страж NT

система защиты информации
от несанкционированного
доступа

Руководство пользователя

Версия
4.0

ООО «РУБИНТЕХ»

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 4.0» RU.64476697.00040-01 (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 8.1.

Структура документа

Материал руководства организован следующим образом:

- В главе **Общие сведения** приводятся сведения о назначении системы защиты информации, условиях её применения, а также базовые понятия, связанные с системой защиты.
- В главе **Вход в систему** рассматриваются подробные действия пользователя при входе в систему, а также действия при возможных нештатных ситуациях.
- В главе **Блокировка и разблокировка компьютера** рассматриваются действия пользователя для блокировки и разблокировки компьютера.
- 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, папок и 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» представляет собой программный комплекс средств защиты информации с использованием аппаратных идентификаторов.

СЗИ «Страж NT» предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа. СЗИ «Страж NT» может применяться при разработке систем защиты информации для одно- и многопользовательских автоматизированных систем и информационных систем обработки персональных данных в соответствии с требованиями законодательства Российской Федерации.

Условия применения

СЗИ «Страж NT» может применяться на персональных компьютерах в настольном исполнении, портативных компьютерах, промышленных компьютерах, серверах, в том числе и в составе кластера. СЗИ «Страж NT» может устанавливаться на автономных рабочих станциях, рабочих станциях в составе рабочей группы или домена и серверах. СЗИ «Страж NT» может функционировать на одно- и многопроцессорных системах под управлением 32-х и 64-х разрядных операционных систем, перечисленных в разделе 3 документа «Система защиты информации от несанкционированного доступа «Страж NT». Версия 4.0. Формуляр» RU.64476697.00040-01 30 01.

Компьютер, на котором устанавливается СЗИ «Страж NT», должен удовлетворять требованиям, необходимым для загрузки операционной системы. СЗИ «Страж NT» поддерживает установку как на компьютеры с BIOS, так и компьютеры с UEFI, в том числе и при разбиении системного жесткого диска в стиле GPT.

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

Для всех пользователей СЗИ «Страж NT» предусмотрена единственная роль – Пользователь. 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.
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.

Принципы безопасной работы средства

К основным принципам безопасной работы СЗИ «Страж NT» относятся:

1. Выполнение ограничений по эксплуатации СЗИ «Страж NT», перечисленных в п.4.3 документа «Система защиты информации от несанкционированного доступа «Страж NT». Версия 4.0. Формуляр» RU.64476697.00040-01 30 01.
2. Выполнение действий при работе с СЗИ «Страж NT» строго в соответствии с эксплуатационной документацией на неё.
3. Контроль физической сохранности средств вычислительной техники с установленной СЗИ «Страж NT».
4. Сохранение в секрете пароля пользователя.
5. Исключение доступа посторонних лиц к персональному идентификатору.

Действия после сбоев и ошибок эксплуатации средства

В случае возникновения сбоев и ошибок эксплуатации средства необходимо:

1. Прекратить эксплуатацию СЗИ «Страж NT».
2. Сообщить о возникновении сбоев и ошибок эксплуатации средства администратору СЗИ.

Типы событий безопасности, связанных с доступными пользователю функциями средства

В СЗИ «Страж NT» реализована собственная подсистема регистрации событий. Все регистрируемые события, связанные с доступными пользователю функциями средства, разделены на следующие категории:

- события контроля целостности;
- события входа в систему;
- события запуска программ;
- события доступа к объектам;
- события управления объектами доступа;
- события управления носителями;
- события управления устройствами;
- события печати.

При возникновении какого-либо события регистрируются следующие параметры:

- дата и время;
- код события;
- имя пользователя;
- другие параметры, зависящие от категории события.

Вход в систему

В данной главе рассматриваются подробные действия пользователя при входе в систему, а также действия при возможных нештатных ситуациях.

Первоначальный вход в систему

Для входа в систему и загрузки операционной системы пользователь должен быть зарегистрирован 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, а также назначает ему пароль, служащий для подтверждения подлинности пользователя.

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

После регистрации пользователя Администратор системы защиты должен выдать ему 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 необходимо предъявить персональный идентификатор, выданный Администратором системы защиты.

