страж NT

система защиты информации
от несанкционированного
доступа

Руководство администратора

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 администратора «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 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 8.1.

Структура документа

Материал руководства организован следующим образом:

- В главе **Общие сведения** приводятся сведения о назначении системы защиты информации, условия и варианты ее применения, перечисляются возможности системы защиты и описывается организация управления СЗИ. Также в этой главе даются общие сведения о программах настройки и управления системой защиты.
- В главе **Установка и удаление** описаны процедуры установки и удаления системы защиты информации, а также порядок входа пользователей в систему. Дополнительно в этой главе рассматриваются действия администратора системы защиты при возникновении нештатных ситуаций.
- В главе **Вход в систему** главе приводятся сведения о способах идентификации пользователей в системе, а также действия при возможных нештатных ситуациях.
- В главе **Управление пользователями** приводятся сведения о подсистеме управления пользователями, о возможностях и настройках средств администрирования системы защиты. Также описаны типовые действия администратора системы защиты при работе с учетными записями пользователей и персональными идентификаторами.
- В главе **Замкнутая программная среда** описываются сведения о механизмах замкнутой программной среды, способах ее настройки и режимах автозапуска.

- В главе **Управление доступом** приводится описание дискреционного и мандатного принципов контроля доступа, описываются правила их работы и настройки.
- В главе **Управление носителями информации** приводятся сведения о подсистеме учета носителей информации. Описаны интерфейсы средств администрирования системы защиты при работе с подсистемой, а также типовые действия администратора при управлении политиками использования носителей информации.
- В главе **Контроль устройств** приводятся сведения о работе с подсистемой контроля устройств. Описаны интерфейсы средств администрирования системы защиты при работе с подсистемой, а также типовые действия администратора при управлении политиками использования групп устройств.
- В главе **Целостность ресурсов** приводятся сведения о механизмах системы защиты, отвечающих за целостность ресурсов. Описываются сценарии выполнения администраторами системы защиты настройки и контроля целостности защищаемых ресурсов.
- В главе **Регистрация событий** приводятся сведения о подсистеме регистрации событий, ее возможностях и настройках. Описываются сценарии выполнения администраторами системы защиты настройки параметров дополнительного аудита.
- В главе **Работа с журналами** приводятся сведения о средствах администрирования, предназначенных для ознакомления и управления журналами событий, их возможностях и настройках.
- В главе **Сценарии** приводятся сведения о сценариях настроек системы защиты, их типах и функциях. Описан порядок создания и применения сценариев настроек администратором системы защиты.
- В главе **Дополнительные механизмы и настройки** приводится описание дополнительных механизмов и функций системы защиты, а также их настроек.
- В главе **Сетевое развертывание** приводятся сведения о подсистеме сетевого развертывания системы защиты. Описаны возможности средств администрирования при работе с подсистемой, а также типовые действия администратора при сетевом развертывании СЗИ.
- В главе **Тестирование системы** приводятся сведения о подсистеме тестирования механизмов системы защиты. Также описаны типовые действия администратора при тестировании механизмов 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, 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 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, перечисляются возможности системы защиты и описывается организация управления СЗИ. Также в этой главе даются общие сведения о программах настройки и управления 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.

В случае установки СЗИ на компьютер, функционирующий под управлением операционной системы MS Windows 7 или MS Windows Server 2008 R2, требуется установка Пакета обновлений 1 (Service Pack 1) для указанных ОС.

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.

Компьютер, на который устанавливается СЗИ «Страж NT», должен удовлетворять требованиям, необходимым для загрузки операционной системы, а также:

- жесткий диск компьютера, на котором установлена операционная система, должен иметь свободное пространство объемом не менее 100 Мб;
- тип файловой системы на жестких дисках компьютера может быть любой, поддерживаемый операционной системой, например, FAT32 или NTFS;
- для компьютеров с разбиением загрузочного жесткого диска в стиле MBR он должен иметь не менее 63 секторов перед началом первого раздела (32 256 байтов);
- при использовании USB-идентификаторов требуется наличие не менее 1 свободного USB-порта (для компьютеров с разбиением загрузочного диска в стиле MBR требуется наличие хотя бы одного USB-контроллера 2.0 или 1.1);
- язык программ, не поддерживающих Юникод, должен быть установлен в значение «Русский».

В качестве персональных идентификаторов в СЗИ «Страж NT» могут применяться устройства следующих типов:

- гибкие магнитные диски 3,5";
- устройства iButton: DS 1993, DS 1995, DS 1996;
- USB-токены eToken Pro 32K, eToken Pro Java 72K, JaCarta PKI и JaCarta-2 ГОСТ, а также смарт-карты eToken Pro SC, eToken Pro Java SC, JaCarta PKI и JaCarta-2 ГОСТ – при использовании USB смарт-карт ридера ASEDrive от компании Athena Smartcard Solutions;
- USB-токены Guardant ID;
- USB-токены Рутокен S, Рутокен Lite, Рутокен ЭЦП PKI, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Flash, а также смарт-карты Рутокен ЭЦП SC;
- USB-токены eSmart, а также смарт-карты eSmart при использовании USB смарт-карт ридеров ACR38, ACR39 компании Advanced Card Systems;
- USB-флэш-накопители.

При использовании в качестве идентификаторов устройств типа iButton необходимо применение специального считывателя (контактного устройства), подключаемого к последовательному порту компьютера или к порту USB.

При использовании считывателя USB для устройств iButton, USB-токенов или смарт-карт дополнительно требуется установка драйверов устройств в соответствии с документацией на эти устройства и настоящим Руководством администратора.

При использовании в качестве идентификаторов USB-токенов JaCarta PKI и JaCarta-2 ГОСТ, а также смарт-карт JaCarta PKI и JaCarta-2 ГОСТ должны быть установлены драйверы для устройств JaCarta (не входят в состав установочного комплекта). В интерфейсах компонентов системы защиты данные устройства относятся к типу «USB eToken Pro».

При использовании в качестве идентификаторов USB-флэш-накопителей они должны иметь логическую структуру, подобную жестким дискам, т.е. должны содержать раздел.

Процедура определения возможности использования выбранных типов персональных идентификаторов описана в разделе **Тестирование подсистемы идентификации**.

Если система защиты устанавливается на компьютер под управлением операционной системы MS Windows 8 и старше, необходимо, чтобы режим быстрого запуска операционной системы был выключен.

Перед началом установки СЗИ «Страж NT» рекомендуется установить все системное и прикладное программное обеспечение, предусмотренное на данном рабочем месте.

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 входить 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» с единым ключом администратора.

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

Возможности системы защиты

СЗИ «Страж NT» предоставляет следующие возможности:

- идентификация и аутентификация пользователей до загрузки операционной системы при предъявлении персонального идентификатора и пароля;
- идентификация и аутентификация при смене пользователей без перезагрузки операционной системы;
- терминальная идентификация пользователей при подключении к терминальному серверу;
- блокировка компьютера при изъятии персонального идентификатора пользователя;
- ограничение неуспешных попыток входа в систему;
- сокрытие логической структуры жесткого диска в целях доверенной загрузки операционной системы;
- управление учетными записями пользователей и персональными идентификаторами;
- реализация дискреционного принципа контроля доступа к защищаемым ресурсам, таким как носители информации, папки, файлы, принтеры, устройства;
- реализация мандатного принципа контроля доступа к защищаемым ресурсам, таким как носители информации, папки, файлы, принтеры;
- контроль потоков информации, в том числе и именованных каналов;
- настройка замкнутой программной среды для пользователей, в том числе и в автоматических режимах;
- контроль запуска DOS-приложений в 32-х разрядных ОС;
- учет и контроль носителей информации;
- преобразование информации на флэш-накопителях;
- контроль подключаемых устройств;
- регистрация всех действий пользователей и администраторов системы защиты;
- маркировка и регистрация документов, выдаваемых на печать;
- работа с журналами событий, их фильтрация и поиск;
- архивирование журналов (в том числе и по расписанию);
- контроль целостности защищаемых файлов и модулей системы защиты;
- очистка файлов при их удалении;

- очистка файлов подкачки страниц при завершении работы;
- восстановление работоспособности системы защиты в случае сбоя;
- ведение резервных копий модулей системы защиты;
- тестирование механизмов системы защиты;
- формирование отчетов по настройкам системы защиты;
- управление сценариями настроек системы защиты;
- архивирование (в том числе и по расписанию) и восстановление настроек защищаемых ресурсов;
- экспорт настроек СЗИ на удаленные компьютеры;
- развертывание системы защиты на удаленных компьютерах;
- настройку подсистем и механизмов системы защиты на удаленных компьютерах.

Более полная информация о возможностях системы защиты с подробным описанием интерфейсов средств администрирования и действий администратора системы защиты приведено в соответствующих главах данного руководства.

Функции администратора системы защиты

В общем случае, администратор системы защиты в рамках своих полномочий по администрированию СЗИ от НСД должен выполнять следующие функции:

- осуществлять приёмку поставленной СЗИ от НСД в соответствии с разделом **Приёмка поставленного средства**;
- вести перечень установленных в подразделениях организации защищенных рабочих станций с указанием наименований и версий установленных на них средств защиты;
- осуществлять учет и периодический контроль за пользователями рабочих станций и их полномочиями;
- периодически осуществлять смену паролей пользователей;
- осуществлять администрирование применяемых на защищаемых рабочих станциях средств защиты;
- периодически анализировать содержимое системных журналов всех рабочих станций и адекватно реагировать на возникающие нештатные ситуации;
- обеспечивать своевременное архивирование журналов событий защищенных рабочих станций и надлежащий режим хранения данных архивов;

- периодически проверять состояние используемых средств защиты, осуществлять проверку правильности их настройки;
- при необходимости осуществлять обновление средств защиты на защищаемых рабочих станциях;
- осуществлять удаление или отключение средств защиты информации при выводе рабочих станций из эксплуатации;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования защищенных рабочих станций и осуществления НСД к информации.

Приёмка поставленного средства

При приемке СЗИ «Страж NT» администратор системы защиты должен выполнить следующие действия:

1. Провести проверку комплектности поставки в соответствии с разделом 5 документа «Система защиты информации от несанкционированного доступа «Страж NT». Версия 4.0. Формуляр» RU.64476697.00040-01 30 01.
2. Провести расчёт контрольных сумм файлов, входящих в состав установочного комплекта, с использованием программы «ФИКС» версии 2.0.2 по алгоритму «Уровень-1, программно» и сравнить их с эталонными значениями, указанными п.5.3 документа «Система защиты информации от несанкционированного доступа «Страж NT». Версия 4.0. Формуляр» RU.64476697.00040-01 30 01.
3. Выполнить установку СЗИ «Страж NT» в соответствии с данным Руководством.
4. Провести расчёт контрольных сумм файлов СЗИ «Страж NT», расположенных на жёстком диске после установки, с использованием программы «ФИКС» версии 2.0.2 по алгоритму «Уровень-1, программно» и сравнить их с эталонными значениями, указанными в п.5.4 документа «Система защиты информации от несанкционированного доступа «Страж NT». Версия 4.0. Формуляр» RU.64476697.00040-01 30 01.
5. При расхождении рассчитанных контрольных сумм файлов с их эталонными значениями необходимо обратиться в службу поддержки производителя СЗИ «Страж NT».

Организация управления системой защиты

Исходя из функций администратора системы защиты можно сформулировать основные принципы настройки и эксплуатации системы защиты информации.

Перед установкой системы защиты администратор должен подготовить компьютеры, на которые планируется установка системы защиты, таким образом, чтобы имя и пароль администратора системы защиты совпадали. Также необходимо подготовить устройства, которые будут играть роль персональных идентификаторов администратора системы защиты и пользователей.

После установки системы защиты необходимо выполнить все настройки для выполнения требований, предъявляемых к системе защиты соответствующими нормативными документами. Также на это шаге необходимо сформировать замкнутую программную среду, единую политику паролей, аудита, регистрации событий и т.д..

После настройки основных подсистем системы защиты необходимо создать пользователей, назначить им пароли и сформировать персональные идентификаторы. Желательно осуществить вход пользователями в систему и запуск необходимых программ для формирования полного профиля пользователя.

После создания пользователей необходимо настроить подсистемы контроля устройств, учета съемных носителей и контроля доступа.

После настройки системы защиты администратор осуществляет периодический контроль за работой защитных механизмов СЗИ, анализирует журналы событий, осуществляет при необходимости донастройку программ с помощью сценариев настроек.

Программы настройки и управления

Администратор системы защиты осуществляет установку, удаление и настройку подсистем и механизмов системы защиты с помощью программ, перечисленных ниже. Большинство программ управления системой защиты расположены в папке **%SystemRoot%\Guard**, которая доступна только администраторам системы. Программы, которые доступны пользователям, расположены в папке пользовательских программ **%ProgramFiles%\Страж NT** для 32-х разрядных операционных систем и в папке **%ProgramFiles(x86)%\Страж NT** – для 64-х разрядных.

Установка и удаление системы защиты

Программа установки и удаления системы защиты предназначена для загрузки всех компонентов системы защиты информации, выполнения необходимых настроек в операционной системе, а также удаления всех компонентов при удалении системы защиты. Файл программы **GInstall.exe** расположен в папке **%SystemRoot%\Guard**.

Подробнее о программе установки и удаления системы защиты см. раздел **Установка и удаление**.

Монитор системы защиты

Программа **Монитор системы защиты** предназначена для отображения состояния системы защиты, а также для быстрого вызова функций управления системой защиты. Файл программы **GTray.exe** расположен в папке пользовательских программ. Программа **Монитор системы защиты** автоматически запускается при загрузке операционной системы и отображает значок программы в системном лотке, находящемся в правой нижней части панели задач. Значок программы зависит от режима, в котором работает система защиты (см. раздел **Режимы автозапуска**).

При нажатии правой клавиши мыши на значке появляется контекстное меню, позволяющее запустить некоторые сервисные функции системы защиты:

Пункт меню	Описание
Останов	Останавливает механизмы системы защиты до перезагрузки системы или до их запуска.
Запуск	Запускает механизмы системы защиты в штатном режиме.
Включение/Отключение ЗПС	Включает или отключает механизм замкнутой программной среды (см. раздел **Включение и отключение ЗПС**).
Режим автозапуска...	Включает или отключает режимы автозапуска (см. раздел **Режимы автозапуска).**
Режим блокировки	Включает или отключает режим блокировки (см. раздел **Блокировка и разблокировка компьютера**).
Менеджер файлов	Запускает программу **Менеджер файлов**.

Менеджер файлов (администратор)	Запускает программу **Менеджер файлов** в режиме одобрения администратором.
Просмотр процессов	Запускает программу **Просмотр процессов**.
Сетевое развертывание	Запускает программу **Сетевое развертывание**.
Консоль управления	Запускает программу **Консоль управления**.
О программе...	Показывает сведения о программе.

Консоль управления

Основной программой настройки и управления системой защиты является программа **Консоль управления**. Файл программы **GManager.exe** расположен в папке **%SystemRoot%\Guard**. Программа **Консоль управления** предназначена для выполнения администратором системы защиты следующий действий:

- настройка общих параметров системы защиты информации;
- создание замкнутой программной среды;
- управление пользователями системы и идентификаторами;
- учет носителей информации и настройка параметров их использования;
- настройку параметров контроля подключенных устройств компьютера;
- работа с журналом событий системы защиты;
- создание и применение сценариев настроек защиты;
- формирование отчетов по настройкам системы защиты;
- тестирование механизмов системы защиты;
- архивирование и восстановление настроек системы защиты.

Для запуска программы необходимо выбрать пункт **Консоль управления** контекстного меню программы **Монитор системы защиты** при работе с рабочим столом или выбрать пункт **Консоль управления** в представлении «Приложения» начального экрана. Главное окно программы содержит следующие области (см. Рис. 1):

1. Меню с набором пунктов в зависимости от выбранной вкладки.
2. Панель инструментов с наиболее часто используемыми командами в зависимости от выбранной вкладки.
3. Вкладки подсистем.
4. Панель со списком компьютеров в сети и их статусами.

5. Дополнительная панель выбора вкладок с содержанием в зависимости от выбранной вкладки.
6. Основное окно с наполнением в зависимости от выбранной вкладки.

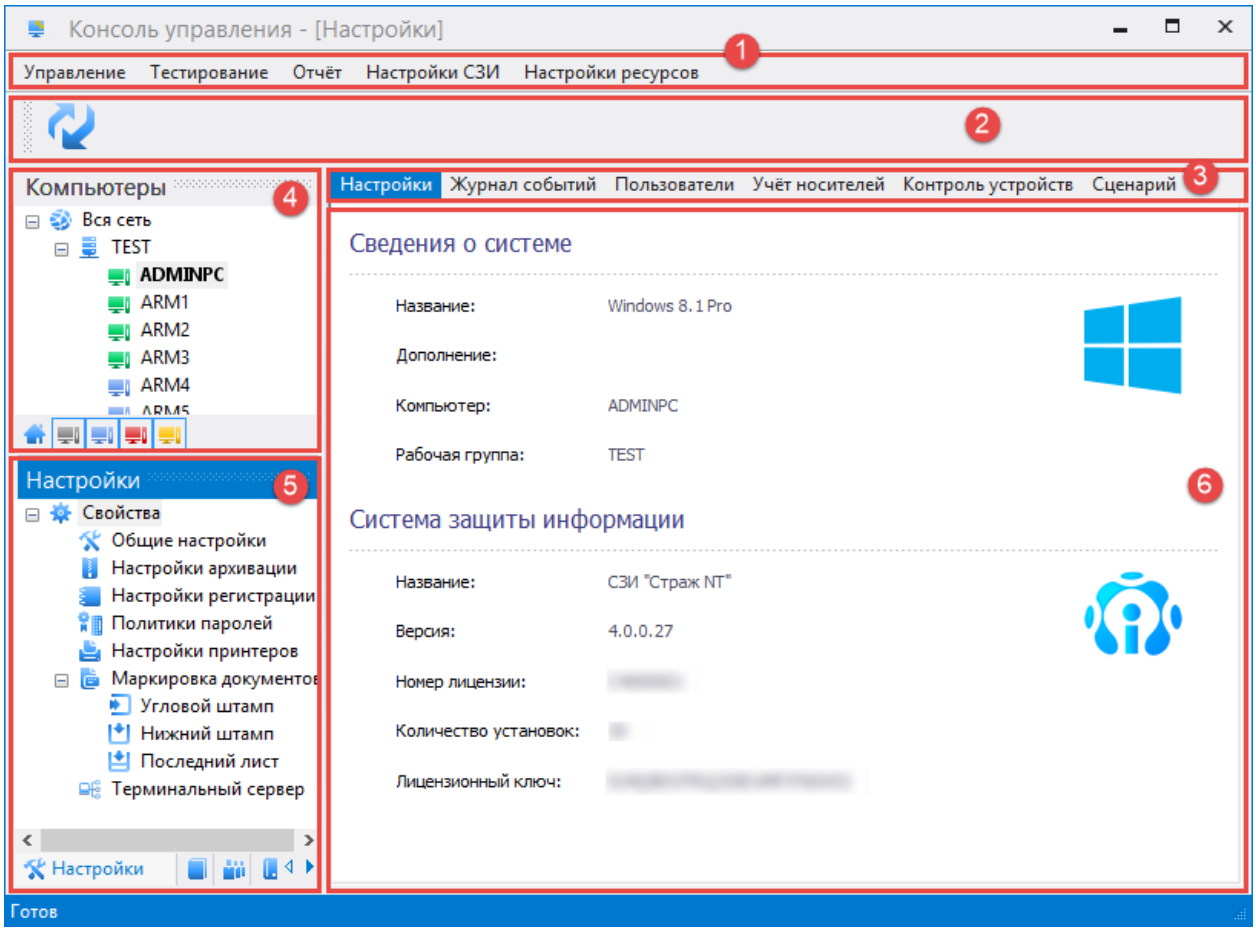


*Рис. 1. Общий вид программы **Консоль управления**.*

Вкладка **Настройки** предназначена для управления настройками системы защиты и получения сведений о СЗИ.

Вкладка **Журнал событий** предназначена для работы с журналами событий.

Вкладка **Пользователи** содержит инструменты для работы с подсистемой управления пользователями и идентификаторами.

Вкладка **Учет носителей** содержит инструменты для работы с подсистемой управления носителями информации.

Вкладка **Контроль устройств** содержит инструменты для работы с подсистемой контроля устройств.

Вкладка **Сценарий** предназначена для работы со сценариями настроек системы защиты.

Панель компьютеров представляет собой дерево компьютеров, которые на настоящий момент видимы в локальной сети, а также их статусы. Для отображения дерева компьютеров необходимо, чтобы на компьютере, на котором запущена программа **Консоль управления**, параметр сетевого обнаружения был установлен в состояние **Включено**.

Родительский узел списка компьютеров определяет название рабочей группы или домена, куда входят компьютеры. Иконка компьютера определяет его статус:

 - компьютер недоступен или выключен

 - компьютер включен, СЗИ не установлена

 - компьютер включен, не удалось получить информацию о состоянии СЗИ

 - компьютер включен, СЗИ остановлена

 - компьютер включен, СЗИ включена, работает или настраивается

На панели компьютеров можно выбрать компьютер, если на нём установлена и работает система защиты, либо он является контроллером домена. Локальный компьютер (компьютер, на котором запущена программа) выделяется **полужирным** начертанием. При выборе какого-либо компьютера вся отображаемая в окнах программы информация и все дальнейшие действия в этой программе относятся к выбранному компьютеру.

При выборе домена в дереве компьютеров производится попытка подключения к контроллеру домена. Вся отображаемая в окнах программы информация и все дальнейшие действия в этой программе относятся к ***контроллеру выбранного домена.***

Более подробное описание интерфейсов будет дано в разделах, описывающих соответствующие подсистемы.

Просмотр процессов

Программа **Просмотр процессов** предназначена для просмотра списка запущенных в системе процессов с их текущими допусками. Файл программы **GProcess.exe** расположен в папке пользовательских программ. Подробнее о программе **Просмотр процессов** см. раздел **Просмотр процессов**.

Сетевое развертывание

Программа **Сетевое развертывание** предназначена для удаленной установки и удаления системы защиты на компьютеры в локальной сети, а также для удаленной установки

драйверов поддержки идентификаторов. Файл программы **GDeploy.exe** расположен в папке **%SystemRoot%\Guard**. Подробные сведения о функциях программы и ее использовании приводятся в разделе **Сетевое развертывание**.

Менеджер файлов

Управление ресурсами, а также их защитными атрибутами, осуществляется с помощью программы **Менеджер файлов**. Файл программы **GExplorer.exe** расположен в папке пользовательских программ. Программа **Менеджер файлов** предназначена для выполнения следующих операций:

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

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. 2.

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.

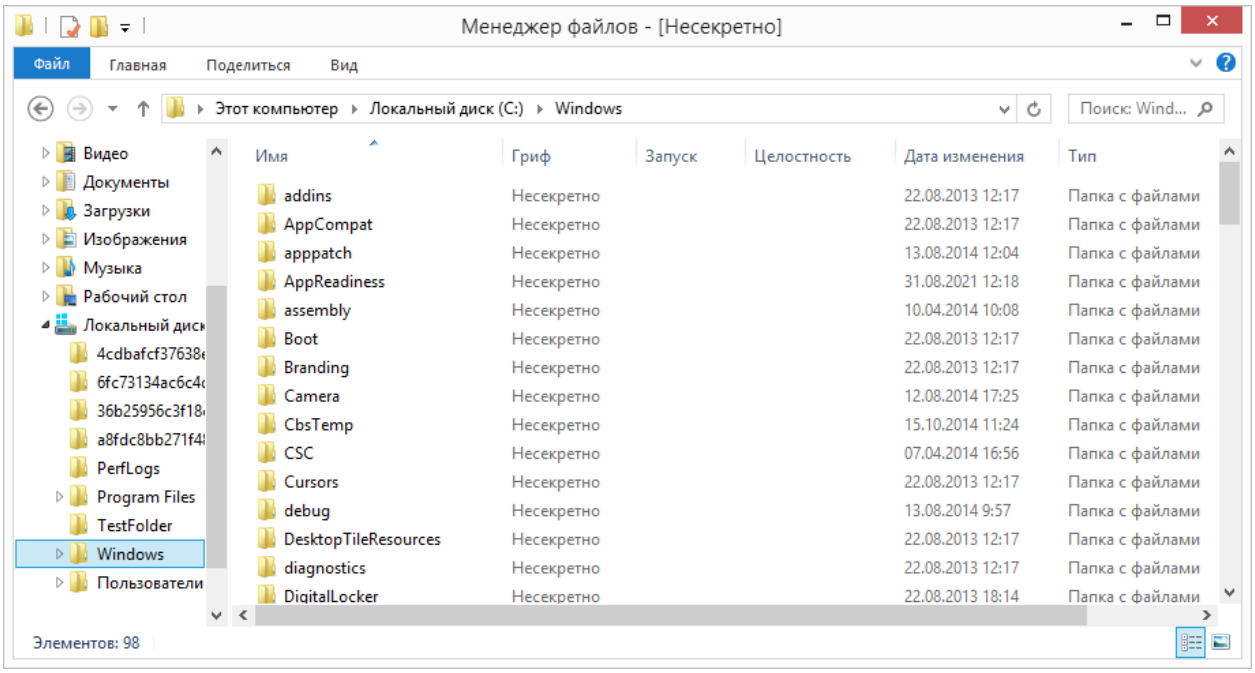


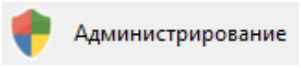
Рис. 2. Общий вид программы Менеджер файлов.

Работа с параметрами безопасности

С помощью программы **Менеджер файлов** над файловыми ресурсами можно выполнять следующие связанные с параметрами безопасности 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)	Пользователям, входящим в локальную группу администраторов
Операция	**Доступ**
Изменение владельца	Пользователям, входящим в локальную группу администраторов
Проверка целостности	Всем пользователям
Назначение грифа документов Установка режима запуска и допуска программ Редактирование параметров дополнительного аудита Установка параметров целостности	Администраторам системы защиты в режиме администрирования

Некоторые операции можно выполнить только в режиме администрирования. Для перехода в режим администрирования необходимо в программе **Менеджер файлов** нажать кнопку 

на панели инструментов. Для выхода из режима администрирования необходимо еще раз нажать кнопку 

на панели инструментов.

Более подробно операции, связанные с параметрами безопасности, будут описаны в соответствующих главах настоящего документа.

Установка и удаление

В данной главе описываются мероприятия, которые необходимо выполнить до установки системы защиты информации, подробно описывается процесс установки и снятия СЗИ. Отдельно разбираются нештатные ситуации, возникающие в процессе установки и снятия СЗИ.

Подготовка к установке

Во избежание непредвиденных ситуаций и предотвращении разного рода ошибок при установке и эксплуатации системы защиты, следует предварительно подготовить рабочее место. Для этого необходимо провести ряд процедур:

- проверить оперативную память компьютера, а так же его жесткий диск на отсутствие вирусов;
- убедиться, что на компьютере в данный момент не работают 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;
- убедиться, что пароль пользователя, устанавливающего систему защиты, не содержит 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 зашиты.

После установки системы защиты изменение логической структуры жестких дисков запрещается.

Тестирование подсистемы идентификации

Тестирование подсистемы идентификации проводится перед установкой системы защиты информации. Данный программный модуль предназначен для определения работоспособности системы считывания персональных идентификаторов.

Для начала тестирования подсистемы идентификации необходимо в BIOS Setup компьютера выставить настройки, определяющие принудительную загрузку системы с носителя информации, на котором поставляется установочный комплект СЗИ.

Для получения корректных результатов тестирования загружаться с носителя следует в том же режиме (UEFI или Legacy), в котором компьютер загружается с жёсткого диска.

После перезагрузки компьютера, когда появится диалог, изображённый на Рис. 3, необходимо предъявить идентификатор, который планируется использовать в качестве персонального идентификатора администратора системы защиты.

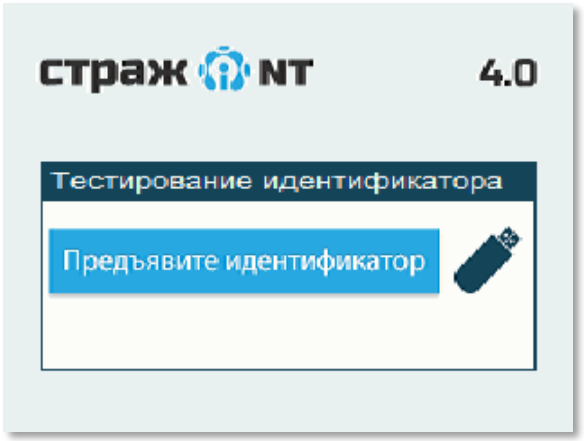


Рис. 3. Тестирование подсистемы идентификации.

Если подсистема идентификации распознает и прочитает предъявленный идентификатор, на экран будет выведено сообщение «Тест завершен». В противном случае установку СЗИ с данным идентификатором выполнять не следует. Необходимо проверить работоспособность идентификатора и считывающего устройства, а также убедиться, что порт (устройство), куда устанавливается персональный идентификатор, в настройках BIOS включен(о), и снова провести проверку.

После проведения тестирования идентификатора следует перезагрузить компьютер.

Установка системы защиты

Для начала процесса установки СЗИ «Страж NT» необходимо установить в компьютер носитель информации, на котором поставляется установочный комплект СЗИ. При этом в зависимости от настроек операционной системы и типа носителя возможен автоматический запуск программы **Autorun.exe**. Если окно программы **Autorun.exe** не появляется, необходимо запустить ее самостоятельно, например, с помощью программы **Проводник**. При запуске программы на экране может появиться окно, как показано на Рис. 4. Для продолжения необходимо нажать кнопку Да.

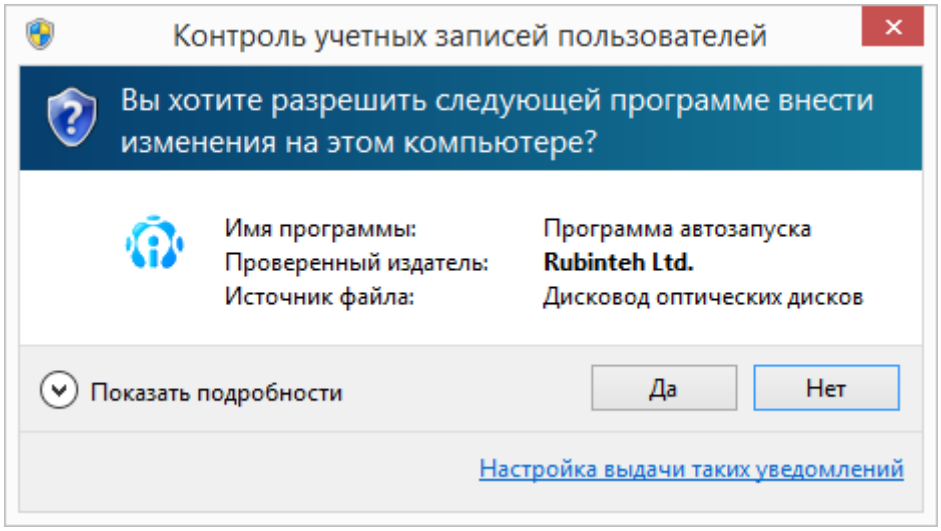


Рис. 4. Сообщение подсистемы контроля учетных записей пользователей.

Перед началом установки системы защиты необходимо установить драйверы устройств, которые будут использоваться в качестве персональных идентификаторов (см. Рис. 5).

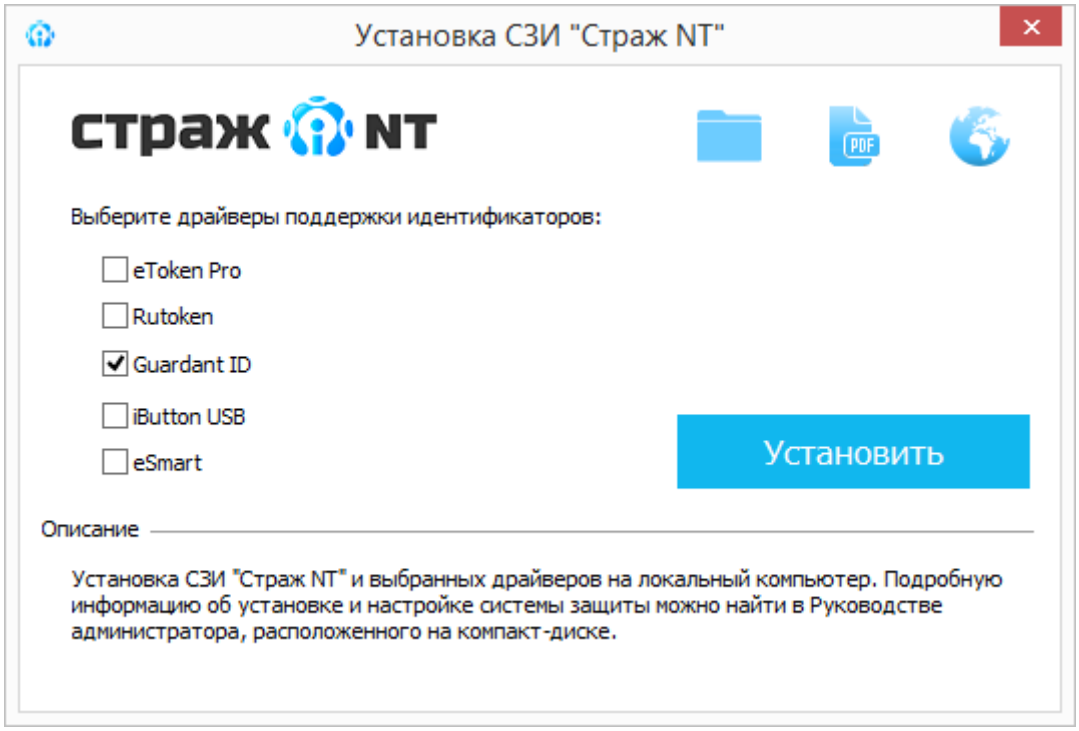


*Рис. 5. Окно программы **Autorun.exe**.*

Для этого необходимо установить флаги в соответствующие поля. Если драйверы какого-либо устройства уже установлены на компьютере, соответствующее поле будет отмечено.

Для старта **Программы установки** необходимо нажать кнопку **Установить**. При этом сначала последовательно будут установлены выбранные драйверы устройств, а потом запустится **Программа установки**.

Все драйверы устройств устанавливаются в «тихом» режиме без взаимодействия с пользователем кроме драйверов считывателя USB для устройств iButton, для установки которых необходимо следовать указанием инсталлятора при его запуске. Также при установке драйверов USB-токенов eSmart может понадобиться подтверждение установки программного обеспечения.

Также **Программу установки** можно запустить непосредственно открыв в **Проводнике** носитель с установочным комплектом системы защиты и запустив программу **Setup.exe**.

Программы установки при запуске проверяет наличие установленной системы защиты. Если система защиты уже установлена на данном компьютере, **Программа установки** проинформирует об этом и предложит снять систему защиты, иначе на экране появится окно, как показано на Рис. 6.

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

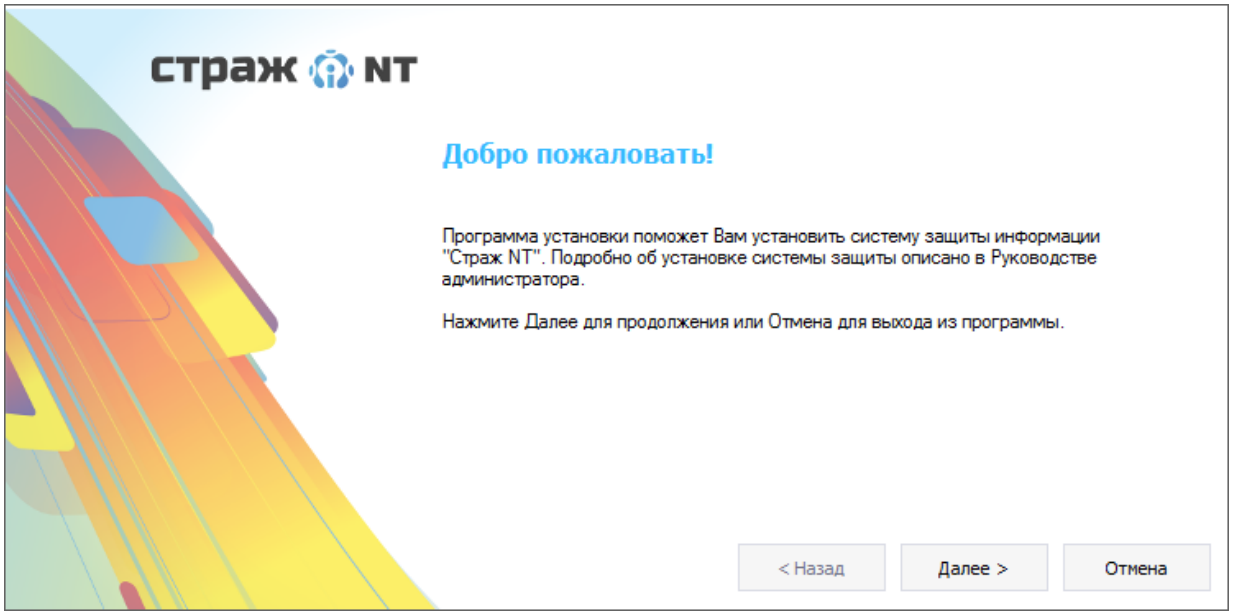


Рис. 6. Окно приветствия Программы установки.

После нажатия кнопки Далее > на экране появится окно с текстом лицензионного соглашения (см. Рис. 7). Внимательно прочитайте его. Для продолжения установки системы защиты необходимо установить флаг в поле **Я принимаю условия лицензионного соглашения** и нажать кнопку Далее >.

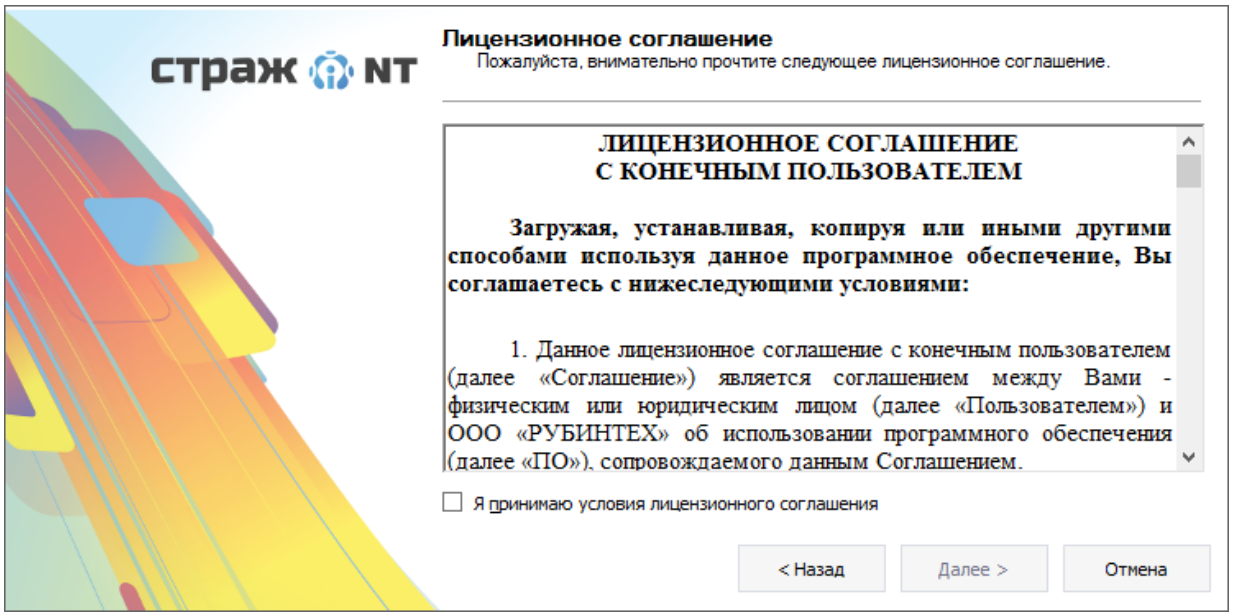


Рис. 7. Лицензионное соглашение.

При этом на экране появится диалог, в котором требуется ввод лицензионного ключа, указанного на бланке Лицензии, входящем в комплект поставки (см. Рис. 8).

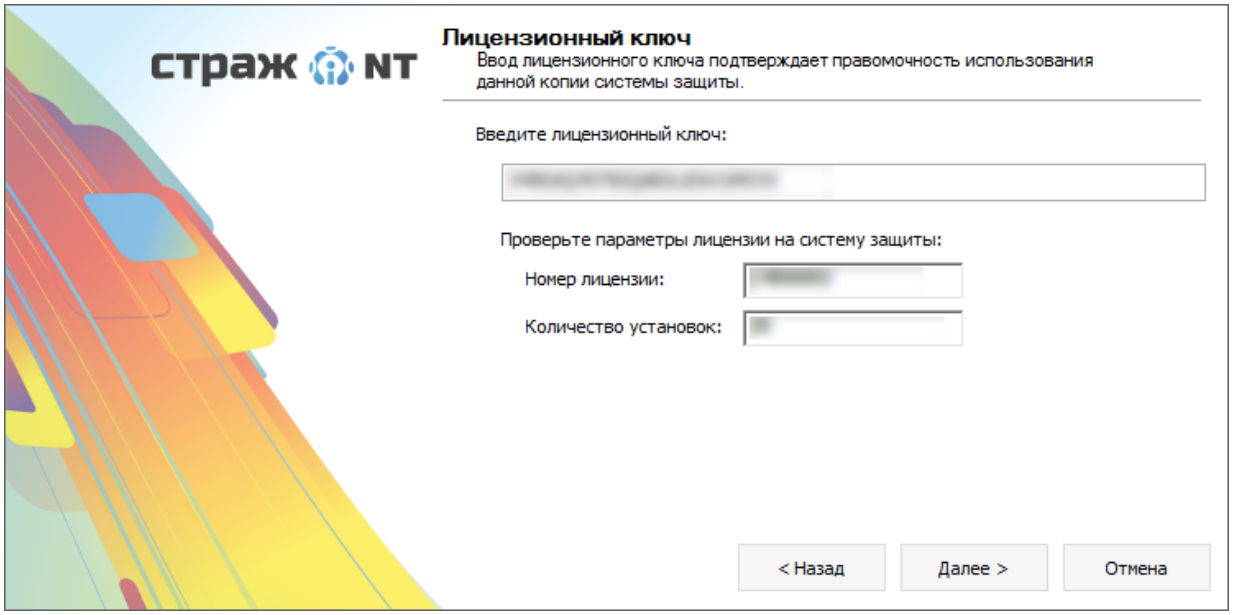


Рис. 8. Ввод лицензионного ключа.

Лицензионный ключ определяет номер лицензии и количество компьютеров, на которые возможна установка системы защиты с данным лицензионным ключом, а также тип лицензии. Лицензионный ключ указывается в лицензии на систему защиты. После правильного ввода лицензионного ключа в окне будут отображены параметры лицензии, а также будет активизирована кнопка Далее > .

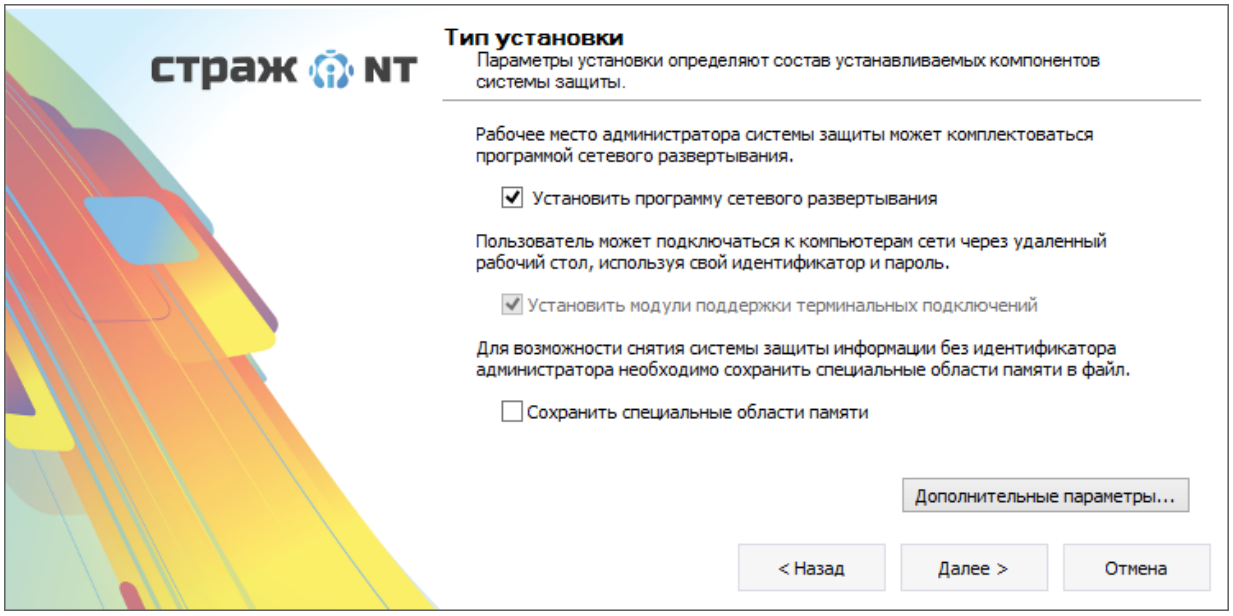


Рис. 9. Выбор дополнительных компонентов.

В следующем диалоговом окне необходимо определить параметры установки системы защиты (см. Рис. 9):

- **Установить программу сетевого развертывания**

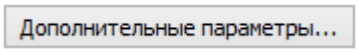
  Данная программа необходима для удаленной установки системы защиты на компьютеры, находящиеся в одной локальной сети (см. раздел **Сетевое развертывание**).

- **Установить модули поддержки терминальных подключений**

  Пользователь может подключаться к терминальному серверу, используя свой идентификатор и пароль (см. раздел **Терминальный доступ**).

- **Сохранить специальные области памяти**

  Для возможности удаления системы защиты информации без идентификатора администратора системы защиты необходимо сохранить специальные области памяти в файл (см. раздел **Аварийное снятие системы защиты**). Данный параметр отображается только при разбиении системного жесткого диска в стиле MBR.

При нажатии на кнопку 

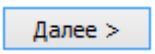
будет открыто окно, в котором можно задать дополнительные параметры установки системы защиты:

- **Отключить блокировку загрузки**

  Для некоторых BIOS необходимо включить данный параметр для правильной загрузки компьютера. Данный параметр доступен для изменения только при разбиении системного жесткого диске в стиле MBR.

- **Включить режим совместимости со средствами доверенной загрузки**

  В режиме совместимости со средствами доверенной загрузки специальные области жесткого диска не преобразуются.

Для продолжения установки необходимо нажать кнопку 

. На данном этапе начинается копирование файлов, регистрация необходимых служб системы защиты и настройка параметров компьютера. Следует обратить внимание, что после выполнения данной процедуры возврат к предыдущим страницам **Программы установки** будет невозможен.

Если в процессе настройки параметров компьютера **Программа установки** определит, что на компьютере включен режим быстрого запуска операционной системы, на экран появится сообщение, как показано на Рис. 10 или Рис. 11.

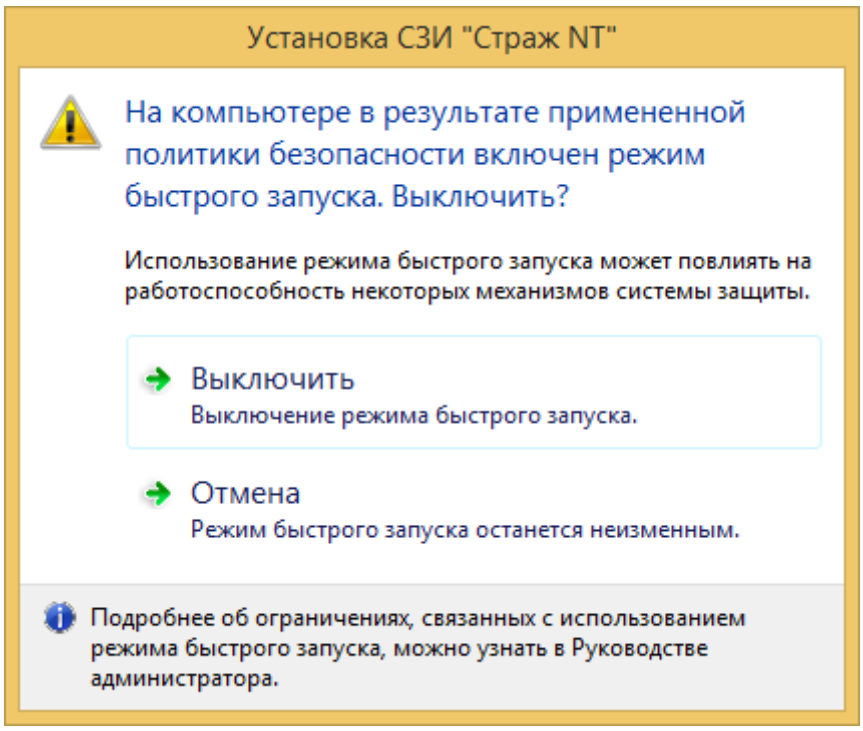


Рис. 10. Запрос на отключение режима быстрого запуска.

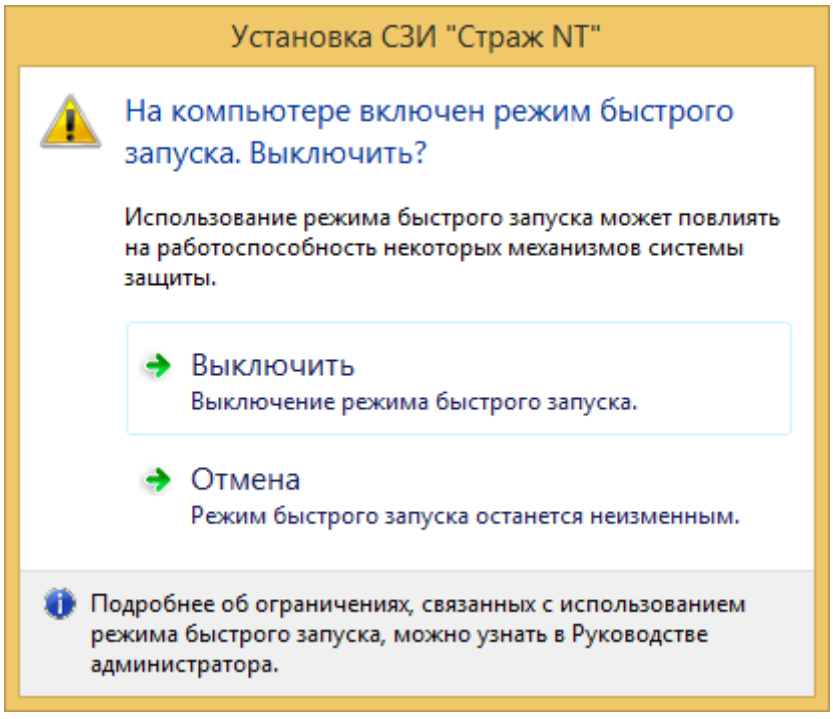


Рис. 11. Запрос на отключение режима быстрого запуска.

Включенный режим быстрого запуска операционной системы вносит следующие ограничения в работу системы защиты:

- Завершение сеанса работы с компьютером необходимо будет осуществлять только через процедуру перезагрузки компьютера. Процедура выключения компьютера не будет выполнять сброс некоторых параметров системы защиты (режим автозапуска, режим блокировки) при смене пользователя и стирать содержимое файла подкачки.
- При включении компьютера после процедуры выключения пользователю необходимо будет два раза проводить процедуру идентификации.

Режим быстрого запуска может включаться на компьютере в результате применения политик безопасности AD. Если так происходит, для выключения режима быстрого запуска необходимо самостоятельно сделать соответствующие изменения в политиках безопасности.

После выполнения необходимых действий по настройке параметров компьютера на экране появится диалоговое окно формирования персонального идентификатора администратора (см. Рис. 12).

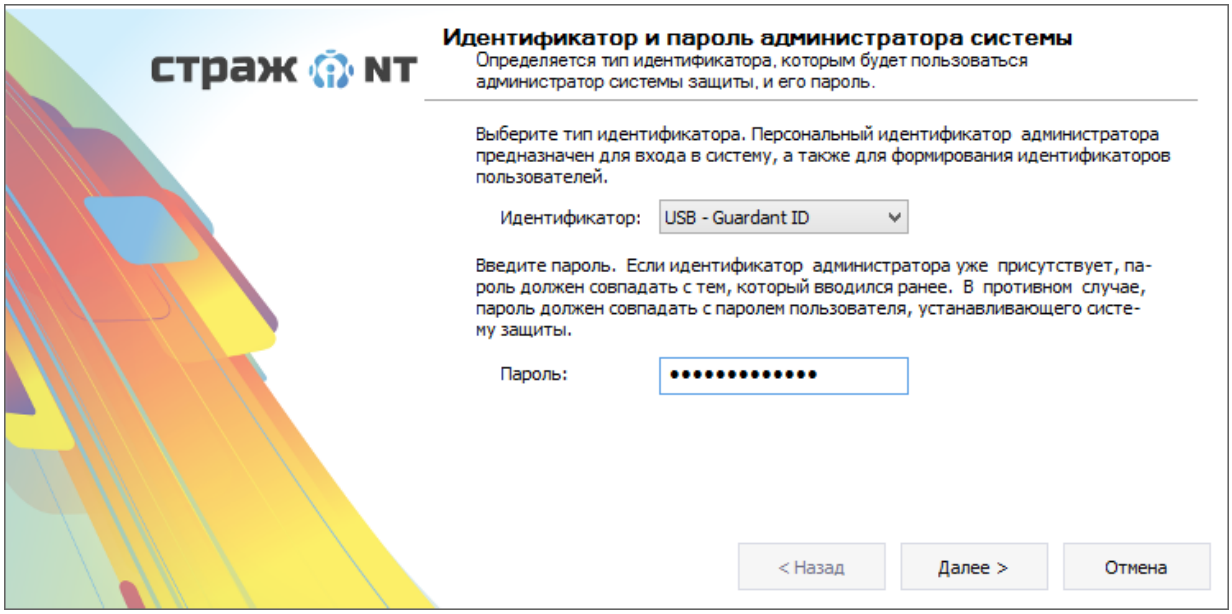


Рис. 12. Формирование идентификатора администратора.

В поле **Идентификатор** перечислены все поддерживаемые операционной системой на момент запуска программы типы идентификаторов кроме USB-флэш-накопителей, так как при установке системы защиты запрещено использовать идентификаторы данного типа. Если в списке типов идентификаторов нет какого-либо типа идентификаторов, значит

либо он недоступен в данной аппаратной конфигурации либо не установлены поддерживающие данный тип драйверы.

В поле **Идентификатор** необходимо выбрать тип идентификатора, которым будет пользоваться администратор системы защиты.

После определения типа идентификатора администратора системы защиты необходимо ввести его пароль и нажать кнопку Далее >. 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, **Программа установки** выдаст сообщение о некорректности введенного пароля и предложит установить его (см. Рис. 13).

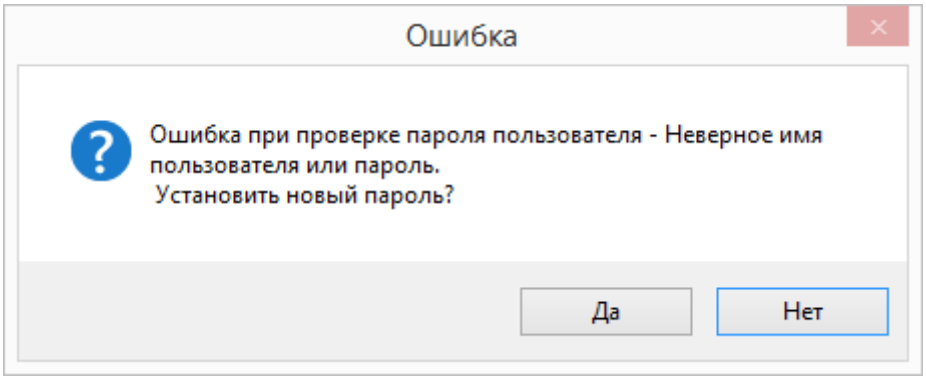


Рис. 13. Ошибка при проверке пароля.

На данное предложение необходимо ответить утвердительно. При этом пользователю, устанавливающему СЗИ, будет предложено подтвердить новый пароль (см. Рис. 14).

Если на предъявленном идентификаторе уже записана информация о данном компьютере, созданная с использованием другой лицензии, на экран будет выведено соответствующее предупреждение с предложением перезаписать данную информацию. При положительном ответе информация о данном компьютере будет перезаписана с учетом нового номера лицензии. При отказе вновь появится диалог, как показано на Рис. 12.

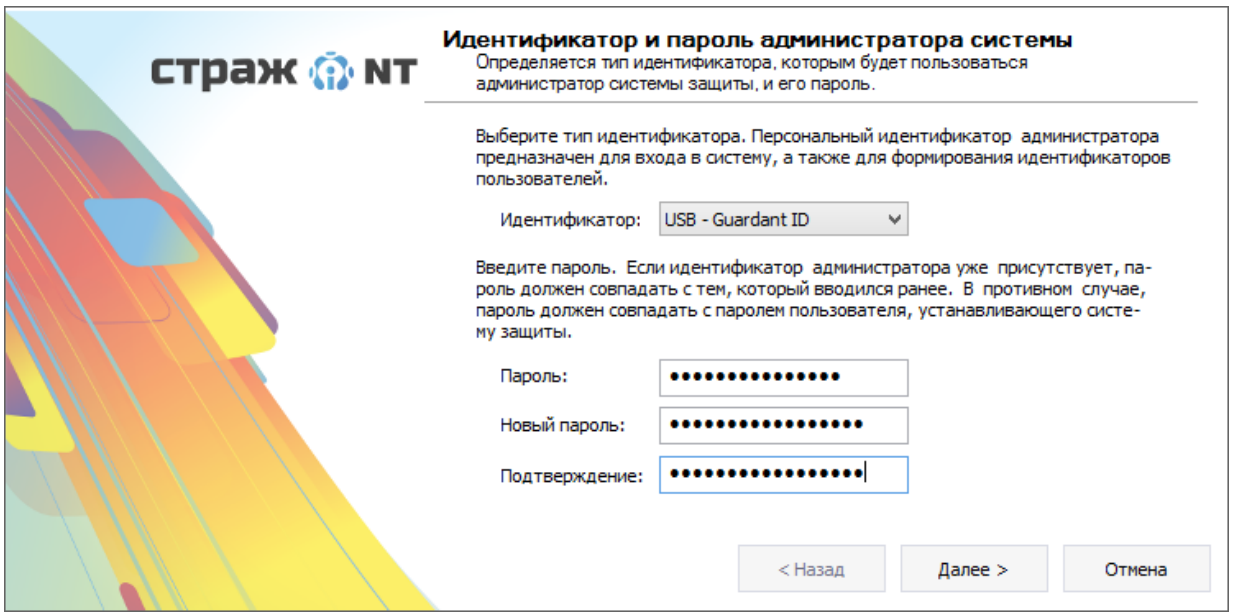


Рис. 14. Ввод и подтверждение нового пароля.

Если на предъявленном идентификаторе уже записана какая-то информация, которую **Программа установки** не сможет распознать, на экран будет выдано предупреждение о перезаписи идентификатора. Если информация, записанная на идентификаторе, не нужна, необходимо ответить положительно. При этом информация, записанная на идентификаторе, будет утеряна. При нажатии кнопки Отмена вновь появится диалог, как показано на Рис. 12.

Систему защиты с помощью одного лицензионного ключа можно устанавливать на такое количество компьютеров, которое указано в лицензии. При наличии нескольких лицензионных ключей количество компьютеров определяется суммарным значением для всех лицензий. Если количество установок превышается, **Программа установки** предупредит об этом, и установка системы защиты будет прекращена. В противном случае, программа считает записанную информацию и добавит к ней информацию о данном компьютере.

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

Если ранее в окне **Параметры установки** был установлен флаг в поле **Сохранить специальные области памяти**, то после нажатия кнопки Далее > появится окно, в котором необходимо выбрать путь для записи файла **GuardRecover.iso**. В данный файл

будет записан образ загрузочного диска восстановления системы, в котором будет находиться информация о системных областях жесткого диска.

Рекомендуется хранить сформированный образ на внешнем носителе информации, например, на USB-флэш-диске в надежном и недоступном, кроме администратора системы защиты, месте.

Подробнее об использовании данного файла описано в разделе **Аварийное снятие системы защиты**.

После формирования персонального идентификатора **Программа установки** завершается кратким отчетом о результате установки (см. Рис. 15).

