Комплекс средств защиты информации от несанкционированного доступа

«Гриф» версии 3

Описание комплекса

редакция 11

Киев 2016

Список используемых сокращений

АРМ – автоматизированное рабочее место

АС – автоматизированная система

БД – база данных

ИсОД – информация с ограниченным доступом

ККЦ – код контроля целостности

КСЗ – комплекс средств защиты

КСЗИ – комплексная система защиты информации

НСД – несанкционированный доступ

ОП – оперативная память

ОС – операционная система

ПБ – политика безопасности

ПО – программное обеспечение

ППС – прикладная программная система

ПС – программные средства

ПЭВМ – персональная электронная вычислительная машина

РС – рабочая станция

ТС – технологическая схема

ИНСТИТУТ
КОМПЬЮТЕРНЫХ
ТЕХНОЛОГИЙ

пр-т Воздухофлотский,54 , Киев-151,
Украина, 03151
E-mail: ict@ict.com.ua
http://www.ict.com.ua

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Комплекс средств защиты (КСЗ) информации от несанкционированного доступа (НСД) **«Гриф»** версии 3 (далее - комплекс **«Гриф»**) предназначен для обеспечения защиты информации с ограниченным доступом (ИсОД) (включая информацию составляющую государственную тайну, служебную информацию, конфиденциальную информацию о личности (персональные данные), информацию, составляющую коммерческую тайну, и т.д.) при ее обработке в автоматизированных системах (АС) класса «1», которые строятся на базе персональных электронных вычислительных машин (ПЭВМ), включая как настольные, так и мобильные платформы, функционирующих под управлением операционных систем (ОС) Windows XP, Windows Vista, Windows Server 2008/ 2008 R2, Windows 7, Windows 8/ 8.1 **и** Windows Server 2012/ 2012 R2 (в т.ч. 64-разрядных), а также в АС класса «2», которые строятся на базе одноранговых локальных вычислительных сетей, в состав которых входят ПЭВМ, функционирующие под управлением ОС Windows XP, Windows Vista, Windows Server 2008/ 2008 R2, Windows 7, Windows 8/ 8.1 **и** Windows Server 2012/ 2012 R2 (в т.ч. 64-разрядных).

Комплекс может также использоваться на рабочих станциях и серверах распределенных вычислительных сетей, функционирующих под управлением указанных ОС (кроме случаев, когда рабочие станции и серверы вычислительной сети объединены в единый домен Active Directory).

В отличие от политики доверительного управления доступом, реализуемой штатными средствами защиты указанных ОС, использование комплекса **«Гриф»** позволяет обеспечить реализацию политики административного управления доступом к защищаемой информации, т.е. такого разграничения доступа, при котором назначать права доступа пользователей к защищенным информационным ресурсам могут только специально уполномоченные пользователи (администраторы). Комплекс полностью заменяет штатные средства администрирования ОС собственными средствами, поддерживающими реализацию административного разграничения доступа к защищенным ресурсам.

Комплекс обеспечивает защиту информации, представленной в виде файлов данных произвольного типа (электронных документов, электронных таблиц, конструкторских чертежей, данных геоинформационных систем и т.п)

Установка на ПЭВМ комплекса **«Гриф»** обеспечивает:

- невозможность неконтролируемого и несанкционированного ознакомления, копирования и восстановления информации;
- невозможность неконтролируемой и несанкционированной модификации и удаления информации;
- предоставление доступа к информации только при условии достоверного распознавания пользователей и с учетом полномочий, предоставленных согласно служебной необходимости;
- учет действий пользователей и регистрацию попыток нарушения установленного порядка доступа к информации, включая блокировку доступа к информации в случае выявления таких попыток, а также возможность осуществления контроля за доступом к информации со стороны уполномоченных лиц.

В состав программных средств (ПС) комплекса **«Гриф»** входят следующие основные компоненты:

- модуль обслуживания носителей данных аутентификации пользователей;
- интерфейсный модуль идентификации и аутентификации (провайдер аутентификации);
- модуль контроля запросов доступа к ресурсам и управления доступом к ресурсам (системный драйвер и резидентный модуль пользовательского режима);
- модуль контроля операций экспорта данных (программа экспорта данных комплекса **«Гриф»**);
- модуль контроля операций печати (программа печати комплекса **«Гриф»**);
- модуль администрирования (программа автоматизированного рабочего места (АРМ) администратора КСЗ);
- модуль восстановления целостности и обновления КСЗ;
- модуль сохранения данных аудита;
- модуль анализа данных аудита (программа АРМ анализа данных аудита);
- интерфейсный модуль взаимодействия с прикладным программным обеспечением.