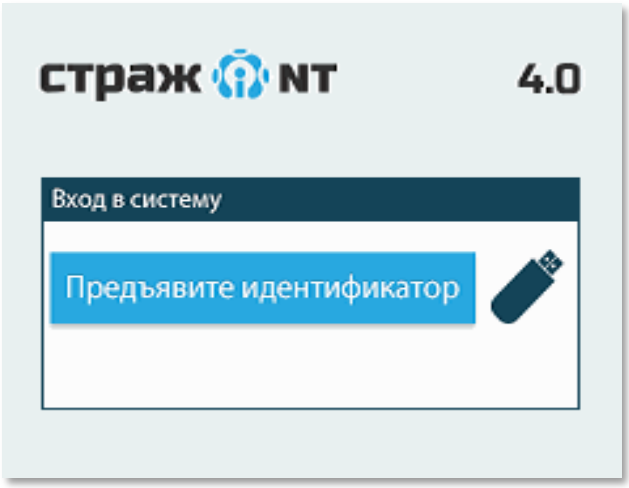

Рис. 1. Стартовый диалог входа в систему.

После считывания предъявленного правильного идентификатора на экран выводится запрос на ввод пароля (см. Рис. 2). Если пользователю назначен пустой пароль, загрузка системы продолжится автоматически.

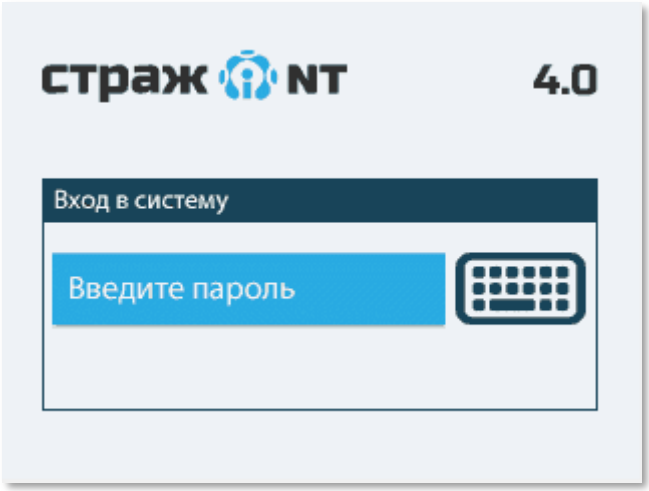

Рис. 2. Ввод пароля пользователя.

Если пароль пользователя был введен неправильно, подсистема идентификации визуально и с помощью звука просигнализирует об этом и предложит ввести пароль заново. Если пароль трижды был введен неправильно или если пользователю запрещено входить на данный компьютер, клавиатура компьютера блокируется, и на экране появляется сообщение о попытке несанкционированного доступа (см. Рис. 3), сопровождаемое звуковой сигнализацией. В этом случае для осуществления следующей попытки входа в систему следует произвести перезагрузку компьютера посредством нажатия кнопки RESET или выполнить выключение и включение компьютера.

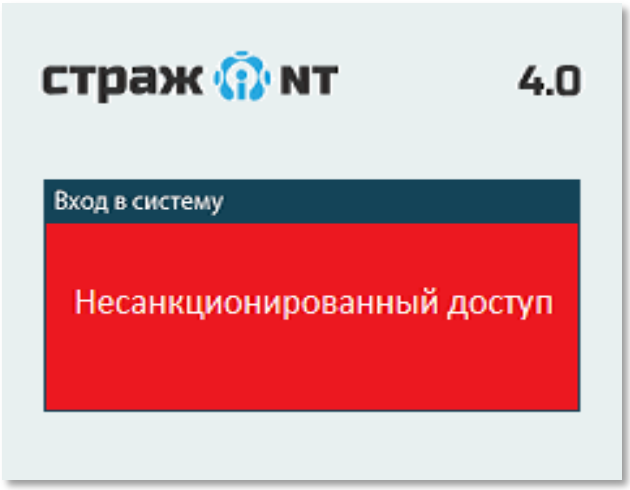

Рис. 3. Сообщение о попытке несанкционированного входа в систему

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

После ввода 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 либо начального экрана. На рабочем столе пользователя в системном лотке, находящемся в правой нижней части панели задач, должен появиться значок программы **Монитор системы защиты**.

