать пункт меню **Сервис | Добавить в Избранное...**. При этом на экране появится диалог, как показано на Рис. 69, в котором необходимо будет ввести имя, под которым ссылка на выбранную папку будет отображаться в панели избранных папок, и нажать кнопку . Для удаления ссылки на папку из панели избранных папок необходимо вызвать ее контекстное меню и выбрать пункт **Удалить ссылку**.

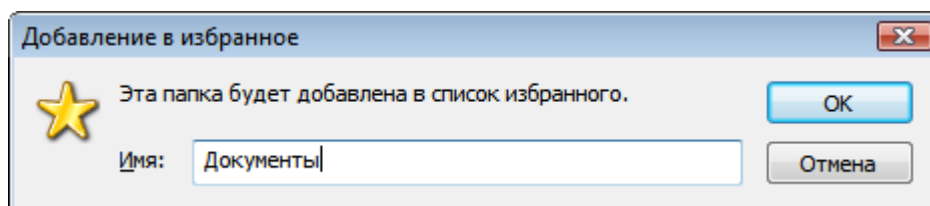




Рис. 69. Диалог добавления ссылки в панель Избранное.


Функции подключения и отключения сетевых дисков доступны в меню **Сервис** либо в панели инструментов (кнопки  и ).

Для обновления дерева папок в панели папок и содержимого выбранной папки необходимо выбрать пункт меню **Вид | Обновить**.

Используя пункты меню **Вид | Панели инструментов** можно управлять отображением панелей инструментов, настраивать их, управлять так называемыми «горячими клавишами», а также изменять общий вид программы. Список «горячих клавиш» по умолчанию приведен ниже.

Сочетание клавиш	Действие
Alt + <Стрелка влево>	Перемещение по истории выбранных папок назад.
Alt + <Стрелка вправо>	Перемещение по истории выбранных папок вперед.
Ctrl + F6 Ctrl + Tab	Переход фокуса ввода на следующую панель.
Ctrl + Shift + F6 Ctrl + Shift + Tab	Переход фокуса ввода на предыдущую панель.
Ctrl + F	Включение/отключение панели избранных папок.
F5	Обновление дерева папок и содержимого выбранной папки.
Ctrl + A	Выделение всех объектов.
Ctrl + C Ctrl + Ins	Выбор выделенных объектов для операции копирования.
Ctrl + X	Выбор выделенных объектов для операции перемещения.
Ctrl + V Shift + Ins	Выполнение операции копирования или перемещения для выбранных объектов.
Del	Удаление выделенных объектов в Корзину.
Shift + Del	Безвозвратное удаление выделенных объектов.

## Представление файлов и папок

Список ресурсов может быть представлен как значки, список, плитка и таблица. Различные представления доступны в меню папки **Вид** либо в панели инструментов (кнопка ) , а также из контекстного меню папки. В представлениях «Значки» и «Плитка» файлы и папки отображаются в виде значков, рядом с которыми выводится имя файла или папки. В представлении «Список» содержимое папки выводится в виде списка имен файлов или папок, впереди каждого из которых стоит маленький значок. В представлении «Таблица» для каждого ресурса отображается детализированная информация, такая как тип, гриф, режим запуска, владелец и время изменения. Для файлов дополнительно отображается их размер. Для упорядочивания содержимого папки необходимо нажать левую клавишу мыши над соответствующим столбцом представления. При этом выбранный столбец будет отмечен значком направления упорядочивания. Для изменения направления необходимо еще раз нажать левую клавишу мыши над этим столбцом.

### Выбор столбцов

Выбор отображаемых столбцов, их ширину, а также порядок их отображения можно выполнить, нажав правую клавишу мыши над любым из столбцов или вызвав пункт меню **Вид | Выбор столбцов в таблице...** .

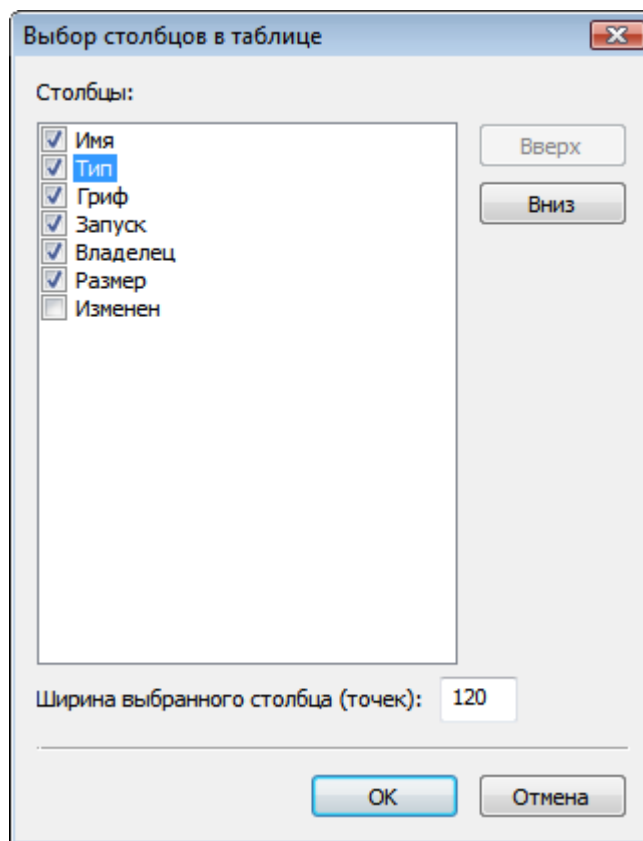
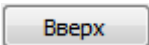
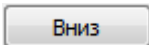
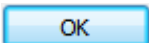


Рис. 70. Выбор отображаемых столбцов.

При этом на экране появится диалог, как показано на Рис. 70. Столбец отображается в табличном представлении, если флажок напротив его названия установлен. В противном случае столбец не отображается. Для изменения порядка отображения столбца необходимо выбрать его и, используя кнопки  и , задать ему требуемое положение. Столбец **Имя** не может быть скрыт или перемещен. Для каждого столбца можно указать его ширину. Для этого необходимо его выделить и в поле **Ширина выбранного столбца (точек)**: задать требуемое значение. Для сохранения сделанных изменений необходимо нажать кнопку .

## Файловые операции

С помощью программы **Менеджер файлов** можно выполнять следующие файловые операции: создание, копирование, перемещение, переименование, удаление ресурсов, а также все другие операции, доступные через контекстное меню. Для выполнения операции необходимо выбрать объекты, над которыми будет проводиться операция, и выбрать соответствующие пункты меню **Правка** или контекстного меню. Чтобы выделить несколько объектов, необходимо выделять их левой клавишей мыши, удерживая клавишу Ctrl. Для выделения всех объектов необходимо выбрать пункт меню **Правка | Выделить все**. Чтобы инвертировать выделение (снять выделение со всех выделенных ресурсов и выделить те, которые не были выделены), необходимо выбрать пункт меню **Правка | Обратить выделение**.

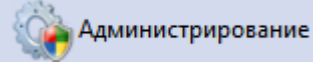
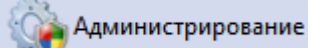
Некоторые операции можно выполнить, нажав соответствующую кнопку на панели инструментов. Такие операции как копирование, перемещение и создание ярлыка можно выполнить с помощью стандартных механизмов «перетаскивания» объектов.

## Работа с файловыми ресурсами

С помощью программы **Менеджер файлов** над файловыми ресурсами можно выполнять следующие операции:

Операция	Доступ
Назначение списка разграничительного контроля доступа (редактирование разрешений)	Всем пользователям в рамках своих полномочий
Назначение системного списка контроля доступа (редактирование параметров системного аудита) Изменение владельца	Пользователям, входящим в локальную группу администраторов
Проверка целостности	Всем пользователям

Операция	Доступ
Назначение грифа документов	
Установка режима запуска и допуска программ	
Редактирование параметров дополнительного аудита	Администраторам системы защиты в режиме администрирования
Установка параметров целостности	

Некоторые операции можно выполнить только в режиме администрирования. Для перехода в режим администрирования необходимо выбрать пункт меню **Файл | Администрирование** или нажать кнопку  на панели инструментов. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей, на экране появится окно, как показано на Рис. 71. Для включения режима администрирования необходимо нажать кнопку . Для выхода из режима администрирования необходимо еще раз выбрать пункт меню **Файл | Администрирование** или нажать кнопку  на панели инструментов.

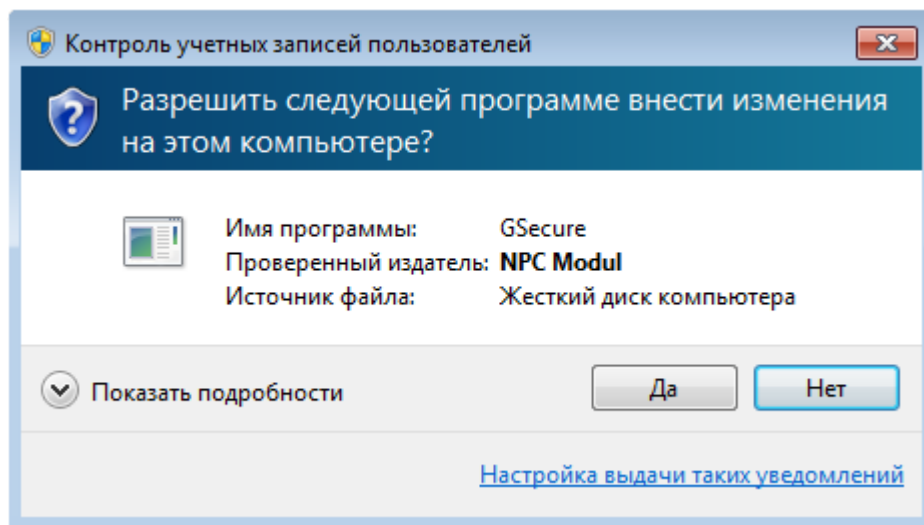


Рис. 71. Сообщение подсистемы контроля учетных записей пользователей.



*Изменение параметров безопасности для корневых папок носителей осуществляется в программе **Учет носителей**.*

### Редактирование разрешений

Для редактирования разрешений необходимо выбрать пункт **Свойства** из контекстного меню выбранных объектов. В появившемся окне свойств необходимо выбрать вкладку **Безопасность** (см. Рис. 72), в которой выводится окно редактора списка контроля доступа, отображающий дискреционный список контроля доступа выбранных объектов.



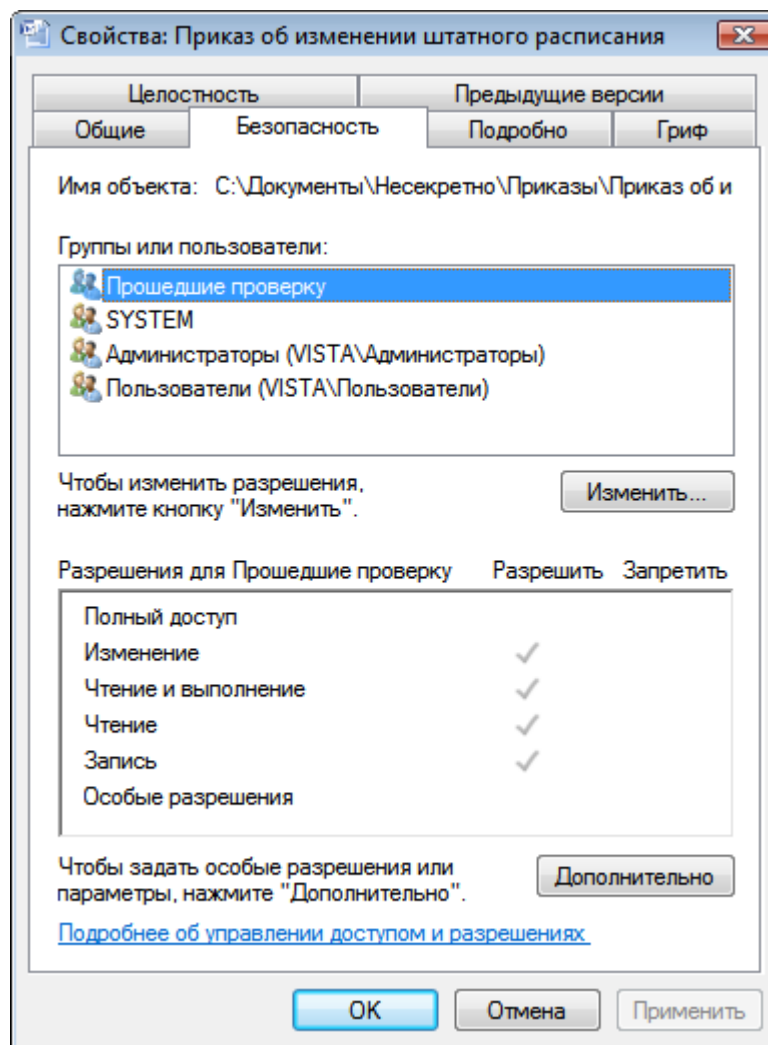


Рис. 72. Свойства выбранных объектов – Безопасность.

Для добавления записи в дискреционный список контроля доступа необходимо последовательно нажать кнопки **Изменить...** и **Добавить...**. В появившемся окне необходимо ввести имя пользователя или группы пользователей либо выбрать их из списка, который появляется при последовательном нажатии кнопок **Дополнительно...** и **Поиск**. После выбора субъекта доступа необходимо задать ему маску доступа. Для удаления пользователя или группы пользователей из дискреционного списка контроля доступа необходимо выбрать их и последовательно нажать кнопки **Изменить...** и **Удалить**.

Нажав кнопку **Дополнительно**, можно получить более подробную информацию о списке разграничительного контроля доступа.



Элементы интерфейсов редактора ACL могут отличаться от представленных. Более подробную информацию о редакторе ACL можно получить в документации на операционную систему.

### Изменение владельца

Для отображения владельца необходимо выбрать пункт **Свойства** из контекстного меню выбранных объектов. В появившемся окне свойств необходимо выбрать вкладку **Безопасность** и нажать кнопку **Дополнительно**, затем выбрать вкладку **Владелец** (см. Рис. 73).

