СЗИ «Страж NT»

Руководство пользователя

ЗАО НПЦ «Модуль»

Телефон/факс: +7 (495) 955-9029

E-mail: info@guardnt.ru

Web: http://www.guardnt.ru

Оглавление

Введение

Документ предназначен для пользователей системы защиты информации от несанкционированного доступа «Страж NT» (версия 3.0) (далее в документе СЗИ «Страж NT»). В документе приведены сведения, необходимые пользователю для работы с системой защиты, а также приводится порядок работы с компонентами СЗИ.

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, условиях ее применения, а также базовые понятия, связанные с системой защиты.
- В главе Начало и завершение работы рассматриваются подробные действия пользователя при входе в систему, выходе из нее, при блокировке и разблокировке компьютера, а также действия при возможных нештатных ситуациях.
- Глава Работа с ресурсами посвящается описанию правил работы с защищаемыми ресурсами и типовых действий пользователя.
- 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 краху системы.

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 ее применения, а также базовые понятия, связанные с системой защиты.

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».

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.

Защищаемые ресурсы

Защищаемыми ресурсами в СЗИ «Страж NT» являются логические диски (в том числе и отчуждаемые), папки, файлы и принтеры. Дополнительно, система защиты обеспечивает разграничение по входу пользователей в компьютер и по доступу к его устройствам.

Доступ к защищаемому ресурсу определяется, исходя из его списка контроля доступа, а также метки конфиденциальности (грифа). Список контроля доступа определяет избирательные права доступа субъектов к защищаемому ресурсу. Метка конфиденциальности защищаемого ресурса определяет полномочные права субъекта доступа.

Механизмы разграничения доступа

Пользователю, работающему на компьютере под управлением СЗИ «Страж NT», необходимо иметь представление о следующих механизмах разграничения доступа.

Избирательное разграничение доступа	Механизм избирательного (дискреционного) разграничения доступа основан на сопоставлении полномочий пользователей и списков контроля доступа защищаемых ресурсов. Пользователь в рамках своих полномочий может просматривать и изменять списки контроля доступа с помощью стандартной программы **Проводник**, а также программы **Менеджер файлов**.
Полномочное разграничение доступа	Механизм полномочного (мандатного) разграничения доступа основан на сопоставлении меток конфиденциальности пользователя (допуска), прикладной программы (текущего допуска) и защищаемого ресурса (грифа). Пользователь может просматривать информацию о метке конфиденциальности защищаемого ресурса с помощью стандартной программы **Проводник**, а также программы **Менеджер файлов**.
Замкнутая программная среда	Механизм замкнутой программной среды предназначен для обеспечения целостности и замкнутости программной среды и реализован 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. Режим запуска относится не только к программам, но и динамическим загружаемым библиотекам. Пользователь может просматривать информацию о режиме запуска защищаемого ресурса с помощью стандартной программы **Проводник**, а также программы **Менеджер файлов**.
Контроль носителей информации	Контроль носителей информации позволяет управлять доступом к носителям информации в соответствии с установленными списками контроля доступа и метками конфиденциальности. Таким образом, доступ пользователя к носителям информации определяется политикой, задаваемой Администратором системы защиты.

Контроль устройств	Механизмы контроля устройств позволяют формировать необходимую конфигурацию устройств для пользователя в соответствии с установленными списками контроля доступа. Таким образом, доступ пользователя к устройствам компьютера определяется политикой, задаваемой Администратором системы защиты.
Преобразование носителей информации	Механизм преобразования информации на отчуждаемых носителях позволяет включить дополнительную защиту для съемных носителей с помощью режима прозрачного преобразования всей информации на носителе. В зависимости от режима работы данного механизма обмен информацией с преобразованного носителя может быть осуществлен либо только на данном компьютере, либо на компьютерах, входящих в логическую сеть, определяемую Администратором системы защиты.
Маркировка печатных документов	Механизмы маркировки документов обеспечивает автоматическое проставление учетных признаков в документах, выдаваемых пользователем на печать. Порядок и параметры маркировки документов определяются политикой, задаваемой Администратором системы защиты.
Контроль целостности	Механизм контроля целостности предназначен для периодической проверки параметров целостности файлов. Список файлов, для которых производится проверка целостности, а также ее параметры определяются Администратором системы защиты. Пользователь может просматривать информацию о параметрах проверки целостности файлов с помощью стандартной программы **Проводник**, а также программы **Менеджер файлов**. Также с помощью указанных программ Пользователь может самостоятельно проверить целостность файлов.

Начало и завершение работы

В данной главе рассматриваются подробные действия пользователя при входе в систему, выходе из нее, при блокировке и разблокировке компьютера, а также действия при возможных нештатных ситуациях.

Вход в систему

Для входа в систему и загрузки операционной системы Вы, прежде всего, должны быть зарегистрированы как пользователь в системе защиты информации. Регистрация пользователей осуществляется Администратором системы защиты.

При регистрации нового пользователя Администратор системы защиты присваивает ему имя, наделяет его соответствующими правами по доступу к защищаемым ресурсам, формирует персональный идентификатор пользователя для опознания при входе в систему, а также назначает (формирует) пароль, служащий для подтверждения подлинности пользователя, чей идентификатор предъявляется при входе в систему.

В качестве персональных идентификаторов могут использоваться: дискеты 3,5", устройства типа iButton, USB-ключи Guardant ID, ruToken и eToken Pro, а также USB флэш-накопители.

После регистрации Вас, как пользователя системы, Администратор системы защиты должен выдать Вам персональный идентификатор и сообщить пароль, который следует запомнить.

Не записывайте пароль где-либо, не сообщайте его кому бы то ни было, а также не передавайте и не оставляйте без присмотра Ваш персональный идентификатор.

При включении питания или перезагрузке компьютера на экран выдается сообщение, как показано на Рис. 1 с мигающей надписью «Предъявите идентификатор...». Для осуществления входа в систему Вам необходимо предъявить персональный идентификатор, выданный Администратором системы защиты.