Программа **Монитор системы защиты** предназначена для отображения состояния системы защиты и для выполнения некоторых сервисных функций, описанных ниже.

Повторная идентификация пользователей

Для осуществления возможности входа в систему другого пользователя без перезагрузки операционной системы существует механизм повторной идентификации. Для ее выполнения, во-первых, необходимо завершить текущий сеанс пользователя штатными средствами операционной системы и, в случае использования в качестве персонального идентификатора пользователя USB-токена, изъять его. Во-вторых, необходимо предъявить персональный идентификатор другого пользователя и ввести его пароль.

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

Терминальная идентификация

При подключении пользователя к терминальному серверу или удаленному рабочему столу другого компьютера, на котором установлена система защиты, происходит терминальная идентификация пользователя.

Если на компьютере, с которого происходит удаленное подключение, установлена и работает система защиты, идентификация пользователя происходит автоматически, используя данные, записанные в памяти персонального идентификатора пользователя. В противном случае, идентификация пользователя происходит через стандартный запрос имени и пароля пользователя.

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 предъявлении персонального идентификатора не происходит запроса пароля.	
Причина	На идентификаторе нет идентификационной информации.
Действия	Необходимо обратиться к Администратору системы защиты.
При включении компьютера сразу появляется надпись «Введите пароль:».	
Причина	Информация с персонального идентификатора уже была считана.
Действия	Следует продолжить вход в систему, т. е. ввести пароль.
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.

После появления рабочего стола выдается сообщение о нарушении целостности файлов.

Причина	При загрузке операционной системы при проверке целостности файлов системой защиты было обнаружено нарушение целостности по крайней мере одного файла.
Действия	Необходимо обратиться к Администратору системы защиты.

Блокировка и разблокировка компьютера

В данной главе рассматриваются действия пользователя для блокировки и разблокировки компьютера.

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. 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 выбрать пункт меню **Режим блокировки** (см. Рис. 4). Включение режима блокировки происходит путем повторного выбора указанного пункта меню.

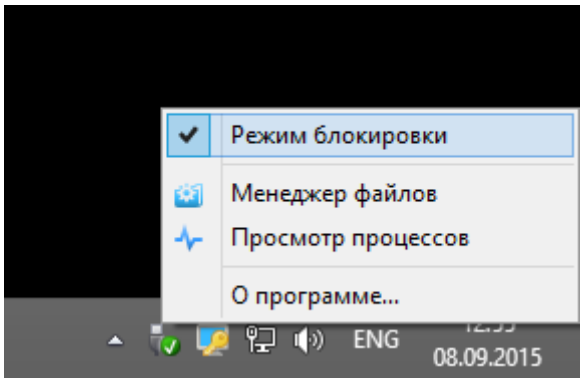

Рис. 4. Включение/выключение режима блокировки.

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. 5.