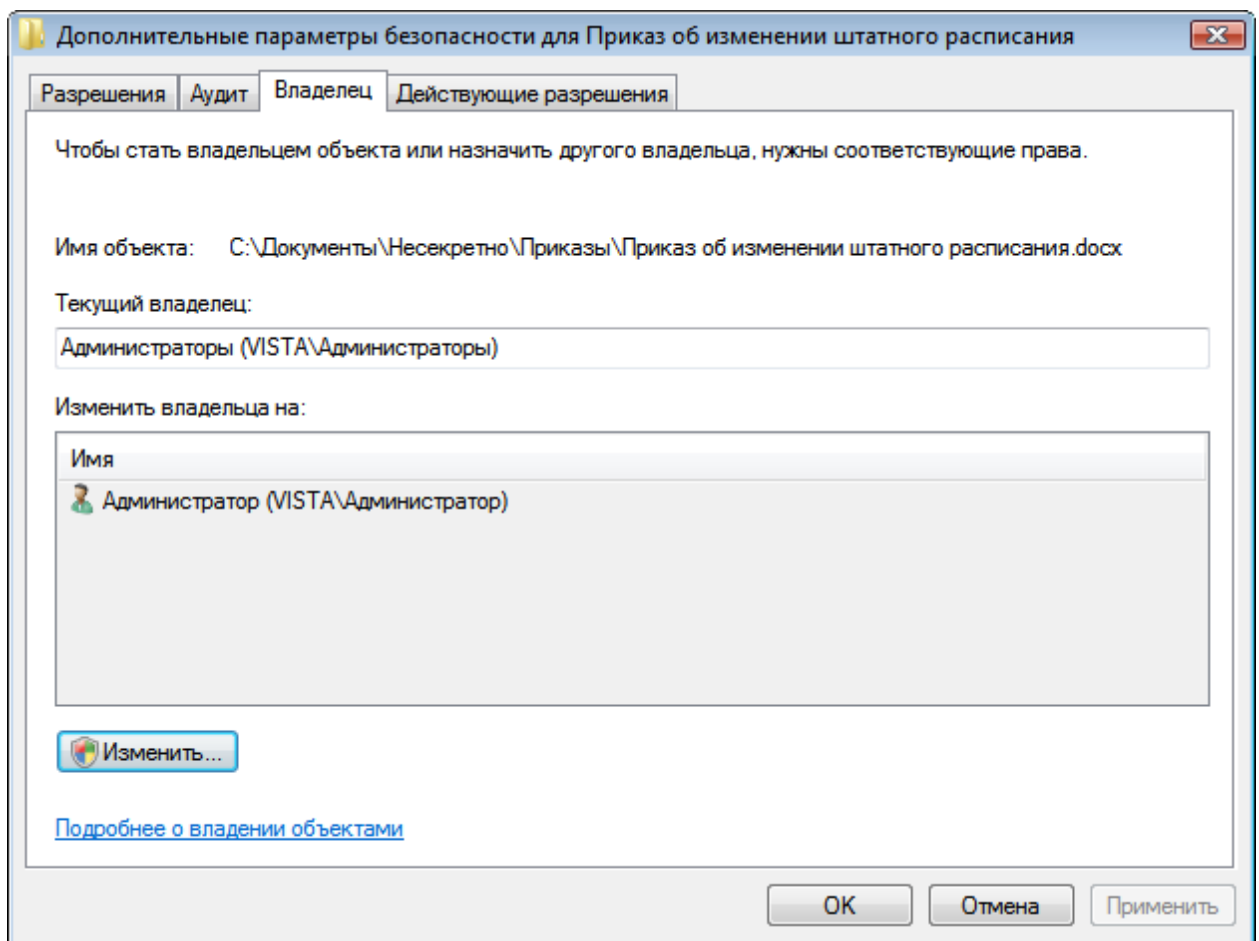


Рис. 73. Свойства выбранных объектов – Владелец.

Для изменения владельца необходимо нажать кнопку **Изменить...** и в поле **Изменить владельца на:** выбрать нового владельца и нажать кнопку **ОК** или **Применить**. Если в вышеуказанном поле отсутствует необходимая учетная запись необходимо нажать кнопку **Другие пользователи или группы...** и выбрать требуемого пользователя или группу пользователей как описано в предыдущем разделе.



Элементы интерфейсов редактора ACL могут отличаться от представленных. Более подробную информацию о редакторе ACL можно получить в документации на операционную систему.

### Редактирование параметров системного аудита

Для отображения параметров системного аудита необходимо выбрать пункт **Свойства** из контекстного меню выбранных объектов. В появившемся окне свойств необходимо выбрать вкладку **Безопасность** и нажать кнопку **Дополнительно**, затем выбрать вкладку **Аудит**. Если режим администрирования включен, необходимо нажать кнопку **Изменить...**, в противном случае – кнопку **Продолжить**, и на экране появится окно, отображающее список системного аудита выбранных объектов (см. Рис. 74).

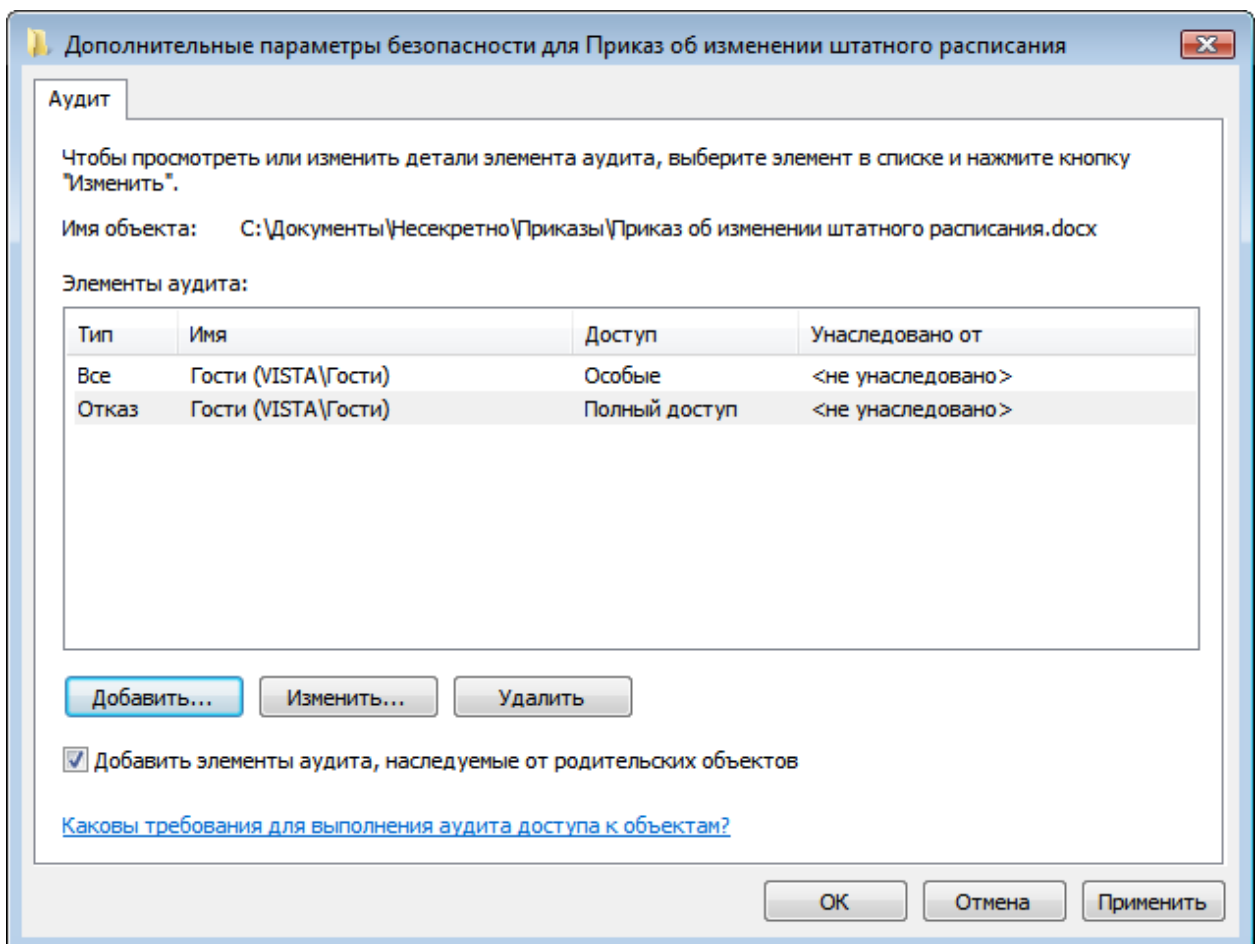


Рис. 74. Свойства выбранных объектов – Аудит.

Принцип работы со списком системного аудита такой же, как и со списком разграничительного контроля доступа.

## Назначение грифа

Назначение грифа можно выполнить только в режиме администрирования. Для назначения грифа необходимо выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Гриф** (см. Рис. 75).

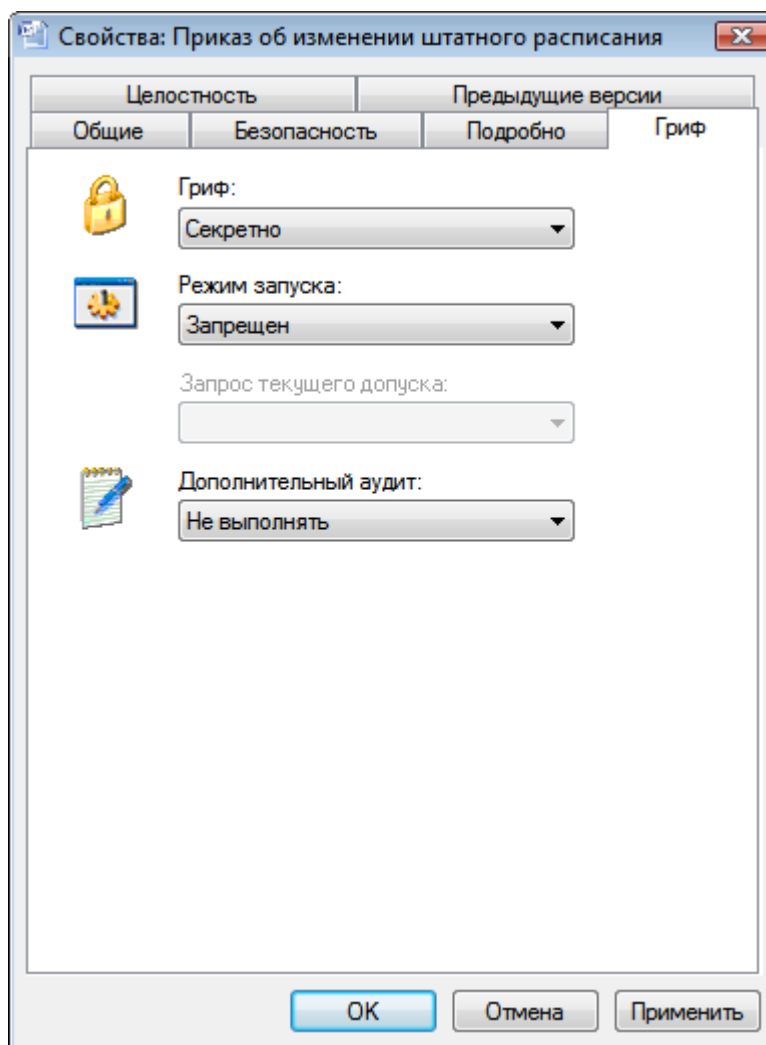
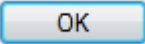
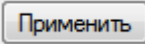


Рис. 75. Свойства выбранных объектов – Гриф и режим запуска.

Для изменения грифа выбранных объектов необходимо выбрать соответствующее значение из раскрывающегося списка в поле **Гриф:** и для сохранения сделанных изменений нажать кнопку **OK** или **Применить**.

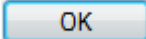

## Установка режима запуска и допуска

Установку режима запуска и допуска можно выполнить только в режиме администрирования и только для файлов. Для установки режима запуска и допуска необходимо выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Гриф** (см. Рис. 75).

Для изменения режима запуска выбранных объектов необходимо выбрать соответствующее значение из раскрывающегося списка в поле **Режим запуска**:. Если значение поля **Режим запуска** отлично от «Запрещен» и значение поля **Гриф** выше «Несекретно», необходимо также определить значение поля **Запрос текущего допуска**. Для сохранения сделанных изменений нажать кнопку  или .

### Редактирование параметров дополнительного аудита

Редактирование параметров дополнительного аудита можно выполнить только в режиме администрирования. Для редактирования параметров дополнительного аудита необходимо выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Гриф** (см. Рис. 75).

Для изменения параметров дополнительного аудита выбранных объектов необходимо выбрать соответствующее значение из раскрывающегося списка в поле **Дополнительный аудит**: и для сохранения сделанных изменений нажать кнопку  или .

### Дополнительные параметры для папок

При выборе вкладки **Гриф** для папки на экране появится следующий диалог (см. Рис. 76). Поля **Режим запуска** и **Запрос текущего допуска** для свойств папки будут неактивны.

При установке флажка **Проверять разрешения для папки при доступе к вложенным объектам** при попытках доступа к дочерним ресурсам выбранной папки будут проверяться и учитываться установленные для данной папки разрешения.

При установке флажка **Сменить параметры для подпапок** все установленные параметры для данной папки будут установлены для всех дочерних подпапок.

При установке флажка **Сменить параметры для существующих файлов** все установленные параметры для данной папки кроме флага **Проверять разрешения для папки при доступе к вложенным объектам** будут установлены для всех файлов, находящихся в данной папке.

Если установлены оба вышеуказанных флажка, все установленные параметры для данной папки будут установлены для всех подпапок и файлов, в них входящих.

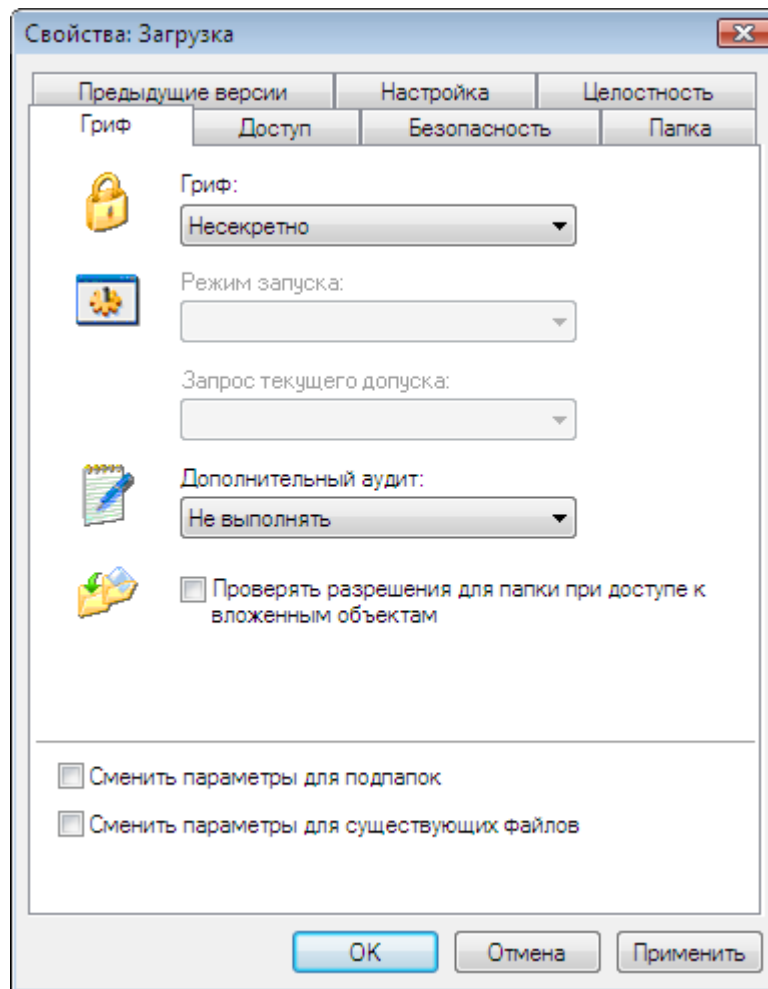


Рис. 76. Свойства выбранных папок – Гриф.

### Установка параметров целостности

Установку параметров целостности можно выполнить только в режиме администрирования. Для установки параметров целостности необходимо выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Целостность** (см. Рис. 77).

При выборе вкладки **Целостность** для папки автоматически будет установлен флажок **Сменить параметры для существующих файлов**, который недоступен для изменения. Это означает, что установить параметры целостности можно только для файлов.