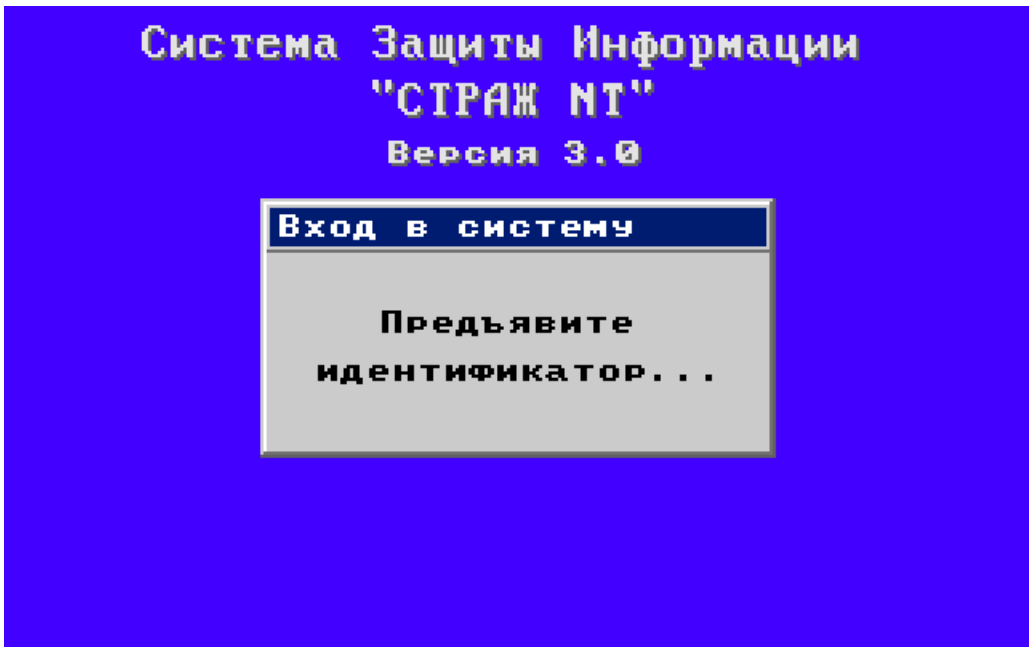


Рис. 1. Стартовый диалог входа в систему

Если после предъявления идентификатора на экране остается сообщение, представленное на Рис. 1, то Вам следует убедиться в том, что Вы предъявили персональный идентификатор, выданный Вам администратором системы защиты. В том случае, если данный идентификатор действительно является Вашим персональным идентификатором для входа в систему, Вам следует обратиться к Администратору системы защиты.

После считывания предъявленного Вами правильного идентификатора на экран выводится запрос на ввод пароля (см. Рис. 2).

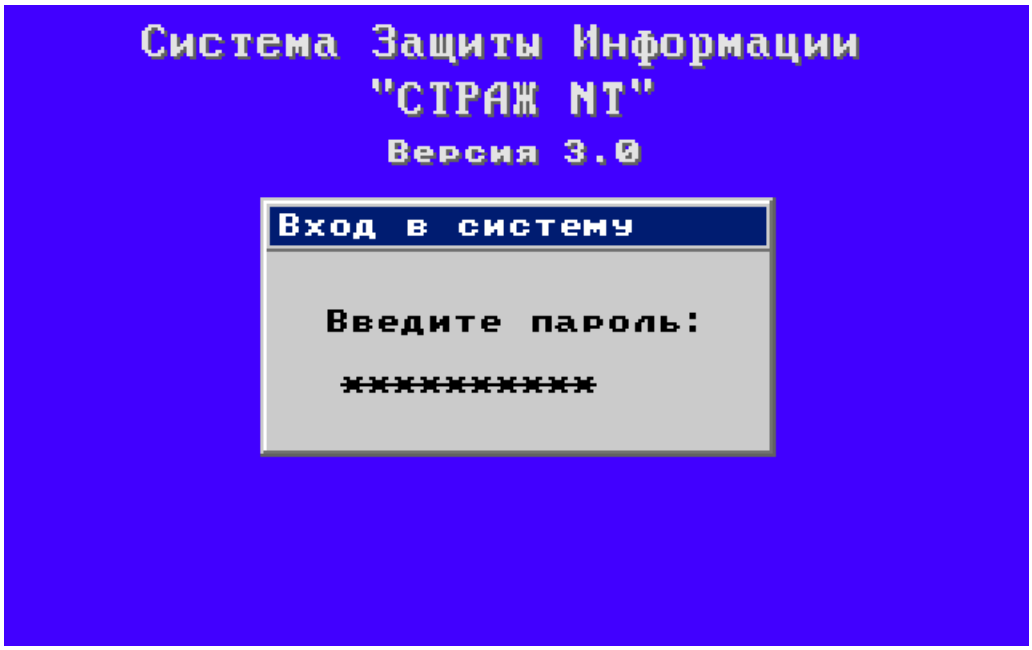


Рис. 2. Запрос на ввод пароля

Если Вам назначен пустой пароль, загрузка системы продолжится автоматически.

Вам предоставляется 3 попытки для ввода пароля. После набора с помощью клавиатуры значения пароля Вам следует нажать клавишу <Enter>. После третьей попытки ввода неправильного пароля компьютер блокируется и на экран выдается сообщение (см. Рис. 3), сопровождаемое звуковой сигнализацией.