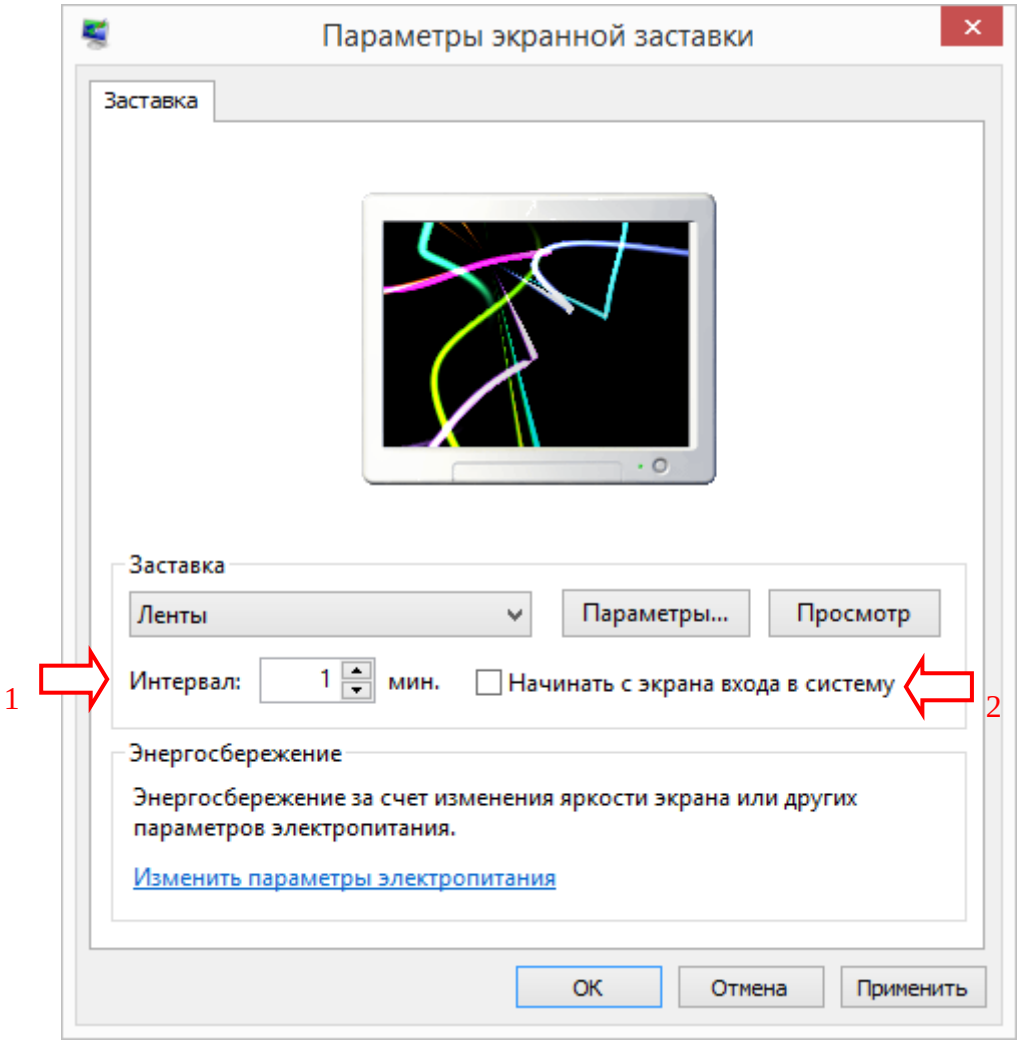

Рис. 5. Задание блокировки компьютера по истечении заданного интервала.

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.

В зависимости от настроек, сделанных Администратором системы защиты, после разблокировки компьютера может запрашиваться пароль пользователя, чей идентификатор установлен в системе.

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:

- Для получения права работы с ресурсами, имеющими метку конфиденциальности, приложению должен быть назначен соответствующий допуск.
- Работа приложения, имеющего допуск, осуществляется в рамках полномочий пользователя, от имени которого произошел его запуск.
- 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.
- Пользователь может получить доступ к ресурсу по чтению и записи в том случае, если текущий допуск приложения, осуществляющего доступ, равен метке конфиденциальности данного ресурса.
- Пользователь может получить доступ к ресурсу, исходя из типа запрашиваемого доступа и списка контроля доступа данного ресурса.
- При создании нового ресурса ему присваивается метка конфиденциальности, равная текущему допуску приложения.
- Допускается одновременная работа приложений с разными текущими допусками.

Работа с Менеджером файлов

Для работы с защищаемыми ресурсами рекомендуется использовать программу **Менеджер файлов** из состава СЗИ «Страж NT». Для запуска программы необходимо выбрать пункт **Менеджер файлов** контекстного меню программы **Монитор системы защиты** или выбрать пункт **Менеджер файлов** в представлении «Приложения» меню «Пуск». При этом на экране появится окно, пример которого показан на Рис. 6.

