ИНСТИТУТ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

«Гриф–Мережа»

Комплекс средств защиты информации в локальных вычислительных сетях от несанкционированного доступа

версия 3

Описание комплекса

редакция 2

Киев 2015

ИНСТИТУТ
КОМПЬЮТЕРНЫХ
ТЕХНОЛОГИЙ
Тел.: (044) 499-98-44
E-mail: ict@ict.com.ua
http://www.ict.com.ua

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место

АС – автоматизированная система

БД – база данных

ИсОД – информация с ограниченным доступом

КСЗ – комплекс средств защиты

ЛВС – локальная вычислительная сеть

НД ТЗИ – нормативный документ системы технической защиты информации

НСД – несанкционированный доступ

ОКД – основной контроллер домена

ОП – оперативная память

ОС – операционная система

ПБ – политика безопасности

ПО – программное обеспечение

ППС – прикладные программные средства

ПРД – правила разграничения доступа

ПС – программные средства

РВС – распределенная вычислительная сеть

РС – рабочая станция

СУБД – система управления базой данных

ТС – технологическая схема

ФС – файловый сервер

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

КСЗ **«Гриф–Мережа»** предназначен для защиты ИсОД, обрабатываемой в АС, построенных на базе ЛВС, в состав которых входят РС, функционирующие под управлением ОС MS Windows XP Professional/ MS Windows Vista (Professional, Enterprise, Ultimate)/ MS Windows 7 (Professional, Enterprise, Ultimate в т.ч. 64-разрядных), Windows 8/ 8.1 (Professional, Enterprise в т.ч. 64-разрядных) и ФС, функционирующие под управлением ОС MS Windows 2003 Server/ MS Windows 2008 Server/ MS Windows 2008 Server R2/ MS Windows 2012 Server/ MS Windows 2012 Server R2, от угроз целостности, конфиденциальности и доступности при реализации политики административного управления доступом к информации.

Использование КСЗ **«Гриф–Мережа»** в ЛВС обеспечивает:

- регистрацию всех лиц, которые принимают участие в обработке ИсОД, в качестве пользователей ЛВС;
- предоставление доступа к ИсОД только при условии достоверного опознания пользователей ЛВС и с учетом предоставленных им согласно со служебной необходимостью полномочий;
- возможность своевременного доступа зарегистрированных пользователей к ИсОД;
- невозможность неконтролируемого и несанкционированного ознакомления, размножения, распространения, копирования и восстановления ИсОД в процессе ее обработки в ЛВС;
- невозможность неконтролируемой и несанкционированной модификации ИсОД в процессе ее обработки в ЛВС;
- возможность создания в ЛВС "замкнутой программной среды" и использования для обработки ИсОД только прошедших соответствующую проверку программных средств;
- возможность пресечения захвата пользователем чрезмерного объема ресурсов (дискового пространства) ФС ЛВС, при котором становится невозможной дальнейшая работа других пользователей;
- учет действий всех пользователей ЛВС, касающихся обработки ИсОД, регистрацию попыток нарушения установленного порядка доступа к информации, а также возможность блокирования доступа к информации в случае выявления таких попыток;
- возможность доступа к функциям администрирования (управления правами доступа к ИсОД) только при условии достоверного опознания администраторов и с учетом предоставленных им в соответствии со служебной необходимостью полномочий;
- учет действий администраторов КСЗ, касающихся управления полномочиями доступа пользователей к ИсОД;
- возможность проведения непрерывного контроля за всеми событиями, имеющими отношение к безопасности обрабатываемой ИсОД, со стороны уполномоченных лиц.

2 СОСТАВ И АРХИТЕКТУРА КСЗ

В состав КСЗ **«Гриф–Мережа»** входят следующие основные компоненты:

– средства разграничения доступа, устанавливаемые на РС и ФС ЛВС, основной функцией которых является реализация административного управления доступом к защищаемым информационным ресурсам, содержащим ИсОД (далее – базовое ПО КСЗ):

  - интерфейсный модуль аутентификации (провайдер аутентификации);

  - модуль восстановления целостности и обновления КСЗ;

  - модуль контроля запросов доступа к ресурсам и управления правами доступа к ресурсам (системный драйвер и резидентный модуль пользовательского режима);

  - модуль обслуживания носителей данных аутентификации пользователей;

  - модуль контроля операций экспорта данных;

  - модуль контроля операций печати;

– средства регистрации данных аудита, устанавливаемые на РС и ФС ЛВС, основной функцией которых является сбор, передача и регистрация, в том числе в реальном времени, информации о событиях, имеющих отношение к безопасности обрабатываемой ИсОД:

  - агент модуля регистрации данных аудита (используется в конфигурации с повышенными требованиями к обеспечению наблюдаемости);

  - модуль сохранения локальных данных аудита;

  - модуль анализа локальных данных аудита (АРМ анализа локальных данных аудита);

– модуль регистрации данных аудита, устанавливаемый на ФС-ОКД (используется в конфигурации с повышенными требованиями к обеспечению наблюдаемости);

– АРМ администратора КСЗ, устанавливаемое на РС администратора КСЗ и РС администратора безопасности, основными функциями которого являются: регистрация пользователей, выработка данных идентификации и аутентификации с сохранением их на носителях данных аутентификации; регистрация защищаемых ресурсов; управление разграничением доступа пользователей к выбранным каталогам; контроль целостности и самотестирование КСЗ по запросу администратора; управление разграничением доступа прикладных программ к выбранным каталогам; управление квотами пользователей; включение/ выключение режима контроля программного обеспечения (запрет запуска незарегистрированных программ), активизация/ деактивизация учетных записей пользователей;

– АРМ администратора безопасности, устанавливаемое на РС администратора безопасности, основными функциями которого являются: настройка и управление параметрами аудита защищенных ресурсов и активного сетевого оборудования; управление параметрами оповещения и прием оповещений о критичных для безопасности событиях в режиме реального времени; возможность просмотра,

анализа и обработки протоколов аудита; работа с архивом данных аудита (используется в конфигурации с повышенными требованиями к обеспечению наблюдаемости);

– модуль взаимодействия с ППС, устанавливаемый на РС и ФС ЛВС и предназначенный для реализации взаимодействия между средствами КСЗ и ППС автоматизированных систем, функционирующих в ЛВС.

Архитектура КСЗ «Гриф-Мережа» (в конфигурации с повышенными требованиями к обеспечению наблюдаемости) приведена на рис. 2.1. Подробное описание функций, реализуемых различными компонентами КСЗ, приведено в разделе 3.