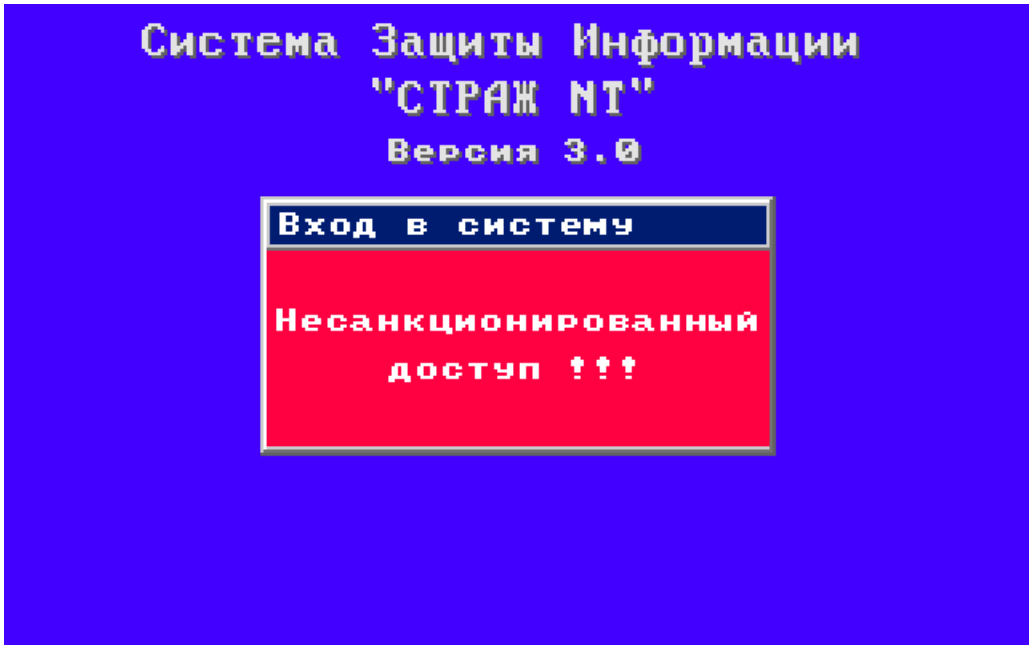


Рис. 3. Сообщение о попытке несанкционированного входа в систему

В этом случае для осуществления входа в систему Вам следует произвести перезагрузку компьютера посредством нажатия кнопки RESET или выключить и заново включить компьютер. После этого на экране снова появится сообщение, приведенное на Рис. 1.

При вводе Вами корректного пароля происходит загрузка операционной системы и автоматический вход в систему с загрузкой Ваших персональных настроек. Под корректным или правильным паролем понимается пароль, соответствующий предъявленному персональному идентификатору.

После ввода Вами корректного пароля происходит временная блокировка клавиатуры до момента входа в систему.

Результатом удачной загрузки системы является появление на экране монитора так называемого рабочего стола пользователя. В системном лотке, находящемся в правой нижней части панели задач, может появиться (задается Администратором системы защиты) значок программы **Монитор системы защиты**.

Программа **Монитор системы защиты** предназначена для отображения состояния системы защиты и для выполнения некоторых сервисных функций, описанных ниже. Также меню программы может использоваться для быстрого запуска пользовательских программ, перечень которых задается Администратором системы защиты.

Ситуации, возникающие при входе в систему

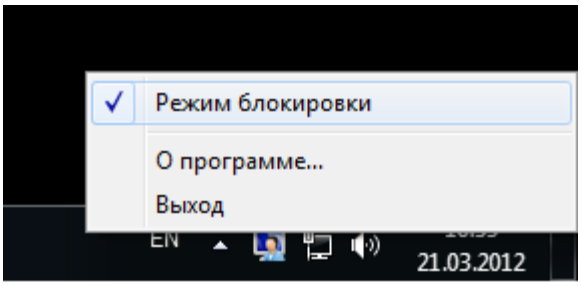
Ниже описаны ситуации, которые могут возникнуть при входе в систему. Рассматриваются причины и действия для преодоления возникших ситуаций. В случае возникновения ситуаций, не описанных ниже, следует обратиться к Администратору системы защиты.

При включении компьютера сразу появляется надпись «Введите пароль:»	
Причина	В дисковод ГМД вставлена дискета, являющаяся персональным идентификатором, которая уже была считана.
Действия	Вам следует продолжить вход в систему, т. е. ввести пароль.
При включении компьютера сразу появляется надпись «Установите загрузку системы с диска С:»	
Причина	Компьютер пытается загрузить систему с дискеты, вставленной в один из дисководов ГМД.
Действия	Необходимо предъявлять идентификатор после запроса, показанного на Рис. 1. Рекомендуется обратиться к Администратору системы защиты для того, чтобы он изменил порядок загрузки операционной системы на Вашем компьютере.
Надпись «Предъявите идентификатор...» не мигает или отсутствует на экране	
Причина	Одно из устройств, подключенное к USB-порту, не отвечает на запрос.
Действия	Необходимо либо выключить устройство, либо предъявлять идентификатор до появления запроса, показанного на Рис. 1
После начала загрузки ОС происходит зависание компьютера, автоматическая перезагрузка или появление «синего экрана смерти»	
Причина	При загрузке ОС происходит сбой, приводящий к невозможности дальнейшей работы. Чаще всего сбои обусловлены запретом на запуск пользователем системных приложений или нарушением целостности программной среды.
Действия	Необходимо обратиться к Администратору системы защиты.

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 прислонить 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. Для запрета блокировки компьютера при изъятии USB-ключа необходимо снять режим блокировки (возможность задается Администратором системы защиты). 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**. Включение режима блокировки происходит путем установки флажка на указанный пункт меню.

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. 4.

