УТВЕРЖДЕН

МАВУ.00030-01 31-ЛУ

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «СТРАЖ NT»

Версия 3.0

Описание применения

МАВУ.00030-01 31

Листов 77

2010

Аннотация

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

СЗИ ***«Страж NT»*** функционирует на однопроцессорных и многопроцессорных компьютерах, серверах, кластерах в среде операционных систем фирмы *Microsoft Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server, Windows 2008 Server R2, Windows 7*. Далее в документе перечисленные операционные системы будут называться ОС *Windows*.

Настоящий документ предназначен для администраторов защиты, руководителей служб и отделов по защите информации, аттестационных центров, а также всех заинтересованных специалистов в области защиты информации, и представляет собой описание применения СЗИ ***«Страж NT»***. В нем приведены сведения о назначении, вариантах и условиях применения СЗИ ***«Страж NT»***, ее архитектуре и общих принципах функционирования, используемых механизмах защиты, входных и выходных данных, а также требования к аппаратным средствам и прикладному программному обеспечению.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

СЗИ ***«Страж NT»*** предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах на базе персональных ЭВМ. СЗИ ***«Страж NT»*** обеспечивает реализацию требований по защите информации в различных классах защищенных информационных систем, в том числе в системах обработки персональных данных. СЗИ ***«Страж NT»*** значительно упрощает аттестацию объектов информатизации, предусматривая весь комплекс мер защиты автоматизированных систем класса защищенности до 1Б включительно.

СЗИ ***«Страж NT»*** функционирует в среде операционных систем Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7 и устанавливается как на автономных рабочих местах, так и на рабочих станциях и файл-серверах локальной вычислительной сети, а также на кластерных системах. СЗИ ***«Страж NT»*** представляет собой программно-аппаратный комплекс, включающий в свой состав следующие компоненты:

- *устройства идентификации пользователей;*
- *драйверы устройств идентификации;*
- *модуль входа в систему;*
- *драйверы ядра системы защиты;*
- *библиотеку модуля входа в Windows;*
- *библиотеку пользовательских интерфейсов;*
- *программу «Установка и снятие системы защиты»;*
- *программу «Настройка системы защиты»;*
- *программу «Менеджер файлов»;*
- *программу «Менеджер пользователей»;*
- *программу «Учет носителей»;*
- *программу «Контроль устройств»;*
- *программу «Вход пользователей»;*
- *программу «Тестирование системы защиты»;*
- *службу контроля устройств;*
- *библиотеку маркировки документов;*

- *библиотеку модуля режима одобрения администратора;*
- *библиотеку модуля оболочки;*
- *библиотеку применения шаблонов настроек;*
- *программу «Редактор шаблонов настроек»;*
- *программу «Преобразование журнала событий»;*
- *программу «Журнал событий»;*
- *программу «Монитор системы защиты».*

1.1. Устройства идентификации пользователей

Назначение:

- хранение идентификационной информации пользователей

Функции:

- хранение данных
- хранение уникального серийного номера

Описание:

В СЗИ ***«Страж NT»*** предусмотрена возможность работы пользователей (в том числе и администратора безопасности) на различных компьютерах с использованием единого идентификатора и пароля для входа. В качестве *устройств идентификации пользователя* в СЗИ ***«Страж NT»*** могут применяться стандартная 3,5” дискета, устройства iButton (таблетка), USB – ключи eToken Pro, eToken Pro Java, Guardant ID, Rutoken S, USB флэш-накопители. Устройства для идентификации пользователей представляют собой энергонезависимые носители информации, на которые записываются необходимые для идентификации пользователей данные. Устройства идентификации пользователей поставляются по заявке заказчика в комплекте с программным обеспечением СЗИ ***«Страж NT»***, либо могут приобретаться заказчиком отдельно у производителей и продавцов устройств идентификации.

1.2. Драйверы устройств идентификации

Назначение:

- обеспечение доступа к устройствам идентификации в среде ОС Windows.

Функции:

- поиск подключенных устройств;
- взаимодействие с операционной системой и прикладными программами.

Описание:

В состав СЗИ ***«Страж NT»*** включены оригинальные драйверы разработчиков для устройств идентификации типа iButton, eToken, Rutoken и Guardant ID. Для работы других устройств используются либо стандартные драйверы операционной системы, либо функции, включенные в состав СЗИ. Драйверы для устройств идентификации типа iButton, eToken, Rutoken и Guardant ID поставляются в каждом комплекте СЗИ ***«Страж NT»*** и инсталлируются в момент установки системы защиты. Для устройств eToken и Rutoken существует возможность отказа от установки драйверов.

1.3. Модуль входа в систему

Назначение:

- обеспечение идентификации пользователя до загрузки операционной системы.

Функции:

- идентификация и аутентификация пользователей при входе в систему по идентификатору и паролю;
- блокировка клавиатуры на время загрузки операционной системы (за исключением администратора безопасности);
- регистрация событий входа в систему;
- защита данных на системном диске от загрузки посторонней операционной системы.

Описание:

Модуль входа в систему прописывается в начало загрузочного жесткого диска и заменяет стандартный загрузчик операционной системы и таблицу разделов. При успешной идентификации пользователя модуль входа подставляет исходный загрузчик ОС и передает ему управление.

1.4. Драйверы ядра системы защиты

Назначение:

- реализация основных механизмов и функций защиты информации.

Функции:

- управление запуском всех системных компонентов, включая драйверы, службы и прикладные программы пользователей;
- создание замкнутой программной среды для пользователей;
- перехват всех запросов к ресурсам системы и реализация единого диспетчера доступа;
- дискреционный контроль доступа к ресурсам системы на основе списков управления доступом;
- полнофункциональный мандатный контроль доступа на основе меток конфиденциальности пользователей, защищаемых ресурсов и прикладных программ;
- контроль потоков защищаемой информации;
- автоматическое затирание файлов при их удалении;
- затирание файла подкачки страниц при завершении работы;
- контроль целостности компонентов системы защиты;
- контроль целостности постоянных информационных массивов и программного обеспечения;
- регистрация обращений к защищаемым ресурсам;
- регистрация событий входа в систему;
- защита ввода-вывода на отчуждаемые носители;
- работа в режиме преобразования информации на отчуждаемых носителях.

Описание:

В *драйверах ядра системы защиты* реализованы основные механизмы и функции, обеспечиваемые СЗИ ***«Страж NT»***. Ядро системы защиты встраивается в ядро операционной системы Windows NT, существенно расширяя и усиливая механизмы защиты ОС. Реализованная в ядре защиты концепция единого диспетчера доступа

гарантирует полный контроль доступа к защищаемым ресурсам и носителям информации, независимо от типов носителей и файловых систем.

1.5. Библиотека модуля входа в Windows

Назначение:

- обеспечение автоматического входа в систему по параметрам идентификации пользователей для ОС Windows Vista и выше.

Функции:

- идентификация и аутентификация пользователей при входе в ОС Windows Vista и выше по идентификатору и паролю;
- блокировка компьютера при изъятии идентификатора (только для USB-идентификаторов);
- завершение сеанса пользователя и вход другим пользователей без перезагрузки операционной системы;
- регистрация в журнале событий фактов успешного входа в систему, а также ошибок входа.

Описание:

Библиотека модуля входа в Windows обеспечивает автоматический вход в систему по параметрам идентификации пользователей, полученным от ядра системы защиты, в среде операционной системы Windows Vista и выше. Библиотека представляет собой стандартный Credential Provider Windows Vista, адаптированный для работы с СЗИ ***«Страж NT»***.

1.6. Библиотека пользовательских интерфейсов

Назначение:

- обеспечение автоматического входа в операционную систему до версии Windows Vista;
- обеспечение интерфейса с пользователем и программами управления и настройки СЗИ.

Функции:

- автоматический ввод параметров идентификации и аутентификации пользователей при входе в Windows;
- блокировка компьютера при изъятии идентификатора (только для USB-идентификаторов);
- завершение сеанса пользователя и вход другим пользователей без перезагрузки операционной системы;
- регистрация в журнале событий фактов успешного входа в систему, а также ошибок входа;
- запрос и назначение текущего допуска приложений;
- поддержка *подсистемы маркировки документов*;
- защита папки обмена;
- поддержка работы с идентификаторами пользователей;
- вывод сообщений системы защиты.

Описание:

Библиотека пользовательских интерфейсов обеспечивает автоматический вход в операционную систему версии до Windows Vista, а также интерфейс с пользователем и программами управления и настройки СЗИ. Библиотека загружается автоматически в каждом пользовательском процессе и реализует механизмы защиты на уровне прикладных задач.

1.7. Установка и снятие системы защиты

Назначение:

- загрузка всех компонентов системы защиты информации ***«Страж NT»*** в ПЭВМ;
- выполнение необходимых настроек в операционной системе;
- удаление всех компонентов при снятии системы защиты.

Функции:

- копирование всех компонентов системы с установочного носителя на жесткий диск при установке СЗИ ***«Страж NT»***;
- создание идентификатора администратора безопасности (при первой установке);

- удаление всех компонентов системы при снятии СЗИ ***«Страж NT»***.

Описание:

Программа установки запускается автоматически с установочного диска при его обнаружении в устройстве CD-ROM, если соответствующие настройки автозапуска программ выполнены в операционной системе. При запуске *Программа установки* проверяет, установлена ли СЗИ ***«Страж NT»*** на данной ПЭВМ. Если СЗИ ***«Страж NT»*** не установлена, то *Программа установки* предлагает ее установить. В противном случае, т.е. если СЗИ ***«Страж NT»*** уже установлена, *Программа установки* предлагает ее снять.

1.8. Настройка системы защиты

Назначение:

- выполнение первоначальных настроек системы защиты;
- изменение параметров и настроек системы защиты в процессе работы.

Функции:

- установка необходимых первоначальных настроек защищаемых ресурсов;
- установка параметров контроля целостности на файлы системы защиты;
- изменение названий меток конфиденциальности;
- создание ярлыков для программ системы защиты;
- упрощенное формирование замкнутой программной среды;
- применение готовых шаблонов настроек;
- настройка параметров дополнительного аудита;
- управление режимами преобразования информации на отчуждаемых носителях;
- настройка монитора системы защиты;
- настройка параметров маркировки документов;
- отказ от настроек ресурсов системы защиты.