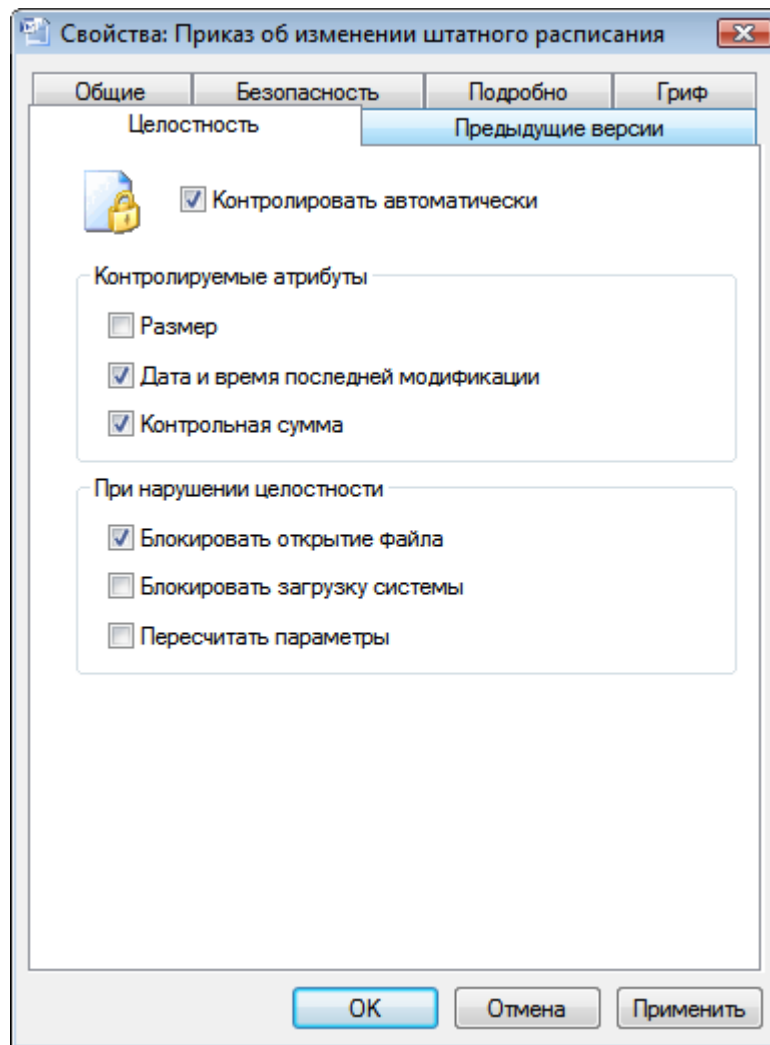


Рис. 77. Свойства выбранных объектов – Целостность.

### Проверка целостности

Проверка целостности осуществляется путем выбора пункта **Проверить целостность** контекстного меню выбранного файла. При этом на экране появится сообщение о результатах проверки (см. Рис. 78).

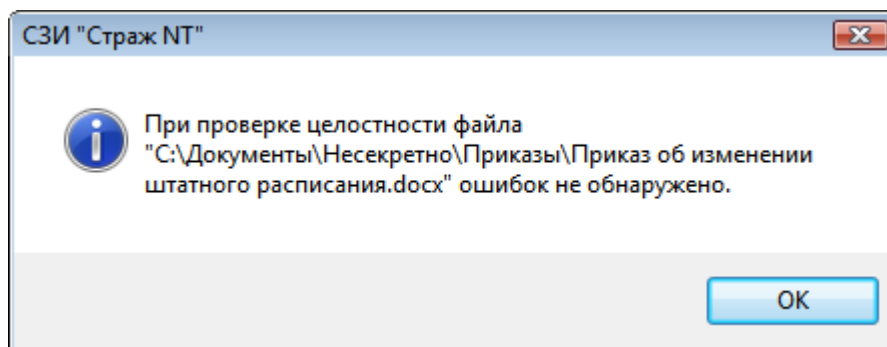


Рис. 78. Сообщение о результате проверки целостности файла.

## Работа с принтерами

С помощью программы **Менеджер файлов** можно выполнять следующие операции над принтерами:

Операция	Доступ
Назначение списка разграничительного контроля доступа (редактирование разрешений)	Всем пользователям в рамках своих полномочий
Изменение владельца	Пользователям, входящим в локальную группу администраторов
Назначение грифа	Администраторам системы защиты в режиме администрирования

Для просмотра и редактирования свойств принтера необходимо открыть необходимый принтер, как показано на Рис. 79, и выбрать пункт **Свойства принтера** из контекстного меню.

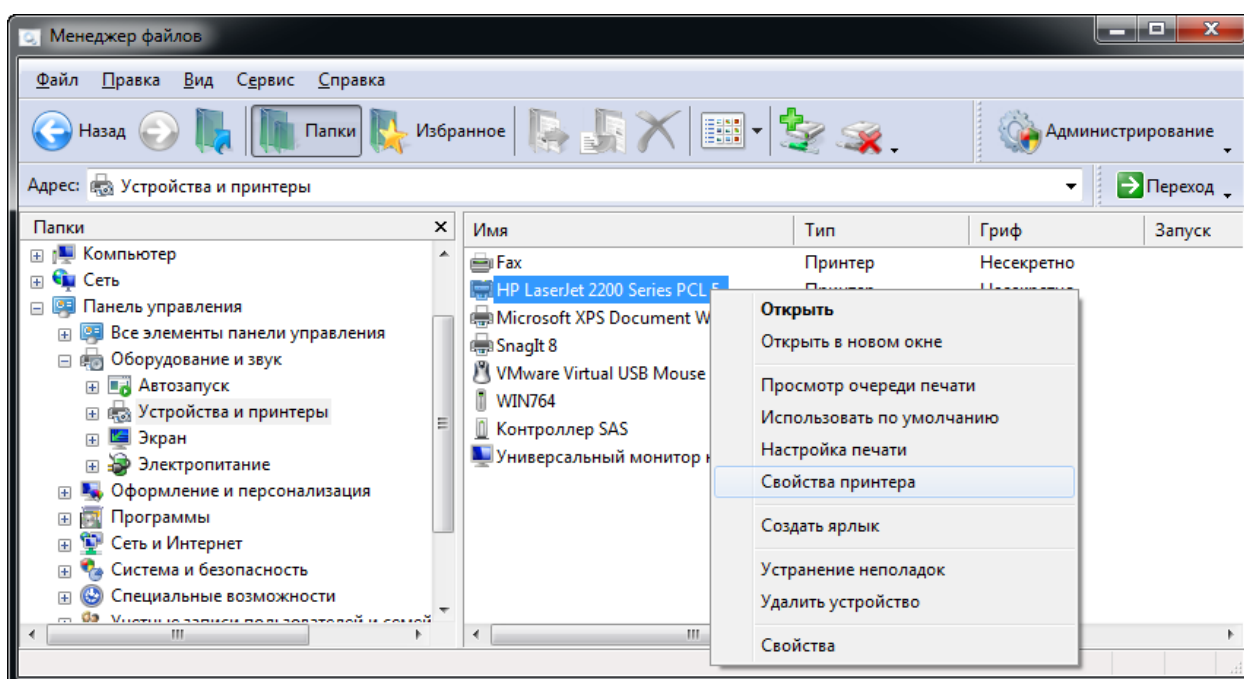


Рис. 79. Выбор свойств принтера.

### Редактирование разрешений и смена владельца

В появившемся окне свойств для редактирования разрешений или смены владельца необходимо выбрать вкладку **Безопасность** (см. Рис. 80), в которой выводится окно редактора списка контроля доступа, отображающий дискреционный список контроля доступа выбранного принтера. Нажав кнопку **Дополнительно**, можно получить более подробную информацию о списке разграничительного контроля доступа, а также изменить



владельца принтера. Порядок действий для изменения разрешений и владельца принтера такой же как и для файловых объектов.

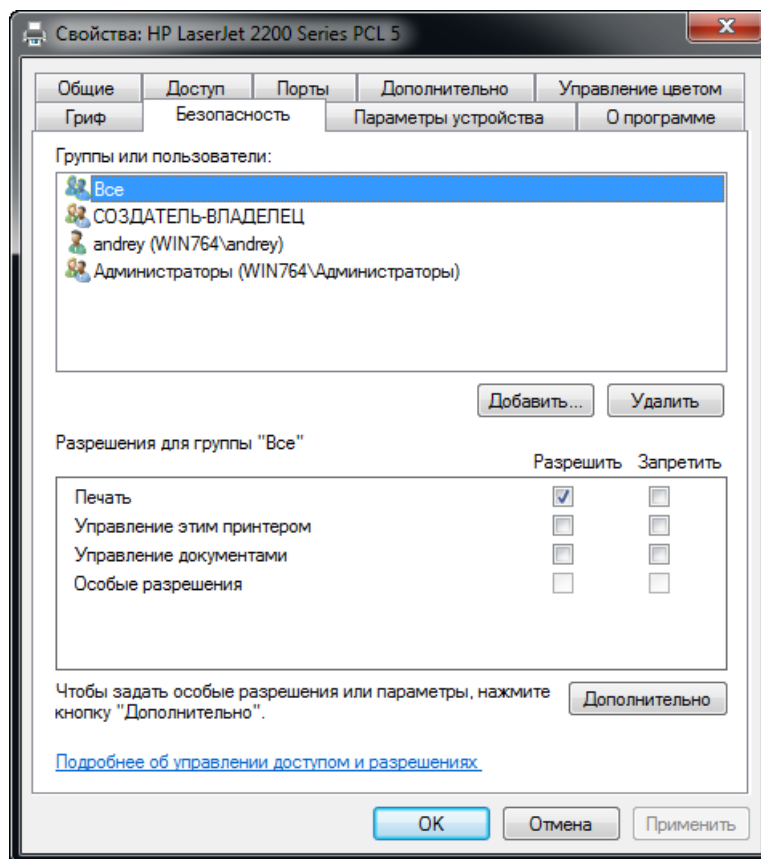




Рис. 80. Свойства принтера – Безопасность.

### Назначение грифа

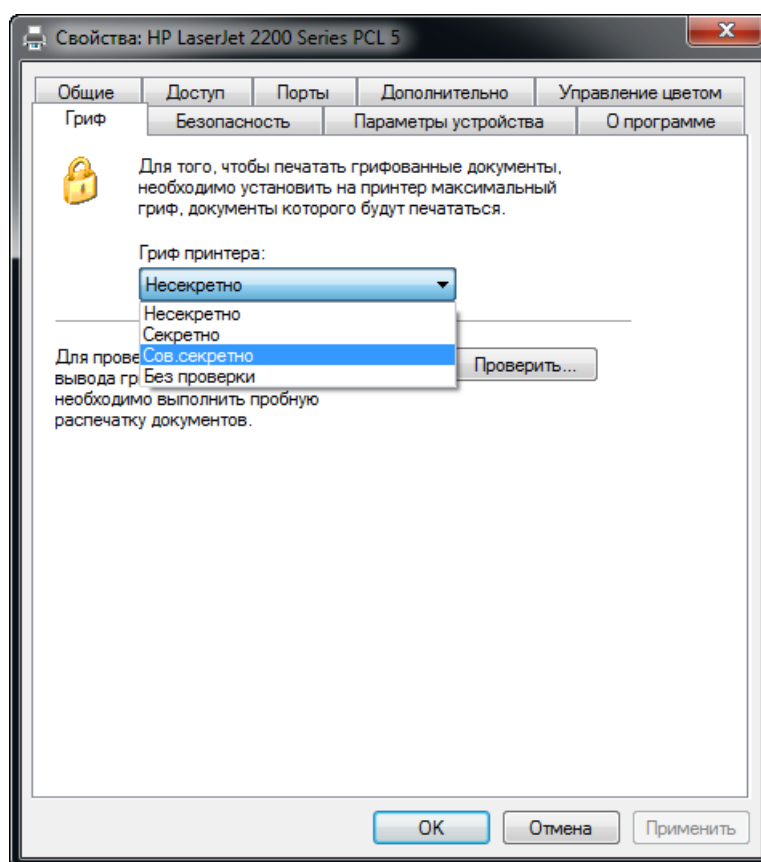
Операцию по назначению грифа принтера можно выполнить только в режиме администрирования. Для перехода в режим администрирования необходимо выбрать пункт меню **Файл | Администрирование** или нажать кнопку  **Администрирование** на панели инструментов. При использовании операционной системы Microsoft Windows Vista, Windows Server 2008 или Windows 7 с включенным режимом контроля учетных записей (UAC – User Account Control) на экране появится окно, как показано на Рис. 71. Для включения режима администрирования необходимо нажать кнопку **Разрешить**. Для выхода из режима администрирования необходимо еще раз выбрать пункт меню **Файл | Администрирование** или нажать кнопку  **Администрирование** на панели инструментов.

Гриф принтера выставляется, исходя из следующих правил:

- Метка 1 («Несекретно») позволяет выводить на печать только документы с грифом Метки 1 (несекретные);

- Метка 2 («Секретно») позволяет выводить на печать только документы с грифом Метки 2 (секретные);
- Метка 3 («Сов.секретно») позволяет выводить на печать документы с грифами Метки 2 и Метки 3 (секретные и совершенно секретные);
- гриф «Без проверки» позволяет выводить на печать документы любого грифа.

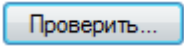
Для назначения грифа принтера необходимо выбрать пункт **Свойства принтера** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Гриф** (см. Рис. 81). В выбранной вкладке необходимо выбрать соответствующее значение из раскрывающегося списка в поле **Гриф принтера:** и для сохранения сделанных изменений нажать кнопку **ОК** или **Применить**.



*Рис. 81. Свойства принтера – Гриф.*

Для выдачи грифованных документов на печать может понадобиться дополнительная настройка системы защиты, которая зависит от установленных драйверов на используемый принтер. Типовая настройка подсистемы печати заключается в применении соответствующего шаблона, который можно найти на [сайте продукта](#), или в установке на папки `%SystemRoot%\system32\spool\PRINTERS`, `%SystemRoot%\Temp`, `%Temp%` грифа

«Без проверки», а на файл `%SystemRoot%\system32\spoolsv.exe` – режима запуска «Сервер-приложение».

Для проверки корректности настройки подсистемы печати необходимо нажать кнопку . При этом на печать должны быть выданы тестовые страницы документов всех трех грифов.

Если указанные действия не приведут к положительному результату, то необходимо воспользоваться механизмами дополнительного аудита или обратиться в службу технической поддержки.

# Контроль устройств

В данной главе приводятся сведения о назначении и применении программы **Контроль устройств**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты.

СЗИ «Страж NT» контролирует доступ ко всем устройствам, присутствующим в компьютере. Программа **Контроль устройств** предназначена для настройки правил работы системы защиты с устройствами компьютера.

Программа **Контроль устройств** запускается при выборе администратором системы защиты в программном меню пункта **Программы | Страж NT | Контроль устройств**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей, при запуске программы на экране появится окно, как показано на Рис. 82. Для продолжения необходимо нажать кнопку .

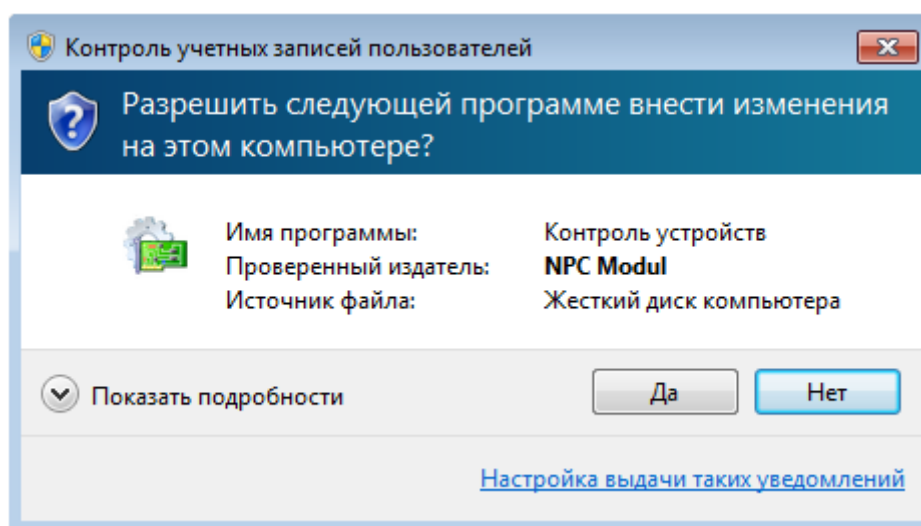


Рис. 82. Сообщение подсистемы контроля учетных записей пользователей.