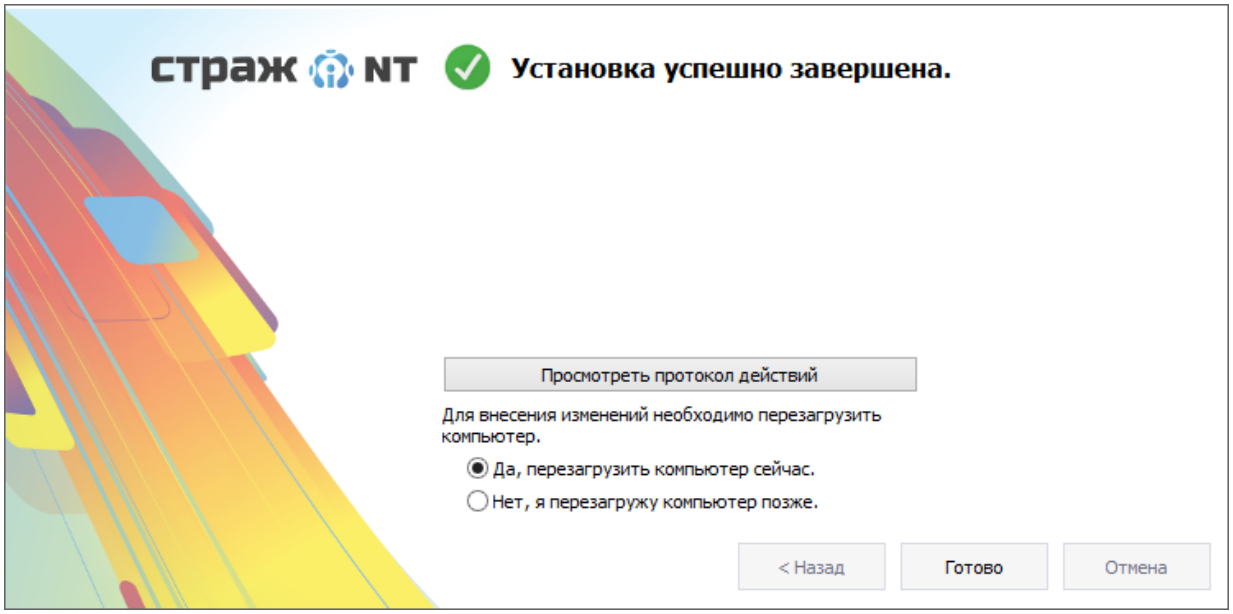


Рис. 15. Завершение установки системы защиты.

В случае обнаружения ошибок при установке системы защиты, программа проинформирует об этом с указанием этапа установки, на котором произошла ошибка. В протоколе действий **Программы 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 Просмотреть протокол действий.

Для перехода к этапу настройки системы защиты необходимо перезагрузить компьютер. Компьютер автоматически перегружается, если при нажатии кнопки Готово было выбрано поле **Да, Перезагрузить компьютер сейчас**. В противном случае необходимо перезагрузить компьютер самостоятельно.

После перезагрузки компьютера для входа в систему необходимо будет предъявить сформированный персональный идентификатор администратора системы защиты и ввести его пароль. Подробнее о процедуре идентификации пользователей описано в главе **Вход в систему**.

Удаление системы защиты

Удаление СЗИ «Страж NT» может выполнить только пользователь, имеющий привилегии администратора системы защиты. Удаление СЗИ «Страж NT» осуществляется через оснастку **Удаление программ** в **Панели управления.** При запуске программы на экране может появиться окно, как показано на Рис. 4. Для продолжения необходимо нажать кнопку Да. При этом на экране появится диалоговое окно, представленное на Рис. 16.

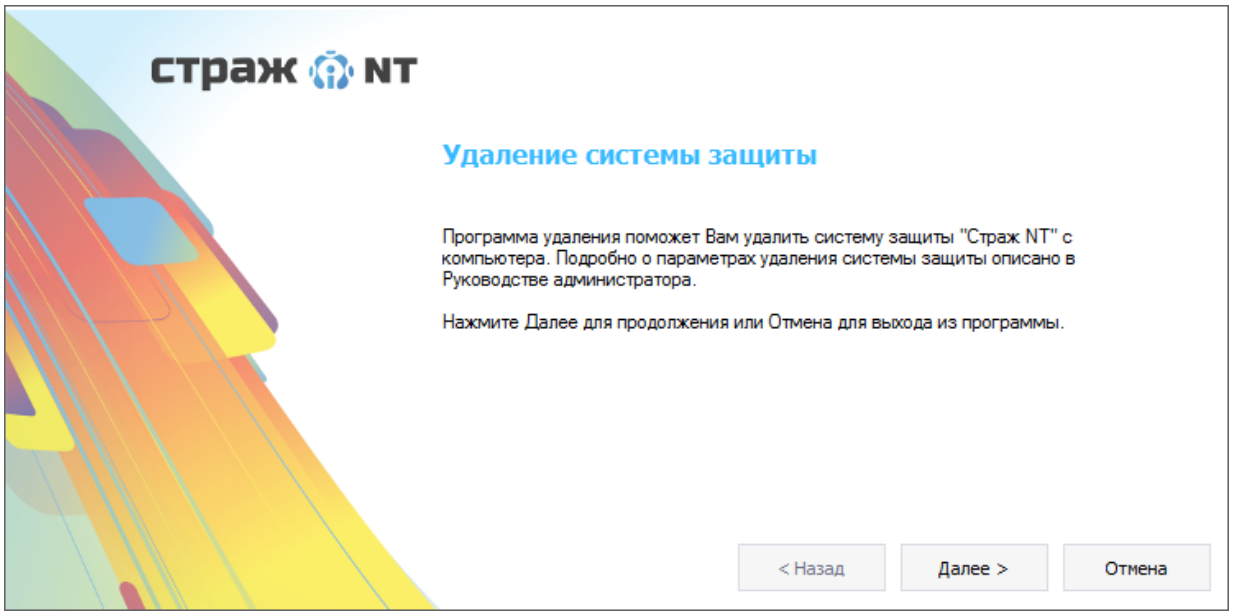


Рис. 16. Начальный диалог Программы удаления.

Для начала удаления системы защиты необходимо нажать кнопку Далее >. При этом на экране появится диалог с параметрами удаления системы защиты (см. Рис. 17):

- **Сохранить параметры настройки защищенных ресурсов**

  Если предполагается последующая установка системы защиты на данный компьютер, имеется возможность сохранения всех настроек системы защиты. Для этого необходимо, чтобы флаг в этом поле был установлен. В противном случае его необходимо снять. При этом все настройки системы защиты будут удалены.

- **Сохранить журналы событий**

  Если необходимо сохранить журналы событий, в том числе и находящиеся в архиве, надо установить флаг в данном поле.

- **Сохранить файлы сценариев**

  Если необходимо сохранить файлы сценариев настройки системы защиты для последующего применения, надо установить флаг в данном поле.

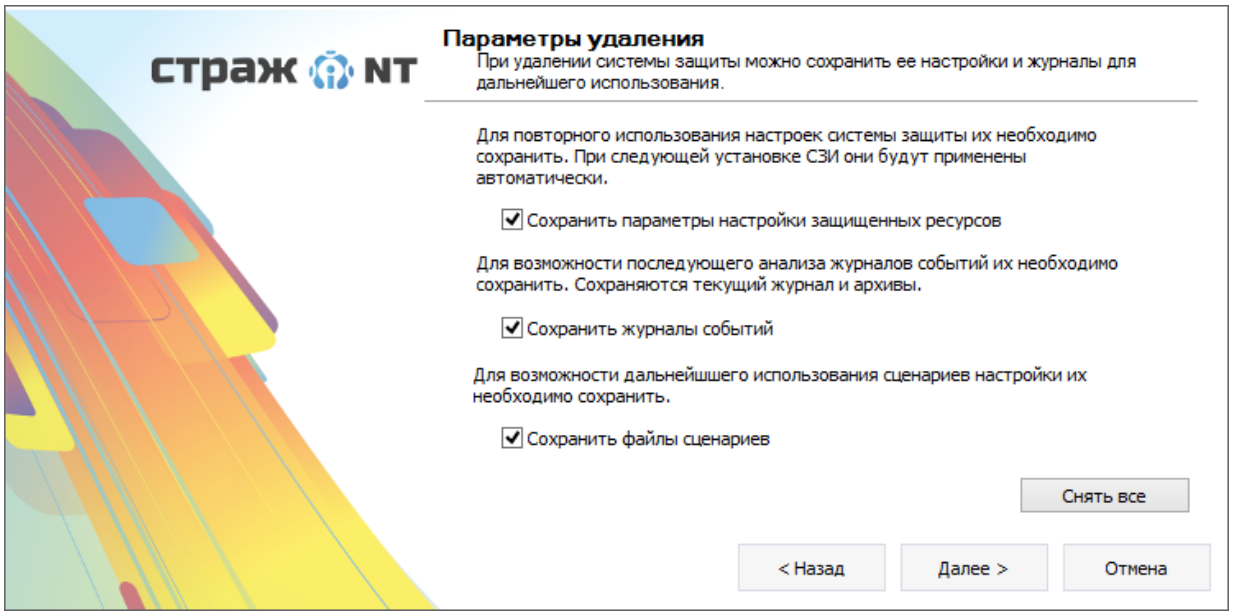


Рис. 17. Параметры удаления системы защиты.

Для продолжения удаления системы защиты необходимо нажать кнопку Далее >.

После удаления системы защиты, если был выбран режим сохранения параметров 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 удалении системы защиты удалены не будут. После удаления СЗИ со всех компьютеров, входящих в домен, в том числе и с контроллера домена, при необходимости глобальные группы GAdmins, GLevel1, GLevel2, GLevel3 удаляются самостоятельно штатными средствами операционной системы.

Если при удалении 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 удаления СЗИ «Страж NT» рекомендуется перезагрузить компьютер (см. Рис. 18). Для этого необходимо выбрать поле **Да, перезагрузить компьютер сейчас** и нажать кнопку Готово.

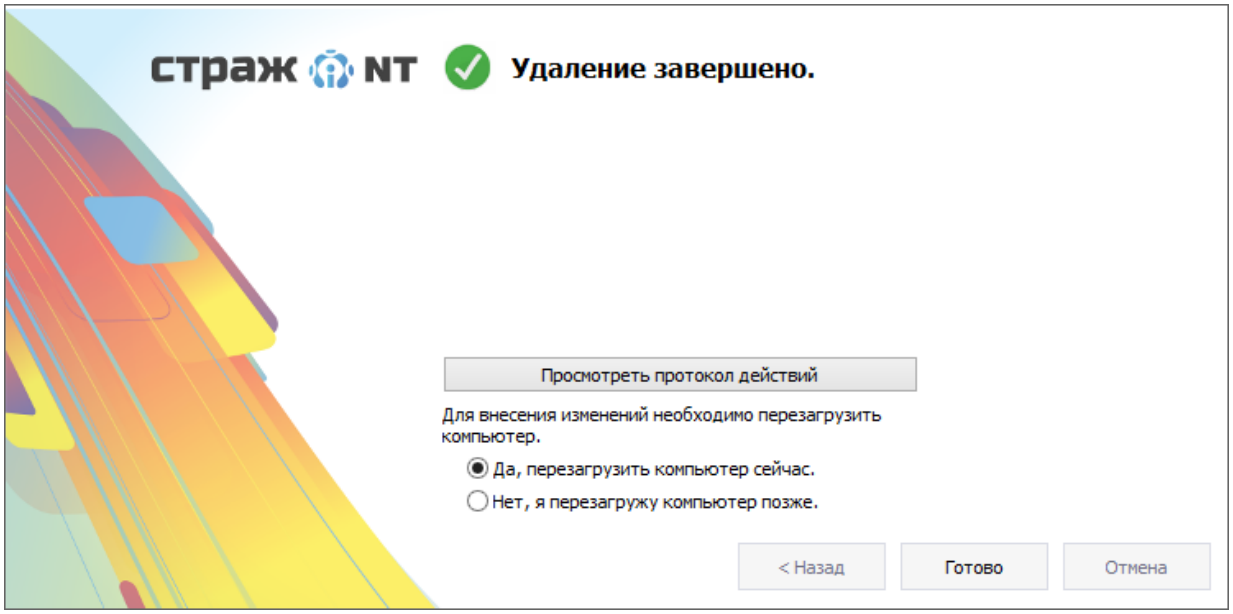


Рис. 18. Завершение Программы удаления.

Обновление системы защиты

Изготовитель оповещает потребителей о выходе обновлений и первичных организационно-технических мерах по нейтрализации выявленных уязвимостей следующими способами:

- в форме информационного письма, направляемого на электронную почту контактного лица, указанного потребителем в Анкете конечного пользователя при оформлении права на использование СЗИ «Страж NT»;
- в форме информационного письма, размещенного в разделе новостей на сайте www.guardnt.ru.

Ответственный за эксплуатацию системы защиты информации обязан периодически проверять наличие сообщений об обновлениях на сайте изготовителя www.guardnt.ru.

Загрузка актуального дистрибутива осуществляется по ссылке www.guardnt.ru/download/40_setup.zip. Автоматическое обновление сертифицированной СЗИ «Страж NT» не предусмотрено. В случае необходимости потребитель может оформить заказ через отдел продаж изготовителя на актуальный установочный комплект с

формуляром в печатном виде и/или копию извещения об изменении формуляра с указанием новых контрольных сумм файлов, входящих в состав установочного комплекта.

Обновление СЗИ «Страж NT» или компенсирующие меры, направленные на устранение уязвимости критического уровня опасности, необходимо применить незамедлительно после получения оповещения от изготовителя о возможности загрузки дистрибутива установочного комплекта (или организационно-технических мерах по нейтрализации выявленных уязвимостей). В остальных случаях сроки выполнения обновления СЗИ определяются эксплуатирующей организацией самостоятельно.

Для инсталляции сертифицированных обновлений, полученных с сайта изготовителя СЗИ, администратор информационной безопасности должен выполнить следующие действия:

- распаковать скачанный архив 40_setup.zip, содержащий:
  - файл образа диска с обновлённым комплектом (guardnt40.iso);
  - файл с информацией о комплекте (ReadMe.txt);
- выполнить прожиг образа диска guardnt40.iso на CD-R или CD-RW носитель, либо открыть его с помощью проводника Windows (доступно не во всех версиях ОС);
- провести расчёт контрольных сумм файлов, входящих в состав установочного комплекта, с использованием программы «ФИКС» версии 2.0.2 по алгоритму «Уровень – 1, программно»;
- провести верификацию СЗИ – сравнить контрольные суммы файлов обновлений с эталонными значениями, указанными в файле ReadMe.txt;
- при несовпадении контрольных сумм с эталонными значениями необходимо обратиться в службу поддержки производителя СЗИ «Страж NT».

Для установки обновления необходимо открыть в Проводнике Windows носитель с обновлённым комплектом системы защиты и запустить программу установки СЗИ – файл Setup.exe, расположенный в корневом каталоге носителя с обновлённым комплектом СЗИ. Программа установки проверит установленную версию СЗИ и сравнит её с версией обновлённого комплекта. В случае различия версий программа установки СЗИ предложит выполнить обновление системы защиты (см. Рис. 19).

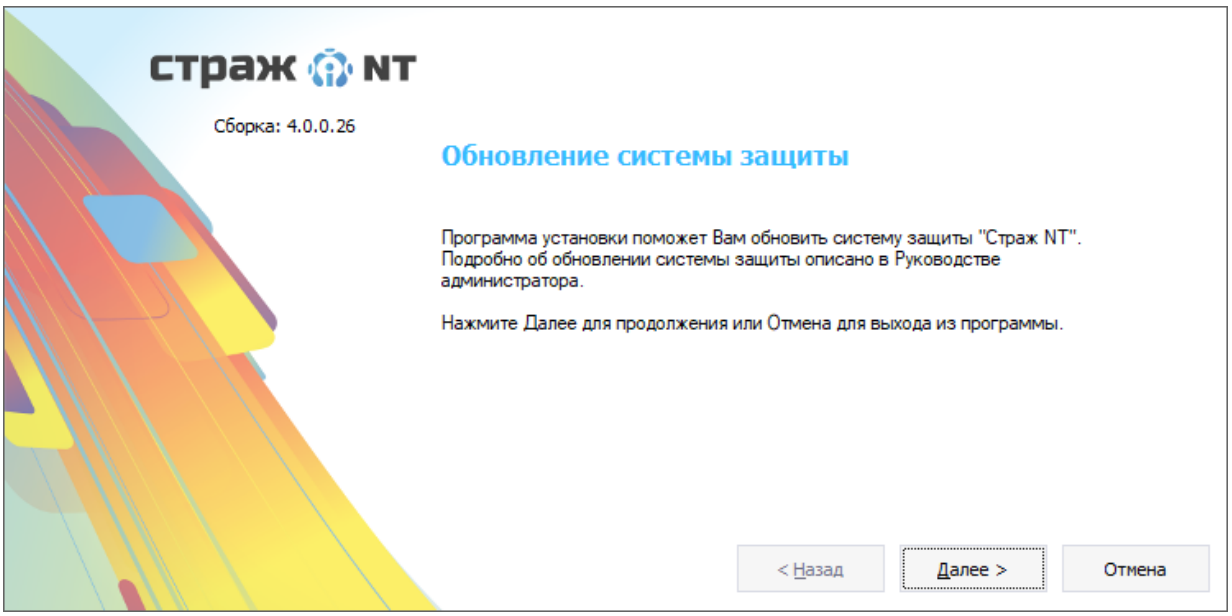


Рис. 19. Начальный диалог процедуры обновления СЗИ.

Для запуска процедуры обновления необходимо нажать кнопку Далее >. Для отказа от выполнения процедуры обновления следует нажать кнопку Отмена.

Для завершения процедуры обновления СЗИ необходимо выполнить перезагрузку компьютера (см. Рис. 20). Для этого необходимо выбрать поле **Да, перезагрузить компьютер сейчас** и нажать кнопку Готово.

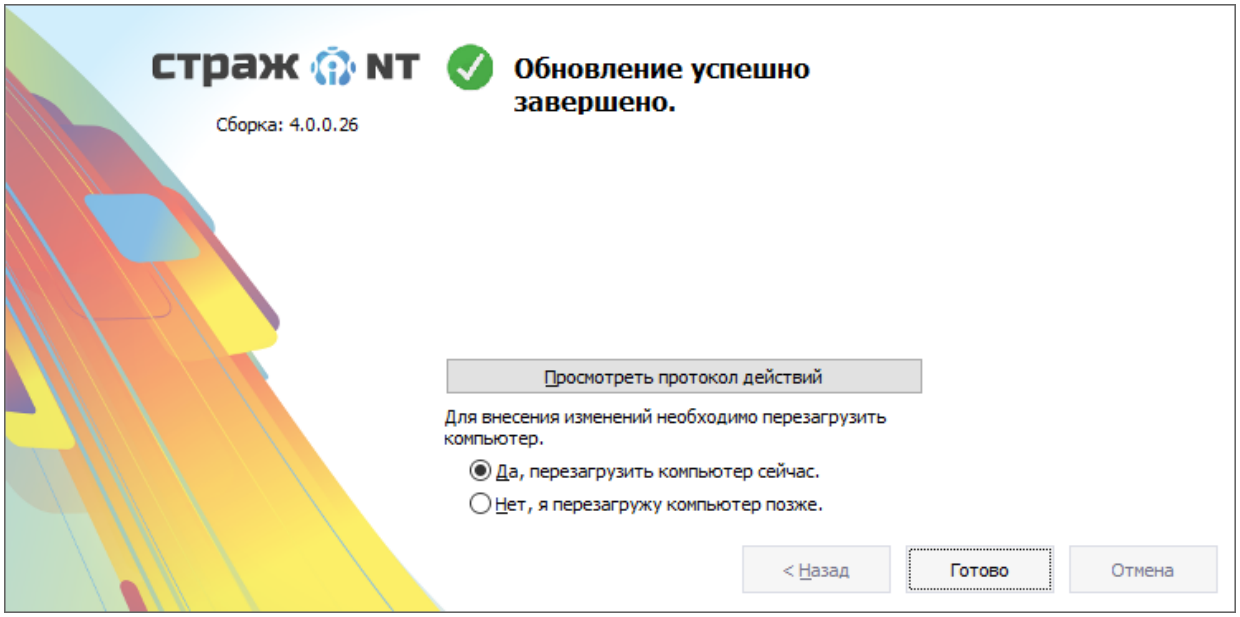


Рис. 20. Завершение процедуры обновления СЗИ.

Рекомендации при возникновении нештатных ситуаций

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

Ошибки при установке и удалении СЗИ

В процессе установки и удаления системы защиты ведется подробный протокол действий, выполняемых программой, который находится в папке временных файлов текущего пользователя **%Temp%** и называется **GInstall.log**.

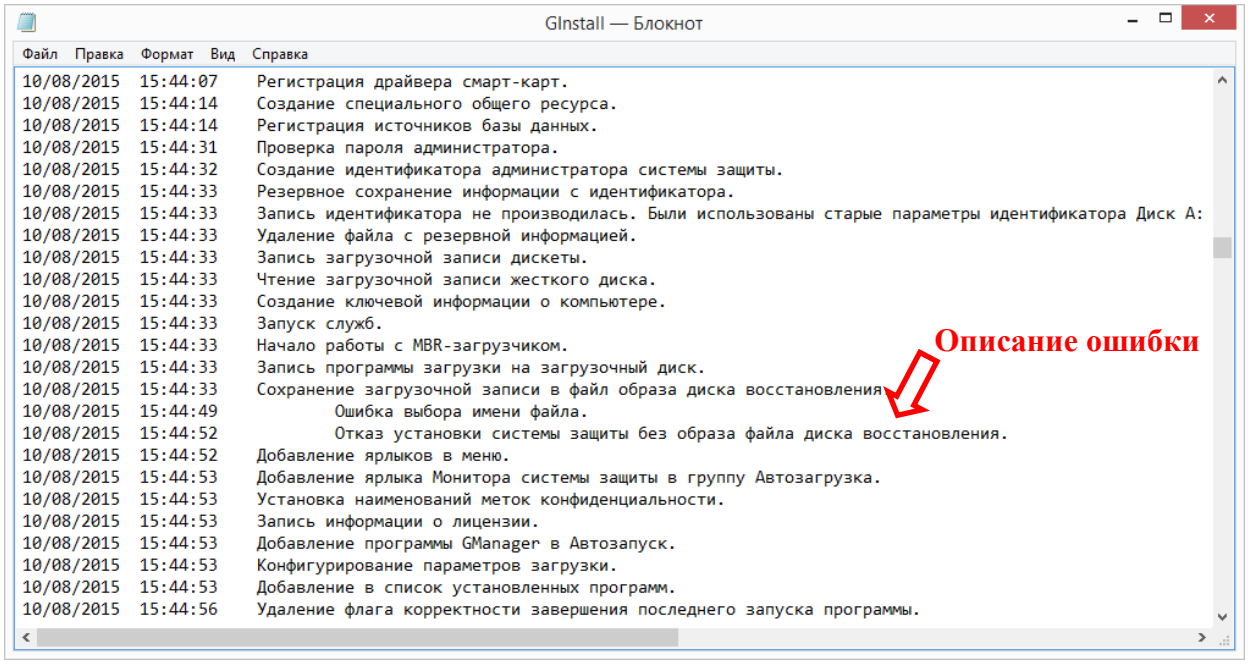


Рис. 21. Пример протокола действий.

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. 21.

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 или удаления системы защиты возможно возникновение нештатных 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 **Программу установки**, которая определит, что во время прошлого запуска произошел сбой, последовательно удалит все компоненты системы защиты и выдаст запрос на перезагрузку (см. Рис. 22). То же самое произойдет при сбое выполнения **Программы удаления**.

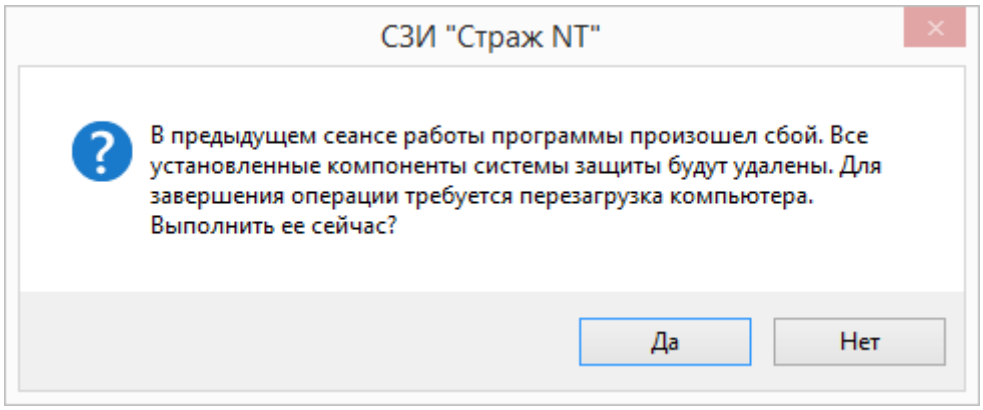


Рис. 22. Реакция на сбой при установке/удалении системы защиты.

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 **Программу установки**, которая обнаружит резервную информацию и предложит записать ее на идентификатор (см. Рис. 23).

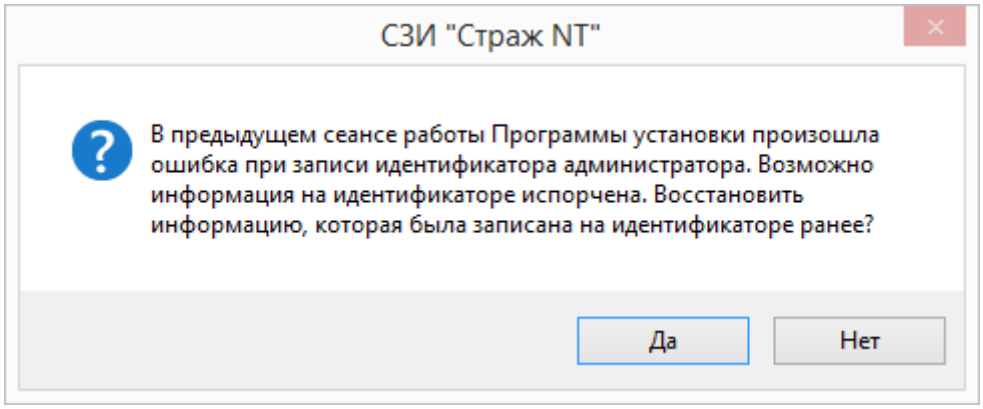


Рис. 23. Процедура восстановления персонального идентификатора.

Если же на предъявленном идентификаторе уже записана какая-то информация, **Программа установки** предупредит об этом. После этого программа предупредит об удалении всех компонентов системы защиты и выдаст запрос на перезагрузку (см. Рис. 22).

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. 24.

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

Рис. 24. Пример «синего экрана смерти».

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 дополнительных параметров системы, выбрать вкладку **Дополнительно** и нажать кнопку **Параметры…** в группе **Загрузка и восстановление** (см. Рис. 25).

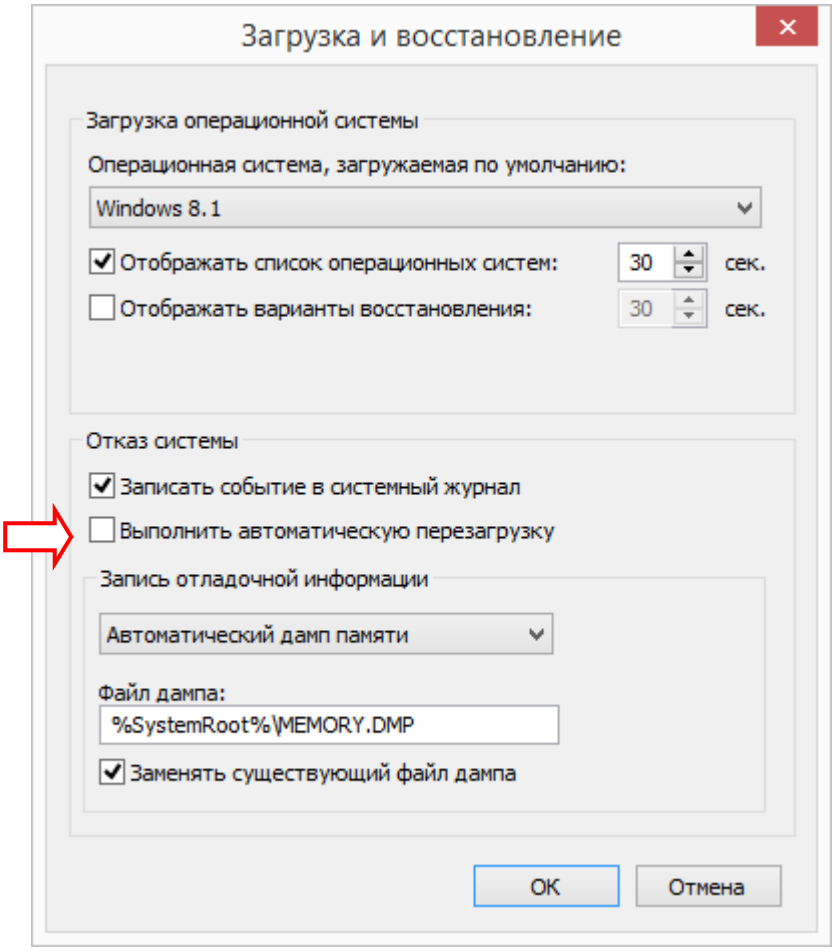


Рис. 25. Параметры загрузки и восстановления системы.

- Снять флаг в поле **Выполнить автоматическую перезагрузку** и сохранить выполненные изменения.
- Восстановить подсистему идентификации системы защиты и осуществить попытку загрузки операционной 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. Загрузка операционной системы после успешного выполнения действий по аварийному снятию системы защиты будет выполняться в обычном режиме без процедуры идентификации до загрузки операционной системы. Также при этом будет восстановлена логическая структура разделов системного жесткого диска.

При наличии персонального идентификатора и пароля администратора системы защиты

Для выполнения аварийного снятия системы защиты необходимо в BIOS Setup компьютера установить принудительную загрузку с носителя информации, на котором поставляется установочный комплект системы защиты.

Для корректного выполнения аварийного снятия СЗИ загружаться с носителя следует в том же режиме (UEFI или Legacy), в котором компьютер загружается с жёсткого диска.

После появления диалога, приведённого на Рис. 26, необходимо предъявить персональный идентификатор администратора системы защиты и ввести его пароль.

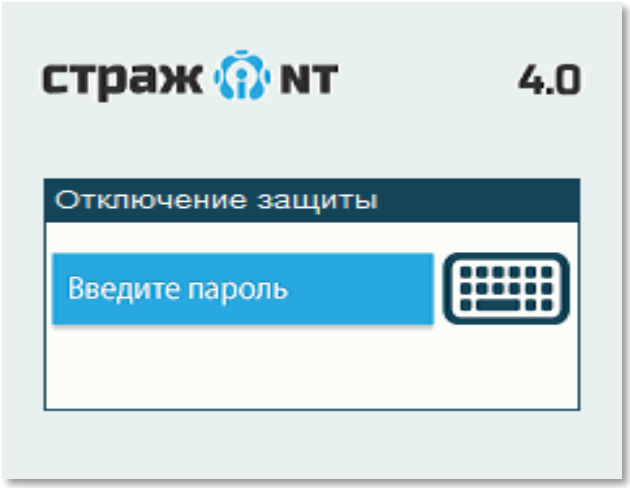


Рис. 26. Аварийное снятие системы защиты информации.

После появления сообщения об отключении системы защиты следует перезагрузить компьютер и в BIOS Setup компьютера восстановить порядок загрузки системы с жесткого диска. После загрузки операционной системы и выяснения причины отказа необходимо либо снять систему защиты штатным образом, как описано в разделе **Удаление системы защиты**, либо восстановить подсистему идентификации и работоспособность основных служб системы защиты, повторно загрузившись с носителя информации, на котором поставляется установочный комплект системы защиты и аналогично предъявив персональный идентификатор и пароль администратора системы защиты.

При отсутствии персонального идентификатора либо пароля администратора системы защиты

Если при установке системы защиты был сформирован образ загрузочного диска восстановления системы, восстановить доступ к системе можно, выполнив следующие действия:

- записать сохраненный образ загрузочного диска восстановления на CD-ROM;
- в BIOS Setup компьютера установить принудительную загрузку с CD-ROM;
- осуществить загрузку с CD-ROM;
- после появления сообщения о завершении работы механизмов аварийного снятия перезагрузить компьютер и в BIOS Setup компьютера восстановить порядок загрузки системы с жесткого диска.

После загрузки операционной системы необходимо снять систему защиты штатным образом, как описано в разделе **Удаление системы защиты**.

Для идентификации в операционной системе потребуется ввод имени и пароля администратора или другого пользователя системы защиты.

Вход в систему

В данной главе приводятся сведения о способах идентификации пользователей в системе, а также действия при возможных нештатных ситуациях.

Первоначальный вход в систему

Загрузка компьютера с установленной системой защиты информации начинается диалогом, представленным на Рис. 27.

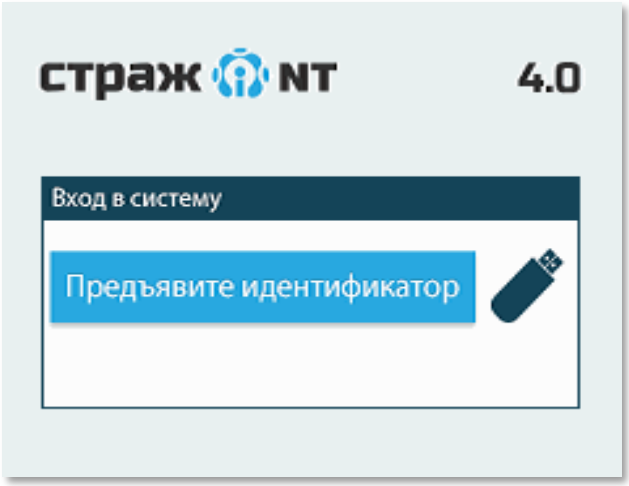


Рис. 27. Окно входа в систему.

Для входа в систему необходимо предъявить идентификатор пользователя СЗИ и после того, как система распознает идентификатор, ввести его пароль (см. Рис. 28).

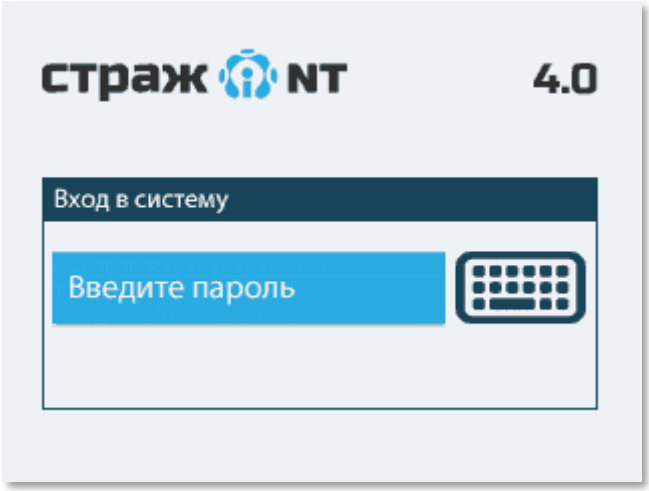


Рис. 28. Ввод пароля пользователя.

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. 29), 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.

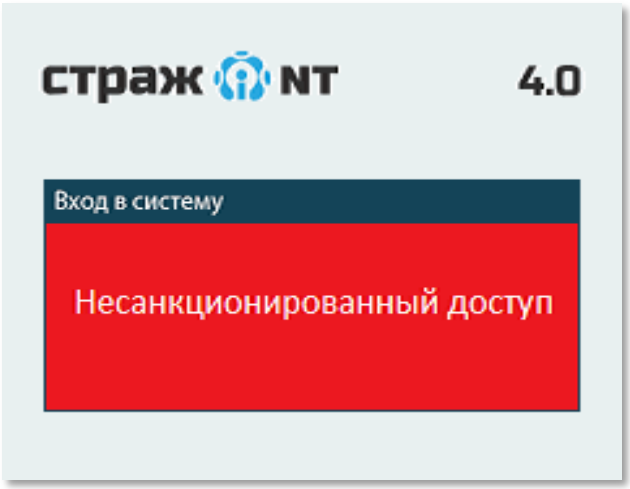


Рис. 29. Реакция на попытку несанкционированного доступа.

При вводе правильного пароля загрузка компьютера продолжается обычным образом. Идентификация пользователя в операционной системе осуществляется автоматически, используя информацию, записанную в памяти персонального идентификатора входящего пользователя, а также введенный пароль. После успешного входа в систему автоматически запускается программа **Монитор системы защиты**.

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.

Параметры повторной идентификации

Если при повторной идентификации 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 трижды произошла другая ошибка идентификации, на экране появляется сообщение о попытке несанкционированного доступа, сопровождаемое звуковой сигнализацией. Через 10 секунд, если включен параметр перезагрузки компьютера при ошибках идентификации, компьютер перезагрузиться. В противном случае запрос идентификатора и пароля повторится.

Чтобы включить параметр перезагрузки компьютера при ошибках идентификации пользователя необходимо запустить программу **Консоль управления** и в разделе **Политики паролей** вкладки **Настройки** установить флаг в поле **Перезагружать компьютер при ошибках идентификации** (см. Рис. 30).

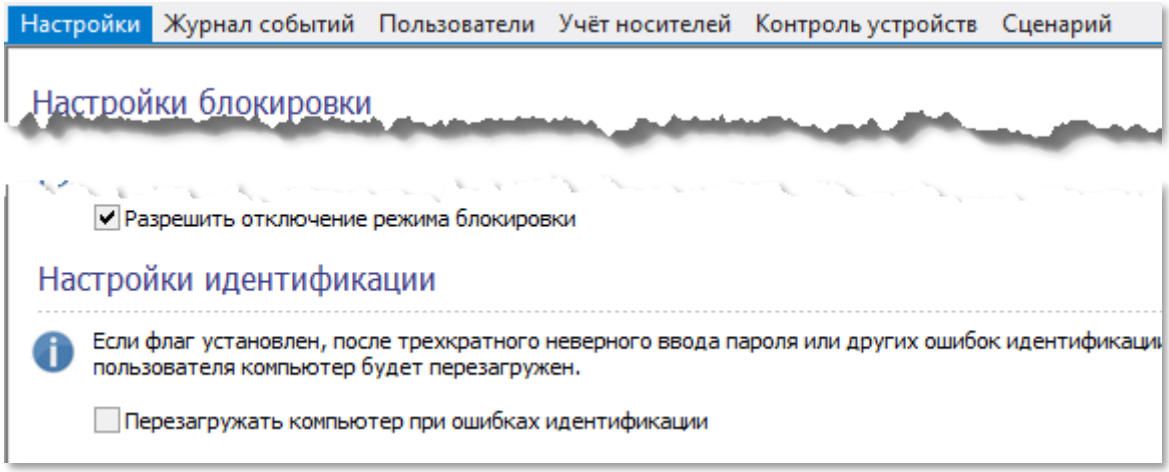


Рис. 30. Настройка параметра перезагрузки компьютера при ошибках идентификации.

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. При этом вход пользователю будет разрешен, если на

удаленном компьютере добавлены терминальные лицензии, и имя пользователя либо имя его компьютера (IP-адрес) внесены в разрешенный для подключения список.

Подробнее о терминальных лицензиях описано в разделе **Терминальный доступ**.

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 нештатных ситуаций**.

При включении компьютера сразу появляется надпись «Введите пароль:»	
Причина	Информация с персонального идентификатора уже была считана.
Действия	Следует либо продолжить вход в систему, т. е. ввести пароль, либо установить другой идентификатор и перезагрузить компьютер.
Надпись «Предъявите идентификатор…» не мигает или отсутствует на экране	
Причина	Одно из устройств, подключенных к USB-порту, не отвечает на запрос.
Действия	Необходимо либо выключить устройство, либо предъявлять идентификатор до появления запроса, показанного на Рис. 27.

Управление пользователями

В данной главе приводятся сведения о подсистеме управления пользователями. Описаны интерфейсы утилит администратора системы защиты при работе с подсистемой, а также его типовые действия при управлении пользователями и персональными идентификаторами.

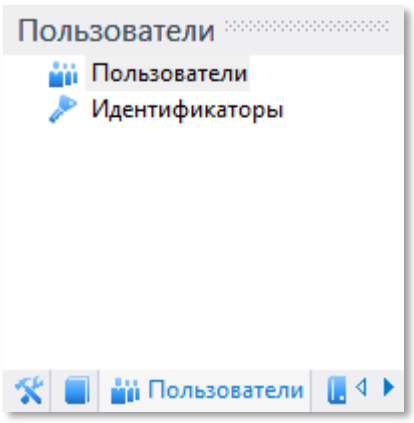
Общие сведения

Чтобы пользователь мог работать в системе, необходимо создать его учетную запись, назначить ей допуск (уровень конфиденциальности), пароль и сформировать для пользователя персональный идентификатор. Только предъявив персональный идентификатор и пароль, пользователь может войти в систему. При входе в Windows система защиты автоматически подставляет имя и домен пользователя, считанные с идентификатора, и его пароль, введенный до загрузки ОС. Полученная идентификационная информация сопоставляется с информацией, хранящейся в базе пользователей, и подсистема идентификации и аутентификации принимает решение о входе пользователя или отказе ему в доступе. При этом информация о пользователях автономных рабочих станций и рабочих станций в составе рабочей группы хранится в локальных базах SAM, тогда как информация о пользователях домена – в базе Active Directory на контроллерах домена. В составе идентификационной информации также присутствуют данные о компьютерах, на которые может входить пользователь.

Чтобы пользователь мог работать на нескольких компьютерах с одним персональным идентификатором и паролем необходимо, во-первых, на каждой рабочей станции или сервере, не входящих в домен, создать пользователей под одним и тем же именем и назначить им одинаковые пароли. Если компьютеры находятся в домене, необходимо просто создать пользователя в Active Directory. И во-вторых, необходимо сформировать идентификатор пользователя, в котором будет включена информация обо всех необходимых компьютерах.

Управление пользователями на рабочих станциях и серверах в составе рабочей группы, а также в составе домена может осуществляться с единого рабочего места администратора системы защиты, входящего в эту рабочую группу или домен.

Управление пользователями и персональными идентификаторами осуществляется с помощью вкладки **Пользователи** программы **Консоль управления**, перейдя в которую администратор системы защиты может выполнять следующие функции:



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

Панель пользователей содержит два пункта: **Пользователи** и **Идентификаторы**. Если выбран пункт **Пользователи**, в основной части окна будет отображён список пользователей выбранного компьютера или домена (если выбран контроллер домена) (см. Рис. 31), если выбран пункт **Идентификаторы** – список зарегистрированных в системе персональных идентификаторов (см. Рис. 44).

Настройки | Журнал событий | Пользователи | Учёт носителей | Контроль устройств | Сценарий

Имя	Полное имя	Описание	Допуск	Пароль	Идентификатор
Andrey			Несекретно	Не назначен	Не сформирован
Администратор		Встроенная учетная за...	Сов.секретно	********	Сформирован
Гость		Встроенная учетная за...	Несекретно	Не назначен	Не сформирован
Пользователь 1	Пользователь 1		Секретно	Не назначен	Не сформирован
Пользователь 2	Пользователь 2		Секретно	Не назначен	Не сформирован
Пользователь 3	Пользователь 3		Секретно	Не назначен	Не сформирован
Пользователь 4	Пользователь 4		Сов.секретно	Не назначен	Не сформирован
Пользователь 5	Пользователь 5		Секретно	Не назначен	Не сформирован
Пользователь 6	Пользователь 6		Сов.секретно	Не назначен	Не сформирован
Пользователь 7	Пользователь 7		Секретно	Не назначен	Не сформирован
Пользователь 8	Пользователь 8		Сов.секретно	Не назначен	Не сформирован
Пользователь 9	Пользователь 9		Секретно	Не назначен	Не сформирован

Рис. 31. Список пользователей.

Список пользователей представляет собой таблицу, содержащую нескольких полей.

Поле	Описание
Имя	Название учетной записи пользователя в системе.  *Имя пользователя не должно превышать 15 символов.*
Полное имя	Полное имя пользователя.
Описание	Дополнительная информация о пользователе.
Допуск	Допуск пользователя определяет максимальный гриф ресурса, доступный пользователю для чтения.
Пароль	Пароль пользователя и его текущее состояние. Звездочки в колонке **Пароль** означают, что значение пароля сохранено в базе системы защиты. Значение «Не назначен» означает, что пароль данного пользователя неизвестен системе защиты. Такому пользователю невозможно сформировать персональный идентификатор.  *Пароль пользователя не должен превышать 15 символов и может содержать символы только латинского алфавита, цифры, а также специальные символы.*
Идентификатор	Текущее состояние персонального идентификатора пользователя. Значение «Не сформирован» 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 или допуск.

Администратор системы защиты имеет возможность сортировать список пользователей по любому из полей. Неактивные учетные записи отображаются серым цветом.

Пароли пользователей в списке отображаются в виде звёздочек. Для просмотра паролей в явном виде необходимо выбрать пункт меню ***Пользователи | Показать пароль****. Для возврата к режиму отображения паролей в виде звёздочек, необходимо ещё раз выбрать пункт меню* ***Пользователи | Показать пароль.***

Фильтрация и поиск пользователей

Для удобства просмотра списка пользователей реализован механизм фильтрации и поиска пользователей. Для фильтрации пользователей необходимо выбрать пункт меню **Пользователи | Фильтр…** (см. Рис. 32). Фильтрация пользователей возможна по следующим параметрам:

- уровень допуска;
- роль пользователя;
- состояние идентификатора.

При нажатии кнопки Применить в списке пользователей будут отображены только те пользователи, которые удовлетворяют введенному фильтру. Для возврата к отображению всех пользователей необходимо выбрать пункт меню **Пользователи | Все пользователи**.

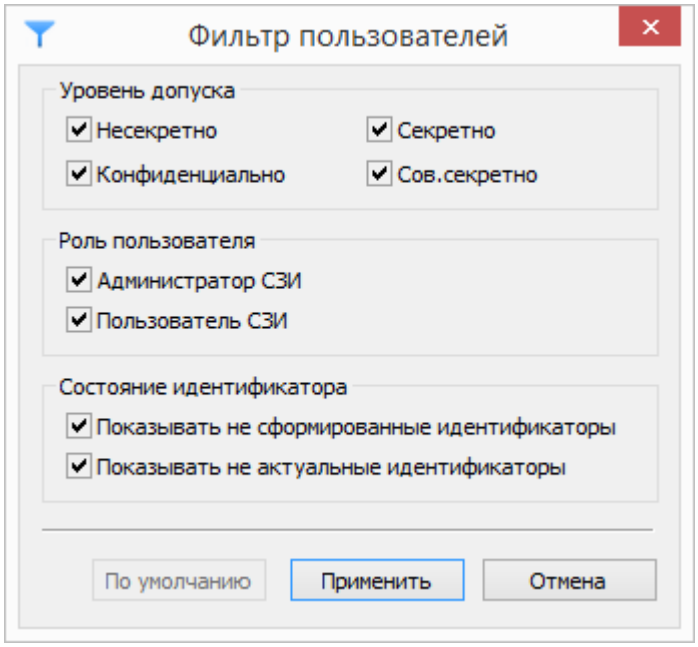


Рис. 32. Фильтр пользователей.

Для вызова окна поиска пользователей необходимо выбрать пункт меню **Пользователи | Поиск…** (см. Рис. 33). Поиск пользователей возможен по следующим параметрам:

- имя пользователя;
- уровень допуска;
- роль пользователя;
- состояние идентификатора.

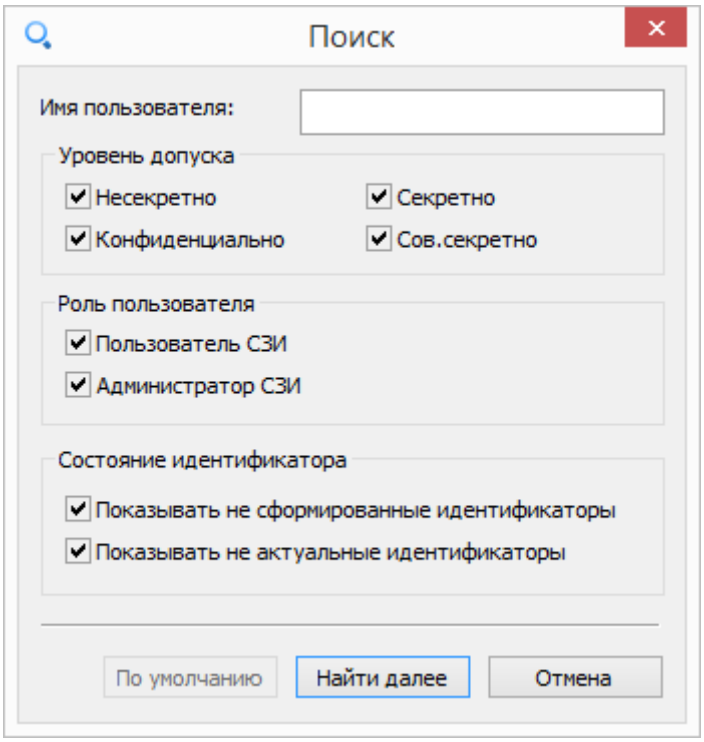


Рис. 33. Поиск пользователей.

При нажатии кнопки Найти далее будет выбран первый пользователь, удовлетворяющий введенным критериям поиска, нижерасположенный по списку от выбранного в настоящий момент.

Создание пользователя

Для создания нового пользователя необходимо выбрать пункт меню **Пользователи** | **Создать пользователя…** или нажать соответствующую кнопку на панели инструментов. В открывшемся окне (см. Рис. 34) администратор системы защиты может задать следующие параметры:

- имя пользователя;
- полное имя пользователя;
- описание;
- флаг создания профиля пользователя;
- расположение пользователя в Active Directory (при наличии домена);

- допуск (уровень конфиденциальности) пользователя;
- признак администратора системы защиты;
- пароль пользователя;
- флаг запрета смены пароля пользователем;
- флаг обязательной смены пароля пользователя при следующем входе.

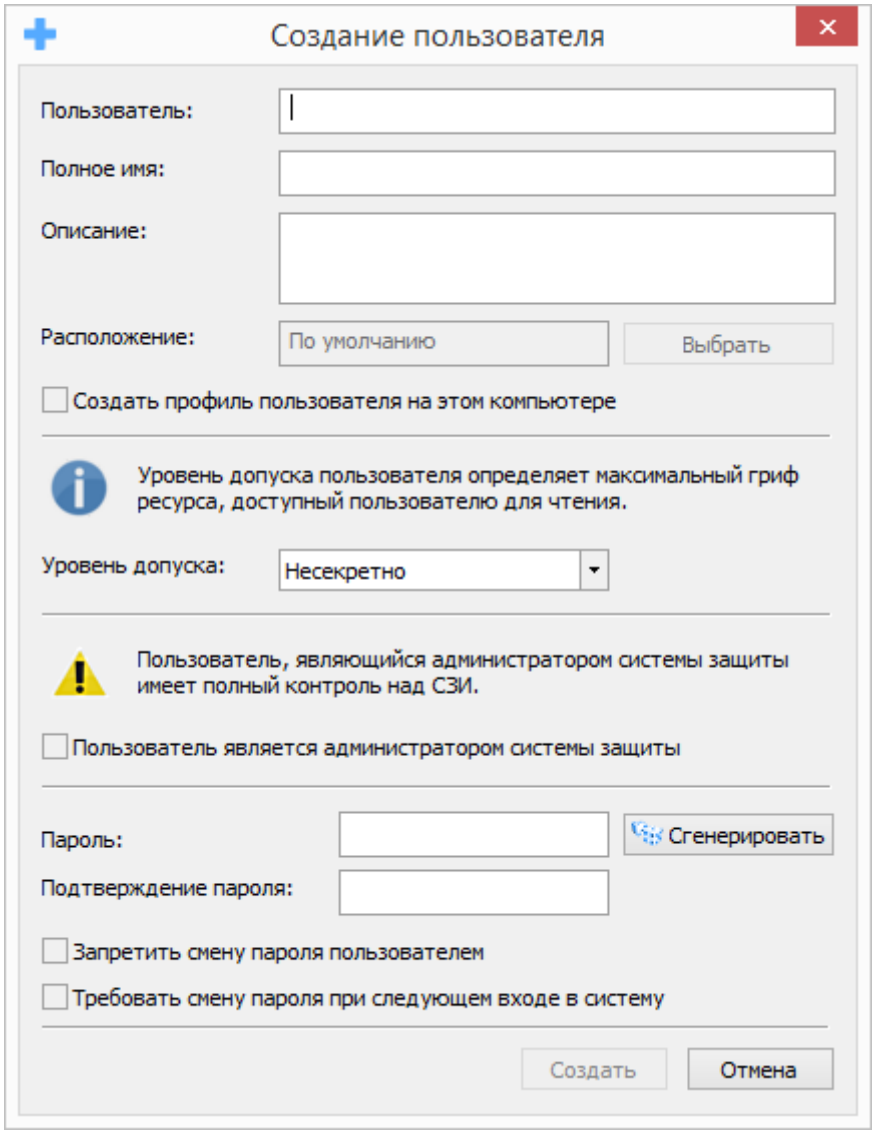


Рис. 34. Создание пользователя.

Флаг **Требовать смену пароля при следующем входе в систему** определяет, требуется ли принудительная смена пароля пользователем при следующем входе в систему.

Флаг **Запретить смену пароля пользователем**" определяет, запрещена ли смена назначенного пароля пользователем. Данный параметр не распространяется на членов группы **Администраторы**.

Для автоматической генерации пароля необходимо нажать кнопку Сгенерировать. При этом будет сгенерирован пароль, удовлетворяющий требованиям, заданным в настройках генерации паролей (см. раздел **Политика генерации паролей**). После нажатия кнопки OK пользователь будет создан и на экране появится соответствующее сообщение.

В случае успешного создания пользователя будет предложено создать его персональный идентификатор (см. раздел **Формирование идентификаторов**).

Редактирование свойств пользователя

Для просмотра и редактирования свойств пользователя необходимо выбрать пункт меню **Пользователи | Свойства пользователя…** или нажать соответствующую кнопку на панели инструментов. Окно редактирования свойств состоит из трёх вкладок: **Общие**, **Безопасность** и **Идентификаторы**.

С помощью вкладки **Общие** (см. Рис. 35) можно переименовать пользователя, создать профиль, а также изменить полное имя и описание пользователя.

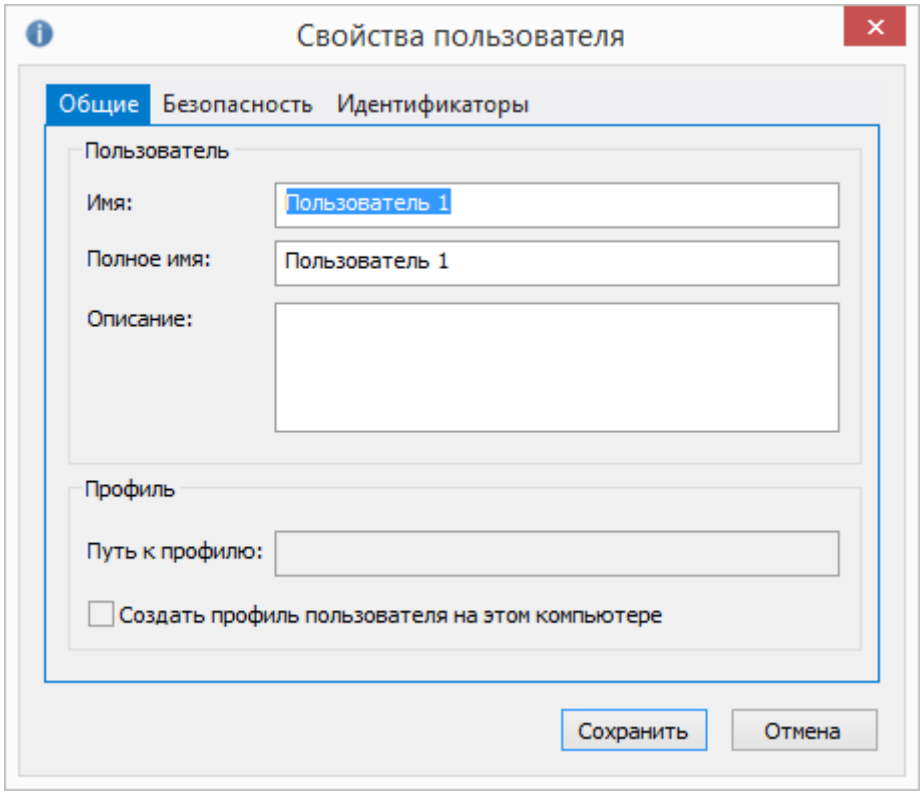


*Рис. 35. Редактирование свойств пользователя - вкладка **Общие**.*

На вкладке **Безопасность** (см. Рис. 36) отображена и доступна для редактирования информация о допуске пользователя, признаке администратора системы защиты и пароле.

Флаг в поле **Пользователь является администратором системы защиты** определяет признак того, что пользователь является администратором системы защиты.

*Для пользователей, пароль которых неизвестен системе защиты, флаг **Создать профиль пользователя на этом компьютере** будет заблокирован*

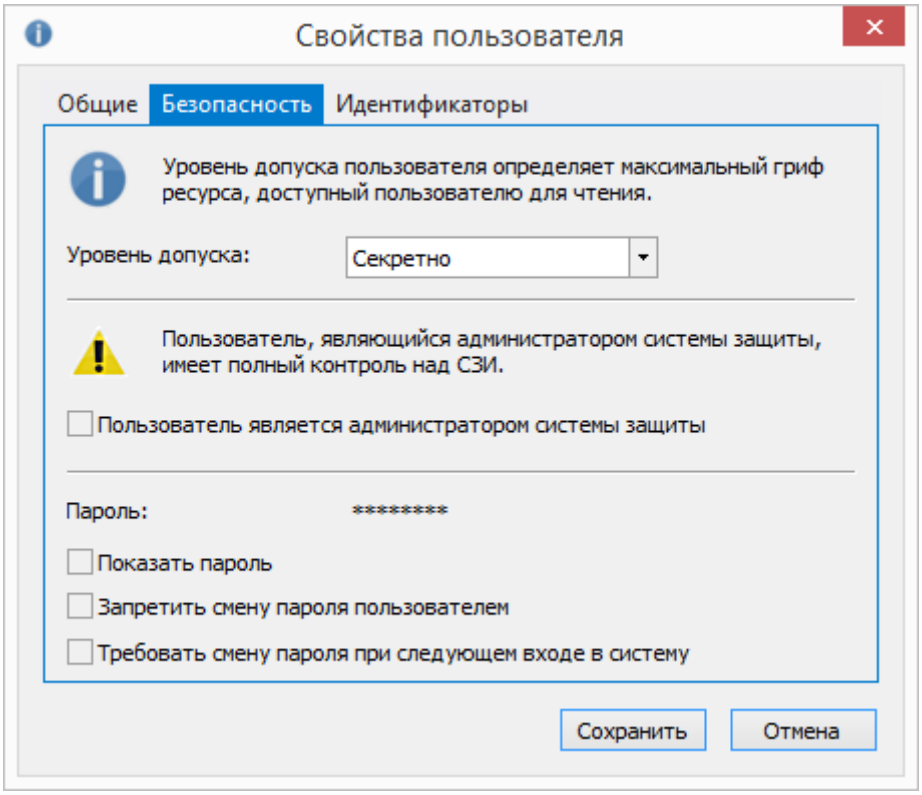


*Рис. 36. Редактирование свойств пользователя - вкладка **Безопасность**.*

Вкладка **Идентификаторы** (см. Рис. 37) служит для управления списком персональных идентификаторов выбранного пользователя.