Описание:

Программа *Настройка системы защиты* запускается как автоматически при первом входе администратора защиты после установки системы защиты, так и по запросу администратора в процессе работы системы. При запуске в автоматическом

режиме программа выполняет необходимые первоначальные настройки защищаемых ресурсов, а также настройку параметров контроля целостности для файлов системы защиты.

1.9. Менеджер файлов

Назначение:

- настройка параметров доступа к защищаемым ресурсам;
- выполнение файловых операций.

Функции:

- отображение списка защищаемых ресурсов системы;
- установка и изменение прав доступа к защищаемым ресурсам;
- назначение режимов и параметров запуска исполняемых модулей;
- управление параметрами регистрации обращений к защищаемым ресурсам;
- настройка параметров контроля целостности;
- установка при необходимости режима Администрирования;
- выполнение отдельных функций программы *Проводник*.

Описание:

Менеджер файлов представляет собой основной инструмент администратора безопасности по настройке параметров доступа к защищаемым ресурсам операционной системы. К ресурсам системы, которые могут быть настроены с помощью *Менеджер файлов*, относятся локальные и сетевые диски, папки и файлы. Помимо функций по настройке параметров защищаемых ресурсов *Менеджер файлов* может применяться пользователем в качестве программы для выполнения файловых операций, аналогичной программе *Проводник*. При этом на программу *Менеджер файлов* может быть установлен допуск, что позволяет пользователю осуществлять операции с ресурсами различного уровня конфиденциальности.

1.10. Менеджер пользователей

Назначение:

- управление списком пользователей системы защиты.

Функции:

- создания, удаления, переименования пользователей;
- включение пользователей в группы;
- назначение и смена паролей пользователей;
- создание профилей пользователей;
- формирование идентификаторов пользователей;
- просмотр свойств идентификаторов;
- стирание идентификаторов.

Описание:

Менеджер пользователей является инструментом администратора безопасности для создания, удаления и управление свойствами пользователей и их идентификаторов. Программа поддерживает работу в составе локальной сети и позволяет с каждого рабочего места выполнять перечисленные функции по работе с пользователями любого другого рабочего места.

1.11. Учет носителей

Назначение:

- обеспечение работы с журналом учета носителей.

Функции:

- добавление и удаление носителей в журнал учета;
- изменение параметров регистрации носителей;
- изменение разрешений по доступу к зарегистрированным носителям;
- экспорт зарегистрированных носителей на другие компьютеры локальной сети;
- изменение разрешений по доступу по умолчанию к различным типам носителей;
- распечатка журнала учтенных носителей.

Описание:

Различные носители, установленные или подключаемые к системе, могут быть зарегистрированы в журнале учета системы защиты. Для учтенных носителей действуют правила контроля доступа, установленные для данного конкретного устройства. Для неучтенных носителей применяются правила доступа по

умолчанию, принятые для конкретного типа носителей. Тома на локальных жестких дисках компьютера, существующие на момент установки системы защиты, регистрируются в журнале учета автоматически. Все остальные носители могут быть зарегистрированы с помощью программы *Учета носителей.* В СЗИ ***«Страж NT»*** поддерживаются следующие типы носителей:

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

Все другие типы носителей попадают в категорию *неопознанный тип.*

При учете носителя указываются следующие параметры:

- учетный номер;
- гриф;
- ответственный пользователь;
- дата учета;
- тип доступа;
- разрешения.

Учет носителя осуществляется по его типу, серийному номеру и при наличии метки тома. Если для носителя указан тип доступа *простой*, то к нему применяются упрощенные правила контроля доступа, при котором все папки и файлы на носителе имеют одинаковый гриф и разрешения, соответствующие грифу и разрешениям самого носителя. В противном случае к носителю применяются обычные правила разграничения доступа, когда папки и файлы могут иметь различные грифы и разрешения.

Для каждого типа носителей задается значение разрешений по умолчанию, которые действуют для носителей, не прописанных в журнале учета. Кроме того, для неучтенных носителей всегда установлен *простой* тип доступа и гриф *несекретно*.

Программа также поддерживает работу в составе локальной сети и позволяет с каждого рабочего места выполнять перечисленные функции по учету носителей на любом другом рабочем месте, а также осуществлять экспорт настроек с одного компьютера на другой.

1.12. Контроль устройств

Назначение:

- обеспечение настройки *подсистемы контроля устройств* компьютера.

Функции:

- установка разрешений на различные типы устройств.

Описание:

Программа контроля устройств обеспечивает настройку *подсистемы контроля устройств* компьютера и позволяет устанавливать разрешения на различные типы устройств. В соответствии с разрешениями после входа пользователя в систему устройства, запрещенные данному пользователю, будут отключены. При попытке подключить устройство, запрещенное данному пользователю, *подсистема контроля устройств* отключит данное устройство. В СЗИ ***«Страж NT»*** контролируются следующие типы устройств:

- биометрические устройства;
- bluetooth устройства;
- HID устройства;
- устройства IEE 1394;
- инфракрасные порты;
- модемы;
- мультифункциональные устройства;
- сетевые карты;
- PCMCIA устройства;
- порты (COM и LPT);
- принтеры;
- устройства чтения смарткарт;

- устройства USB;
- переносные устройства.

Любые другие устройства компьютера, не вошедшие ни в один из перечисленных типов, попадают в тип *другие устройства*.

Программа также поддерживает работу в составе локальной сети и позволяет с каждого рабочего места выполнять перечисленные функции по настройке классов устройств на любом другом рабочем месте, а также осуществлять экспорт настроек с одного компьютера на другой.

1.13. Вход пользователей

Назначение:

- обеспечение контроля входа и выхода пользователей в систему (из системы).

Функции:

- передача параметров вошедшего пользователя *службе контроля устройств*;
- оповещение *службы контроля устройств* о завершении сеанса пользователя;
- создание ярлыков для администратора системы защиты.

Описание:

Программа запускается автоматически при входе каждого пользователя в систему и передает необходимые параметры в *службу контроля устройств*.

1.14. Тестирование системы защиты

Назначение:

- автоматическое комплексное тестирование основных функций и механизмов защиты, реализованных в СЗИ ***«Страж NT»***.

Функции:

- тестирование механизма дискреционного контроля доступа;
- тестирование механизма мандатного контроля доступа;
- тестирование защиты ввода-вывода на отчуждаемые носители;
- тестирование механизма контроля целостности;
- сохранение и печать отчета о тестировании.

Описание:

Программа тестирования представляет собой инструмент администратора безопасности, предназначенный для автоматического комплексного тестирования основных функций и механизмов защиты, реализованных в СЗИ ***«Страж NT»***, как на локальном компьютере, так и на любом компьютере в составе ЛВС при наличии у администратора соответствующих прав.

1.15. Служба контроля устройств

Назначение:

- реализация механизмов *подсистемы контроля устройств*.

Функции:

- запуск и останов устройств при входе пользователя в соответствии с установленными разрешениями;
- регистрация в журнале событий операций запуска и останова устройств;
- обеспечение запуска программы *Входа пользователей.*

Описание:

Служба контроля устройств запускается автоматически при загрузке системы. Она использует настройки, выполненные программой контроля устройств, и, получив от программы *Вход пользователей* информацию о пользователе, осуществившем вход в систему, обеспечивает создание необходимой конфигурации устройств для данного пользователя.

1.16. Библиотека маркировки документов

Назначение:

- реализация *подсистемы маркировки документов.*

Функции:

- автоматическая маркировка документов по заданным параметрам при выдаче на печать;
- регистрация фактов печати документов в журнале событий.

Описание:

Библиотека маркировки документов запускается автоматически при выдаче документов на печать прикладными программами. Она взаимодействует с библиотекой пользовательских интерфейсов и использует настройки параметров маркировки, выполненные программой Настройки системы защиты.

1.17. Библиотека модуля режима одобрения администратора

Назначение:

- обеспечение работы программ администратора в ОС Windows Vista и выше с включенным режимом контроля учетных записей.

Функции:

- предоставление механизма повышения прав администратора при работе в Windows Vista.

Описание:

Библиотека обеспечивает выполнение функций операционной системы Windows Vista и выше в режиме одобрения администратора для программ Менеджер файлов, Менеджер пользователей и Монитор защиты.

1.18. Библиотека модуля оболочки

Назначение:

- внедрение интерфейсов отображения и изменения параметров безопасности в окно свойств защищаемых ресурсов.

Функции:

- отображение и изменение параметров безопасности защищаемых ресурсов;
- установка грифа на принтеры.

Описание:

Библиотека создает интерфейс для отображения и изменения параметров безопасности защищаемых ресурсов.

1.19. Библиотека применения шаблонов настроек

Назначение:

- применение шаблонов настроек.

Функции:

- анализ шаблонов и выдача команд на установку параметров безопасности.

Описание:

Библиотека применения шаблонов настроек используется программами Настройка системы защиты и Редактор шаблонов настроек и реализует функции работы с шаблонами настроек.

1.20. Редактор шаблонов настроек

Назначение:

- обеспечение работы с шаблонами настроек защищаемых ресурсов.

Функции:

- формирование шаблонов настроек;
- редактирование шаблонов настроек.

Описание:

Программа позволяет администратору безопасности формировать шаблоны для настройки сложных программных комплексов и применять их на других компьютерах.

1.21. Преобразование журнала событий

Назначение:

- обеспечение переноса записей о событиях системы защиты из журнала ядра системы защиты в базу данных Журнала событий.

Функции:

- сброс журнала ядра системы защиты в отдельный файл;
- очистка журнала ядра системы защиты;
- перенос записей журнала ядра системы защиты в базу данных Журнала событий;
- семантическое сжатие Журнала событий.

Описание:

Программа преобразования журнала событий запускается автоматически при старте системы и обеспечивает периодическую запись в базу данных событий, зарегистрированных в ядре системы защиты.

1.22. Журнал событий

Назначение:

- обеспечение работы с базой данных Журнала событий.

Функции:

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

Описание:

Программа журнала событий предназначена для просмотра всех предусмотренных в СЗИ событий, а также фактов печати документов. Все события регистрируются в специальном файле в формате MS Access Database на локальном компьютере. При просмотре зарегистрированных событий предусмотрена возможность чтения журналов регистрации на любом компьютере, включенном в локальную сеть и защищенном СЗИ ***«Страж NT»***. *Журнал событий* позволяет осуществлять выборочное ознакомление с регистрационной информацией путем сортировки журналов по любому из полей отображения, применения различных фильтров при выборке записей из журнала, а также поиска записей по основным полям. Кроме того в программе предусмотрена возможность архивирования, очистки и распечатки журнала, а также просмотра ранее сохраненных журналов. Программа также поддерживает работу в составе локальной сети и позволяет с каждого

рабочего места выполнять перечисленные функции по работе с журналом событий на любом другом рабочем месте.