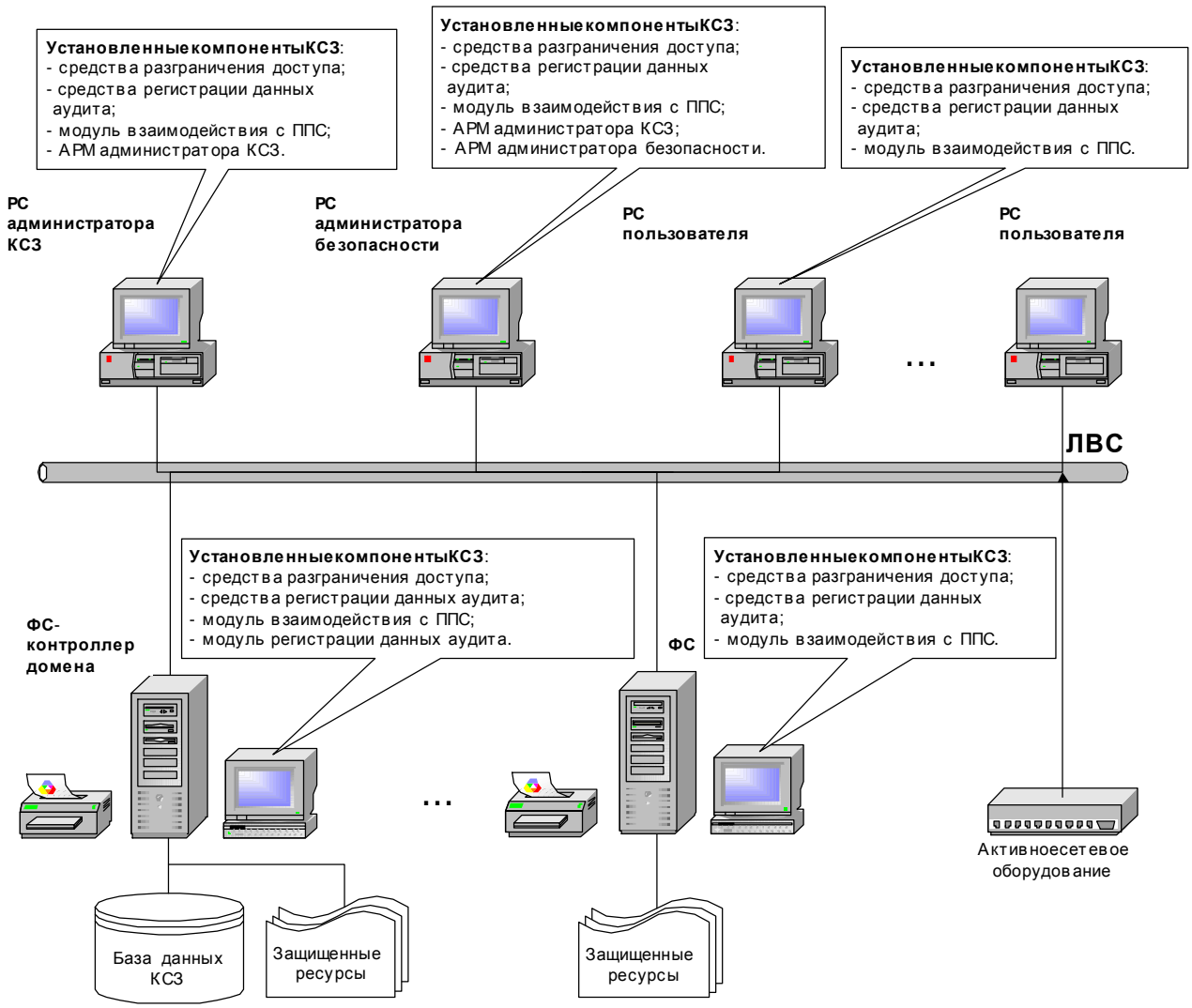

Рисунок 2.1 – *Архитектура КСЗ "Гриф-Мережа"*

3 ОПИСАНИЕ ФУНКЦИЙ КСЗ

3.1 Функции комплекса

КСЗ **«Гриф–Мережа»** реализует следующие функции:

- *идентификацию и аутентификацию пользователей* на основании имени, пароля и носителя данных аутентификации (Flash Drive, CD-RW, DVD-RW, дискеты, другого съемного файлового носителя или устройства Touch Memory) при загрузке ОС РС до загрузки каких-либо программных средств с дисков, что позволяет заблокировать использование РС посторонним лицом, а также опознать конкретного легального пользователя и в дальнейшем реагировать на запросы этого пользователя в соответствии с его полномочиями;
- *возможность блокировки устройств интерфейса пользователя* (клавиатуры, мыши, монитора) на время его отсутствия;
- *контроль целостности и самотестирование КСЗ* при старте и по запросу администратора, что позволяет обеспечить устойчивое функционирование КСЗ и не допустить обработку ИсОД в случае нарушения его работоспособности;
- *разграничение обязанностей пользователей* и выделение нескольких ролей администраторов, которые могут выполнять различные функции по администрированию (регистрацию защищаемых ресурсов, регистрацию пользователей, назначение прав доступа, обработку протоколов аудита и т.п.).
- *разграничение доступа пользователей к выбранным каталогам*, размещенным на РС и ФС ЛВС, и находящимся в них файлам, что позволяет организовать одновременную совместную работу нескольких пользователей ЛВС, имеющих разные служебные обязанности и права по доступу к ИсОД;
- *управление потоками информации* и блокировку потоков информации, приводящих к снижению ее уровня конфиденциальности;
- *контроль за выводом информации на печать* с возможностью маркирования печатных листов выводимых документов (в формате "Office Open XML") согласно требований действующих нормативных документов в области охраны государственной тайны;
- *контроль за экспортом информации на съемные носители* с возможностью ограничения перечня используемых съемных носителей;
- *контроль за импортом информации* со съемных носителей;
- *гарантированное удаление остаточной информации* путем затирания содержимого файлов, содержащих ИсОД, при их удалении;
- *разграничение доступа прикладных программ к выбранным каталогам* и находящимся в них файлам, что позволяет обеспечить защиту ИсОД от случайного удаления, модификации и соблюдение технологии ее обработки;
- *контроль целостности прикладного и системного ПО*, а также блокировку загрузки программ, целостность которых нарушена, что позволяет обеспечить защиту от вредоносных программ и соблюдение технологии обработки ИсОД;
- *контроль за использованием дискового пространства ФС пользователями (квоты)*, что исключает возможность блокирования одним из пользователей возможности работы других;
- *восстановление функционирования КСЗ после сбоев*, что гарантирует доступность информации с обеспечением соблюдения правил доступа к ней;

- *непрерывную регистрацию, анализ и обработку критичных для безопасности событий* (фактов входа пользователей в ОС, попыток несанкционированного доступа, фактов запуска программ, фактов работы с ИсОД, фактов вывода на печать, событий, связанных с работой активного сетевого оборудования и т.п.) в специальных протоколах аудита, что позволяет администраторам контролировать доступ к ИсОД, следить за тем, как используется КСЗ, а также правильно его конфигурировать;
- *немедленное оповещение* администратора безопасности обо всех выявленных нарушениях установленных ПРД (в конфигурации с повышенными требованиями к обеспечению наблюдаемости);
- *ведение архива зарегистрированных данных аудита*.

3.2 **Функциональные профили защищенности и уровень гарантии**

В соответствии с НД ТЗИ 2.5–004–99 "Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа" КСЗ **«Гриф–Мережа»** реализует следующие функциональные профили защищенности.

Функциональный профиль защищенности, реализуемый КСЗ в базовой конфигурации:

{ КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-3, НО-2 }

Функциональный профиль защищенности, реализуемый КСЗ в конфигурации с повышенными требованиями к обеспечению наблюдаемости:

{ КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НК-1, НЦ-2, НТ-2, НИ-3, НО-2 }

где

КА-2 – базовая административная конфиденциальность;

КО-1 – повторное использование объектов;

ЦА-2 – базовая административная целостность;

ЦО-1 – ограниченный откат;

ДР-1 – квоты;

ДС-1 – устойчивость при ограниченных отказах;

ДЗ-1 – модернизация;

ДВ-1 – ручное восстановление после сбоев;

НР-2 – защищенный журнал;

НР-5 – анализ в реальном времени;

НИ-3 – множественная идентификация и аутентификация

НК-1 – однонаправленный достоверный канал;

НО-2 – разграничение обязанностей администраторов;

НЦ-2 – КСЗ с гарантированной целостностью;

НТ-2 – самотестирование при старте.

Разработка выполнена в соответствии с требованиями уровня гарантий Г–4, установленными НД ТЗИ 2.5– 004–99.

Реализованный функциональный профиль, политика функциональных услуг безопасности и уровень гарантий соответствуют требованиям НД ТЗИ 2.5-008-2002 «Требования по защите конфиденциальной информации от несанкционированного доступа во время обработки в автоматизированных системах класса 2» при использовании технологии обработки информации, выдвигающей повышенные требования к обеспечению конфиденциальности, целостности и доступности информации и при условии отсутствия необходимости реализации доверительного управления доступом пользователей к информационным объектам.