При этом на экране появляется диалоговое окно, пример которого показан на Рис. 83.

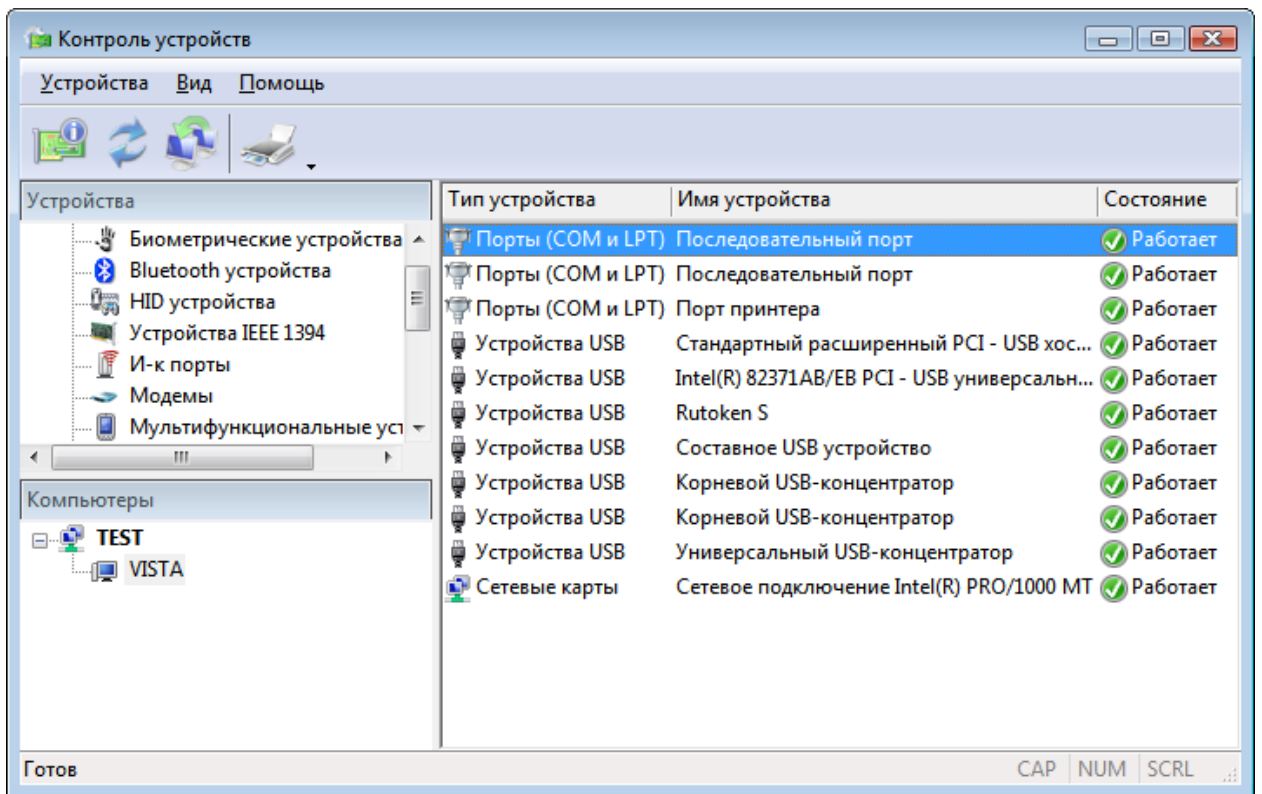


Рис. 83. Общий вид окна программы Контроль устройств.

Слева вверху отображён список групп контролируемых устройств. Слева внизу находится список компьютеров, входящих в рабочую группу или домен. Справа представлен список присутствующих на выбранном компьютере устройств с их свойствами:

Имя поля	Описание
Тип устройства	Определяет тип устройства, присутствующего на данный момент в системе.
Имя устройства	Определяет имя устройства, присутствующего на данный момент в системе.
Состояние	Определяет состояние устройства (работает либо остановлено).

## Редактирование свойств для групп устройств

При установке системы защиты для всех групп устройств устанавливаются разрешения по умолчанию: всем пользователям, системе, локальным администраторам – полный доступ. Для просмотра и редактирования разрешений для выбранной группы устройств необходимо выбрать пункт меню **Устройства | Свойства** и в появившемся диалоговом окне, пример которого показан на Рис. 84, выбрать вкладку **Безопасность**. При этом

выводится окно редактора списка контроля доступа, в котором отображается дискреционный список контроля доступа для выбранной группы устройств.

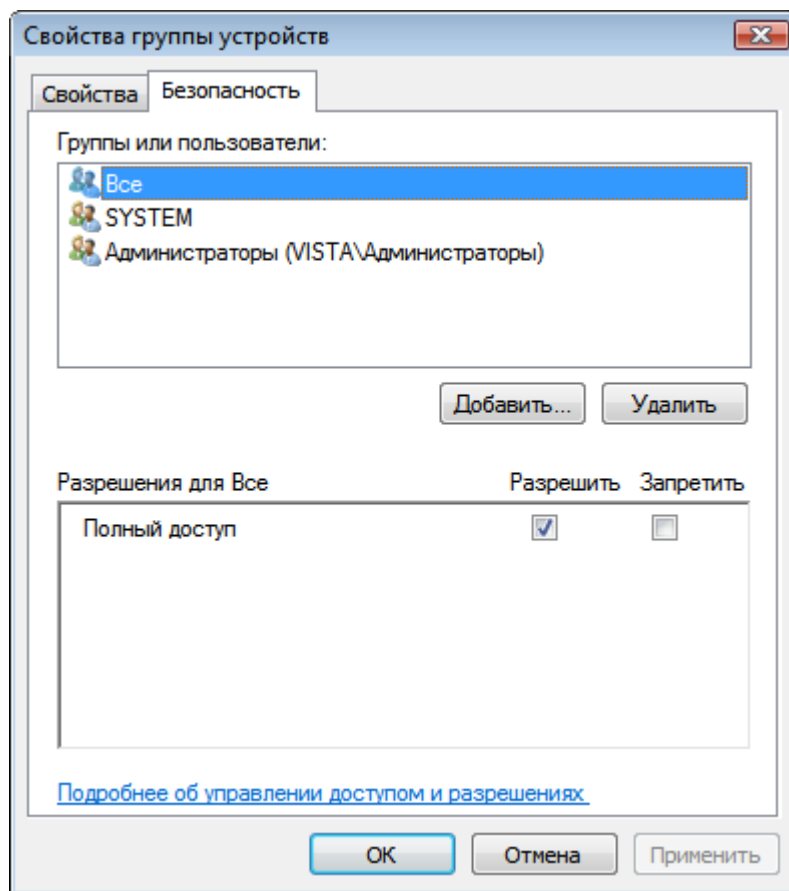


Рис. 84. Свойства группы устройств.

### Экспорт настроек

Для экспорта настроек на другие компьютеры необходимо выбрать пункт меню **Устройства | Экспорт настроек**. После этого на экране появится мастер экспорта настроек (см. Рис. 85). В данном окне необходимо выбрать группы устройств, параметры которых будут экспортироваться, и нажать кнопку **Далее >**. На экране появится окно выбора компьютеров (см. Рис. 86).

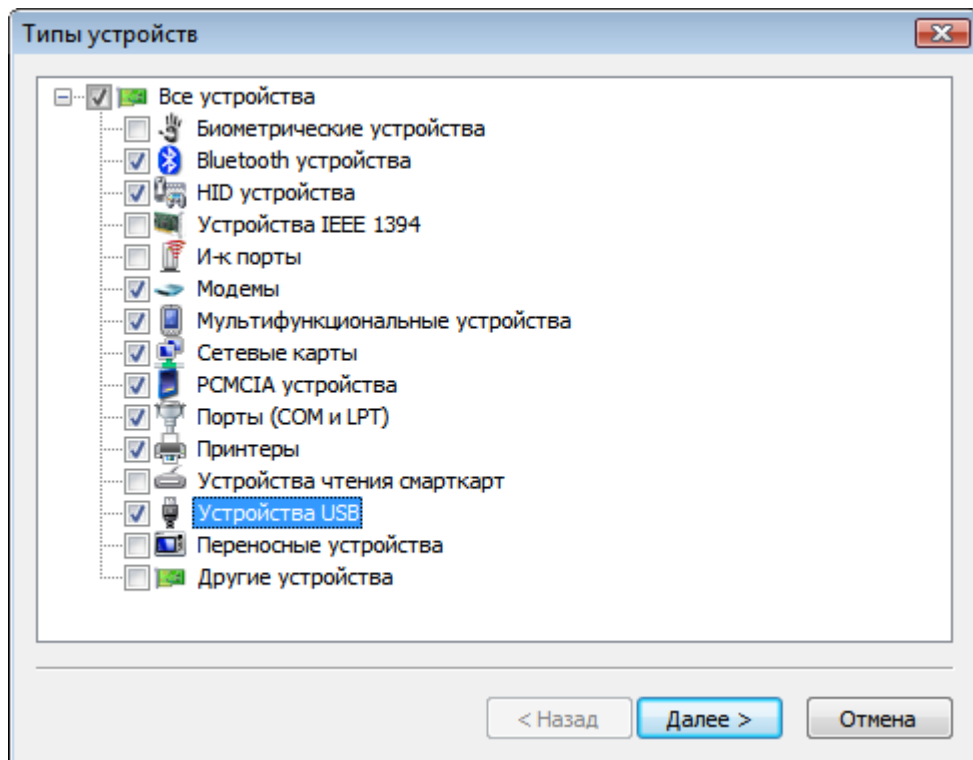


Рис. 85. Мастер экспорта настроек – выбор параметров групп устройств.

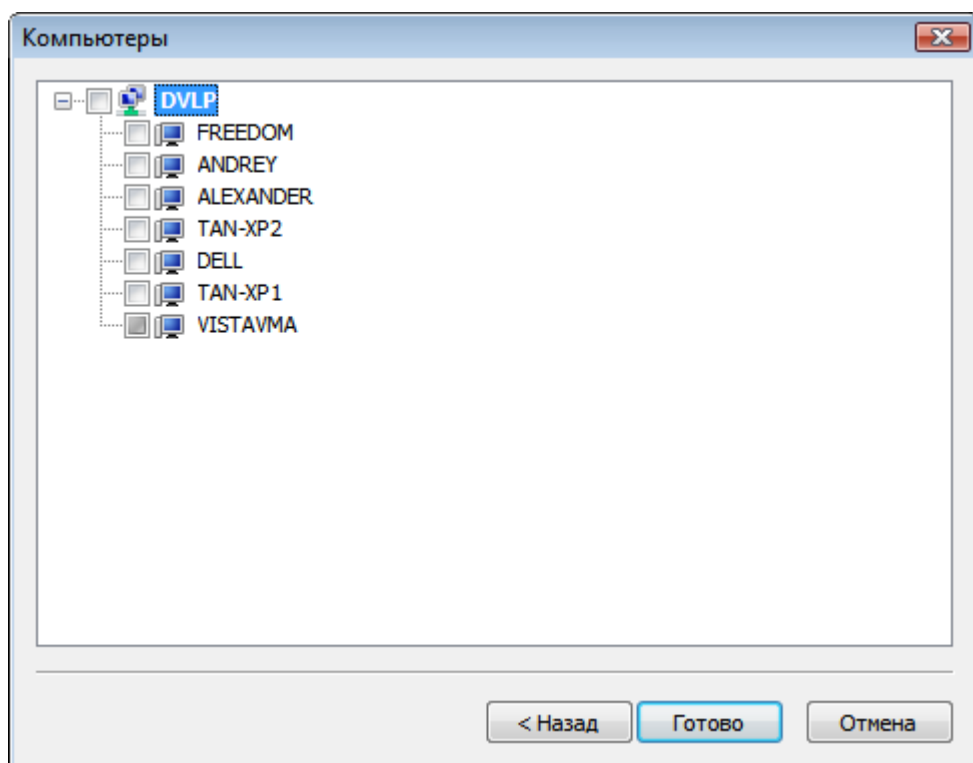
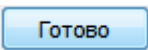


Рис. 86. Мастер экспорта настроек – выбор компьютеров.

После нажатия кнопки  настройки будут перенесены на отмеченные компьютеры.

# Журнал событий

---

В данной главе приводятся сведения о механизмах подсистемы регистрации, а также о назначении и применении программы **Журнал событий**, ее экранные формы и параметры. Также описаны типовые действия администратора системы защиты при работе с журналом событий.

Подсистема регистрации обеспечивает регистрацию запросов на доступ к ресурсам компьютера и возможность выборочного ознакомления с регистрационной информацией и ее распечатки. Хранение событий системы защиты осуществляется в файле журнала событий `%SystemRoot%\Guard\GReport.mdb` в формате базы данных Microsoft Access. При достижении размера этого файла в 1Гб он переносится в папку `%SystemRoot%\Guard\Reports` с новым именем формата "YYMMDD\_HHMM". На его место копируется пустая база из резервной копии.



*Более подробные сведения о механизмах подсистемы регистрации можно найти в документе **МАНУ.00030-01 з1. Система защиты информации от несанкционированного доступа «Страж NT». Версия 3.0. Описание применения.***

Программа **Журнал событий** предназначена для работы с журналом событий системы защиты и позволяет выполнять следующие функции:

- просмотр списка событий;
- просмотр свойств выбранного события;
- применение фильтра при просмотре списка событий;
- сортировка событий по основным полям;
- поиск событий в журнале по любому из критериев;
- сохранение журнала;
- очистка журнала;
- печать журнала.

Программа **Журнал событий** обеспечивает просмотр всех предусмотренных в СЗИ событий, а также фактов печати документов. **Журнал событий** позволяет осуществлять выборочное ознакомление с регистрационной информацией путем сортировки журналов по любому из полей отображения, применения различных фильтров при выборке записей из журнала, а также поиска записей по основным полям. Кроме того в программе



предусмотрена возможность архивирования, очистки и распечатки журнала, а также просмотра ранее сохраненных журналов.

Программа **Журнал событий** запускается при выборе администратором системы защиты в программном меню пункта **Программы | Страж NT | Журнал событий**. При этом на экране появляется диалоговое окно, пример которого показан на Рис. 87.

Слева сверху отображён список групп событий. Все события в системе защиты делятся на группы **События СЗИ** и **События печати**, внутри которых администратор системы защиты может создавать свои группы с необходимыми параметрами.