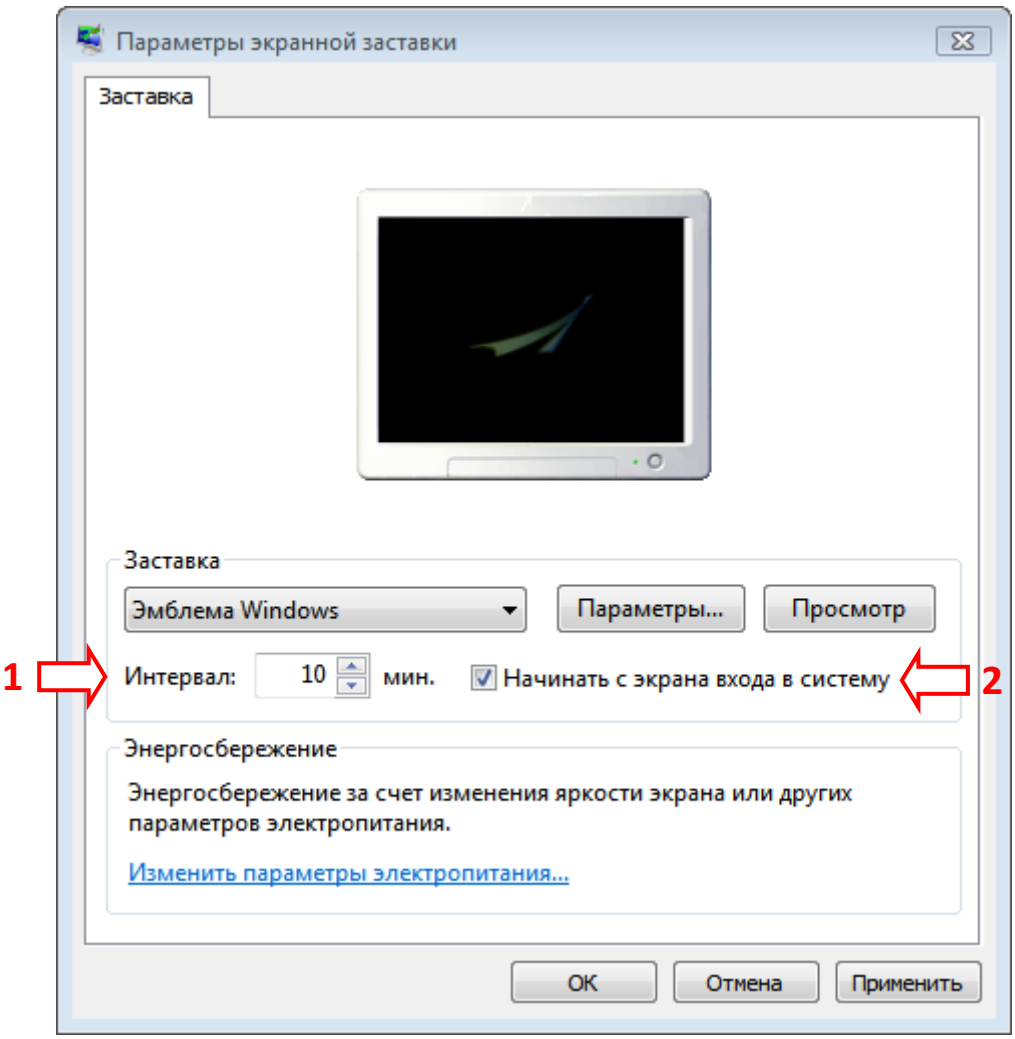


Рис. 4. Задание блокировки компьютера по истечении заданного интервала

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

Для выполнения повторной идентификации необходимо завершить текущий сеанс пользователя. Для этого необходимо на панели задач нажать кнопку **Пуск** и в появившемся на экране разворачивающемся меню выбрать соответствующий пункт (см. Рис. 5).

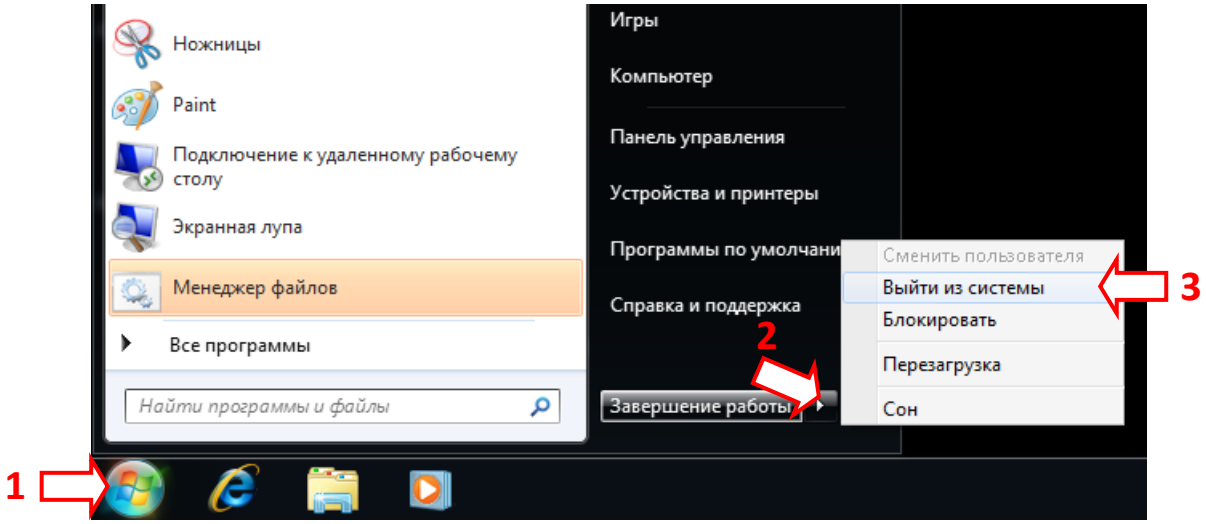


Рис. 5. Завершение сеанса пользователя для переидентификации.

В случае использования в качестве персонального идентификатора USB-ключа, изъять его, предъявить персональный идентификатор и ввести пароль другого 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.

Выход из системы

По окончании работы Вам следует перезагрузить или выключить компьютер. Для этого необходимо на панели задач нажать кнопку **Пуск** и в появившемся на экране разворачивающемся меню выбрать соответствующие пункты (см. Рис. 6).