1.23. Монитор системы защиты

Назначение:

- обеспечение отображения состояния системы защиты;
- обеспечение быстрого вызова функций управления системы защиты.

Функции:

- отображение состояния системы защиты;
- включение/выключение режима автозапуска;
- включение/выключение режима блокировки;
- быстрый запуск программ системы защиты.

Описание:

Монитор системы защиты загружается автоматически после входа пользователя в систему. При этом на панели задач создается значок для быстрого вызова всех функций управления СЗИ. Существует возможность подключения новых функций, необходимых администратору безопасности для частого использования.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

Система защиты информации ***«Страж NT»*** может устанавливаться на автономных рабочих местах, переносных компьютерах, рабочих станциях ЛВС, файл-серверах и кластерных системах под управлением операционных систем Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7. Данная программа поддерживает работу на одно- и многопроцессорных компьютерных системах. Компьютер, на котором устанавливается СЗИ ***«Страж NT»,*** должен удовлетворять требованиям, необходимым для загрузки операционной системы.

В силу особенностей реализации защитных механизмов СЗИ ***«Страж NT»*** загрузочный жесткий диск должен иметь не менее 63 секторов перед началом первого раздела.

На компьютере должна быть установлена одна из операционных систем Windows фирмы Microsoft, основанных на технологии NT. К ним относятся Windows 2000 (Professional, Server или Advanced Server), Windows XP (Home Edition и Professional), Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7. Тип файловой системы на жестких дисках компьютера не имеет значения, это может быть FAT 32 или NTFS. Жесткий диск компьютера, на котором установлена операционная система, должен иметь свободное пространство объемом не менее 100 Мб.

Объем памяти на жестком диске, занимаемый СЗИ ***«Страж NT»*** сразу после установки, достигает 60 Мб. Однако в процессе функционирования объем занимаемой памяти существенно возрастает в зависимости от объема жесткого диска, количества защищаемых ресурсов, включенных режимах регистрации и т.д.

Перед началом установки СЗИ ***«Страж NT»*** должно быть установлено все прикладное программное обеспечение, предусмотренное на данном рабочем месте. Установка дополнительного программного обеспечения в процессе функционирования СЗИ ***«Страж NT»*** является нежелательной. С этой целью можно воспользоваться режимом обновления программного обеспечения либо

функцией временного останова системы защиты на текущий сеанс, если это не вызывает сбоев при установке дополнительного программного обеспечения. В ряде случаев при установке дополнительного программного обеспечения может потребоваться полное снятие системы защиты с сохранением текущих настроек и последующая ее установка.

СЗИ ***«Страж NT»*** предусматривает возможность работы пользователей на различных компьютерах, используя единый идентификатор и пароль для входа. Каждый поставляемый комплект СЗИ ***«Страж NT»*** защищен от несанкционированного использования при помощи уникального номера продукта, количества установок и специального лицензионного номера. Количество установок комплекта СЗИ ***«Страж NT»*** означает максимальное число компьютеров, которые можно защитить с помощью данного комплекта, используя один идентификатор администратора.

При работе в составе локальной вычислительной сети СЗИ ***«Страж NT»*** должна устанавливаться на все рабочие станции и файл-серверы, работающие под управлением перечисленных выше операционных систем. При наличии в ЛВС рабочих станций, работающих в другой среде, либо на которых не установлена СЗИ ***«Страж NT»***, они считаются незащищенными и имеют ограниченный доступ. В частности, на такие рабочие станции запрещается запись информации, имеющей гриф секретности, а также с данных станций запрещается запуск программ.

Для установки, настройки и управления функционированием СЗИ ***«Страж NT»*** должен быть назначен администратор безопасности. Это должен быть пользователь, включенный в группу *локальных Администраторов*. Пользователь, являющийся администратором, должен быть создан либо в контроллере домена ЛВС, либо в локальном домене каждого компьютера, на котором планируется установка СЗИ ***«Страж NT»***. Администратор должен иметь одинаковое имя и пароль для входа на всех компьютерах. Администратор должен быть создан перед началом установки СЗИ ***«Страж NT»*** стандартными средствами операционной системы.

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

СЗИ ***«Страж NT»*** практически не накладывает ограничений на прикладное программное обеспечение. Тем не менее, прикладное программное обеспечение, работающее под СЗИ ***«Страж NT»***, должно быть тщательно протестировано и по возможности проверено на отсутствие компьютерных вирусов и недекларированных возможностей. СЗИ ***«Страж NT»*** накладывает ограничения на доступ программ к защищаемым ресурсам, в связи с этим в программах должна предусматриваться обработка соответствующих ошибок и учитываться действующие правила разграничения доступа.

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Обзор подсистемы защиты информации операционных систем, основанных на технологии Windows NT

Для понимания принципов и механизмов защиты информации, реализованных в СЗИ ***«Страж NT»***, необходимо изучить архитектуру системы безопасности операционных систем, под управлением которых данная система функционирует. СЗИ ***«Страж NT»*** не только использует механизмы, заложенные в операционную систему, но и существенно дополняет их и расширяет. Далее следует краткое описание компонентов подсистемы защиты информации операционных систем Windows NT. Для более подробного изучения данного вопроса необходимо использовать дополнительную литературу.

В операционных системах Windows, построенных по технологии NT, существует единая система для идентификации, проверки подлинности, контроля доступа и записи информации о событиях, связанных с безопасностью. В рамках данной архитектуры все объекты и все процессы подчиняются требованиям подсистемы защиты информации, которая включает в себя несколько основных компонентов.

Процессы входа в систему обрабатывают запросы пользователей на вход в систему. Сюда включается начальный *интерактивный вход в систему,* осуществляемый через диалоговое окно входа пользователя, и процессы *удаленного входа,* открывающие доступ к серверу с удаленных компьютеров. Вход в систему является обязательным для работы с сервером или рабочей станцией.

Центральная часть подсистемы защиты – *Локальный администратор безопасности* – проверяет, есть ли у пользователя необходимые полномочия для входа в систему. Этот компонент создает маркеры доступа, управляет локальными правилами безопасности, обеспечивает службы интерактивной проверки подлинности. Локальный администратор безопасности также контролирует правила

аудита и записывает в журнал аудита сообщения, полученные от монитора безопасности.

Журнал безопасности содержит записи о событиях, связанных с работой подсистемы защиты информации.

Пакет проверки подлинности проверяет подлинность пользователя. Операционные системы поддерживают несколько таких пакетов, выполненных как динамические библиотеки. Пакет проверки подлинности обращается к диспетчеру учетных записей, причем последний может находиться как на локальном, так и на удаленном компьютере. Это достигается разбиением пакета на две части. Одна выполняется на компьютере, где осуществляется вход пользователя, другая – на компьютере, который хранит базу учетных записей. Пакет по имени домена определяет, где находится база данных учетных записей, и, если она расположена на удаленном компьютере, первая часть пакета передает запрос на удаленный компьютер, где вторая часть пакета проверяет подлинность. Этот процесс называется сквозной проверкой подлинности.

Диспетчер учетных записей поддерживает базу данных учетных записей, в которой хранятся все учетные записи пользователей и групп. Эта база является частью реестра операционной системы и недоступна обычным пользователям в ходе нормальной работы. Диспетчер учетных записей обеспечивает службы подтверждения подлинности пользователя, используемые администратором локальной безопасности.

Монитор безопасности проверяет, имеет ли пользователь достаточные права для доступа к объекту. В отличие от других компонентов подсистемы защиты информации он работает в режиме ядра операционной системы. Компоненты ядра и пользовательские процессы обращаются к монитору безопасности, чтобы выяснить, имеют ли право пользователи и процессы получить доступ к объекту.

3.2. Описание компонентов системы защиты информации *«Страж NT»*

Технология, реализованная в СЗИ ***«Страж NT»***, обладает широкими возможностями по построению системы защиты информации, соответствующей

современным требованиям. Она усиливает практически все компоненты подсистемы защиты информации операционных систем. Указанная технология реализуется несколькими программными модулями, функционирующими во всех режимах операционной системы. Часть модулей составляет ядро защиты, другие модули служат для управления функциями защиты. Каждый модуль является логически завершенной программой, инициализируемой на определенном этапе загрузки операционной системы и выполняющей определенные механизмы защиты.

Перед началом загрузки операционной системы инициализируется *модуль входа в систему*, реализующий интерфейс входа пользователя в систему. Этот же модуль раскрывает логическую структуру жесткого диска, давая возможность корректной работы загрузчику операционной системы. Ниже приводится описание интерфейса входа пользователя в систему.

При включении питания или перезагрузке компьютера на экран выдается сообщение: *Предъявите идентификатор*. В качестве идентификаторов могут быть использованы дискеты, устройства iButton, USB ключи eToken Pro, eToken Pro Java, Rutoken S, Guardant ID, а также USB флэш-накопители. На данном этапе система защиты поочередно опрашивает все устройства для ввода идентификаторов, пока не обнаружит правильный идентификатор. Неправильные или испорченные идентификаторы отвергаются системой защиты. При одновременном предъявлении нескольких идентификаторов вход в систему осуществляется по первому правильному идентификатору. После считывания правильного идентификатора на экран выводится запрос на ввод пароля. Пользователю предоставляется 3 попытки для ввода корректного пароля. После третьей попытки ввода неправильного пароля регистрируется данное событие и компьютер блокируется. При вводе корректного пароля происходит загрузка операционной системы. При этом параметры идентификации, считанные с идентификатора, и пароль, введенный пользователем, используются для входа пользователя в операционную систему.

Загрузка посторонней операционной системы с дискеты или CD-ROM диска при установке данного модуля становится невозможной. При попытке прочитать

содержимое диска при его подключении к другому компьютеру логическая структура диска будет недоступной.

На этапе работы загрузчика операционной системы загружается второй модуль системы защиты, называемый *модулем загрузки*. При инициализации данный модуль считывает параметры идентификации, передаваемые модулем входа в систему, и восстанавливает логическую структуру диска для последующей загрузки компонентов операционной системы в режиме ядра.

На этапе загрузки системных компонентов операционной системы инициализируется основной модуль *ядра системы защиты*. Данный модуль реализован в виде драйвера ядра операционной системы. В нем реализованы основные механизмы защиты, описываемые ниже.