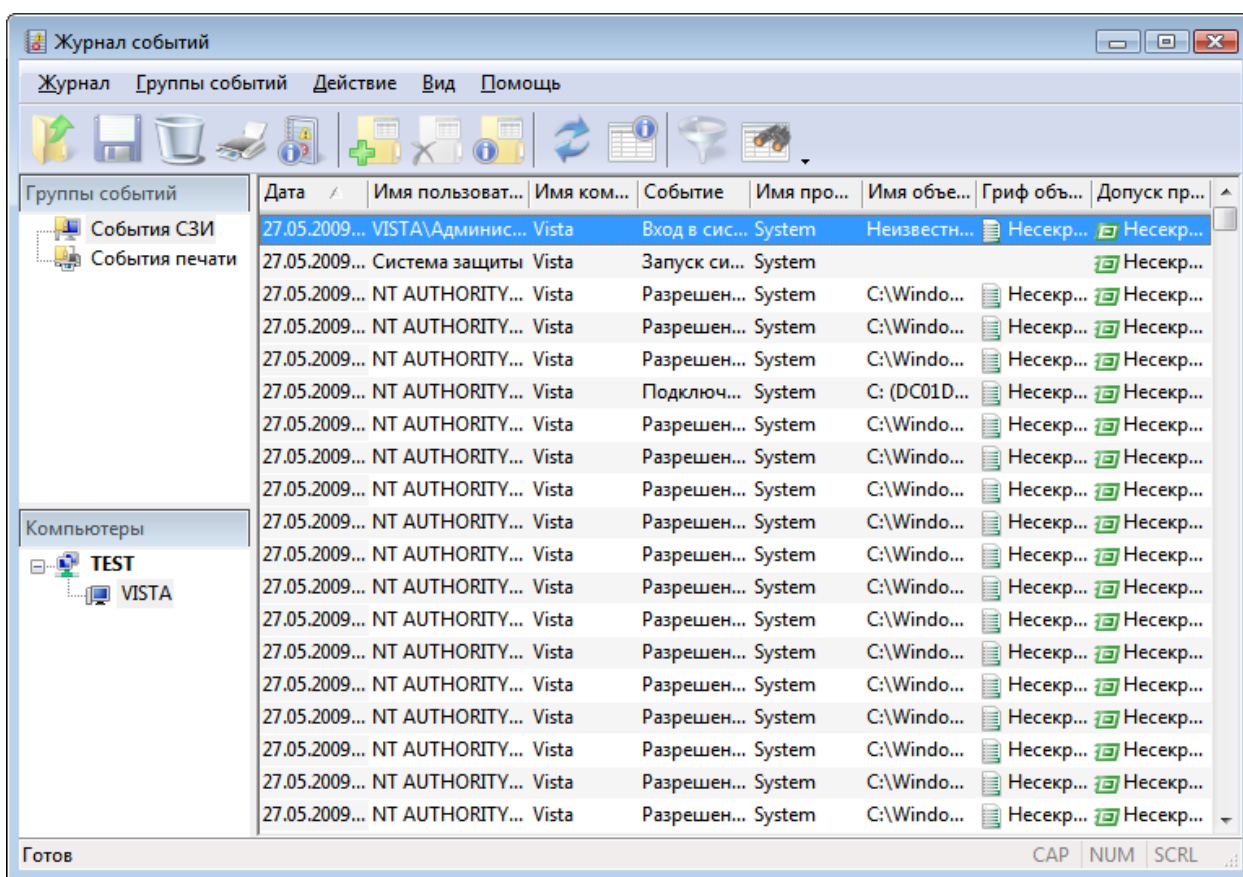


Рис. 87. Общий вид окна программы журнала событий.

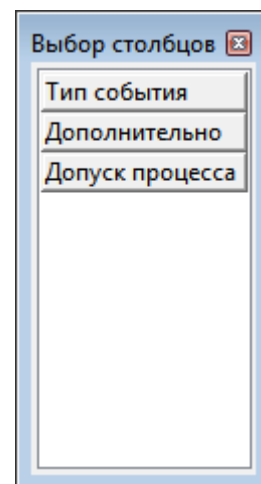
Слева внизу находится список компьютеров, входящих в рабочую группу или домен. Справа представлен список событий выбранного компьютера с их основными свойствами. Список свойств события зависит от группы событий.

<b>Свойство</b>	<b>Описание</b>
Дата	Определяет дату и время события.
Имя пользователя	Определяет имя пользователя, от имени которого произошло событие.
Имя компьютера	Определяет имя компьютера, на котором произошло событие.
Событие	Определяет название события.
Имя процесса	Определяет имя процесса-источника события.
Имя объекта	Определяет имя объекта.
Гриф объекта	Определяет метку конфиденциальности объекта.
Допуск процесса	Определяет текущий допуск процесса-источника события.
Тип события	Определяет тип события (уведомление, предупреждение, ошибка).
Дополнительно	Определяет дополнительную информацию о событии.

Следующие свойства относятся только к событиям печати.

<b>Свойство</b>	<b>Описание</b>
Количество экземпляров	Определяет количество экземпляров распечатанного документа.
Номер документа	Определяет учётный номер документа.
Количество листов	Определяет количество листов в экземпляре распечатанного документа.
Имя принтера	Определяет имя принтера, на котором была произведена печать документа.
Количество листов брака	Определяет количество листов брака (определяется администратором).
Отметка об уничтожении	Определяет специфическую информацию об уничтоженных листах документа (определяется администратором).

Список событий позволяет менять порядок и ширину столбцов, а также позволяет отображать только те столбцы, которые наиболее важны для администратора. Порядок отображения столбцов меняется путём перетаскивания их мышью. Для настройки списка отображаемых столбцов необходимо вызвать контекстное меню заголовка списка событий и выбрать пункт меню **Выбор столбцов**. При этом на экране появится окно, в котором будут отображены названия столбцов, не отображенных в списке. Добавление и удаление столбцов происходит путем перетаскивания их мышью.



Для отображения всех свойств события необходимо выбрать пункт меню **Действие | Свойства** или дважды нажать на событии на левую клавишу мыши. При этом на экране появится диалог, пример которого показан на Рис. 88.

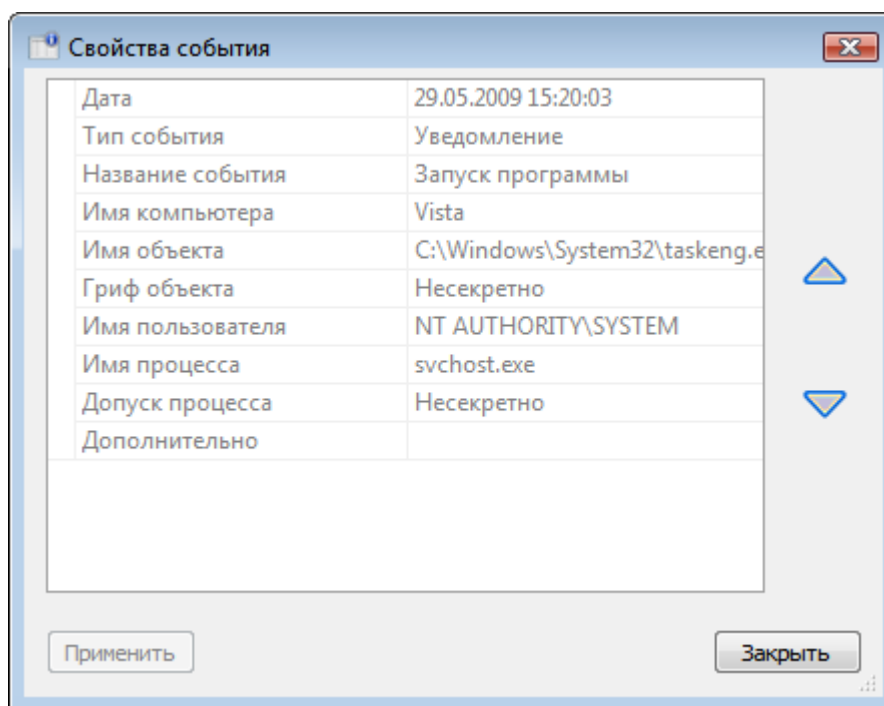


Рис. 88. Свойства события.

Для событий печати поля **Количество листов брака** и **Отметка об уничтожении брака** доступны для редактирования.

Для обновления списка необходимо выбрать пункт меню **Действие | Обновить**.

### Открытие и сохранение журнала событий

При запуске программы по умолчанию будет отображён журнал событий локального компьютера, находящийся в файле `%SystemRoot%\Guard\GReport.mdb`. Для открытия

другого файла журнала (например архивов журналов событий из папки %SystemRoot%\Guard\Reports) необходимо выбрать пункт меню **Журнал | Открыть файл журнала...** и в появившемся диалоговом окне выбрать необходимый файл журнала.

Для сохранения журнала событий в файл необходимо выбрать пункт меню **Журнал | Сохранить журнал как...** и в появившемся диалоговом окне ввести имя файла журнала. Журнал сохраняется в виде файла базы данных **Microsoft Access**.

## Группы событий

С помощью групп событий администратор системы защиты имеет возможность группировать события по некоторому списку признаков. Для добавления группы событий необходимо выбрать пункт меню **Группы событий | Добавить группу** либо выбрать пункт **Добавить группу** контекстного меню на панели **Группы событий**. При этом на экране появится окно, пример которого показан на Рис. 89.

Добавление группы событий	
Группа событий	
Имя группы событий	
Тип группы событий	События СЗИ
Дата	
От:	<input type="checkbox"/>
До:	<input type="checkbox"/>
Компьютер	
Имя компьютера	(Все)
События	
Тип события	Уведомление, Предупреждение, Ошибка
Категория события	(Все)
Название события	(Все)
Объект	
Имя объекта	
Гриф объекта	Несекретно, Секретно, Сов.секретно
Субъект	
Имя пользователя	(Все)
Имя процесса	
Допуск процесса	Несекретно, Секретно, Сов.секретно

Сохранить      Закрыть

Рис. 89. Добавление группы событий.

После задания имени группы и необходимых характеристик необходимо нажать кнопку **Сохранить**. При этом новая группа будет добавлена в список групп событий, а в списке событий будут отображены события, удовлетворяющие заданным в группе условиям.

Для удаления выбранной группы событий необходимо выбрать пункт меню **Группы событий | Удалить группу** либо выбрать пункт **Удалить группу** контекстного меню.

Для изменения свойств выбранной группы событий необходимо выбрать пункт меню **Группы событий | Свойства группы** либо выбрать пункт **Свойства группы** контекстного меню. При этом на экране появится окно свойств группы, как показано на Рис. 90.

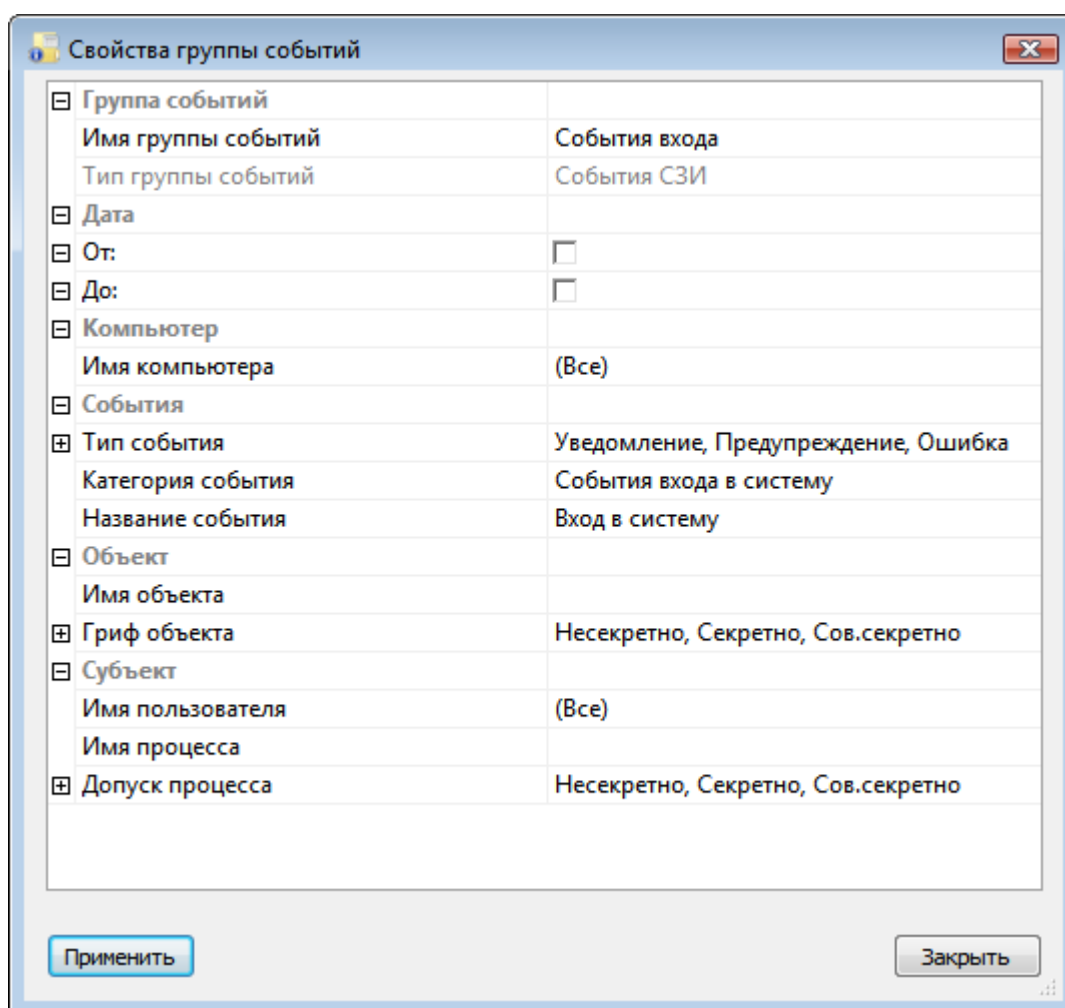


Рис. 90. Свойства группы событий.

После нажатия кнопки **Применить** свойства группы будут изменены, а в списке событий будут отображены события удовлетворяющие новым условиям.

## Фильтрация и поиск

Для включения фильтра отображения событий необходимо выбрать пункт меню **Вид | Фильтр...** . При этом на экране появится окно настройки фильтра (см. Рис. 91). Фильтрация может быть осуществлена по следующим параметрам:

- Дата первого события;
- Дата последнего события;
- Имя компьютера;
- Тип события;
- Категория события;
- Название события;
- Имя объекта;
- Гриф объекта;
- Имя пользователя;
- Имя процесса;
- Допуск процесса.

Для событий печати доступны также следующие параметры:

- Номер документа;
- Количество экземпляров;
- Количество листов в экземпляре;
- Количество листов брака;
- Отметка об уничтожении брака;
- Имя принтера.