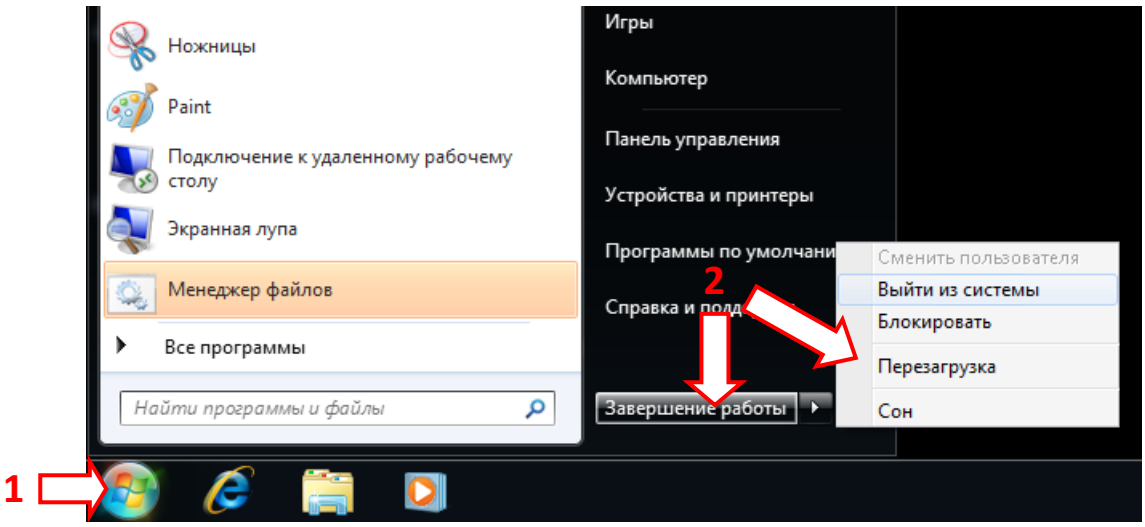


Рис. 6. Завершение работы пользователя.

При завершении работы компьютера с установленной СЗИ, по умолчанию, осуществляется затирание файла подкачки. В связи с этим возможны некоторые задержки при выключении компьютера, а также гашение экрана монитора. В любом случае необходимо дождаться завершения этого процесса и отключения питания компьютера.

Работа с ресурсами

Данная глава посвящена описанию правил работы с защищаемыми ресурсами и типовых действий пользователя.

Правила работы с защищаемыми ресурсами

При работе с защищаемыми ресурсами в операционной системе, работающей под управлением СЗИ «Страж NT» существуют следующие правила:

1. Для получения права работы с ресурсами, имеющими метку конфиденциальности, приложению должен быть назначен соответствующий допуск.
2. Работа приложения, имеющего допуск, осуществляется в рамках полномочий пользователя, от имени которого произошел его запуск.
3. Пользователь может получить доступ к ресурсу по чтению в том случае, если текущий допуск приложения, осуществляющего доступ, не ниже метки конфиденциальности данного ресурса. В противном случае ресурс для приложения будет недоступен на чтение и невидим.
4. Пользователь может получить доступ к ресурсу по чтению и записи в том случае, если текущий допуск приложения, осуществляющего доступ, равен метке конфиденциальности данного ресурса.
5. Пользователь может получить доступ к ресурсу, исходя из типа запрашиваемого доступа и списка контроля доступа данного ресурса.
6. При создании нового ресурса ему присваивается метка конфиденциальности, равная текущему допуску приложения.
7. Допускается одновременная работа приложений с разными текущими допусками.

Изменение текущего допуска приложения

При запуске приложения, имеющего допуск, возможны следующие варианты.

- Текущий допуск не запрашивается и устанавливается минимально возможным. Изменение текущего допуска возможно в процессе работы приложения.
- Появляется окно с выбором текущего допуска. Изменение текущего допуска возможно в процессе работы приложения.
- Текущий допуск не запрашивается и устанавливается в определенное значение. Изменение текущего допуска в процессе работы приложения невозможно.

Для изменения текущего допуска приложения необходимо в его системном меню (см. Рис. 8) выбрать пункт меню **Текущий допуск**.

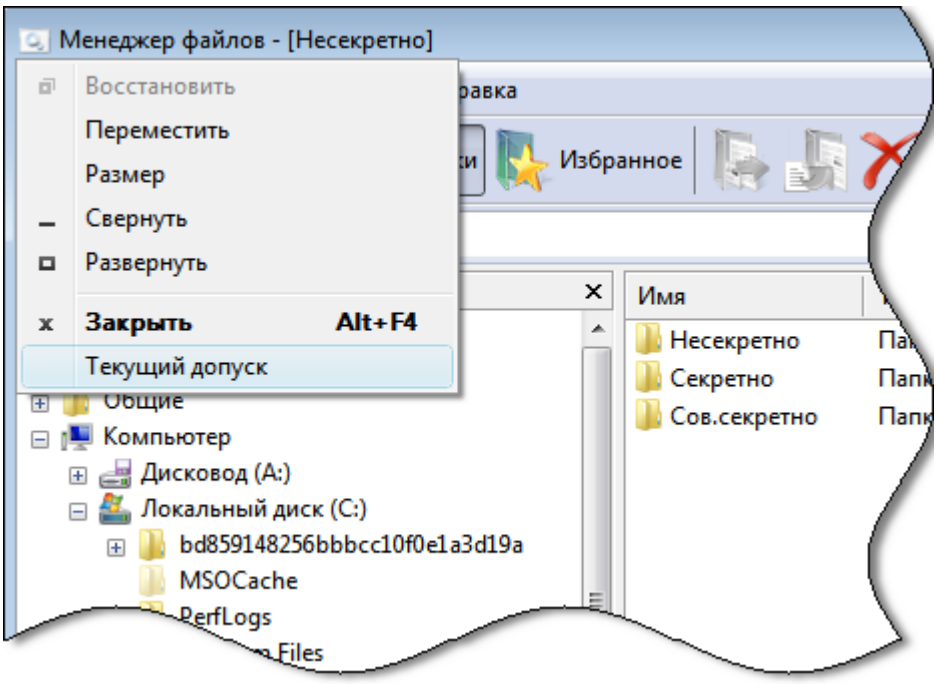


Рис. 8. Запрос изменения текущего допуска приложения.