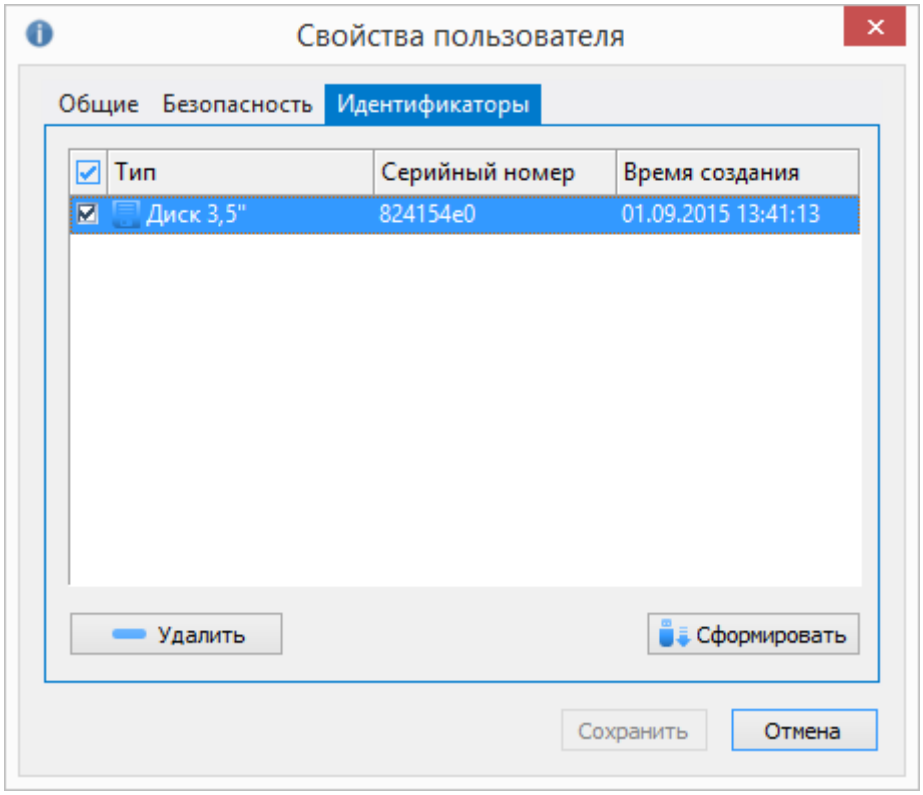


*Рис. 37. Редактирование свойств пользователя - вкладка **Идентификаторы**.*

Список идентификаторов содержит информацию о типе, серийном номере и дате формирования идентификатора. Администратор системы защиты может удалить идентификатор из списка, а также сформировать новый. Для удаления идентификатора его необходимо отметить и нажать кнопку Удалить. Для формирования идентификатора, необходимо нажать кнопку Сформировать.

После изменения уровня допуска или признака администратора системы защиты пользователя ему необходимо переформировать персональный идентификатор.

Удаление пользователя

Для удаления пользователя из списка необходимо выбрать его в списке и выбрать пункт меню **Пользователи | Удалить пользователя** или нажать соответствующую кнопку на панели инструментов. При удалении пользователя, на экран будет выдано предупреждение с указанием имени удаляемого пользователя (см Рис. 38). В случае положительного ответа, пользователь будет удален из базы пользователей, также будет удален список его персональных идентификаторов.

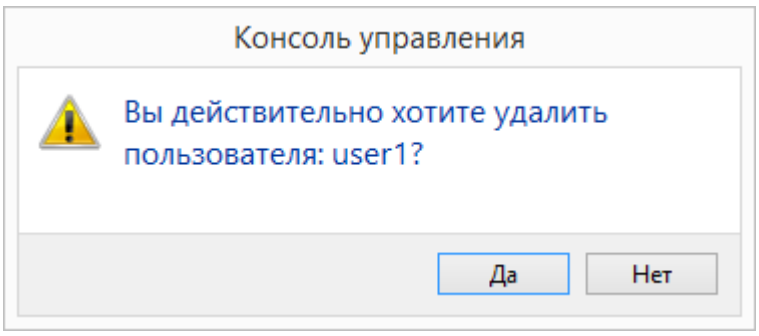


Рис. 38. Удаление пользователя.

Смена пароля пользователя

Для смены пароля пользователя необходимо выбрать пользователя в списке и выбрать пункт меню **Пользователи | Изменить пароль...** . При это на экране появится диалог, как показано на Рис. 39.

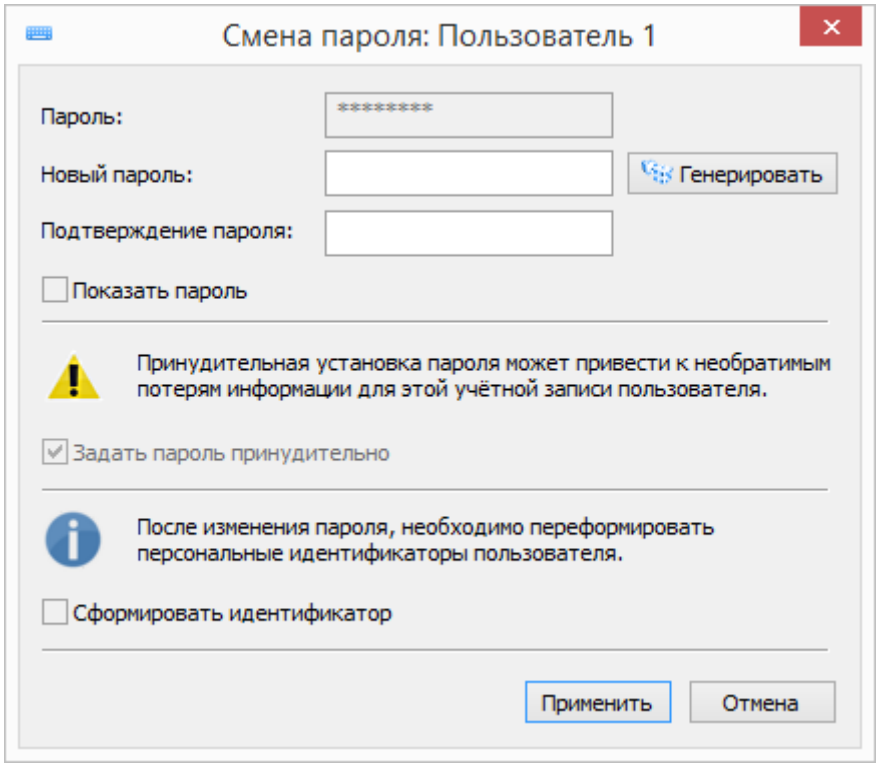
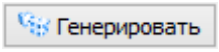


Рис. 39. Смена пароля пользователя.

Если значение текущего пароля сохранено в базе пользователей системы защиты, поле **Пароль** будет автоматически заполнено. В противном случае для корректной смены пароля пользователя необходимо ввести в указанное поле значение текущего пароля. В поле **Новый пароль** необходимо ввести значение нового пароля, а в поле **Подтверждение 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 

. При этом в оба поля будет автоматически введен случайный пароль, удовлетворяющий требованиям, заданным для генерации паролей. Если значение старого пароля пользователя неизвестно, можно принудительно назначить ему новый пароль, установив флаг в поле **Задать пароль принудительно**. Если выбранному пользователю запрещена смена пароля, флаг в поле **Задать пароль принудительно** будет установлен автоматически.

После смены пароля пользователя ему необходимо переформировать персональный идентификатор.

Печать карточки пользователя

В целях доведения пользователям паролей предусмотрена печать карточки пользователя. Для печати карточки пользователя необходимо выбрать пользователя в списке и выбрать пункт меню **Пользователи | Печать карточки…**. При этом откроется стандартное окно выбора принтера, на который будет осуществляться печать карточки.

Карточка пользователя содержит информацию об имени пользователя, его допуске, пароле и статусе его персонального идентификатора.

Политика генерации паролей

Генерация паролей пользователей выполняется в соответствии с настройками генерации паролей, которые задаются в разделе **Политики паролей** вкладки **Настройки** (см. Рис. 40). Длина пароля может варьироваться от 3 до 15 символов. В алфавит пароля могут быть включены цифры, заглавные и строчные символы латинского алфавита.

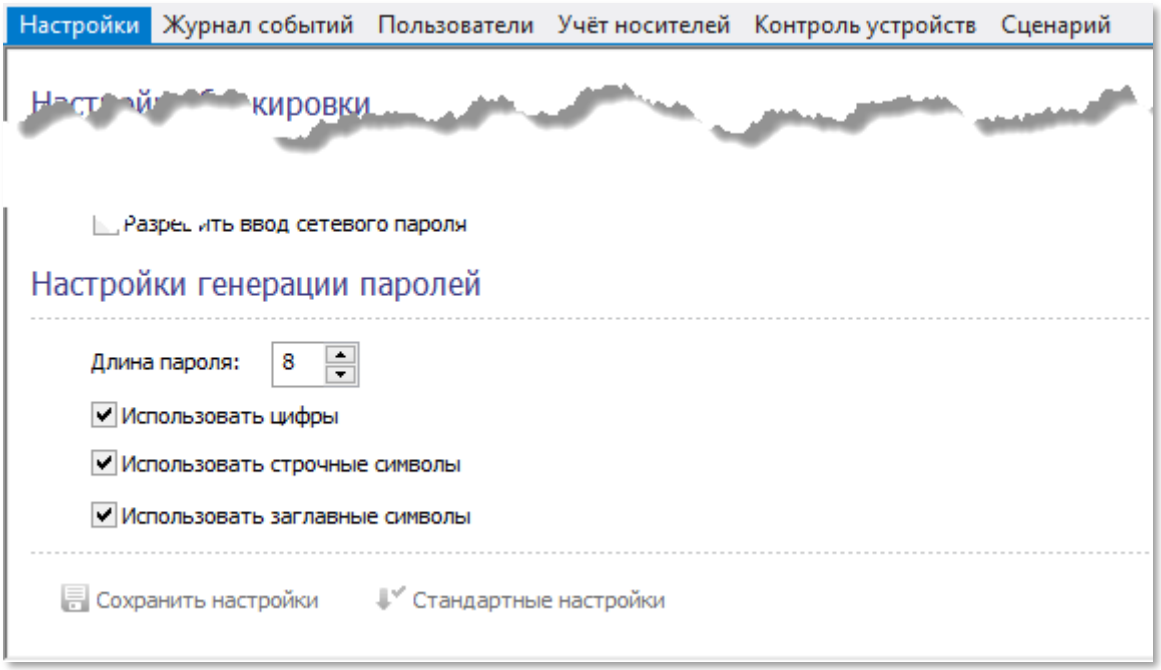


Рис. 40. Настройки генерации паролей.

Формирование идентификаторов

Для формирования идентификаторов необходимо выбрать пункт меню **Идентификатор | Сформировать идентификатор…**, или нажать соответствующую кнопку на панели инструментов.

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. 41.

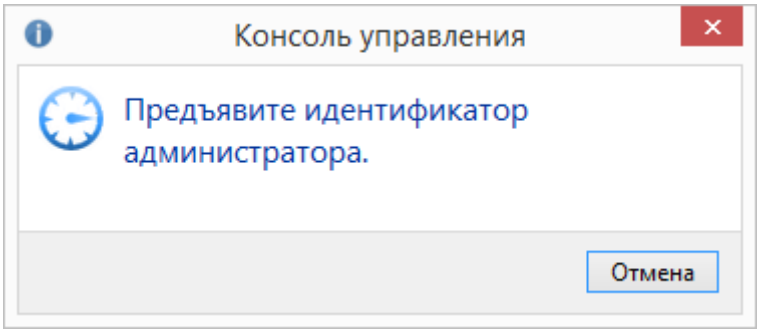


Рис. 41. Предъявление идентификатора администратора системы защиты.

Персональный идентификатор администратора системы защиты предъявляется только один раз за сеанс работы программы. После считывания предъявленного идентификатора на экране появляется диалог формирования идентификатора пользователя (см. Рис. 42).

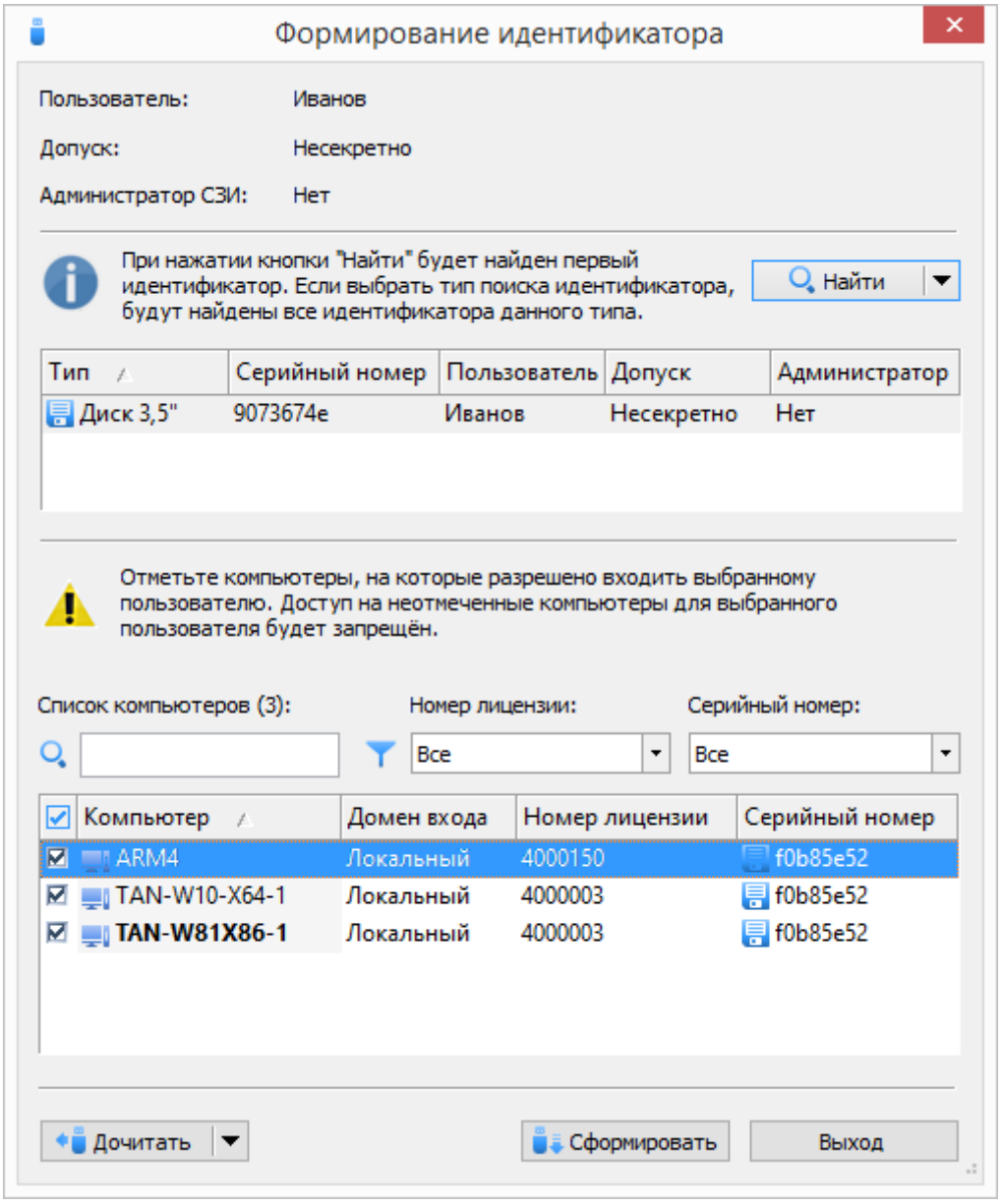


Рис. 42. Формирование идентификатора.

Окно формирования идентификаторов содержит информацию об имени пользователя, его допуске, признаке администратора системы защиты, а также списки доступных идентификаторов и компьютеров.

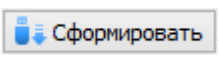
Для формирования идентификатора, его сначала необходимо найти в системе. Для поиска идентификаторов необходимо нажать кнопку Найти. Кнопка Найти поддерживает выпадающий список типов идентификаторов. Если просто нажать кнопку Найти, будет найден первый идентификатор, если же выбрать тип

идентификатора – будут найдены все идентификаторы указанного типа. В списке идентификаторов представлена информация о типе, серийном номере, пользователе, допуске и признаке администратора. Список компьютеров содержит имена компьютеров и доменов входа, которые были считаны с персонального идентификатора администратора системы защиты. При необходимости можно заменить домен входа, нажав левой клавишей мыши на поле **Домен** в списке компьютеров.

Существует возможность прочитать список доступных компьютеров с нескольких зарегистрированных идентификаторов администратора. Для этого необходимо предъявить дополнительный идентификатор администратора и нажать кнопку **Дочитать**. При успешном чтении в список доступных компьютеров будут добавлены компьютеры с дополнительного идентификатора администратора. Если на идентификаторах содержаться записи компьютеров с одинаковыми именами, конфликтные записи будут отмечены красным цветом. Для сброса списка прочитанных со всех предъявленных идентификаторов администратора компьютеров без перезапуска программы **Консоль управления** следует выбрать пункт меню **Идентификатор | Сбросить идентификаторы администратора**.

Перед формированием персонального идентификатора пользователя необходимо отметить компьютеры, вход на которые будет ему разрешен. Чтобы выбрать все компьютеры необходимо нажать кнопку  .

Список отмеченных компьютеров сохраняется на сеанс работы программы «Консоль управления». Если формируемый идентификатор был корректно прочитан, и на нём уже присутствует информация о некоторых компьютерах, то их имена будут отмечены в списке компьютеров, считанном с персонального идентификатора администратора системы защиты. Список компьютеров, считанный с формируемого идентификатора, имеет более высокий приоритет, чем список, сохранённый при формировании предыдущего идентификатора в текущем сеансе работы программы «Консоль управления».

Для начала процедуры формирования персонального идентификатора необходимо нажать кнопку 

.

Чтение идентификаторов

Для чтения идентификаторов необходимо выбрать пункт меню **Идентификатор | Считать идентификатор…**. Окно чтения идентификаторов (см. Рис. 43) содержит два списка: **Список идентификаторов** и **Список компьютеров**.

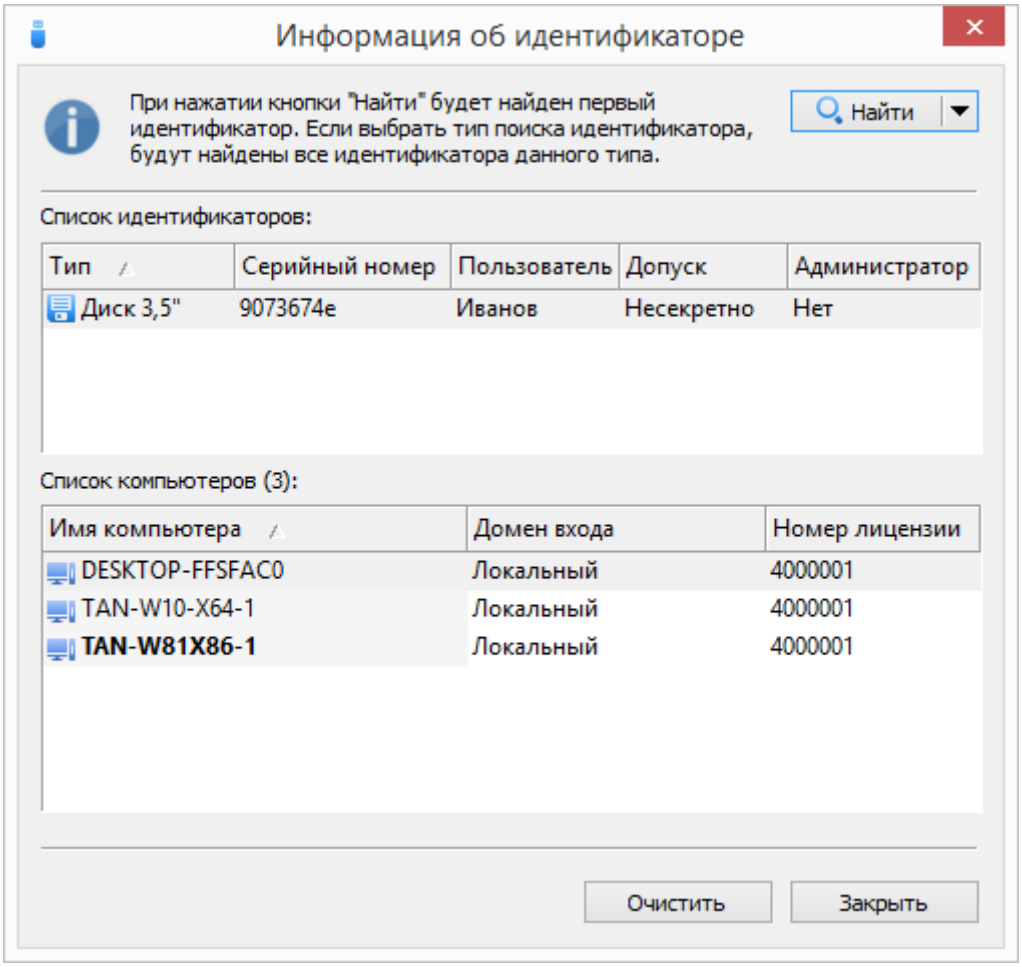
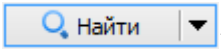
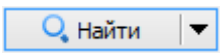
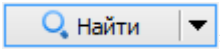
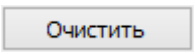


Рис. 43. Информация об идентификаторе.

Для поиска идентификаторов необходимо нажать кнопку 

. Кнопка 

поддерживает выпадающий список типов идентификаторов. Если просто нажать кнопку 

, будет найден первый идентификатор, если выбрать тип идентификатора – будут найдены все идентификаторы указного типа. В списке идентификаторов представлена информация о типе, серийном номере, пользователе, допуске и признаке администратора. В списке компьютеров, содержится информация об имени компьютера и домене входа. Для очистки идентификатора, необходимо выбрать запись в списке идентификаторов и нажать кнопку 

.

Отображение списка идентификаторов

Для отображения списка сформированных идентификаторов всех пользователей, необходимо выбрать пункт **Идентификаторы** на панели пользователей. После этого в основной части окна появится список идентификаторов. Список идентификаторов представляет собой таблицу, содержащую нескольких полей (см. Рис. 44).

Свойство	Описание
Тип	Определяет тип идентификатора.
Номер	Определяет серийный номер идентификатора.
Имя пользователя	Определяет название учетной записи пользователя, которому принадлежит идентификатор.
Дата формирования	Определяет дату и время формирования идентификатора.
Статус	Определяет текущее состояние персонального идентификатора пользователя. Значение «Не актуален» означает, что после формирования персонального идентификатора у пользователя был изменен пароль, допуск или статус администратора СЗИ.

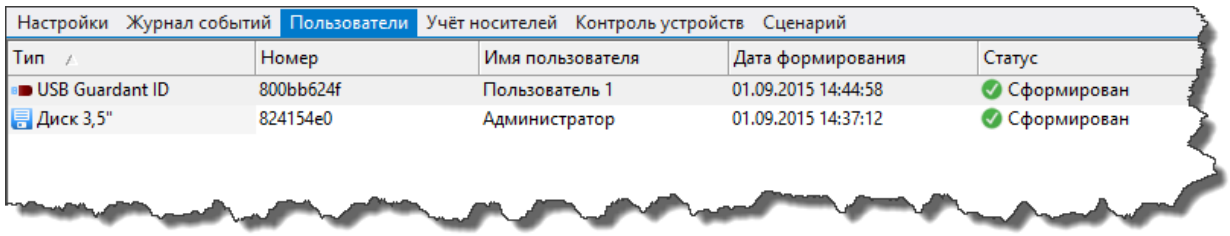


Рис. 44. Список идентификаторов.

Администратор системы защиты имеет возможность сортировать список идентификаторов по любому из перечисленных полей.

Фильтрация и поиск идентификаторов

Для удобства просмотра списка идентификаторов реализован механизм фильтрации и поиска идентификаторов. Для фильтрации идентификаторов необходимо выбрать пункт

меню **Идентификаторы | Фильтр…**. При этом на экране появится окно, пример которого показан на Рис. 45.

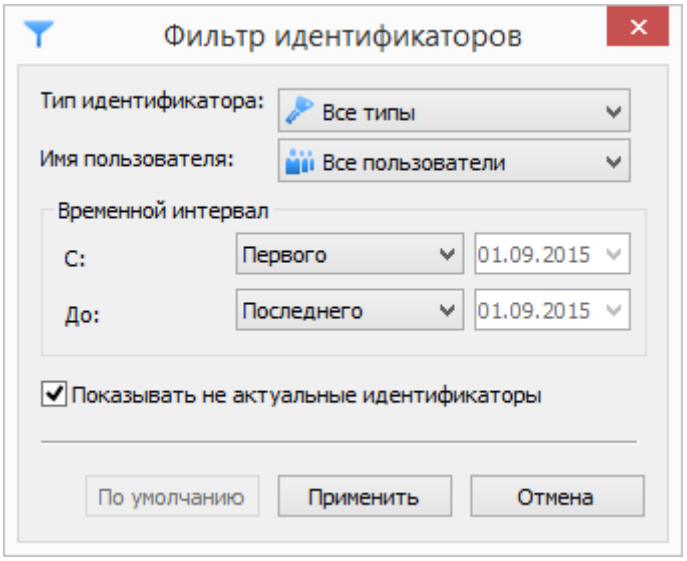


Рис. 45. Фильтр идентификаторов.

Фильтрация идентификаторов возможна по следующим параметрам:

- тип идентификатора;
- имя пользователя;
- временной интервал формирования идентификаторов.
- флаг фильтрации не актуальных идентификаторов.

При нажатии кнопки Применить в списке пользователей будут отображены только те идентификаторы, которые удовлетворяют введенному фильтру. Для возврата к отображению всех идентификаторов необходимо выбрать пункт меню **Идентификаторы | Все идентификаторы**.

Для вызова окна поиска идентификаторов необходимо выбрать пункт меню **Идентификаторы | Поиск…**. При этом на экране появится окно, пример которого показан на Рис. 46.

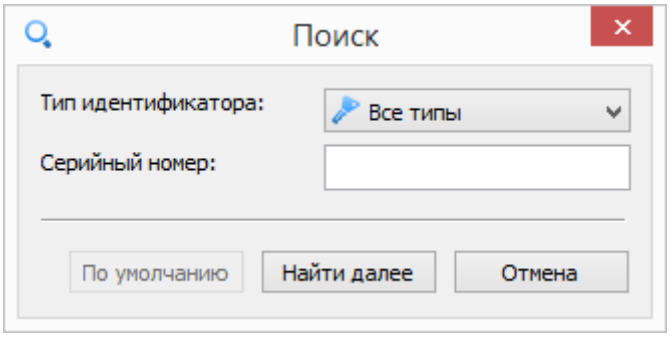


Рис. 46. Поиск идентификаторов.

Поиск идентификаторов возможен по следующим атрибутам:

- тип идентификатора;
- серийный номер.

При нажатии кнопки Найти далее будет выбран первый идентификатор, удовлетворяющий введенным критериям поиска, нижерасположенный по списку от выбранного в настоящий момент.

Замкнутая программная среда

В данной главе даются сведения о замкнутой программной среде и методах ее настройки. Описываются сценарии выполнения администраторами системы защиты сервисных функций, связанных с изменением программной среды.

Общие сведения

В целях обеспечения безопасности при работе пользователей в СЗИ «Страж NT» реализован механизм замкнутой программной среды. Данный механизм заключается в том, что каждый исполняемый файл системы, необходимый для работы пользователя, должен иметь разрешение на запуск. Для этого служит защитный атрибут – режим запуска, который может иметь следующие значения:

- «Запрещен» (по умолчанию);
- «Приложение»;
- «Сервер-приложение»;
- «Инсталлятор».

Пользователь может запустить программу, хранящуюся в файле, на выполнение, если для данного файла значение режима запуска отличается от значения «Запрещен». Если режим запуска файла имеет значение «Запрещен», запрос на выполнение не будет выполнен. Изменение режима запуска файла может дать только администратор системы защиты. Таким образом, для пользователей формируется замкнутая программная среда, при которой пользователь не может запустить программу, для которой не разрешен режим запуска. Различие замкнутых программных сред для разных пользователей осуществляется дискреционным принципом контроля доступа.

Все файлы, для которых значение режима запуска отличается от значения «Запрещен», доступны пользователям только на чтение, что обеспечивает целостность программной среды.

Режим запуска «Приложение» разрешает запуск программы, хранящейся в файле, для всех пользователей.

Режим запуска исполняемых файлов «Инсталлятор» предназначен для поддержки программы **Microsoft Installer**, а также некоторых приложений, защищенных специальным образом от несанкционированного использования. Данный режим запуска позволяет программе **Microsoft Installer** обходить требования замкнутой программной

среды. Для настройки данной программы необходимо установить режим запуска исполняемых файлов «Инсталлятор» на файл **%SystemRoot%\Windows\system32\msiexec.exe**, а также на все файлы с расширениями **msi** и **msp**, расположенные в папке **%SystemRoot%\Installer**. На указанные файлы автоматически устанавливаются соответствующие режимы запуска после установки системы защиты. Режим запуска «Инсталлятор» позволяет также обеспечить работоспособность некоторых приложений, защищенных от несанкционированного использования. Такие приложения в процессе своей работы создают временные файлы, которые пытаются загрузить и выполнить как отдельные процессы или динамически загружаемые библиотеки. При создании таких новых файлов системой защиты на них устанавливается режим запуска «Запрещен». В этом случае пользователю, не являющемуся администратором системы защиты, запуск таких файлов в качестве исполняемых модулей будет запрещен, соответственно приложения будут работать некорректно или не смогут запускаться совсем. Чтобы обойти такое ограничение и обеспечить работоспособность защищенных приложений, необходимо на файл, являющийся приложением, установить режим запуска «Инсталлятор». В этом случае такое приложение сможет загружать и выполнять динамически загружаемые библиотеки и программы, даже если соответствующие файлы не разрешены на запуск. При этом на запуск процессов действует ограничение – приложение с режимом запуска «Инсталлятор» может запускать не более двух процессов, не разрешенных на запуск. Для отключения данного ограничения необходимо во вкладке **Настройки** программы **Консоль управления** при выборе группы настроек **Общие настройки** снять флаг в поле **Ограничивать режим запуска «Инсталлятор»** и нажать кнопку **Сохранить настройки** (см. Рис. 47).

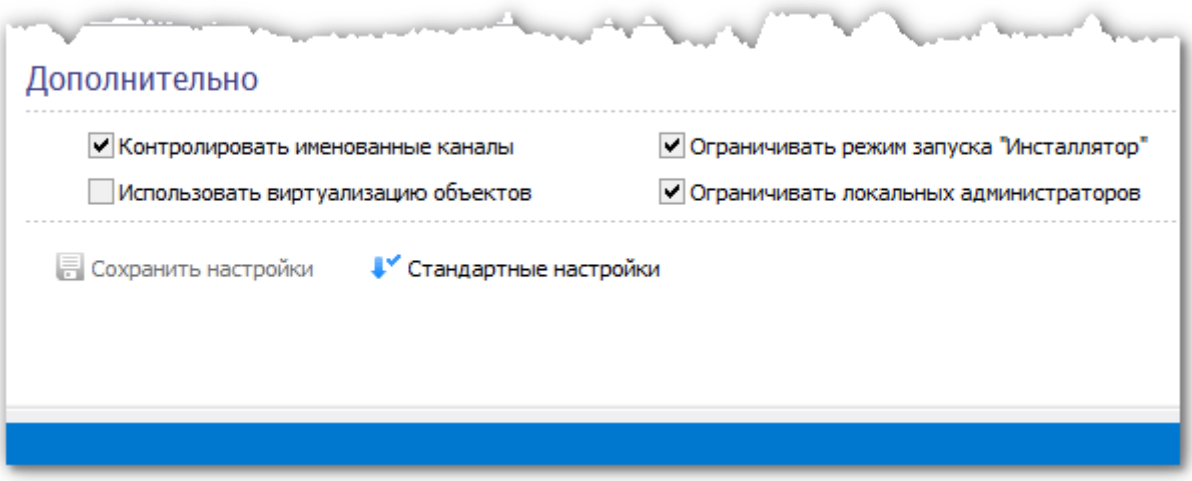


Рис. 47. Дополнительные параметры.

После отключения данного ограничения приложение с режимом запуска «Инсталлятор» сможет запускать неограниченное количество процессов, не имеющих разрешения на запуск.

Назначение режима запуска исполняемых файлов «Сервер-приложение» будет подробно описано в разделе **Мандатный принцип контроля доступа**.

В СЗИ «Страж NT» в среде 32-х разрядных операционных систем предусматривается возможность контроля запуска и изменения текущего допуска приложений MS-DOS. С этой целью на программу **%SystemRoot%\System32\ntvdm.exe** устанавливается режим запуска «Приложение». После этого на все необходимые для работы пользователей программы MS-DOS необходимо установить режим запуска «Приложение».

Включение и отключение ЗПС

В СЗИ «Страж NT» механизмы замкнутой программной среды могут быть отключены. При отключении механизмов ЗПС пользователи, в том числе и учетная запись **Система,** могут беспрепятственно запускать на выполнение любые программы. При этом события запуска программ так же заносятся в журнал событий.

Для отключения механизмов замкнутой программной среды необходимо вызвать контекстное меню программы **Монитор системы защиты**, иконка которого находится в системном лотке панели задач, и выбрать пункт меню **Отключение ЗПС**. При появлении окна как на Рис. 48 необходимо нажать кнопку **Отключить.**

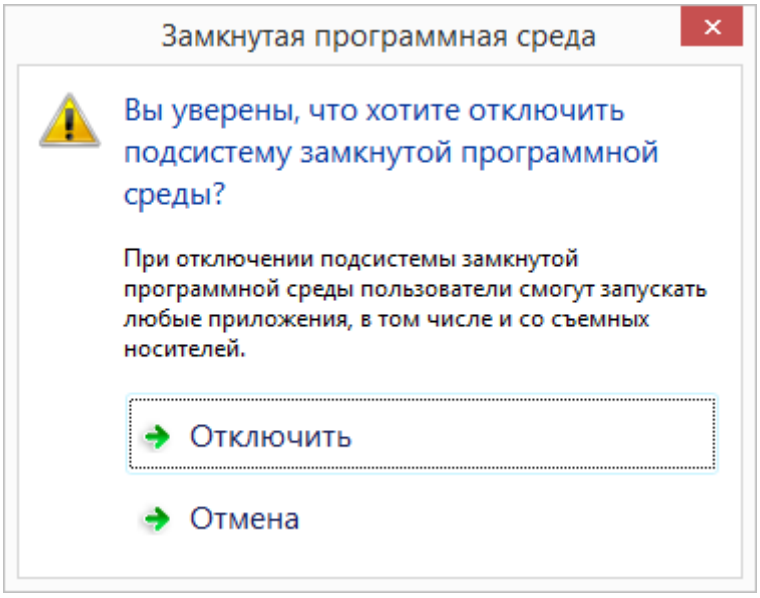


Рис. 48. Отключение механизмов ЗПС.

При этом механизмы замкнутой программной среды будут отключены для всех пользователей до их включения администратором системы защиты.

Для включения механизмов замкнутой программной среды необходимо вызвать контекстное меню программы **Монитор системы защиты** и выбрать пункт меню **Включение ЗПС**.

Режимы 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. 49), в котором необходимо выбрать необходимый режим автозапуска.

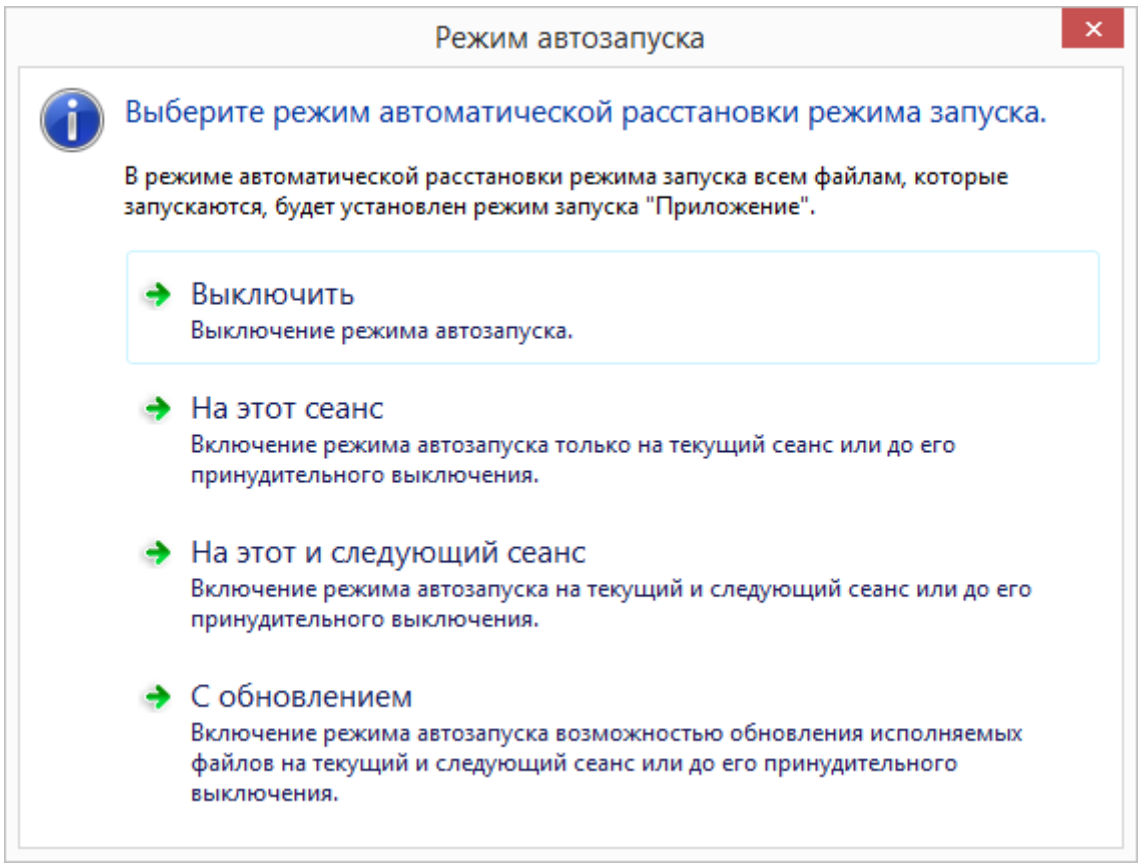


Рис. 49. Выбор режима автозапуска.

При выборе пункта **Выключить** происходит принудительное выключение режима автозапуска.

При выборе пункта **На этот сеанс** происходит включение режима автозапуска только на текущий сеанс работы системы защиты. При завершении сеанса работы режим автозапуска автоматически отключается.

При выборе пункта **На этот и 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 выборе пункта **С обновлением** 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 этот и следующий сеанс**, за исключением того, что исполняемые файлы становятся доступными на изменение и удаление.

Установка режима запуска

Установку режима запуска можно выполнить с помощью любого файлового менеджера, например, программы **Менеджер файлов** и только в режиме администрирования. Для установки режима запуска необходимо включить режим администрирования, выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Гриф и режим запуска** (см. Рис. 50). Также режим администрирования можно включить, нажав на кнопку Администрирование на самом диалоге.

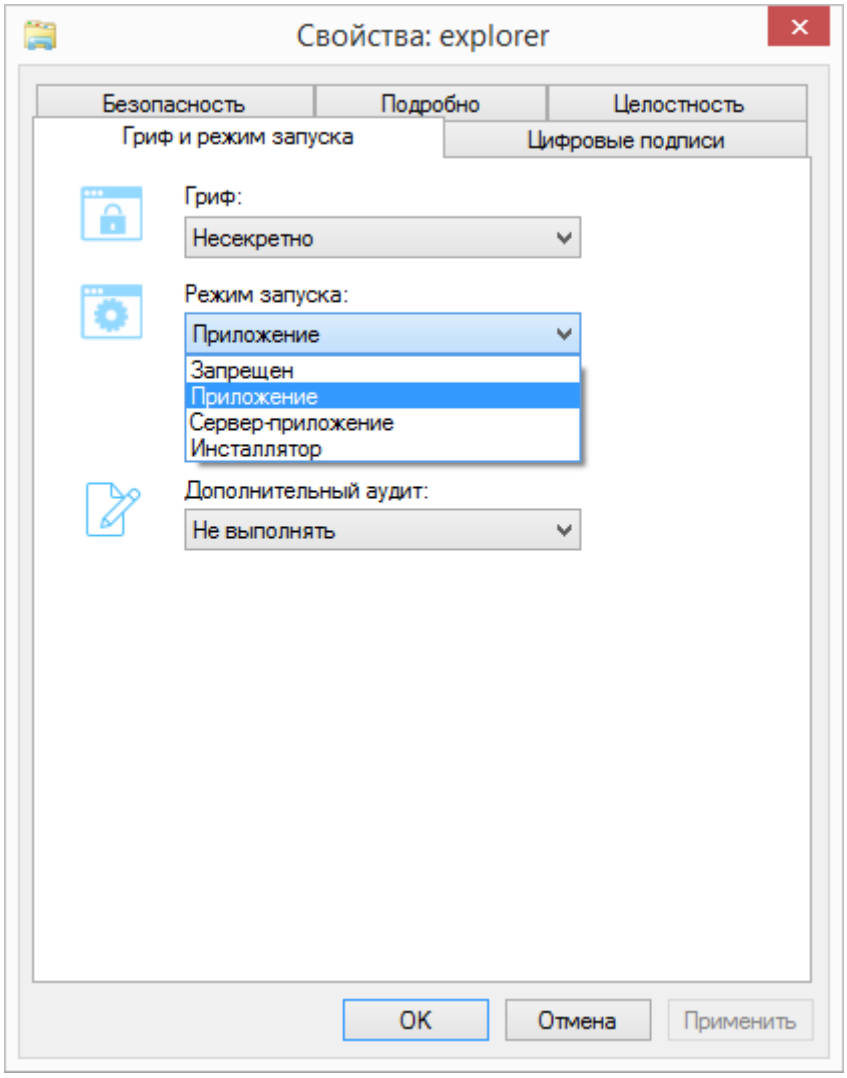


Рис. 50. Установка режима запуска.

Для изменения режима запуска выбранных объектов необходимо выбрать соответствующее значение из раскрывающегося списка в поле **Режим запуска**. Для сохранения сделанных изменений нажать кнопку OK или Применить.

Настройка ЗПС

В системе защиты существует возможность автоматизированной настройки замкнутой программной среды. Настройка ЗПС осуществляется при помощи вкладки **Настройки** программы **Консоль управления**. Для запуска процесса настройки необходимо выбрать пункт меню **Настройки ресурсов | Замкнутая программная среда...** . При этом начинается процесс построения дерева папок, длительность которого зависит от параметров компьютера и может занять несколько минут. В результате в появившемся диалоге администратор сможет выбрать папки, которые будут анализироваться при настройке замкнутой программной среды (см. Рис. 51).

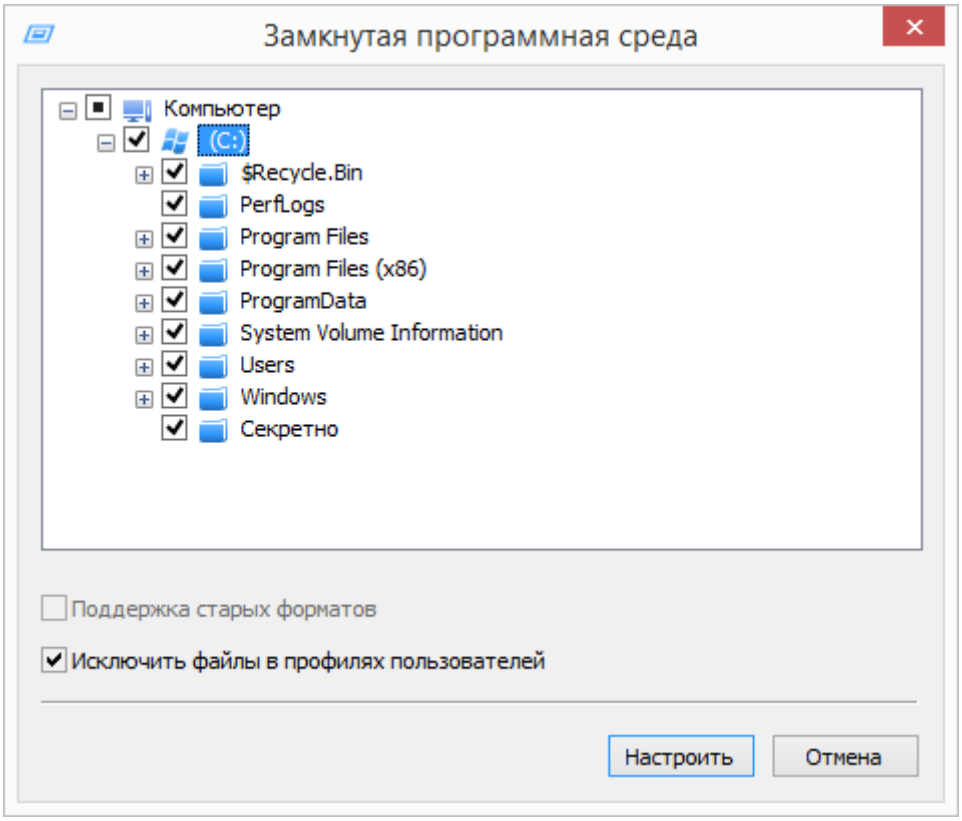
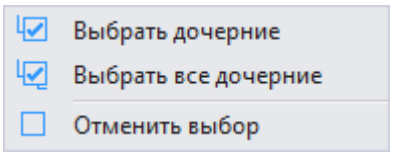


Рис. 51. Выбор папок для настройки ЗПС.



Если папка отмечена флагом, поиск будет производиться только в этой папке без учёта вложенных папок. При нажатии правой кнопки мыши в области дерева папок, на экране появится контекстное меню. Пункт **Выбрать дочерние**, позволяет отметить все папки в указанной папке, вложенные папки отмечены не будут. Пункт **Выбрать все дочерние**, позволяет выбрать все папки в указанной папке, в том числе и все вложенные папки. Пункт **Отменить выбор**, снимает флаги со всех вложенных папок. При нажатии

кнопки Настроить на все исполняемые файлы в отмеченных папках будет установлен режим запуска «Приложение» за исключением:

- исполняемые файлы в папке **%SystemRoot%\Installer** и во вложенных папках не будут менять значения режима запуска, если они не имеют расширения **msi** или **msp**;
- все файлы с расширениями **msi** и **msp** - на них устанавливается режим запуска «Инсталлятор»;
- файл **%SystemRoot%\system32\msiexec.exe** - на него устанавливается режим запуска «Инсталлятор»;
- в 64-х разрядных операционных системах файл **%SystemRoot%\SysWOW64\msiexec.exe** - на него устанавливается режим запуска «Инсталлятор».

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 флаг **Поддержка старых форматов**.

Установка флага **Исключить файлы в профилях пользователей** означает, что на исполняемые файлы, находящиеся в папках профилей пользователей, не будет устанавливаться режим запуска.

В процессе установки режима запуска на найденные исполняемые файлы, записи об этих событиях будут появляться в таблице результатов (см. Рис. 52).

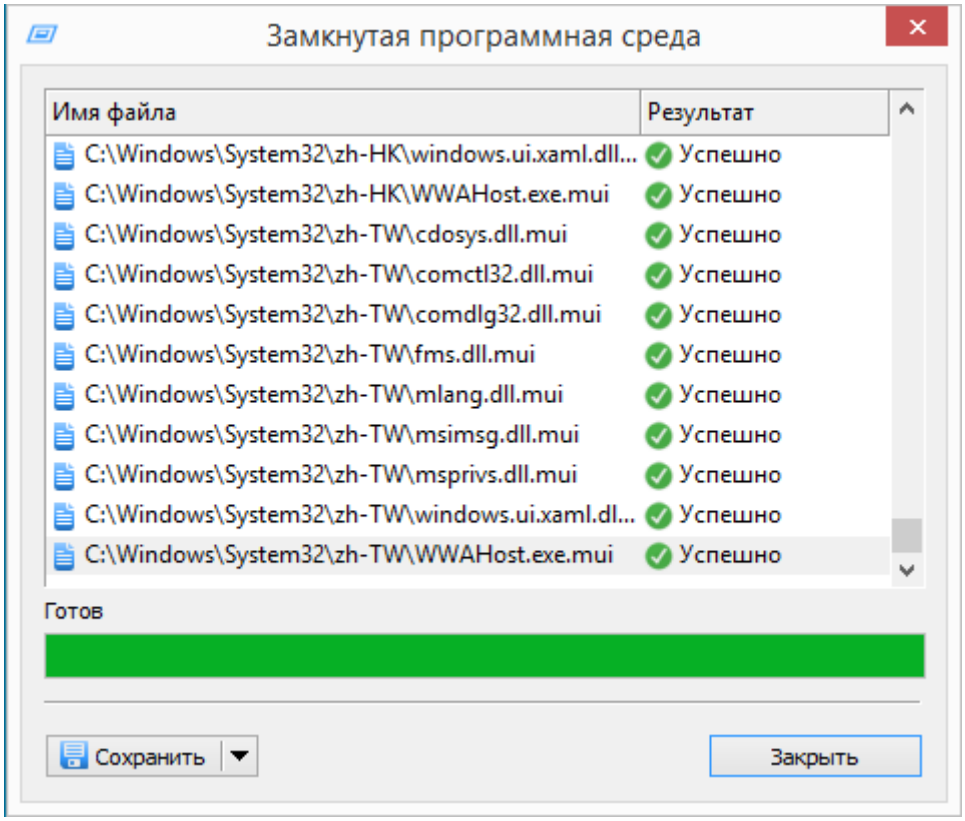
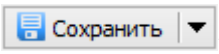
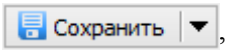
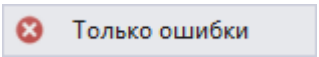


Рис. 52. Процесс настройки ЗПС.

После завершения процесса настройки список файлов, на которые был установлен режим запуска, можно сохранить в формате HTML или CSV. Для сохранения списка результатов необходимо нажать кнопку 

. Кнопка поддерживает выпадающий список типов сохраняемых результатов. Если просто нажать кнопку 

, то будет сохранён весь список результатов, если же выбрать пункт 

– будет сохранён только список неудачных попыток установки режима запуска.

Управление доступом

В данном разделе даются сведения о дискреционном и мандатном принципах контроля доступа, списках доступа, правах пользователей на доступ к ресурсам, о метках конфиденциальности и контроле потоков информации. Описываются сценарии выполнения администраторами системы защиты функций по разграничению доступа пользователей к ресурсам системы.

Дискреционный принцип контроля доступа

Для работы с файлами и папками на дисках операционная система MS Windows поддерживает несколько файловых систем, включая FAT, NTFS, CDFS. Между данными файловыми системами много различий, но главное, что только NTFS обеспечивает защиту файлов и папок при локальном доступе. В отличие от MS Windows, дискреционный принцип контроля доступа, реализованный в системе защиты «Страж NT», не зависит от типа файловой системы и поддерживает защиту ресурсов для любых файловых систем.

В рамках дискреционного принципа контроля доступ к защищаемым ресурсам контролируется механизмами системы защиты с помощью разрешений, содержащихся в записях списка контроля доступа. К защищаемым ресурсам компьютера относятся носители информации, папки, файлы, принтеры и устройства. Список контроля доступа может содержать как разрешающие, так и запрещающие записи.

Существуют следующие основные разрешения на доступ к ресурсам: **Полный доступ**, **Изменение**, **Чтение и выполнение**, **Чтение** и **Запись**. Каждое из этих разрешений представляет собой логическую группу особых разрешений, описание которых перечислены и описаны ниже.

Разрешение **Чтение и выполнение** включает в себя разрешения: **Обзор папок/Выполнение файлов**, **Содержание папки/Чтение данных**, **Чтение атрибутов**, **Чтение дополнительных атрибутов**, **Чтение разрешений**, **Синхронизация**.

Разрешение **Чтение** аналогично разрешению **Чтение и выполнение** за исключением **Обзор папок/Выполнение файлов**.

Разрешение **Запись** включает в себя **Создание файлов/Запись данных**, **Создание папок/Дозапись данных**, **Запись атрибутов**, **Запись дополнительных атрибутов**, **Чтение разрешений**, **Синхронизация**.

Разрешение **Изменение** включает все за исключением **Удаление подпапок и файлов**, **Смена разрешений** и **Смена владельца**.

Разрешение **Полный доступ** включает в себя все выше перечисленные разрешения. Группы и пользователи, которым предоставлен полный доступ к папке, могут удалять любые файлы в такой папке, независимо от разрешений на доступ к этим файлам.

Дополнительные сведения об управлении разрешениями можно найти в документе "Система защиты информации "Страж NT". Версия 4.0. Описание применения" RU.64476697.00040-01 31 01 и в технической документации на ОС MS Windows ***https://technet.microsoft.com/ru-ru/library/cc770749.aspx***.

Если папка или файл недоступны пользователю на чтение, они становятся невидимыми для пользователя.

Контроль доступа

Контроль доступа к защищаемым ресурсам реализован в ядре защиты системы защиты в виде диспетчера доступа. При попытке пользовательского или системного процесса получить доступ к ресурсу диспетчер доступа сравнивает информацию безопасности в маркере доступа процесса, созданного локальным администратором безопасности MS Windows, с атрибутами защиты ресурса.

Основываясь на типе доступа к ресурсу, операционная система создает маску запроса на доступ. Эта маска последовательно сравнивается с масками доступа, находящимися в списке контроля доступа ресурса. Каждый элемент в списке контроля доступа обрабатывается следующим образом:

- Идентификатор безопасности пользователя или группы из элемента списка контроля доступа сравнивается со всеми идентификаторами безопасности, находящимися в маркере доступа процесса, осуществляющего запрос. Если совпадений не обнаружено, данный элемент пропускается. В случае совпадения дальнейшая обработка зависит от типа элемента (разрешающий или запрещающий). Запрещающие элементы всегда должны располагаться раньше, чем разрешающие.
- Для запрещающего элемента типы доступа сравниваются с маской запроса на доступ. Если какой-либо тип доступа есть в обеих масках, дальнейшая обработка

списка не производится, и доступ запрещается. В противном случае обрабатывается следующий элемент.

- Для разрешающего элемента типы доступа сравниваются с маской запроса на доступ. Если все запрашиваемые типы разрешены, последующая обработка не требуется, и процесс получает доступ к объекту. В противном случае разрешения на недостающие типы доступа ищутся в следующих элементах.
- Если не все типы доступа маски запроса разрешены, и весь список контроля доступа просмотрен, доступ к ресурсу запрещается.
- Если доступ запрещен, проверяется случай, когда маска запроса содержит только типы доступа на чтение и запись списка контроля доступа ресурса. Если это имеет место, система проверяет, не является ли пользователь владельцем ресурса. В этом случае доступ разрешается.

Описанный выше алгоритм обработки списка контроля доступа является общим для всех защищаемых ресурсов. Однако для каждого типа ресурсов имеются свои особенности.

Для файлов и папок, находящихся на локальных жестких дисках компьютера, действуют следующие правила контроля доступа.

- Маска запроса, созданная процессом, осуществляющим доступ к файлу (папке), сравнивается с масками доступа, находящимися в списке контроля доступа файла (папки). При запросе на создание нового файла (папки) или перезаписи существующего, в маску запроса добавляется разрешение на запись. При запрете доступа дальнейшая проверка не производится и доступ запрещается.
- В случае разрешения доступа к файлу (папке) проверяется разрешение на доступ последовательно ко всем родительским папкам, включая корневую папку локального диска, на котором хранится файл (папка), для которых установлен флаг **Проверять разрешения для папки при доступе к вложенным объектам**. При запрете доступа хотя бы к одной такой папке доступ к файлу (папке) запрещается. При разрешении доступа ко всем таким папкам или при отсутствии параметра проверки разрешений при доступе к вложенным объектам на всех родительских папках доступ разрешается.
- Если запрашивается доступ на переименование файла (папки), то дополнительно проверяется доступ на создание файлов и папок для всех родительских папок нового имени файла (папки) с установленным параметром проверки разрешений при доступе к вложенным объектам. При запрете доступа хотя бы к одной такой

папке переименование файла (папки) запрещается. В противном случае переименование разрешается.

- При запросе на чтение файла, у которого включен контроль целостности с параметром блокировки при открытии и обнаружено нарушение целостности, доступ будет запрещен с ошибкой нарушения целостности.
- Для исполняемых файлов с разрешенным режимом запуска разрешен доступ только на чтение, независимо от установленных разрешений на сам файл и родительские папки, если только разрешения не запрещают доступ по чтению. Данное ограничение не действует в режиме обновления ПО, который используется для установки обновлений MS Windows и программного обеспечения.
- При запросе к файлу или папке на удаленном компьютере решение о предоставлении доступа принимается на удаленном компьютере.
- При создании новых файлов или папок действуют правила наследования разрешений, реализованные в файловой системе NTFS.
- Если носитель зарегистрирован в системе защиты с типом простой, то ко всем папкам и файлам данного носителя применяются одинаковые разрешения, соответствующие разрешениям, установленным на носитель в программе Учет носителей.

Разграничение доступа к компьютерам реализуется в подсистеме идентификации и аутентификации и основано на ведении списка компьютеров, на которых разрешено работать пользователю. Разграничение доступа пользователя к компьютерам настраивается в момент формирования персонального идентификатора пользователя и рассматривается в разделе **Формирование идентификаторов**

Установка разрешений

Установку разрешений на папки и файлы можно выполнить с помощью программы **Менеджер файлов**. Для установки разрешений необходимо выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Безопасность**, как показано на Рис. 53, или выбрать пункт **Разрешения и аудит**.

*Для установки разрешений для объектов, имеющих гриф, отличный от «Без проверки» и от низшего, следует выбирать пункт **Разрешения и аудит**.*

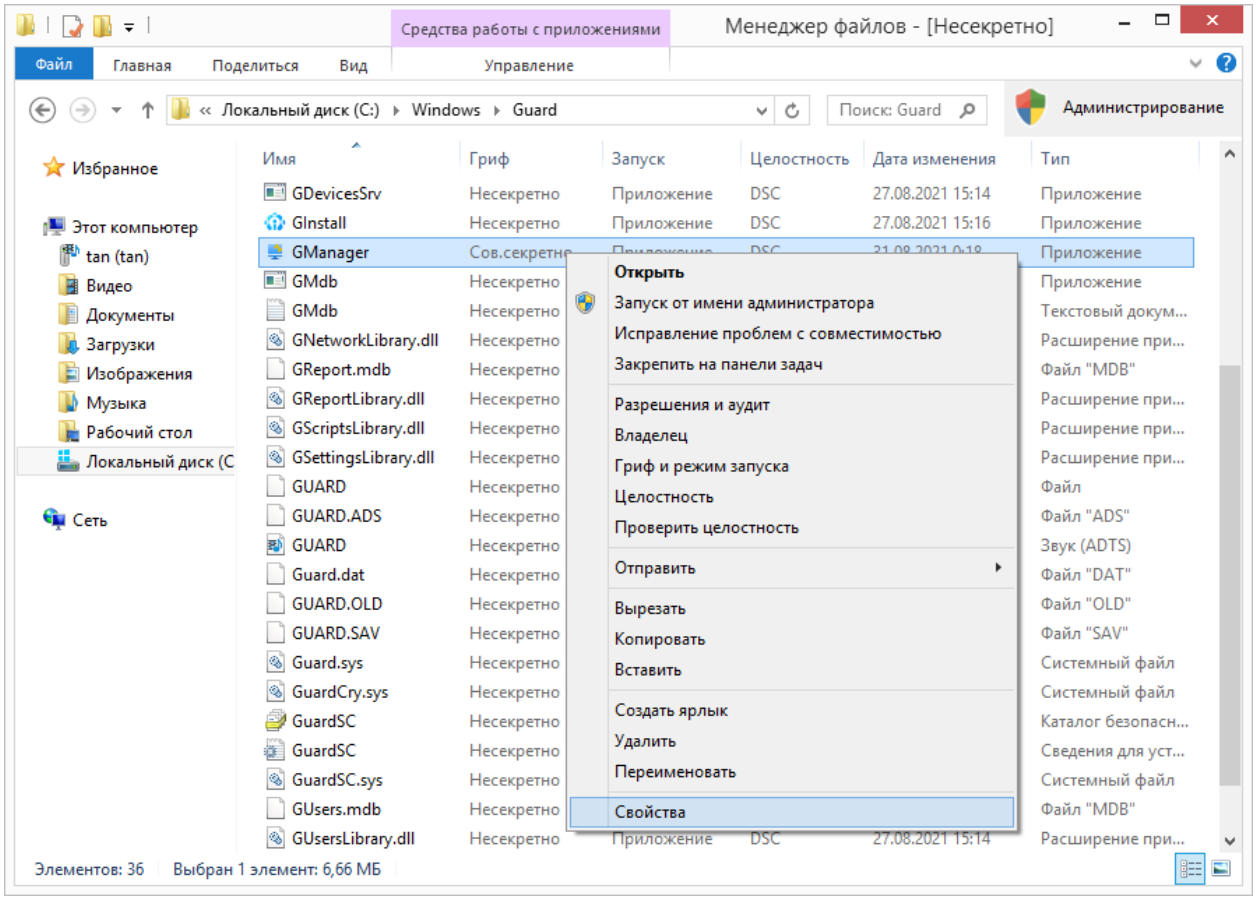


Рис. 53. Изменение разрешений защищаемых ресурсов.

При этом появляется окно (см. Рис. 54), в котором отображается список пользователей и групп пользователей, перечисленных в списке контроля доступа, а также разрешения для выбранного выше субъекта доступа. Для изменения разрешений выбранных ресурсов необходимо нажать кнопку Изменить... или последовательно нажать кнопки Дополнительно и Изменить. Если разрешения для выбранных ресурсов наследуются от родительских папок, для изменения разрешений необходимо нажать кнопку Отключение наследования и потом либо преобразовать наследованные разрешения в явные разрешения либо удалить все наследованные разрешения для выбранных ресурсов.