Следующим компонентом, загружающимся при запуске пользовательских программ, использующих графический интерфейс, является модуль, реализующий интерфейс с пользователями и программами управления и настройки СЗИ.

Ниже рассматриваются основные механизмы защиты информации, реализуемые СЗИ ***«Страж NT»***.

3.3. Описание механизмов защиты

В СЗИ ***«Страж NT»*** реализована смешанная разрешительно-запретительная модель защиты информации с жестким администрированием, означающая что для отдельных механизмов защиты применяется разрешительная политика, а для других - запретительная. Система защиты представляет собой совокупность следующих основных подсистем:

- *идентификации и аутентификации;*
- *разграничения доступа;*
- *контроля потоков информации;*
- *управление запуском программ;*
- *управления защитой;*
- *регистрации событий;*

- *маркировки документов;*
- *контроля целостности;*
- *очистки памяти;*
- *учета носителей информации;*
- *преобразования информации на отчуждаемых носителях;*
- *контроля устройств;*
- *тестирования системы защиты.*

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

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

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

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

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

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

Подсистема *запуска программ* предназначена для обеспечения целостности и замкнутости программной среды и реализована путем разрешения для исполняемых файлов режима запуска. Если режим запуска программы не разрешен, то файл не является исполняемым и не может быть запущен пользователем ни при каких условиях. Кроме того, пользователю запрещен запуск исполняемых файлов с носителей, имеющих *простой* тип доступа. Режим запуска может быть разрешен только для исполняемых файлов, записанных на локальных дисках компьютера, для которых не установлен *простой* тип доступа, и только администратором защиты. Тем самым обеспечивается защита от несанкционированного использования программ, разработанных или скопированных пользователями. Кроме того, в данной подсистеме предусмотрен режим автоматического разрешения режима запуска для всех запускаемых компонентов операционной системы. Этот режим может включаться только администратором безопасности при настройке системы защиты и служит для облегчения настройки системы. Предусмотрена возможность включения режима автозапуска на следующий сеанс работы, что позволяет выполнять настройку драйверов и сервисных программ операционной системы, программ, запускаемых один раз при создании нового пользовательского профиля и в других сложных ситуациях. В рамках данной подсистемы реализован режим обновления программного обеспечения, который позволяет производить установку обновлений без отключения системы защиты.

Подсистема *управления защитой* включает в себя программы администрирования системы защиты, к которым относятся следующие:

- *Установка и снятие системы защиты;*
- *Настройка системы защиты;*
- *Менеджер файлов;*
- *Менеджер пользователей;*
- *Учет носителей;*

- *Контроль устройств;*
- *Редактор шаблонов настроек;*
- *Монитор системы защиты.*

Назначение и функции программ администрирования описаны в разделе 1 настоящего документа.

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

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

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

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

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

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

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

Подсистема *тестирования системы защиты* предназначена для комплексного тестирования основных механизмов системы защиты, как на

локальном компьютере, так и на удаленном, с использованием локальной вычислительной сети.

3.3.1. Идентификация и аутентификация

Идентификация пользователей в СЗИ ***«Страж NT»*** происходит дважды. *Первоначальная идентификация* производится до загрузки операционной системы. Это обстоятельство имеет важное значение, поскольку пользователь не имеет возможности получить доступ к информации на жестком диске, не осуществив успешно процедуру *первоначальной идентификации*. В том случае, если при первоначальной идентификации зарегистрировался пользователь, не являющийся администратором СЗИ ***«Страж NT»***, становится возможной *повторная идентификация* пользователей без перезагрузки компьютера. Для *повторной идентификации* необходимо завершить текущий сеанс пользователя, предъявить персональный идентификатор и ввести пароль другого пользователя. Если при *повторной идентификации* будет предъявлен идентификатор завершившего сеанс пользователя, то вход в систему произойдет автоматически без запроса пароля. *Повторная идентификация* не предусмотрена для устройств типа iButton и дискет в среде операционных систем Windows Vista, Windows 7 и Windows Server 2008.

Процедура *первоначальной идентификации* состоит в сопоставлении идентификатора пользователя и идентификационной информации компьютера, на котором происходит вход в систему.

В качестве идентификатора пользователя применяется энергонезависимый носитель информации, на который записываются параметры идентификации пользователя. Данные идентификаторы имеют уникальный неизменный серийный номер, который также используется в процедуре идентификации.

В СЗИ ***«Страж NT»*** могут применяться устройства идентификации следующих типов:

- Стандартные гибкие магнитные диски с объемом свободной памяти до 32 килобайтов;
- Устройства iButton: DS1992, DS 1993, DS1995, DS1996;

- USB ключи фирмы Aladdin: eToken Pro 32K и eToken Pro Java 72K;
- USB ключи Guardant ID и Rutoken S компании Актив;
- 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. Данный считыватель имеет кабель и контактную площадку, которая может быть укреплена в любом удобном месте на передней панели компьютера. При использовании считывателя USB дополнительно требуется установка драйвера устройства в соответствии с инструкциями, опубликованными на сайте продукта *www.guardnt.ru*.

При использовании в качестве идентификаторов USB ключей они могут устанавливаться непосредственно в USB порт компьютера, с помощью удлинителя выводиться в любое удобное для пользователя место, либо устанавливаться в любое из подключенных к компьютеру USB устройств, имеющих дополнительные USB порты (мониторы, клавиатуры, USB разветвители и т.д.)

В зависимости от размера внутренней памяти идентификатора или свободного пространства на идентификатор может быть добавлено различное количество записей для входа в компьютеры. В общем случае, максимальное количество компьютеров, в которые может осуществляться вход с использованием одного идентификатора рассчитывается по формуле:

Количество компьютеров = (Размер свободной памяти – 140) / 50

Для устройств типа iButton максимальное количество компьютеров принимает следующие значения:

DS1992 – 1 компьютер (данный тип не может использоваться для создания идентификатора администратора);

DS1993 – 8 компьютеров;

DS1995 – 38 компьютеров;

DS1996 – 160 компьютеров.

Для USB ключей максимальное количество компьютеров превышает 300.

USB флэш-накопители используются для создания идентификаторов пользователей и администратора только в программе *Менеджер пользователей.* Это означает, что при установке системы защиты нельзя использовать идентификаторы на USB флэш-накопителях. Тем не менее в последующем, после того как будет установлено, что вход в систему возможен с помощью USB флэш-накопителей, администратор сможет сформировать другой идентификатор на указанном типе устройств.

К параметрам идентификации пользователя, которые записываются на персональный идентификатор в специальном формате, относятся:

- имя пользователя;
- личный ключ и имитовставка ключа пользователя;
- главный ключ, преобразованный на пароле пользователя;
- ключ администратора (только для администратора безопасности);
- список имен и рабочих ключей компьютеров, на которых пользователю разрешен вход с данным идентификатором;
- список имен доменов, в которые пользователь осуществляет вход с каждого из разрешенных компьютеров.

В свою очередь идентификационная информация, записанная на жестком диске компьютера, включает в себя:

- имя компьютера;
- имитовставки главного ключа, ключа администратора и рабочего ключа компьютера;
- главную загрузочную запись компьютера.

В процедуре идентификации и аутентификации пользователя для повышения гарантий качества защиты применяется алгоритм криптографического преобразования ГОСТ 28147-89. В качестве ключей применяются ключи длиной 256 бит (32 байта), а в качестве имитовставок – предусмотренные алгоритмом значения имитовставки длиной 32 бита (4 байта).

Как параметры идентификации пользователя, так и идентификационная информация компьютера хранятся на носителях в преобразованном виде. В качестве ключа используется главный ключ.

Для защиты информации, записанной на идентификаторе пользователя, от несанкционированного изменения, а также для защиты идентификаторов от несанкционированного копирования применяется дополнительное преобразование идентификационной информации на уникальных ключах идентификаторов и вычисление контрольной суммы содержимого идентификаторов.

Алгоритм первоначальной идентификации и аутентификации пользователя состоит из нескольких шагов.

Шаг 1. После включения компьютера запускается модуль входа в систему, который начинает опрос устройств идентификации. В этом модуле записана идентификационная информация компьютера. При обнаружении идентификатора в одном из устройств при первом опросе происходит переход к шагу 2. В противном случае на экран выдается сообщение *Предъявите идентификатор…*, и программа производит последовательный опрос устройств идентификации до тех пор, пока не обнаружит идентификатор. Переход к следующему шагу невозможен без предъявления идентификатора.

Шаг 2. Модуль входа в систему считывает информацию с предъявленного идентификатора в оперативную память и раскрывает ее с помощью уникального ключа идентификатора. Затем осуществляется подсчет имитовставки раскрытой информации и сравнение ее со значением, записанным в идентификаторе. В случае несовпадения имитовставок предъявленный идентификатор считается некорректным и осуществляется поиск другого идентификатора. После трех попыток предъявления некорректного идентификатора происходит переход к шагу 4. Далее осуществляется попытка раскрыть главный ключ, используя пустой пароль. В случае, если имитовставка раскрытого главного ключа совпадет с имитовставкой, записанной в

идентификационной информации компьютера, происходит переход к шагу 3. В противном случае на экран выдается запрос *Введите пароль:*, и программа запрашивает с клавиатуры пароль пользователя. В качестве пароля может использоваться любая последовательность символов, вводимых с клавиатуры, длиной не более 15. Программа не позволяет вводить символы на русском языке, но различает строчные и прописные символы. Пароль при вводе на экране не отображается. Пользователю предоставляется 3 попытки ввода правильного пароля. После каждого ввода пароля программа пытается раскрыть главный ключ, используя введенный пароль. В случае, если имитовставка раскрытого главного ключа совпадет с имитовставкой, записанной в идентификационной информации компьютера, происходит переход к шагу 3. После третьей неудачной попытки ввода пароля происходит переход к шагу 4.

Шаг 3. Используя раскрытый главный ключ, модуль входа в систему раскрывает параметры идентификации пользователя и идентификационную информацию компьютера. Затем на главном ключе раскрывается личный ключ пользователя и вычисляется его имитовставка, которая сравнивается со значением, записанным в параметрах идентификации. При несовпадении значений происходит переход к шагу 4. Далее на главном ключе раскрывается администраторский ключ и вычисляется его имитовставка, которая сравнивается со значением, записанным в идентификационной информации компьютера. При совпадении значений устанавливается признак администратора. В списке имен компьютеров осуществляется поиск имени компьютера, записанного в идентификационной информации. Если имя компьютера не найдено, происходит переход к шагу 4. Для найденного имени компьютера выбирается соответствующий рабочий ключ, который раскрывается на главном ключе. Затем вычисляется имитовставка рабочего ключа, которая

сравнивается со значением, записанным в идентификационной информации компьютера. При несовпадении значений происходит переход к шагу 4, в другом случае происходит переход к шагу 5.