2 РЕАЛИЗУЕМЫЕ ФУНКЦИИ

2.1 ФУНКЦИИ КОМПЛЕКСА

Комплекс **«Гриф»** реализует следующие основные функции защиты:

- *идентификацию и аутентификацию пользователей* на основании имени (псевдонима), пароля и носителя данных аутентификации (съемного файлового носителя или устройства Touch Memory);
- *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* (папкам) и содержащимся в них файлам, что позволяет организовать совместную работу нескольких пользователей, 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* с возможностью ограничения перечня используемых съемных носителей;
- *гарантированное удаление ИсОД* путем затирания содержимого файлов при их удалении;
- *разграничение доступа прикладных программ к выбранным каталогам* и содержащимся в них файлам, что позволяет обеспечить защиту ИсОД от случайного удаления или модификации и соблюсти технологию ее обработки;
- *контроль целостности прикладного программного обеспечения (ПО)* и ПО комплекса, а также блокировку загрузки программ, целостность которых нарушена, что позволяет обеспечить защиту от вирусов и соблюдение технологии обработки ИсОД;
- *контроль за использованием дискового пространства пользователями (квоты)*, что исключает возможность блокирования одним из пользователей возможности работы других;
- *возможность блокировки устройств интерфейса пользователя* (клавиатуры, мыши, монитора) на время его отсутствия;
- *контроль целостности и самотестирование комплекса* при старте;
- *восстановление функционирования комплекса после сбоев*, что гарантирует доступность информации при соблюдении правил доступа к ней;
- *регистрацию, анализ и обработку информации о критичных для безопасности событиях* (входа пользователя в ОС, попыток несанкционированного доступа, фактов запуска программ, работы с ИсОД, импорта/экспорта информации, вывода на печать и т.п.), что позволяет администраторам контролировать доступ к ИсОД, следить за тем, как используется комплекс, а также правильно его конфигурировать;

- *ведение архива зарегистрированных данных аудита;*
- *взаимодействие с прикладными программными системами (ППС) через определенный производителем комплекса интерфейс*, что позволяет обеспечить непрерывность защиты ИсОД при ее обработке как штатными средствами ОС, так и средствами различных ППС.

Все указанные функции защиты реализуются комплексом в полном объеме для всех ОС, указанных в разделе 1.

2.2 ФУНКЦИОНАЛЬНЫЙ ПРОФИЛЬ ЗАЩИЩЕННОСТИ И УРОВЕНЬ ГАРАНТИЙ

В терминах НД ТЗИ 2.5–004–99 "Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа" комплекс **«Гриф»** реализует следующий функциональный профиль защищенности:

{КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-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 – регистрация: защищенный журнал;

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 комплекса выполнена в соответствии с требованиями уровня Г-4 гарантий корректности реализации функциональных услуг, установленными НД ТЗИ 2.5–004–99.

2.2.1 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 несъемных носителях информации, которые содержат как ИсОД всех уровней конфиденциальности, так и требующую открытую информацию;
- защищенные информационные объекты (каталоги и файлы) на зарегистрированных или незарегистрированных съемных носителях информации, которые содержат как ИсОД всех уровней конфиденциальности, так и требующую открытую информацию;
- системные и прикладные ПС, которые предназначены для обработки защищенных объектов (файлов), содержащих ИсОД;
- технологическую информацию КСЗ;
- отдельные виды периферийных устройств (принтеры, плоттеры и т.п.), подключенные к соответствующим портам ввода/ вывода рабочих станций (РС).

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.

Комплекс 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.

Комплекс 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.