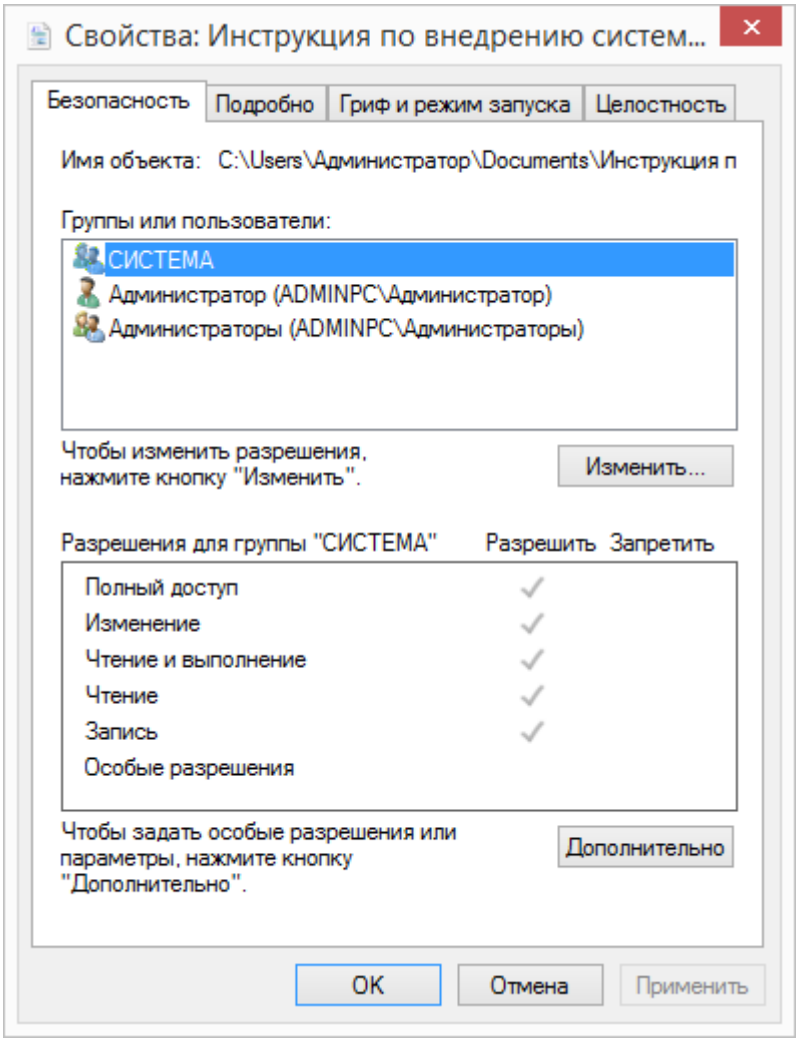


Рис. 54. Установка разрешений.

Для сохранения сделанных изменений нажать кнопку OK или Применить.

Изменение разрешений для корневых папок носителей информации описано в разделе ***Управление носителями информации****.*

Изменение разрешений для принтеров описано в разделе Настройка принтеров.

Мандатный принцип контроля доступа

Мандатный принцип контроля доступа реализован посредством назначения защищаемым ресурсам, каждому пользователю системы и прикладным программам меток конфиденциальности и сравнения их при запросах на доступ. В качестве меток конфиденциальности выступают:

- для защищаемых ресурсов – *гриф секретности*;
- для пользователей – *уровень допуска*;

- для прикладных программ – *допуск* и *текущий допуск*.

Гриф секретности ресурса представляет собой уровень его конфиденциальности в иерархической классификации. *Уровень допуска* пользователя определяет максимальный гриф секретности ресурса, доступный пользователю для чтения. *Допуск* прикладной программы определяет максимальный гриф секретности ресурса, доступный программе для чтения. *Текущий допуск* прикладной программы представляет собой действующее в конкретный момент времени значение *допуска* программы. При контроле доступа к защищаемым ресурсам непосредственно сравнению подлежат только значения *грифа секретности* ресурса и *текущего допуска* прикладной программы. *Уровень допуска* пользователя и *допуск* прикладной программы имеют значение только лишь при установке *текущего допуска* прикладной программы.

В СЗИ «Страж NT» по умолчанию используются следующие значения меток конфиденциальности в порядке повышения:

- «Несекретно»;
- «Конфиденциально»;
- «Секретно»;
- «Совершенно секретно».

Существует возможность переименования меток конфиденциальности в процессе эксплуатации системы защиты, как описано в разделе **Редактирование названий меток конфиденциальности**.

Дополнительно для папок и файлов вводится значение метки конфиденциальности «Без проверки». Ресурсы, имеющие такую метку, исключаются из процедуры контроля доступа.

При установке метки конфиденциальности на папку все вложенные объекты наследуют эту метку. Исключение составляет метка «Без проверки». Если на папку устанавливается метка «Без проверки», то метки конфиденциальности вложенных объектов останутся неизменными. При изменении метки конфиденциальности на папке меняются и мандатные метки вложенных объектов. В случае, когда на какие-либо из вложенных объектов устанавливается другая метка, отличная от метки папки, изменение метки папки не приводит к изменению метки вложенного объекта.

После установки системы защиты все объекты, участвующие в процессе контроля доступа по мандатному принципу, имеют метки конфиденциальности «Несекретно». Это означает, что мандатный контроль доступа не включен, поскольку все ресурсы имеют одинаковые метки конфиденциальности. Для использования мандатного принципа контроля доступа необходимо выполнение нескольких условий.

- В системе должны существовать или могут создаваться ресурсы, имеющие различные метки конфиденциальности.
- К обработке защищаемых ресурсов должны быть допущены пользователи, обладающие различными уровнями допуска.
- В системе установлены и определены прикладные программы, с помощью которых планируется производить обработку ресурсов, имеющих метки конфиденциальности выше «Несекретно».

При соблюдении всех этих условий администратор должен выполнить настройку системы защиты в части мандатного принципа контроля доступа. С этой целью необходимо:

- в соответствии с политикой безопасности назначить каждому пользователю уровень допуска и сформировать для него персональный идентификатор;
- для прикладных программ, предназначенных для обработки ресурсов, установить необходимый режим запуска и установить значение допуска;
- определить защищаемые ресурсы и установить на них мандатную метку.

Все указанные действия могут выполняться только администратором системы защиты.

При запуске прикладной программы со значением допуска выше «Несекретно» пользователем, имеющим уровень допуска выше «Несекретно», в системном меню программы появляется пункт **Текущий допуск**, с помощью которого пользователь может изменить значение текущего допуска программы, но только в сторону повышения. Максимальное значение текущего допуска, которое может установить пользователь, определяется минимальным значением среди уровня допуска пользователя и допуска прикладной программы.

На прикладную программу, имеющую допуск, может быть установлен параметр, позволяющий изменять значение текущего допуска непосредственно в момент запуска программы. Данный параметр имеет следующие значения:

- **Не запрашивать**. Текущий допуск программы становится «Несекретно»;

- **По умолчанию**. Текущий допуск программы становится равным допуску, присвоенному программе, при условии, если допуск программы не превышает уровень допуска пользователя. Если же допуск программы выше уровня допуска пользователя, то происходит отказ при запуске программы.
- **При старте**. На экран выдается диалоговое окно, позволяющее изменять текущий допуск программы, перед началом работы самой программы;
- **При создании окна**. На экран выдается диалоговое окно, позволяющее изменять текущий допуск программы, в момент создания главного окна программы.

Выбор значения данного параметра определяется способами обработки информации, а также некоторыми особенностями при запуске программ.

Существует еще один способ автоматической установки текущего допуска программы. Он состоит в присвоении специальной переменной окружения процесса ***@GuardNT@*** значения необходимого текущего допуска. Данная переменная окружения может принимать значения 0 – «Несекретно», 1 – «Конфиденциально», 2 – «Секретно», 3 – «Сов.секретно». Например, для запуска программы **Notepad** с текущим допуском «Секретно» можно создать пакетный файл следующего содержания:

```
set @GuardNT@ = 2

notepad
```

При запуске программы, для которой возможно изменение текущего допуска, значение текущего допуска отображается в заголовке главного окна программы (за исключением консольных приложений, а также приложений с ленточными, кастомизированными интерфейсами и приложений Windows Store). Для определения текущего допуска программ, у которых значение текущего допуска не отображается, служит программа **Просмотр процессов** (си. раздел **Просмотр процессов**).

При описании мандатных правил разграничения доступа используется понятие типа доступа. В СЗИ «Страж NT» рассматриваются следующие типы доступа:

- «чтение»;
- «запись»;
- «добавление».

Тип доступа «чтение» включает в себя чтение данных с произвольным доступом к ресурсу, а также чтение атрибутов, расширенных атрибутов, разрешений, параметров аудита и запуск исполняемой программы.

Тип доступа «запись» включает в себя запись данных с произвольным доступом к ресурсу, а также запись атрибутов, расширенных атрибутов, разрешений, смена владельца и удаление ресурса.

Тип доступа «добавление» разрешает только последовательную запись данных после конца ресурса.

Общие мандатные правила разграничения доступа состоят в следующем.

- Пользователь получает доступ к ресурсу по чтению в том случае, если текущий допуск прикладной программы, осуществляющей доступ, не ниже грифа секретности данного ресурса. В противном случае ресурс для прикладной программы будет недоступен на чтение и невидим.
- Пользователь получает доступ к ресурсу по чтению и записи в том случае, если текущий допуск прикладной программы, осуществляющей доступ, равен грифу секретности данного ресурса.
- Пользователь получает доступ к ресурсу на добавление данных в том случае, если текущий допуск прикладной программы, осуществляющей доступ, ниже грифа секретности данного ресурса. При этом защищаемый ресурс не виден для пользователя.
- При создании нового ресурса ему присваивается гриф секретности, равный текущему допуску прикладной программы.

Применительно к файлам и папкам в СЗИ «Страж NT» реализован следующий алгоритм проверки мандатных ПРД:

- Основываясь на типе доступа к ресурсу, операционная система создает маску запроса на доступ.
- При запросе на доступ к файлу или папке определяются гриф секретности файла или папки и текущий допуск программы. В соответствии с общими мандатными правилами разграничения доступа определяются запрещенные типы доступа к файлу или папке.
- Осуществляется проверка разрешения на доступ в соответствии с дискреционными правилами. При запрете доступа дальнейшая проверка не производится, доступ к файлу или папке запрещается.

- Маска запроса сравнивается с запрещенными типами доступа. Если маска запроса содержит хотя бы один из запрещенных типов доступа, дальнейшая проверка не производится, доступ к файлу или папке запрещается.
- Осуществляется проверка разрешений на доступ ко всем родительским папкам. Решение на доступ принимается одновременно по дискреционным и мандатным ПРД. В соответствии с мандатными ПРД доступ к файлу или папке разрешен, если при запросе на чтение разрешен доступ по чтению ко всем родительским папкам, включая корневой, а при запросе на запись разрешен доступ на запись хотя бы к одной из родительских папок, включая корневой каталог.

Практически данный алгоритм означает следующее.

При запросе на чтение файла или папки доступ разрешается только в том случае, если метка конфиденциальности самого файла или папки и всех родительских папок, включая корневую, равна или ниже текущего допуска программы либо имеет значение «Без проверки».

При запросе на запись файла или папки доступ разрешается только в том случае, если метка конфиденциальности самого файла или папки равна текущему допуску программы или имеет значение «Без проверки», а также если среди родительских папок, включая корневую, нет ни одной, имеющей метку конфиденциальности выше текущего допуска программы, а также имеется хотя бы одна папка, имеющая метку конфиденциальности, равную текущему допуску программы либо значению «Без проверки».

При запросе только на добавление данных файла или папки доступ разрешается в том случае, если метка конфиденциальности самого файла или папки выше текущего допуска программы или имеет значение «Без проверки», а также если среди родительских папок, включая корневую, имеется хотя бы одна папка, имеющая метку конфиденциальности, выше или равную текущему допуску программы либо значению «Без проверки».

В СЗИ «Страж NT» предусмотрена возможность настройки отдельных программ таким образом, чтобы мандатные правила разграничения доступа не применялись. Данные программы разрабатываются с учетом интерфейсов работы СЗИ «Страж NT» и могут получать значения меток конфиденциальности защищаемых ресурсов, а также изменять их и назначать любые метки для вновь создаваемых ресурсов. Как правило, такие программы должны разрабатываться для сопряжения различных систем защиты с СЗИ «Страж NT» и позволяют передавать метки конфиденциальности защищаемых ресурсов в

различные среды. Для выполнения такой настройки необходимо установить режим запуска программы в значение «Сервер-приложение».

При настройке системы защиты администратор должен обратить особое внимание на установку необходимых меток конфиденциальности на папки для временных файлов и корзины для удаленных файлов.

Контроль потоков информации

Контроль потоков информации основывается на мандатном принципе контроля доступа и описывается правилами чтения и записи информации на сетевых дисках.

При получении от программы запроса на создание или изменение файла или папки на сетевом диске система защиты в первую очередь проверяет текущий допуск программы. Если текущий допуск программы выше «Несекретно», система защиты выдает запрос на удаленный компьютер, поддерживается ли на нем мандатный контроль доступа. Если мандатный контроль доступа на удаленном компьютере не поддерживается, то запрос отклоняется и программе возвращается ошибка.

Для запросов на чтение ресурсов на сетевых дисках, а также при любых запросах от программ с текущим допуском «Несекретно» проверка поддержки мандатных правил на удаленном компьютере не производится.

Далее в сетевой запрос на доступ к ресурсу вставляется значение текущего допуска программы и признак режима администрирования. В таком виде запрос отправляется на удаленный компьютер. Таким образом, решение о допуске к ресурсу на удаленном компьютере принимается системой защиты на удаленном компьютере.

При получении сетевого запроса на доступ система защиты использует значение текущего допуска, установленного в сетевом запросе, и применяет обычные мандатные правила.

В рамках подсистемы контроля потоков информации реализован механизм, предотвращающий повышение текущего допуска прикладной программы при наличии файлов, открытых данной программой на запись. Система защиты для каждого процесса в системе создает счетчик открытых на запись файлов. При открытии файла на запись счетчик увеличивается, при закрытии уменьшается. Счетчик не меняет своего значения, если метка конфиденциальности файла имеет значение «Без проверки». Если на момент повышения текущего допуска программы счетчик открытых на запись файлов не равен нулю, то текущий допуск не будет повышен, а пользователю выдается сообщение о

наличии открытых на запись файлов. В том случае, если прикладная программа всегда открывает на запись некоторые служебные файлы и требуется повысить ее текущий допуск, то необходимо воспользоваться одной из перечисленных ниже возможностей.

- Установить на служебные файлы метку конфиденциальности «Без проверки». При этом необходимо исключить возможность записи защищаемой информации в эти файлы.
- Установить параметр запроса текущего допуска программы в значение «При старте».
- Использовать специальную переменную процесса **@GuardNT@** для установки текущего допуска программы.

Контроль буфера обмена

Помимо управления доступом при сетевых запросах СЗИ «Страж NT» контролирует перенос информации с использованием папки обмена. При помещении информации в папку обмена, ей присваивается текущий гриф, равный текущему допуску программы, выполняющей запись. При попытке чтения информации из папки обмена сравнивается текущий гриф папки обмена и текущий допуск программы. Программа может прочитать информацию из папки обмена, если текущий гриф папки обмена не выше текущего допуска программы.

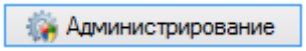
Контроль именованных каналов

В рамках подсистемы контроля потоков дополнительно предусмотрен механизм контроля именованных каналов. При его включении каждому именованному каналу, созданному программой-сервером, назначается метка конфиденциальности, соответствующая текущему допуску данной программы. При подключении к именованному каналу программы-клиента действуют следующие мандатные правила контроля доступа:

- программа клиент получает доступ к именованному каналу по чтению в том случае, если текущий допуск программы клиента не ниже метки конфиденциальности именованного канала.
- программа клиент получает доступ к именованному каналу по записи в том случае, если текущий допуск программы клиента ниже или равен метки конфиденциальности именованного канала.

Для включения контроля именованных каналов необходимо во вкладке **Настройки** программы **Консоль управления** при выборе группы настроек **Общие настройки** установить флаг в поле **Контролировать именованные каналы** и нажать кнопку **Сохранить настройки** (см. Рис. 47).

Установка меток конфиденциальности на ресурсы

Установку метки конфиденциальности на папки и файлы можно выполнить с помощью любого файлового менеджера, например, программы **Менеджер файлов** и только в режиме администрирования. Для установки метки конфиденциальности необходимо включить режим администрирования, выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Гриф и режим запуска**. Также режим администрирования можно включить, нажав на кнопку 

на самом диалоге.

Для изменения метки конфиденциальности выбранных объектов необходимо выбрать соответствующее значение из раскрывающегося списка в поле **Гриф**, как показано на Рис. 55.

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

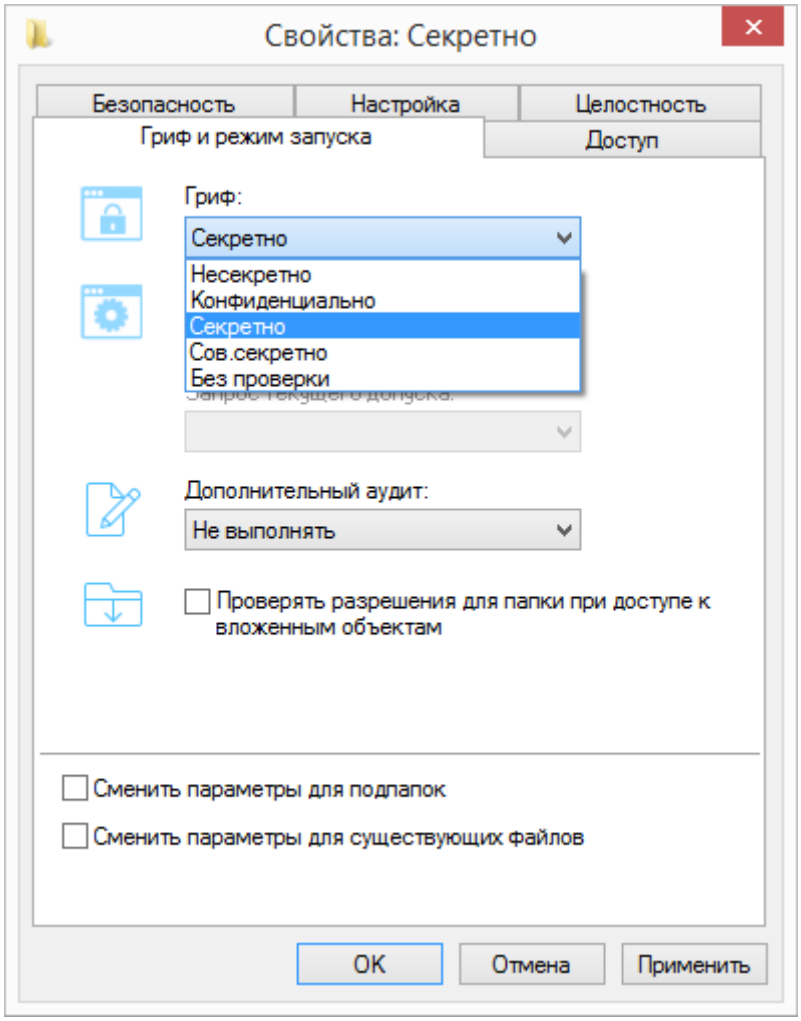


Рис. 55. Установка грифа ресурсу.

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

Если установлены флаги в обоих вышеуказанных полях, все установленные параметры для данной папки будут установлены для всех подпапок и файлов, в них входящих.

Для сохранения сделанных изменений нажать кнопку OK или Применить.

*Изменение меток конфиденциальности корневых папок носителей информации описано в разделе **Управление носителями информации**.*

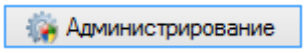
Изменение меток конфиденциальности принтеров описано в разделе Настройка принтеров.

Виртуализация объектов

При настройке приложений для работы с различными текущими допусками часто возникает проблема выявления файлов, которые используются для сохранения служебной информации приложения и должны быть доступны для чтения и записи при работе приложения со всеми значениями текущего допуска. Как правило, на такие файлы должен устанавливаться гриф «Без проверки».

Альтернативой указанному методу является включение механизма виртуализации объектов и установка на родительскую папку таких объектов флага виртуализации. При установке на папку флага виртуализации для каждого грифа будет при необходимости создан свой образ исходной папки, на которую будет автоматически перенаправляться запрос при обращении к ней приложения с соответствующим текущим допуском.

Механизм виртуализации объектов по умолчанию выключен. Дополнительные сведения о включении и работе механизма виртуализации объектов можно найти в документе "Система защиты информации "Страж NT". Версия 4.0. Описание применения" RU.64476697.00040-01 31 01.

Установку флага виртуализации на папки можно выполнить с помощью любого файлового менеджера, например, программы **Менеджер файлов** и только в режиме администрирования. Для установки флага виртуализации необходимо включить режим администрирования, выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Гриф и режим запуска** (см. Рис. 56). Режим администрирования также можно включить, нажав кнопку 

на вкладке **Гриф и режим запуска**.

Для установки флага виртуализации на папку необходимо установить флаг в поле **Виртуализация объектов**. Если механизм виртуализации объектов выключен, данное поле будет недоступно для изменения.

Для включения механизма виртуализации объектов необходимо во вкладке **Настройки** программы **Консоль управления** при выборе группы настроек **Общие настройки** установить флаг в поле **Использовать виртуализацию объектов** и нажать кнопку **Сохранить настройки** (см. Рис. 47).

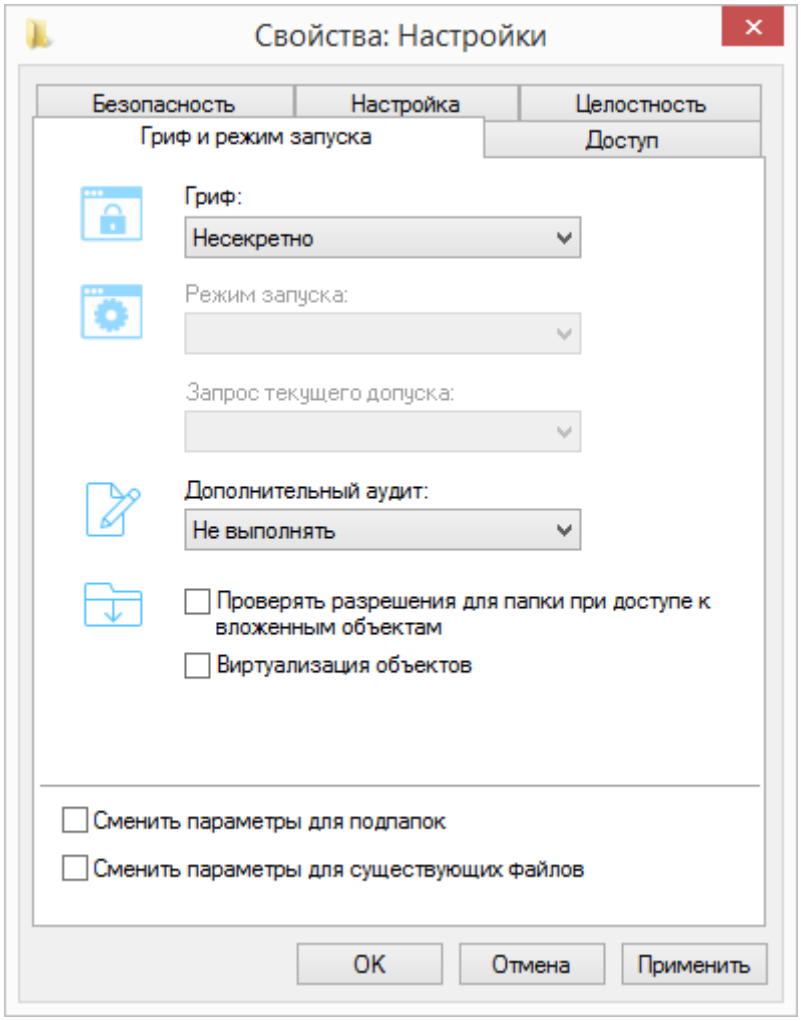


Рис. 56. Установка флага виртуализации.

Для сохранения сделанных изменений нажать кнопку OK или Применить.

Редактирование названий меток 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», «Конфиденциально», «Секретно» и «Сов.секретно».

Метка 1 соответствует самому низкому уровню конфиденциальности в иерархической классификации, а Метка 4 – самому высокому.

Для изменения названий меток конфиденциальности необходимо во вкладке **Настройки** программы **Консоль управления** выбрать группу настроек **Общие настройки** и отредактировать их названия в соответствующих полях (см. Рис. 57).

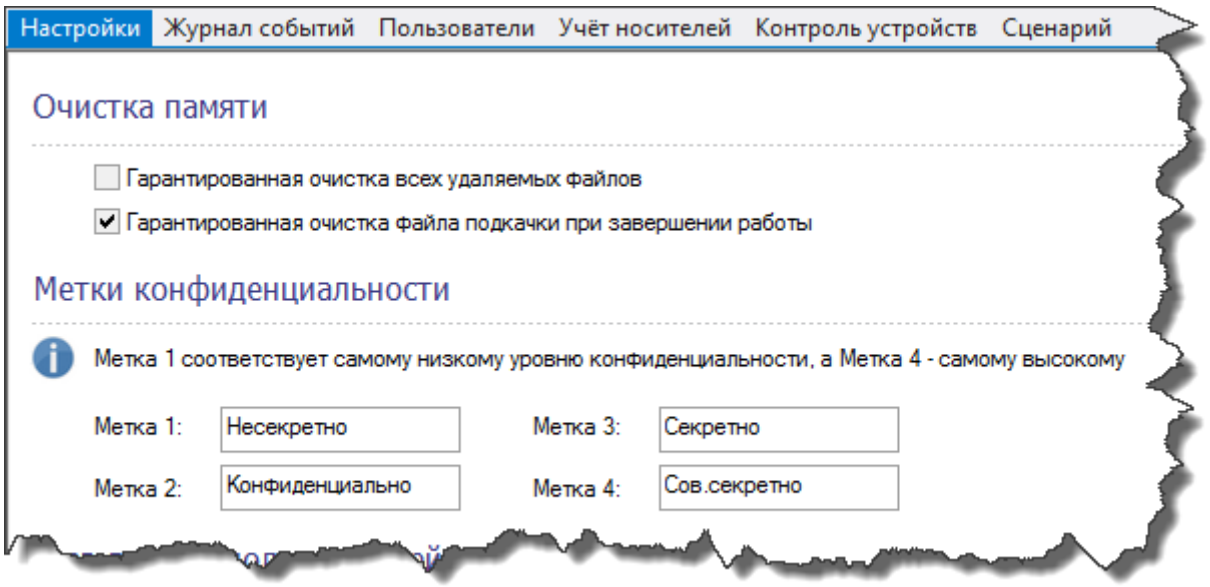
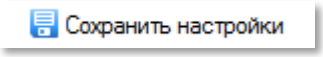


Рис. 57. Редактирование меток конфиденциальности.

Для сохранения настроек необходимо нажать кнопку 

, для возврата к настройкам по умолчанию – кнопку 

.

Просмотр процессов

Как уже был описано ранее, при установке программе текущего допуска, в заголовке ее главного окна появляется наименование метки конфиденциальности, соответствующей установленному текущему допуску. Однако, данное правило работает только для программ со стандартным главным окном. Для приложений с ленточными, кастомизированными интерфейсами и приложений Windows Store данное правило не актуально.

Программа **Просмотр процессов** предназначена для однозначного определения текущих допусков всех запущенных процессов. Для запуска программы необходимо выбрать пункт **Просмотр процессов** контекстного меню программы **Монитор системы защиты** при работе с рабочим столом или выбрать пункт **Просмотр процессов** в представлении «Приложения» начального экрана. Примерный вид программы представлен на Рис. 58. Список процессов представляет собой таблицу, содержащую следующие поля.

Свойство	Описание
Имя процесса	Определяет имя процесса.
ИД процесса	Число, уникально идентифицирующее выполняющийся процесс.
Пользователь	Определяет учетную запись пользователя, от имени которого выполняется процесс.
Допуск	Определяет текущий допуск процесса.
Путь	Определяет расположение файла процесса на носителе.

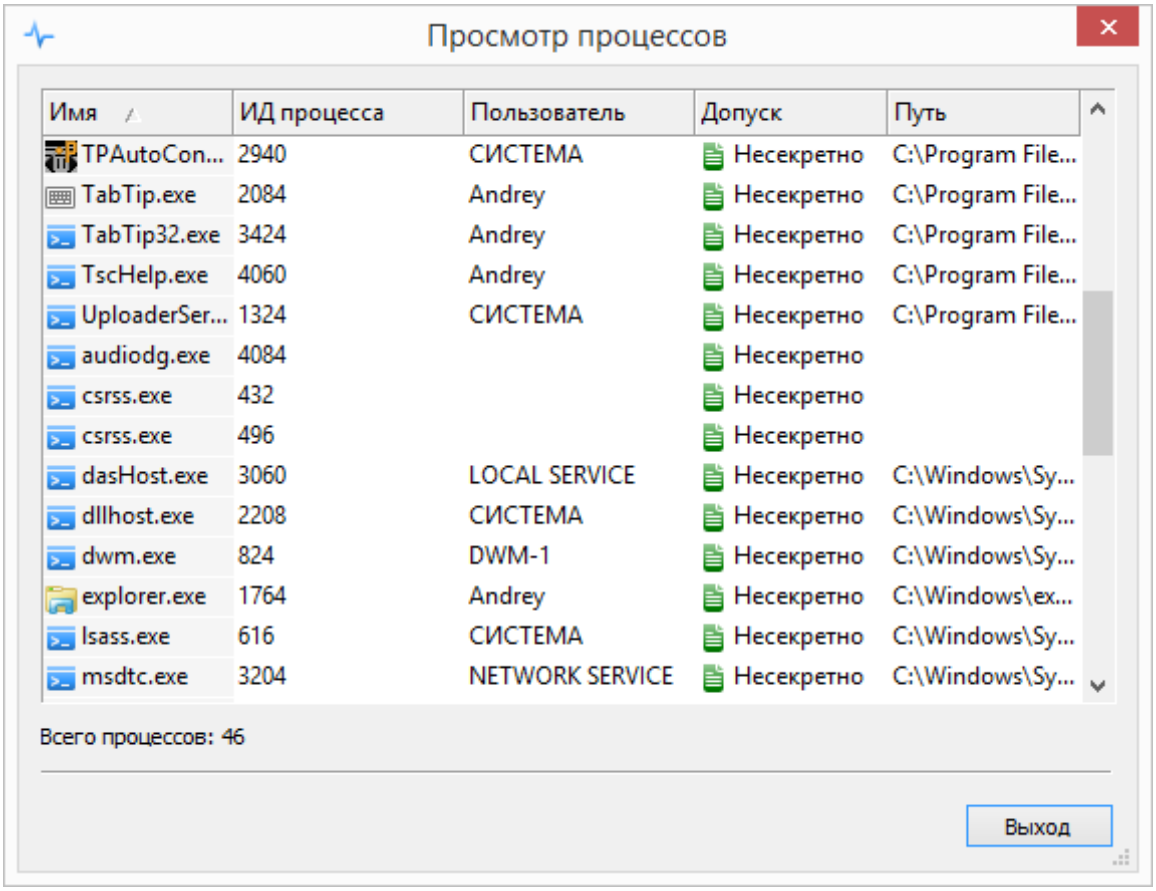


*Рис. 58. Общий вид программы **Просмотр процессов**.*

Управление носителями информации

В данной главе приводятся сведения о подсистеме учета носителей информации. Описаны интерфейсы утилит администратора системы защиты при работе с подсистемой, а также его типовые действия при управлении политиками использования носителей информации.

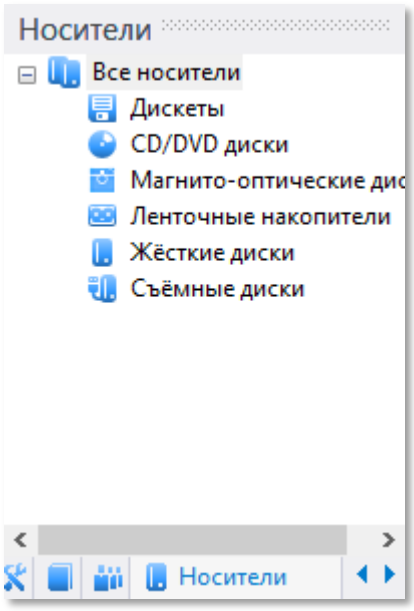
Общие сведения

СЗИ «Страж NT» контролирует доступ ко всем носителям информации, используемым в процессе работы. При подключении носителя информации система защиты проверяет, зарегистрирован ли он в системе. Если носитель является зарегистрированным, 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.

В СЗИ «Страж NT» поддерживаются следующие типы носителей:

- дискеты;
- CD/DVD диски;
- магнито-оптические диски;
- ленточные накопители;
- жесткие диски;
- съёмные диски.

В процессе установки системы защиты в список зарегистрированных носителей будут добавлены все присутствующие на момент установки носители типа «Жёсткий диск». В дальнейшем администратор системы защиты может поменять свойства зарегистрированных носителей.



Учет носителей осуществляется с помощью вкладки **Учет носителей** программы **Консоль управления** (см. Рис. 59). В панели носителей будет отображён список групп носителей, определяющих типы носителей.

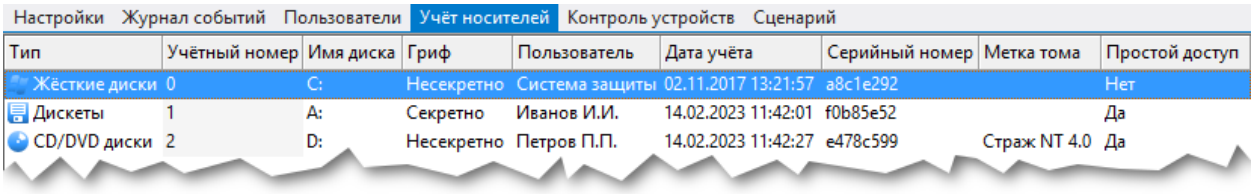


Рис. 59. Список учтенных носителей.

Список носителей представляет собой таблицу, содержащую следующие поля.

Поле	Описание
Тип	Отображает тип носителя.
Учётный номер	Отображает учётный номер носителя, заданный администратором при регистрации носителя.
Имя диска	Отображает букву диска, которую носитель (том) имеет в системе. Пустое поле «Имя диска» означает, что этот данный носитель в настоящий момент отсутствует в системе или не имеет буквы диска.
Гриф	Отображает метку конфиденциальности носителя.
Пользователь	Отображает фамилию должностного лица, за которым закреплён данный носитель.
Дата учёта	Отображает дату и время регистрации носителя.
Серийный номер	Отображает серийный номер носителя.
Метка тома	Отображает значение метки тома носителя.
Простой доступ	Отображает, с каким типом доступа учтён носитель. Значение «Да» означает, что носитель учтён с простым доступом. Значение «Нет» означает, что носитель учтён без простого доступа. Простой тип доступа означает, что назначенные носителю мандатные и дискреционные параметры безопасности (гриф и разрешения) распространяются на все ресурсы, находящиеся на данном носителе. В противном случае указанные параметры распространяются только на корневой каталог носителя (тома), и на носителе могут находиться ресурсы с разными мандатными и дискреционными параметрами безопасности.

Администратор системы защиты имеет возможность сортировать список носителей по любому из перечисленных полей. Кроме того, администратор может осуществлять выборку носителей по типам. Для этого необходимо выбрать соответствующую группу носителей на панели носителей. По умолчанию в списке отображаются все зарегистрированные носители.

Редактирование свойств 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. Таким образом, при подключении незарегистрированного носителя информации администраторы системы защиты получат к нему полный доступ, а пользователи доступа не получат.

Для просмотра и редактирования свойств группы носителей необходимо выбрать пункт **Свойства...** контекстного меню группы или дважды кликнуть на соответствующей группе носителей в панели носителей. При этом откроется окно свойств группы носителей (см. Рис. 60), в котором можно настроить аудит для группы носителей.

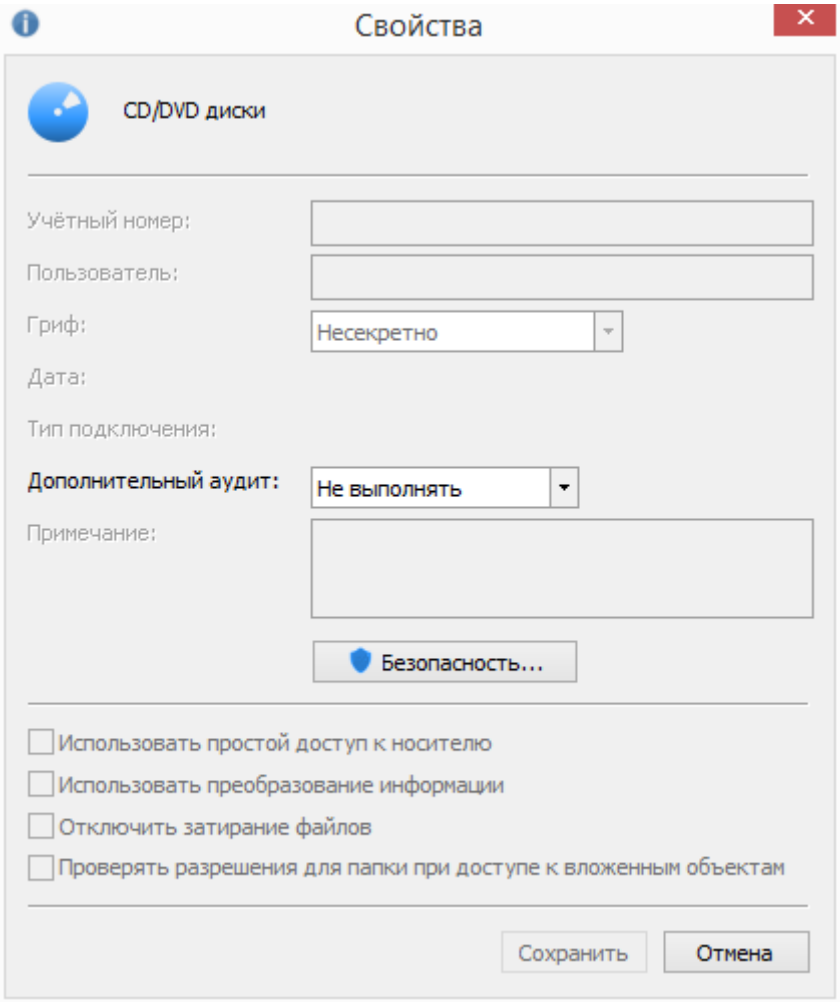
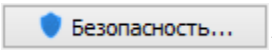


Рис. 60. Свойства группы носителей.

Для вызова окна редактора разрешений необходимо нажать кнопку 

. В открывшемся окне (см. Рис. 61) можно менять разрешения для выбранной группы носителей. Сохраненные разрешения будут применяться при подключении незарегистрированных носителей выбранного типа.

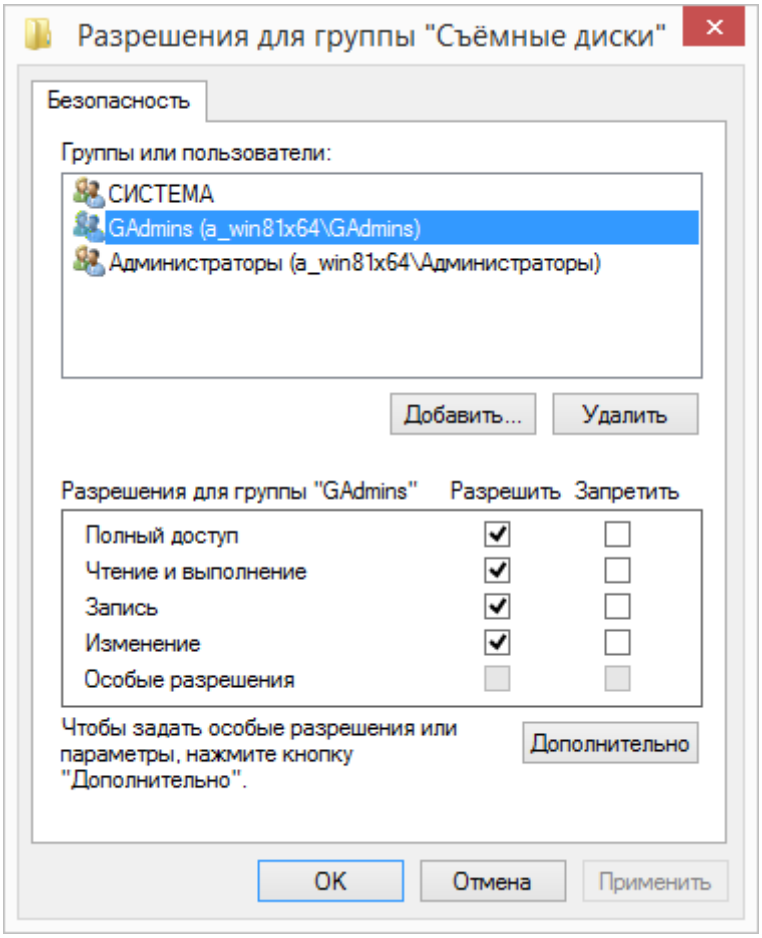


Рис. 61. Редактирование разрешений для группы носителей информации.

Регистрация носителя

Для разграничения доступа к конкретному носителю информации администратор системы защиты должен его зарегистрировать. Если носитель зарегистрирован, к нему не будут применяться правила разграничения доступа для группы носителей, к которой он принадлежит.

Для регистрации нового носителя необходимо выбрать пункт меню **Носители | Добавить...** или нажать соответствующую кнопку на панели инструментов. При этом откроется окно (см. Рис. 62), в котором необходимо выбрать регистрируемый носитель информации.

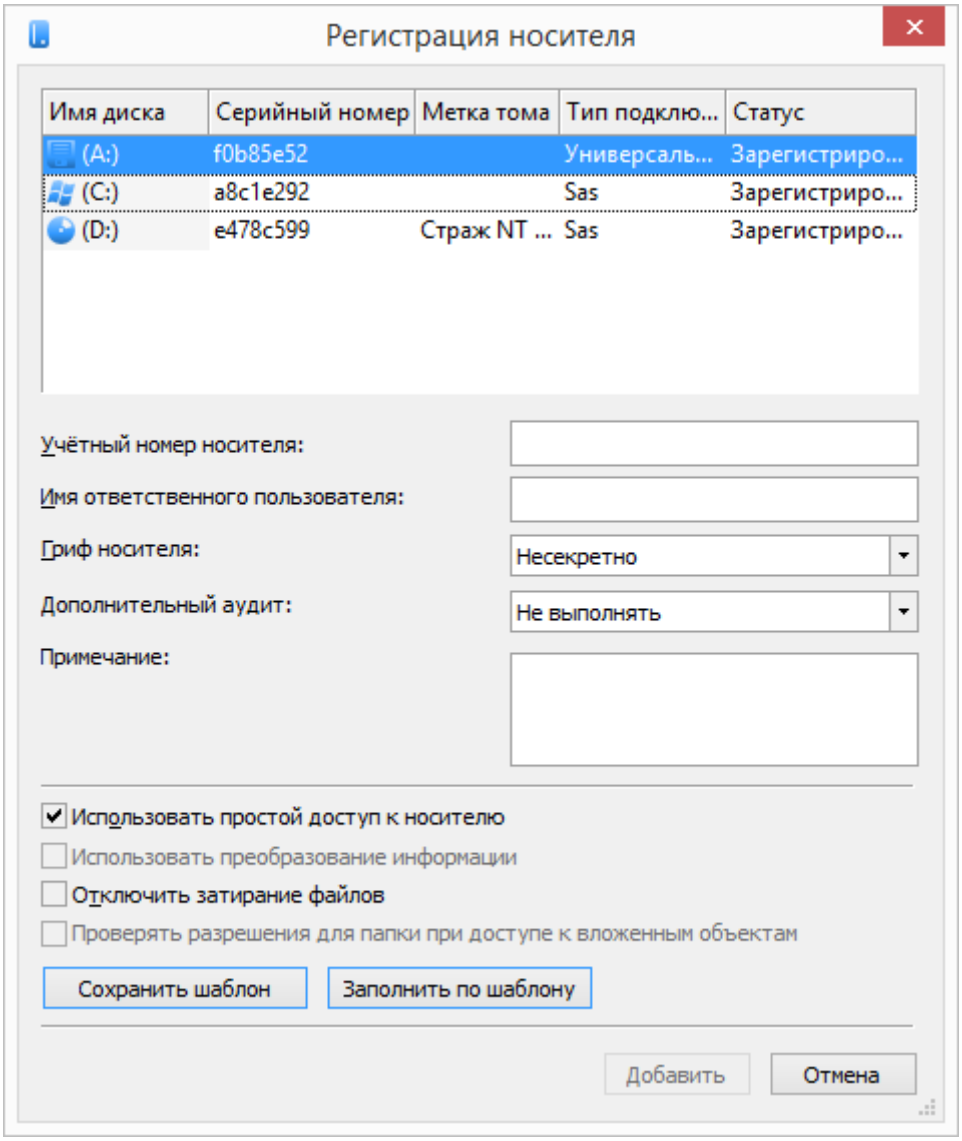


Рис. 62. Регистрация носителя информации.

При учёте носителя информации необходимо задать следующие регистрационные данные:

- учётный номер носителя;
- имя ответственного пользователя;
- гриф носителя;
- параметры дополнительного аудита;
- примечание.

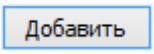
При установке флага в поле **Использовать простой доступ к носителю** носитель будет учтён с указанным грифом. Все файлы и папки, присутствующие на носителе на момент учёта, а также вновь создаваемые файловые объекты будут иметь указанный гриф.

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

При установке флага в поле **Использовать преобразование информации** носитель будет отформатирован при постановке на учёт. Вся информация на носителе будет храниться в преобразованном виде. При использовании режима преобразовании информации носитель может быть прочитан только на компьютерах, система защиты которых устанавливалась с использованием одного и того же персонального идентификатора администратора системы защиты.

В режиме преобразования информации можно зарегистрировать только съёмные носители, например USB-флэш-диски. В процессе регистрации носителя с параметром преобразования информации все данные на носителе будут уничтожены.

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

После нажатия кнопки 

носитель информации будет зарегистрирован. Если носитель с таким серийным номером уже присутствует в списке, будет выдано сообщение с предложением перезаписать параметры зарегистрированного носителя. При положительном ответе новые параметры заменят уже существующие.

Удаление носителя

Для удаления носителя из списка необходимо выбрать его в списке и выбрать пункт меню **Носитель | Удалить носитель** или нажать соответствующую кнопку на панели инструментов. При удалении носителя, будет выдано предупреждение с указанием номера удаляемого носителя.

В контекстном меню списка носителей доступен пункт **Удалить с сетевых компьютеров..**. Выбор данного пункта запускает мастер, позволяющий снять с регистрации на компьютерах сети те или иные носители, содержащиеся в списке учтённых на данном компьютере.

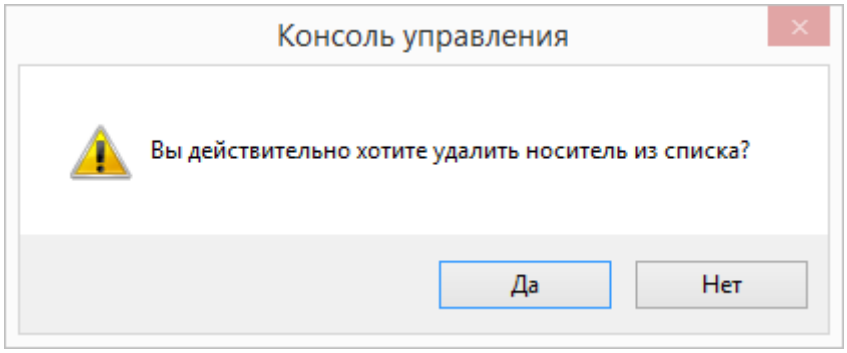


Рис. 63. Предупреждение об удалении носителя.

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 для выбранного носителя информации необходимо выбрать пункт меню **Носитель | Свойства...** или нажать соответствующую кнопку на панели инструментов. При этом будет отображено окно (см. Рис. 64), в котором выводится вся информация о носителе.

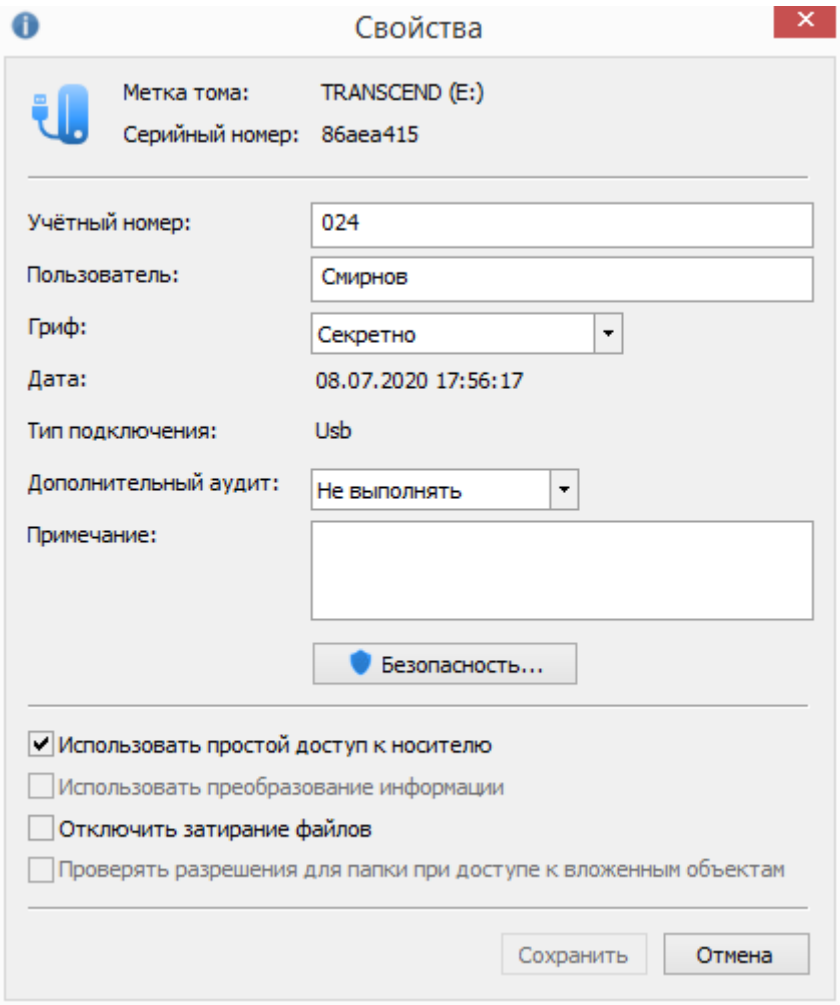


Рис. 64. Свойства носителя информации.

При установке флага в поле **Отключить затирание файлов** при удалении файлов на выбранном носителе их содержимое не будет заполняться случайной последовательностью байтов.

Для отключения режима преобразования носителя информации необходимо снять носитель с учета в программе **Консоль управления** и выполнить повторную постановку на носителя на учет. При этом опция преобразования информации на носителе уже будет включена. Если при этом снять опцию преобразования, то программа предложит произвести его форматирование, по завершении которого носитель будет учтен без режима преобразования.

Для просмотра и редактирования разрешений для выбранного носителя информации необходимо в окне его свойств нажать кнопку 

. При этом будет отображено окно (см. Рис. 65), в котором можно менять разрешения для данного носителя.

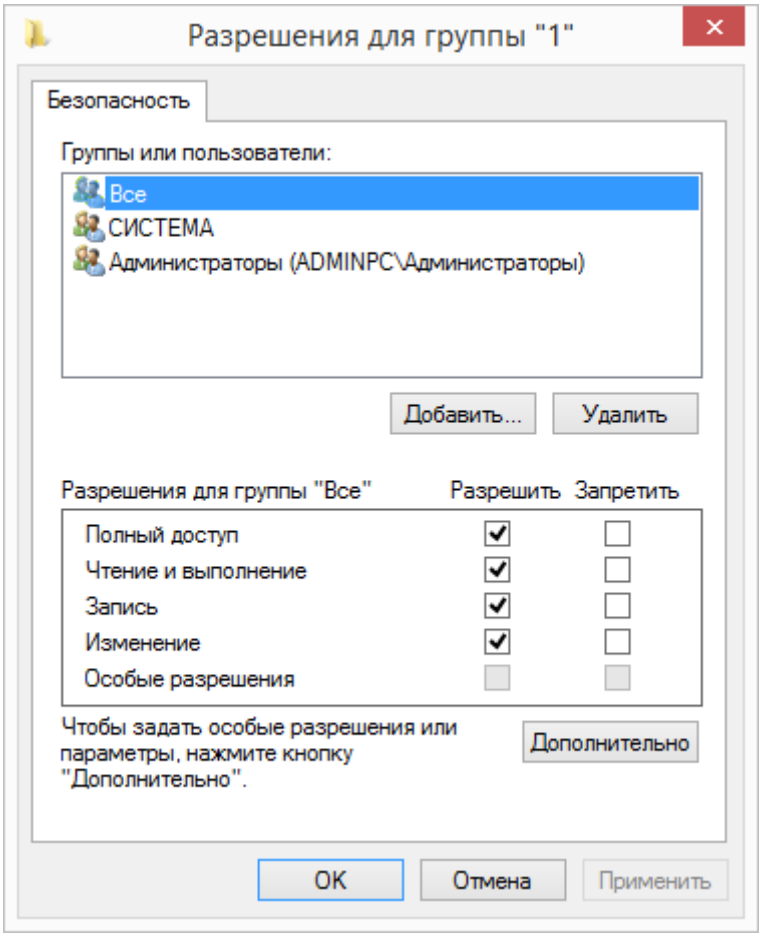


Рис. 65. Редактирование разрешений для носителя.

Экспорт настроек

Для удобства распространения выполненных настроек групп носителей и носителей информации на другие компьютеры существует механизм экспорта настроек. Экспорт настроек можно осуществлять как через локальную сеть, так и через файл настроек, например, при отсутствии сети.

При экспорте настроек в списках контроля доступа, определяющих дискреционные права к группам носителей и носителям информации, указываются идентификаторы безопасности пользователей и групп пользователей (Security Identifier или SID). В этой связи полностью корректное применение дискреционных прав по доступу к указанным объектам (при импорте их из файла на другом компьютере или экспорте по сети на другой компьютер) возможно только для пользователей и групп пользователей, имеющих полностью идентичные SIDы на всех компьютерах. Таковыми, в частности, являются пользователи и группы пользователей:

- одного домена;

- имеющие хорошо известные идентификаторы безопасности (Well-known security identifiers), например, группы Все (Everyone), Администраторы (Administrators) и т.п..

Для экспорта настроек необходимо выбрать пункт меню **Носители | Экспорт...**, или нажать соответствующую кнопку на панели инструментов. После этого на экране появится мастер экспорта настроек (см. Рис. 66).

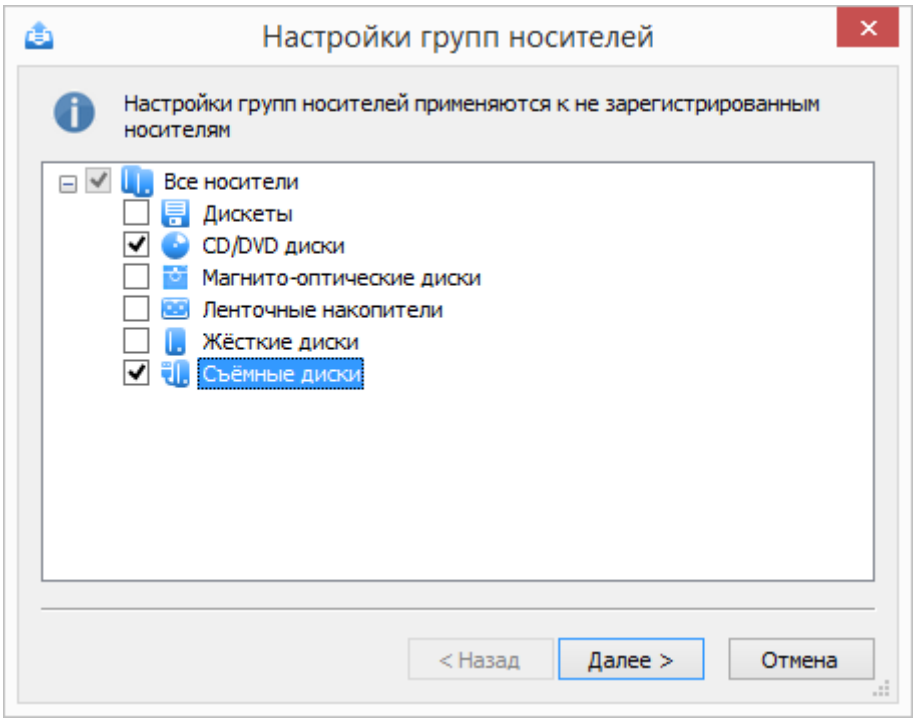


Рис. 66. Экспорт настроек групп носителей.

В данном окне необходимо выбрать группы носителей, параметры которых будут экспортироваться, и нажать кнопку Далее >.

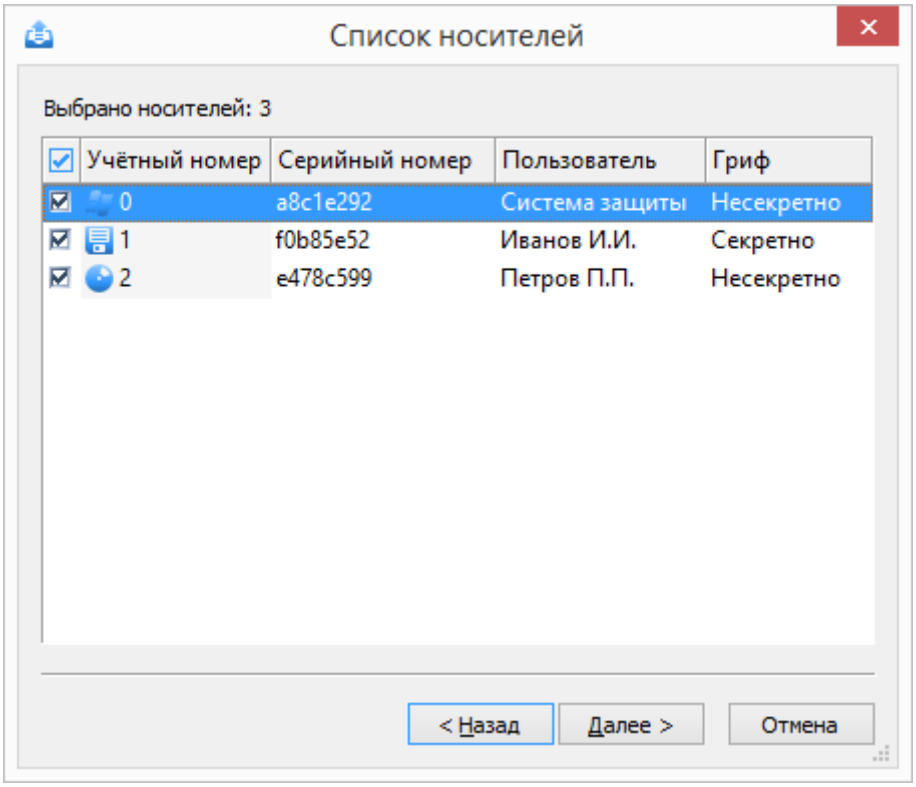


Рис. 67. Экспорт списка носителей.

На экране появится окно экспорта списка зарегистрированных носителей информации (см.Рис. 67). В данном окне необходимо выбрать записи о зарегистрированных носителях информации, настройки которых будут экспортироваться. Если администратор системы защиты не выбрал для экспорта ни одного носителя, или группы носителей, кнопка Далее > будет недоступна. В следующем окне (см. Рис. 68), администратор системы защиты может выбрать перечень компьютеров, на которые будут экспортированы настройки, а также выбрать файл, в котором эти настройки будут сохранены. Для начала экспорта настроек необходимо нажать кнопку Экспорт.

Если на компьютере, куда экспортируются настройки, уже присутствует зарегистрированный носитель с таким серийным номером и установлен флаг в поле **Требовать подтверждение изменения параметров носителей**, администратору будет предложено заменить настройки. В противном случае, замена на новые настройки будет выполнена автоматически.

В списке компьютеров будут отображены только те компьютеры, к которым в данный момент возможен доступ с правами администратора системы защиты.