Шаг 4. На экран выдается сообщение *Несанкционированный доступ*, которое сопровождается звуковой сигнализацией. В журнал регистрации заносится соответствующее сообщение. При этом компьютер блокируется.

Шаг 5. В журнал регистрации заносится сообщение об успешном входе в систему. Формируется структура параметров идентификации, для передачи следующим модулям системы защиты. В случае, если не установлен признак администратора, блокируется клавиатура. Затирается буфер ввода с клавиатуры с целью сокрытия введенного значения пароля пользователя. Восстанавливается главная загрузочная запись компьютера. Происходит старт операционной системы.

Шаг 6. При запуске главного модуля ядра защиты оно считывает параметры идентификации, переданные модулем входа в систему. Затем программа ожидает события завершения инициализации подсистемы защиты информации операционной системы. При наступлении данного события ядро защиты разрешает начать идентификацию пользователя в Windows NT, используя параметры идентификации, считанные с идентификатора пользователя. При использовании для входа в систему идентификатора на USB ключе, последний должен быть установлен. Если к данному моменту ключ будет изъят, то на экран будет выдано стандартное сообщение Windows NT о необходимости нажать комбинацию клавиш *Alt-Ctrl-Del* или вставить карту, и компьютер будет заблокирован. Для продолжения входа в систему необходимо вставить USB ключ. Если процесс входа в систему Windows NT правильно обрабатывает запрос на вход пользователя, то происходит беспрепятственный вход пользователя в

систему. В противном случае на экран выдается стандартное сообщение о причинах запрета при входе в Windows NT. К возможным причинам запрета входа в Windows NT относятся недоступность контроллера домена, отсутствие соединения по локальной сети, несовпадение пароля пользователя в Windows NT и на идентификаторе и другие. После устранения причины запрета пользователь закрывает стандартное сообщение, и программа автоматически повторяет попытку входа в Windows NT. После трех неудачных попыток входа в систему пользователю предоставляется возможность корректно завершить сеанс работы путем выключения или перезагрузки компьютера.

Шаг 7. При завершении работы пользователя происходит стирание из оперативной памяти всех параметров идентификации пользователя. Вход в систему другого пользователя возможен только с выполнения шага 1 после перезагрузки компьютера.

Повторная идентификация пользователей возможна только в том случае, если при первоначальной идентификации зарегистрировался пользователь, не являющийся администратором СЗИ ***«Страж NT»***. Такое ограничение введено в связи с тем, что при входе администратора могут быть запущены службы или сервисы, не разрешенные для запуска пользователям и способные нарушить работоспособность системы защиты. При *повторной идентификации* возможен вход как администратора системы защиты, так и обычного пользователя.

Для выполнения *повторной идентификации* необходимо завершить текущий сеанс пользователя, предъявить персональный идентификатор и ввести пароль другого пользователя. Алгоритм *повторной идентификации* пользователей аналогичен алгоритму *первоначальной идентификации*, за исключением того, что *повторная идентификация* происходит, когда операционная система уже загружена. Если при *повторной идентификации* будет предъявлен идентификатор завершившего сеанс пользователя, то вход в систему произойдет автоматически тем же пользователем без запроса пароля.

В СЗИ ***«Страж NT»*** реализована функция временной блокировки и разблокировки компьютера с помощью персонального идентификатора. В зависимости от типа используемого идентификатора алгоритм работы данного механизма различен.

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

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

При использовании USB идентификаторов для блокировки компьютера необходимо извлечь идентификатор. Компьютер будет заблокирован. Для разблокировки компьютера необходимо вставить идентификатор на место. Компьютер будет разблокирован.

Для всех типов идентификаторов допускается блокировка компьютера вручную путем нажатия комбинации клавиш *Alt-Ctrl-Del* и в появившемся окне кнопки *Блокировка*. Разблокировка компьютера происходит только при предъявлении идентификатора, как описано выше.

3.3.2. Дискреционный принцип контроля доступа

Для работы с файлами и папками на дисках операционная система 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 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.

К защищаемым ресурсам компьютера относятся логические диски, папки и файлы. Для дисков, имеющих *простой* тип доступа, все папки и файлы имеют одинаковые разрешения. Если на диск не установлен *простой* тип доступа, то каждый файл и каждая папка на диске могут иметь свои уникальные разрешения. Локальные жесткие диски, существующие на момент установки системы защиты, учитываются автоматически, при этом *простой* тип доступа не устанавливается. Съемные носители типа дискет, CD и DVD дисков, USB накопителей учитываются, как правило, с *простым* типом доступа. Тип доступа носителя может быть изменен с помощью программы *Учет носителей.*

Доступ к защищаемым ресурсам контролируется системой защиты с помощью разрешений, содержащихся в записях списка контроля доступа. Список контроля доступа может содержать как разрешающие, так и запрещающие записи.

Существуют следующие разрешения на доступ к папкам и файлам: *Полный доступ*, *Изменение*, *Чтение и выполнение*, *Список содержимого папки*, *Чтение* и *Запись*. Каждое из этих разрешений представляет собой логическую группу особых разрешений, которые перечислены и описаны ниже.

Обзор папок / Выполнение файлов

Для папок: *«Обзор папок»* разрешает или запрещает перемещение по структуре папок в поисках других файлов или папок, даже если пользователь не обладает разрешением на доступ к просматриваемым папкам (применимо только к папкам).

Для файлов: *«Выполнение файлов»* разрешает или запрещает запуск программ (применимо только к файлам).

Разрешение *«Обзор папок»* для папки не означает автоматическую установку разрешения *«Выполнение файлов»* для всех файлов в этой папке.

Содержание папки / Чтение данных

«Содержание папки»: разрешает или запрещает просмотр имен файлов и подпапок, содержащихся в папке. Это разрешение относится только к содержимому

данной папки и не означает, что имя самой этой папки также должно включаться в список (применимо только к папкам).

«Чтение данных»: разрешает или запрещает чтение данных, содержащихся в файлах (применимо только к файлам).

Чтение атрибутов

Разрешает или запрещает просмотр таких атрибутов файла или папки, как «Только чтение» и «Скрытый».

Чтение дополнительных атрибутов

Разрешает или запрещает просмотр дополнительных атрибутов файла или папки. Дополнительные атрибуты определяются программами и могут различаться для разных программ.

Создание файлов / Запись данных

«Создание файлов»: разрешает или запрещает создание файлов в папке (применимо только к папкам).

«Запись данных»: разрешает или запрещает внесение изменений в файл и запись поверх имеющегося содержимого (применимо только к файлам).

Создание папок / Дозапись данных

«Создание папок»: разрешает или запрещает создание папок внутри папки (применимо только к папкам).

«Дозапись данных»: разрешает или запрещает внесение данных в конец файла, но не изменение, удаление или замену имеющихся данных (применимо только к файлам).

Запись атрибутов

Разрешает или запрещает смену таких атрибутов файла или папки, как «Только чтение» и «Скрытый».

Разрешение *«Запись атрибутов»* не подразумевает права на создание или удаление файлов или папок: разрешается только вносить изменения в их атрибуты.

Запись дополнительных атрибутов

Разрешает или запрещает смену дополнительных атрибутов файла или папки. Дополнительные атрибуты определяются программами и могут различаться для разных программ.

Разрешение «*Запись дополнительных атрибутов»* не подразумевает права на создание или удаление файлов или папок: разрешается только вносить изменения в их атрибуты.

Удаление подпапок и файлов

Разрешает или запрещает удаление подпапок и файлов даже при отсутствии разрешения «Удаление» (применимо только к папкам).

Удаление

Разрешает или запрещает удаление файла или папки. Если для файла или папки отсутствует разрешение *«Удаление»*, объект все же можно удалить при наличии разрешения *«Удаление подпапок и файлов»* для родительской папки.

Чтение разрешений

Разрешает или запрещает чтение таких разрешений на доступ к файлу или папке, как *«Полный доступ»*, *«Чтение»* и *«Запись».*

Смена разрешений

Разрешает или запрещает смену таких разрешений на доступ к файлу или папке, как *«Полный доступ»*, *«Чтение»* и *«Запись»*.

Смена владельца

Разрешает или запрещает вступать во владение файлом или папкой. Владелец файла или папки всегда может изменять разрешения на доступ к ним независимо от любых разрешений, защищающих этот файл или папку.

Синхронизация

Разрешает или запрещает ожидание различными потоками файлов или папок и синхронизацию их с другими потоками, могущими занимать их. Это разрешение применимо только к программам, выполняемым в многопоточном режиме с несколькими процессами.

Разрешение *Полный доступ* включает в себя все выше перечисленные особые разрешения.

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

Разрешение *Чтение и выполнение*, а также *Список содержимого папки* включают в себя *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*.

Группы и пользователи, которым предоставлен полный доступ к папке, могут удалять любые файлы в такой папке, независимо от разрешений на доступ к этим файлам.

Если ресурс недоступен пользователю на чтение, он становится невидимым для пользователя, т.е. имя ресурса не возвращается в стандартных запросах на поиск файла.

Система защиты информации позволяет на каждый защищаемый ресурс устанавливать атрибуты защиты, к которым относятся список контроля доступа и идентификатор безопасности владельца ресурса. Список контроля доступа состоит из отдельных элементов, каждый из которых определяет пользователя или группу пользователей и разрешенный для них тип доступа. Владелец ресурса имеет право изменять список контроля доступа, даже если это право ему явно не разрешено. Кроме того, при определении разрешенного типа доступа к ресурсу учитываются и другие атрибуты защиты, в частности метки конфиденциальности и режим запуска. Информация о метках конфиденциальности приводится в разделе, описывающем мандатный принцип контроля доступа. Доступ к ресурсам (исполняемым файлам), у которых разрешен режим запуска, запрещен по записи (за исключением режима обновления ПО). Тем самым обеспечивается целостность программной среды.

Контроль доступа к защищаемым ресурсам реализован в ядре защиты системы ***«Страж NT»*** 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 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:

1. 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.
2. 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.
3. 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.
4. Если не все типы доступа маски запроса разрешены, и весь список контроля доступа просмотрен, доступ к ресурсу запрещается.
5. 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.