3.2.1 **Описание политики функциональных услуг безопасности**

КА-2 - базовая административная конфиденциальность

Реализация данной услуги обеспечивает возможность администратору КСЗ управлять потоками информации от защищенных объектов к пользователям.

Политика данной услуги распространяется на:

- пользователей всех категорий;
- защищенные информационные объекты (каталоги и файлы) на дисках РС и ФС ЛВС, которые содержат как ИсОД всех уровней конфиденциальности, так и открытую информацию;
- системные и прикладные ПС, которые предназначены для обработки защищенных объектов (файлов), содержащих ИсОД;
- технологическую информацию КСЗ;
- отдельные виды периферийных устройств (принтеры, накопители на съемных носителях).

Разграничение доступа пользователей к защищенным объектам выполняется на основании атрибутов защищенных объектов, которые характеризуют степень конфиденциальности информации, содержащейся в этих объектах, и атрибутов пользователя, которые характеризуют уровень его полномочий по доступу к информации. Атрибуты доступа защищенных объектов (каталогов и файлов) назначаются при их создании.

Запросы на назначение и изменение прав доступа обрабатываются только в случае, если они поступают от администраторов КСЗ.

КСЗ предоставляет возможность администратору КСЗ для каждого защищенного каталога путем включения (исключения) пользователей в список пользователей, имеющих права доступа к данному каталогу по чтению, определить конкретных пользователей, которые имеют право получать информацию из файлов, содержащихся в защищенном каталоге или запускать программы, исполняемые коды которых в виде файлов хранятся в данном каталоге.

КСЗ реализует управление потоками информации с целью запрета потоков, которые приводят к снижению уровня конфиденциальности информации, путем блокировки копирования и перемещения (переименования) файлов из каталогов с более высоким

уровнем конфиденциальности в каталоги с более низким уровнем конфиденциальности, а также запрета возможности использования системного буфера обмена (clipboard) ОС для переноса данных из файлов с более высоким уровнем конфиденциальности в файлы с более низким уровнем конфиденциальности.

КСЗ предоставляет возможность администратору КСЗ предоставлять/ отменять пользователям полномочия импорта/ экспорта ИсОД с использованием съемных носителей и права вывода информации на печать. Кроме непосредственного управления доступом пользователей к устройствам импорта/ экспорта и устройствам печати в соответствии с предоставленными полномочиями, КСЗ, с целью повышения достоверности регистрации фактов выполнения операций экспорта и печати, запрещает экспорт информации и печать с использованием произвольных приложений, разрешая выполнять данные операции только с использованием:

- модуля контроля операций экспорта данных и модуля контроля операций печати, входящих в состав КСЗ;
- специально зарегистрированных программ.

КО-1 - повторное использование объектов

Реализация данной услуги обеспечивает корректность повторного использования разделяемых объектов, гарантируя, что в случае, если разделяемый объект выделяется новому пользователю или процессу, в нем не содержится информация, которая осталась после использования его предшествующим пользователем или процессом.

Политика данной услуги распространяется на:

- сегменты ОП РС и ФС ЛВС;
- носители информации (жесткие диски) РС и ФС, используемые системными и функциональными ПС при обработке ИсОД;
- технологическую информацию КСЗ (учетные записи пользователей).

Относительно сегментов ОП РС и ФС данная услуга реализуется путем очистки содержимого объекта перед выделением его другому пользователю или процессу.

Относительно носителей информации (жестких дисков) данная услуга реализуется путем очистки дискового пространства, занимаемого файлом с ИсОД, сразу после удаления соответствующего файла.

При реализации данной услуги относительно учетных записей пользователей обеспечена невозможность наследования новым пользователем с псевдонимом, который совпадает с псевдонимом ранее удаленного пользователя, назначенных удаленному пользователю прав.

ЦА-2 - базовая административная целостность

Реализация данной услуги обеспечивает возможность администратору КСЗ управлять потоками информации от пользователей к защищенным объектам.

Политика данной услуги распространяется на:

- пользователей всех категорий;
- защищенные информационные объекты (каталоги и файлы) на дисках РС и ФС ЛВС, которые содержат ИсОД всех уровней конфиденциальности;

- системные и функциональные ПС, которые предназначены для обработки защищенных объектов (файлов), содержащих ИсОД;
- технологическую информацию КСЗ.

Разграничение доступа пользователей с использованием соответствующих процессов к защищенным объектам выполняется на основании атрибутов защищенных объектов и процессов, которые характеризуют их принадлежность к одной и той же ТС, под которой понимается определенная именованная совокупность защищенных объектов и процессов (программ), с использованием которых разрешено осуществление модификации этих защищенных объектов, а также атрибутов пользователя, которые характеризуют уровень его полномочий по модификации информации. Атрибуты доступа защищенных объектов (каталогов и файлов) назначаются при их создании.

Запросы на назначение и изменение прав доступа обрабатываются только в случае, если они поступают от администраторов КСЗ.

КСЗ предоставляет возможность администратору КСЗ для каждого защищенного каталога путем включения (исключения) пользователей в список пользователей, имеющих права доступа к данному каталогу по записи, определить конкретных пользователей, которые имеют право модифицировать информацию в файлах, содержащихся в защищенном каталоге, или удалять файлы.

КСЗ предоставляет возможность администратору КСЗ путем включения защищенных каталогов и каталогов, содержащих исполняемые модули программ, в одну и ту же ТС, определять процессы, только с использованием которых разрешено создание, изменение или удаление файлов в защищенном каталоге.

ЦО-1 - ограниченный откат

Реализация данной услуги обеспечивает возможность отмены последовательности определенных операций и возвращения (отката) защищенного объекта в предыдущее состояние.

Политика данной услуги распространяется на технологическую информацию КСЗ и на последовательность операций, выполняемых КСЗ при установке защиты на каталог.

КСЗ обеспечивает возможность автоматизированного осуществления отката БД технологической информации КСЗ в предшествующее состояние, если в процессе выполнения последовательности операций, связанных с установкой защиты на каталог, возникли сбои и данная последовательность операций не была полностью завершена.

ДР-1 - квоты

Реализация данной услуги обеспечивает предотвращение захвата пользователями чрезмерного объема ресурсов.

Политика данной услуги распространяется на:

- пользователей всех категорий;
- защищенные информационные объекты (файлы) в каталогах, размещенных на ФС ЛВС, которые содержат ИсОД всех уровней конфиденциальности;

КСЗ предоставляет администраторам КСЗ средства для управления максимально допустимым размером дискового пространства для одного пользователя на любом из дисков

ФС, а также задания предельного значения размера занятого пользователем дискового пространства.

При превышении пользователем предельного значения генерируется соответствующая запись в протоколе аудита, попытки выделения пользователю дискового пространства свыше квоты блокируются.

Запросы на изменение значений дисковых квот обрабатываются только в том случае, если они поступают от администраторов КСЗ.

ДС-1 - устойчивость при ограниченных отказах

Реализация данной услуги обеспечивает возможность использования отдельных функций КСЗ после отказа его компонента (с ухудшением характеристик обслуживания).

Политика данной услуги распространяется на компоненты КСЗ, реализующие уровень НР-5 (анализ в реальном времени) услуги "Регистрация" (агент модуля регистрации данных аудита, модуль регистрации данных аудита, модуль обработки и анализа данных аудита).

При возникновении любых отказов компонентов КСЗ, реализующих услугу "Регистрация", КСЗ в состоянии продолжать функционирование со снижением уровня услуги до НР-2 (защищенный журнал).