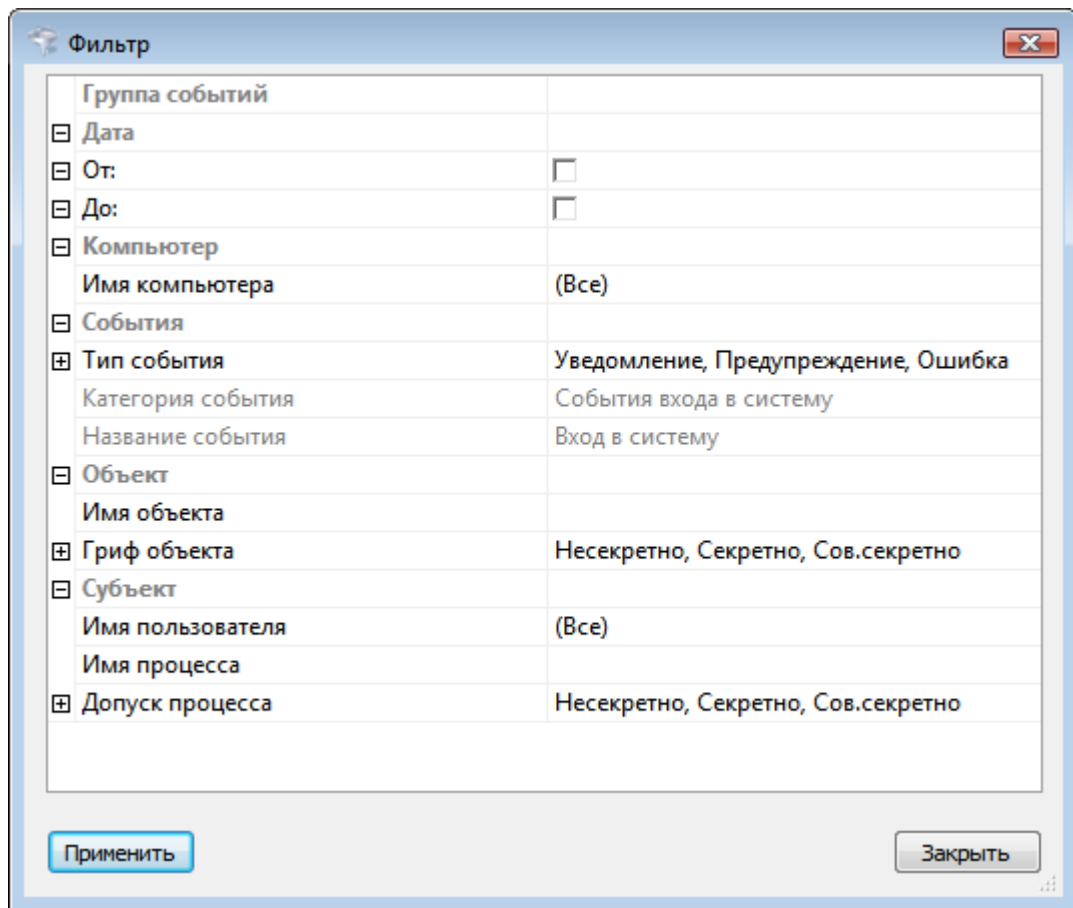


Рис. 91. Настройка фильтра событий.

После нажатия кнопки  список событий будет отображаться с учетом заданных в фильтре условий.

Для отображения всех событий без учета фильтра необходимо выбрать пункт меню **Вид | Все записи**.

Для поиска событий необходимо выбрать пункт меню **Вид | Найти...**. При этом на экране появится окно поиска событий (см. Рис. 92).

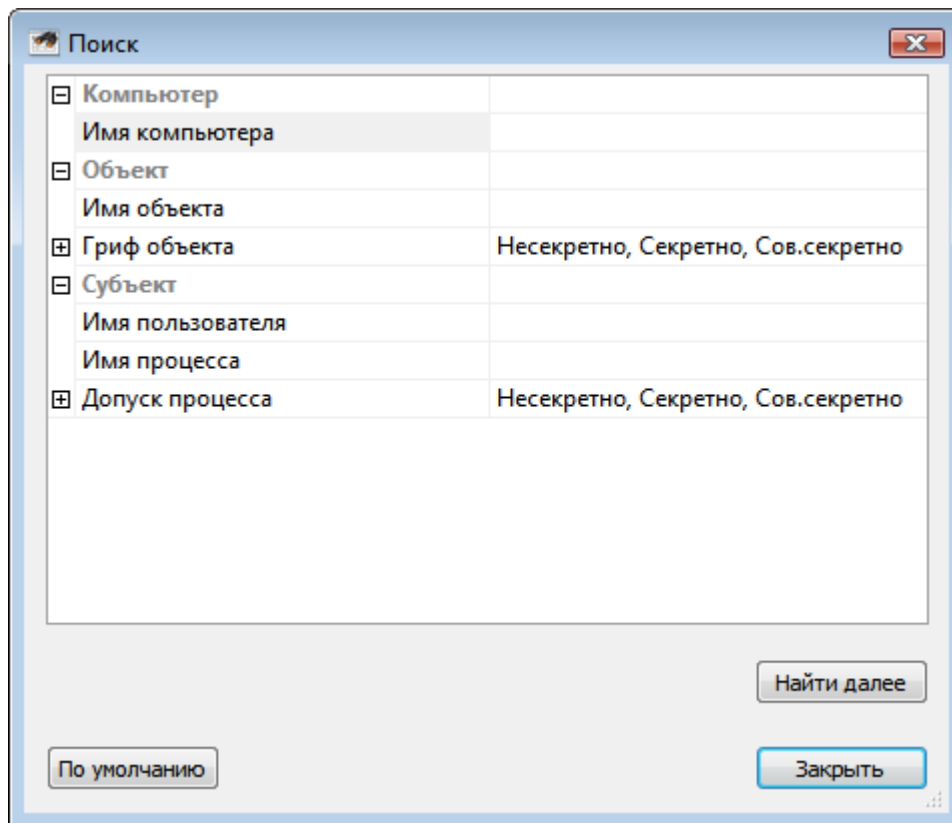


Рис. 92. Поиск событий.

Поиск событий может осуществляться по следующим параметрам:

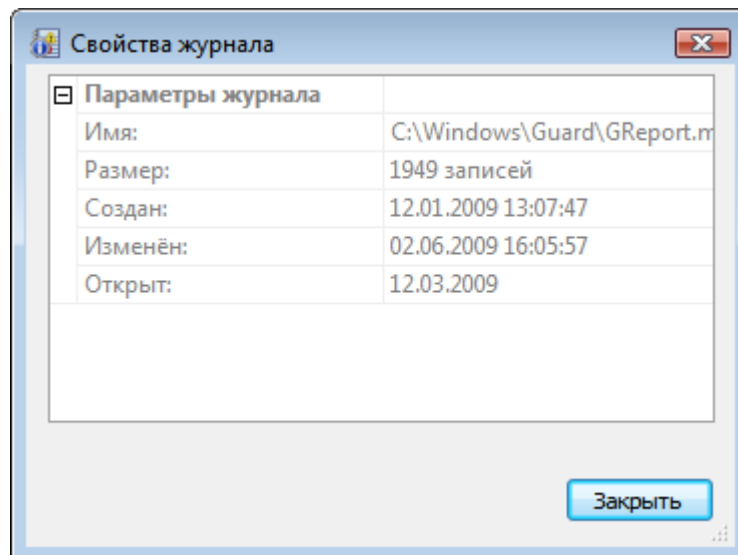
- Имя компьютера;
- Имя объекта;
- Гриф объекта;
- Имя пользователя;
- Имя процесса;
- Допуск процесса.

При нажатии кнопки **Найти далее** программа будет сравнивать события с заданными условиями. Поиск будет осуществляться сверху вниз от выделенного события. Если в списке будет найдено событие, удовлетворяющее заданным условиям, оно будет выделено. Чтобы вернуться к стандартным настройкам поиска, необходимо нажать кнопку **По умолчанию**.

### Дополнительно

Для получения информации о просматриваемом журнале событий необходимо выбрать пункт меню **Журнал | Свойства журнала...** (см. Рис. 93).





*Рис. 93. Свойства журнала событий.*

Для очистки журнала событий необходимо выбрать пункт меню **Журнал | Очистить журнал**. При этом будут удалены все записи, и в журнал будет добавлено событие очистки журнала.

# Редактор шаблонов настроек

В данной главе приводятся сведения о назначении и применении программы **Редактор шаблонов настроек**, ее экранные формы и параметры. Также описан порядок создания шаблонов настроек и работы с ними.

Программа **Редактор шаблонов настроек** предназначена для автоматизированного создания шаблонов настроек СЗИ «Стаж NT». Созданные шаблоны настроек могут применяться с помощью программы **Настройка системы защиты**.

Программа **Редактор шаблонов настроек** запускается при выборе администратором системы защиты в программном меню пункта **Программы | Стаж NT | Редактор шаблонов настроек**. При этом на экране появляется диалоговое окно, пример которого показан на Рис. 94.

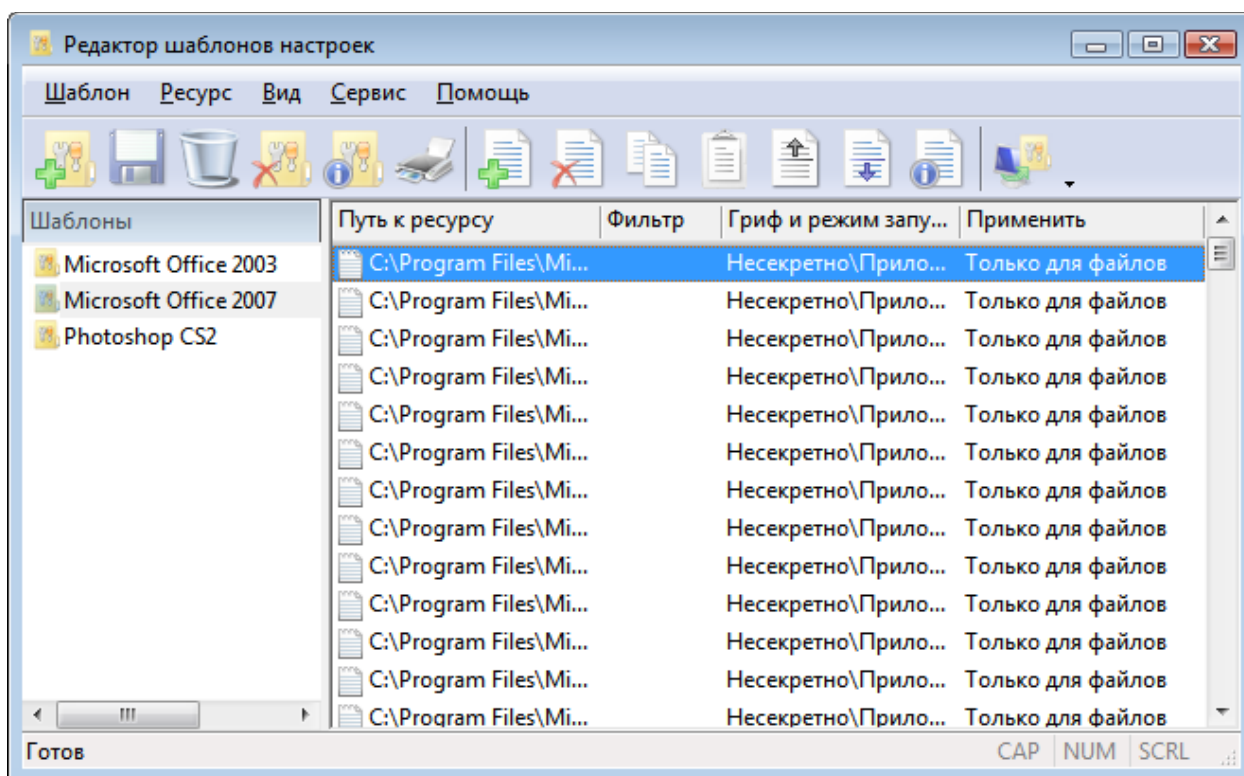


Рис. 94. Общий вид окна программы Редактор шаблонов настроек.

Слева отображён список шаблонов, находящихся в заданной папке. Справа представлен список ресурсов выбранного шаблона. Для изменения папки, из которой будет читаться список шаблонов, необходимо выбрать пункт меню **Сервис | Путь к папке шаблонов...** и в появившемся диалоге выбрать необходимую папку.

## Работа с шаблонами

Для добавления нового шаблона настроек необходимо выбрать пункт меню **Шаблон | Добавить...**. В открывшемся окне (см. Рис. 95) необходимо задать отображаемое имя шаблона и имя файла, в котором он будет сохранён.

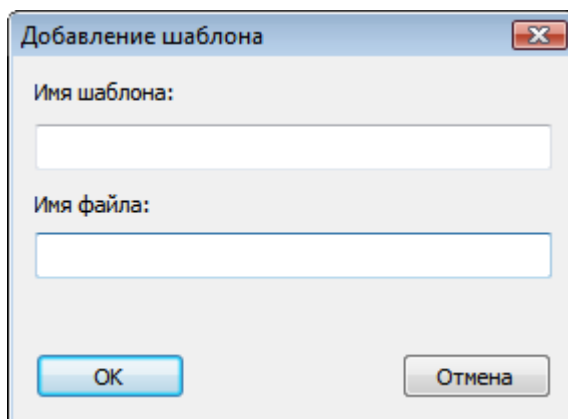


Рис. 95. Добавление шаблона.

Для сохранения внесенных в шаблон изменений необходимо выбрать пункт меню **Шаблон | Сохранить**.

Для удаления всех записей шаблона необходимо выбрать пункт меню **Шаблон | Очистить**.

Для удаления шаблона необходимо выбрать пункт меню **Шаблон | Удалить**.

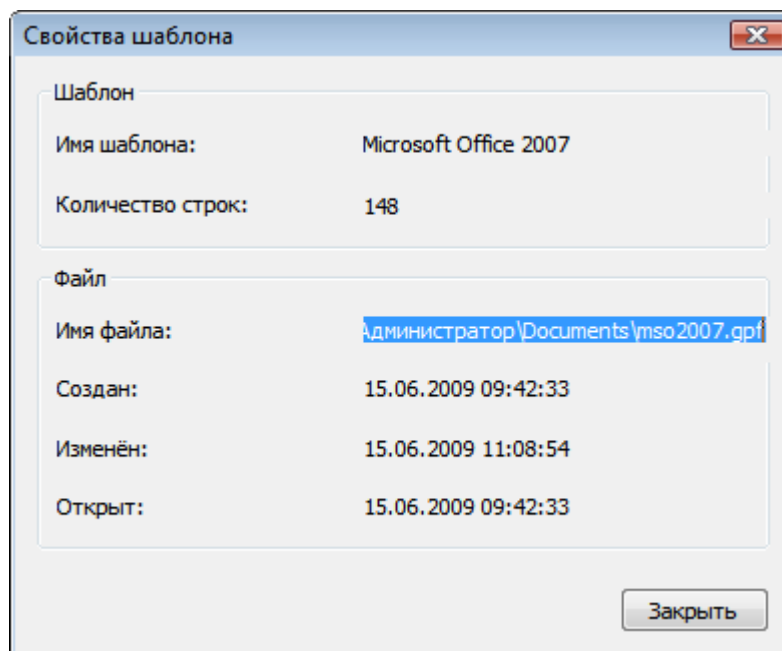


Рис. 96. Свойства шаблона.

Для просмотра основных сведений о шаблоне необходимо выбрать пункт меню **Шаблон | Свойства**. При этом на экране появится окно свойств шаблона (см. Рис. 96).

## Работа с ресурсами

Для добавления нового ресурса в шаблон необходимо выбрать пункт меню **Ресурс | Добавить...** . При этом на экране появится окно добавления ресурса (см. Рис. 97).