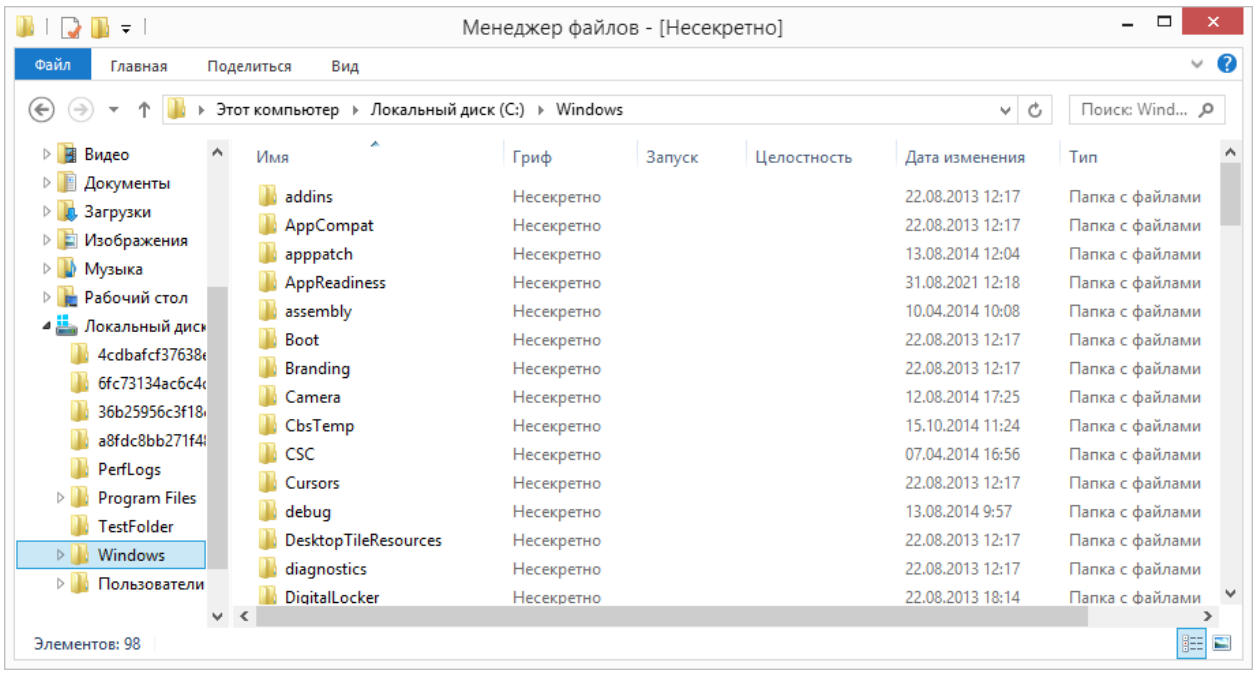

Рис. 6. Общий вид программы Менеджер файлов.

Функционал и интерфейс программы **Менеджер файлов** аналогичен интерфейсу стандартной программы операционной системы **Проводник**. Дополнительно в программе **Менеджер файлов** реализовано отображение специфических атрибутов безопасности СЗИ «Страж NT» – гриф, режим запуска и т.п.

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. 7) выбрать пункт меню **Текущий допуск**.