ДЗ-1 - модернизация

Реализация данной услуги обеспечивает возможность использования КСЗ после замены отдельных его компонентов.

Политика данной услуги распространяется на:

- ПС КСЗ;
- технологическую информацию КСЗ.

Системному администратору КСЗ с использованием специальных ПС предоставлена возможность выполнения модернизации (upgrade) ПС КСЗ. Модернизация ПС КСЗ не приводит к необходимости повторной инсталляции ПС КЗЗ или повторной настройки КСЗ.

ДВ-1 - ручное восстановление

Реализация данной услуги обеспечивает возвращение КСЗ в известное защищенное состояние после отказа или прерывания обслуживания.

Политика данной услуги распространяется на:

- ПС КСЗ;
- технологическую информацию КСЗ.

При реализации данной услуги в случае отказа ПС КСЗ или нарушения целостности БД технологической информации КСЗ переводится в состояние, в котором запрещена обработка ИсОД. Возвратить КСЗ к нормальному функционированию может только системный администратор КСЗ.

Системному администратору КСЗ с использованием специальных ПС предоставлена возможность восстановления работоспособности ПС КСЗ (из эталонной копии), а также восстановления корректности содержимого БД технологической информации КСЗ.

НР-2 – защищенный журнал

Реализация данной услуги обеспечивает возможность контроля опасных для КСЗ и системы в целом событий.

Политика данной услуги распространяется на:

- пользователей всех категорий;
- защищенные информационные объекты (каталоги и файлы), которые содержат ИсОД всех уровней конфиденциальности;
- системные и функциональные ПС, предназначенные как для обработки защищенных объектов, которые содержат ИсОД, так и объектов, содержащих открытую информацию;
- ПС КСЗ;
- технологическую информацию КСЗ.

Средства КСЗ обеспечивают регистрацию в соответствующих протоколах, анализ и обработку в отложенном режиме таких событий, имеющих прямое отношение к безопасности:

- вход пользователя в ОС и завершение работы пользователя (выход);
- запуск АРМ администратора КСЗ;
- изменение состояния БД технологической информации и ПС КСЗ:
- регистрация, удаление пользователей;
- регистрация, удаление защищенных ресурсов (установка/ снятие защиты на каталог);
- факты назначения/ изменения прав доступа пользователей к защищенным ресурсам;
- факты доступа пользователей к защищенным каталогам и файлам;
- факты вывода файлов с ИсОД на печать;
- факты экспорта файлов с ИсОД на съемные носители;
- факты импорта файлов с ИсОД со съемных носителей;
- факты нарушения прав доступа пользователей к защищенным ресурсам;
- факты перезагрузки, выключения РС и ФС и возникновения других системные события;
- событий, связанные с наблюдением за процессами (запуск, завершение).

В каждой записи протокола аудита фиксируется дата и время события, тип и атрибуты операции, атрибуты процесса и пользователя, инициировавших событие, признак успешности завершения операции, в случае отказа – причина, а также другая информация.

Средствами КСЗ обеспечена защита протоколов регистрации от несанкционированного доступа (ознакомления, модификации или разрушения), а также возможность анализа протоколов уполномоченными администраторами.

НР-5 - анализ в реальном времени

Реализация данной услуги обеспечивает возможность контроля опасных для КСЗ и системы в целом событий.

Политика данной услуги распространяется на:

- пользователей всех категорий;
- защищенные информационные объекты (каталоги и файлы), которые содержат ИсОД всех уровней конфиденциальности;
- системные и функциональные ПС, предназначенные как для обработки защищенных объектов, которые содержат ИсОД, так и объектов, содержащих открытую информацию;
- ПС КСЗ;
- технологическую информацию КСЗ.

Средства КСЗ обеспечивают регистрацию в соответствующих протоколах, анализ и обработку в реальном времени таких событий, имеющих прямое или косвенное отношение к безопасности:

- вход пользователя в ОС и завершение работы пользователя (выход);
- запуск АРМ администратора КСЗ;
- запуск АРМ администратора безопасности;
- изменение состояния БД технологической информации и ПС КСЗ:
- регистрация, удаление пользователей;
- регистрация, удаление защищенных ресурсов (установка/ снятие защиты на каталог);
- факты назначения/ изменения прав доступа пользователей к защищенным ресурсам;
- факты доступа пользователей к защищенным каталогам и файлам;
- факты вывода файлов с ИсОД на печать;
- факты экспорта файлов с ИсОД на съемные носители;
- факты импорта файлов с ИсОД со съемных носителей;
- факты нарушения прав доступа пользователей к защищенным ресурсам;
- факты перезагрузки, выключения РС и ФС и возникновения другие системные события;
- событий, связанные с наблюдением за процессами (запуск, завершение);
- событий, связанные с функционированием активного сетевого оборудования.

В каждой записи протокола аудита фиксируется дата и время события, тип и атрибуты операции, атрибуты процесса и пользователя, инициировавших событие, признак успешности завершения операции, в случае отказа – причина, а также другая информация.

Средствами КСЗ обеспечена защита протоколов регистрации от несанкционированного доступа (ознакомления, модификации или разрушения), а также возможность анализа протоколов уполномоченными администраторами.

Средства КСЗ обеспечивают возможность контроля единичных или повторяющихся регистрационных событий, свидетельствующих о прямых нарушениях ПБ информации, обрабатываемой в ЛВС, и немедленного информирования администратора безопасности о превышении установленных порогов безопасности. В составе КСЗ реализованы средства, позволяющие администратору безопасности осуществить неразрушительные действия по прекращению повторения этих событий (путем блокировки учетной записи соответствующего пользователя).

С целью исключения возможности потери информации аудита при сбоях средствами КСЗ реализуется возможность сохранения локальных данных аудита в виде соответствующих протоколов непосредственно на ФС или РС, на которых были

зарегистрированы соответствующие события. В составе КСЗ реализованы средства, позволяющие администратору безопасности осуществлять просмотр и анализ сохраненных протоколов аудита.

НИ-3 - множественная идентификация и аутентификация

Политика данной услуги распространяется на пользователей всех категорий, которые пытаются получить доступ к:

- средствам КСЗ;
- защищенным информационным объектам (каталогам и файлам), которые содержат ИсОД всех уровней конфиденциальности;
- системным и функциональным ПС, предназначенным как для обработки защищенных объектов, которые содержат ИсОД, так и объектов, содержащих открытую информацию;
- периферийному оборудованию, задействованному в обработке ИсОД;
- технологической информации КСЗ.

Услуга реализована путем идентификации пользователей на основании введенного псевдонима и аутентификации по установленному протоколу на основании предъявленного носителя с данными аутентификации и введенного пароля.

Данные аутентификации защищены от несанкционированного доступа, модификации или разрушения с использованием тех же механизмов, что и при реализации услуг КА-2, ЦА-2. С этой целью в КСЗ реализована встроенная ТС КСЗ, в которую включены ПС КСЗ и файлы БД технологической информации КСЗ.

НК-1 - однонаправленный достоверный канал

Реализация данной услуги гарантирует пользователям всех категорий возможность непосредственного взаимодействия с КСЗ в процессе выполнения их идентификации и аутентификации.

Политика данной услуги распространяется на:

- пользователей всех категорий;
- ПС КСЗ.

Достоверный канал реализуется в компонентах КСЗ, через которые осуществляется взаимодействие с пользователем в процессе его идентификации и аутентификации. Связь с использованием данного канала инициируется пользователем непосредственно перед выполнением ввода данных аутентификации при входе в ОС.

НО-2 - разграничение обязанностей администраторов

Реализация данной услуги обеспечивает возможность разграничения полномочий пользователей путем определения категорий пользователей с определенными для каждой категории функциями (ролями).