1. 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.
2. 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 установлена *проверка разрешений 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.
3. 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.
4. 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.

5. 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 Windows и программного обеспечения.

6. При запросе к файлу или папке на удаленном компьютере решение о предоставлении доступа принимается на удаленном компьютере.

7. При создании новых файлов или папок действуют правила наследования разрешений, реализованные в файловой системе NTFS.

8. 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. В идентификаторе пользователя должны находиться записи только для тех компьютеров, к которым пользователь допущен.

3.3.3. 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»*** используются следующие значения меток конфиденциальности в порядке повышения:

- несекретно;
- секретно;
- совершенно секретно.

Существует возможность переименования меток конфиденциальности в процессе эксплуатации системы защиты.

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

В полном объеме мандатные правила применяются к учтенным носителям, для которых не установлен *простой* тип доступа. Для учтенных носителей с *простым* типом доступа действуют упрощенные мандатные правила, при которых все файла и папки на носителе имеют одинаковый гриф, который соответствует грифу носителя.

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 вложенные объекты останутся несекретными. При изменении метки конфиденциальности на папке меняются и мандатные метки вложенных объектов. В случае, когда на какой-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.

1. В системе должны существовать или могут создаваться ресурсы, имеющие различные грифы секретности.
2. К обработке защищаемых ресурсов должны быть допущены пользователи, обладающие различными уровнями допуска.
3. В системе установлены и определены прикладные программы, с помощью которых планируется производить обработку защищаемых ресурсов.

При соблюдении всех этих условий администратор безопасности 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, сформировать идентификатор и обновить информацию в домене;
- для прикладных программ, предназначенных для обработки защищаемых ресурсов, разрешить режим запуска и установить значение допуска;
- определить защищаемые ресурсы и установить на них мандатную метку.

Все указанные действия могут выполняться только администратором безопасности.

После выполнения всех необходимых настроек реализация мандатного доступа к защищаемым ресурсам происходит следующим образом.

При запуске прикладной программы со значением допуска выше *несекретно* пользователем, имеющим уровень допуска выше *несекретно*, как правило происходит следующее:

- текущий допуск программы становится *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 4 значения:

- *Не запрашивать* – текущий допуск программы становится *несекретно*;
- *По умолчанию*. В данном случае при запуске 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 и самих 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 – *секретно*, 2 – *сов.секретно*. Например, для запуска программы *Notepad* с текущим допуском *секретно* можно создать пакетный файл следующего содержания:

set @GuardNT@ = 1

notepad

При запуске данного пакетного файла программе *Notepad* будет назначен текущий допуск *секретно*, если такое разрешено, в противном случае текущий допуск останется без изменений.

При запуске программы, для которой возможно изменение текущего допуска, значение текущего допуска отображается в заголовке главного окна программы (за исключением консольных приложений).

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:

1. 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.

2. Пользователь получает доступ к ресурсу по чтению и записи в том случае, если текущий допуск прикладной программы, осуществляющей доступ, равен грифу секретности данного ресурса.
3. 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.
4. 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:

1. Основываясь на типе доступа к ресурсу, операционная система создает маску запроса на доступ.
2. 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.
3. Осуществляется проверка разрешения на доступ в соответствии с дискреционными правилами. При запрете доступа дальнейшая проверка не производится, доступ к файлу или папке запрещается.
4. 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.
5. 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 гриф секретности самого файла или папки и всех родительских папок, включая корневой каталог диска, равен или ниже текущего грифа программы либо имеет значение *без проверки*.

При запросе на запись файла или папки доступ разрешается только в том случае, если гриф секретности самого файла или папки равен текущему грифу программы или имеет значение *без проверки*, а также если среди родительских папок, включая корневой каталог, нет ни одной, имеющей гриф секретности выше текущего допуска программы, а также имеется хотя бы одна папка, имеющая гриф секретности, равный текущему допуску программы либо значению *без проверки*.

При запросе только на добавление данных файла или папки доступ разрешается в том случае, если гриф секретности самого файла или папки выше текущего грифа программы или имеет значение *без проверки*, а также если среди родительских папок, включая корневой каталог, имеется хотя бы одна папка, имеющая гриф секретности, выше или равный текущему грифу программы либо равный 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.

Чтобы автоматизировать настройку сложных программных продуктов для обработки конфиденциальной информации используются шаблоны настроек (см. *Руководство администратора*). Шаблон настроек представляет собой набор правил и защитных атрибутов для папок и файлов, входящих в состав пакета прикладных программ. Шаблоны наиболее используемых пакетов прикладных программ опубликованы на сайте продукта *www.guardnt.ru*.

Мандатные правила контроля доступа действуют также в отношении принтеров при выдаче документов на печать. Более подробно данный вопрос рассмотрен в пункте 3.3.12 *Маркировка документов*.

3.3.4. 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 прикладной 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. Другими словами, установлена ли на удаленном компьютере СЗИ ***«Страж NT»***. 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.

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.

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 гриф секретности 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 гриф *без проверки*. При этом необходимо исключить возможность записи защищаемой информации в эти файлы;
- Установить один из предусмотренных параметров запроса текущего допуска программы при старте;

- Использовать специальную переменную процесса *@GuardNT@* для установки текущего допуска программы.

3.3.5. Управление запуском программ

Каждый исполняемый файл системы, необходимый для работы пользователя, должен иметь разрешение на запуск. Для этого служит атрибут *режим запуска*. В СЗИ ***«Страж NT»*** предусмотрены следующие значения *режима запуска*:

- *Запрещен*;
- *Приложение*;
- *Сервер-приложение*;
- *Инсталлятор*.

Пользователь может запустить программу, хранящуюся в файле, на выполнение, если для данного файла разрешен *режим запуска*. Если режим запуска файла запрещен, запрос на выполнение не будет выполнен. Разрешение на запуск файла может дать только администратор безопасности и только в режиме администрирования. 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 разрешен *режим запуска*, доступны пользователям только на чтение, что обеспечивает целостность программной среды.

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

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 Windows\system32\msiexec.exe, а также на все файлы с расширением .msi,

расположенные в папке Windows\Installer. *Программа установки и снятия* автоматически устанавливает *режим запуска* на указанные файлы 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. Естественно при создании новых файлов на них устанавливается режим запуска *Запрещен*. В этом случае пользователю, не являющемуся администратором защиты, запуск таких файлов в качестве исполняемых модулей будет запрещен, соответственно приложения будут работать некорректно или не смогут запускаться совсем. Для того 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.

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 значение *приложение*. Таким образом облегчается настройка режимов запуска сложных программных комплексов.

Режим автозапуска всегда включается после установки системы защиты или отказа от настроек системы защиты. В этом случае происходит автоматическое разрешение *режима запуска* на все системные компоненты, загружающиеся при входе пользователя в систему. Разрешение *режима запуска* для прикладных программ состоит в запуске данных программ при первом после установки системы защиты сеансе работы или при включении *режима автозапуска*. Включается

режим автозапуска только администратором безопасности в программе *Монитор системы защиты*.

В случае, если снятие системы защиты информации происходит с сохранением текущих настроек, то после установки в первом сеансе работы *режим автозапуска* будет выключен.

Предусмотрена возможность включения *режима автозапуска* на следующий сеанс работы, что позволяет выполнять настройку драйверов и сервисных программ операционной системы, программ, запускаемых один раз при создании нового пользовательского профиля и в других сложных ситуациях. Для включения *режима автозапуска* на следующий сеанс работы необходимо в программе *Монитор системы защиты* включить *режим автозапуска* и включить параметр *Оставить на следующий сеанс. Режим автозапуска* будет включен на следующий сеанс работы либо до его завершения, либо до момента явного отключения *режима автозапуска* в программе *Монитор системы защиты*.

Существует также еще один режим работы системы защиты, который называется *режим обновления программного обеспечения.* Он устанавливается и работает аналогично режиму автозапуска на следующий сеанс, за исключением того, что исполняемые файлы становятся доступными на изменение и удаление. Данный режим предназначен для установки обновлений операционной системы и прикладных программ без необходимости снятия системы защиты.

3.3.6. Контроль DOS приложений

В СЗИ ***«Страж NT»*** предусматривается возможность контроля запуска и изменения текущего допуска приложений MS DOS. С этой целью на программу NTVDM.EXE устанавливается режим запуска *приложение* и допуск, соответствующий максимальному грифу информации, обрабатываемому с помощью программ MS DOS. После этого на все необходимые для работы пользователей программы MS DOS устанавливается режим запуска *приложение* и требуемый допуск. Режим запуска может быть установлен автоматически с помощью *режима автозапуска*. При запуске программы MS DOS с установленным допуском на экран выдается диалоговое окно для выбора текущего допуска программы. Для изменения

текущего допуска необходимо запустить программу заново. Если программе MS DOS в процессе работы необходимо запустить другую программу MS DOS, то действуют следующие правила. Программа может запустить другую программу, только если текущий допуск новой программы будет равен или выше текущего допуска вызывающей программы. При завершении вызванной программы, если текущий допуск вызываемой программы был ниже текущего допуска вызванной программы, то вызывающая программа будет закрыта.

Контроль DOS приложений отсутствует в среде 64-разрядных операционных систем.

3.3.7. Управление защитой

Механизмы защиты, реализованные в ядре СЗИ ***«Страж NT»***, функционируют и обеспечивают работоспособность прикладных программных средств и системы в целом только при условии правильной настройки системы защиты, а также своевременного контроля функционирования системы защиты и ее периодического тестирования. К числу настроек и контролируемых функций, которые необходимо выполнять на каждом компьютере, относятся следующие:

- установка и снятие системы защиты;
- установка и изменение атрибутов защиты файлов и папок (списков контроля доступа, идентификаторов безопасности владельцев, режимов запуска, параметров контроля целостности и аудита и др.);
- установка и изменение списков контроля доступа и грифа секретности носителей и принтеров;
- установка и изменение списков контроля доступа для типов устройств;
- просмотр и анализ журнала регистрации событий;
- включение режимов аудита системы защиты;
- настройка подсистемы маркировки документов;
- управление списком пользователей и их свойствами;
- смена паролей пользователей;
- формирование идентификаторов пользователей;

- ведение журнала учета носителей;
- тестирование системы защиты.