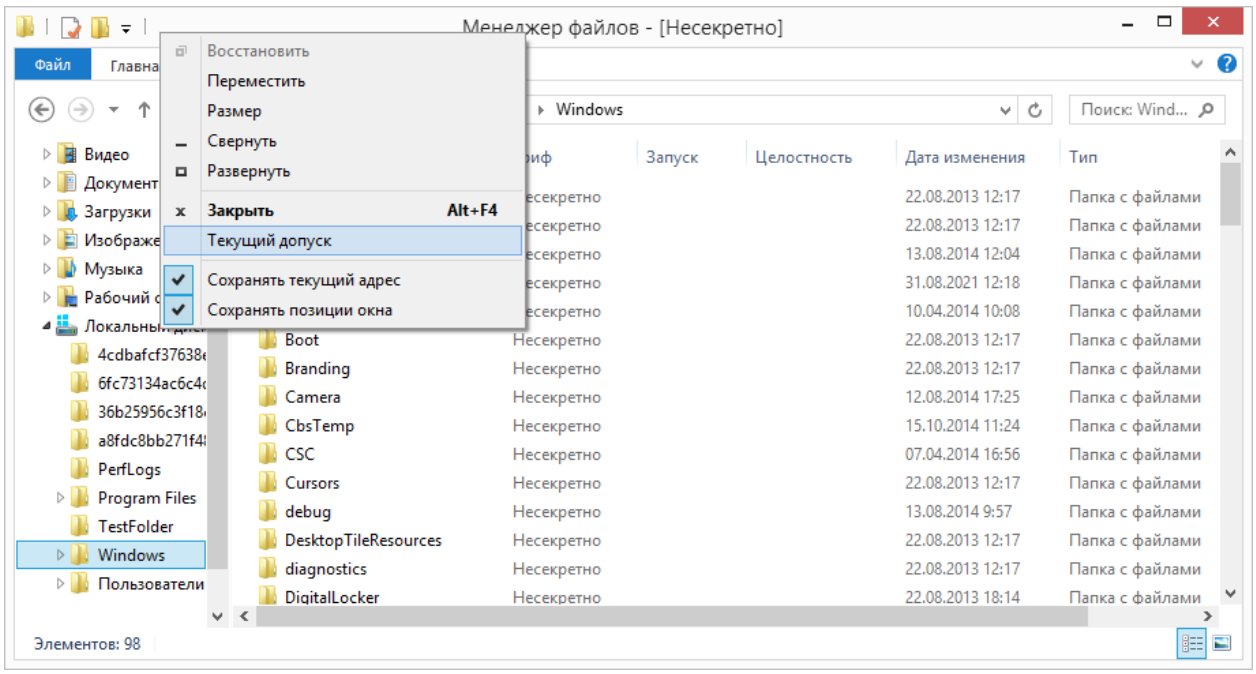

Рис. 7. Запрос изменения текущего допуска приложения.

Из представленного списка (см. Рис. 8) необходимо выбрать, с ресурсами какого уровня Вы собираетесь работать, и нажать кнопку OK.

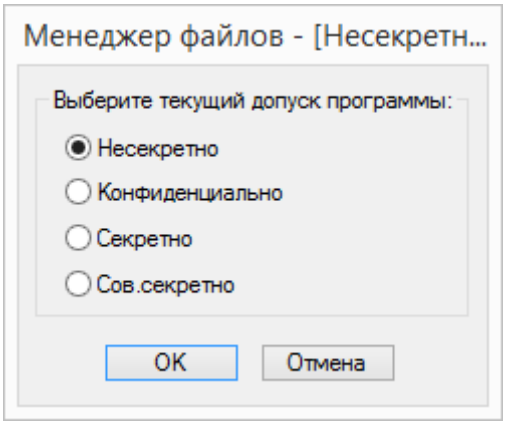

Рис. 8. Диалог выбора текущего допуска приложения.

При попытке изменения текущего допуска приложения на экран может выдаваться сообщение об ошибке, пример которого приведен на Рис. 9.

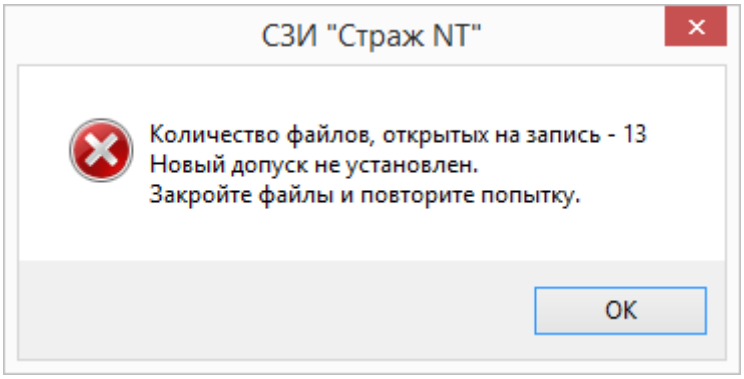

Рис. 9. Пример сообщения о файлах, открытых на запись.

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.

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. 10. 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.