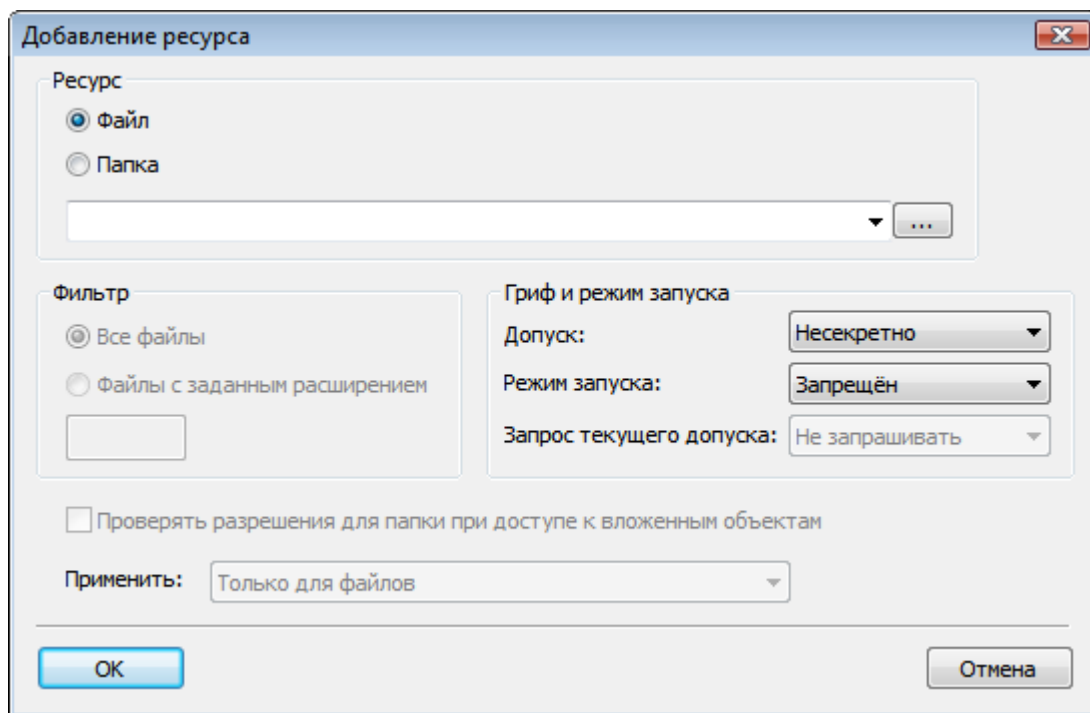


Рис. 97. Добавление ресурса в шаблон.

В данном окне необходимо задать следующие параметры ресурса:

- Тип ресурса (файл, папка);
- Путь к ресурсу;
- Фильтр (если необходимо);
- Гриф или Допуск;
- Режим запуска;
- Режим запроса текущего допущка (если необходимо);
- Флаг проверки разрешений для папки при доступе к вложенным объектам;
- Параметры применения настроек данного ресурса.

Путь к ресурсу может быть как абсолютным, так и заданным с помощью переменных окружения, список которых приведен ниже.

Переменная окружения	Значение
%SystemDrive%	Диск, на котором находится операционная система.
%SystemRoot%	Папка, в которой находится Windows.
%WINDIR%	Папка, в которой находится Windows.
%ProgramFiles%	Папка, в которой находятся программы.
%AllUsersProfile%	Папка профилей всех пользователей.
%UserProfile%	Папка профиля пользователя.
%AppData%	Папка данных программ в профиле пользователя.
%Temp%	Временная папка.
%Tmp%	Временная папка.

В процессе применения профиля, переменная окружения будет преобразована в абсолютный путь к ресурсу.

Если тип добавляемого ресурса – «Папка», и параметры применения настроек включают вложенные файлы, администратор может задать фильтр применения. Если в поле **Фильтр** задано значение, настройки будут применяться ко всем файлам, расширение которых будет совпадать с фильтром, в противном случае – ко всем файлам.

Для удаления ресурса из шаблона необходимо выбрать пункт меню **Ресурс | Удалить**.

В программе предусмотрена возможность копировать записи. Для копирования записи в буфер необходимо выбрать ее в списке и выбрать пункт меню **Ресурс | Копировать**. Для вставки записи из буфера необходимо выбрать пункт меню **Ресурс | Вставить**. При этом вставленная запись помещается в конец шаблона.

Так как в процессе применения профиля настройки применяются последовательно с первой записи, важен порядок их взаимного расположения. Для изменения этого порядка предназначены пункты меню **Ресурс | Переместить вверх** и **Ресурс | Переместить вниз**.

Для просмотра и изменения параметров записи шаблона можно с помощью окна свойств (см. Рис. 98), которое вызывается путем выбора пункт меню **Ресурс | Свойства**.

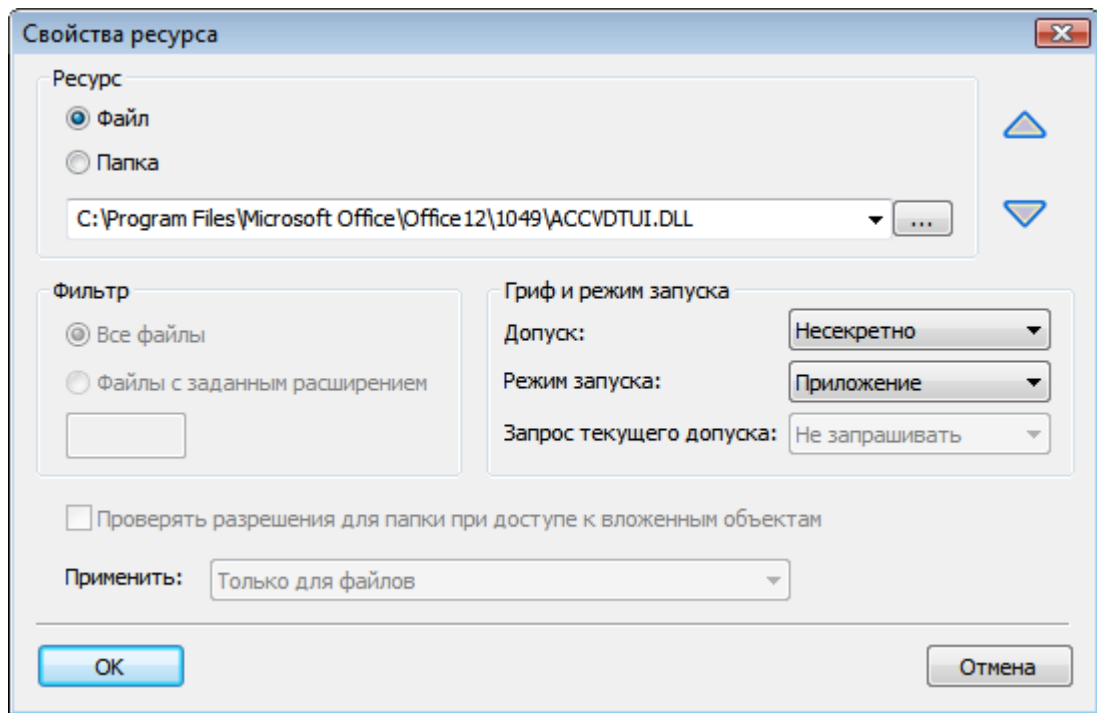


Рис. 98. Свойства ресурса.

### Импорт разрешений

Для импорта настроек необходимо выбрать пункт меню **Сервис | Импорт настроек...** и в появившемся окне выбрать необходимую папку. При этом записи о настройках всех ресурсов, находящихся в выбранной папке, будут добавлены в конец шаблона.

# Тестирование системы защиты

В данной главе приводятся сведения о назначении и применении программы **Тестирование системы защиты**, ее экранные формы и параметры. Также описаны типовые действия администратора при тестировании механизмов системы защиты.

Программа **Тестирование системы защиты** предназначена для проверки функционирования основных механизмов системы защиты таких как:

- дискреционный контроль доступа;
- мандатный контроль доступа;
- контроль ввода-вывода информации на отчуждаемые носители;
- контроль целостности.

Программа **Тестирование системы защиты** запускается при выборе администратором системы защиты в программном меню пункта **Программы | Страж NT | Тестирование системы защиты**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей, при запуске программы на экране появится окно, как показано на Рис. 99.

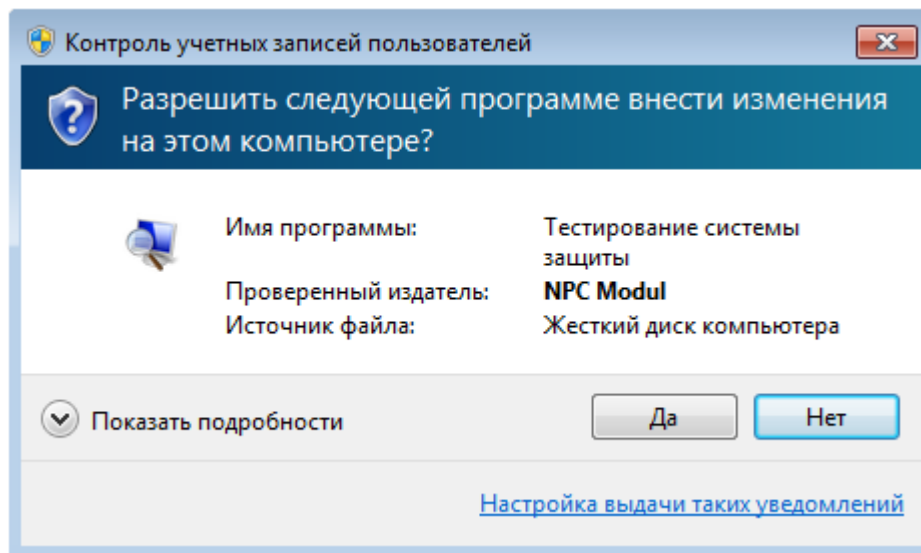


Рис. 99. Сообщение подсистемы контроля учетных записей пользователей.

Для продолжения необходимо нажать кнопку . При этом на экране появляется диалоговое окно, пример которого показан на Рис. 100.

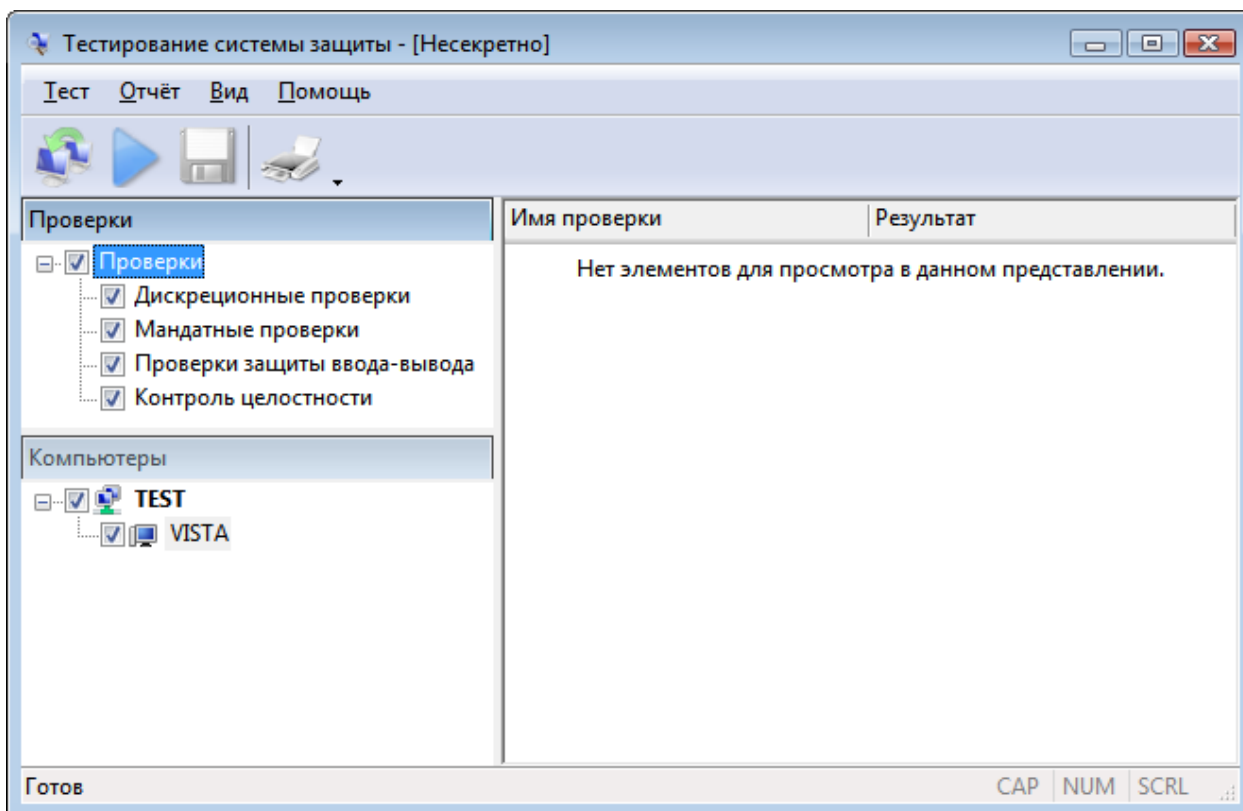


Рис. 100. Общий вид окна программы Тестирование системы защиты.

Слева вверху отображается список доступных для данного компьютера проверок. Слева внизу находится список компьютеров, входящих в рабочую группу или домен. Справа представлен список результатов проверок.



*Для корректной работы программы необходимо, чтобы на запускаемом модуле был установлен максимально возможный гриф. В противном случае при запуске программы на экран будет выдано предупреждение, и проверки функционирования мандатного контроля доступа будут завершены с ошибкой.*

*При выполнении проверок на операционных системах семейства MS Windows 2000, у администратора должна присутствовать привилегия «Работа в режиме операционной системы». В противном случае проверки будут выполнены с ошибкой.*

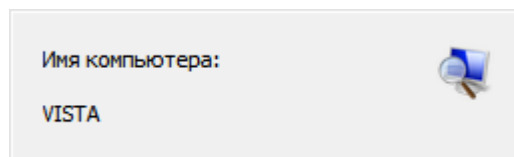
В списке компьютеров необходимо выбрать те из них, на которых будут проводиться проверки. Для каждого выбранного компьютера необходимо определить перечень проверок. Для копирования настроек выбранного компьютера на все остальные необходимо выбрать пункт меню **Тест | Экспорт настроек**.





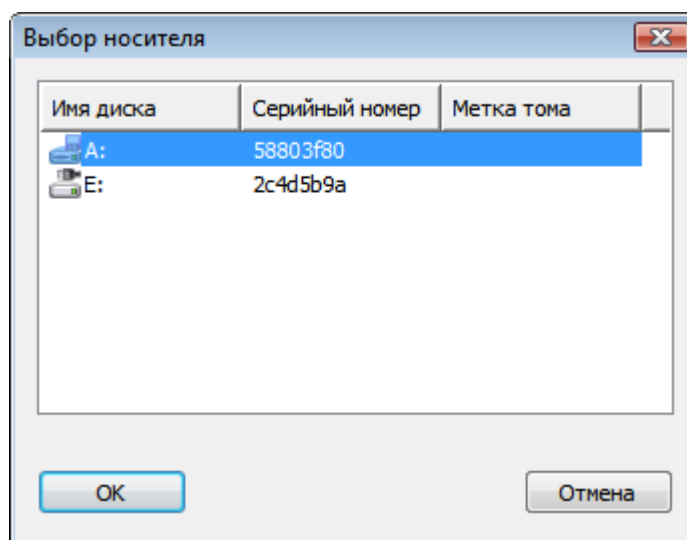
*Проверки механизмов защиты ввода-вывода можно выполнить только на локальном компьютере.*

Для начала тестирования необходимо выбрать пункт меню **Тест | Запуск теста**. В процессе тестирования на экране будет отображаться окно с указанием проверяемого в данный момент компьютера (см. Рис. 101).

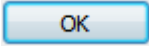


*Рис. 101. Отображение хода процесса тестирования.*

При выполнении проверок защиты ввода-вывода в локальном компьютере должен присутствовать незарегистрированный носитель. Если в системе присутствует более одного незарегистрированного носителя, программа выдаст на экран окно, содержащее список доступных носителей (см. Рис. 102).



*Рис. 102. Выбор носителя для проверок защиты ввода-вывода.*

Администратор должен будет выбрать один из предложенных носителей для выполнения проверок ввода-вывода и нажать кнопку . Если на момент процесса тестирования в системе не будет присутствовать незарегистрированный носитель, в отчёте появится запись: «Устройство не готово».