Из представленного списка (см. Рис. 9) необходимо выбрать, с ресурсами какого уровня Вы собираетесь работать, и нажать кнопку OK.

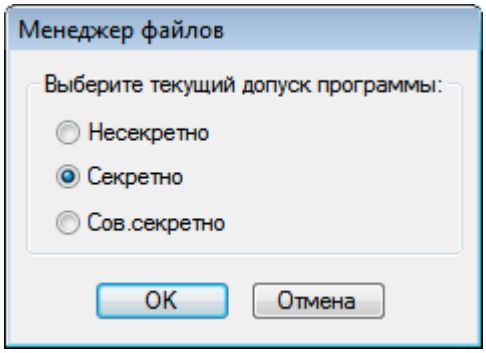


Рис. 9. Диалог выбора текущего допуска приложения.

При попытке изменения текущего допуска приложения на экран может выдаваться сообщение об ошибке, пример которого приведен на Рис. 10.

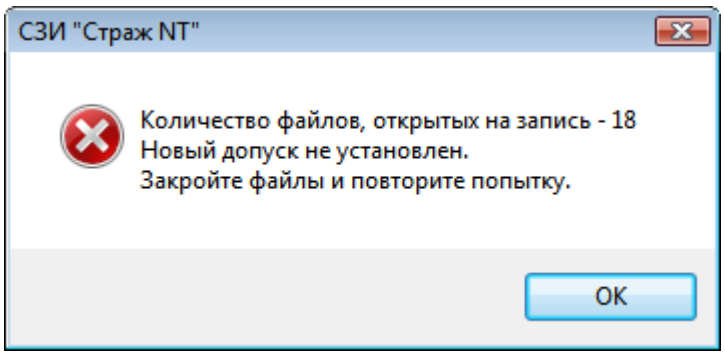


Рис. 10. Пример сообщения о файлах, открытых на запись.

При появлении на экране подобного сообщения Вам следует нажать кнопку OK и закрыть все файлы, открытые данным приложением, а затем повторить попытку изменения значения текущего допуска. Если на экране вновь появляется сообщение об ошибке, Вам следует нажать кнопку OK и перезапустить данное приложение, а затем вновь повторить попытку изменения значения текущего допуска. Если и в этом случае на экране появляется сообщение об ошибке, Вам следует обратиться к Администратору системы защиты.

Следует помнить, что максимальный текущий допуск приложения не может быть выше Вашего допуска. Текущий допуск приложения можно повысить, но невозможно понизить, поэтому при необходимости работы с защищаемыми ресурсами, метки конфиденциальности которых ниже текущего допуска приложения, Вам необходимо закрыть приложение и запустить его вновь.

Проверка целостности файла

Для проверки целостности файла необходимо правой клавишей мыши вызвать его контекстное меню и выбрать в нем пункт **Проверить целостность** (см. Рис. 11).

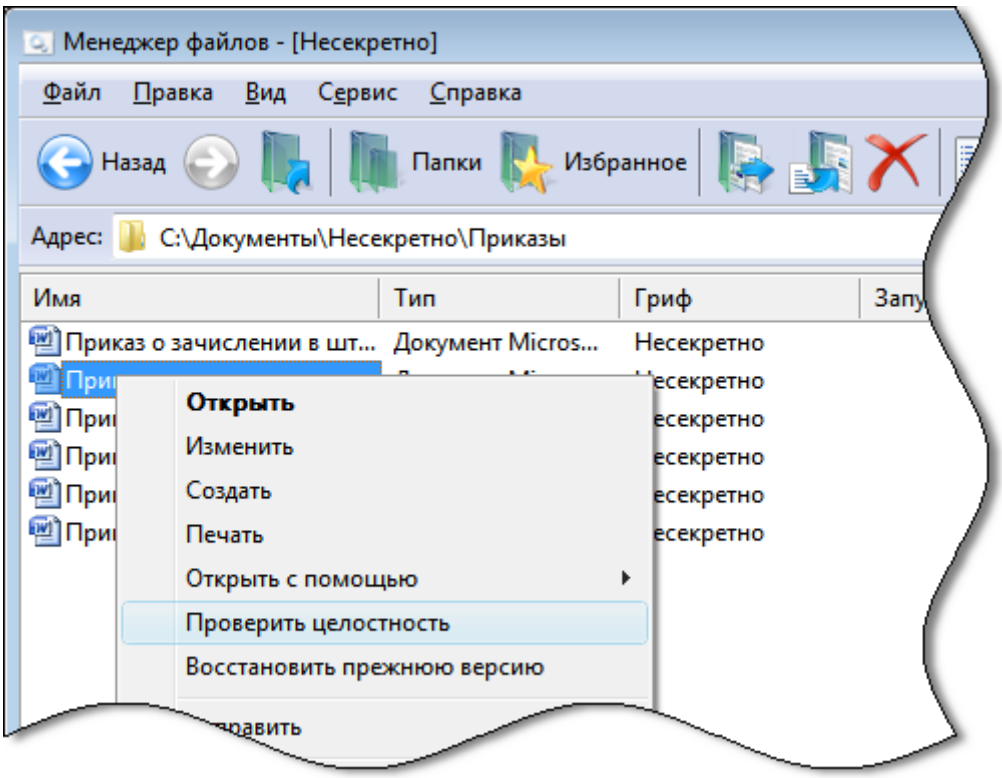


Рис. 11. Проверка целостности файла.

При этом на экране появится сообщение с результатом проверки (см. Рис. 12).