Комплекс предоставляет возможность администратору КСЗ предоставлять/ отменять пользователям полномочия импорта/ экспорта ИсОД с использованием съемных носителей, а также, при необходимости, ограничить перечень используемых съемных носителей только зарегистрированными соответствующими средствами КСЗ. КСЗ предоставляет возможность администратору КСЗ предоставлять/ отменять пользователям 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 комплекса;
- 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 оперативной памяти (ОП) РС;
- несъемные и съемные носители информации, используемые системными и функциональными ПС при обработке ИсОД;
- технологическую информацию КСЗ (учетные записи пользователей).

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

Относительно несъемных и съемных носителей информации 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 несъемных носителях информации, которые содержат как ИсОД всех уровней конфиденциальности, так и требующую открытую информацию;
- защищенные информационные объекты (каталоги и файлы) на зарегистрированных или незарегистрированных съемных носителях информации, которые содержат как ИсОД всех уровней конфиденциальности, так и требующую открытую информацию;
- системные и прикладные 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 технологической схеме (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.

Комплекс 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.

Комплекс 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.

Комплекс предоставляет возможность администратору КСЗ предоставлять/ отменять пользователям полномочия импорта/ экспорта ИсОД с использованием съемных носителей, а также, при необходимости, ограничить перечень используемых съемных носителей только зарегистрированными соответствующими средствами комплекса.

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 комплексом при установке защиты на каталог.

Комплекс обеспечивает возможность автоматизированного осуществления отката базы данных (БД) технологической информации в предшествующее состояние, если в процессе выполнения последовательности операций, связанных с установкой защиты на каталог несъемного диска или с регистрацией ТС, 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 несъемных дисков РС, которые содержат ИсОД всех уровней конфиденциальности;

Комплекс предоставляет администраторам КСЗ средства для управления максимально допустимым размером дискового пространства для одного пользователя на любом из несъемных дисков, 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 комплекса после отказа его компонента (с ухудшением характеристик обслуживания).

ДЗ-1 - модернизация

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

Политика данной услуги распространяется на:

- ПС комплекса;
- технологическую информацию КСЗ.

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

ДВ-1 - ручное восстановление

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

Политика данной услуги распространяется на:

- ПС комплекса;
- технологическую информацию КСЗ.

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

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

НР-2 – защищенный журнал

Реализация данной услуги обеспечивает возможность контроля опасных для комплекса 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 комплекса;
- технологическую информацию КСЗ.

Средства комплекса 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 КСЗ и ПС комплекса:
- 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 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 комплекса обеспечена защита протоколов регистрации от несанкционированного доступа (ознакомления, модификации или разрушения), а также возможность анализа протоколов уполномоченными администраторами.

НИ-3 - множественная идентификация и аутентификация

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

- средствам комплекса;
- 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 комплексе реализована встроенная ТС КСЗ, в которую включены ПС комплекса и файлы БД технологической информации КСЗ.

НК-1 - однонаправленный достоверный канал

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

Политика данной услуги распространяется на:

- пользователей всех категорий;
- ПС комплекса.

Достоверный канал реализуется в компонентах комплекса, 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;
- администраторы КСЗ;
- администраторы безопасности;
- пользователи.

Пользователь, который устанавливает комплекс, является системным администратором. Учетная запись системного администратора не может быть удалена или отключена. В обязанности системного администратора входит инсталляция и начальная инициализация комплекса, обновление при необходимости ПС комплекса, восстановление при необходимости целостности ПС и БД комплекса, восстановление при необходимости работоспособности ОС, установка и настройка дополнительных прикладных ПС. В процессе штатного функционирования комплекса учетная запись системного администратора 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 (прав доступа и административных полномочий) 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 после изменения их атрибутов.

Пользователь, успешно прошедший идентификацию и аутентификацию и не назначенный на роль системного администратора, 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 комплексу возможность защищать себя от внешних воздействий и гарантировать свою способность управлять защищенными объектами.

Политика данной услуги распространяется на:

- ПС комплекса;
- 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 комплекс определяет и поддерживает собственный домен исполнения (домен КСЗ), отличный от доменов всех других процессов, и реализует механизмы разграничения доменов.

В собственном домене комплекс обеспечивает защиту от несанкционированной модификации средств комплекса, реализующих механизмы защиты, и/ или потери управления КСЗ, 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 комплексе реализована встроенная ТС КСЗ, в которую включены ПС комплекса и файлы БД технологической информации КСЗ.