Для выполнения большинства настроек требуется включение *режима администрирования* системы защиты. Данный режим может быть включен только администратором безопасности. В *режиме администрирования* отключаются некоторые механизмы, реализованные в ядре системы защиты. Таким образом, администратор безопасности имеет право изменять любые настройки в системе. К числу механизмов защиты, которые отключаются при установке *режима администрирования*, относятся следующие:

- дискреционные правила разграничения доступа к носителям, файлам, папкам, принтерам;
- мандатные правила разграничения доступа к носителям, файлам, папкам, принтерам;
- контроль потоков информации;
- запрет включения режима автоматического разрешения режима запуска;
- запрет изменения грифа или допуска файлов и папок, режимов запуска, параметров дополнительного аудита, параметров контроля целостности.

Если *режим администрирования* выключен, то для администратора действуют те же правила и ограничения, как и для пользователя системы, за исключением запуска программ. Администратору безопасности всегда разрешен запуск программ, как с локальных дисков компьютера, так и с отчуждаемых и сетевых носителей.

Управление защитой осуществляется при помощи программ:

- *установка и снятие системы защиты;*
- *настройка системы защиты;*
- *менеджер файлов;*
- *менеджер пользователей;*
- *учет носителей;*

- *контроль устройств;*
- *журнал событий;*
- *редактор шаблонов настроек;*
- *монитор системы защиты.*

При настройке атрибутов защиты ресурсов системы могут возникать ситуации, при которых некоторые приложения перестают правильно функционировать. Для разрешения подобных конфликтных ситуаций рекомендуется шире использовать возможности подсистемы регистрации либо применять дополнительные средства мониторинга системных событий.

3.3.8. Регистрация

В СЗИ ***«Страж NT»*** реализована собственная подсистема регистрации событий. Для хранения событий системы защиты предусмотрен специальный файл в формате базы данных Microsoft Access. Полный перечень регистрируемых системой защиты событий приведен в Приложении 1. Все регистрируемые события включены в следующие категории:

- события входа в систему
- события запуска программ
- события доступа к объектам
- события контроля целостности
- 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. Для данной категории регистрируются следующие параметры:

- дата и время
- код события
- тип идентификатора
- серийный номер идентификатора
- имя пользователя
- пароль в случае неправильного ввода

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. Для данных категорий событий регистрируются следующие параметры:

- дата и время
- код события
- имя объекта
- имя процесса
- имя пользователя
- гриф объекта
- допуск процесса

В категорию контроля целостности входят все факты нарушения целостности защищаемых файлов. В параметрах регистрации указывается:

- дата и время
- код события
- имя файла

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. Практически все события регистрируются в обязательном порядке, исключение составляет лишь категория событий доступа к объектам. Для данной категории предусмотрена настройка регистрации отдельных событий.

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. *Дополнительный аудит* может устанавливаться только администратором безопасности и только при включенном режиме администрирования. 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 секретности *секретно* или *совершенно секретно* и при этом файл не является исполняемым, т.е. файлу не разрешен *режим запуска*.

При запросах на переименование регистрация 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 режиме затирания всех файлов при удалении.

Дополнительно предусмотрена возможность включать и отключать регистрацию событий для различных запросов на доступ. По умолчанию после установки системы защиты включена регистрация следующих событий:

- успешные запись, изменение, удаление и переименование
- отказ чтения, записи, изменения, удаления и переименования

Изменение параметров дополнительного аудита производится в программе *Настройка системы защиты.*

События безопасности, регистрируемые ядром СЗИ ***«Страж NT»***, помещаются в специальный регистрационный журнал. Периодически и по запросу администратора данный журнал переписывается в базу данных Журнала событий с помощью программы *Преобразования журнала.* Прочитать записи журнала можно с помощью программы *Журнал событий*. Программа предоставляет возможность выборочного ознакомления с журналом путем сортировки и поиска по любым значимым полям, а также сохранения, стирания и распечатки журнала.

СЗИ ***«Страж NT»*** также обеспечивает регистрацию документов, выдаваемых на печать с помощью стандартного графического интерфейса Windows. Более подробно данный механизм описан в пункте 3.3.12 *Маркировка документов*.

3.3.9. Контроль целостности

В системе защиты предусмотрен контроль целостности защищаемых файлов и файлов системы защиты. Контроль целостности может осуществляться автоматически при загрузке операционной системы, при открытии файлов на чтение и по запросу администратора. 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 фиксируется факт нарушения целостности, и дальнейшая проверка не производится.

При обнаружении нарушения целостности файлов предусмотрены следующие реакции системы защиты:

- *блокировка открытия файла* – при открытии файла на чтение пользователем произойдет отказ в доступе с ошибкой нарушения целостности;
- *блокировка загрузки системы* – действует только для файлов на системном диске компьютера при автоматическом контроле целостности во время загрузки операционной системы. В случай нарушения целостности произойдет регистрация факта в журнале и блокировка дальнейшей загрузки операционной системы;
- *пересчет параметров* – в случае нарушения целостности произойдет регистрация факта в журнале, после чего параметры контроле целостности для данного файла будут обновлены.

В рамках этой же подсистемы реализован контроль целостности исполняемых файлов системы защиты. Контроль целостности на файлы системы защиты устанавливается автоматически, при этом включаются все параметры контроля целостности с блокировкой загрузки системы в случае нарушения целостности.

3.3.10. Очистка памяти

В СЗИ ***«Страж NT»*** реализована функция очистки файлов при их удалении. По умолчанию при установке системы защиты очистка включается только для файлов, имеющих гриф секретности *секретно* или *сов.секретно*. Возможно включение режима очистки всех удаляемых файлов вне зависимости от грифа секретности. Для этого необходимо установить параметр *Гарантированная очистка*

всех удаляемых файлов в программе *Настройка системы защиты*. Если для удаляемого файла должна выполняться очистка, то по команде удаления файла его содержимое затирается случайной последовательностью с использованием алгоритма ГОСТ 28147-89, а затем файл удаляется.

Для обеспечения очистки файлов, помещаемых в корзину, должен быть установлен режим уничтожения файлов сразу после удаления, не помещая их в корзину.

В СЗИ ***«Страж NT»*** реализован механизм очистки оперативной памяти нулями при выделении страницы по запросу программ, а также включается режим очистки файла подкачки страниц при завершении работы.

Существует возможность отключения механизма очистки файла подкачки.

3.3.11. Изоляция модулей

Операционная система Windows содержит встроенные механизмы, предотвращающие доступ одних процессов к оперативной памяти других процессов. Данные механизмы основаны на системе виртуальной памяти и поддерживается как на аппаратном уровне средствами процессора, так и на уровне ядра Windows.

3.3.12. Маркировка документов

В СЗИ ***«Страж NT»*** реализована подсистема маркировки документов. Маркировке подлежат документы, выдаваемые на печать при помощи стандартного унифицированного графического интерфейса Windows (GDI). Не маркируются документы, выдаваемые напрямую на принтер, без использования графического интерфейса. Как правило, так печатаются документы в консольных приложениях, не использующих оконный интерфейс Windows.

При установке системы защиты информации по умолчанию включена маркировка всех документов, выдаваемых на печать. В программе *Настройка системы защиты* может быть включена или отключена маркировка документов любого грифа.

Для всех документов, выдаваемых на печать, автоматически регистрируется факт печати документа в *Журнале событий*.

В случае вывода на печать документов с грифом выше *Несекретно* необходимо выполнить дополнительную настройку для устройств вывода (принтеров).

Во-первых, на принтер необходимо установить соответствующий гриф. При этом реализуются следующие правила:

- если принтер имеет гриф *Несекретно*, на него разрешается выводить только несекретные документы;
- если принтер имеет гриф *Секретно*, на него разрешается выводить только секретные документы;
- если принтер имеет гриф *Сов.секретно*, на него разрешается выводить только секретные или сов.секретные документы;
- если принтер имеет гриф *Без проверки*, на него разрешается выводить любые документы.

Во-вторых, необходимо выполнить настройку драйверов принтера для печати документов соответствующего грифа. В силу многообразия подходов к реализации процесса вывода на печать различными производителями принтеров, универсальных методик настройки драйверов не существует. Вариант настройки драйверов для типовых моделей принтеров содержится в шаблоне *Подсистема печати*, опубликованном на нашем сайте *www.guardnt.ru*.

Далее необходимо запустить программу *Настройка системы защиты* и установить требуемые параметры маркировки документов. К параметрам маркировки документов относятся:

- свойства углового штампа, печатаемого на первом листе документа;
- свойства нижнего штампа, печатаемого на каждом листе документа, кроме последнего;
- свойства штампа на последнем листе документа.

Угловой штамп выводится на первом листе документа в верхнем правом углу листа. В угловом штампе могут указываться гриф документа, поле номера экземпляра и при необходимости 3 дополнительных поля. Для несекретных документов вывод грифа может быть отключен.

Нижний штамп выводится в нижней части каждого листа, кроме последнего. В нижнем штампе указывается учетный номер и гриф документа, учетные реквизиты АС, учетный номер носителя, номер листа, дата печати документа и при необходимости дополнительное поле.

Штамп на последнем листе документа содержит следующую информацию:

- количество экземпляров и адрес для каждого экземпляра;
- фамилия и телефон исполнителя;
- фамилия отпечатавшего документ;
- учетный номер и гриф документа;
- учетные реквизиты АС;
- общее количество листов документа;
- дату выдачи документа на печать;
- дополнительное поле.

Настройка всех параметров маркировки осуществляется только Администратором безопасности, т.е. пользователем, включенным в группу локальных администраторов. Некоторые параметры могут быть удалены из маркировки документов.

Процесс маркировки осуществляется следующим образом:

1. Пользователь создает документ при помощи какого-либо Windows приложения. Гриф документа соответствует текущему допуску приложения.
2. Пользователь отправляет документ на печать на какой-либо из принтеров с соответствующим грифом.

3. Система защиты перехватывает запрос приложения на распечатку документа и выдает диалоговое окно для заполнения дополнительных полей маркировки.
4. После ввода необходимых полей и закрытия диалогового окна происходит автоматическая маркировка каждого листа документа и документ отправляется на принтер.
5. Система защиты автоматически фиксирует факт печати документа в *Журнале событий*.

При регистрации фактов печати документов в *Журнал событий* записывается следующая информация:

- гриф документа;
- дата и время выдачи документа на печать;
- регистрационный номер документа;
- название документа;
- имя компьютера;
- имя пользователя;
- имя принтера;
- количество экземпляров;
- количество листов в экземпляре.

Количество листов брака, отметка об уничтожении брака, а также примечание заполняются вручную Администратором безопасности.