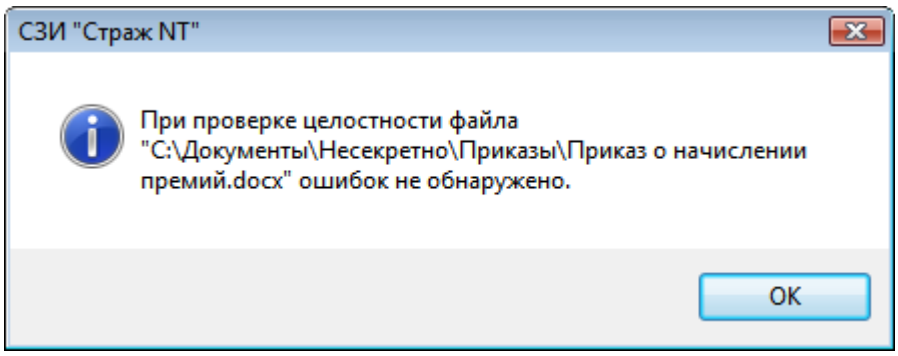


Рис. 12. Результат проверки целостности файла.

Печать документов

При работе на компьютере, оснащенном СЗИ «Страж NT», все документы, выдаваемые на печать, могут маркироваться в соответствии с настройками системы защиты. Маркировка документов происходит автоматически.

При печати документа из какого-либо приложения на экране появится окно, пример которого показан на Рис. 13. В зависимости от настроек поля, отвечающие за реквизиты должностных лиц, могут быть заполнены автоматически и недоступны для редактирования. После заполнения всех требуемых полей для печати документа

необходимо нажать кнопку Печать. Для отмены печати документа необходимо нажать кнопку Отмена.

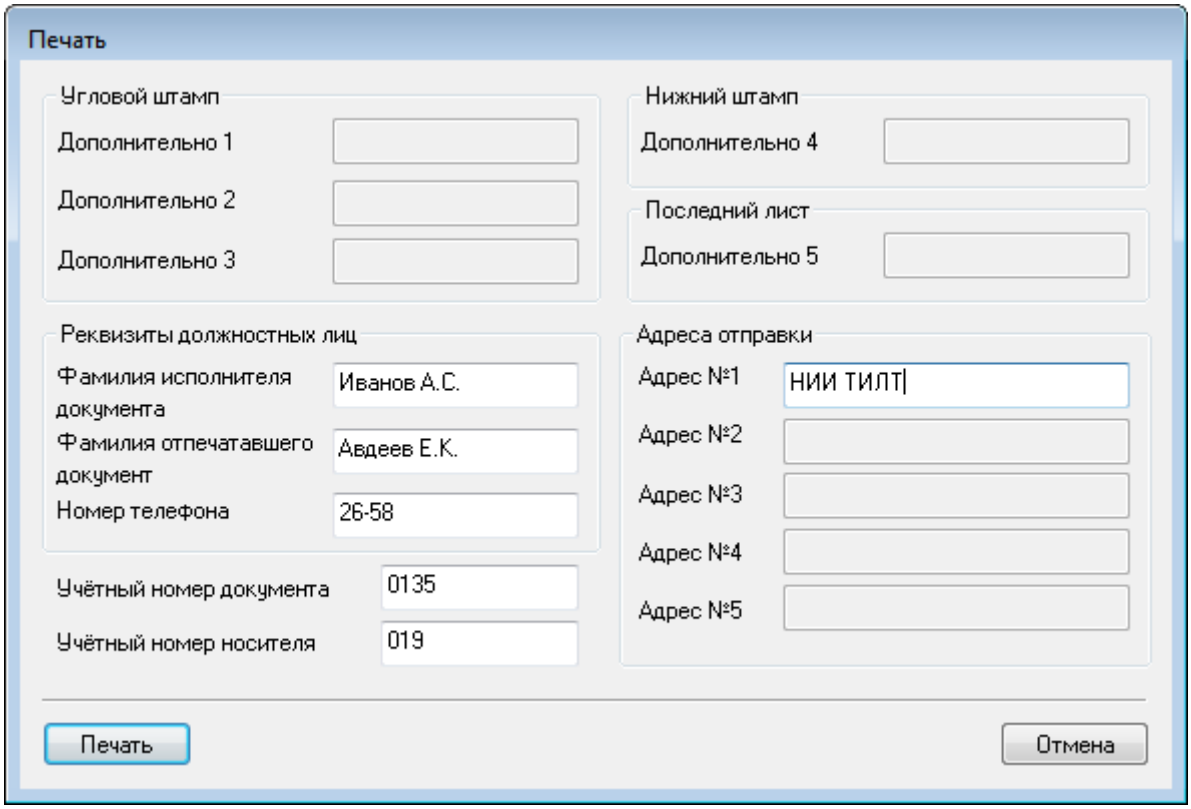


Рис. 13. Пример окна маркировки печати.

Для корректной маркировки документов исполнителями должны выполняться перечисленные ниже требования:

- При подготовке документа должны быть оставлены поля для соответствующих штампов.
- Длина текста в полях, предназначенных для заполнения пользователем, должна быть соответствующей для размещения на листе.
- Документ должен выводиться на печать целиком с первого по последний лист. Выборочная печать отдельных листов или печать листов в обратном порядке не допускается.
- Двусторонняя печать и печать брошюр не допускается, если эта функция не поддерживается принтером.
- Не рекомендуется применять средства окончательной обработки документа, предоставляемые драйвером принтера.

Работа с Менеджером файлов

Для работы с защищаемыми ресурсами рекомендуется использовать программу **Менеджер файлов**. Программа **Менеджер файлов** позволяет выполнять следующие операции:

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

Для запуска программы **Менеджер файлов** необходимо выбрать пункт программного меню **Программы | Страж NT | Менеджер файлов**. При этом на экране появится окно, пример которого показан на Рис. 14.