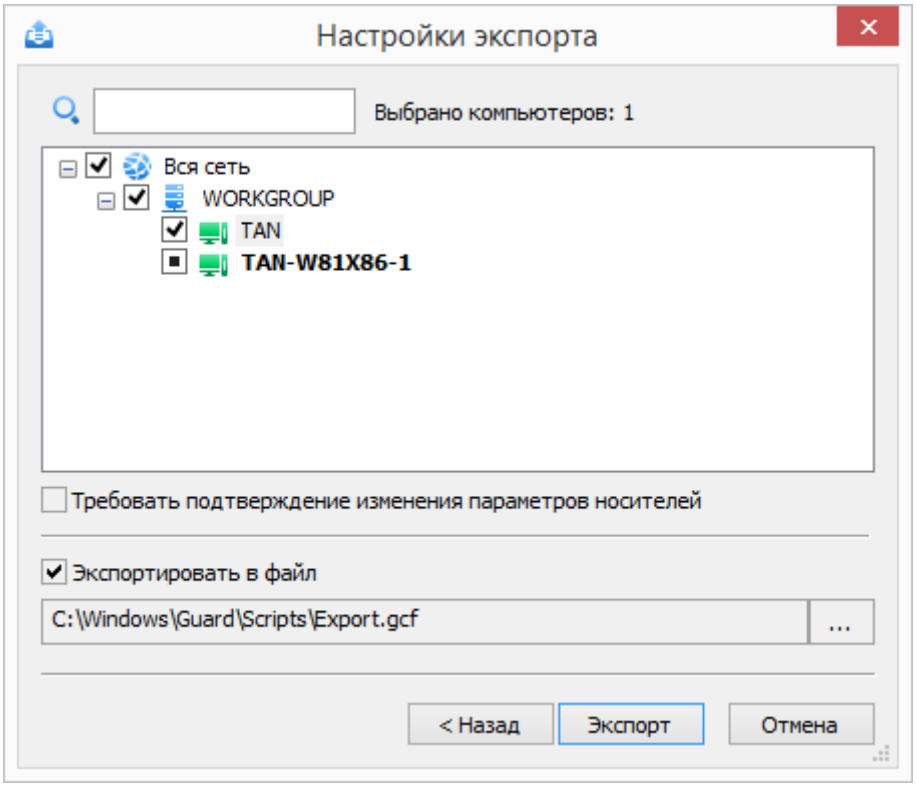


Рис. 68. Определение параметров экспорта настроек.

Импорт настроек

При наличии файла с экспортированными настройками групп носителей и носителей информации его можно импортировать на другом компьютере с установленной СЗИ «Страж NT».

Для импорта настроек необходимо выбрать пункт меню **Носители | Импорт...**, или нажать соответствующую кнопку на панели инструментов. После этого на экране появится окно (см. Рис. 69), на котором размещены две вкладки: **Группы носителей** и **Список носителей.**

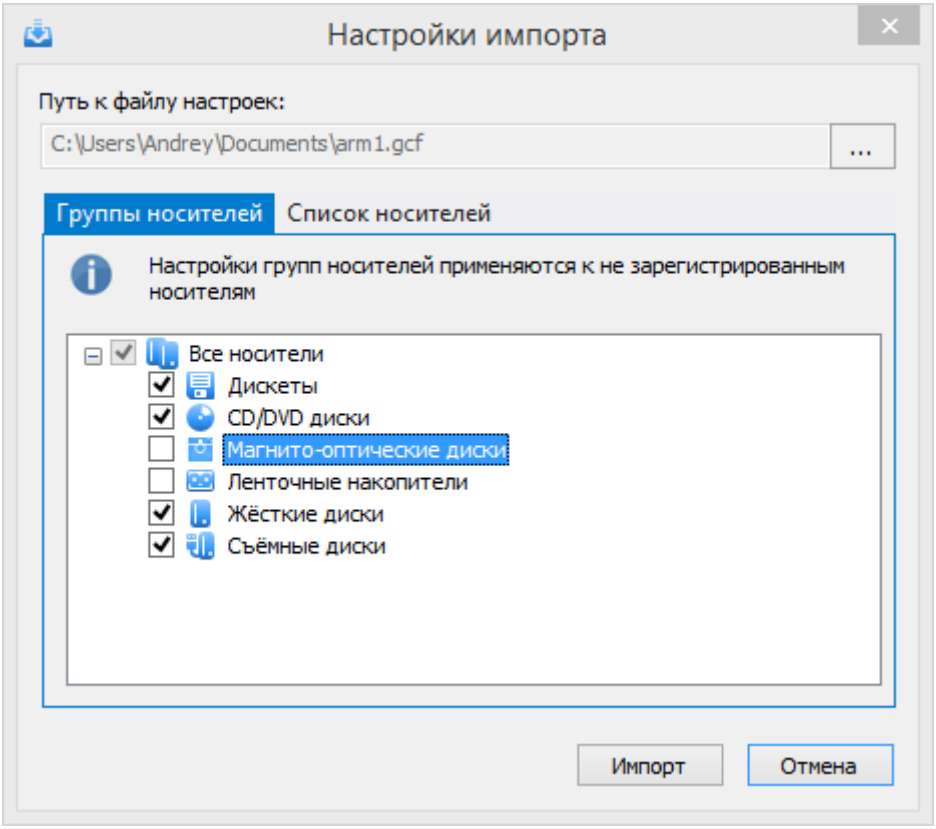


Рис. 69. Параметры импорта настроек групп носителей.

После выбора файла с сохраненными настройками дерево типов носителей станет доступно для редактирования, а в списке носителей (см. Рис. 70) появится информация о настройках сохранённых носителей.

Если на компьютере, уже присутствует зарегистрированный носитель с таким серийным номером и установлен флаг в поле **Требовать подтверждение изменения параметров носителей**, администратору системы защиты будет предложено заменить существующие настройки. В противном случае, замена на новые настройки будет выполнена автоматически. После нажатия кнопки Импорт выбранные настройки будут импортированы.

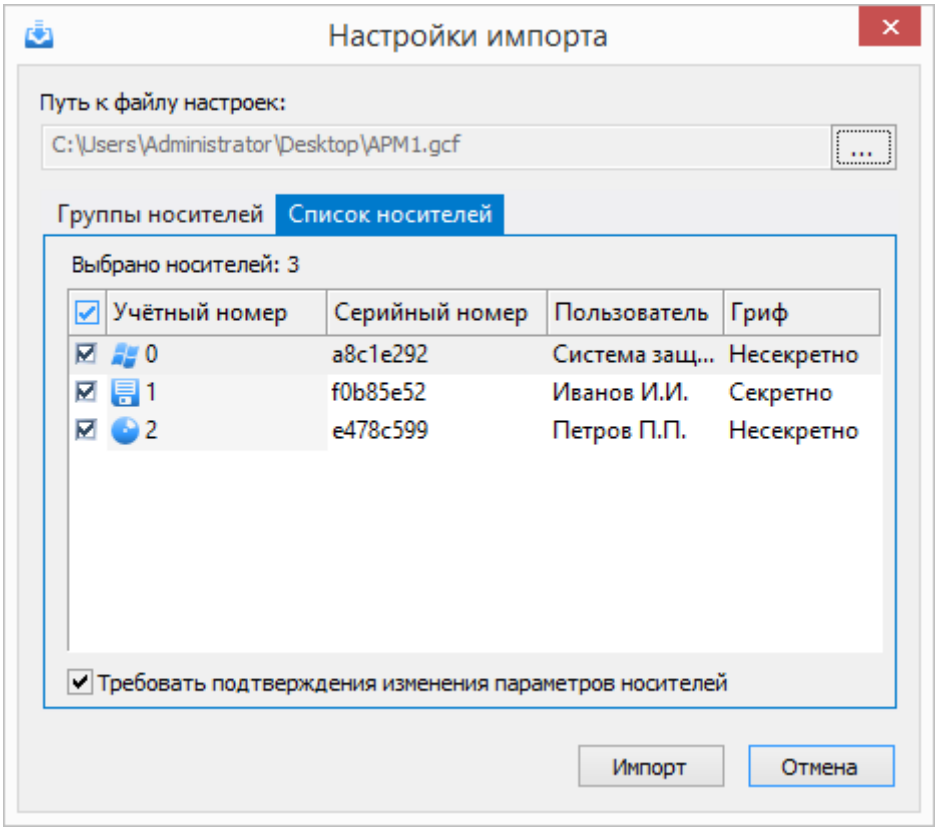


Рис. 70. Параметры импорта настроек носителей информации.

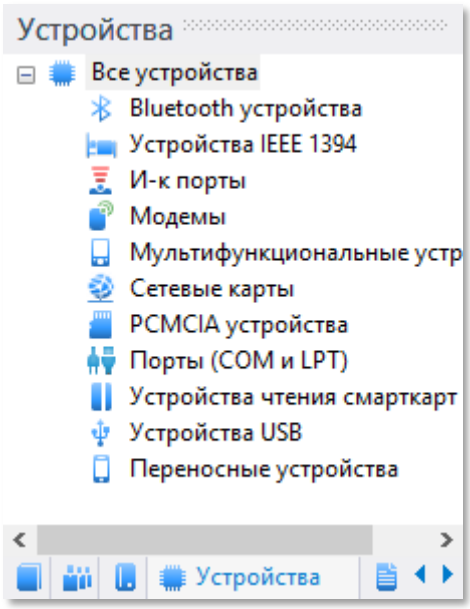
Контроль устройств

В данной главе приводятся сведения о работе с подсистемой контроля устройств. Описаны интерфейсы утилит администратора системы защиты при работе с подсистемой, а также его типовые действия при управлении политиками использования групп устройств.

Общие сведения

СЗИ «Страж NT» контролирует доступ к устройствам, присутствующим в компьютере, через подсистему контроля устройств, которая позволяет устанавливать разрешения на различные типы устройств. В соответствии с разрешениями после интерактивного входа пользователя в систему устройства, запрещенные данному пользователю, будут отключены. При попытке подключить устройство, запрещенное пользователю, подсистема контроля устройств отключит данное устройство. В СЗИ «Страж NT» контролируются следующие типы устройств:

- Bluetooth устройства;
- устройства IEEE 1394;
- инфракрасные порты;
- модемы;
- мультифункциональные устройства;
- сетевые карты;
- PCMCIA устройства;
- порты (COM и LPT);
- устройства чтения смарткарт;
- устройства USB;
- переносные устройства.



Контроль устройств осуществляется с помощью вкладки **Контроль устройств** программы **Консоль управления** (см. Рис. 71). В панели устройств будет отображён список групп устройств, определяющих типы устройств.

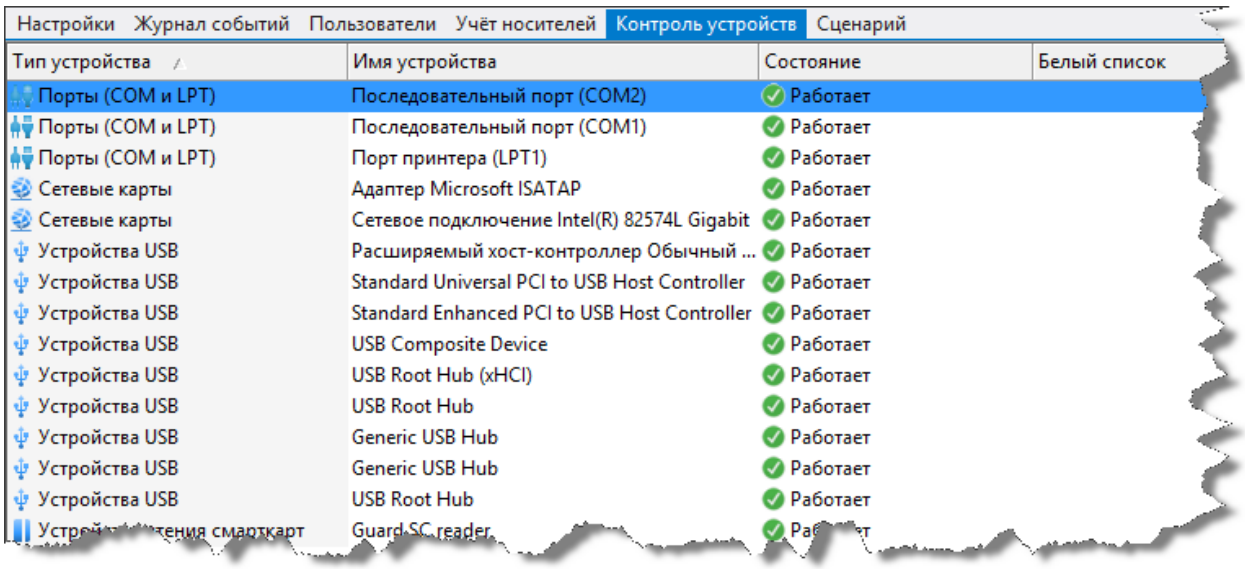


Рис. 71. Список устройств в системе.

Список устройств представляет собой таблицу, содержащую следующие поля.

Поле	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**).
Белый список	Определяет присутствие устройства в списке исключений

Администратор системы защиты имеет возможность сортировать список устройств по любому из перечисленных полей. Кроме того, администратор может осуществлять выборку устройств по типам. Для этого необходимо выбрать соответствующую группу устройств на панели устройств. По умолчанию, в списке отображаются устройства всех типов.

Просмотр параметров устройства

В списке устройств приведены основные параметры устройства, более подробную информацию об устройстве можно увидеть, вызвав окно свойств устройства. Для вызова окна свойств устройства (см. Рис. 72) необходимо выбрать пункт меню **Устройства | Свойства...** или нажать соответствующую кнопку на панели инструментов. В окне

свойств устройства отображена информация о типе, имени, состоянии, изготовителе и размещении устройства.

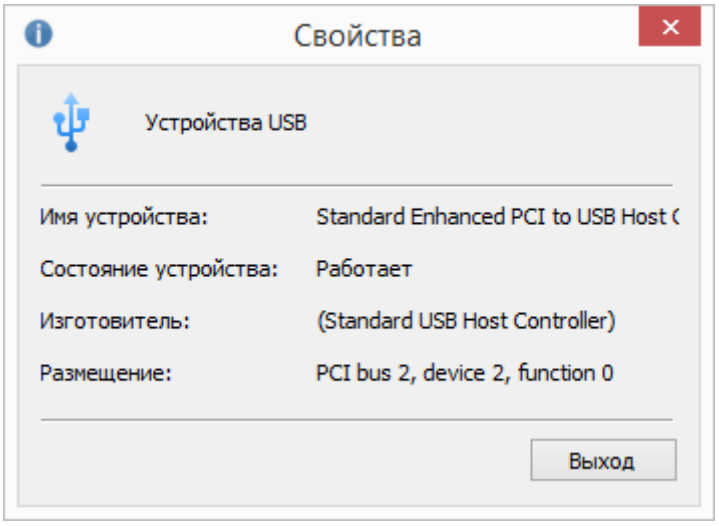


Рис. 72. Свойства устройства.

Редактирование свойств для группы устройств

При установке системы защиты для всех групп устройств устанавливаются разрешения по умолчанию: всем пользователям, системе, локальным администраторам – полный доступ.

Для редактирования разрешений по умолчанию необходимо выбрать пункт **Свойства...** контекстного меню группы или дважды кликнуть на соответствующей группе устройств в панели устройств. При этом откроется окно редактора разрешений (см. Рис. 73), в котором можно менять разрешения для выбранной группы устройств.

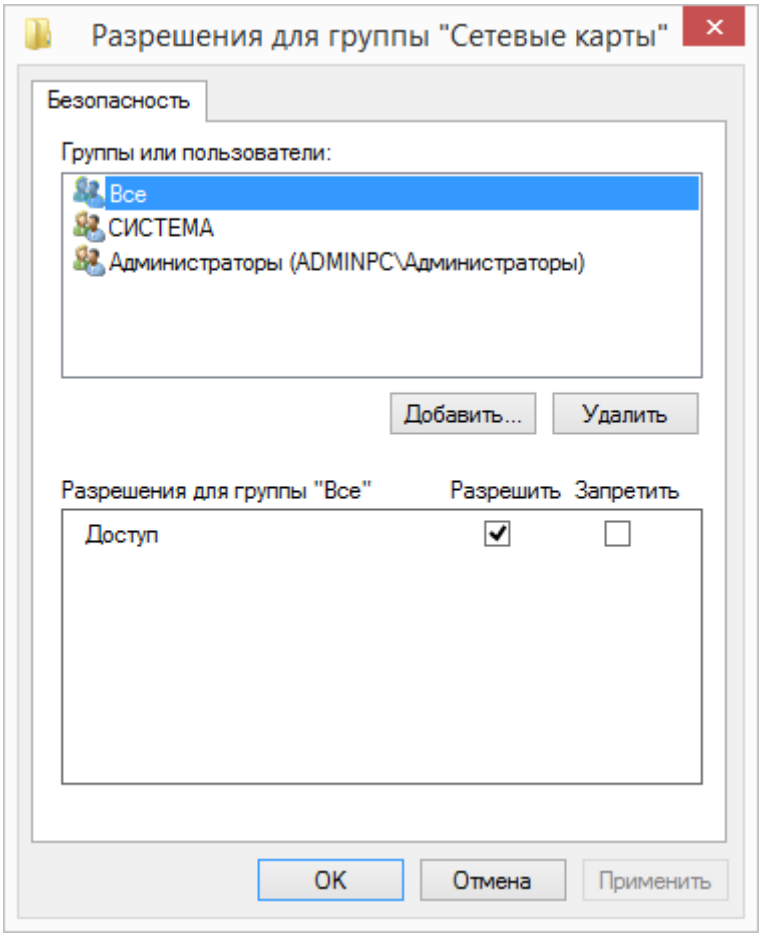


Рис. 73. Редактирование разрешений для группы устройств.

Работа со списком исключений

В СЗИ «Страж NT» реализована работа с «белым списком» устройств или списком исключений. Для устройства, которое добавлено в список исключений, не действуют разрешения, заданные для соответствующей группы устройств. Для добавления устройства в список исключений необходимо выбрать его в списке устройств, вызвать для него контекстное меню и выбрать пункт **Добавить в исключения**. Для удаления устройства из этого списка необходимо выбрать пункт меню **Удалить из исключений**. Существует возможность добавить в исключения все устройства, присутствующие в системе. Для этого необходимо выбрать пункт меню **Устройства | Исключения | Сформировать список исключений.** Для удаления всех устройств из списка исключений необходимо выбрать пункт меню **Устройства | Исключения | Очистить список исключений.**

В СЗИ «Страж NT» реализована возможность создания замкнутой аппаратной среды. Создание замкнутой аппаратной среды подразумевает добавление устройств в список исключений и назначение запрещающих политик для групп устройств. Замкнутую

аппаратную среду можно создать для всех поддерживаемых СЗИ устройств или для определённых типов устройств. Для создания замкнутой аппаратной среды для всех поддерживаемых устройств необходимо выбрать пункт меню **Устройства | Сформировать замкнутую среду.** При этом все поддерживаемые устройства, присутствующие в системе, будут добавлены в список исключений, а для групп устройств будут установлены настройки, запрещающие их использования всеми пользователями, кроме администраторов.

Для сброса настроек необходимо выбрать пункт меню **Устройства | Сбросить настройки.** При этом все устройства будут удалены из списка исключений, а для групп устройств будут установлены настройки по умолчанию, а именно полный доступ для следующих локальных субъектов доступа: Все, СИСТЕМА, Администраторы.

Для создания замкнутой аппаратной среды для группы устройств необходимо выбрать пункт **Сформировать замкнутую среду** контекстного меню соответствующей группы устройств. Для сброса настроек для группы устройств необходимо выбрать пункт **Сбросить настройки** контекстного меню группы устройств.

Экспорт настроек

Для удобства распространения выполненных настроек групп устройств на другие компьютеры существует механизм экспорта настроек. Экспорт настроек можно осуществлять как через локальную сеть, так и через файл настроек, например, при отсутствии сети.

При экспорте настроек в списках контроля доступа, определяющих дискреционные права к группам устройств, указываются идентификаторы безопасности пользователей и групп пользователей (Security Identifier или SID). В этой связи полностью корректное применение дискреционных прав по доступу к указанным объектам (при импорте их из файла на другом компьютере или экспорте по сети на другой компьютер) возможно только для пользователей и групп пользователей, имеющих полностью идентичные SIDы на всех компьютерах. Таковыми, в частности, являются пользователи и группы пользователей:

- одного домена;
- имеющие хорошо известные идентификаторы безопасности (Well-known security identifiers), например, группы Все (Everyone), Администраторы (Administrators) и т.п..

Для экспорта настроек необходимо выбрать пункт меню **Устройства | Экспорт...**, или нажать соответствующую кнопку на панели инструментов. После этого на экране появится мастер экспорта настроек (см. Рис. 74).

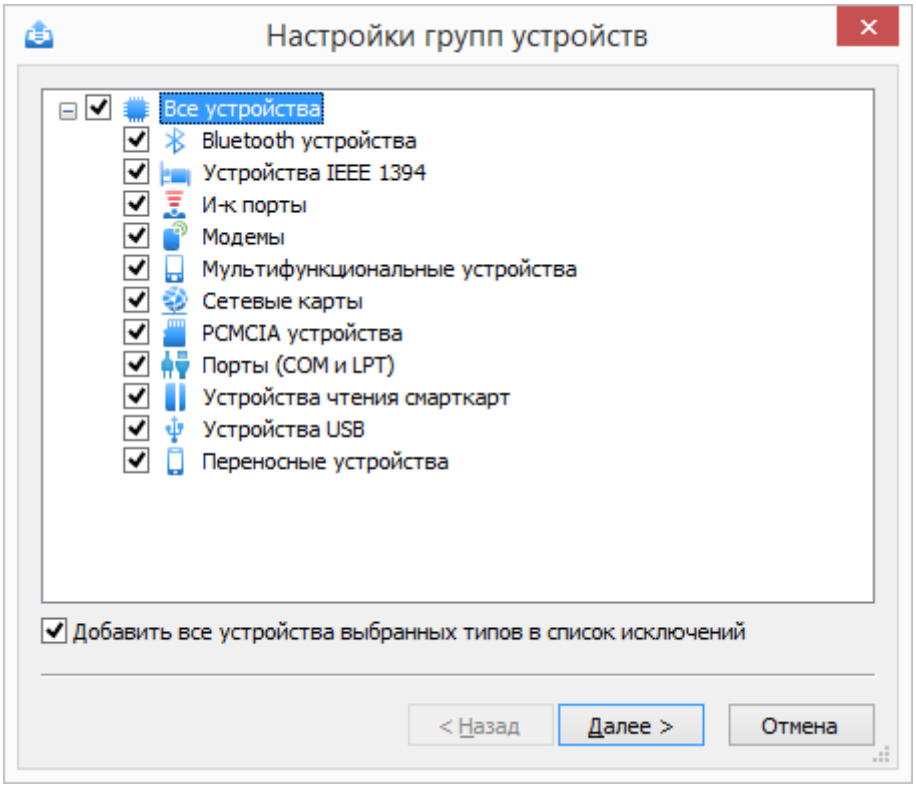


Рис. 74. Экспорт настроек групп устройств.

В данном окне необходимо выбрать группы устройств, параметры которых будут экспортироваться, и нажать кнопку Далее > .

В следующем окне (см. Рис. 75), администратор системы защиты может выбрать перечень компьютеров, на которые будут экспортированы настройки, а также выбрать файл, в котором эти настройки будут сохранены. Для начала экспорта настроек необходимо нажать кнопку Экспорт .

В списке компьютеров будут отображены только те компьютеры, к которым в данный момент возможен доступ с правами администратора системы защиты.

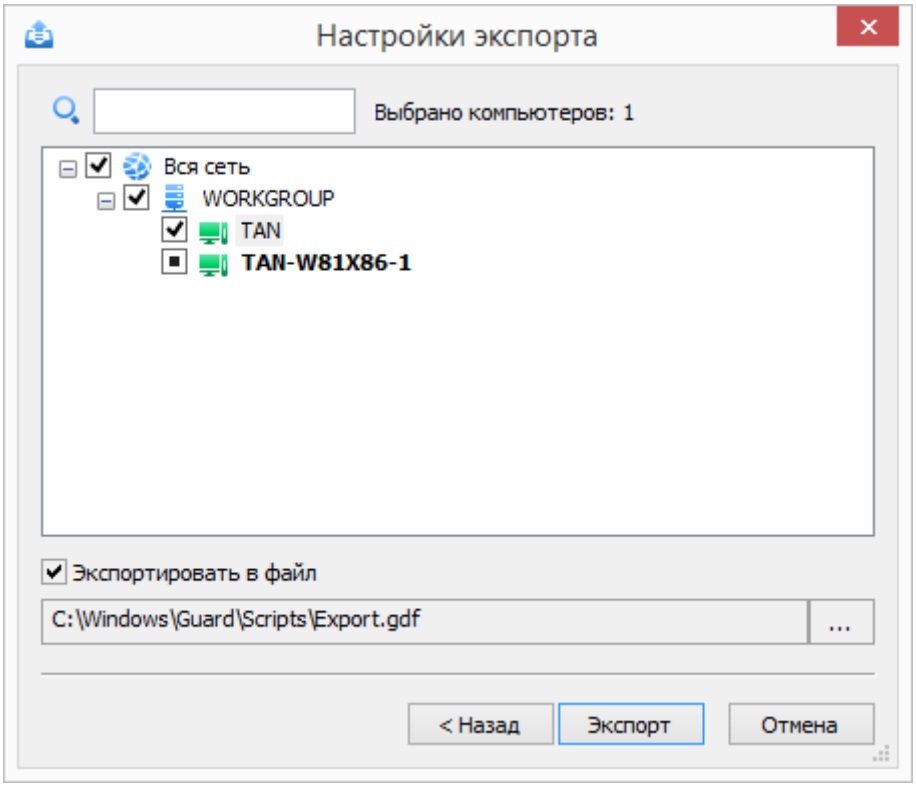


Рис. 75. Определение параметров экспорта.

Импорт настроек

При наличии файла с экспортированными настройками групп устройств его можно импортировать на другом компьютере с установленной СЗИ «Страж NT».

Для импорта настроек необходимо выбрать пункт меню **Устройства | Импорт...**, или нажать соответствующую кнопку на панели инструментов. После этого на экране появится окно, содержащее дерево групп устройств, которое станет доступно для редактирования после выбора файла с сохраненными настройками (см. Рис. 76). После нажатия кнопки Импорт, настройки будут импортированы.

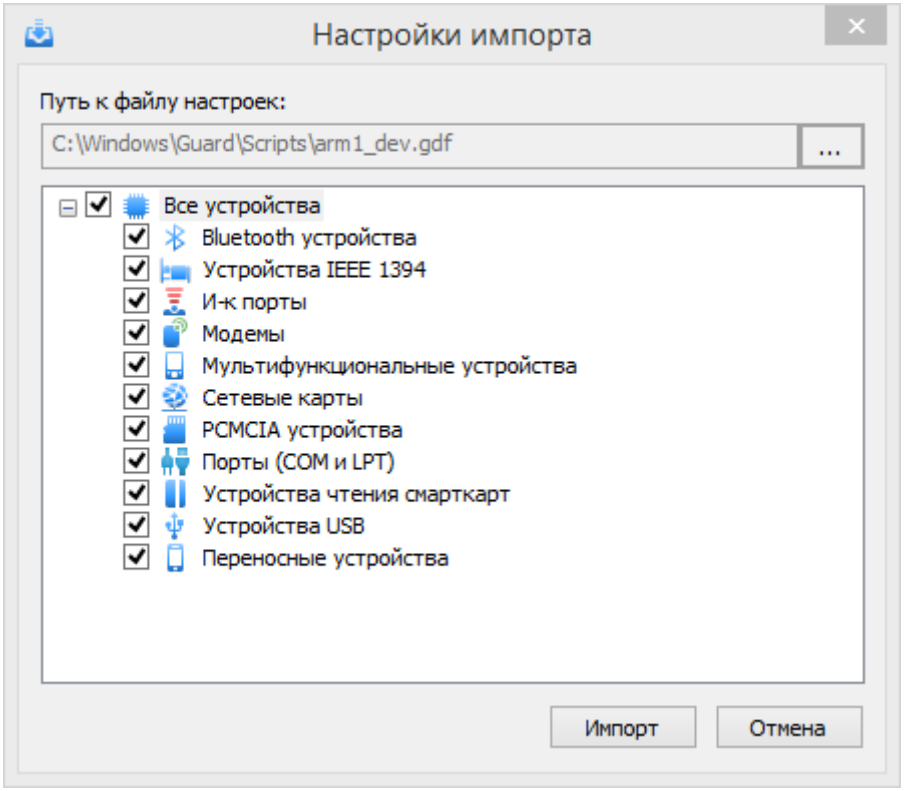


Рис. 76. Параметры импорта настроек.

Целостность ресурсов

В данной главе даются сведения о механизмах системы защиты, отвечающих за целостность ресурсов. Описываются сценарии выполнения администраторами системы защиты настройки и контроля целостности защищаемых ресурсов.

Общие сведения

В системе защиты предусмотрен контроль целостности защищаемых файлов и файлов системы защиты. Контроль целостности файлов может осуществляться автоматически при загрузке операционной системы, при открытии файлов на чтение и по запросу. СЗИ «Страж NT» обеспечивает контроль целостности файлов по следующим параметрам:

- наличие файла;
- контрольная сумма данных, содержащихся в файле. Для контрольного суммирования данных применяется алгоритм вычисления имитовставки ГОСТ 28147-89;
- длина файла;
- дата и время последней модификации.

При контроле целостности файлов параметры контроля проверяются в последовательности, приведенной выше. При нарушении какого-либо параметра подсистемой регистрации фиксируется факт нарушения целостности, и дальнейшая проверка не производится.

В рамках этой же подсистемы реализован контроль целостности исполняемых файлов системы защиты. Контроль целостности на файлы системы защиты устанавливается автоматически при установке системы защиты и его параметры не могут быть изменены.

При обнаружении нарушения целостности файлов, параметры которых контролируются автоматически при загрузке операционной системы, после загрузки рабочего стола у пользователя на экран появляется окно с сообщением, как показано на Рис. 77. При появлении такого сообщения необходимо открыть журнал событий и проанализировать, у каких файлов и по какой причине нарушена целостность.

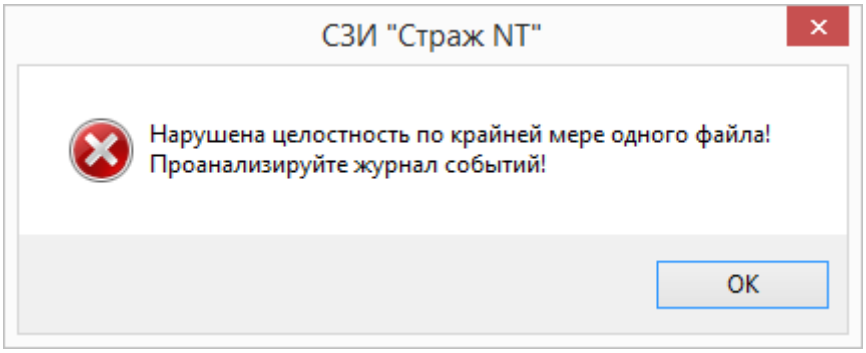
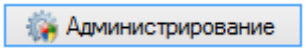


Рис. 77. Сообщение о нарушении целостности файлов.

Настройка контроля целостности ресурсов

Установку параметров целостности на файлы можно выполнить с помощью любого файлового менеджера, например, программы **Менеджер файлов** и только в режиме администрирования. Для установки параметров целостности необходимо включить режим администрирования, выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Целостность** (см. Рис. 78). Также режим администрирования можно включить, нажав на кнопку 

на самом диалоге.

Установка флага в поле **Контролировать автоматически** означает, что контроль целостности выбранных ресурсов будет осуществляться автоматически при загрузке операционной системы. Поля группы **Контролируемые атрибуты** определяют, какие именно параметры будут контролироваться. Поля группы **При нарушении целостности** определяют реакцию системы защиты при нарушении целостности выбранных ресурсов:

- **Блокировать открытие файла** – при попытке открытия файла на чтение произойдет отказ в доступе с ошибкой нарушения целостности.
- **Блокировать загрузку системы** – при загрузке операционной системы произойдет блокирование загрузки с регистрацией факта нарушения в журнале событий. Действует только для файлов на системном диске компьютера при автоматическом контроле целостности во время загрузки операционной системы.
- **Пересчитать параметры** – выполнится регистрация факта нарушения в журнале событий с последующим пересчетом параметров контроля целостности для данного файла.

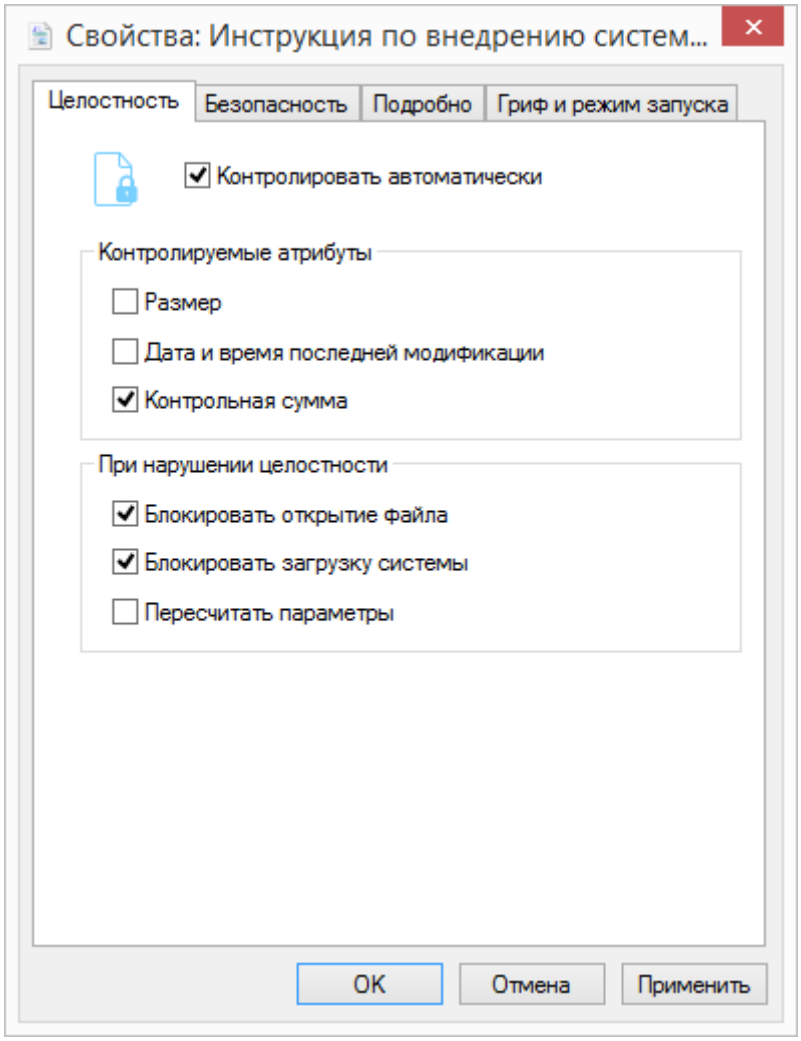


Рис. 78. Установка параметров целостности.

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

При установке флага **Сменить параметры для файлов в подпапках** все выбранные параметры будут установлены для всех файлов в дочерних подпапках.

Для изменения параметров целостности выбранных объектов необходимо установить флаги в соответствующие поля. Для сохранения сделанных изменений нажать кнопку OK или Применить.

Пересчет контрольных сумм файлов СЗИ

СЗИ «Страж NT» контролирует целостность исполняемых файлов системы защиты. В некоторых случаях контрольная сумма файлов СЗИ может быть изменена. Например, если снять СЗИ с сохранением настроек, и переустановить её с другим идентификатором администратора системы защиты, контрольная сумма файлов будет не актуальна. В этом случае при загрузке операционной системы на экран будет выдано сообщение о нарушении целостности файлов СЗИ (см. Рис. 79).

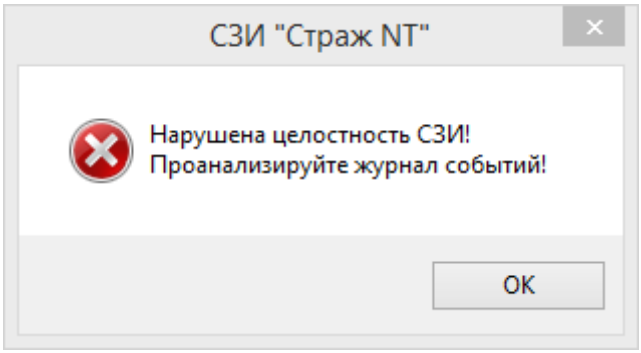


Рис. 79. Сообщение о нарушении целостности файлов СЗИ.

Администратор системы защиты имеет возможность обновить контрольные суммы файлов СЗИ с помощью вкладки **Настройки** программы **Консоль управления.** Для этого необходимо выбрать пункт меню **Настройки ресурсов | Пересчитать контрольные суммы файлов СЗИ**. После завершения процесса обновления контрольных сумм файлов, на экран будет выдано окно с результатом пересчета (см. Рис. 80).

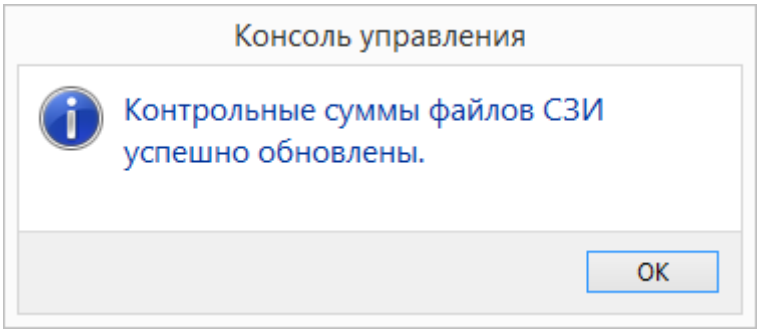


Рис. 80. Сообщение об успешном пересчете контрольных сумм файлов СЗИ.

Если процесс пересчёта завершился с ошибкой, на экран будет выдано сообщение об ошибке. Подробная информация о процессе обновления контрольных сумм файлов СЗИ содержится в файле **%Temp%\GInit.log**.

Регистрация событий

В данной главе даются сведения о подсистеме регистрации событий, категориях регистрируемых событий и правил их регистрации. Описываются действия администратора системы защиты по настройке параметров дополнительного аудита защищаемых ресурсов, а также настройке списка регистрируемых событий.

Общие сведения

В СЗИ «Страж NT» реализована собственная подсистема регистрации событий. Все регистрируемые события включены в следующие категории:

- события контроля целостности;
- события входа в систему;
- события запуска программ;
- события доступа к объектам;
- события действий администратора;
- события управления объектами доступа;
- события управления пользователями;
- события управления носителями;
- события управления устройствами;
- события системы защиты;
- события печати.

В категорию входа в систему включены события успешного входа в систему, а также все ошибки идентификации пользователей. Категория запуска программ включает события успешного запуска процессов, попытки запуска неразрешенных программ, попытки установки текущего допуска, режима администрирования и автозапуска. Категория доступа к объектам объединяет подключение томов, попытки обращения к защищаемым файлам и папкам, а также установку атрибутов безопасности на файлы. В категорию контроля целостности входят все факты нарушения целостности защищаемых файлов. События из перечисленных выше категорий, а также действия администратора и события системы защиты, регистрируются средствами ядра системы защиты. Остальные категории событий регистрируются в соответствующих подсистемах.

При возникновении какого-либо события регистрируются следующие параметры:

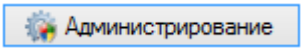
- дата и время;
- код события;
- имя пользователя;
- другие параметры, зависящие от категории события.

Для регистрации событий доступа к защищаемым файлам и папкам в системе защиты предусмотрен специальный атрибут безопасности, который называется **Дополнительный аудит** и может быть установлен как на процесс, так и на любой защищаемый файл или папку. При запросе на доступ к файлу или папке на открытие, чтение, запись или изменение регистрация события безопасности происходит при выполнении любого из следующих условий:

- параметры дополнительного аудита текущего процесса, которые установлены на исполняемом файле, требуют регистрации события безопасности;
- текущий допуск процесса выше «Несекретно», и произошел отказ доступа к запрашиваемому ресурсу;
- параметры дополнительного аудита, установленные на файле или папке, а в случае их отсутствия параметры дополнительного аудита родительской папки, требуют регистрации события безопасности;
- файл или папка имеют гриф выше «Несекретно» и при этом файл не является исполняемым, т.е. файл имеет режим запуска «Запрещен».

При запросах на переименование регистрация события происходит во всех случаях, когда на переименовываемый объект установлены какие-либо параметры безопасности. Запросы на удаление файлов регистрируются всегда для файлов с грифом выше «Несекретно», а также для всех файлов при включенном в настройках системы защиты флаге в поле **Гарантированная очистка всех удаляемых файлов**.

Настройка параметров дополнительного аудита

Установку параметров дополнительного аудита на папки и файлы можно выполнить с помощью любого файлового менеджера, например, программы **Менеджер файлов** и только в режиме администрирования. Для установки параметров дополнительного аудита необходимо включить режим администрирования, выбрать пункт **Свойства** из контекстного меню выбранных объектов, и в появившемся окне свойств выбрать вкладку **Гриф и режим запуска** (см. Рис. 81). Также режим администрирования можно включить, нажав на кнопку 

на самом диалоге.

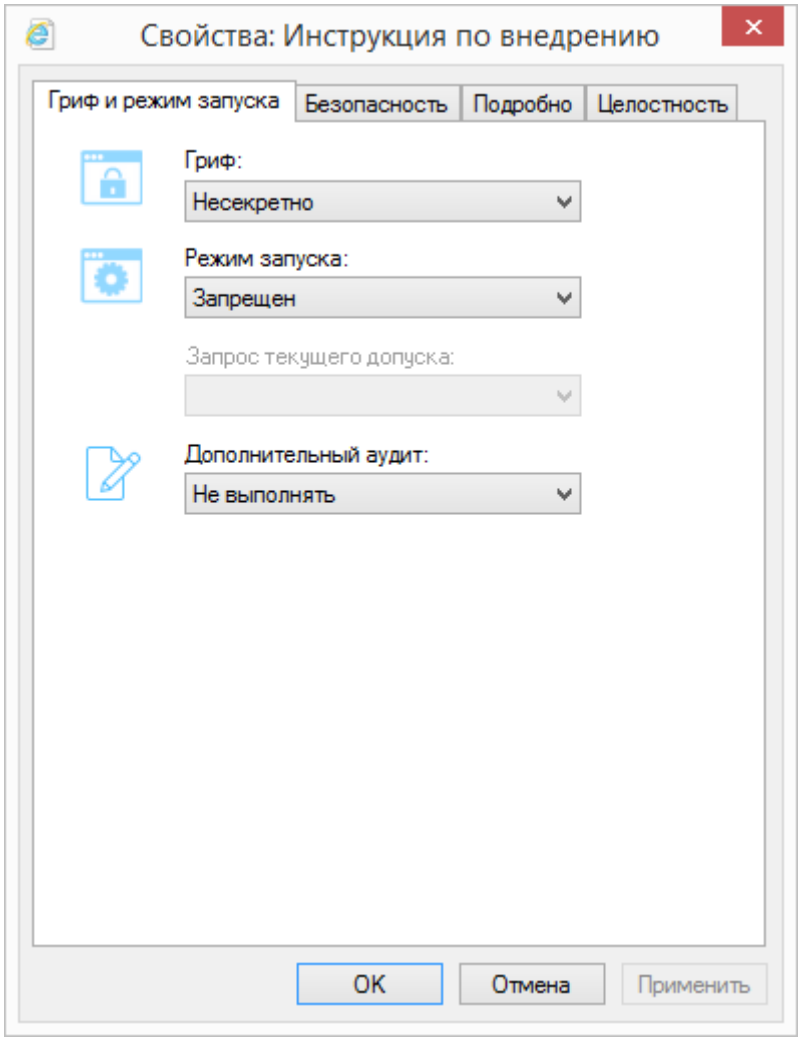


Рис. 81. Настройка параметров дополнительного аудита.

Для изменения параметров дополнительного аудита выбранных объектов необходимо выбрать соответствующее значение из раскрывающегося списка в поле **Дополнительный аудит:**

- «Не выполнять» – параметры дополнительного аудита снимаются.
- «Аудит успехов» – регистрации подлежат только успешные события.
- «Аудит отказов» – регистрации подлежат только неуспешные события.
- «Полный аудит» – регистрации подлежат все события.

Для сохранения сделанных изменений нажать кнопку OK или Применить.

Настройка списка регистрируемых событий

Администратор системы защиты имеет возможность редактировать список регистрируемых событий. Настройка перечня регистрируемых событий осуществляется

при помощи вкладки **Настройки** программы **Консоль управления**. Для отображения окна параметров регистрации событий СЗИ необходимо выбрать пункт **Настройки регистрации** (см. Рис. 82).

По умолчанию включена регистрация всех событий за исключением открытия, чтения и отказа в доступе к объектам.

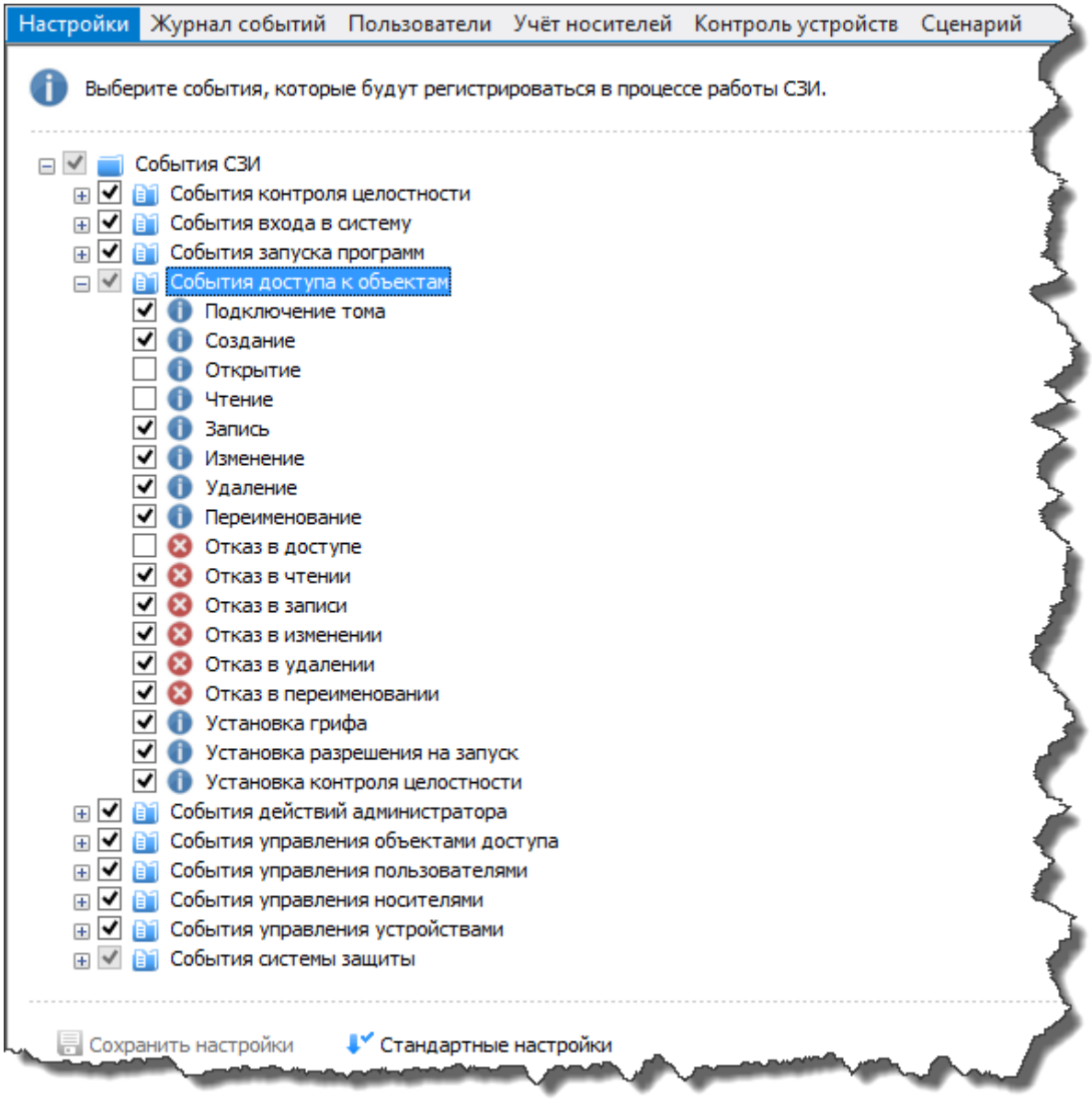


Рис. 82. Настройка перечня регистрируемых событий.

Для сохранения настроек необходимо нажать кнопку Сохранить настройки, для возврата к настройкам по умолчанию – кнопку Стандартные настройки.

Работа с журналами

В данной главе приводятся сведения о работе с журналом событий СЗИ «Страж NT», рассматриваются соответствующие механизмы системы защиты, утилиты администратора, их экранные формы и параметры. Также описаны типовые действия администратора системы защиты при работе с журналом событий.

Общие сведения

Подсистема регистрации кроме регистрации запросов на доступ к ресурсам компьютера также обеспечивает их хранение и возможность выборочного ознакомления с регистрационной информацией. Хранение зарегистрированных событий системы защиты осуществляется в файле журнала событий, который расположен по пути **%SystemRoot%\Guard\GReport.mdb** и имеет формат базы данных **Microsoft Access**. Работа с журналом событий осуществляется с помощью вкладки **Журнал событий** программы **Консоль управления**, перейдя в которую администратор системы защиты может 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 или отдельной выборки событий;
- очистка журнала.

При открытии вкладки **Журнал событий** программы **Консоль управления** в основном окне отображается список событий (см. Рис. 83).

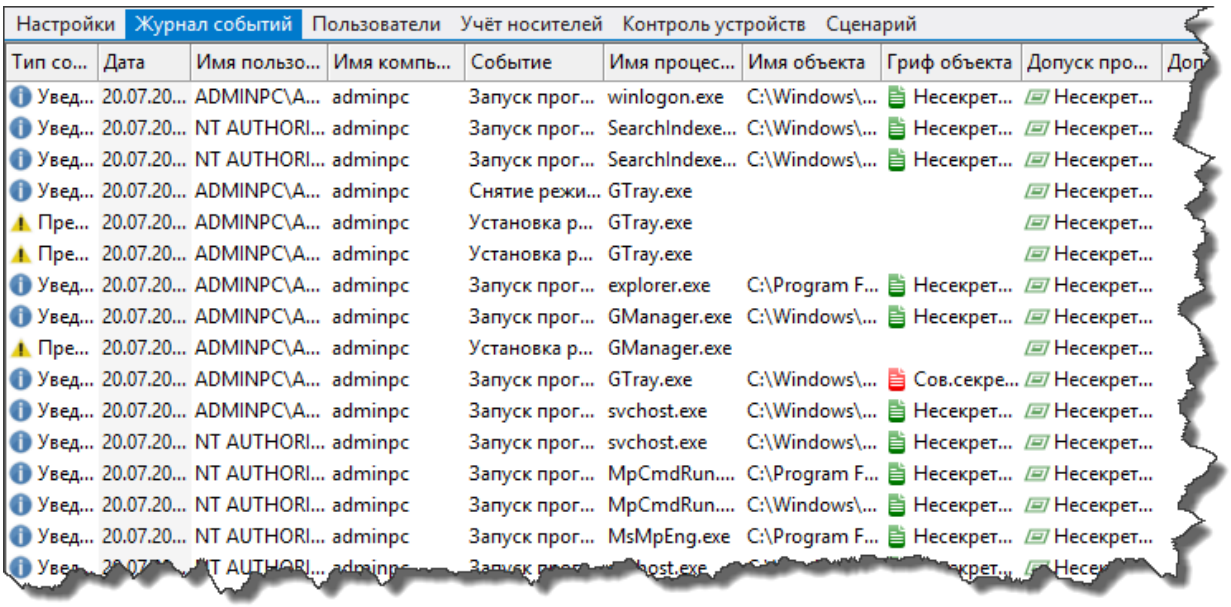


Рис. 83. Общий вид журнала событий.

Список событий представляет собой таблицу, содержащую следующие поля.

Свойство	Описание
Тип события	Определяет тип события (уведомление, предупреждение, ошибка).
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.
Дополнительно	Определяет дополнительную информацию о событии.

Инструменты таблицы списка событий позволяют менять порядок и ширину столбцов, сортировать записи, 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 **Столбцы**. В данном меню администратор системы защиты может отметить те столбцы, которые будут отображаться в списке событий.

Просмотр свойств события

Для отображения всех свойств события необходимо выделить его в списке событий и выбрать пункт меню **События | Свойства события...** или дважды нажать на событии на левую кнопку мыши. При этом на экране появится окно (см. Рис. 84), в котором расположены две вкладки: **Основные** и **Печать**. Вкладка **Печать** (см. Рис. 85) доступна только для событий печати документов.

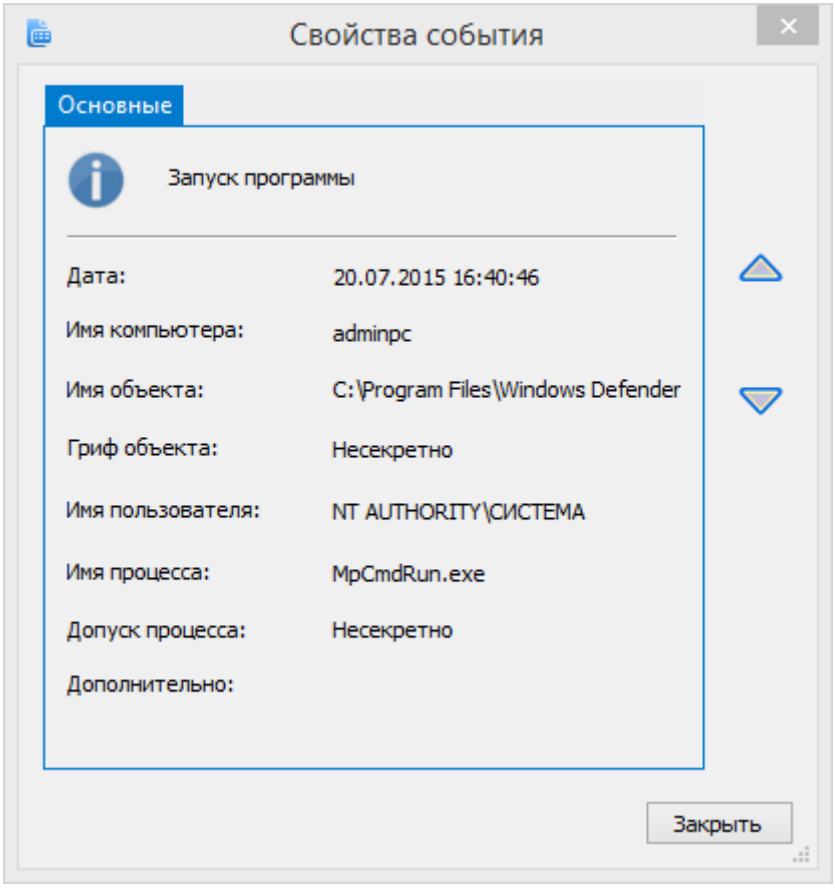


Рис. 84. Свойства события - Основные.

Для перемещения по списку событий служат кнопки  и  .

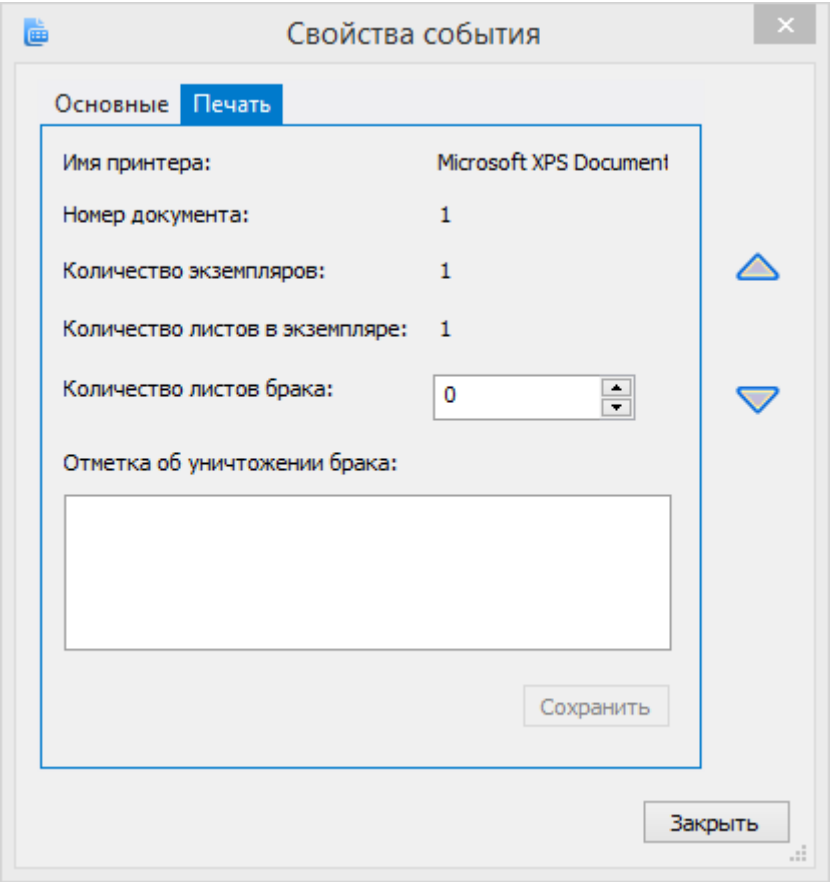


Рис. 85. Свойства события - Печать.

Поля **Количество листов брака** и **Отметка об уничтожении** брака доступны для самостоятельного редактирования.

Открытие и сохранение журнала

При запуске программы **Консоль управления** и выборе вкладки **Журнал событий** по умолчанию будет отображён текущий журнал событий локального компьютера, находящийся в файле **%SystemRoot%\Guard\GReport.mdb**. Для открытия другого файла журнала (например, архивов журналов событий) 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**.

При выборе пункта меню **Журнал | Сохранить выборку…** будет предложено сохранить в файл не весь журнал, а ту выборку, которая в настоящий момент представлена на

экране. Выборка осуществляется применением инструментов группировки и фильтрации событий.

Группировка и фильтрация событий

Для удобства просмотра событий в СЗИ «Страж NT» реализован механизм группировки событий. С помощью групп событий администратор системы защиты имеет возможность группировать события по некоторому списку признаков.

Все группы событий отображаются на панели групп событий. При выборе группы на панели групп событий, в списке событий отображаются только события выбранной группы.

Для добавления группы событий необходимо выбрать пункт меню **Группы событий | Добавить…** либо выбрать пункт **Добавить группу**… контекстного меню на панели **Группы событий**. При этом на экране появится окно (см. Рис. 86), которое состоит из трёх вкладок: **Свойства**, **События** и **Параметры**.

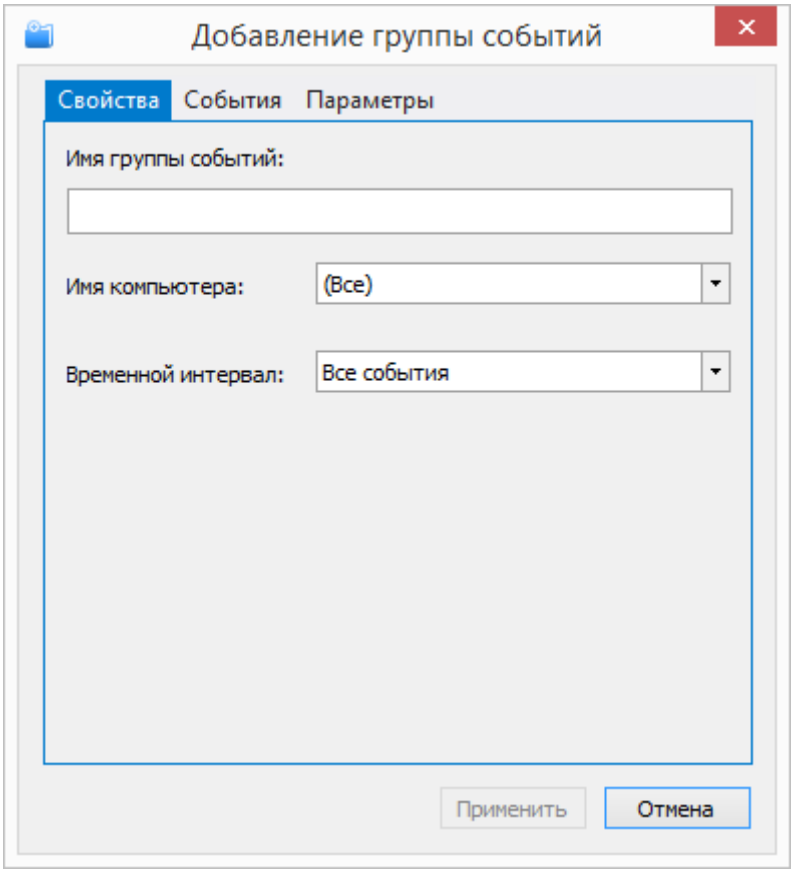


Рис. 86. Добавление группы событий - Свойства.