Просмотр записей журнала производится с помощью программы *Журнал событий*.

Для корректной работы подсистемы маркировки документов исполнителями должны выполняться определенные требования. К ним относятся следующие:

1. При подготовке документа должны быть оставлены поля для соответствующих штампов.

2. Документ должен выводиться на печать целиком с первого по последний лист. Выборочная печать отдельных листов или печать листов в обратном порядке не допускается.
3. Двусторонняя печать и печать брошюр не допускается, если эта функция не поддерживается принтером.
4. Не рекомендуется печать на бумаге различного формата.
5. Не рекомендуется применять средства окончательной обработки документа, предоставляемые драйвером принтера.
6. При выдаче диалогового окна для заполнения дополнительных полей маркировки все доступные поля должны корректно заполняться.

3.3.13. Защита ввода и вывода на отчуждаемый носитель информации

Для защиты ввода вывода на отчуждаемый носитель в СЗИ ***«Страж NT»*** предусмотрены подсистемы *учета носителей* и *преобразования информации на отчуждаемых носителях*. Подсистема *учета носителей* подробно описаны в разделах 1.11.

Подсистема *преобразования информации на отчуждаемых носителях* предоставляет дополнительный механизм защиты съемных носителей, типа дискет и USB-флэш накопителей, путем прозрачного преобразования всей информации, записываемой на носитель. Преобразование информации осуществляется с применением функции гаммирования с обратной связью алгоритма криптографического преобразования ГОСТ 28147-89. В качестве ключей используются записанные на идентификатор пользователя *главный ключ* системы, либо *рабочий ключ* компьютера. Если в качестве ключа выбран *главный ключ* системы, преобразованные носители будут читаться на всех компьютерах, на которых установлена СЗИ ***«Страж NT»*** с помощью единого идентификатора администратора и также включено преобразование на *главном ключе* системы. Если же выбран *рабочий* ключ компьютера, то отчуждаемые носители будут читаться только на данном компьютере. Включение режима *преобразования информации на*

отчуждаемых носителях, а также выбор ключей, осуществляется в программе *Настройка системы защиты* в разделе *Преобразование информации.*

После включения *режима преобразования* не преобразованные ранее носители не будут нормально читаться на компьютере. Для преобразования носителя необходимо его подключить к системе. Когда система распознает носитель, она выдаст сообщение о том, что устройство не отформатировано и предложит произвести форматирование. Необходимо выполнить форматирование носителя и после его завершения произвести учет носителя с помощью программы *Учет носителей*.

Если до преобразования носителя на нем были записаны какие-либо данные, то их при необходимости можно сохранить, например, на жестком диске компьютера.

3.3.14. Сопоставление пользователя с устройством

Для реализации данного механизма служат подсистемы *учета носителей* (1.11) и *контроля устройств* (1.12 и 1.15), описанные выше.

3.3.15. Взаимодействие пользователя с СЗИ

СЗИ ***«Страж NT»*** представляет собой программный комплекс, состоящий из отдельных модулей, каждый из которых выполняет четко определенные функции. Назначение модулей системы защиты описано в разделе 1 **Назначение программы** настоящего документа.

Интерфейс пользователя и СЗИ четко определен и описан. Вход пользователя в систему по шагам описан в пункте 3.3.1 настоящего документа. К другим элементам интерфейса относятся установление текущего допуска прикладных программ, а также сообщения о событиях безопасности, выдаваемые на экран при работе пользователя.

3.3.16. Надежное восстановление

В СЗИ ***«Страж NT»*** предусмотрен механизм восстановления параметров разграничения доступа при сбоях и отказах оборудования. С этой целью ведется две копии базы данных, в которой хранятся настройки системы защиты. Вторая копия

базы данных обновляется каждый раз при завершении работы пользователей. Если при входе в систему первая копия базы данных оказывается разрушенной, то система защиты автоматически использует вторую копию и при этом восстанавливает первую. При этом пользователю на экран выдается соответствующее сообщение.

3.3.17. Целостность СЗИ

Для осуществления периодического контроля целостности системы защиты информации при настройке системы защиты устанавливаются параметры автоматического контроля целостности при входе в систему на все модули системы защиты. При нарушении целостности модулей системы защиты работа пользователей блокируется, и вход в систему становится возможным только для администратора защиты.

Все модули системы защиты выполняются в отдельной части оперативной памяти компьютера, что обеспечивается встроенными в Windows механизмами поддержки виртуальной памяти.

3.3.18. Тестирование СЗИ

Для осуществления периодического тестирования функций и механизмов системы защиты информации предназначена программа *Тестирование системы защиты*. Данная программа позволяет проводить автоматическое тестирование по запросу администратора следующих механизмов защиты:

- дискреционных правил разграничения доступа;
- мандатных правил разграничения доступа;
- защиты ввода-вывода на отчуждаемый носитель;
- контроля целостности.

При тестировании функций защиты ввода-вывода на отчуждаемый носитель проверяется работа дискреционных и мандатных правил разграничения доступа, а также запись меток конфиденциальности на гибких магнитных дисках. Для тестирования данной функции необходимо, чтобы в дисковод была установлена отформатированная дискета.

Программа тестирования может осуществлять тестирование СЗИ как на локальном компьютере, так и на любом доступном сетевом компьютере, на котором установлена СЗИ ***«Страж NT»***. На удаленных компьютерах функция тестирования защиты ввода-вывода на отчуждаемый носитель недоступна.

Результаты тестирования системы защиты оформляются в виде отчета, который может быть сохранен на диске или распечатан.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными для системы защиты информации ***«Страж NT»*** являются политика безопасности и правила разграничения доступа, разработанные и реализуемые в конкретной автоматизированной системе. Эти данные преобразуются в конкретные значения атрибутов защиты ресурсов системы и полномочия пользователей, при помощи которых система защиты реализует свои механизмы. Выходными данными СЗИ ***«Страж NT»*** являются сообщения об отказе в доступе в случае нарушения ПРД и других несанкционированных действиях, а также журналы безопасности, печати и контроля целостности.

Перечень сокращений

АС	Автоматизированная система
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ПРД	Правила разграничения доступа
ПЭВМ	Персональная электронная вычислительная машина
ОС	Операционная система
СЗИ	Система защиты информации

Приложение 1

Перечень регистрируемых событий

Наименование события	Описание события
События контроля целостности	
Ошибка контрольной суммы	Несовпадение контрольной суммы при проверке целостности файла
Несовпадение даты изменения	Несовпадение даты изменения файла при проверке целостности
Несовпадение размера файла	Несовпадение размера файла при проверке целостности
Файл не найден	Не найден файл, для которого установлен контроль целостности
Ошибки при проверке целостности	Непредвиденная ошибка при проверке целостности
Нарушение целостности файла СЗИ	Произошло нарушение целостности файла системы защиты
События входа в систему	
Успешный вход в систему	Успешный вход пользователя в систему
Идентификатор испорчен	Предъявленный идентификатор не содержит идентификационную информацию, либо информация испорчена
Неверный пароль	Произошла трехкратная попытка ввода неверного пароля
Ошибка идентификации	Пользователю не разрешен вход в систему на данном компьютере
События запуска программ	
Запуск запрещен	Попытка запуска не разрешенного исполняемого файла
Запуск программы	Успешный запуск процесса
Разрешение запуска программы в режиме автозапуска	На исполняемый файл автоматически установлен режим запуска *приложение*
Установка текущего допуска	Произошло изменение текущего допуска приложения
Отказ установки текущего допуска	Изменение текущего допуска приложения отклонено системой защиты
Установка режима администрирования	Установлен режим администрирования
Снятие режима администрирования	Снят режим администрирования
Отказ установки режима администрирования	При попытке установки режима администрирования произошел отказ

Установка режима автозапуска	Установлен режим автозапуска
Снятие режима автозапуска	Режим автозапуска отключен
События доступа к объектам	
Подключение тома	Произошло обращение к новому тому в системе
Создание файла	Создание нового файла
Открытие файла	Открытие файла
Чтение файла	Открытие файла на чтение
Запись файла	Открытие файла на запись
Изменение файла	Открытие файла на изменение
Удаление файла	Произошло затирание файла перед его удалением
Переименование файла	Выполнен запрос на переименование файла
Отказ в доступе	Отказ при открытии файла
Отказ в чтении	Отказ при открытии файла на чтение
Отказ в записи	Отказ при открытии файла на запись
Отказ в изменении	Отказ при открытии файла на изменение
Отказ удаления	Отказ при открытии файла на удаление
Отказ в переименовании файла	Отказ при переименовании файла
Установка грифа на файл	Установка нового грифа на файл или папку
Установка разрешения на запуск	Установка нового режима запуска файла
Установка контроля целостности	Установка параметров контроля целостности файла
События действий администратора	
Останов системы защиты	Останов системы защиты либо по запросу администратора, либо при завершении системы
Запуск системы защиты	Запуск системы защиты при старте системы, а также по запросу администратора после ее останова
События управления объектами доступа	
Установка грифа на принтер	Установка грифа на принтер
События управления пользователями	
Создание пользователя	Добавление нового пользователя системы
Удаление пользователя	Удаление пользователя из системы
Переименование пользователя	Переименование пользователя системы
Смена (назначение) пароля	Назначение или смена пароля пользователя
Изменение допуска	Изменение уровня допуска пользователя
Изменение статуса администратора СЗИ	Установка или снятие признака администратора системы защиты
Добавление пользователя в группу	Добавление пользователя в локальную или глобальную группу
Удаление пользователя из группы	Удаление пользователя из группы

Формирование идентификатора	Формирование персонального идентификатора пользователя
События управления носителями	
Добавление носителя	Добавление носителя в журнал учета
Удаление носителя	Удаление носителя из журнала учета
Изменение свойств носителя	Изменение свойств носителя в журнале учета
События управления устройствами	
Изменение свойств устройств	Изменение разрешений для класса устройств
Старт устройства	Старт устройства после вынужденного останова
Останов устройства	Останов устройства в случае запрета для пользователя, вошедшего в систему
События системы защиты	
Разрушены настройки системы защиты	Настройки системы защиты и их копия оказались разрушены, вход выполнен с новыми настройками, как при первоначальном входе после установки СЗИ
События печати	
Печать документа	Произошла печать документа
Отмена печати	При запросе параметров маркировки документов пользователь выбрал отмену печати
Очистка журнала печати	Выполнена очистка журнала событий в части событий печати

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
Изм.	Измененных	Замененных	Новых	Аннулированных					