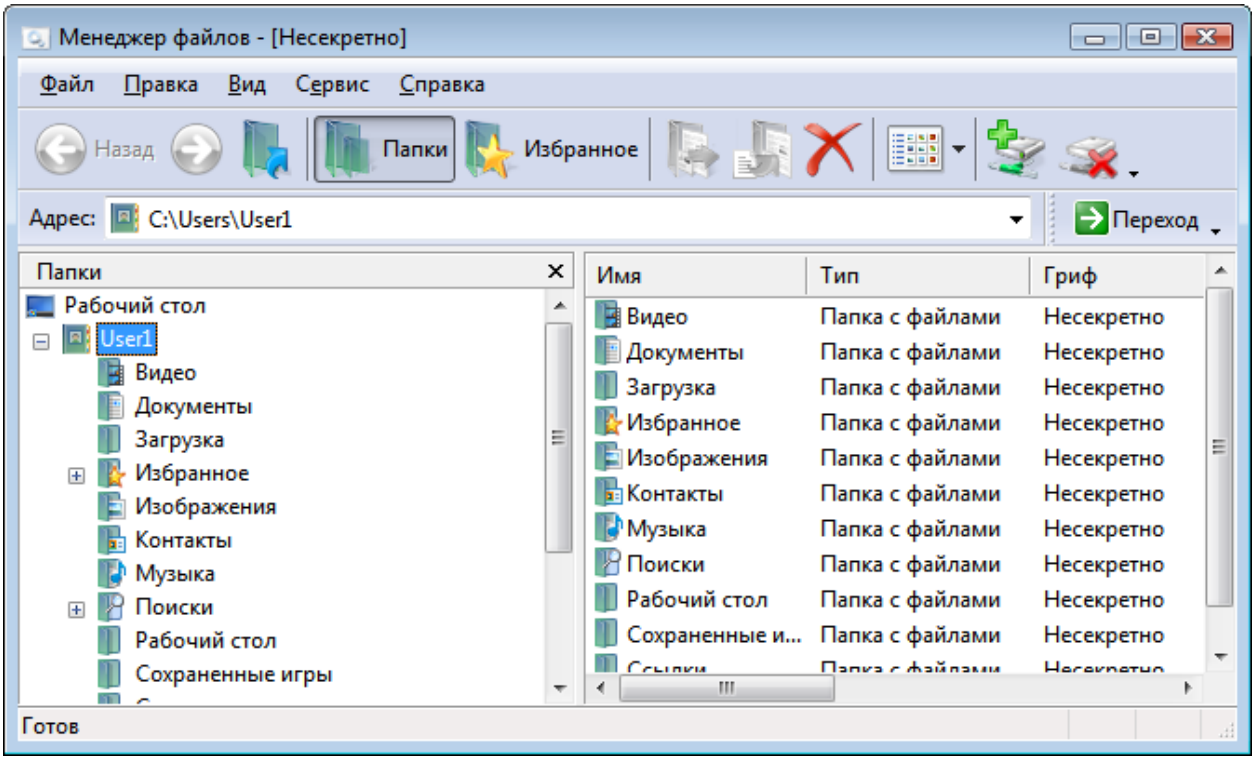


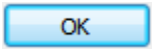
Рис. 14. Общий вид программы Менеджер файлов.

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 .

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. 15, в котором необходимо будет ввести имя, под которым ссылка на выбранную папку будет отображаться в списке избранных папок, и нажать кнопку  . Для удаления ссылки на папку из списка избранных папок необходимо вызвать ее контекстное меню и выбрать пункт **Удалить ссылку**.

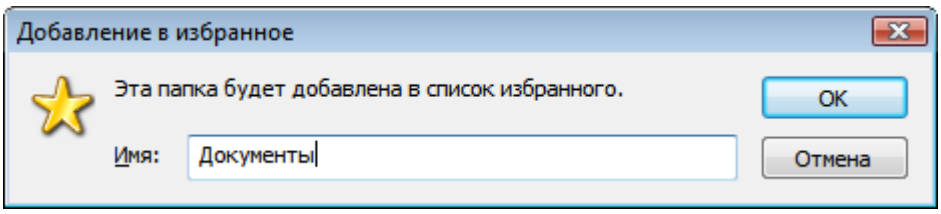


Рис. 15. Диалог добавления ссылки в панель Избранное.

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...** . При этом на экране появится диалог, как показано на Рис. 16.

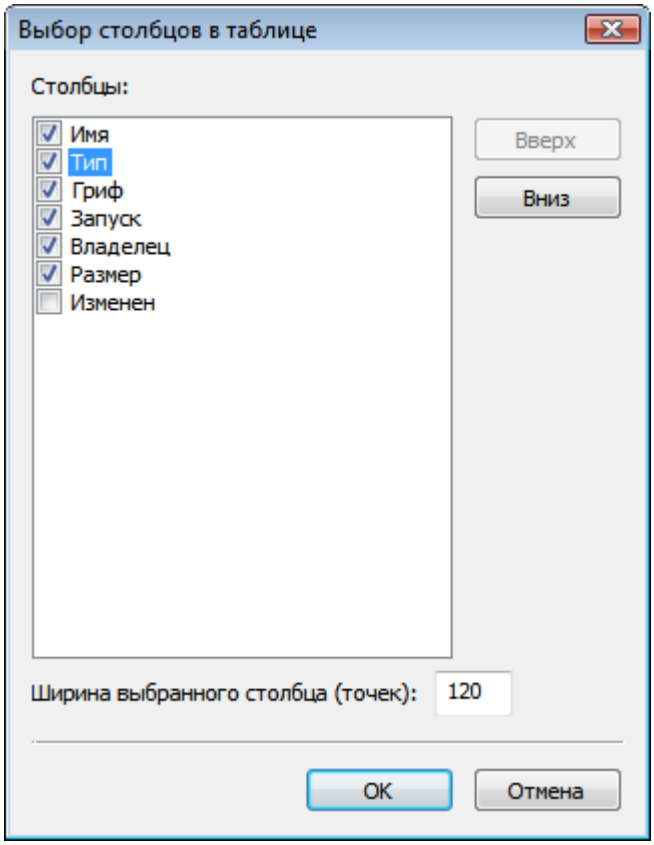


Рис. 16. Выбор отображаемых столбцов

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 Вверх и Вниз, 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 OK.

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.

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.
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.

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.
Н	
Несанкционированный доступ (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.
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.