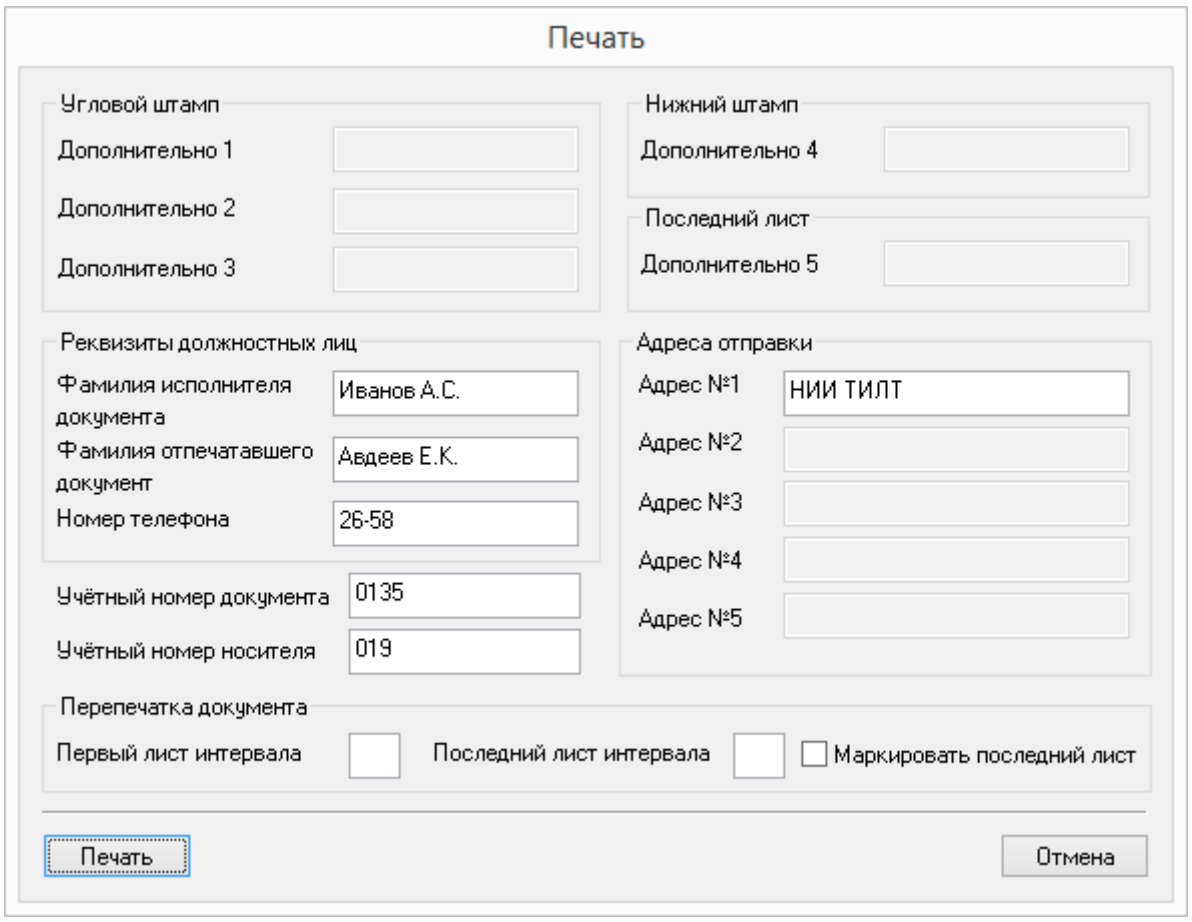

Рис. 10. Пример окна маркировки печати.

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, печать листов в обратном порядке не допускается. Выборочная печать отдельных листов возможна только в режиме допечатки документа.
- Двусторонняя печать и печать брошюр не допускается, если эта функция не поддерживается принтером.
- Не рекомендуется применять средства окончательной обработки документа, предоставляемые драйвером принтера.

Поля **Номер первого листа интервала**, **Номер последнего листа интервала** и флаг **Маркировать последний лист** служат для выборочной печати листов (допечатки

документа). Если указанные поля не заполнены, то листы документа маркируются последовательно, начиная с первого листа. Если поля заполнены, то первый выданный на печать лист будет распечатан под номером, указанным в поле **Номер первого листа интервала**. Дальнейшие листы будут маркироваться последовательно. В случае допечатки документа штамп последнего листа не будет выдаваться на печать, если не установлен флаг **Маркировать последний лист**. Угловой штамп не будет выдаваться на печать, если номер первого листа интервала не равен «1».

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	Режим работы системы, при котором на все запускаемые файлы

расстановки режима запуска (автозапуска)	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).