*Проверки защиты ввода-вывода не могут быть выполнены на носителях типа CD (DVD), а также жёстких дисках.*

После завершения проверок в правой части главного окна программы появится отчёт о проделанных проверках.

Результат	Описание
Выполнено	Все проверки по данному пункту выполнены успешно.
Не выполнено	Проверка была не выполнена.
Не проверялось	Проверки по данному пункту не были заданы.
Ошибка при выполнении теста	При выполнении теста произошла ошибка.
Устройство не готово	Не удалось выполнить проверку по одной из следующих причин: <ul style="list-style-type: none"><li>• на тестируемом компьютере не установлена либо остановлена система защиты;</li><li>• не найдены свободные порты ввода-вывода;</li><li>• нет свободного носителя;</li><li>• удалённый компьютер не доступен.</li></ul>

Для сохранения полученных результатов тестирования необходимо выбрать пункт меню **Отчёт | Сохранение отчёта**.

Для печати полученных результатов тестирования необходимо выбрать пункт меню **Отчёт | Печать отчёта**.

# Дополнительные функции

В данной главе приводится описание дополнительных механизмов и функций системы защиты.

## Режим автозапуска

В системе защиты предусмотрен специальный режим автоматического разрешения режима запуска (режим автозапуска), предназначенный для облегчения настройки системы защиты. При его установке на все запускаемые файлы, включая системные драйверы, динамические библиотеки, а также прикладные программы, автоматически устанавливается режим запуска со значением «Приложение».

Автоматически режим автозапуска всегда включается после установки системы защиты или отказа от настроек системы защиты. Для принудительного включения режима автозапуска необходимо вызвать контекстное меню программы **Монитор системы защиты**, иконка которого находится в системном лотке панели задач, и выбрать пункт меню **Режим автозапуска**. При этом на экране появится окно (см. Рис. 103), в котором необходимо выбрать параметры режима автозапуска.

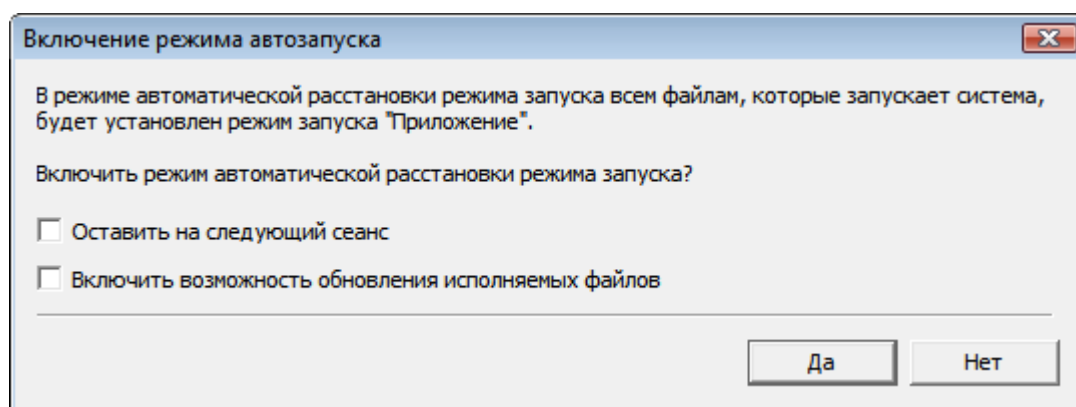


Рис. 103. Параметры режима автозапуска.

При установке флажка **Оставить на следующий сеанс** режим автозапуска включается на текущий и следующий сеанс работы системы защиты до его завершения, либо до момента явного отключения режима автозапуска. Данный режим позволяет выполнять настройку драйверов и сервисных программ операционной системы, программ, запускаемых один раз при создании нового пользовательского профиля и в других сложных ситуациях.

При установке флажка **Включить возможность обновления исполняемых файлов** включается режим обновления программного обеспечения, предназначенный для установки обновлений операционной системы и прикладных программ без необходимости

снятия системы защиты. Данный режим работает аналогично режиму автозапуска на следующий сеанс, за исключением того, что исполняемые файлы становятся доступными на изменение и удаление.

Выключение режима автозапуска происходит путем снятия флажка с пункта меню **Режим автозапуска**.

### Блокировка компьютера

При использовании идентификаторов на гибких магнитных дисках для блокировки компьютера необходимо нажать комбинацию клавиш Ctrl-Alt-Del и в появившемся окне нажать кнопку **Блокировка**. Компьютер будет заблокирован.

При использовании идентификаторов типа iButton для блокировки компьютера необходимо приложить идентификатор к считывающей панели на время не более 5 секунд. Компьютер будет заблокирован.

При использовании в качестве идентификаторов USB-ключей для блокировки компьютера необходимо извлечь идентификатор. Компьютер будет заблокирован, если в данный момент не запущена программа **Менеджер пользователей**. Для запрета блокировки компьютера при изъятии USB-ключа необходимо снять режим блокировки. Для этого необходимо вызвать контекстное меню программы **Монитор системы защиты**, иконка которого находится в системном лотке панели задач, и снять флажок с пункта меню **Режим блокировки** (см. Рис. 104). Включение режима блокировки происходит путем установки флажка на указанный пункт меню.

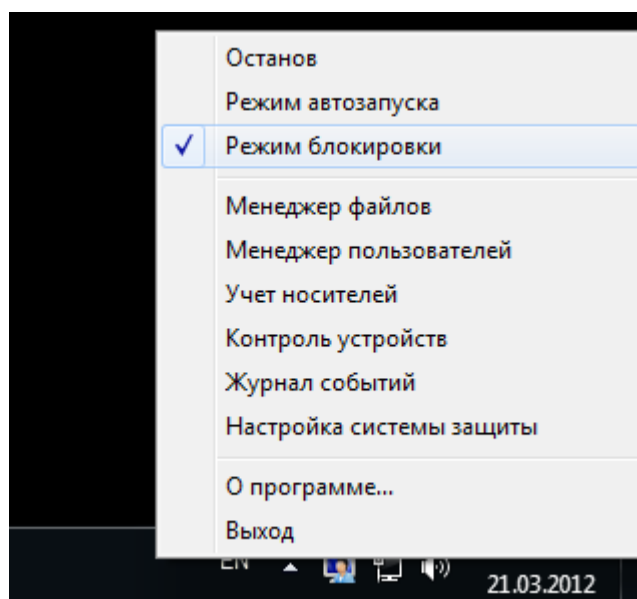


Рис. 104. Режим блокировки.

Для всех типов идентификаторов допускается блокировка компьютера вручную путем нажатия комбинации клавиш Ctrl-Alt-Del и, в появившемся окне, кнопки **Блокировка**. Также компьютер может быть заблокирован по истечении заданного интервала неактивности. Для этого необходимо задать соответствующие параметры, как показано на Рис. 105.

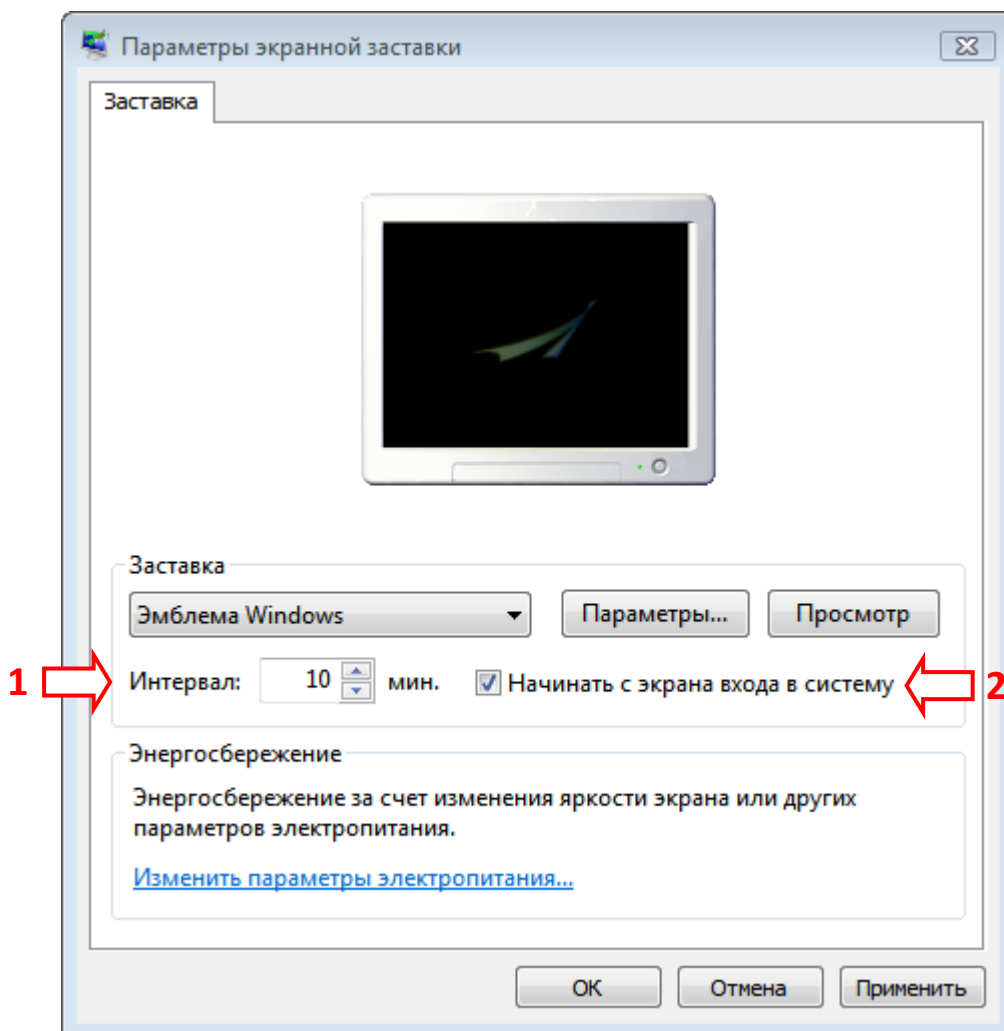


Рис. 105. Задание блокировки компьютера по истечении заданного интервала.

### Разблокировка компьютера

При использовании идентификаторов на гибких магнитных дисках для разблокировки компьютера необходимо установить в дисковод дискету, с помощью которой был осуществлен вход в систему, и нажать комбинацию клавиш Ctrl-Alt-Del. Компьютер будет разблокирован.

При использовании идентификаторов типа iButton для разблокировки компьютера необходимо повторно прислонить идентификатор к считывающей панели на время не более 5 секунд. Компьютер будет разблокирован.

При использовании в качестве идентификаторов USB-ключей для разблокировки компьютера необходимо вставить идентификатор на место и нажать Ctrl-Alt-Del. Компьютер будет разблокирован.

Если блокировка компьютера произошла в результате истечения времени неактивности и запуска заставки, то для его разблокировки необходимо просто нажать Ctrl-Alt-Del. Если идентификатор предъявлен, компьютер будет разблокирован, в противном случае необходимо будет предъявить его и ввести пароль.

### **Повторная идентификация пользователей**

В СЗИ «Страж NT» реализована функция повторной идентификация пользователей без перезагрузки операционной системы. Для выполнения повторной идентификации необходимо завершить текущий сеанс пользователя. В случае использования в качестве персонального идентификатора USB-ключа, изъять его, предъявить персональный идентификатор и ввести пароль другого пользователя. При повторной идентификации возможен вход как администратора системы защиты, так и обычного пользователя.

Если при повторной идентификации будет предъявлен идентификатор завершившего сеанс пользователя, то вход в систему произойдет автоматически тем же пользователем без запроса пароля.



*Повторная идентификация возможна только при использовании пользователями персональных идентификаторов одного типа.*

*Повторная идентификация пользователей на компьютерах под управлением ОС старше MS Windows XP возможна только при использовании USB-идентификаторов.*

*Повторная идентификация пользователей на компьютерах под управлением ОС младше MS Windows Vista возможна только в том случае, если при первоначальной идентификации зарегистрировался пользователь, не являющийся администратором системы защиты.*

*Если во время сеанса работы администратора системы защиты, вошедшего путем повторной идентификации, был произведен останов СЗИ, для дальнейшей работы рекомендуется перезагрузить компьютер.*

# Термины и определения

---

В данном разделе описаны термины и определения, встречающиеся в документации на систему защиты.

## А

Администратор системы защиты	Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.
Аудит	Автоматическая запись в журнал сведений о событиях, связанных с работой системы защиты информации.
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

## Б

Безопасность информации	Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.
-------------------------	--

## В

Владелец объекта	Субъект доступа, который создал объект. Владелец объекта имеет безусловный доступ к дискреционному списку контроля доступа и всегда обладает правом изменять его.
------------------	---

## Г

Гриф объекта	Уровень конфиденциальности объекта. Определяется установленной меткой конфиденциальности.
--------------	---

## Д

Допуск пользователя	Максимальный уровень конфиденциальности объектов, которыми может манипулировать пользователь. Определяется установленной меткой конфиденциальности.
Допуск программы	Максимальный уровень конфиденциальности объектов, которыми может манипулировать программа. Определяется установленной меткой конфиденциальности.
Дискреционный список контроля доступа (DACL)	Массив записей контроля доступа, управляющий доступом пользователей к объекту.

## З

Замкнутая программная среда	Условно неизменная совокупность программных модулей, которые доступны на выполнение пользователем системы.
Запись контроля доступа (ACE)	Элемент списка контроля доступа, который относится к определенной учетной записи и включает маску доступа.

## И

Идентификатор безопасности (SID)	Глобально уникальный идентификатор субъекта системы безопасности.
Идентификация	Выяснение личности пользователя с целью предоставления ему определенного набора прав и привилегий при работе с системой.

## К

Контрольная сумма	Некоторое значение, рассчитанное из последовательности данных путём применения определённого алгоритма, используемое для проверки целостности данных.
-------------------	---

## М

Маска доступа	Число, отдельные биты которого соответствуют разным типам доступа.
---------------	--

## Н

Несанкционированный доступ к информации (НСД)	Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
---	--

## П

Пароль	Идентификатор субъекта доступа, который является его (субъекта) секретом.
Персональный идентификатор пользователя	Средство аппаратной поддержки системы защиты, предназначенное для идентификации пользователя.
Пользователь системы защиты	Лицо, допущенное к обработке информации с использованием средств вычислительной техники.
Правила разграничения доступа	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.



## Р

Режим автоматической расстановки режима запуска (автозапуска)      Режим работы системы, при котором на все запускаемые файлы автоматически устанавливается режим запуска «приложение».

Режим блокировки      Режим работы системы, при котором изъятие USB-идентификатора или прикладывание iButton к считывателю приводит к блокировке системы.

## С

Система защиты информации (СЗИ)      Комплекс организационных мер и программно-технических средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Список контроля доступа (ACL)      Массив записей контроля доступа.

Системный список контроля доступа (SACL)      Массив записей контроля доступа, управляющий аудитом доступа к объекту.

## Т

Текущий допуск программы      Установленный в данный момент допуск экземпляра программы, запущенного на выполнение.

Тип доступа      Множество однотипных операций над объектом. Для объектов разных классов набор типов может быть различен.

## У

Учетная запись      Информация, идентифицирующая субъект системы безопасности. Указателем на учетную запись является ее идентификатор безопасности.

## Ц

Целостность      Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

## Ш

Шаблон настроек      Набор параметров и их значений, позволяющий устанавливать защитные свойства объектов. Шаблоны настроек нужны для упрощения процедуры настройки свойств объектов автоматизированной системы.