Вкладка **Свойства** предназначено для указания имени группы событий, имени компьютера и временного интервала. Временной интервал может быть задан как с точным

указанием границ даты и времени наступления события, так и в «относительном» формате. К «относительным» относятся следующие интервалы:

- За последний час;
- За последние 24 часа;
- За последние 7 дней;
- За последние 30 дней.

Вкладка **События** (см. Рис. 87) предназначена для настройки категорий и перечня отображаемых событий.

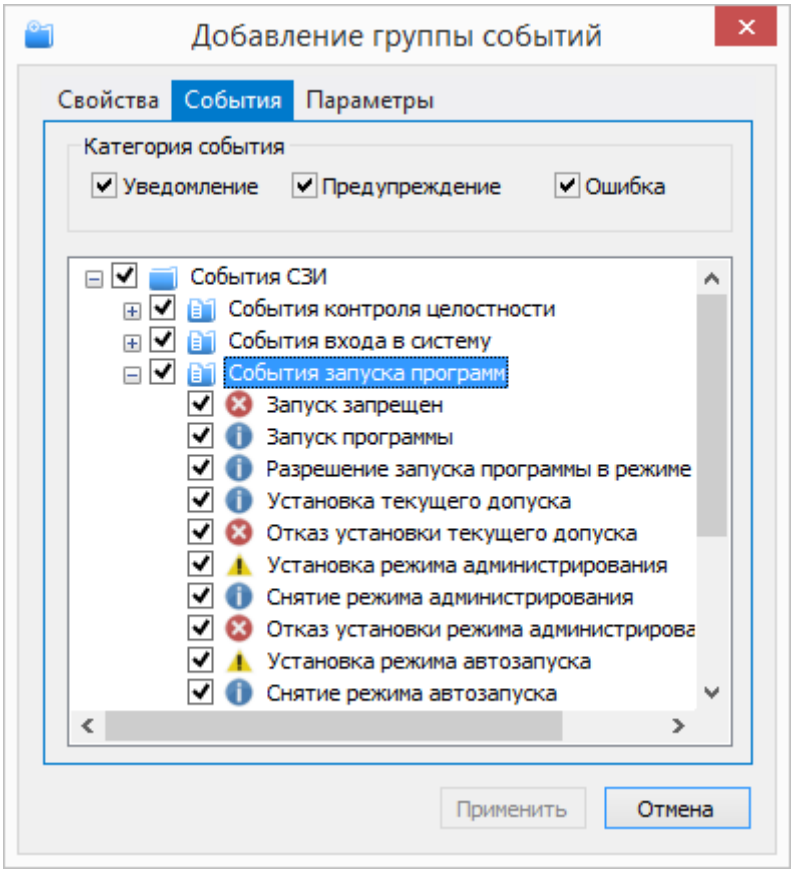


Рис. 87. Добавление группы событий - События.

Вкладка **Параметры** (см. Рис. 88) позволяет осуществлять группировку событий по следующим признакам:

- имя объекта;
- гриф объекта;
- имя пользователя;
- имя процесса;
- допуск процесса.

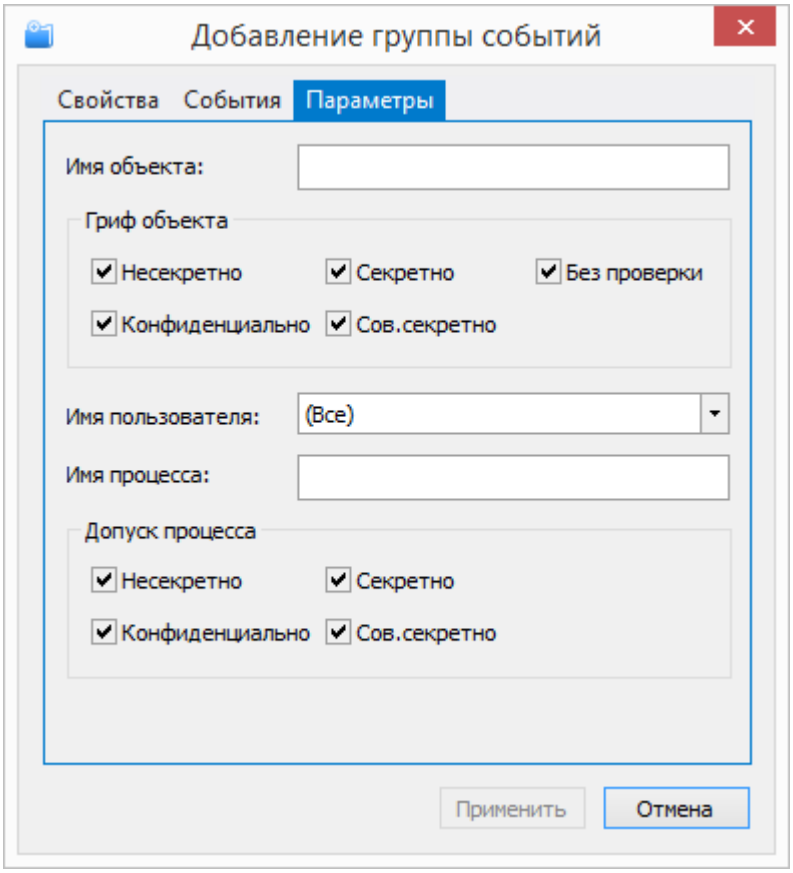


Рис. 88. Добавление группы событий - Параметры.

Для полей **Имя объекта** и **Имя процесса** не обязательно указывать точное значение, группировка будет осуществляться с учётом частичного сравнения строк.

После нажатия кнопки Применить новая группа будет добавлена в дерево групп событий. Если группа с таким именем уже существует, на экран будет выдано соответствующее предупреждение.

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

*Корневая группа событий **События СЗИ** доступна только для чтения. Удаление этой группы или изменение её параметров невозможно.*

Для редактирования группы событий необходимо выбрать пункт меню **Группы событий | Свойства…** либо выбрать пункт **Свойства группы**… контекстного меню на панели **Группы событий**.

Помимо групп событий администратор системы защиты может ограничить список отображаемых событий с помощью механизма фильтрации. Для включения фильтра

отображения событий необходимо выбрать пункт меню **События | Фильтр…** или нажать соответствующую кнопку на панели задач. При этом на экране появится окно настройки фильтра (см. Рис. 89), работа с которым аналогична работе с окном добавления групп.

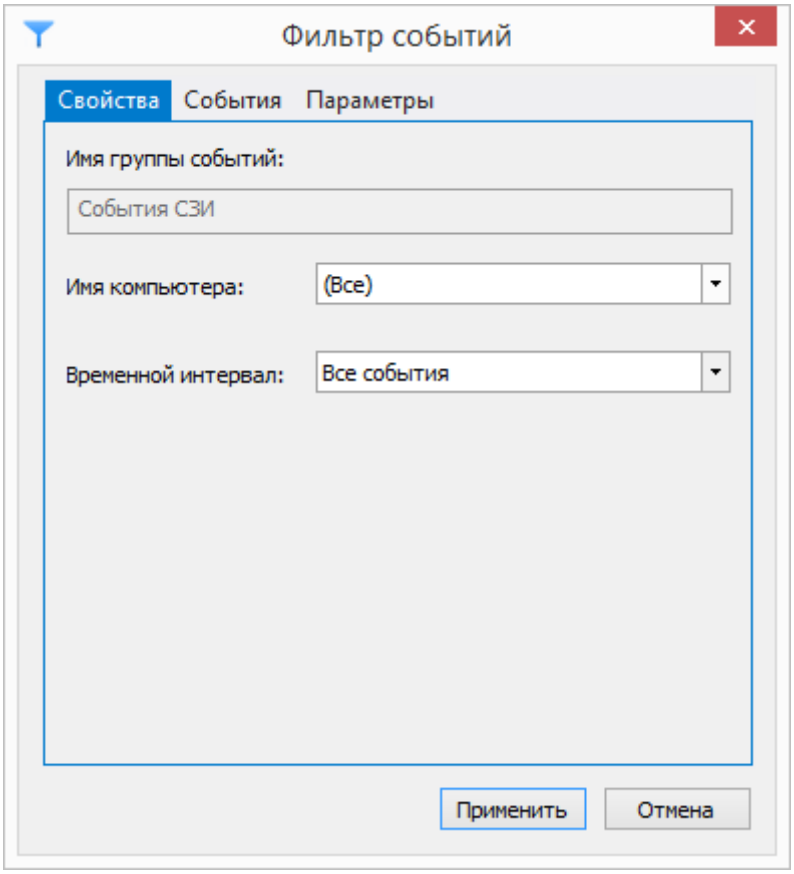


Рис. 89. Фильтр событий.

Если фильтрации производится для группы, отличной от корневой, параметры фильтра будут ограничены параметрами, уже выбранными при создании группы событий. Например, если при создании группы событий были отключены события входа в систему, при выборе фильтра, эти события так же будут недоступны для редактирования.

После нажатия кнопки Применить список событий будет отображаться с учетом заданных в фильтре условий. Для отображения всех событий без учёта фильтра необходимо выбрать пункт меню **События | Все записи**.

Поиск события

Для поиска событий, удовлетворяющих определенным критериям, в общем списке событий необходимо выбрать пункт меню **События | Найти…** или нажать

соответствующую кнопку на панели задач. При этом на экране появится окно поиска событий (см. Рис. 90). Поиск событий может осуществляться по следующим параметрам:

- имя компьютера;
- имя объекта;
- гриф объекта;
- имя пользователя;
- имя процесса;
- допуск процесса.

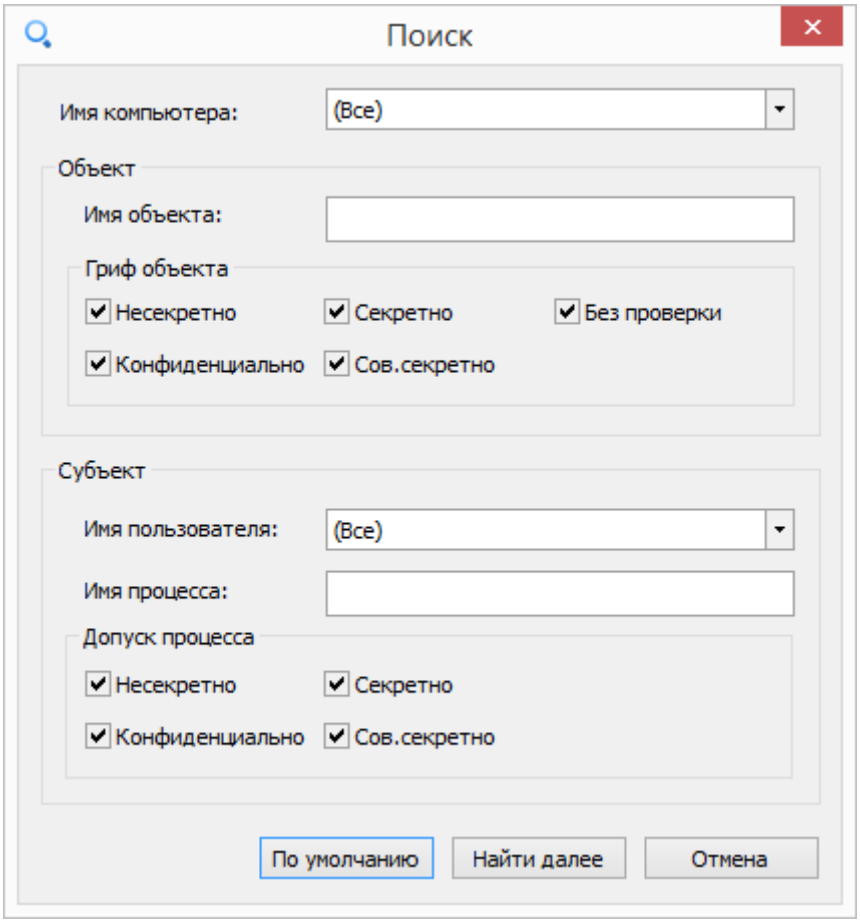


Рис. 90. Параметры поиска событий.

При нажатии кнопки Найти далее программа будет сравнивать события с заданными параметрами. Поиск будет осуществляться сверху вниз от выделенного события. Если в списке будет найдено событие, удовлетворяющее заданным параметрам, оно будет выделено. Для возврата к стандартным настройкам поиска необходимо нажать кнопку По умолчанию. Если в процессе поиска будет достигнут конец списка, на экран будет выдано сообщение с предложением начать поиск с начала.

Параметры журнала

Для получения информации о просматриваемом журнале событий необходимо выбрать пункт меню **Журнал | Свойства журнала…**, или нажать соответствующую кнопку на панели задач. При этом на экране появится окно свойств журнала (см. Рис. 91), в котором приведена информация о расположении файла журнала, его временных характеристиках, размере занимаемом на диске и количестве записей.

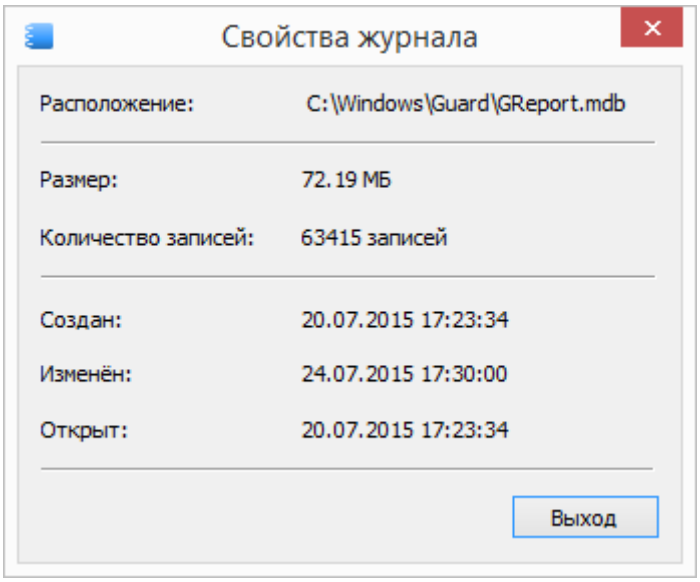


Рис. 91. Свойства журнала событий.

Очистка журнала

Для очистки журнала событий необходимо выбрать пункт меню **Журнал | Очистить журнал** или нажать соответствующую кнопку на панели задач. После рекомендации сохранения журнала из него будут удалены все записи, и будет добавлено событие очистки журнала, если его регистрация предусмотрена настройками регистрации.

Архивирование журнала

В СЗИ «Страж NT» предусмотрены механизмы автоматической архивации журналов событий. Настройка параметров архивации журнала событий осуществляется при помощи вкладки **Настройки** программы **Консоль управления**. Для отображения окна параметров архивации журнала событий необходимо выбрать пункт **Настройки архивации** (см. Рис. 92).

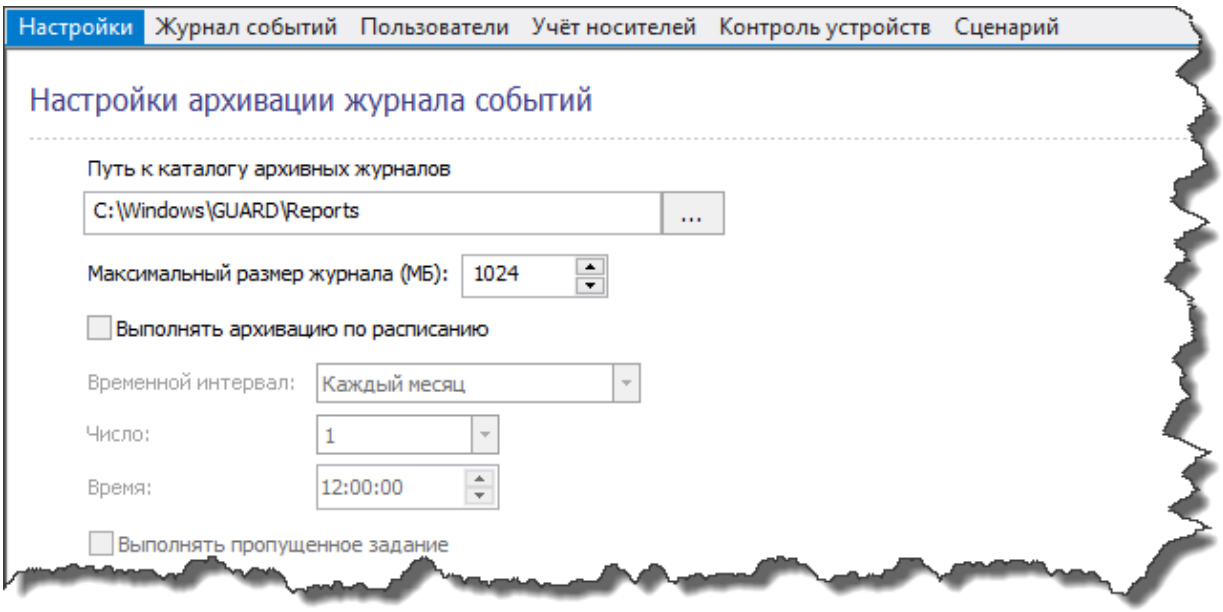
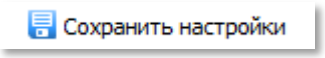


Рис. 92. Настройки автоматической архивации событий.

Администратор системы защиты имеет возможность выбрать папку, в которую будут сохраняться архивные копии журнала событий, а также два варианта архивации журнала: по размеру файла журнала и по расписанию. В случае выбора варианта по расписанию журнал может архивироваться в определённое число месяца или день недели. Флаг в поле **Выполнять пропущенное задание** отвечает за поведение механизмов архивации в случае, если на момент наступления события архивации компьютер был выключен. Если установлен флаг в поле **Выполнять пропущенное задание**, при включении компьютера проверяется наличие пропущенных заданий архивации и, в случае необходимости, журнал событий архивируется по указанному пути. При архивации название файла архивного журнала складывается из имени компьютера и даты и времени создания архивного файла, например, **arm1_20150117_1214.mdb**.

Для сохранения настроек необходимо нажать кнопку 

, для возврата к настройкам по умолчанию – кнопку 

.

Сценарии

В данной главе приводятся сведения о сценариях настроек системы защиты, их назначении, видах, механизмах создания и применения. Также описаны типовые действия администратора системы защиты при работе со сценариями настроек СЗИ.

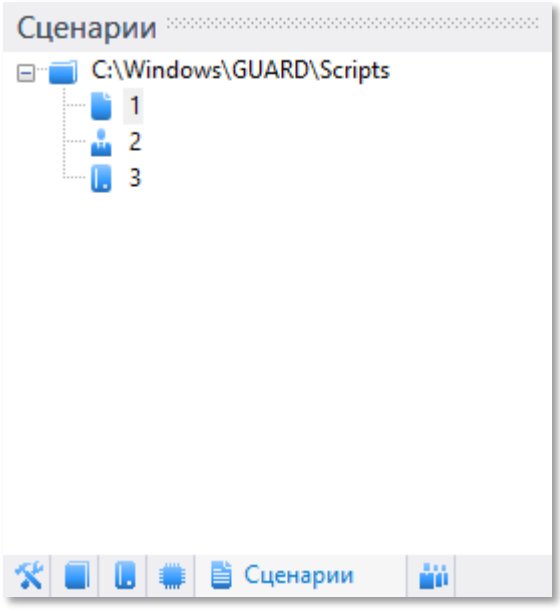
Общие сведения

Сценарии настроек системы защиты представляют собой последовательности действий по настройке системы защиты и могут в себе содержать:

- файловые операции;
- операции с пользователями;
- операции с носителями.

Каждый из типов сценариев поддерживает определённые типы действий. Так, сценарии, содержащие **Операции с пользователями** позволяют создавать пользователей. Сценарии типа **Операции с носителями** позволяют регистрировать носители различных типов. А сценарии типа **Файловые операции** позволяют создавать, удалять, копировать файлы и папки, запускать программы от имени различных пользователей, устанавливать параметры целостности, грифы, параметры запуска и т.д.

Работа со сценариями осуществляется с помощью вкладки **Сценарий** программы **Консоль управления** (см. Рис. 59). В панели сценариев будет отображён список сценариев, расположенных в папке сценариев. По умолчанию сценарии хранятся в папке **%SystemRoot%\Guard\Scripts**. Изменить папку, из которой будет читаться список сценариев, можно в окне общих настроек СЗИ, как описано в разделе **Изменение папки сценариев**.



При выборе сценария в основном окне будет представлен список действий выбранного сценария.

Добавление сценария

Для добавления сценария настроек необходимо выбрать пункт меню **Сценарий | Добавить...** или нажать соответствующую кнопку на панели инструментов. После этого на экране появится окно добавления сценария (см. Рис. 93), в котором администратор системы защиты должен определить название сценария, имя автора, выбрать тип создаваемого сценария, ввести описание сценария и выбрать имя файла, в котором будет храниться сценарий. Поля **Название**, **Автор** и **Имя файла** обязательны для заполнения. Сценарий настроек будет создан после нажатия кнопки Сохранить.

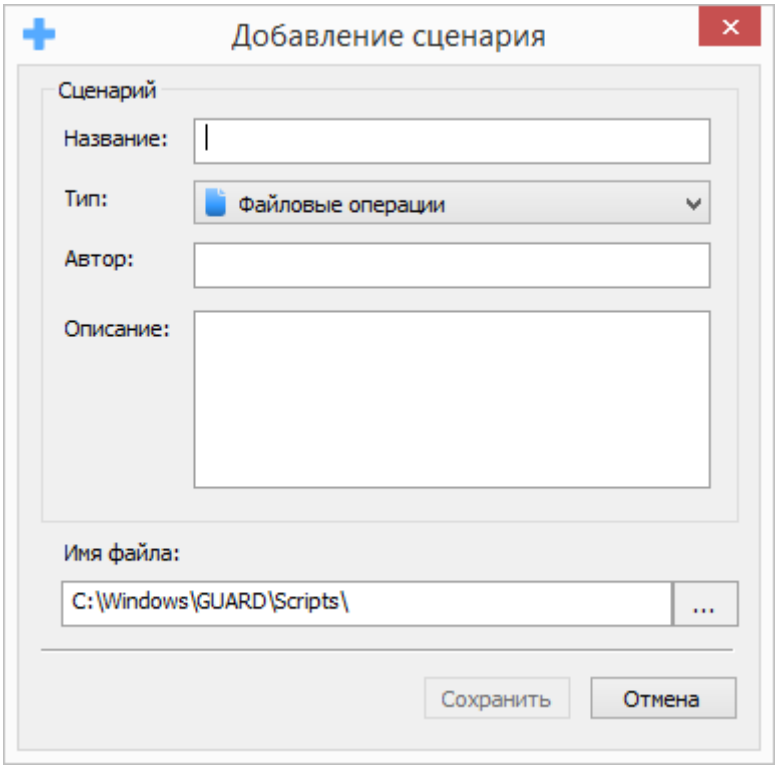


Рис. 93. Добавление сценария.

Удаление сценария

Для удаления сценария настроек необходимо выбрать пункт меню **Сценарий | Удалить** или нажать соответствующую кнопку на панели инструментов. После этого на экран будет выдано предупреждение (см. Рис. 94). При нажатии кнопки Да файл сценария будет удалён из папки хранения сценариев.

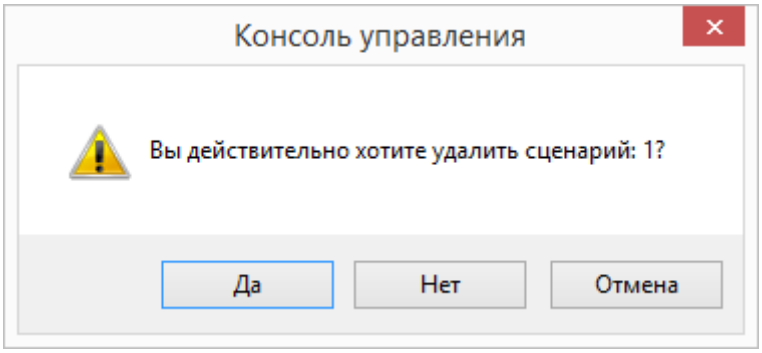


Рис. 94. Запрос подтверждения удаления сценария.

Редактирование свойств сценария

Администратор системы защиты имеет возможность изменить основные параметры сценария настроек. Для этого необходимо выбрать пункт меню **Сценарий | Свойства…** или нажать соответствующую кнопку на панели инструментов. В появившемся окне (см. Рис. 95), можно изменить название сценария, имя автора, а также описание сценария.

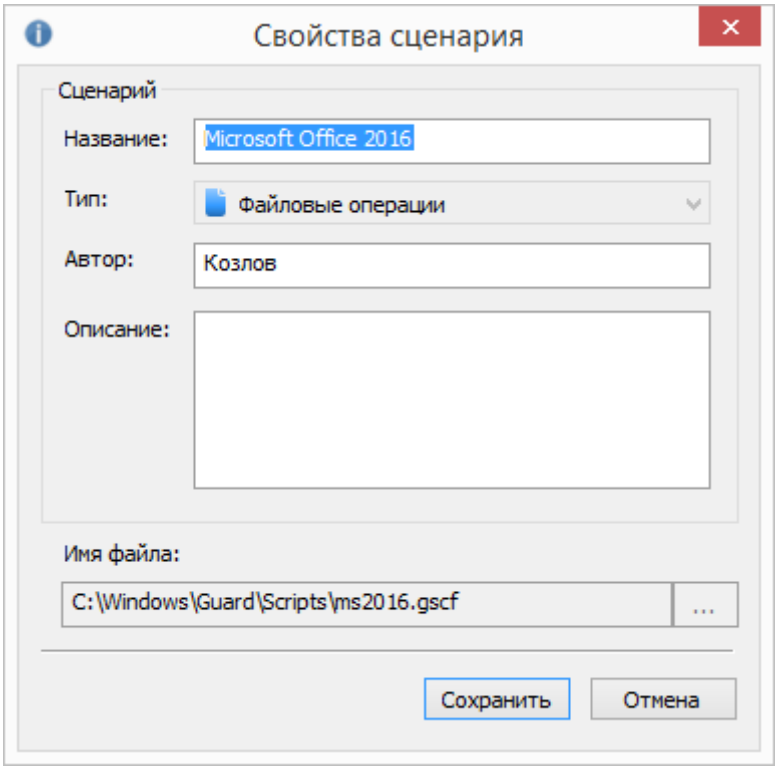


Рис. 95. Редактирование свойств сценария.

При нажатии кнопки Сохранить свойства сценария будут изменены.

Добавление задачи

Для добавления задачи в сценарии настроек необходимо выбрать пункт меню **Задачи | Добавить…** или нажать соответствующую кнопку на панели инструментов. Окно создания задачи зависит от типа сценария, в который добавляется задача.

Добавление задачи для установки разрешений

Одной из задач сценария файловых операций является **Установка разрешений**. Данная задача применяется для установки заданных атрибутов безопасности на указанные ресурсы.

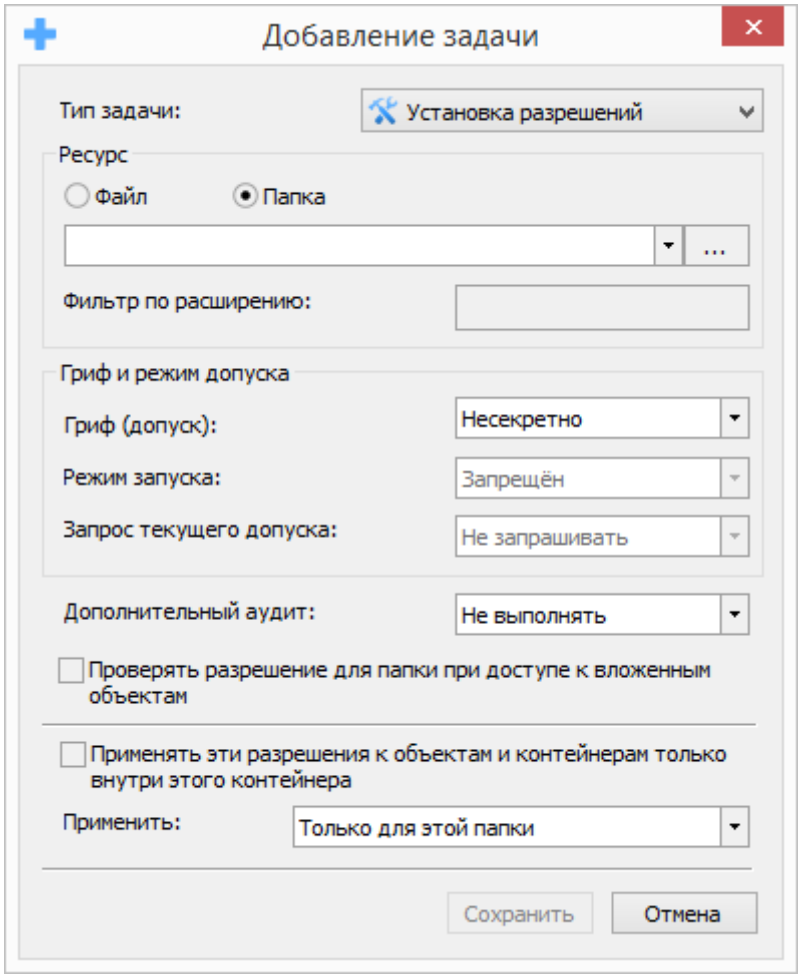


Рис. 96. Добавление задачи установки разрешений.

В окне добавления задачи (см. Рис. 96) необходимо указать тип (файл или папка) и путь к ресурсу, к которому применяются перечисленные ниже атрибуты безопасности:

- гриф или допуск;
- режим запуска;
- режим запроса текущего допуска (если необходимо);

- параметры дополнительного аудита;
- флаг проверки разрешений для папки при доступе к вложенным объектам.

Также поле **Применить:** необходимо указать параметры применения параметров для данного ресурса. Если в качестве ресурса выбрана папка и установлен флаг в поле **Применять эти разрешения к объектам и контейнерам только внутри этого контейнера**, то выбранные параметры будут применяться в соответствии со выбранным значением поля **Применить:** только на один уровень вложения.

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
%ProgramFiles(x86)%	Папка, в которой находятся программы
%CommonProgramFiles%	Папка, в которой находятся компоненты программ
%CommonProgramFiles(x86)%	Папка, в которой находятся компоненты программ
%AllUsersProfile%	Папка профилей всех пользователей
%UserProfile%	Папка профиля пользователя
%AppData%	Папка размещения данных приложений
%LocalAppData%	Папка размещения локальных данных приложений
%Temp%	Папка временных файлов
%Tmp%	Папка временных файлов

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

Если тип добавляемого ресурса – «Папка», и параметры применения настроек включают вложенные файлы, администратор системы защиты 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.

Добавление задачи для запуска программ

Некоторые программы имеют довольно сложную структуру и логику работы. Для корректной настройки этих программ иногда необходимо выполнить их запуск от имени всех пользователей, которые будут работать с ней. Добавление данной задачи позволяет автоматизировать эти действия. В окне (см. Рис. 97) можно задать следующие параметры:

- путь к исполняемому модулю программы;
- параметры командной строки;
- флаг ожидания закрытия программы.
- флаг запуска от имени других пользователей.

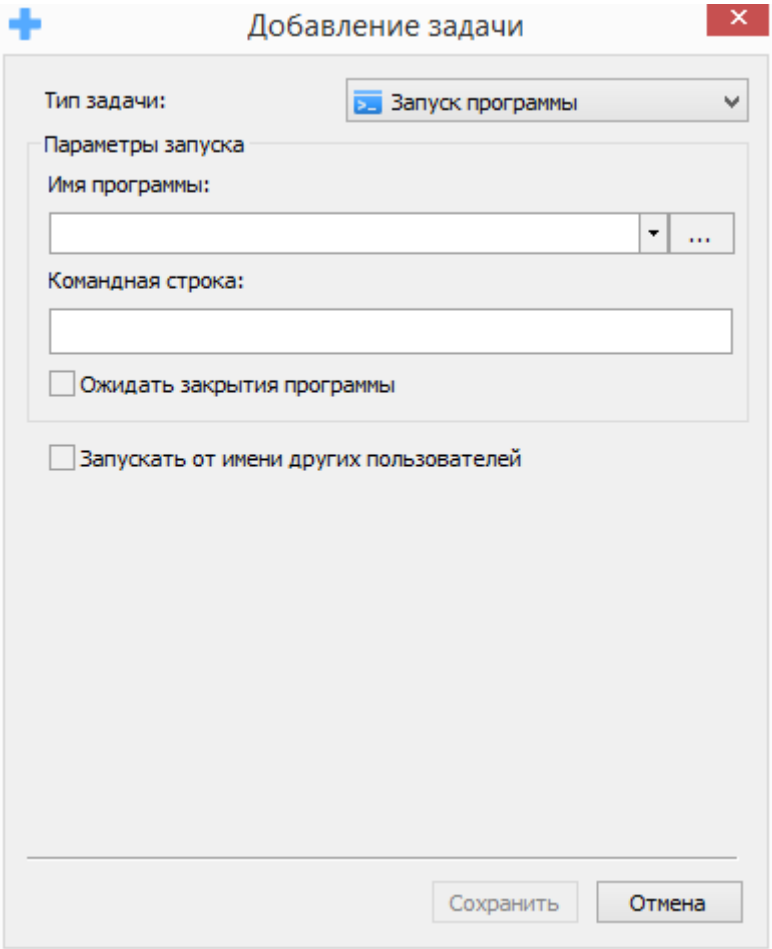


Рис. 97. Добавление задачи запуска программы.

Путь к исполняемому модулю программы может быть как абсолютным, так и заданным с помощью переменных окружения, список которых приведен выше. Если установлен флаг в поле **Запускать от имени других пользователей**, при применении сценария

администратору системы защиты будет предложен список пользователей, от имени которых будет осуществлен запуск программы. Если установлен флаг в поле **Ожидать закрытия программы**, применение сценария будет приостановлено до момента закрытия каждого экземпляра запущенной программы перед запуском следующего.

Добавление задачи по созданию файлов и папок

При необходимости создания файла или папки необходимо добавить задачу создания ресурсов. В окне задачи (см. Рис. 98) необходимо ввести путь к создаваемому ресурсу и флаг замены ресурса, если он уже существует. Путь к ресурсу может быть как абсолютным, так и заданным с помощью переменных окружения, список которых приведен выше.

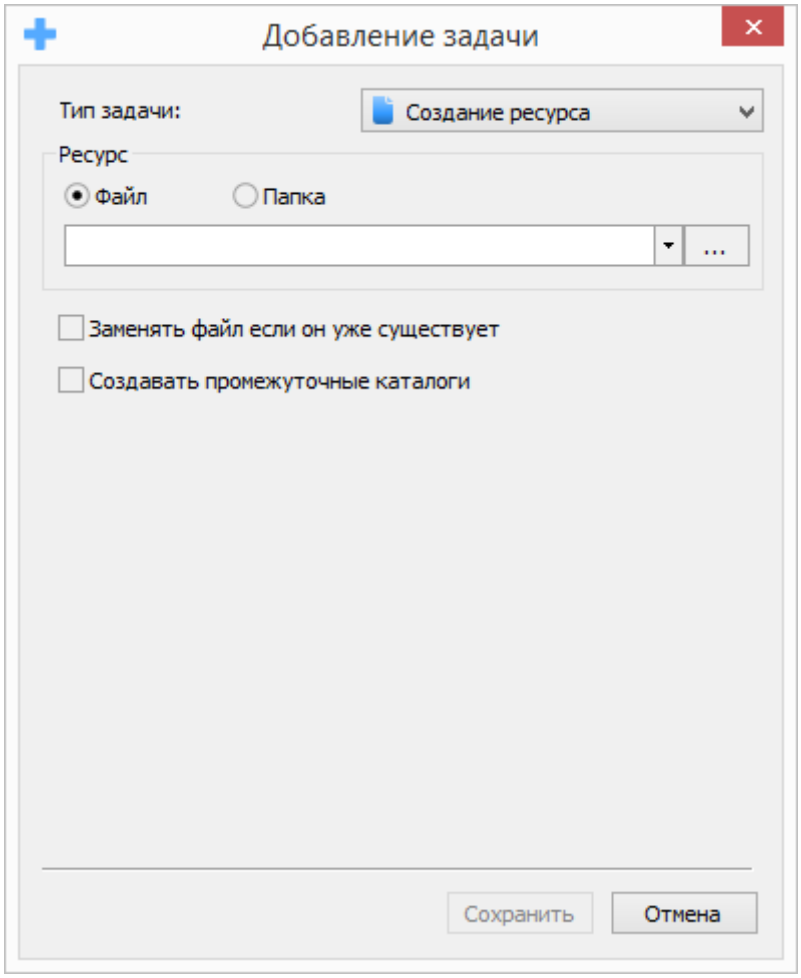


Рис. 98. Добавление задачи создания ресурса.

Если выбрано создание файла и установлен флаг в поле **Заменять файл, если он уже существует**, то перед созданием нового файла старый будет удален. Если выбрано создание папки и установлен флаг в поле **Заменять папку, если она уже существует**, то

перед созданием новой папки старая будет удалена вместе со всеми входящими в неё папками и файлами.

Если установлен флаг в поле **Создавать промежуточные каталоги**, то перед созданием файла или папки буду созданы все промежуточные каталоги. В противном случае процесс создания файла или папки в несуществующем каталоге завершится с ошибкой.

Добавление задачи по удалению файлов и папок

При добавлении задачи удаления ресурса в окне (см. Рис. 99) необходимо ввести путь к удаляемому ресурсу. Путь к ресурсу может быть как абсолютным, так и заданным с помощью переменных окружения, список которых приведен выше. Если удаляемым ресурсом является папка и установлен флаг в поле **Удалять папку, только если она пуста**, папка будет удалена, только если она пуста.

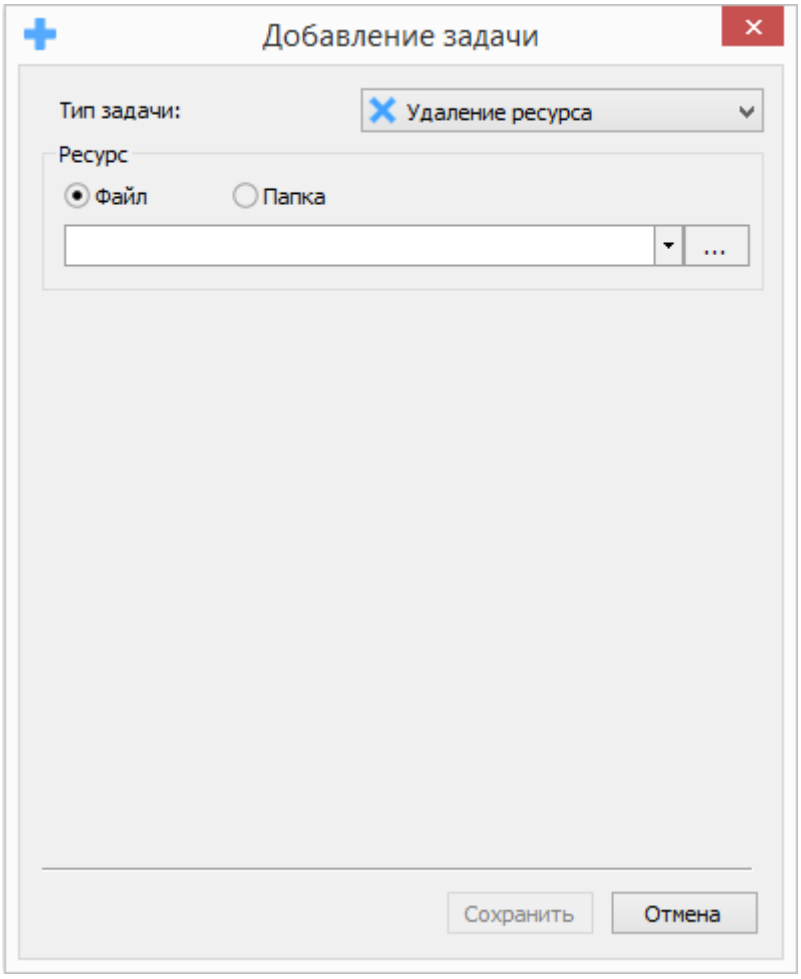


Рис. 99. Добавление задачи удаления ресурса.

Добавление задачи копирования файлов и папок

В окне задачи копирования ресурсов (см. Рис. 100) необходимо ввести путь, откуда будет копироваться ресурс, и путь, куда он будет копироваться. Путь к ресурсам может быть как абсолютным, так и заданным с помощью переменных окружения, список которых приведен выше. Копироваться могут как файлы, так и папки.

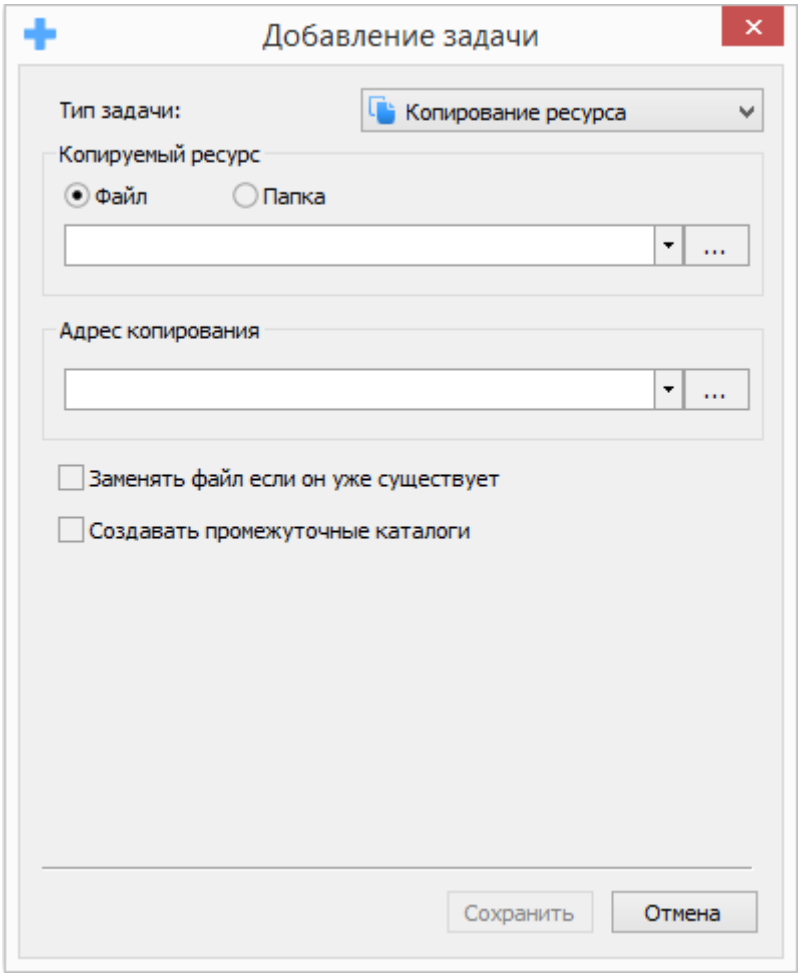


Рис. 100. Добавление задачи копирования ресурса.

Если выбрано копирование файла и установлен флаг в поле **Заменять файл, если он уже существует**, то перед копированием нового файла старый будет удален. Если флаг в данном поле не установлен, то процедура применения сценария не будет копировать новый файл в том случае, если файл с таким же именем уже существует. Если выбрано копирование папки и установлен флаг в поле **Заменять папку, если она уже существует**, то перед копированием новой папки старая будет удалена. Если флаг в данном поле не установлен, то процедура применения сценария не будет копировать новую папку, в том случае, если папка с таким же именем уже существует.

Если установлен флаг в поле **Создавать промежуточные каталоги**, то перед копированием файла или папки буду созданы все промежуточные каталоги. В противном случае при попытке копирования файла или папки в несуществующий каталог будет выдана ошибка.

Добавление задачи настройки контроля целостности

В окне задачи настройки контроля целостности (см. Рис. 101) необходимо ввести путь к ресурсу, на который устанавливаются параметры контроля целостности, а также контролируемые атрибуты и параметры реакции на нарушение целостности. Путь к ресурсу может быть как абсолютным, так и заданным с помощью переменных окружения, список которых приведен выше. Если настраиваемым ресурсом является папка, параметры будут применены ко всем файлам в этой папке. Для установки параметров целостности на файлы во вложенных папках необходимо установить флаг в поле **Сменить параметры для файлов в подпапках**. Более подробно о параметрах контроля целостности описано в разделе **Целостность ресурсов**.

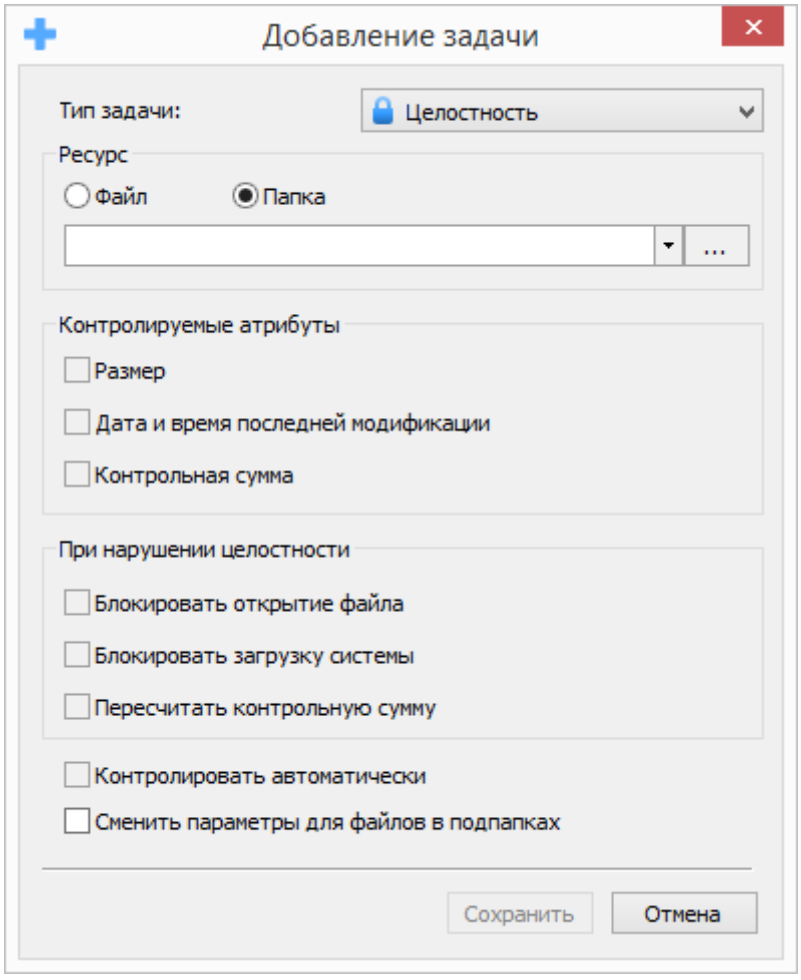


Рис. 101. Добавление задачи настройки контроля целостности.

Добавление задачи создания пользователя

При необходимости автоматизации процесса создания пользователей на компьютерах, не входящих в домен, можно создать соответствующий сценарий, состоящий из нескольких задач по созданию пользователей. В дальнейшем данный сценарий можно применять на всех компьютерах в сети.

Задачу создания пользователя можно добавить только в сценарий с типом **Операции с пользователями**. В окне добавления задачи создания пользователя (см. Рис. 102) необходимо указать следующие параметры:

- имя пользователя;
- полное имя;
- описание;
- допуск;
- пароль;
- флаг администратора системы защиты;
- флаг запрета смены пароля пользователем;
- флаг обязательной смены пароля пользователя при следующем входе.
- флаг создания профиля пользователя.

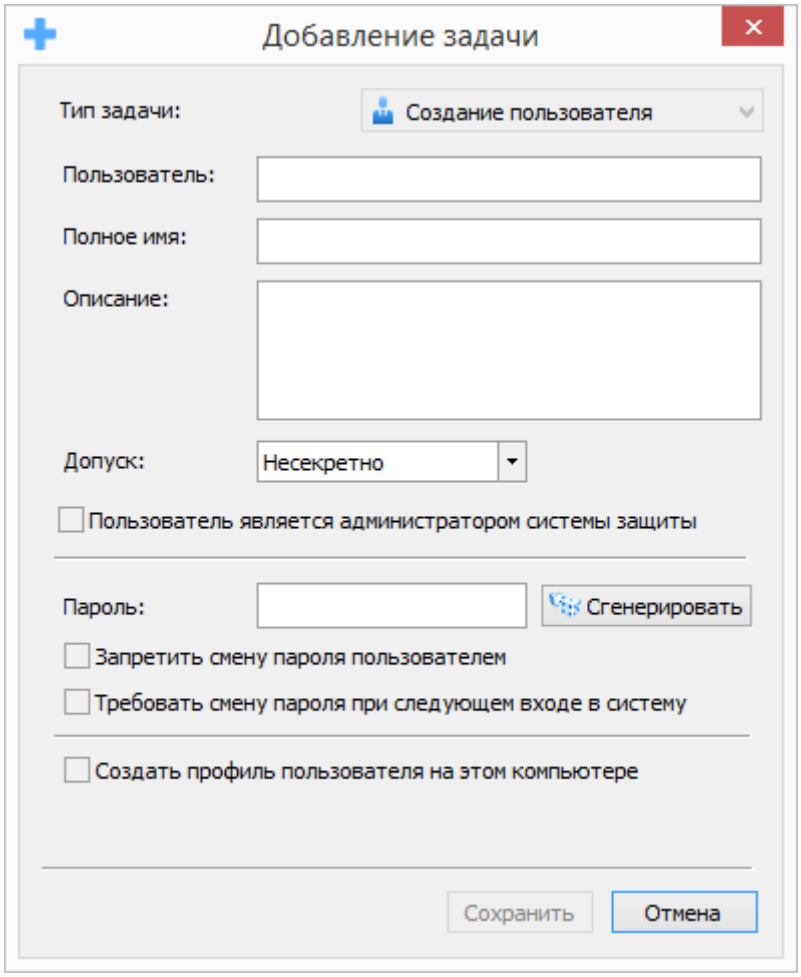


Рис. 102. Добавление задачи создания пользователя.

Подробнее параметры создания пользователя описаны в разделе **Создание пользователя**.

Добавление задачи регистрации носителя

Задачу регистрации носителя можно добавить только в сценарий с типом **Операции с носителями**. В окне добавления задачи регистрации носителя (см. Рис. 103) можно указать следующие параметры:

- тип носителя;
- серийный номер;
- учётный номер;
- пользователь;
- гриф;
- дополнительный аудит;
- признак использования простого доступа к носителю;
- признак проверки разрешения для папки при доступе к вложенным объектам.

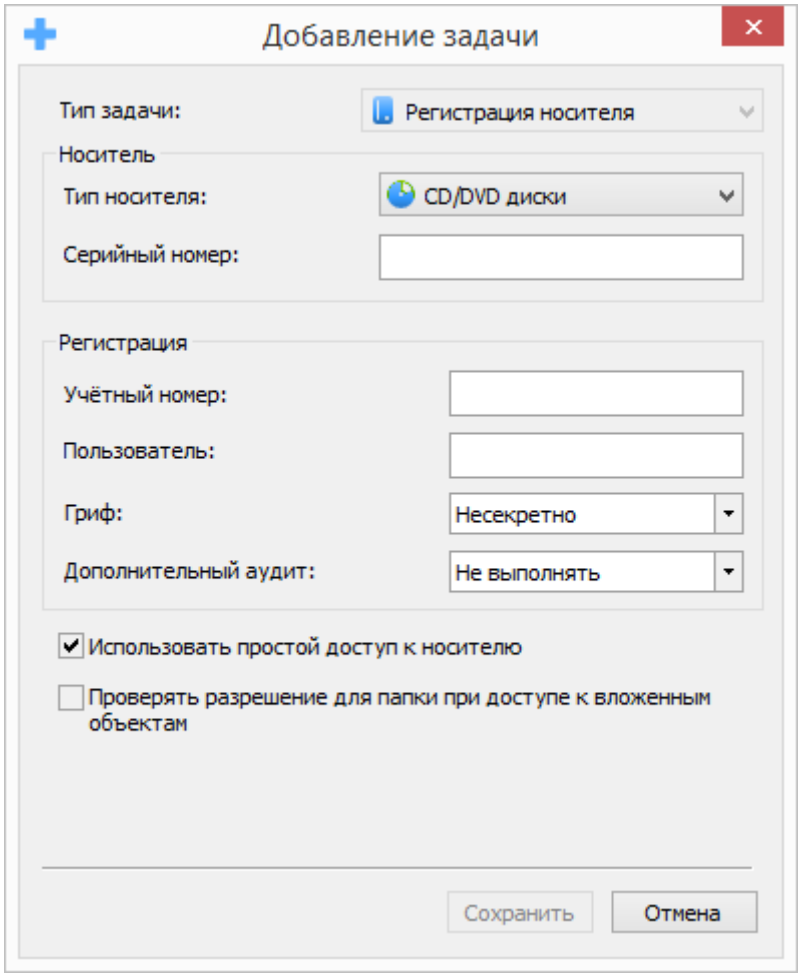


Рис. 103. Добавление задачи регистрации носителя.

Подробнее параметры, используемые при регистрации носителя, описаны в разделе **Регистрация носителя**.

Добавление задачи настройки ЗПС

В окне задачи настройки ЗПС (см. Рис. 104) необходимо ввести путь к папке, в которой будет производиться настройка ЗПС.

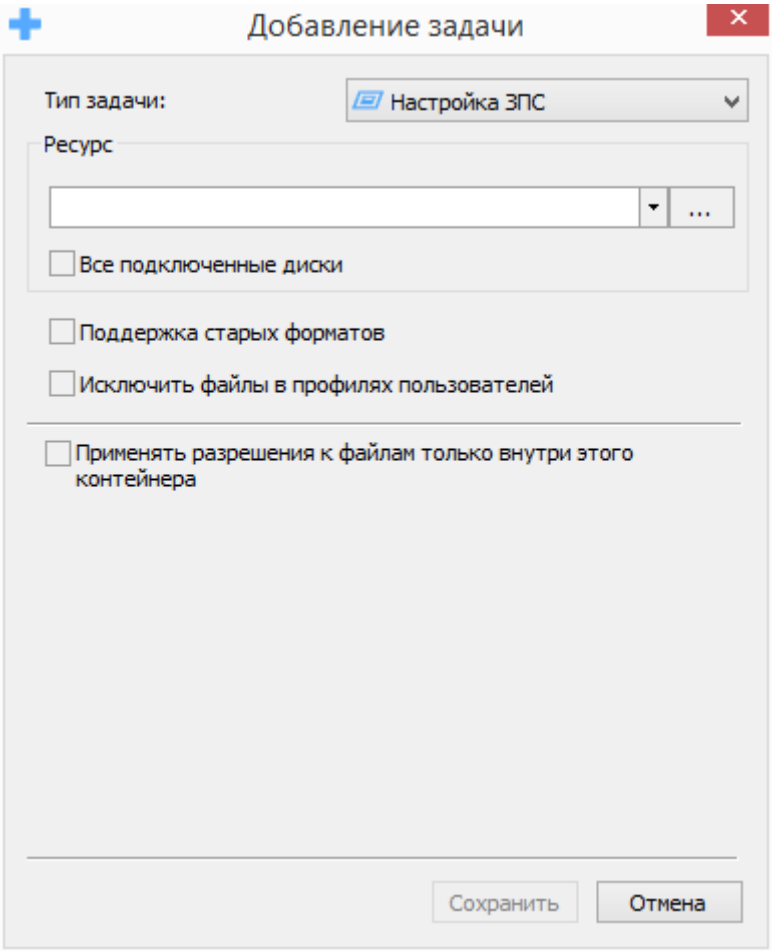


Рис. 104. Добавление задачи настройки ЗПС.

При установке флага в поле **Все подключенные диски** настройка ЗПС будет производиться на всех дисках, значение пути к папке в этом случае будет игнорироваться. Путь к каталогу может быть как абсолютным, так и заданным с помощью переменных окружения. Более подробная информация о параметрах настройки ЗПС приведена в разделе **Настройка ЗПС**.

Редактирование содержимого сценария

Администратор системы защиты имеет возможность удалять, редактировать состав и порядок задач, содержащихся в сценарии. Для удаления задачи из сценария необходимо выбрать пункт меню **Задачи | Удалить** или нажать соответствующую кнопку на панели задач. Для просмотра и редактирования параметров задачи необходимо выбрать пункт меню **Задачи | Свойства...** или нажать соответствующую кнопку на панели задач.

Если сценарий описывает файловые операции, то существует возможность преобразования абсолютного пути указанного в записи ресурса в относительный. Так, например, путь **C:\Program Files\Windows NT\Accessories\wordpad.exe** будет

преобразован в **%ProgramFiles%\Windows NT\Accessories\wordpad.exe**. Для преобразования абсолютного пути в относительный необходимо выбрать запись сценария и в контекстном меню выбрать пункт **Преобразовать путь.**

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

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

Сохранение сценария

При изменении содержимого сценария он будет помечен как «измененный» (см. Рис. 105). Для сохранения изменений необходимо выбрать пункт меню **Сценарий | Сохранить** или нажать соответствующую кнопку на панели задач. Для сохранения изменений во всех отредактированных сценариях необходимо выбрать пункт меню **Сценарий | Сохранить все**.

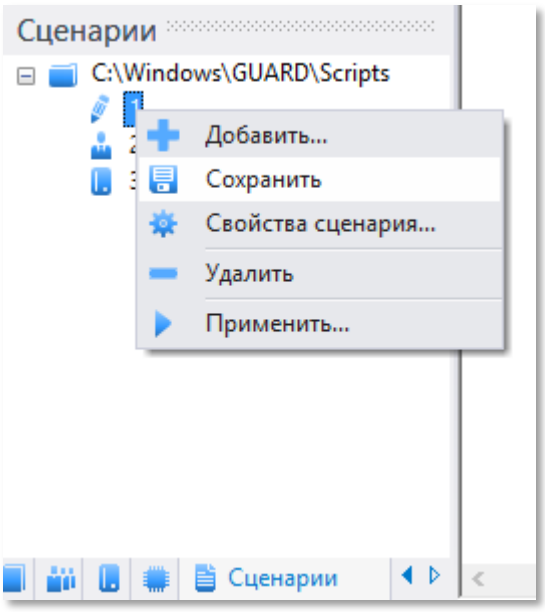


Рис. 105. Сохранение сценария.

Импорт настроек

При настройке сложных программных продуктов появляется необходимость переноса атрибутов безопасности уже настроенных ресурсов в сценарий настроек. Для этого существует механизм импорта настроек.

Для импорта настроек необходимо выбрать пункт меню **Задачи | Импорт …**. Вид окна импорта настроек зависит от типа сценария.

Для импорта настроек файлов и папок необходимо в сценарии типа **Файловые операции** указать путь к родительской папке и нажать кнопку Найти. После этого в списке будут отображены все ресурсы, для которых существуют настройки СЗИ «Страж NT» (см. Рис. 106). Администратор имеет возможность выбрать те файлы и папки, настройки которых будут импортированы в сценарий настроек. После нажатия кнопки Импорт записи о настройках всех ресурсов, находящихся в выбранной папке, будут добавлены в конец сценария.

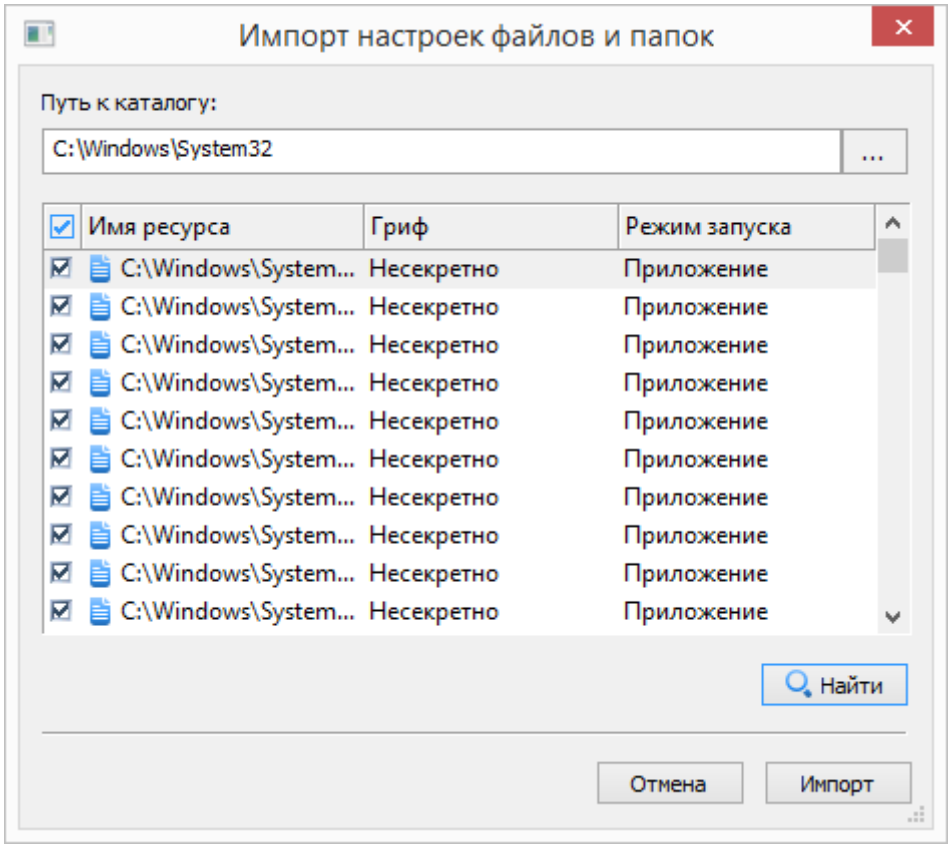


Рис. 106. Импорт настроек разрешений.