Политика данной услуги распространяется на пользователей всех категорий и определяет такие роли:

- системный администратор КСЗ;
- администраторы КСЗ;

- администраторы безопасности;
- пользователи.

Пользователь, который устанавливает КСЗ, является Системным администратором КСЗ. Учетная запись Системного администратора КСЗ не может быть удалена или отключена. В обязанности Системного администратора входит инсталляция и начальная инициализация КСЗ, обновление при необходимости ПС КСЗ, восстановление при необходимости целостности ПС и БД КСЗ, восстановление при необходимости работоспособности ОС, установка и настройка дополнительных прикладных ПС. В процессе штатного функционирования КСЗ учетная запись Системного администратора КСЗ не используется.

В обязанности администраторов КСЗ, которых может быть несколько, входит управление пользователями, защищенными ресурсами и правами доступа к ним. За каждым администратором КСЗ могут быть закреплены полномочия на выполнение различных функций администрирования, при этом на действия администраторов КСЗ накладываются ограничения:

- администраторы КСЗ могут назначать права доступа к защищенным каталогам только другим пользователям, но не себе;
- администраторы КСЗ не могут менять свои административные полномочия;
- изменения атрибутов других администраторов КСЗ (прав доступа и административных полномочий) и пользователей (прав доступа) вступают в силу только после санкции (подтверждения) сделанных изменений администратором безопасности.

В обязанности администраторов безопасности входит контроль за соблюдением правил доступа к ИсОД путем контроля установленных прав доступа, управления правилами аудита и анализа зарегистрированных данных аудита. Только администратор безопасности может активизировать учетные записи других администраторов и пользователей после изменения их атрибутов.

Пользователь, успешно прошедший идентификацию и аутентификацию и не назначенный КСЗ на роль Системного администратора КСЗ, администратора КСЗ или администратора безопасности, назначается на роль обычного пользователя. Обычному пользователю могут быть предоставлены права доступа к защищенным информационным объектам (каталогам и файлам), которые содержат ИсОД, полномочия печати, импорта/ экспорта информации.

НЦ-2 - КСЗ с гарантированной целостностью

Реализация данной услуги обеспечивает КСЗ возможность защищать себя от внешних воздействий и гарантировать свою способность управлять защищенными объектами.

Политика данной услуги распространяется на:

- ПС КСЗ;
- системные и прикладные ПС, предназначенные как для обработки защищенных объектов, которые содержат ИсОД, так и объектов, содержащих открытую информацию;
- технологическую информацию КСЗ.

С целью защиты от внешних воздействий КСЗ определяет и поддерживает собственный домен исполнения, отличный от доменов всех других процессов, и реализует механизмы разграничения доменов.

В собственном домене КСЗ обеспечивает защиту от несанкционированной модификации средств КСЗ, реализующих механизмы КСЗ, и/ или потери управления КЗЗ, а также от НСД к технологической информацию КСЗ с использованием тех же механизмов, что и при реализации услуг КА-2, ЦА-2. С этой целью в КСЗ реализована встроенная ТС КСЗ, в которую включены ПС КСЗ и файлы БД технологической информации КСЗ.

Дополнительно к выделению домена КСЗ, реализован контроль целостности ПС КСЗ и БД технологической информации КСЗ при старте и по запросу администратора КСЗ.

В случае выявления нарушения целостности ПС КСЗ или нарушения целостности БД технологической информации КСЗ переводится в состояние, в котором запрещена обработка ИсОД. Возвратить КСЗ к нормальному функционированию может только Системный администратор КСЗ.

Системному администратору КСЗ с использованием специальных ПС предоставлена возможность восстановления работоспособности ПС КСЗ (из эталонной копии), а также восстановления корректности содержимого БД технологической информации КСЗ.

Дополнительно в рамках политики данной услуги в КСЗ реализован контроль целостности всех системных и функциональных ПС при старте, что обеспечивает:

- исключение попыток поиска и использования уязвимостей КСЗ и ОС;
- невозможность доступа к ресурсам с использованием недокументированных интерфейсов и непосредственного обращения к функциональным уровням ОС, на которых базируется КСЗ;
- исключение возможности внедрения программных закладок и реализации скрытых каналов;
- соблюдение установленной технологии обработки ИсОД.

НТ-2 - самотестирование при старте

Реализация данной услуги обеспечивает КСЗ возможность проверить и на основе этого гарантировать правильность функционирования и целостность определенного множества своих функций.

Политика данной услуги распространяется на:

- ПС КСЗ;
- технологическую информацию КСЗ.

При старте и по запросу администратора КСЗ выполняет набор тестов с целью оценки правильности функционирование своих критических функций (путем проверки целостности соответствующих ПС и БД технологической информации КСЗ).

В случае неуспешного выполнения тестов (выявления нарушения целостности ПС КСЗ или нарушения целостности БД технологической информации) КСЗ переводится в состояние, в котором запрещена обработка ИсОД. Возвратить КСЗ к нормальному функционированию может только Системный администратор КСЗ.

Системному администратору КСЗ с использованием специальных ПС предоставлена возможность восстановления работоспособности ПС КСЗ (из эталонной копии), а также восстановления корректности содержимого БД технологической информации КСЗ.

3.3 **Описание реализованных функций КСЗ**

3.3.1 **Идентификация и аутентификация пользователей**

Прежде чем осуществлять разграничения доступа, КСЗ должен опознать пользователя и блокировать доступ неавторизованных пользователей. Для этого при входе пользователя в систему выполняется его идентификация (опознание) и аутентификация (проверка результатов идентификации).

Идентификация пользователя выполняется на основании вводимого им с клавиатуры имени (псевдонима). Аутентификация пользователя выполняется на основании вводимого с клавиатуры пароля и предъявляемого носителя данных аутентификации. В качестве носителя данных аутентификации может выступать перезаписываемый съемный файловый носитель любого типа (дискета, Flash Drive, CD-RW/DVD-RW и т.п.) или устройство Touch Memory. Таким образом, реализуется аутентификация пользователя с использованием механизмов, функционирующих на основе двух различных принципов: "владею чем-то" – носитель данных аутентификации и "знаю что-то" – пароль (множественная идентификация и аутентификация).

В случае, если предоставленная пользователем информация аутентификации не соответствует эталону, хранящемуся в БД КСЗ, доступ пользователя в ОС блокируется.

Кроме того, КСЗ выполняет контроль за истечением срока действия полномочий пользователя и его пароля, а также за соответствием дня недели и временного интервала, в течение которого пользователь осуществляет вход в ОС, тем, которые заданы администратором.

Важной особенностью является то, что идентификация и аутентификация пользователя осуществляется с использованием достоверного канала. При этом никакая посторонняя программа не может перехватить информацию аутентификации, которую вводит пользователь.

3.3.2 **Возможность блокировки устройств интерфейса пользователя**

Идентификация и аутентификация пользователя выполняется не только при входе в ОС, но и после имевшей место блокировки устройств интерфейса пользователя (клавиатуры, мыши и монитора). Блокировка устройств интерфейса может осуществляется пользователем, например, в случае необходимости покинуть на время рабочее место. Для разблокирования устройств интерфейса пользователю необходимо предъявить свой носитель данных аутентификации и ввести пароль.

3.3.3 **Контроль целостности и самотестирование КСЗ**

Контроль целостности КСЗ выполняется путем проверки целостности ПС КСЗ при каждой загрузке ОС. Кроме того, данная операция может выполняться по желанию администратора КСЗ с использованием АРМ администратора КСЗ. При этом может быть выполнена проверка как ПС КСЗ, размещенных на той РС, на которой установлен АРМ администратора КСЗ, так и ПС КСЗ размещенных на любой другой РС ЛВС или на любом другом ФС ЛВС. В случае обнаружения нарушения целостности пользователю, выполняющему проверку (или вход в ОС), выдается соответствующее сообщение.