Для импорта настроек пользователей необходимо в сценарии типа **Операции с пользователями** нажать кнопку Найти. После этого в списке будут отображены все

пользователи, присутствующие в системе (см. Рис. 107). Администратор системы защиты имеет возможность выбрать тех пользователей, которые будут импортированы в сценарий настроек. После нажатия кнопки Импорт записи о выбранных ресурсах будут добавлены в конец сценария.

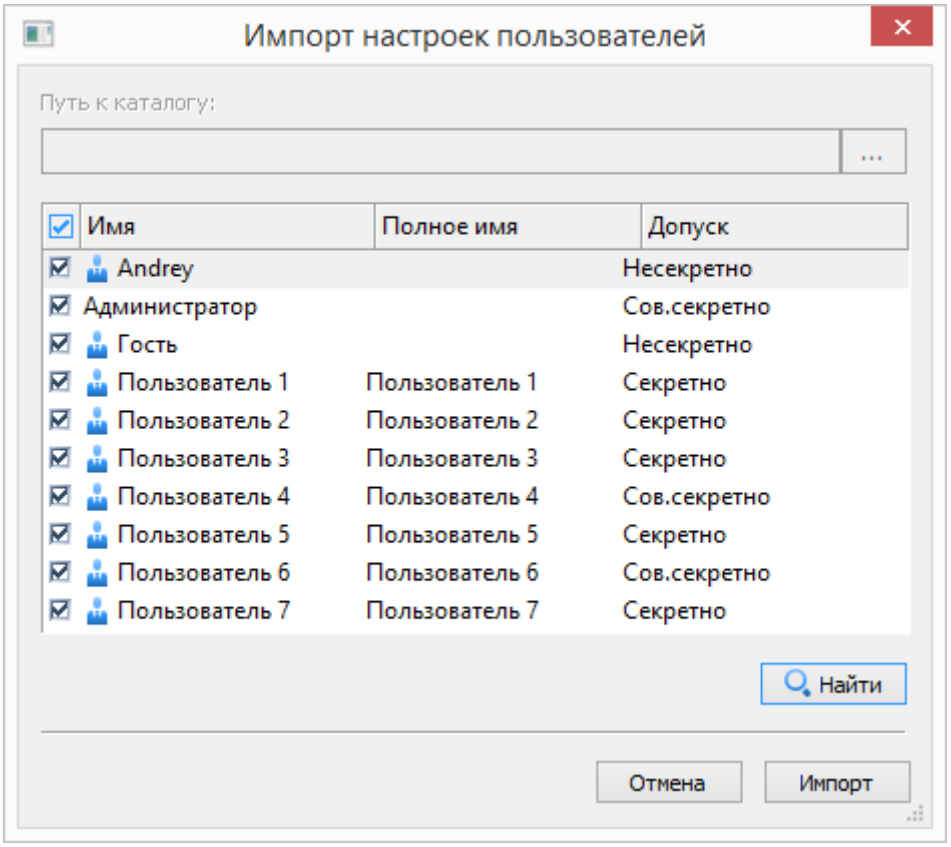


Рис. 107. Импорт настроек пользователей.

Для импорта настроек носителей необходимо в сценарии **Операции с носителями** нажать кнопку Найти. После этого в списке будут отображены все носители, зарегистрированные в системе (см. Рис. 108). Администратор системы защиты имеет возможность выбрать те носители, которые будут импортированы в сценарий настроек. После нажатия кнопки Импорт записи о выбранных носителях будут добавлены в конец сценария.

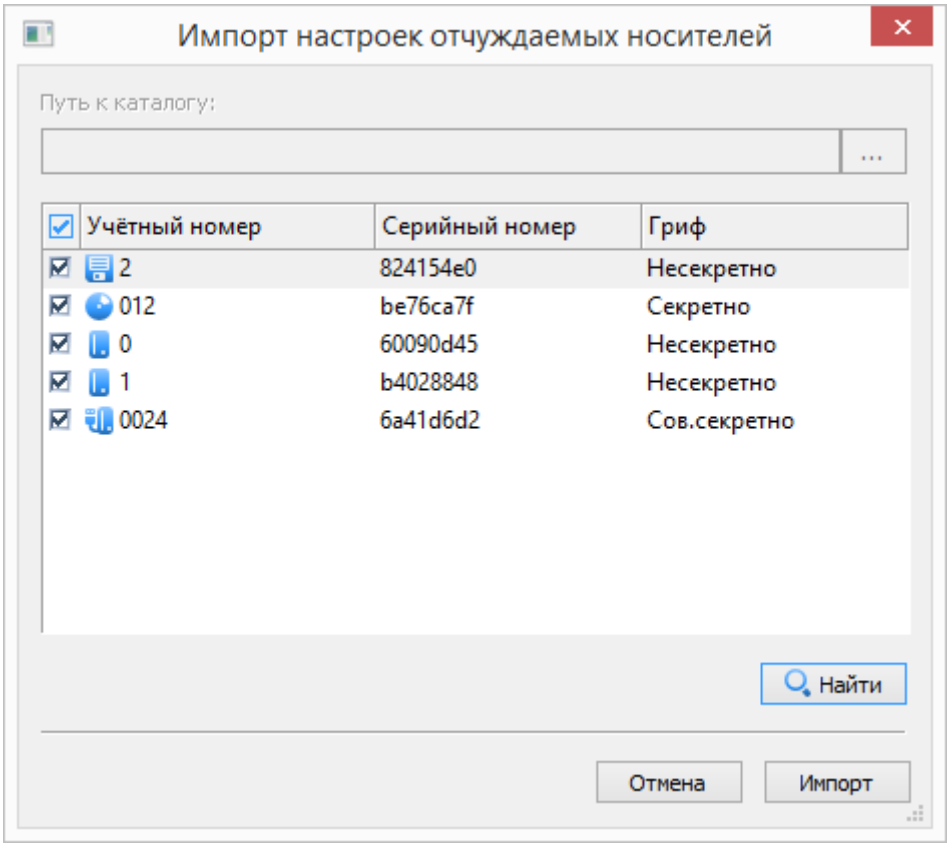


Рис. 108. Импорт настроек носителей.

Применение сценария

Для применения сценария настроек необходимо выбрать пункт меню **Сценарий | Применить…**, или нажать соответствующую кнопку на панели инструментов. Если сценарий настроек типа **Файловые операции** содержит записи, которые по-разному интерпретируются для разных пользователей, необходимо будет выбрать, для каких именно пользователей будет применяться данный сценарий. Например, если сценарий содержит задачу запуска приложения от имени других пользователей, на экран будет выдано окно (см. Рис. 109), в котором администратор системы защиты может выбрать список пользователей.

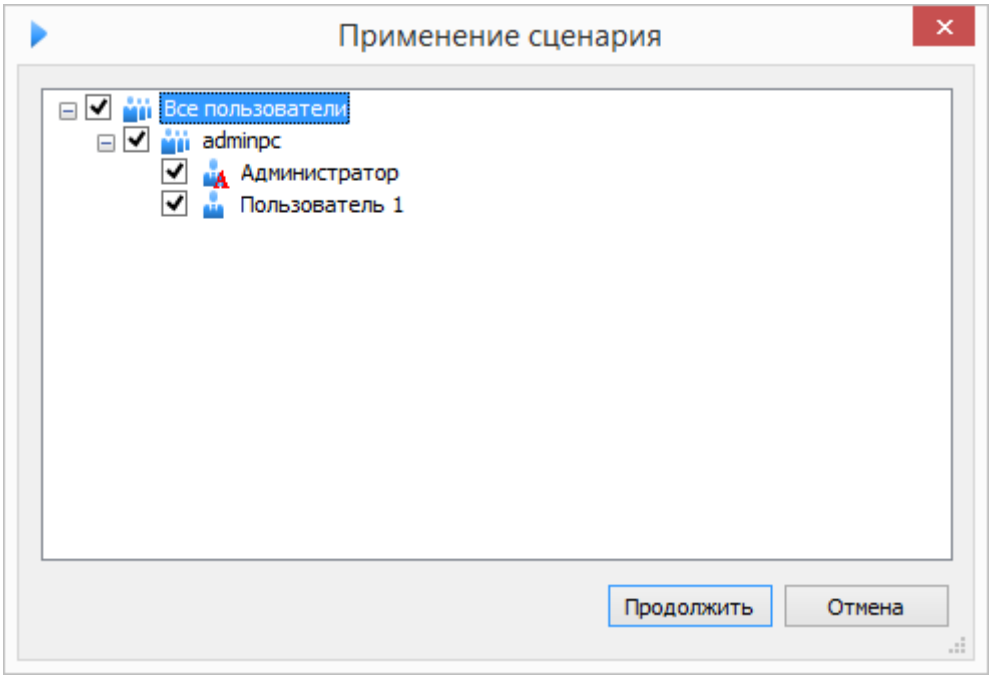


Рис. 109. Применение сценария - выбор пользователей.

В процессе применения сценария настроек на экран будет выведено окно, в котором будет отображаться список выполненных операций с описанием результата их выполнения.

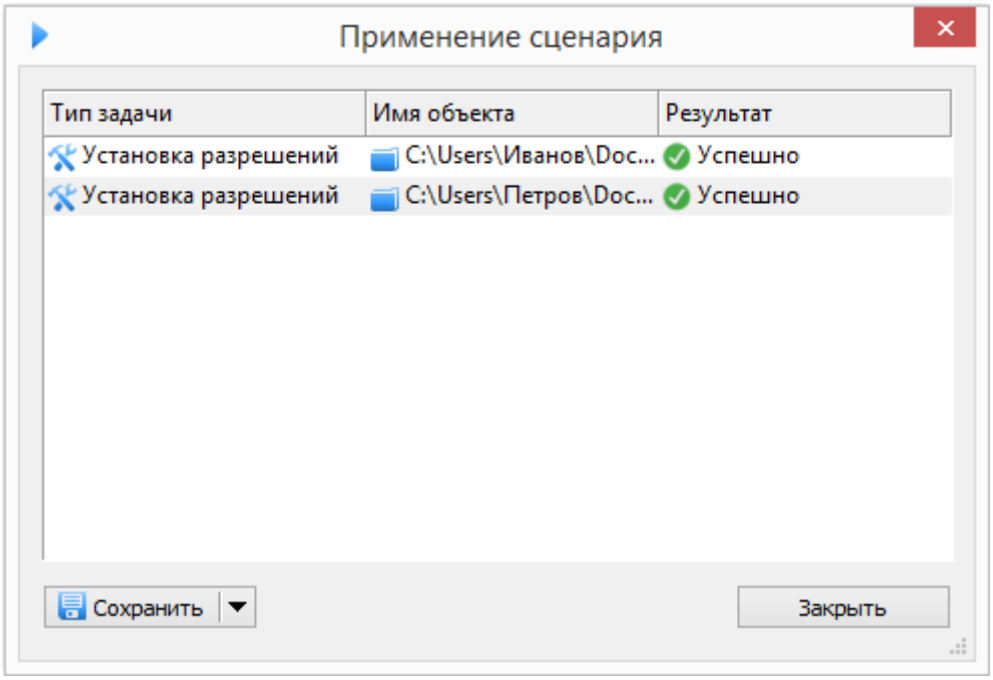


Рис. 110. Применение сценария - отчет.

По окончании применения сценария настроек существует возможность сохранения отчета о выполненных операциях. Для этого необходимо нажать кнопку Сохранить. Кнопка поддерживает выпадающий список типов сохраняемых результатов. Если просто нажать кнопку Сохранить, то будет сохранён весь список результатов, если же выбрать

пункт Только ошибки – будет сохранён только список неудачных попыток выполнения операций. Список сохраняется в файл формата HTML или CSV.

Изменение папки сценариев

По умолчанию сценарии настроек хранятся в папке **%SystemRoot%\Guard\Scripts**. Путь к папке расположения сценариев задается во вкладке **Настройки** программы **Консоль управления** при выборе раздела **Общие настройки** (см. Рис. 111).

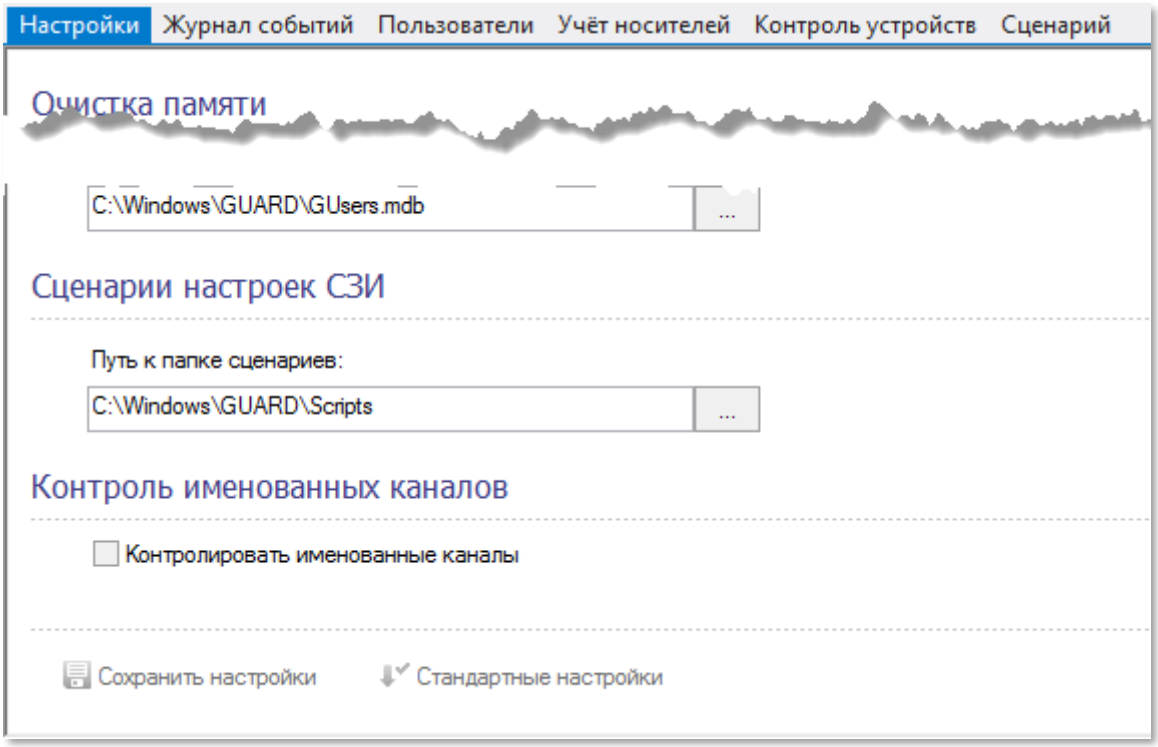


Рис. 111. Изменение папки расположения сценариев.

Для сохранения настроек необходимо нажать кнопку Сохранить настройки, для возврата к настройкам по умолчанию – кнопку Стандартные настройки.

Дополнительные механизмы и настройки

Терминальный доступ

В СЗИ «Страж NT» поддерживаются защитные механизмы при подключении пользователей к терминальному серверу. Если на терминальном сервере установлена система защиты при подключении пользователей к нему выполняется терминальная идентификация пользователей, т.е. запрашивается идентификатор и пароль пользователя. Для успешной идентификации необходимо, чтобы на компьютере-клиенте, с которого происходит подключение, также была установлена СЗИ «Страж NT» данной версии, а также модули поддержки терминальных подключений. Кроме того, на идентификаторе пользователя должен быть разрешен доступ к терминальному серверу, а имя и пароль пользователя на клиенте и терминальном сервере должны совпадать. Также необходимо убедиться, что на клиенте во время удаленного сеанса будут разрешены локальные смарт-карты. При выполнении всех этих условий идентификационная информация пользователя, записанная на персональном идентификаторе, будет передана на терминальный сервер и считана процедурой терминальной идентификации. После чего будет выдан запрос на ввод пароля пользователя с клавиатуры. В случае успешного ввода пароля произойдет вход пользователя в удаленную сессию на терминальном сервере. После трех неудачных попыток ввода пароля на экран выдается сообщение «Несанкционированный доступ», которое сопровождается звуковой сигнализацией. В журнал регистрации заносится соответствующее сообщение, после чего терминальная сессия завершается.

В тех случаях, когда на клиенте терминального сервера по какой-либо причине невозможно установить СЗИ «Страж NT», терминальная идентификация может быть отключена. Для отключения терминальной идентификации требуется ввод специальной терминальной лицензии на определенное количество подключений на терминальном сервере.

Управление терминальными лицензиями осуществляется в программе **Консоль управления** во вкладке **Настройки**. Для отображения терминальных лицензий необходимо выбрать пункт меню **Терминальный сервер** (см. Рис. 112).

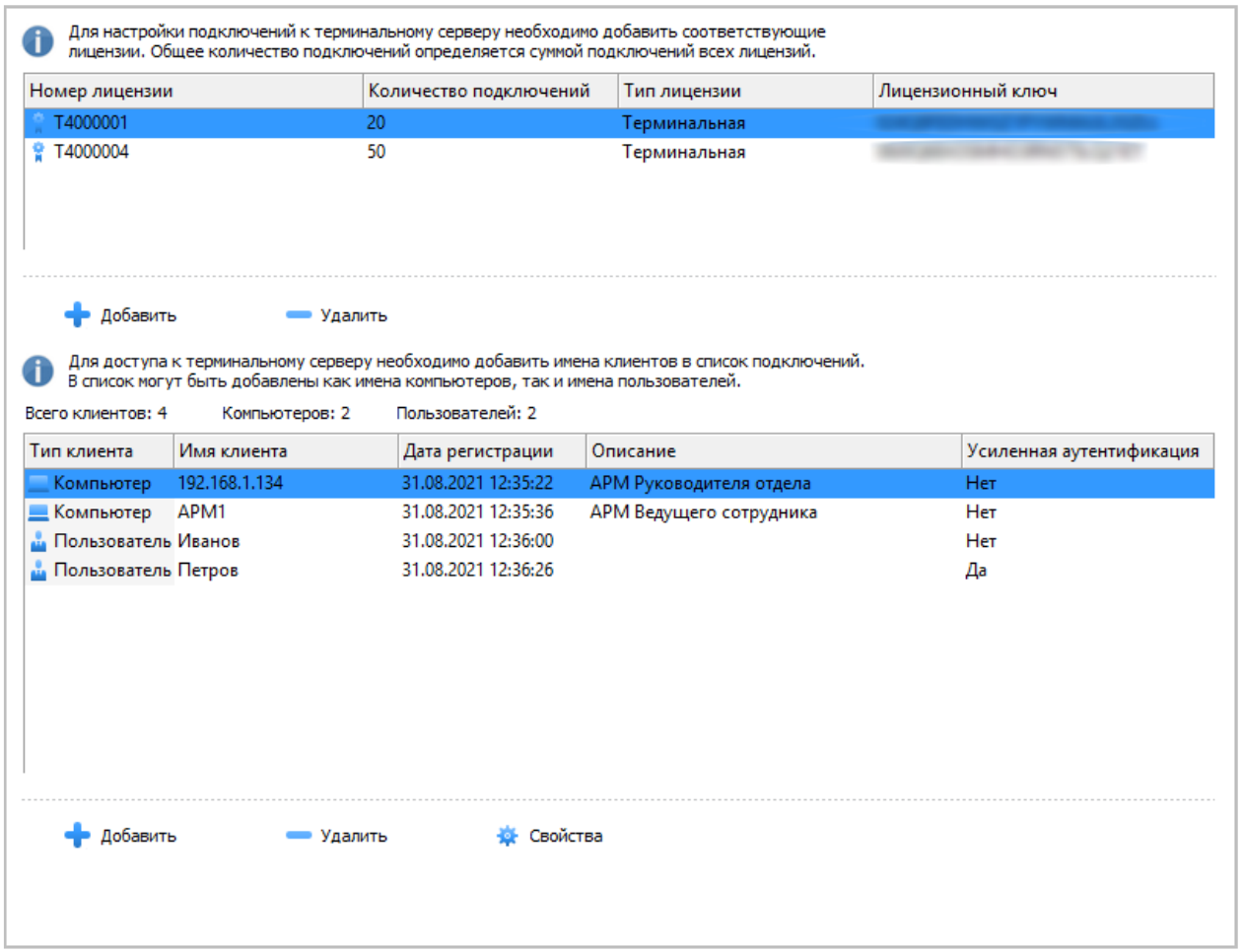
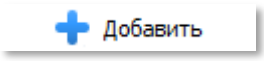


Рис. 112. Управление терминальными лицензиями.

Для добавления терминальной лицензии необходимо нажать кнопку 

, расположенную под списком терминальных лицензий. При этом появится диалог (см. Рис. 113), в котором необходимо ввести лицензионный номер терминальной лицензии.

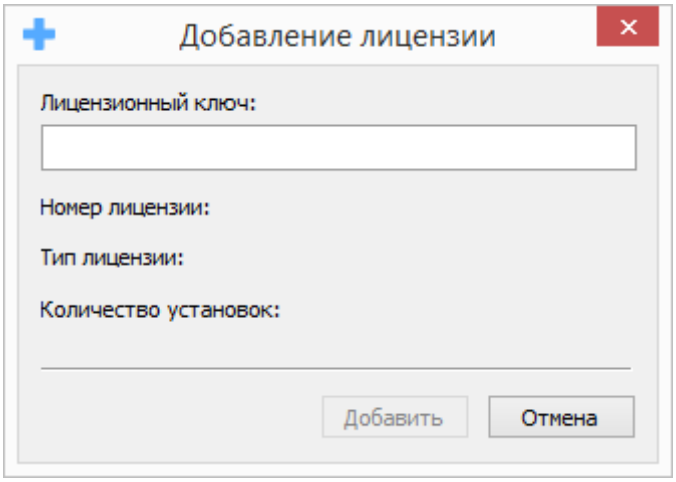
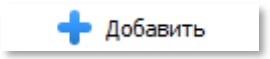


Рис. 113. Добавление терминальной лицензии.

После успешного добавления лицензии необходимо добавить имена или адреса клиентов, при подключении с которых не будет выполняться процедура терминальной идентификации, т.е. для подключения необходимо будет ввести имя пользователя и пароль с клавиатуры. Для добавления терминального клиента необходимо нажать кнопку 

, расположенную под списком терминальных клиентов (см. Рис. 112).

В качестве имени клиента должно указываться NETBIOS имя компьютера, в качестве адреса – IP-адрес. Кроме того, в список подключений можно добавить имена пользователей, для которых также не будет выполняться процедура терминальной идентификации. Для всех клиентов или пользователей, не включенных в список подключений, всегда будет выполняться процедура терминальной идентификации. Также предусмотрен режим усиленной аутентификации для клиента или пользователя, при котором пользователь для входа в терминальный сервер должен будет предъявить идентификатор типа смарт-карты (Рутокен, eToken, JaCarta, eSmart), сформированный для входа пользователя в терминальный сервер средствами СЗИ «Страж NT», и ввести пароль. Для включения данного режима используется флаг **Использовать усиленную аутентификацию** (см. Рис. 114).

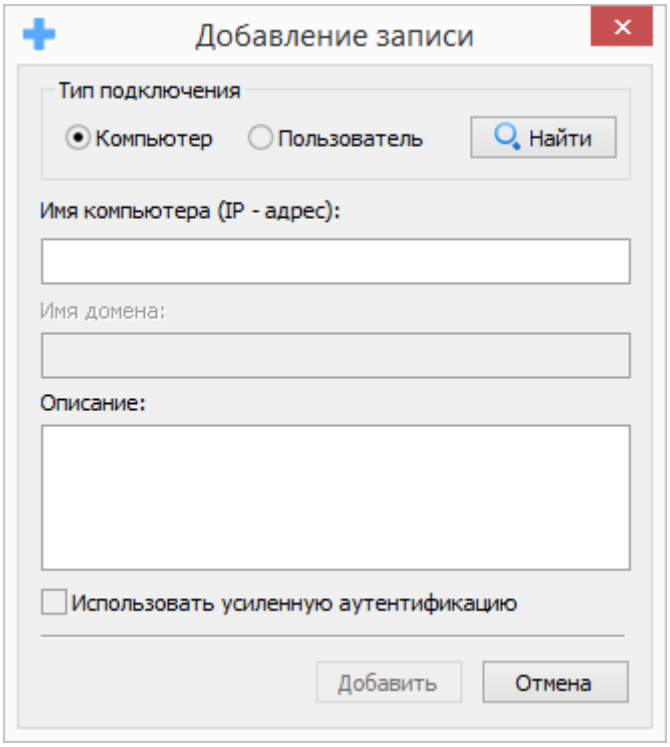


Рис. 114. Добавление записи о терминальном клиенте.

Также предусмотрена возможность импорта и экспорта списка терминальных клиентов, доступная из контекстного меню области терминальных клиентов.

Настройка сетевого доступа

При выборе в программе **Консоль управления** или **Проводник** удаленного компьютера система защиты пытается подключиться к нему, используя имя и пароль пользователя, который вошел в систему. Если на удаленном компьютере нет пользователей с такими же учетными данными, доступ к нему будет отклонен. Чтобы иметь возможность получить доступ к удаленному компьютеру с другими учетными данными необходимо запустить программу **Консоль управления** и в разделе **Политики паролей** вкладки **Настройки** установить флаг в поле **Разрешить ввод сетевого пароля** (см. Рис. 115).

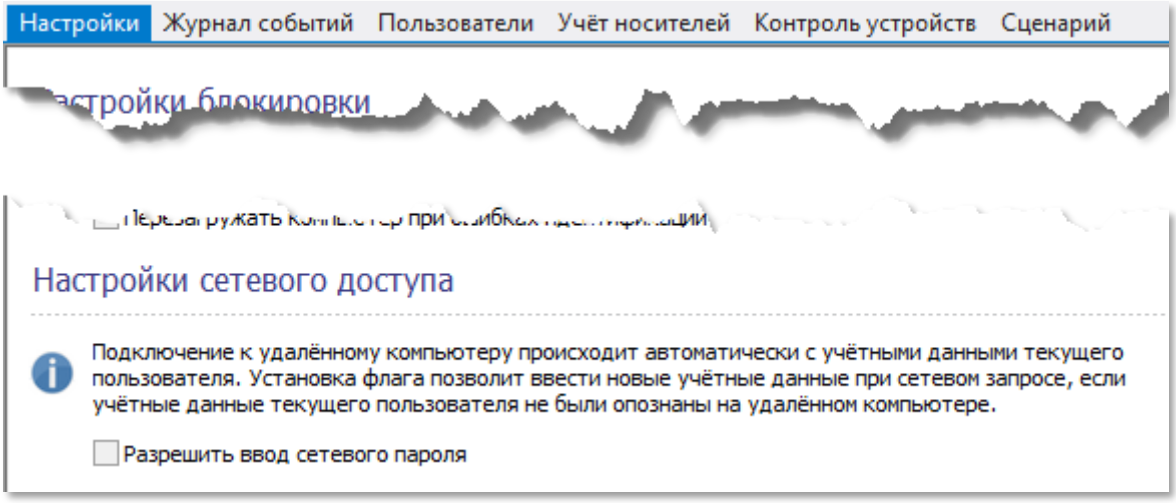


Рис. 115. Настройка сетевого доступа.

Ограничение прав локальных администраторов

В СЗИ «Страж NT» предусмотрен механизм ограничения прав пользователей, не являющихся администраторами системы защиты, но включенных в группу локальных администраторов.

При запуске процессов проверяются полномочия пользователя, и, если пользователь входит в группу локальных администраторов, но не является администратором системы защиты, то для запускаемого таким пользователем процесса отключаются права локального администратора. Данное ограничение по умолчанию включено. Для его отключения необходимо во вкладке **Настройки** программы **Консоль управления** при выборе группы настроек **Общие настройки** снять флаг в поле **Ограничивать локальных администраторов** и нажать кнопку **Сохранить настройки** (см. Рис. 47). После снятия данного флага ограничения для локальных администраторов не действуют.

Настройка принтеров

Для настройки принтеров необходимо запустить программу **Консоль управления** и во вкладке **Настройки** выбрать раздел **Настройки принтеров**. Окно настройки принтеров (см. Рис. 116) представляет собой таблицу со следующими полями: имя принтера, перечень грифов документов, печать которых разрешена на данном принтере, его размещение и статус. В списке указаны все принтеры, которые присутствуют в системе.

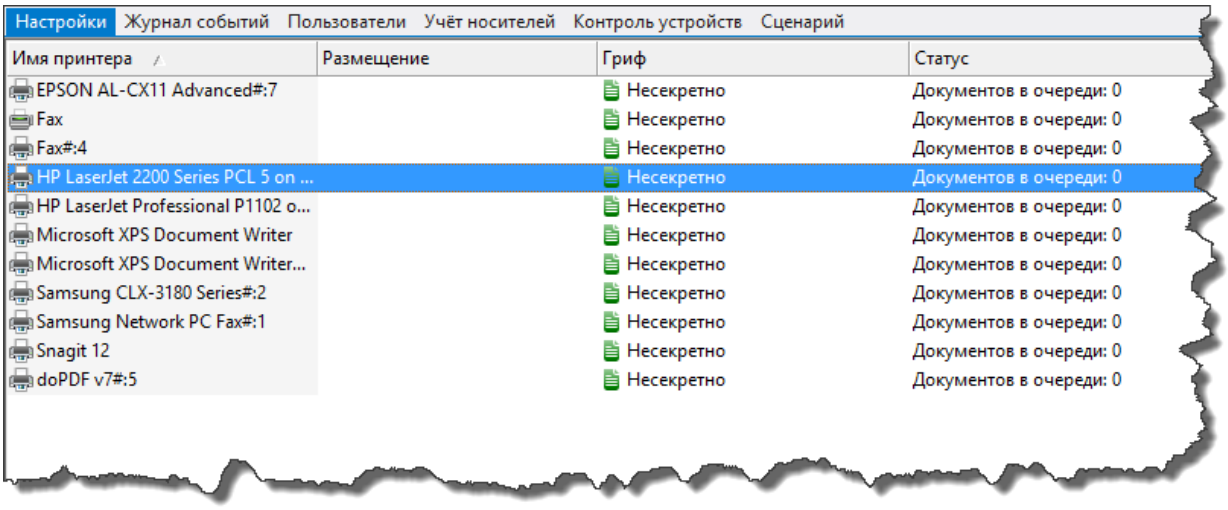


Рис. 116. Список принтеров.

Для каждого принтера существует возможность ограничения печати документов с определённым грифом. Для задания ограничений необходимо вызвать окно параметров принтера путём двойного клика мыши на соответствующей записи принтера и снять флаги с тех грифов, печать которых запрещена на данном принтере (см. Рис. 117).

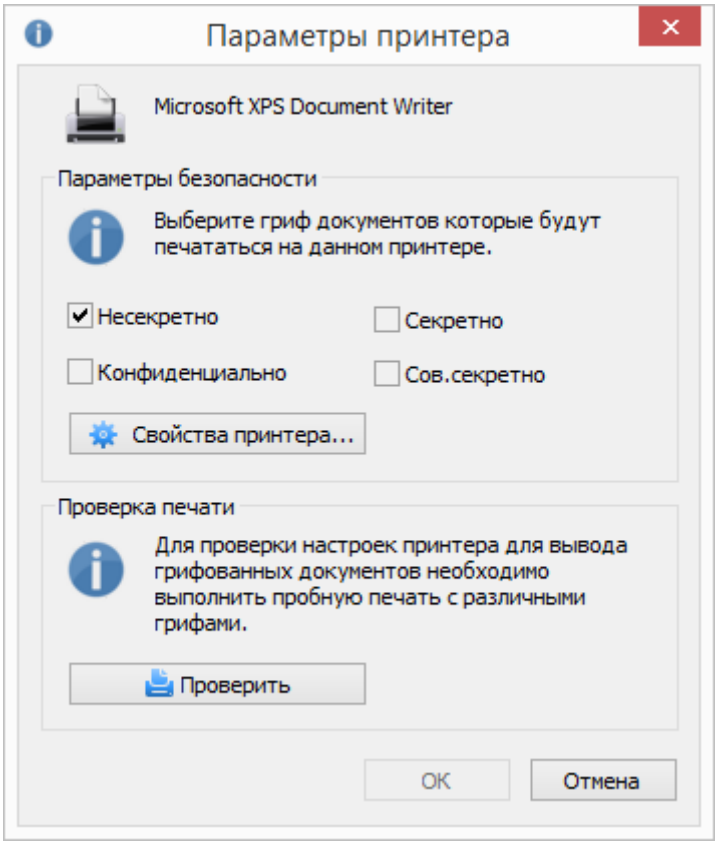


Рис. 117. Свойства принтера.

При нажатии на кнопку Свойства принтера... появляется окно свойств принтера, в котором можно выбрать вкладку **Безопасность**. При ее выборе появляется окно редактора разрешений для выбранного принтера, в котором отображается список пользователей и групп пользователей, перечисленных в списке контроля доступа, а также разрешения для выбранного выше субъекта доступа. Для изменения разрешений выбранного принтера необходимо нажать соответствующие кнопки на диалоге.

Для проверки настроек принтера необходимо нажать кнопку Проверить. При этом на данный принтер будут осуществляться попытки печати тестовых документов всех разрешенных для печати грифов.

Настройка принтеров доступна только для локального компьютера.

В большинстве случаев для осуществления печати грифованных документов дополнительно потребуется применить сценарий настроек «Настройка печати», входящий в комплект типовых сценариев (опубликован на сайте продукта).

Для сохранения настроек принтера, необходимо нажать кнопку OK.

Маркировка документов

В СЗИ «Страж NT» существует возможность маркировки всех документов, выдаваемых на печать. Параметры маркировки документов задаются в программе **Консоль управления** во вкладке **Настройки** при выборе раздела **Маркировка документов**.

Администратор системы защиты может изменять настройки маркировки документов, определяя документы каких грифов будут маркироваться, по каким правилам и какие поля будут заполняться. При этом в правой части окна будет отображен примерный вид маркированного документа.

При изменении настроек для сохранения необходимо нажать кнопку Сохранить настройки, для возврата к настройкам по умолчанию – кнопку Стандартные настройки.

Параметры раздела **Маркировка документов** определяют общие настройки для всех маркируемых страниц (см. Рис. 118).

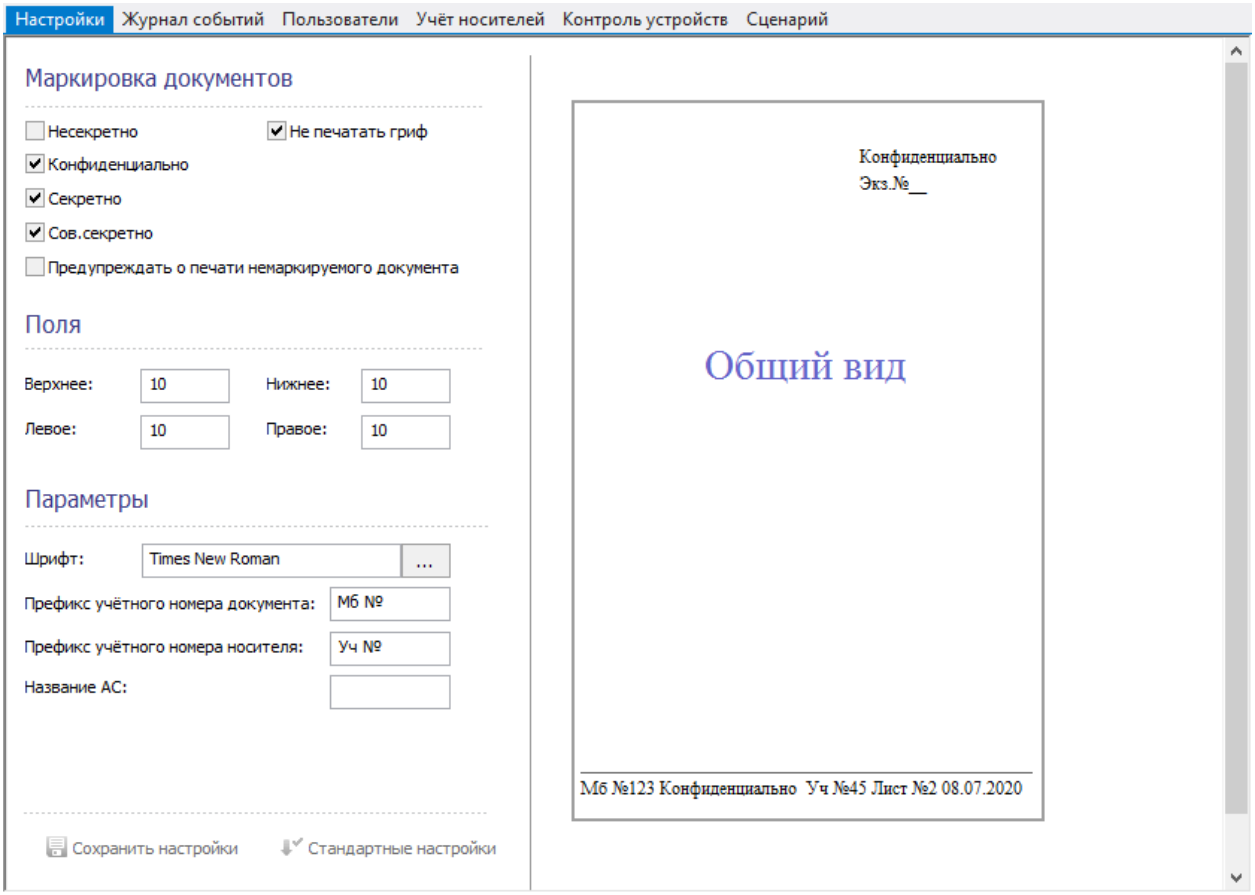


Рис. 118. Настройка параметров маркировки документов - Общие.

В области **Маркировка документов** определены четыре поля с названиями меток конфиденциальности. Установка флагов в этих полях означает, что документы, имеющие соответствующую метку, будут маркироваться согласно установленным правилам. Для документов, имеющих самую низкую метку конфиденциальности, существует возможность не выводить ее значение. Для этого необходимо установить флаг в поле **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.

В случае установки флага в поле **Предупреждать о печати немаркируемого документа** при попытке печати документа, для которого была отключена маркировка, на экран будет выдано предупреждение с указанием грифа распечатываемого документа. Предупреждение выдаётся для документов с грифом выше «Несекретно».

Угловой штамп

Параметры раздела **Угловой штамп** (см. Рис. 119) определяют настройки маркировки углового штампа документа, а именно: позицию, шрифт, поля и их порядок штампа, который печатается в верхнем правом углу первой страницы маркируемого документа.

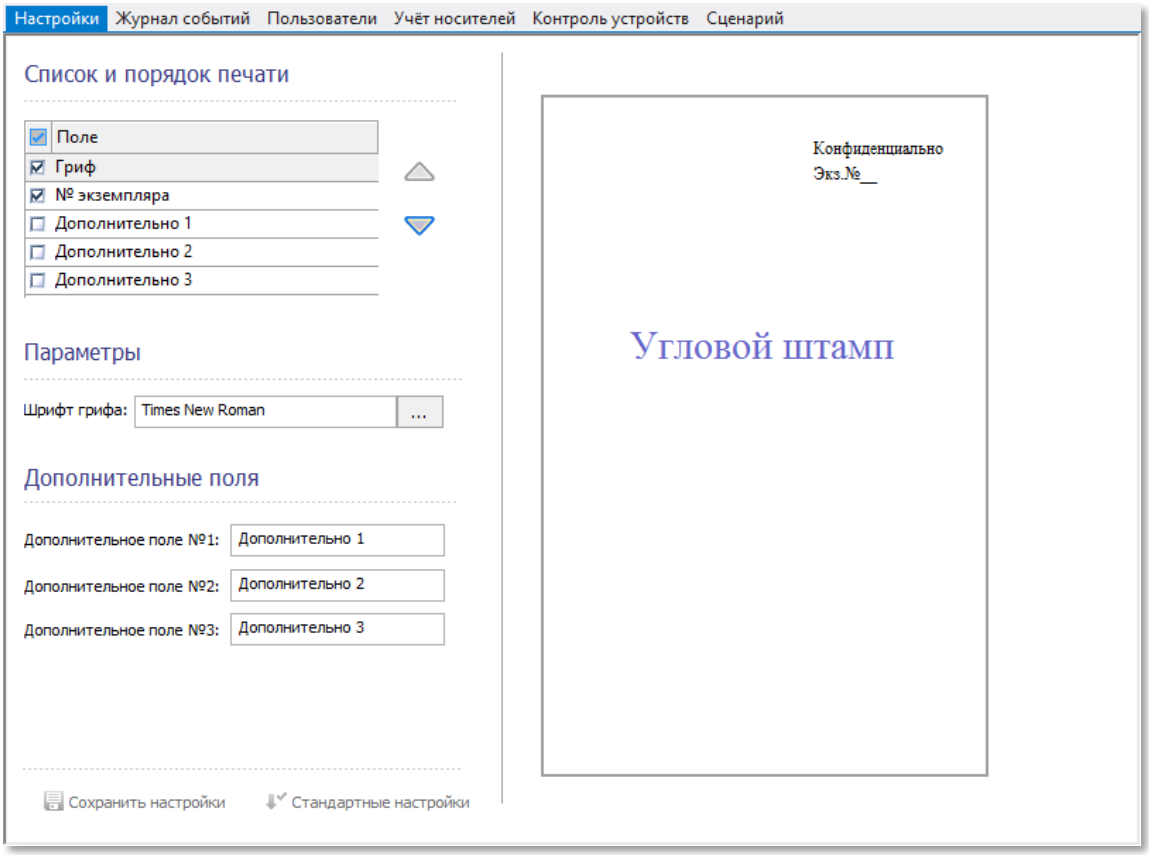


Рис. 119. Настройка параметров маркировки документов - Угловой штамп.

В области **Список и порядок печати** перечислены поля, которые могут быть выведены на печать в угловом штампе. Если флаг в первом столбце поля будет установлен, поле будет выведено на печать. Порядок печати полей можно изменить, нажимая кнопки  и  . Поле **Шрифт грифа** определяет параметры шрифта, которым будет выводиться метка конфиденциальности документа. Изменить шрифт можно, нажав кнопку  .

Дополнительные поля служат для возможности вывода дополнительной информации о документе в угловом штампе. Администратор системы защиты имеет возможность изменить название дополнительных полей, выводимых на печать.

Нижний штамп

Параметры раздела **Нижний штамп** (см. Рис. 120) определяют настройки маркировки нижнего штампа документа, который печатается в низу на каждой страницы маркируемого документа кроме последней.

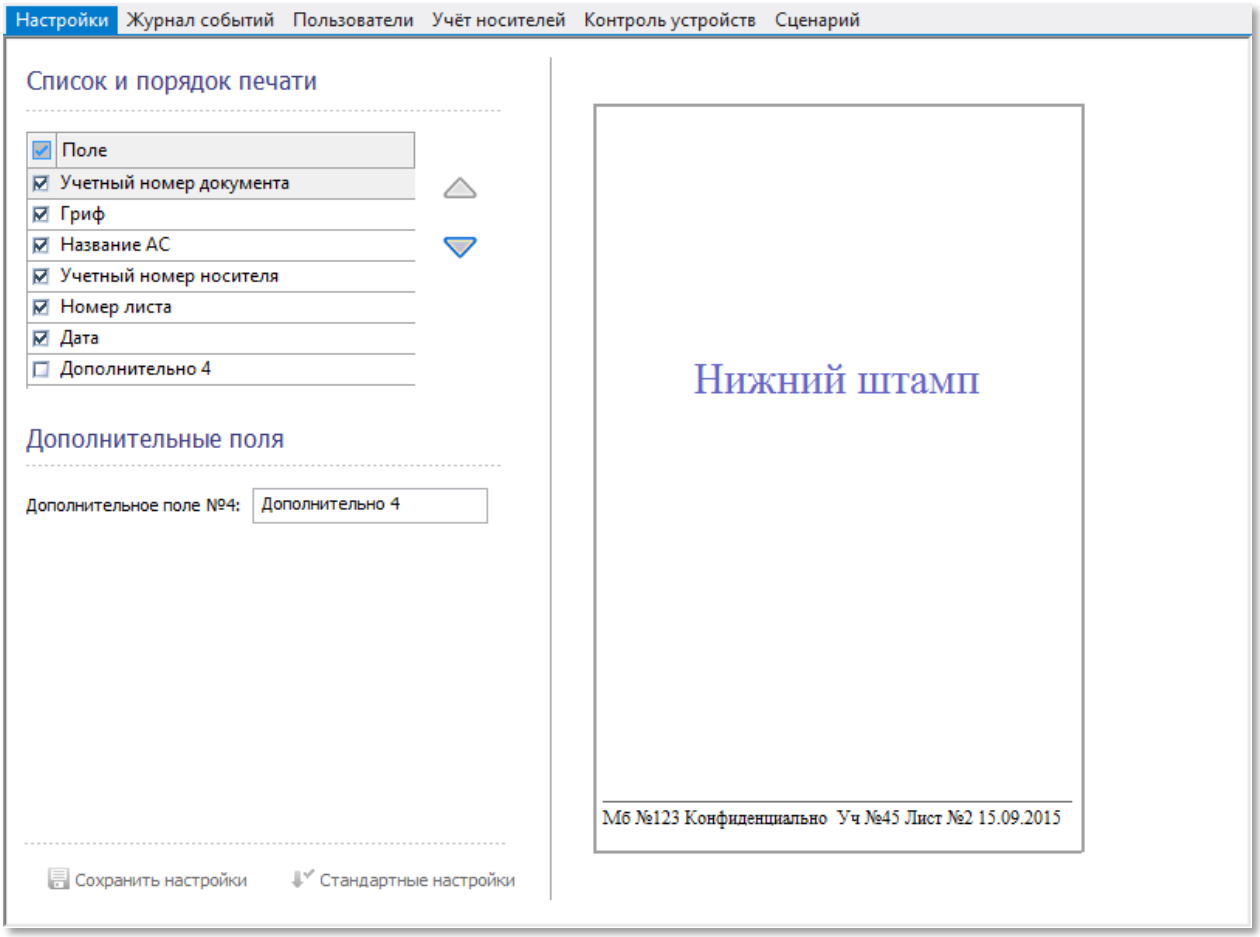


Рис. 120. Настройка параметров маркировки документов - Нижний штамп.

В области **Список и порядок печати** перечислены поля, которые могут быть выведены на печать в нижнем штампе. Если флаг в первом столбце поля будет установлен, поле будет выведено на печать. Порядок печати полей можно изменить, нажимая кнопки  и  . Администратор системы защиты имеет возможность изменить название дополнительного поля, выводимого на печать.

Последний лист

Параметры раздела **Последний** лист (см. Рис. 121) определяют настройки маркировки нижнего штампа, который печатается на последней странице маркируемого документа.

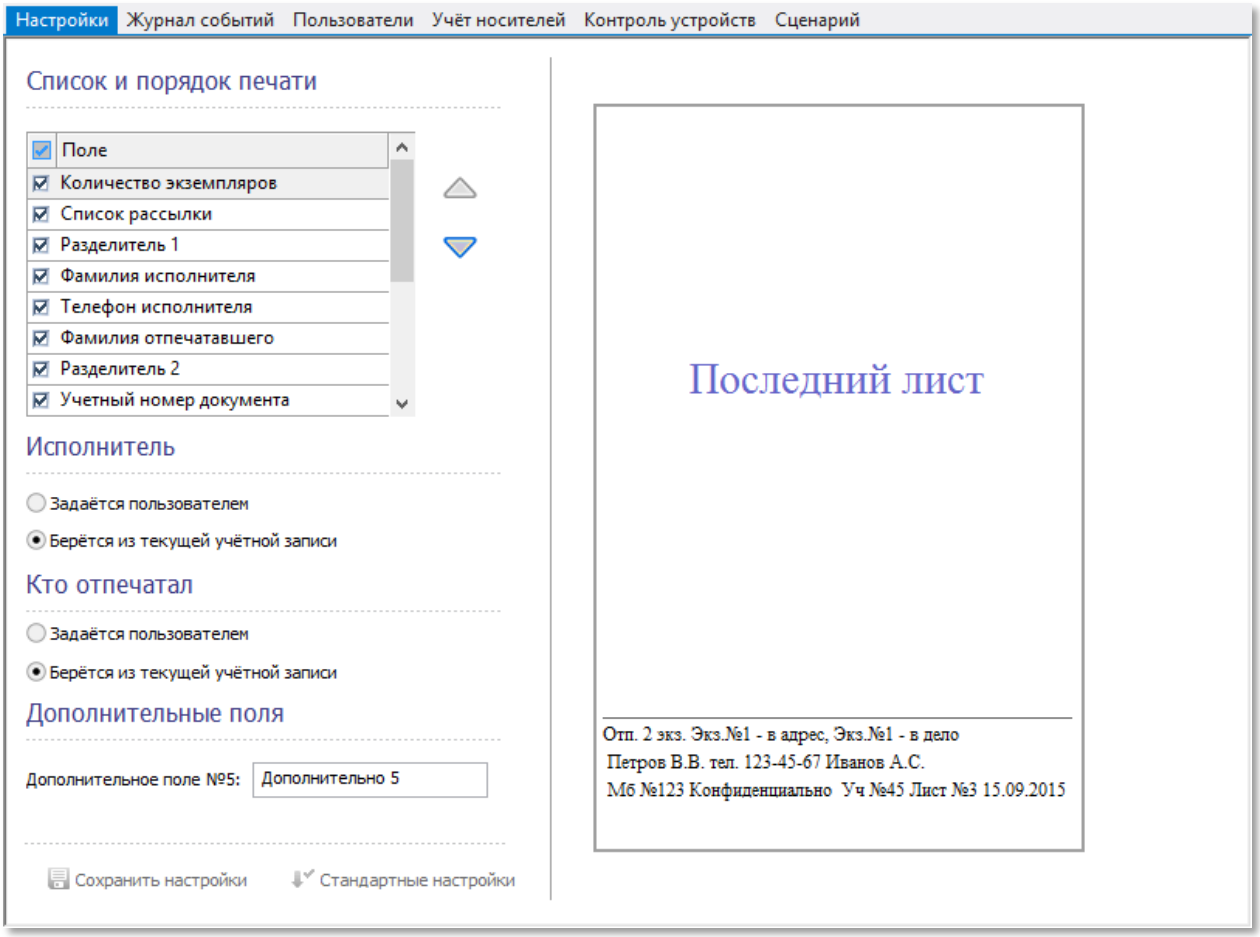


Рис. 121. Настройка параметров маркировки документов - Последний лист.

В области **Список и порядок печати** перечислены поля, которые могут быть выведены на печать в нижнем штампе. Если флаг в первом столбце поля будет установлен, поле будет выведено на печать. Порядок печати полей можно изменить, нажимая кнопки  и  . Администратор системы защиты имеет возможность изменить название дополнительного поля, выводимого на печать. Если в области **Исполнитель** установлен флаг в поле **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 флаг в поле **Задается пользователем**, во время печати документа пользователь самостоятельно должен ввести свое имя. В противном случае, имя пользователя, отпечатавшего документ, берется из текущей учетной записи.

Печать документов

При печати документа из какого-либо приложения на экране появится окно, пример которого показан на Рис. 122. 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.

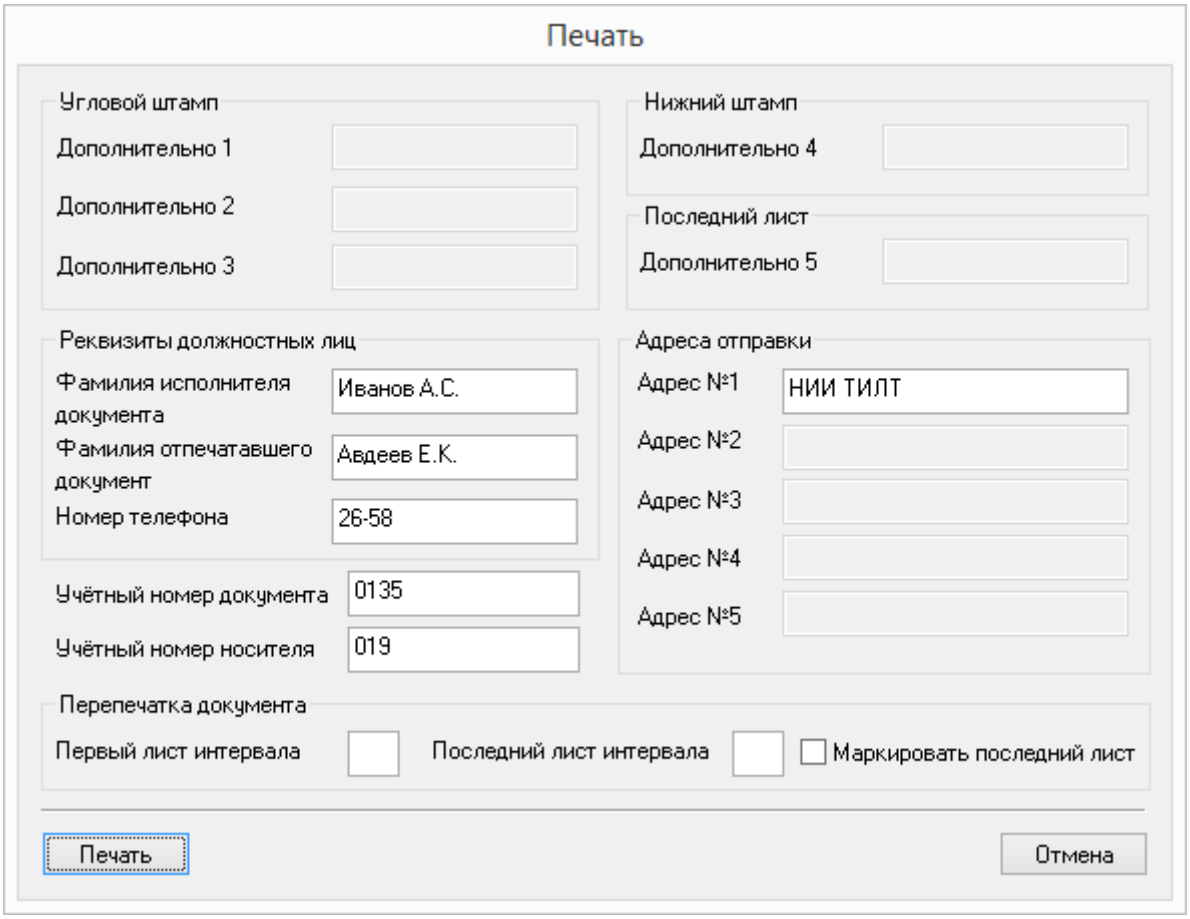


Рис. 122. Пример окна маркировки печати.

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».

Очистка памяти

Параметры очистки памяти задаются во вкладке **Настройки** программы **Консоль управления** при выборе раздела **Общие настройки** (см. Рис. 123).

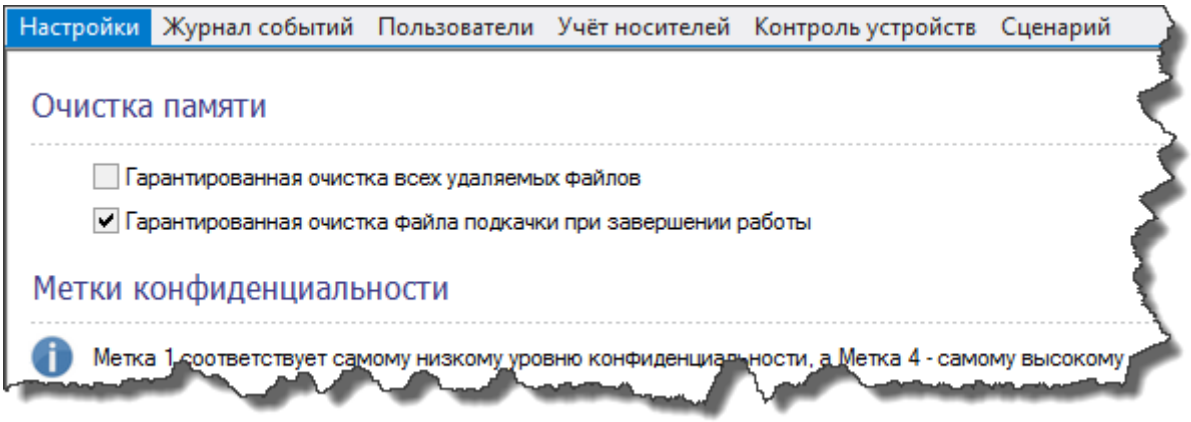


Рис. 123. Параметры очистки памяти.

Установка флага в поле **Гарантированная очистка всех удаляемых файлов** означает, что все удаляемые файлы в системе перед удалением будут заполняться случайной

последовательностью байтов. Если флаг не установлен, данный режим принудительно действует только при удалении файлов, имеющих гриф выше «Несекретно».

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

Установка флага в поле **Гарантированная очистка файла подкачки при завершении работы** означает, что при выключении (перезагрузке) компьютера файл подкачки **pagefile.sys**, а также файл **hyperfil.sys** будет заполняться нулями.

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

Блокировка и разблокировка 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-токенов для блокировки компьютера необходимо извлечь идентификатор. Для запрета блокировки компьютера при изъятии USB-токена 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. 124). Включение режима блокировки происходит путем повторного выбора указанного пункта меню.

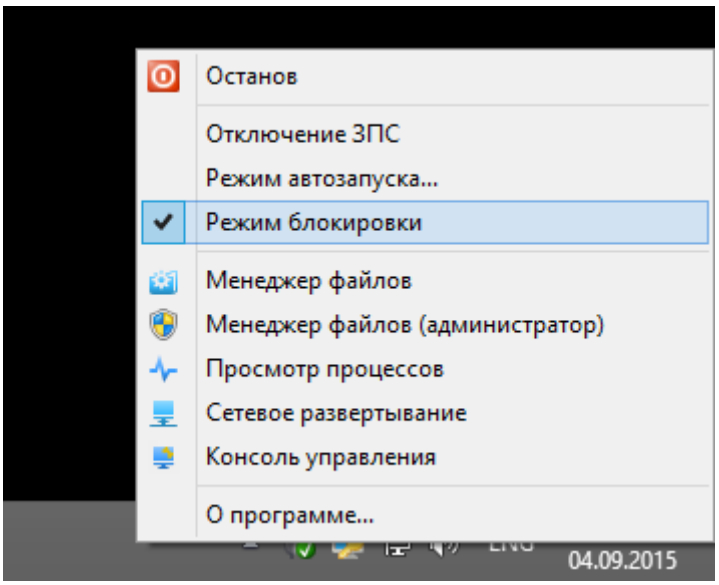


Рис. 124. Включение/выключение режима блокировки.

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. 125.

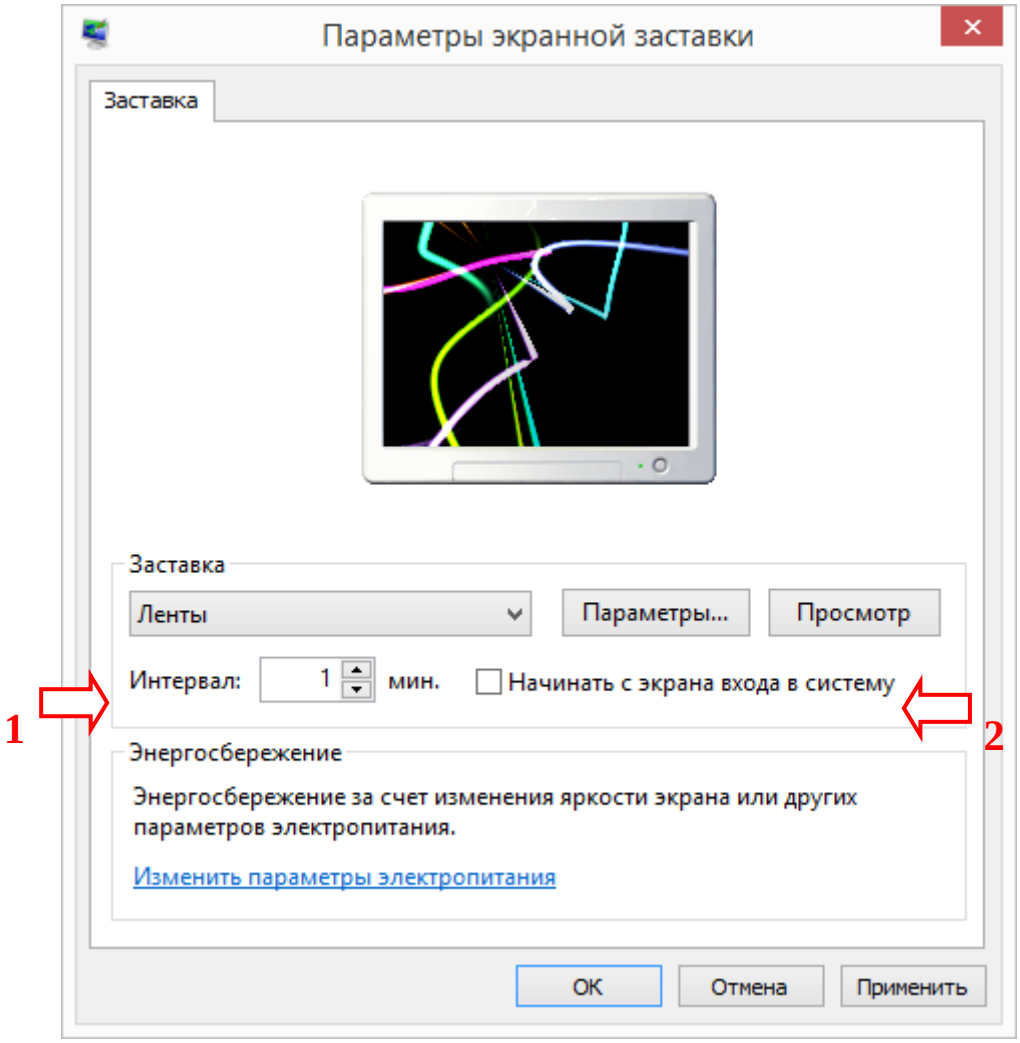


Рис. 125. Задание блокировки компьютера по истечении заданного интервала.

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.

Параметры блокировки/разблокировки компьютера

Параметры разблокировки компьютера задаются во вкладке **Настройки** программы **Консоль управления** при выборе раздела **Политики паролей** (см. 0). При установке флага в поле **Запрашивать пароль при разблокировке компьютера** при каждой разблокировке компьютера будет запрашиваться пароль пользователя, чей идентификатор установлен в системе.

При установке флага в поле **Разрешить отключение режима блокировки** пользователь, не являющийся администратором системы защиты, сможет с помощью контекстного меню программы **Монитор системы защиты** отключить режим блокировки. В противном случае, данный пункт меню ему будет недоступен.

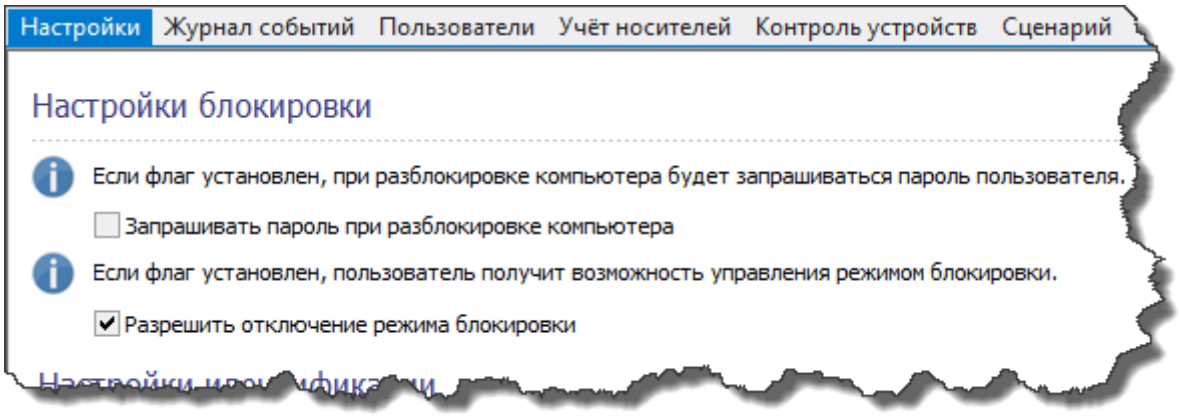


Рис. 126. Параметры разблокировки компьютера.

Управление настройками

В СЗИ «Страж NT» существует возможность управлять настройками защищаемых ресурсов и настройками самой системы защиты. Под управлением настройками защищаемых ресурсов понимается сохранение, автоматическое архивирование и восстановление настроек защищаемых ресурсов, таких как: папки и файлы, носители информации, группы устройств. Механизмы управления настройками защищаемых ресурсов будут необходимы при снятии «слепков настроек», например, перед установкой нового программного обеспечения или пакета обновления операционной системы. Под управлением настройками СЗИ понимается экспорт настроек СЗИ в файл или на другой компьютер и импорт настроек СЗИ из файла.

Архивирование настроек ресурсов

Архивирование настроек осуществляется по расписанию, заданному администратором системы защиты. Задание параметров автоматической архивации настроек ресурсов осуществляется во вкладке **Настройки** программы **Консоль управления** при выборе раздела **Настройки архивации** (см. Рис. 127).

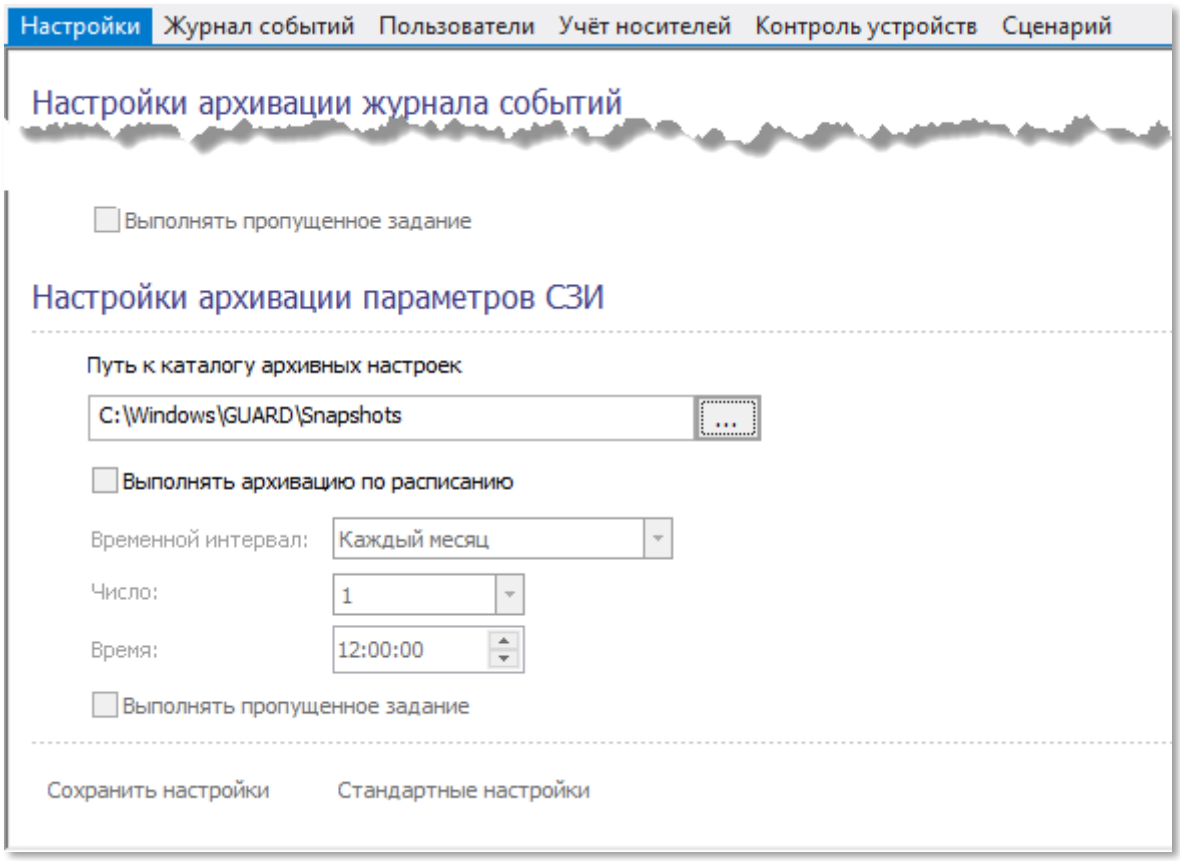
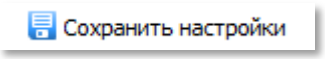


Рис. 127. Параметры архивации настроек ресурсов.

В параметрах необходимо задать папку, в которую будут сохраняться файлы ресурсов, а также периодичность архивации.

Для сохранения настроек необходимо нажать кнопку 

, для возврата к настройкам по умолчанию – кнопку 

.

Сохранение настроек ресурсов

Помимо процедуры периодической архивации настроек, существует возможность самостоятельно сохранить текущие настройки защищаемых ресурсов. Для этого необходимо выбрать пункт меню **Настройки ресурсов | Сохранить...** . На экране

появится стандартный диалог сохранения файла, в котором нужно выбрать путь и ввести имя файла хранения настроек ресурсов.

Восстановление настроек ресурсов

Для восстановления настроек защищаемых ресурсов необходимо выбрать пункт меню **Настройки ресурсов | Восстановить...** . В появившемся окне будут отображены все файлы настроек ресурсов, которые хранятся в выбранной папке сохранённых настроек (см. Рис. 128).

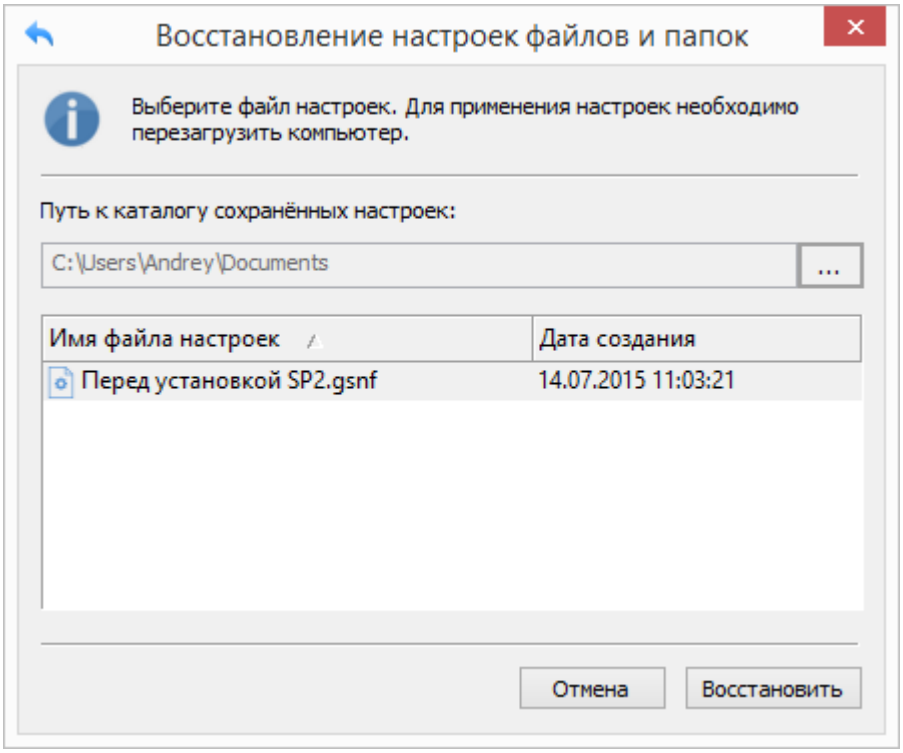


Рис. 128. Восстановление настроек файловых ресурсов.

По умолчанию, настройки защищенных ресурсов хранятся в папке **%SystemRoot%\Guard\Snapshots**. Администратор системы защиты может выбрать другую папку для загрузки настроек ресурсов, для этого необходимо нажать кнопку ... . Для восстановления настроек ресурсов, необходимо выбрать файл настроек из списка и нажать кнопку Восстановить .

Новые настройки ресурсов будут применены после перезагрузки. Выбранный файл настроек ресурсов должен быть доступен на момент загрузки операционной системы.

Экспорт и импорт настроек СЗИ

Для экспорта настроек системы защиты необходимо выбрать пункт меню **Настройки СЗИ | Экспорт...** . При этом появится окно (см.Рис. 129), в котором необходимо выбрать те настройки системы защиты, которые будут экспортироваться и нажать кнопку Далее > .

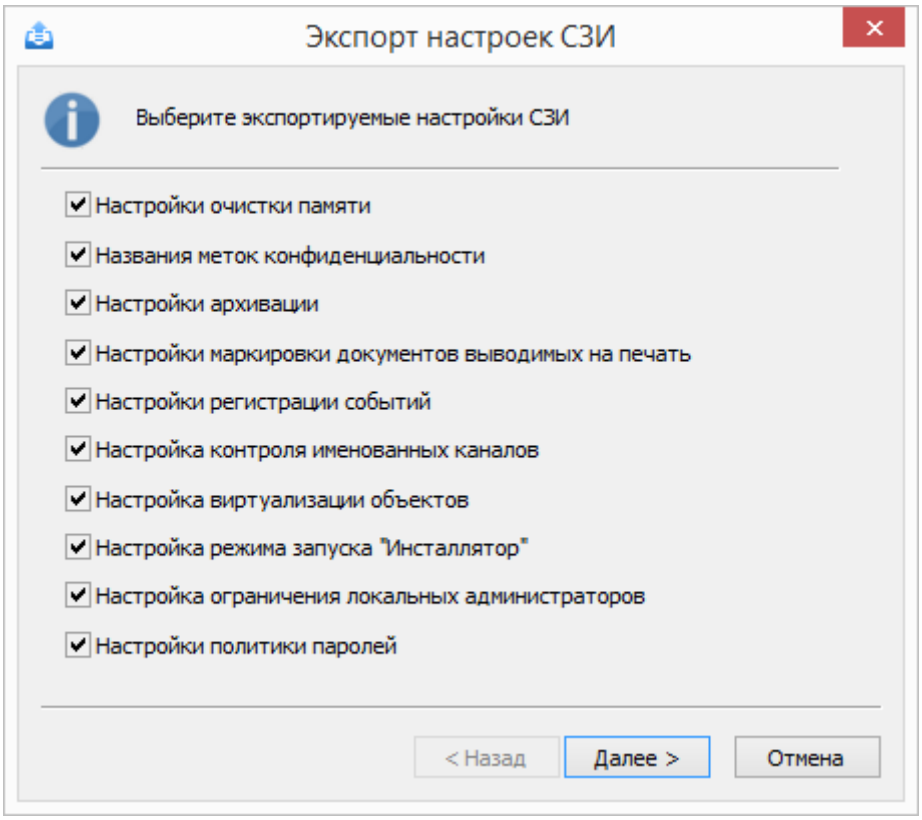


Рис. 129. Экспорт настроек СЗИ - Выбор параметров.

На следующем шаге необходимо выбрать, куда экспортируются выбранные настройки СЗИ. Настройки могут экспортироваться по сети на другие компьютеры, которые необходимо выбрать в дереве компьютеров. Также настройки СЗИ могут сохраняться в файл, путь которого можно задать, нажав на кнопку ... .

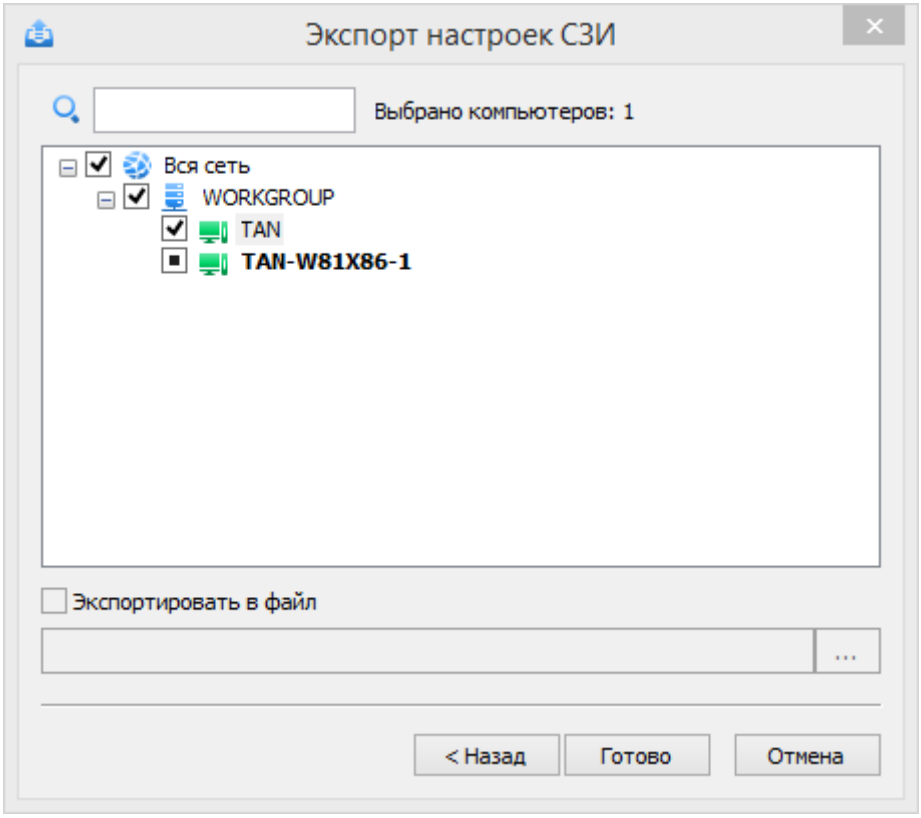


Рис. 130. Экспорт настроек СЗИ - выбор места назначения.

Для импорта настроек СЗИ необходимо выбрать пункт меню **Настройки СЗИ | Импорт...** . После этого на экране появится окно (см. Рис. 131), в котором необходимо выбрать файл, из которого будут импортироваться настройки, нажав кнопку ... .

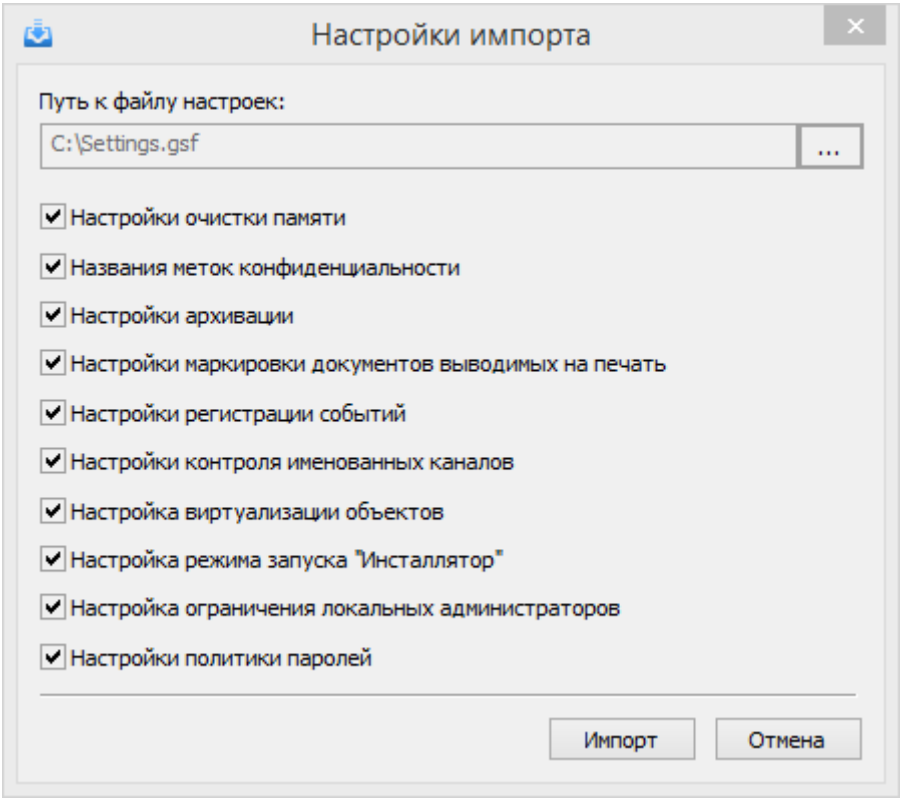


Рис. 131. Выбор параметров импорта настроек СЗИ.

После выбора файла поля, соответствующие различным типам настроек, станут доступны для выбора. Если в выбранном файле отсутствуют настройки определённой категории, соответствующее поле будет недоступно для выбора. После нажатия кнопки Импорт, настройки будут импортированы на локальный компьютер.

Отказ от настроек ресурсов

Для отказа от настроек защищаемых ресурсов системы защиты необходимо выбрать пункт меню **Настройки ресурсов | Отказаться от настроек ресурсов**. Если на предупреждающий вопрос будет дан положительный ответ, при дальнейшей перезагрузке операционной системы (или при остановке/запуске ядра СЗИ) все настройки защищаемых ресурсов будут удалены, и ядро системы защиты автоматически включит режим автозапуска.

Формирование отчетов

В СЗИ «Страж NT» предусмотрена возможность создания отчетов о настройках системы защиты. Отчёты могут содержать информацию:

- о пользователях СЗИ;

- об используемых идентификаторах;
- о зарегистрированных носителях;
- о подключенных устройствах;
- об установленных принтерах;
- о настройках защищаемых ресурсов файловой системы.

Создание отчетов осуществляется при помощи вкладки **Настройки** программы **Консоль управления**. Для создания отчета необходимо выбрать пункт меню **Отчёт | Создать отчёт...** . При этом появляется окно (см. Рис. 132), в котором представлены два списка: список отчётов и список полей, соответствующих выбранному типу отчёта.

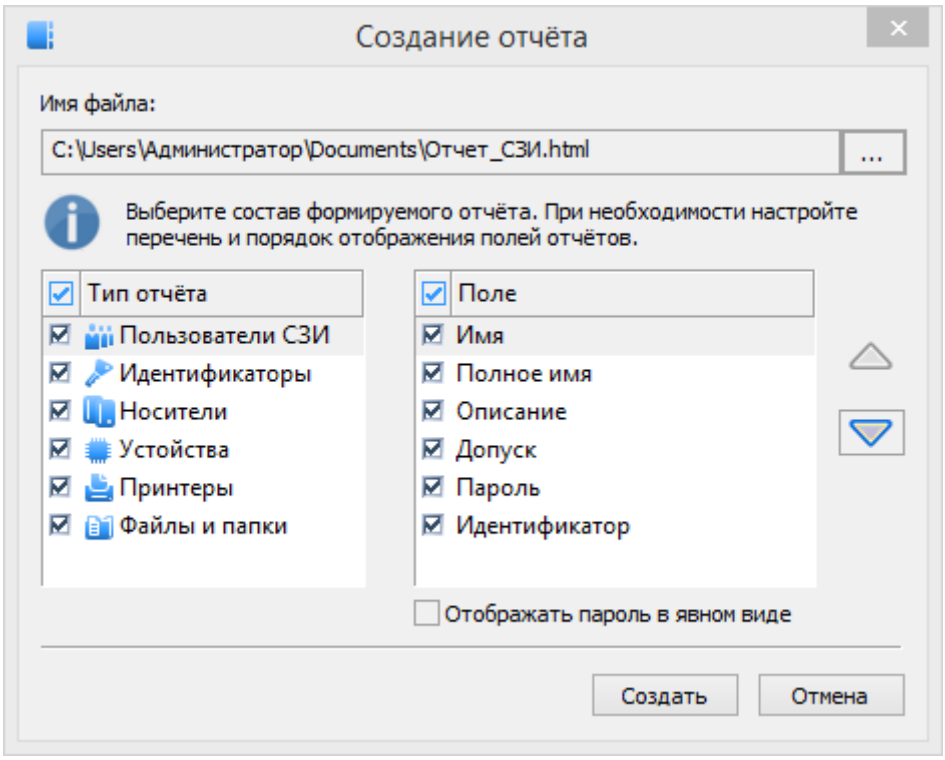


Рис. 132. Создание отчета.

Администратор системы защиты имеет возможность редактировать порядок и состав полей для каждого из типов отчётов.

При формировании отчета о пользователях существует возможность отображения паролей пользователей в открытом виде или скрыть их. Для этого необходимо соответственно установить или снять флаг в поле **Отображать пароль в явном виде**.

Отчет сохраняется в файл в формате HTML, который выберет администратор системы защиты при нажатии кнопки ... .

Сетевое развертывание

В данной главе приводятся сведения о подсистеме сетевого развертывания системы защиты. Описаны интерфейсы программы **Сетевое развертывание**, а также типовые действия администратора при сетевом развертывании системы защиты.

Общие сведения

В СЗИ "Страж NT" существует возможность установки системы защиты на удаленные компьютеры. Удаленная установка может быть осуществлена только пользователем, являющимся администратором системы защиты. Для этого необходимо выполнение следующих условий:

- удаленный компьютер должен быть включен и доступен;
- на удаленном компьютере должен быть зарегистрирован пользователь, входящий в группу локальных администраторов, имя и пароль которого совпадают с именем и паролем пользователя, осуществляющего удаленную установку.

Удаленная установка системы защиты осуществляется с помощью программы **Сетевое развертывание**. Для запуска программы необходимо выбрать пункт **Сетевое развертывание** контекстного меню программы **Монитор системы защиты** при работе с рабочим столом или выбрать пункт **Сетевое развертывание** в представлении «Приложения» начального экрана. Общий вид программы представлен на Рис. 133.

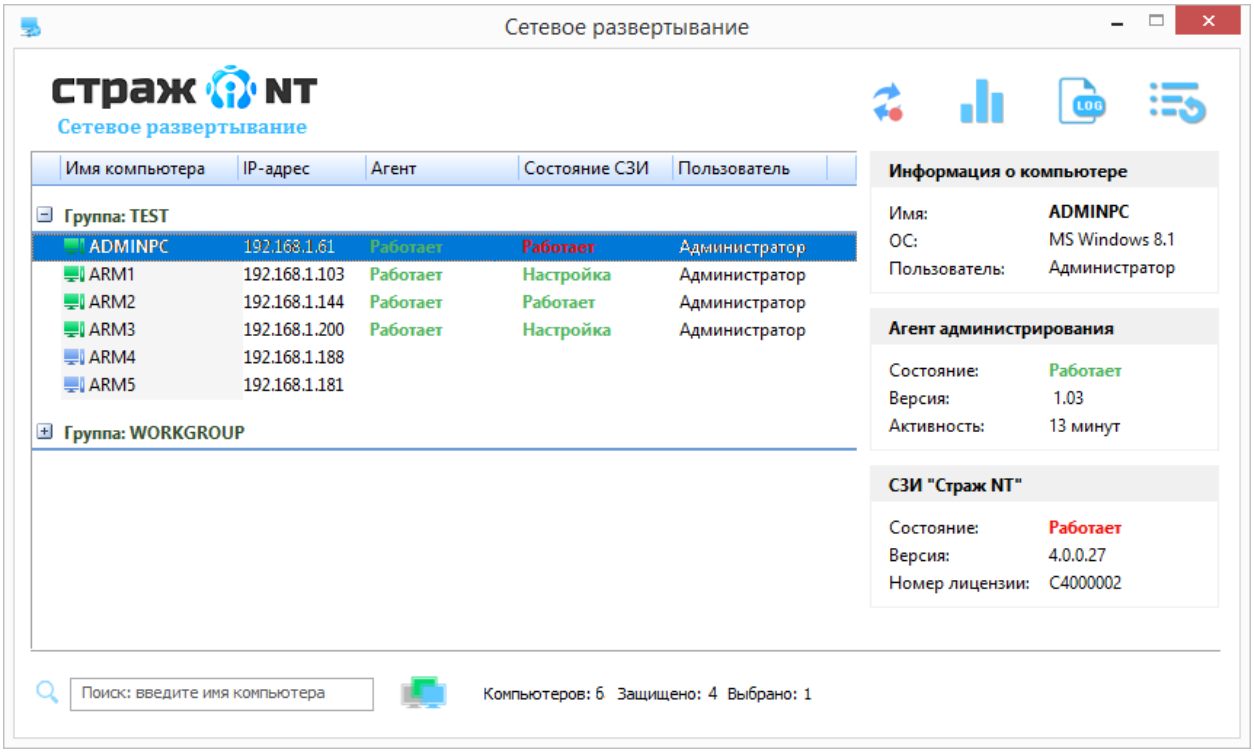


Рис. 133. Общий вид окна программы ***Сетевое развертывание.***

Слева в главном окне программы представлен список компьютеров, которые на настоящий момент видимы в локальной сети. Иконка компьютера определяет его статус:

- компьютер недоступен или выключен
- компьютер включен, СЗИ не установлена
- компьютер включен, не удалось получить информацию о состоянии СЗИ
- компьютер включен, СЗИ остановлена
- компьютер включен, СЗИ включена, работает или настраивается
- компьютер включен, идет выполнение операции

Для отображения дерева компьютеров необходимо, чтобы на компьютере, на котором запущена программа **Сетевое развертывание**, параметр сетевого обнаружения был установлен в состояние **Включено**.

Колонка **Агент** определяет состояние Агента администрирования на данном компьютере, колонка **Состояние СЗИ** – состояние системы защиты информации, колонка **Пользователь** – имя пользователя, интерактивно зарегистрированного на данный момент в системе. При выборе компьютера можно вызвать контекстное меню, в котором перечислены все доступные операции.

Операция	Описание
Обновить	Обновление информации о выбранном компьютере
Добавить компьютер на идентификатор	Добавление информации о компьютере на идентификатор администратора, если на компьютере не установлена СЗИ
Перезагрузить	Перезагрузка выбранного компьютера
Отправить сообщение о перезагрузке	Отправка на Рабочий стол текущего пользователя выбранного компьютера сообщения о необходимости выполнения перезагрузки компьютера
Выключить	Выключение выбранного компьютера
Установить Агент администрирования	Установка **Агента администрирования**
Удалить Агент администрирования	Удаление **Агента администрирования**
Установить СЗИ	Установка системы защиты информации
Удалить СЗИ	Удаление системы защиты информации
Обновить СЗИ	Обновление системы защиты информации
Включение ЗПС	Включение ЗПС на удаленном компьютере
Отключение ЗПС	Отключение ЗПС на удаленном компьютере
Режим автозапуска...	Включение и отключение режима автозапуска на удаленном компьютере
Завершить установку СЗИ	Завершение установка системы защиты информации
Подключиться к удалённому рабочему столу...	Подключение к удалённому рабочему столу выбранного компьютера
Просмотреть протоколы...	Просмотр протоколов установки и удаления СЗИ на выбранном компьютере
Проверить связь	Проверка связи с **Агентом администрирования**
Поддержка идентификаторов...	Удаленная установка драйверов поддержки USB-идентификаторов на выбранный компьютер

Справа от списка компьютеров находится более подробные сведения о выбранном компьютере: его операционная система, состояние, версия и активность **Агента администрирования**, а также состояние, версия и серийный номер системы защиты информации, если она установлена.

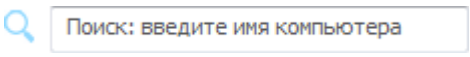
В главном окне программы расположены кнопки:

 – включение автоматического обновления СЗИ в сети;

 – формирование сводного отчета по компьютерам;

 – просмотр общего протокола программы;

 – обновление списка компьютеров.

Внизу главного окна программы расположено поле поиска компьютеров. При вводе в 

данном поле текста, в списке будет выделяться первый компьютер, имя которого удовлетворяет введенному фильтру.

Также внизу главного окна программы расположена кнопка фильтра отображаемых компьютеров  , за которой отображается информация об общем количестве компьютеров в списке и количестве компьютеров с установленной системой защиты

Удаленная установка системы защиты

Удаленная установка системы защиты выполняется в несколько этапов:

- установка Агента администрирования;
- установка СЗИ;
- настройка СЗИ;
- завершение установки.

Все операции по установке и настройке **Агента администрирования** и системы защиты можно проводить параллельно для нескольких компьютеров.

Установка Агента администрирования

Для установки **Агента администрирования** необходимо выбрать в списке компьютер, на который планируется установить систему защиты, вызвать его контекстное меню и выбрать пункт **Установить Агент администрирования**. При этом в поле **Агент** выбранной записи будет отображено значение **Установка...** . После успешной установки **Агента администрирования** в колонке **Агент** будет отображено значение **Работает**. При ошибке установки в поле **Агент** будет отображено значение **Ошибка установки**. Причину возникновения ошибки можно просмотреть, открыв общий протокол программы, как описано выше.

Установка системы защиты информации

Для установки системы защиты информации необходимо выбрать в списке компьютер, на котором уже установлен **Агент администрирования**, вызвать его контекстное меню и выбрать пункт **Установить СЗИ...** . На экране появится диалог, в котором необходимо будет ввести лицензионный номер комплекта СЗИ (см. Рис. 134). После корректного ввода лицензионного номера нажать кнопку Далее > .

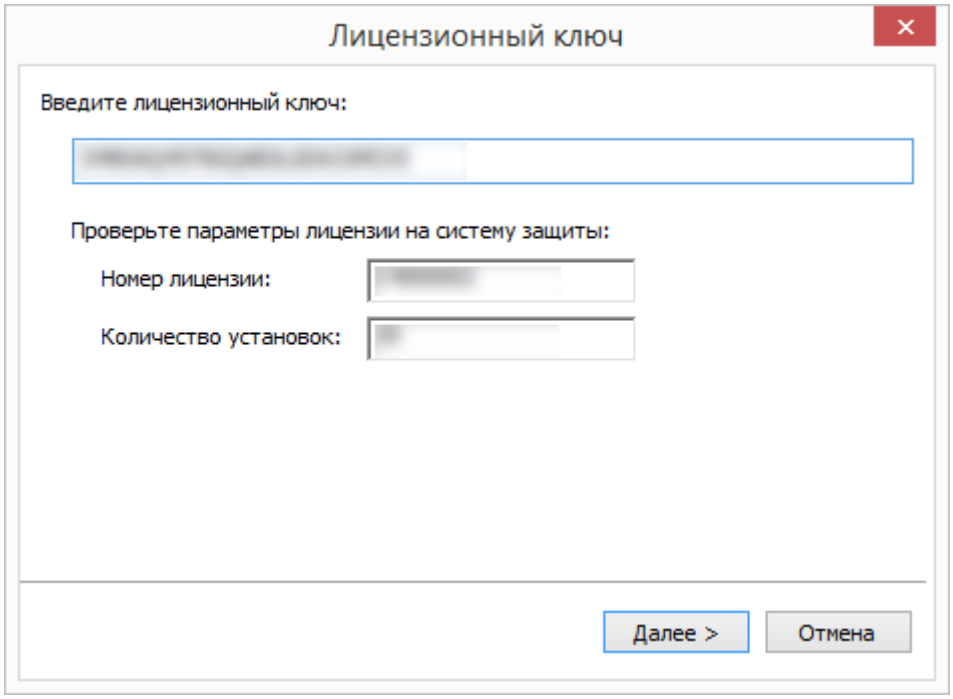


Рис. 134. Ввод лицензионного номера.

В следующем диалоговом окне необходимо определить параметры установки системы защиты. Для настройки дополнительных параметров необходимо нажать кнопку

Дополнительные параметры... . Подробное описание параметров установки системы защиты приведено в разделе **Установка системы защиты**.

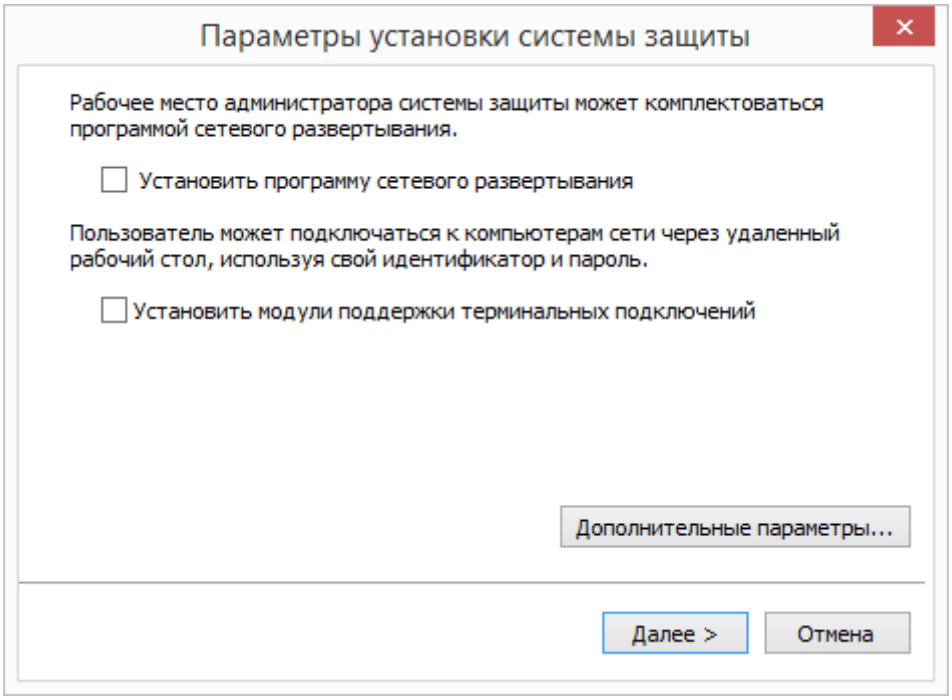


Рис. 135. Определение параметров установки

Если в процессе настройки параметров удаленного компьютера будет определено, что на удаленном компьютере включен режим быстрого запуска операционной системы, на экран появится сообщение, примерный текст которого показан на Рис. 10 или Рис. 11. Рекомендуется выключить режим быстрого запуска операционной системы на удаленном компьютере, как описано в разделе **Установка системы защиты**.

Затем на экране появится диалоговое окно формирования персонального идентификатора администратора системы защиты. В поле **Идентификатор** будет выбрано значение типа идентификатора, с помощью которого администратор системы защиты вошел в систему, а в поле **Пароль** - введен его пароль.

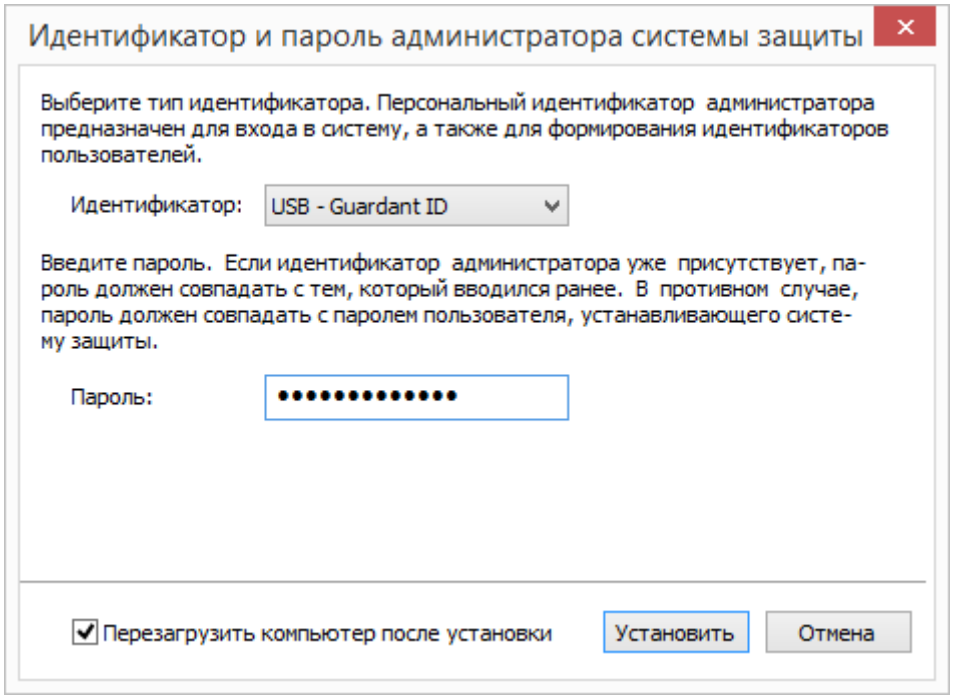


Рис. 136. Формирование идентификатора администратора.

Если необходимо автоматически перезагрузить компьютер после установки системы защиты, требуется установить флаг в поле **Перезагрузить компьютер после установки.** Компьютер будет перезагружен только в случае успешной установки системы защиты. Для начала установки системы защиты необходимо нажать кнопку Установить. При этом в поле **СЗИ** будет отображено значение **Установка...** .

При формировании идентификатора администратора системы защиты на экране появится запрос предъявления идентификатора администратора. Отказаться от установки СЗИ можно, нажав кнопку Отмена.

При ошибке установки в поле **СЗИ** будет отображено значение **Ошибка установки**. Причину возникновения ошибки можно просмотреть, выбрав пункт **Просмотреть протоколы...** контекстного меню компьютера.

В случае успешной установки системы защиты и выполнения перезагрузки компьютера в поле **СЗИ** будет отображено значение **Настройка**. При этом на удаленном компьютере при загрузке операционной системы у пользователей не будет запрашиваться предъявление персонального идентификатора и пароля для возможности удаленной загрузки и настройки системы защиты.

Настройка системы защиты информации

После установки системы защиты и перезагрузки компьютера необходимо последовательно настроить все защитные механизмы, как описано в соответствующих разделах. Для этого можно воспользоваться либо программой **Консоль управления** либо подключиться к удаленному рабочему столу компьютера вызвав его контекстное меню и выбрав пункт меню **Подключиться к удаленному рабочему столу...** . После настройки системы защиты необходимо осуществить завершение ее установки.

Завершение установки системы защиты информации

Для завершения установки системы защиты необходимо выбрать в списке компьютер, для которого в поле **СЗИ** отображено значение **Настройка**, вызвать для него контекстное меню, выбрать пункт **Завершить установку СЗИ** и подтвердить действие.

В появившемся окне (см. Рис. 137) выбрать дальнейшие операции с компьютером.

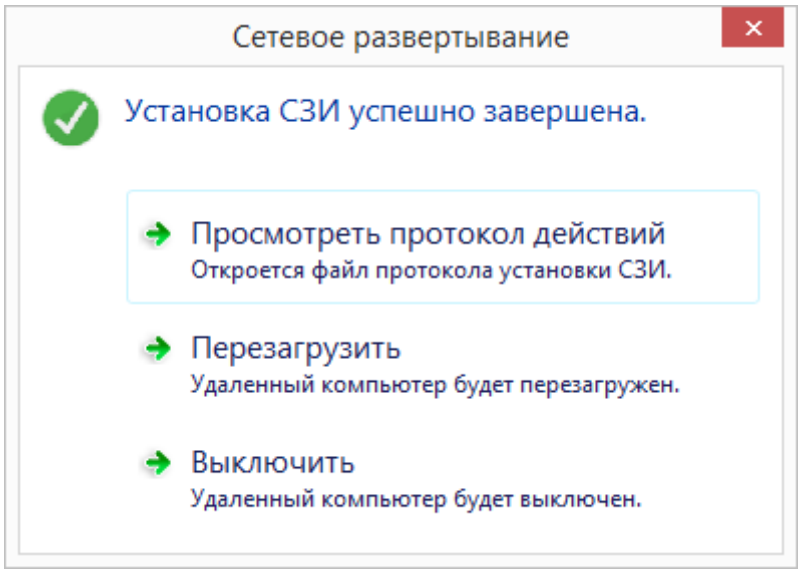


Рис. 137. Запрос действий при завершении установки СЗИ.

Удаление системы защиты

Удаление системы защиты выполняется в несколько этапов:

- удаление системы защиты информации;
- удаление **Агента администрирования** (при необходимости).

Все операции по удалению системы защиты и **Агента администрирования** можно проводить параллельно для нескольких компьютеров.

Удаление системы защиты информации

Для удаления системы защиты информации необходимо выполнить следующие действия выбрать в списке компьютер, на котором установлена система защиты информации, вызвать его контекстное меню и выбрать пункт **Удалить СЗИ...** .

На экране появится диалог (см. Рис. 138), в котором необходимо определить параметры удаления системы защиты, как описано в разделе **Удаление СЗИ**.

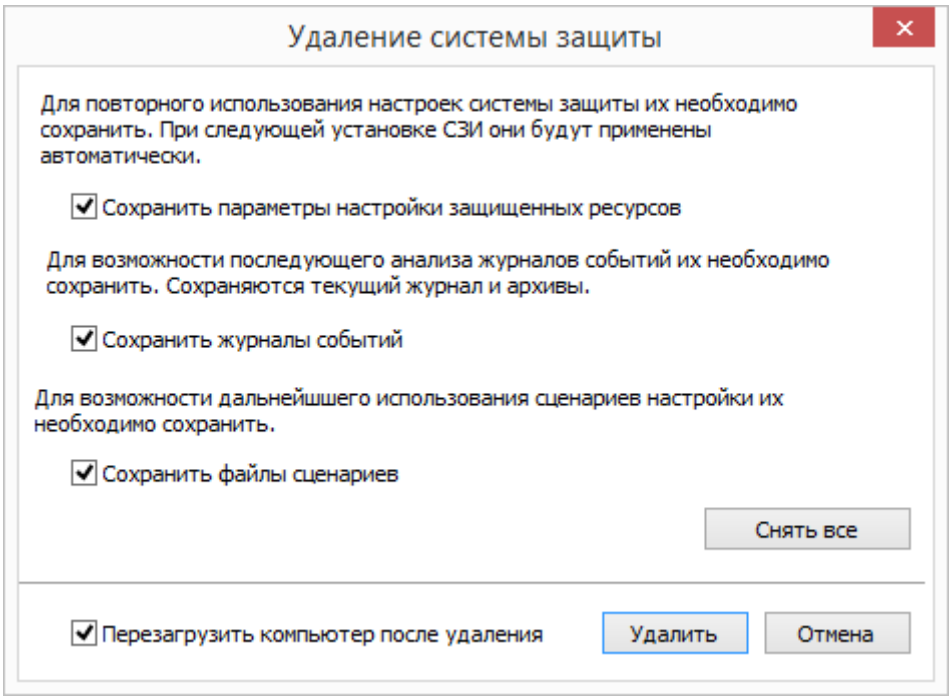


Рис. 138. Определение параметров удаления СЗИ.

Если необходимо автоматически перезагрузить компьютер после установки системы защиты, установить флаг в поле **Перезагрузить компьютер после установки.** Компьютер будет перезагружен только в случае успешного удаления системы защиты.

После нажатия кнопки Удалить начнется удаление системы защиты. При этом в поле **СЗИ** будет отображено значение **Удаление...** . После успешного удаления системы защиты в колонке **СЗИ** будет отображено пустое значение.

При ошибке удаления в поле **СЗИ** будет отображено значение **Ошибка удаления**. Причину возникновения ошибки можно просмотреть, выбрав пункт **Просмотреть протоколы...** контекстного меню компьютера.

Удаление Агента администрирования

Для удаления **Агента администрирования** необходимо выполнить следующие действия выбрать в списке компьютер, на котором уже установлен **Агент администрирования**, вызвать его контекстное меню и выбрать пункт **Удалить Агент администрирования**. При этом в поле **Агент** будет отображено значение **Удаление...** . После успешного удаления **Агента администрирования** в колонке **Агент** будет отображено пустое значение. При ошибке удаления в поле **Агент** будет отображено значение **Ошибка удаления**. Причину возникновения ошибки можно просмотреть, выбрав пункт **Просмотреть протоколы...** контекстного меню компьютера.

Удаленная установка драйверов идентификаторов

С помощью программы **Сетевое развертывание** существует возможность удаленно устанавливать драйверы USB-ключей, используемых в качестве персональных идентификаторов пользователей. Для удаленной установки драйверов необходимо, чтобы на удаленном компьютере уже был установлен **Агент администрирования**.

Для удаленной установки драйверов USB-ключей необходимо выбрать в списке компьютер, на котором уже установлен **Агент администрирования**, вызвать его контекстное меню и выбрать пункт **Поддержка идентификаторов...** .

В появившемся окне (см. Рис. 139) необходимо выбрать соответствующий тип идентификаторов, определить его состояние на удаленном компьютере и при необходимости нажать кнопку **Установить драйверы.**

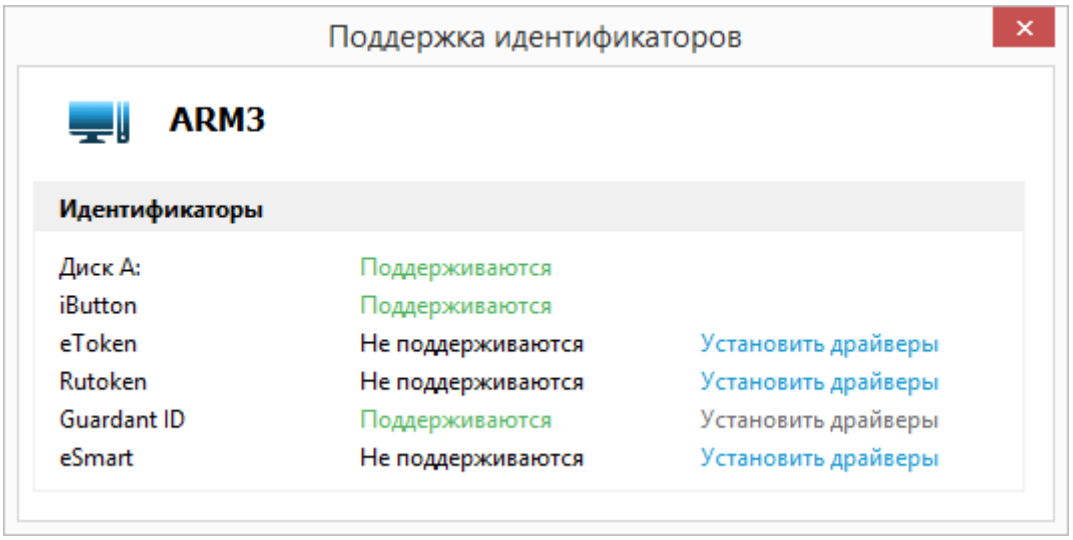


Рис. 139. Установка драйверов.

Тестирование системы

В СЗИ «Страж NT» предусмотрена подсистема тестирования механизмов системы защиты, которая предназначена для проверки функционирования следующих основных механизмов системы защиты:

- Дискреционный контроль доступа;
- Мандатный контроль доступа;
- Контроль ввода-вывода информации на отчуждаемые носители;
- Контроль целостности.

Тестирование механизмов системы защиты осуществляется при помощи вкладки **Настройки** программы **Консоль управления**. Для начала тестирования необходимо выбрать пункт меню **Тестирование | Запуск теста...**. При этом появляется окно (см. Рис. 140) со списком всех проверок, которые могут быть выполнены в рамках тестирования механизмов системы защиты. Администратор должен выбрать перечень необходимых проверок и нажать кнопку Далее > .

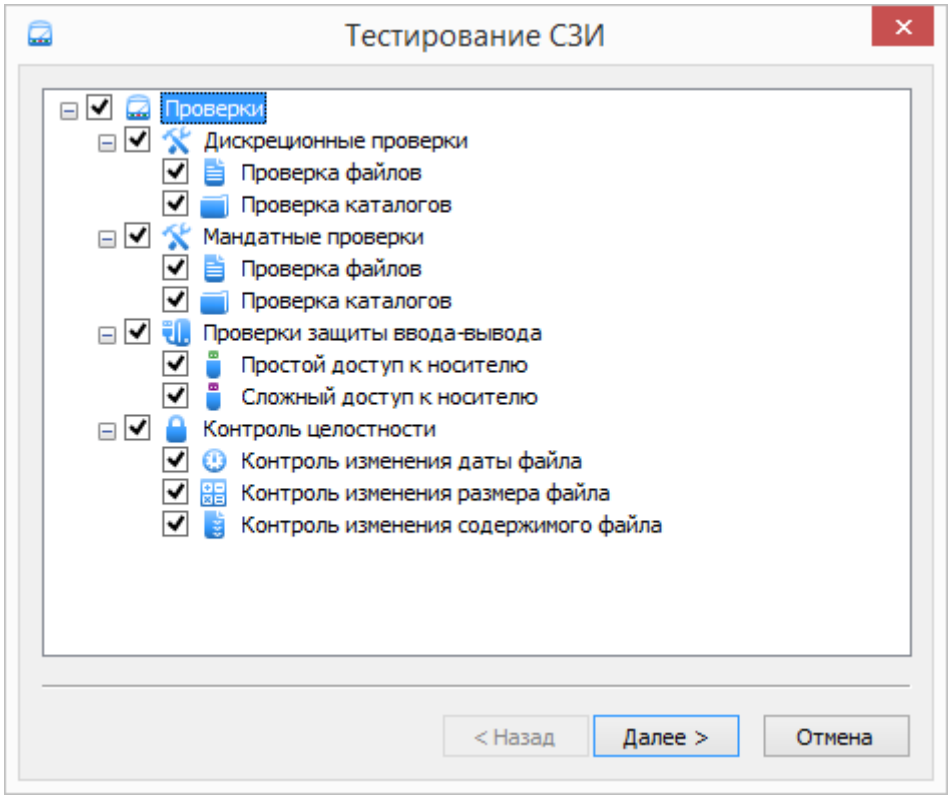


Рис. 140. Выбор проверок тестирования.

После на экране появится окно (см. Рис. 141), содержащее список доступных для тестирования компьютеров. Необходимо выбрать компьютеры для тестирования и нажать кнопку Далее >.

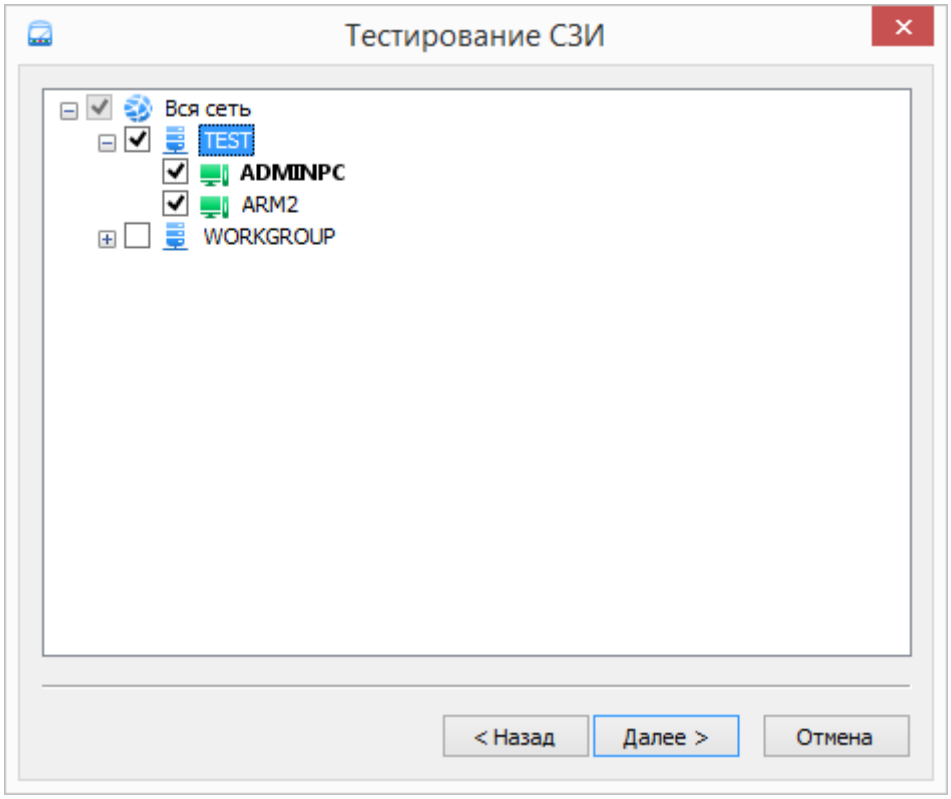


Рис. 141. Выбор компьютеров тестирования.

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

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. 142).

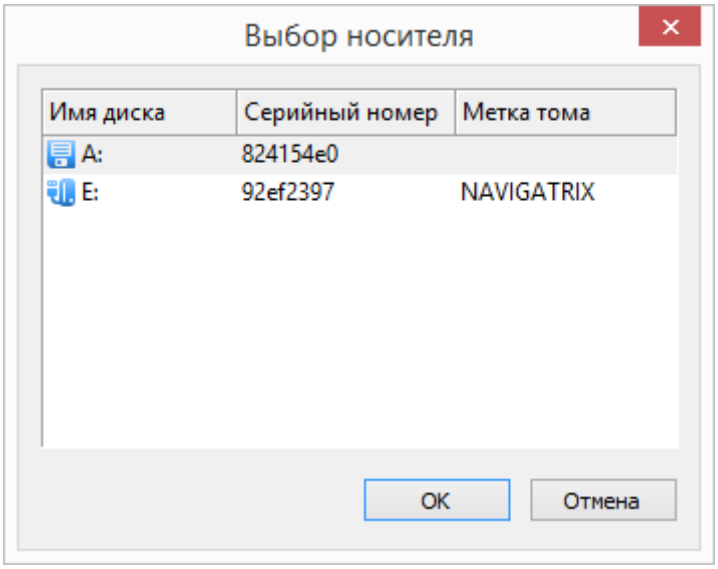


Рис. 142. Выбор носителя информации для тестирования.

Администратор системы защиты должен будет выбрать один из предложенных носителей для выполнения проверок ввода-вывода и нажать кнопку OK. 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 на жёстких дисках.

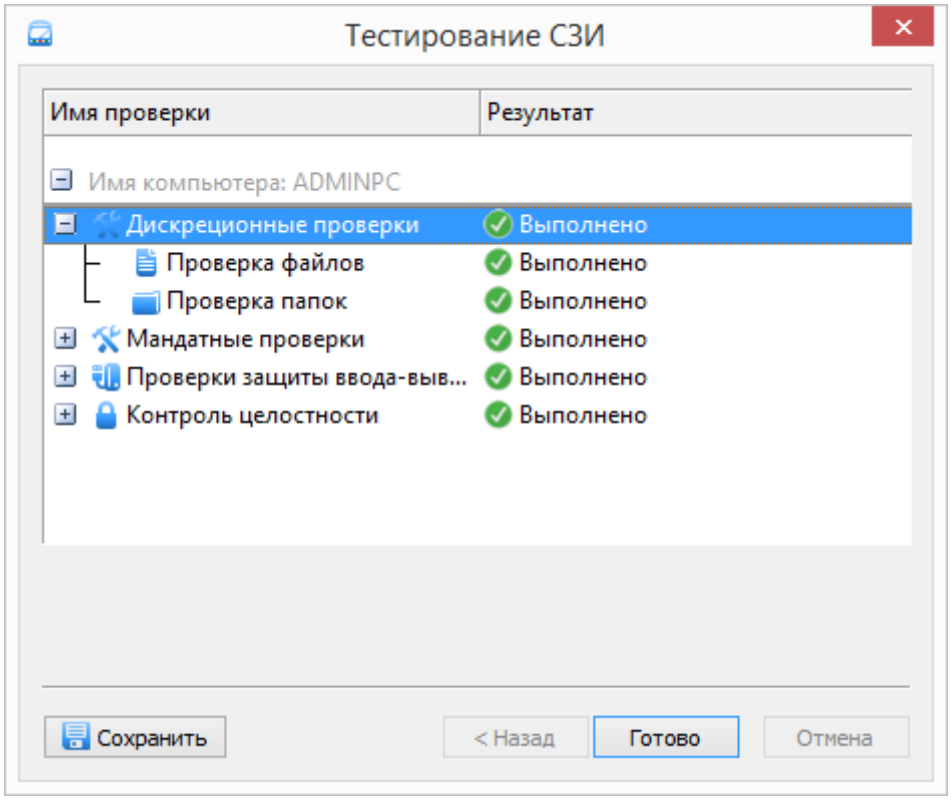
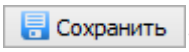


Рис. 143. Отчет о тестировании.

После завершения тестирования на экране появится отчёт о проделанных проверках (см. Рис. 143). Возможные результаты проверок приведены в следующей таблице.

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: • нет свободного носителя; • удалённый компьютер не доступен.

Результаты тестирования можно сохранить в формате HTML или CSV. Для сохранения списка результатов необходимо нажать кнопку 

.

После проведения тестирования механизмов системы защиты в Журнале событий появятся записи, (в том числе, с отказами доступа к ресурсам и ошибками целостности файлов), отражающие ход алгоритмов тестирования.

Также, при тестировании механизмов контроля целостности при повторном входе в систему пользователя без перезагрузки операционной системы, возможно появление сообщения о нарушении целостности по крайней мере одного файла.

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, нарушающий правила разграничения

доступ к информации (НСД)	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	Массив записей контроля доступа.

доступа (ACL)	
Системный список контроля доступа (SACL)	Массив записей контроля доступа, управляющий аудитом доступа к объекту.
Сценарий настроек	Набор параметров и их значений, позволяющий устанавливать защитные свойства объектов. Сценарии настроек нужны для упрощения процедуры настройки свойств объектов автоматизированной системы.
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).