Восстановление целостности ПС КСЗ может быть выполнено Системным администратором КСЗ при помощи специальных программных средств, входящих в состав КСЗ.

3.3.4 **Разграничение обязанностей пользователей**

Любая ПБ кроме ПРД устанавливает правила управления средствами защиты. Функции управления возлагаются на доверенных лиц, которые несут ответственность за безопасность обработки информации в системе. Для компьютерных систем лиц, за которыми закреплены права на выполнение определенных функций управления, принято называть администраторами.

В соответствии с ПБ, реализуемой КСЗ, функции администратора могут быть доступны конкретному пользователю на основании его членства в определенной группе и/ или конкретных привилегий, которые закреплены за данным пользователем и записаны в его учетной записи.

В соответствии с ПБ, реализуемой КСЗ **«Гриф–Мережа»**, все администраторы делятся на:

- Системного администратора КСЗ, выполняющего установку и настройку КСЗ;
- администраторов КСЗ, выполняющих управление средствами КСЗ, защищенными информационными ресурсами и правами доступа пользователей к защищенным ресурсам;
- администраторов безопасности, контролирующих действия администраторов КСЗ и пользователей и соблюдение ими требований установленной ПБ.

Все администраторы включаются в группу администраторов ОС.

Пользователь, который устанавливает КСЗ (учетная запись администратора домена «Администратор»), является Системным администратором КСЗ. Учетная запись Системного администратора КСЗ не может быть удалена. Только Системный администратор КСЗ имеет право на восстановление целостности ПС и БД КСЗ в случае сбоев.

Системный администратор КСЗ **«Гриф–Мережа»** имеет полномочия по работе с данными аудита, зарегистрированными средствами КСЗ. С помощью АРМ анализа локальных данных аудита он может осуществлять анализ информации аудита. Кроме этого, он имеет следующие полномочия:

- управление пользователями (регистрация, удаление неактивизированных учетных записей, модификация атрибутов учетной записи, смена пароля, перегенерация информации аутентификации на носитель, активизация/ деактивации учетных записей сервисов и активизация одного администратора безопасности);
- управление правами доступа пользователей к защищенным каталогам;
- управление правами доступа программ к защищенным каталогам (управление технологическими схемами, см. п.3.3.10);
- управление уровнями конфиденциальности обрабатываемой информации;
- управление учетными записями РС, ФС и квотами дискового пространства на них;
- управление включением/ выключением режима полного контроля запускаемого ПО.

Администратор КСЗ может иметь такие полномочия:

- управление пользователями (регистрация, удаление неактивизированных учетных записей, модификация атрибутов учетной записи, смена пароля, перегенерация информации аутентификации на носитель, активизация/ деактивации учетных записей сервисов);
- управление правами доступа к каталогам со стороны пользователей;
- управление правами доступа к каталогам со стороны программ или технологическими схемами (см. п.3.3.10);
- управление уровнями конфиденциальности;
- управление учетными записями РС, ФС и квотами дискового пространства на них;
- управление включением/ выключением режима полного контроля целостности выполняемого ПО.

Системный администратор КСЗ и администраторы КСЗ могут назначать права доступа к защищенным каталогам только другим пользователям, но не себе. При назначении прав доступа пользователю его учетная запись деактивируется. Назначенные права доступа вступают в силу только после подтверждения администраторами безопасности (путем активизации учетной записи соответствующего пользователя).

Администраторы безопасности имеют полномочия по работе с данными аудита, зарегистрированными средствами КСЗ. С помощью АРМ администратора безопасности они могут менять настройки аудита КСЗ, осуществлять анализ информации аудита, получать в реальном режиме времени оповещения о нарушении установленной ПБ. Кроме этого, администраторы безопасности имеют полномочия на управление пользователями (активизация/ деактивация учетных записей пользователей и сервисов).

3.3.5 **Разграничение доступа пользователей к каталогам**

В соответствии с ПБ, реализуемой КСЗ, защищаемыми объектами являются каталоги жестких дисков РС и ФС ЛВС и находящиеся в них файлы. Разграничение доступа пользователей к каталогам и находящимся в них файлам реализовано в соответствии с принципами административного управления доступом. При этом все разделы всех жестких дисков РС и ФС ЛВС должны быть разделами с файловой системой NTFS.

При регистрации защищенного каталога администратор КСЗ указывает его уровень конфиденциальности, который впоследствии не может быть изменен. Незарегистрированные как защищенные каталоги считаются по умолчанию открытыми (не имеющими уровня конфиденциальности) и доступ к ним разрешается всем пользователям.

Для каждого защищенного каталога администратор КСЗ может создать список доступа, в котором перечислены пользователи, имеющие права доступа к данному каталогу и находящимся в нем (и его подкаталогах) файлам, а также разрешенные для этих пользователей типы доступа (только чтение, чтение и запись).

Пользователь потенциально может получить доступ к каталогу, если его уровень допуска (также задаваемый администратором КСЗ при регистрации пользователя) не ниже, чем уровень конфиденциальности соответствующего каталога.

По умолчанию в КСЗ введены следующие уровни конфиденциальности информации и уровни допуска пользователей:

- «КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ»;
- «ДСП»;

- «СЕКРЕТНО»;
- «СОВ.СЕКРЕТНО»;
- «ОСОБОЙ ВАЖНОСТИ».

Кроме того, администратор КСЗ может создать до 29 произвольных уровней конфиденциальности между уровнями «КОНФИДЕНЦИАЛЬНО» и «ДСП».

Каждому пользователю, который имеет соответствующий уровень допуска, администратор КСЗ может предоставить доступ к защищенному каталогу по чтению или по чтению и записи.

Пользователи имеют только те права доступа к защищенным каталогам, а значит и к находящимся в них файлам с ИсОД, которые явно определены администратором КСЗ. Защита распространяется на всю ветвь дерева, начиная с указанного в БД КСЗ защищенного каталога, включая его подкаталоги. Поэтому не допускается указывать в качестве нового защищенного каталог, который является подкаталогом уже защищенного каталога. КСЗ запрещает выполнять переименование и удаление защищенного каталога и тех каталогов, которые его содержат, вплоть до находящегося в корне диска.

Доступ по записи к каталогам КСЗ разрешен только ПС КСЗ (АРМ администратора КСЗ). Доступ по записи к каталогам ОС разрешен только администраторам.

При попытке пользователя получить запрещенный вид доступа (например, удалить файл в каталоге, к которому разрешен доступ только по чтению) попытка доступа блокируется и в протоколе аудита регистрируется факт НСД.

3.3.6 **Управление потоками информации**

КСЗ поддерживает возможность управления потоками информации, которое заключается в том, что КСЗ следит за тем, чтобы процессы, у которых есть открытые для чтения файлы, находящиеся в защищенных каталогах, не могли открыть для записи файлы, находящиеся в незащищенных (открытых или общих) каталогах или каталогах с меньшим уровнем конфиденциальности. Это, в частности, позволяет блокировать копирование файлов из защищенных каталогов в незащищенные или из каталогов с более высоким уровнем конфиденциальности в каталоги с меньшим уровнем, что позволяет избежать случайного или преднамеренного снижения уровня конфиденциальности информации.

Кроме этого, КСЗ позволяет заблокировать возможность переноса данных с использованием системного буфера обмена ОС (Clipboard) из файлов с более высоким уровнем конфиденциальности в файлы с более низким уровнем конфиденциальности.

3.3.7 **Контроль за выводом информации на печать**

Администраторы КСЗ имеют возможность явным образом указать, кому из пользователей разрешен вывод информации на печать. Все факты вывода информации на принтер фиксируются в протоколах аудита (с указанием имени выводимого на печать файла и имени используемого принтера). При этом, вывод на печать может осуществляться только с использованием специальной программы, входящей в состав КСЗ, а также специально зарегистрированных администратором КСЗ программ.

3.3.8 **Контроль за импортом/ экспортом информации с использованием съемных носителей**

Все съемные носители (жесткие диски, подключаемые через USB-интерфейс, дискеты, Flash Drive, CD-ROM, DVD-ROM и т.п.), установленные на РС и ФС ЛВС, рассматриваются КСЗ как устройства импорта/ экспорта. Доступ к этим устройствам имеют только те пользователи, которым администраторами КСЗ разрешено выполнять операции экспорта информации на съемные носители или импорта информации с них. Все факты импорта/ экспорта информации (с указанием имени файла и типа используемого устройства) фиксируются в протоколах аудита. При этом, экспорт данных на съемные носители может осуществляться только с использованием специальной программы, входящей в состав КСЗ, а также специально зарегистрированных администратором КСЗ программ.

3.3.9 **Гарантированное удаление остаточной информации**

В КСЗ реализовано гарантированное удаление остаточной информации при удалении файлов, содержащих ИсОД. Дополнительно к реализуемой ОС функции очистки дискового пространства перед его выделением для размещения нового файла реализована функция очистки занимаемого файлом дискового пространства непосредственно при удалении файла, находящегося в защищенном каталоге (так называемый wiping). Затирание данных реализовано путем записи поверх этих данных последовательности нулевых байт. Реализация данной функции препятствует проведению атак типа "сбор мусора".

3.3.10 **Разграничение доступа прикладных программ к каталогам**

В КСЗ реализовано разграничение доступа к защищенным каталогам и находящимся в них файлам со стороны создаваемых пользователем процессов, что позволяет обеспечить защиту ИсОД от случайного удаления или модификации и соблюсти технологию ее обработки.

Данная функция реализуется путем создания ТС. ТС представляет собой именованную совокупность защищенных каталогов, содержащих файлы данных, и каталогов, содержащих файлы программ, с использованием которых разрешена модификация этих данных. Если каталог входит в ТС, то, даже если пользователь имеет право доступа к данному каталогу, он сможет осуществить доступ к данным только с помощью определенных, включенных в ТС программ. В одну ТС могут включаться каталоги, размещенные как на одной, так и на разных РС ЛВС, один и тот же каталог может входить в несколько ТС.

С использованием данного механизма ограничивается также доступ к каталогу КСЗ и настройкам реестра, влияющим на безопасность. Доступ к ним по записи могут получить только администраторы КСЗ и только с использованием АРМ администратора КСЗ, который в свою очередь, позволяет выполнять операции только при наличии у администратора КСЗ соответствующих полномочий и в соответствии с установленными правилами.

3.3.11 **Контроль целостности прикладного и системного программного обеспечения**

Реализация контроля целостности прикладного и системного ПО в КСЗ **«Гриф–Мережа»** преследует сразу несколько целей:

- во-первых, это препятствует распространению вирусов, а значит нарушению целостности ОС, КСЗ и обрабатываемой информации;

- во-вторых, это позволяет избежать утечки информации за счет использования скрытых каналов, нарушения установленной технологии обработки информации, а также других действий, связанных с внедрением вредоносных программ (закладок, "троянских коней" и т.п.);
- в-третьих, это позволяет создать условия, когда в системе работает только проверенное ПО, не выполняющее никаких действий, которые могли бы привести к отключению или преодолению средств защиты, что позволяет выполнить требования более высоких уровней услуги "целостность КСЗ".

Контроль целостности ПО заключается в проверке целостности исполняемых модулей при их загрузке с использованием заранее рассчитанных кодов контроля целостности. Загрузка модулей, целостность которых нарушена, блокируется.

3.3.12 **Контроль за использованием дискового пространства**

КСЗ поддерживает возможность квотирования ресурсов и позволяет реализовать контроль за использованием дискового пространства ФС и РС ЛВС пользователями. Администратор имеет возможность для каждого логического диска на любой РС или любом ФС указать, какой максимальный объем дискового пространства может использовать каждый пользователь. Использование данной функции позволяет исключить возможность блокирования одним из пользователей ЛВС возможности работы других.

3.3.13 **Восстановление функционирования КСЗ после сбоев**

В случае обнаружения в процессе самотестирования при старте нарушения работоспособности КСЗ, целостности ПС или БД КСЗ пользователю выдается соответствующее сообщение и дальнейшая работа блокируется. В такой ситуации необходимо вмешательство Системного администратора КСЗ, который имеет возможность (с использованием соответствующих ПС) восстановить целостность средств КСЗ на РС или на ФС (из эталонной копии) или БД КСЗ из резервной копии.

Администратор КСЗ при работе с АРМ администратора КСЗ имеет возможность выполнять откат неудачно завершившихся операций по установке защиты на каталог.

3.3.14 **Непрерывная регистрация, анализ и обработка событий**

Средства КСЗ обеспечивают регистрацию таких событий, имеющих прямое или косвенное отношение к безопасности:

- вход пользователя в ОС и завершение работы пользователя (выход);
- запуск АРМ администратора КСЗ;
- запуск АРМ администратора безопасности;
- изменение состояния БД и ПС КСЗ:
- регистрация, удаление пользователей;
- регистрация, удаление защищенных ресурсов (установка/ снятие защиты на каталог);
- факты назначения/ изменения прав доступа пользователей к защищенным ресурсам;
- факты доступа пользователей к защищенным каталогам и файлам;
- факты вывода файлов с ИсОД на печать;
- факты импорта/ экспорта файлов с ИсОД с использованием съемных носителей;
- факты нарушения прав доступа пользователей к защищенным ресурсам;

- факты перезагрузки, выключения РС и ФС и возникновения других системных событий;
- событий, связанных с наблюдением за процессами (запуск, завершение);
- событий, связанных с функционированием активного сетевого оборудования.

В каждой записи протокола аудита фиксируется дата и время события, тип и атрибуты операции (например, открытие файла для чтения/ записи), атрибуты процесса и пользователя, инициировавших событие, признак успешности завершения операции и, в случае отказа – причина, а также другая информация.

Сбор информации аудита и ее анализ в реальном времени реализуется с использованием входящих в состав КСЗ агентов модуля регистрации данных аудита, функционирующих на РС и ФС ЛВС, а также модуля регистрации данных аудита, функционирующего на ФС-ОКД ЛВС.

Просмотр и анализ протоколов регистрации (в конфигурации с повышенными требованиями к обеспечению наблюдаемости) выполняется с помощью входящего в состав КСЗ АРМ администратора безопасности.

Данные аудита сохраняются в БД КСЗ и могут быть использованы для последующего анализа.

С целью исключения возможности потери информации аудита при сбоях средствами КСЗ реализуется возможность сохранения локальных данных аудита (при помощи модулей сохранения локальных данных аудита) в виде соответствующих протоколов непосредственно на ФС или РС, на которых были зарегистрированы соответствующие события.

В составе КСЗ реализованы средства (АРМ анализа локальных данных аудита), позволяющие администратору безопасности осуществлять просмотр и анализ сохраненных протоколов аудита.

3.3.15 **Немедленное оповещение администратора безопасности о нарушениях установленных ПРД**

Для оперативной реакции на нарушения установленных ПРД в КСЗ **«Гриф–Мережа»** (в конфигурации с повышенными требованиями к обеспечению наблюдаемости) реализована возможность немедленного оповещения администратора безопасности о зарегистрированных фактах таких нарушений. Администратор безопасности с использованием входящего в состав КСЗ АРМ может устанавливать соответствующие правила оповещения. В случае, если возникшее и зарегистрированное в протоколах аудита событие удовлетворяет заданному правилу оповещения, информация о нем немедленно поступает на консоль АРМ администратора безопасности.

3.3.16 **Ведение архива зарегистрированных данных аудита**

С помощью АРМ администратора безопасности (в конфигурации с повышенными требованиями к обеспечению наблюдаемости) или АРМ анализа локальных данных аудита администратор безопасности может создать архивную копию данных аудита и, соответственно, по мере надобности восстановить данные из архивной копии.

4 ВАРИАНТЫ ПРИМЕНЕНИЯ КСЗ

4.1 Применение КСЗ для защиты информации в виде слабосвязанных объектов

При использовании КСЗ **«Гриф–Мережа»** для защиты обрабатываемой в ЛВС с использованием соответствующих ППС информации, представленной в виде слабосвязанных объектов (отдельных файлов), защищаемые ресурсы (каталоги, содержащие файлы с ИсОД) могут быть размещены как на жестких дисках ФС ЛВС, так и на жестких дисках РС ЛВС (рис. 2.1).

Доступ к защищенным каталогам (и, соответственно, сохраняемым в них файлам), должен предоставляться пользователям в соответствии со служебной необходимостью. Если для обработки файлов с ИсОД предполагается использовать ограниченный набор ПС, можно также зарегистрировать данные ПС в качестве технологических программ и создать соответствующие ТС.

4.2 Применение КСЗ для защиты информации в виде сильносвязанных объектов

При использовании КСЗ **«Гриф–Мережа»** для защиты обрабатываемой в ЛВС с использованием соответствующих ППС информации, представленной в виде сильносвязанных объектов, сохраняемых в хранилищах данных (например, таблиц БД), защищаемые ресурсы (каталоги, содержащие файлы с сильносвязанными объектами) должны быть размещены только на жестких дисках ФС ЛВС (рис. 2.1).

Доступ к защищенным каталогам (и, соответственно, сохраняемым в них файлам), должен быть предоставлен только той служебной учетной записи (сервису), под которым функционирует соответствующий сервер СУБД и, в случае необходимости выполнения операций резервного копирования данных, выполняющим эту операцию пользователям. С целью предотвращения возможности модификации файлов, содержащих сильносвязанные объекты, минуя сервер СУБД, должны быть созданы соответствующие ТС, в которые должны быть включены каталоги с ПС сервера СУБД и защищенные каталоги с файлами, содержащими сильносвязанные объекты.

Разграничение доступа к объектам внутри прикладной системы должно реализовываться ее прикладными программными средствами. Для обеспечения надежной непрерывной защиты обрабатываемой ИсОД эти прикладные программные средства должны обеспечивать:

- взаимодействие с КСЗ **«Гриф–Мережа»** (через соответствующий интерфейс, реализуемый интерфейсным модулем взаимодействия с ППС) для получения идентификаторов зарегистрированных пользователей ОС и их атрибутов доступа к ИсОД;
- назначение прав доступа к информационным объектам, обрабатываемым в прикладной системе, в соответствии с полученными идентификаторами и атрибутами доступа пользователей к ИсОД, а также согласно установленным для системы требованиям;
- взаимодействие с КСЗ **«Гриф–Мережа»** (через соответствующий интерфейс, реализуемый интерфейсным модулем взаимодействия с ППС) для получения идентификатора и атрибутов доступа текущего пользователя ОС;

- управление доступом пользователя к информационным объектам, обрабатываемым в прикладной системе, на основании полученных от КСЗ **«Гриф–Мережа»** идентификатора и атрибутов доступа текущего пользователя ОС (в том числе уровня допуска пользователя и уровня конфиденциальности информационного объекта);
- регистрацию всех критичных для безопасности информации событий в протоколах аудита ОС;
- взаимодействие с КСЗ **«Гриф–Мережа»** для получения списка и атрибутов доступа защищенных ресурсов ОС (защищенных каталогов ОС) через соответствующий интерфейс, реализуемый интерфейсным модулем взаимодействия с ППС;
- контроль соответствия атрибутов доступа (уровня конфиденциальности) защищенных информационных объектов, обрабатываемых в прикладной системе, и атрибутов доступа защищенных каталогов ОС при экспорте информационных объектов из хранилища данных прикладной системы в каталоги ОС или импорте информационных объектов из каталогов ОС в хранилище данных прикладной системы.

5 ТРЕБОВАНИЯ К УСЛОВИЯМ ЭКСПЛУАТАЦИИ

В случае, если в ЛВС используются ФС и РС, на которых не установлены средства КСЗ **«Гриф–Мережа»**, путем соответствующего администрирования активного сетевого оборудования (устройств коммутации пакетов) на канальном уровне стека протоколов ЛВС должен быть запрещен доступ с таких ФС и РС к ФС и РС, на которых установлены средства КСЗ **«Гриф–Мережа»**.

Если защищаемые каталоги размещаются на жестких дисках РС ЛВС, соответствующими организационными и/ или техническими мерами (изъятие соответствующих устройств ввода/ вывода; подключение дисковода к контроллеру таким образом, чтобы он опознавался как дисковод, с которого невозможно выполнить загрузку ОС; установка запрета на загрузку со съемных носителей в SETUP BIOS и пароля для доступа к SETUP и т.п.) должна быть заблокирована возможность загрузки ОС со съемных носителей. В случае размещения защищаемых каталогов только на жестких дисках ФС ЛВС в указанных выше мерах по отношению к РС нет необходимости.

Кроме этого, с использованием соответствующих организационных мер (например, механического блокирования доступа к панели управления и клавиатуре) должна быть обеспечена защита ФС-ОКД ЛВС от несанкционированного выключения или перезагрузки.

6 УСЛОВИЯ ПОСТАВКИ

6.1 Комплект поставки

В комплект поставки входит:

- паспорт;
- CD-ROM с программным обеспечением и документацией в электронном виде (описание комплекса, руководство по установке и настройке, руководство по эксплуатации автоматизированного рабочего места администратора КСЗ, руководство по эксплуатации автоматизированного рабочего места администратора безопасности, руководство по эксплуатации автоматизированного рабочего места анализа локальных данных аудита, руководство системного администратора КСЗ, руководство администратора КСЗ, руководство администратора безопасности, руководство пользователя, руководство программиста) – 1 шт;
- упаковка – 1 шт.

6.2 Совместимость

Программные средства КСЗ **«Гриф–Мережа»** предназначены для работы в ЛВС, организованной в виде единого домена Windows 2003, Windows 2008 или Windows 2012, состоящего из одного ФС-ОКД, функционирующего под управлением ОС MS Windows 2003 Server, MS Windows 2008 Server, MS Windows 2008 Server R2, MS Windows 2012 Server или MS Windows 2012 Server R2 с установленной службой Active Directory и включенных в этот домен ФС и РС, функционирующих под управлением ОС MS Windows XP Professional/ MS Windows Vista/ MS Windows 7 (в т.ч. 64-разрядных)/ MS Windows 8/8.1 (в т.ч. 64-разрядных).

Программные средства КСЗ **«Гриф–Мережа»** версии 3 совместимы со средствами, входящими в комплект поставки данных ОС, а также с другим системным, инструментальным и прикладным ПО, использующим стандартные интерфейсы данных ОС.

Программные средства КСЗ могут быть не совместимы (т.е., функционировать некорректно или не в полном объеме) с другими средствами защиты от НСД, антивирусным ПО и ПО, работающим с дисками и файлами на низком уровне в обход файловой системы.

После установки КСЗ **«Гриф–Мережа»** может быть ограничена возможность обновления ПО ОС и использования штатных средств сохранения/ восстановления системных данных ОС.

6.3 Гарантийные обязательства

Гарантийные обязательства Разработчика приведены в Паспорте на КСЗ «Гриф-Мережа». Дополнительная взаимная ответственность Заказчика и Разработчика может быть определена на договорных условиях.