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

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

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

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

- исключение попыток поиска и использования уязвимостей комплекса 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 комплексу возможность проверить и на основе этого гарантировать правильность функционирования и целостность определенного множества своих функций.

Политика данной услуги распространяется на:

- ПС комплекса;
- 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 комплекса или нарушения целостности БД технологической информации) комплекс переводится в состояние, в котором запрещена обработка ИсОД. Возвратить комплекс к нормальному функционированию может только системный администратор.

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

2.3 ОБРАБОТКА ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ

Использование комплекса **«Гриф»** для защиты информации, составляющей государственную тайну, а также для защиты служебной информации и иной информации, требования к защите которой предъявляются законом, допускается только в том случае, если в АС создана КСЗИ. В этой КСЗИ дополнительно к функциональным услугам безопасности, должны быть реализованы организационные и инженерно-технические меры по обеспечению режима секретности при обработке секретной информации в АС и

(при необходимости) по предотвращению утечки информации по техническим каналам. Перечень и содержание указанных мер определяется нормативно-правовыми актами по вопросам защиты государственной тайны и нормативными документами системы технической защиты информации. Полнота и качество реализации указанных мер должны быть подтверждены результатами государственной экспертизы КСЗИ.

Как при создании КСЗИ в целом, так и при планировании использования комплекса **«Гриф»**, должны рассматриваться аспекты всех составляющих АС: физической среды, персонала, вычислительной системы и информации (технологии ее обработки).

3 ОПИСАНИЕ РЕАЛИЗОВАННЫХ ФУНКЦИЙ

3.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Прежде чем осуществлять разграничения доступа, комплекс 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. Таким образом, реализована аутентификация пользователя одновременно по двум принципам: "владею чем-то" – носитель данных аутентификации и "знаю что-то" – пароль (двухфакторная аутентификация). 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. Устройство Touch Memory подключается к последовательному порту COM2 через адаптер DS9097 или совместимый с ним. Допускается использовать устройства Touch Memory следующих типов: DS1995 (позволяет сохранять один набор данных аутентификации для одной учетной записи) и DS1996 (позволяет сохранять до четырех наборов данных аутентификации для четырех учетных записей различного типа).

В случае если предоставленная пользователем информация аутентификации не соответствует эталону, доступ пользователя в систему блокируется.

Кроме того, комплекс ведет контроль за истечением срока действия полномочий пользователя и его пароля, а также за соответствием дня недели и временного интервала, в который пользователь осуществляет вход в систему тем, которые заданы администратором.

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

3.2 РАЗГРАНИЧЕНИЕ ОБЯЗАННОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ

Любая политика безопасности (ПБ), кроме правил разграничения доступа, устанавливает правила управления. Функции управления возлагаются на доверенных лиц, которые несут ответственность за безопасность обработки информации. В АС лиц, за которыми закреплены полномочия на выполнение определенных функций управления, принято называть администраторами.

В соответствии с ПБ, реализуемой комплексом **«Гриф»**, выделены следующие административные роли:

- системный администратор;
- администраторы КСЗ;
- администраторы безопасности.

Выделение именно таких административных ролей преследует следующие цели:

- разграничить функции по управлению средствами комплекса и по контролю за соблюдением принятой ПБ между различными лицами;
- обеспечить невозможность несанкционированного и/или неконтролируемого назначения полномочий по доступу к ИсОД себе или другим пользователям со стороны технического персонала АС (системного администратора);
- обеспечить возможность лицам, ответственным за контроль соблюдения установленного режима обработки ИсОД (администраторам безопасности), выполнять свои обязанности, не вдаваясь в технические детали.

Пользователь, который устанавливает комплекс (первоначально – встроенная учетная запись ОС «Администратор»), является **системным администратором** комплекса. Учетная запись системного администратора не может быть удалена или отключена.

В обязанности системного администратора входит:

- инсталляция и начальная инициализация комплекса;
- обновление при необходимости ПО комплекса;
- восстановление при необходимости целостности ПО и баз данных комплекса;
- восстановление при необходимости работоспособности ОС;
- установка и настройка (с санкции другого администратора) дополнительного прикладного ПО.

Системный администратор должен обладать достаточными для выполнения указанных выше обязанностей квалификацией, знаниями особенностей установки и администрирования ОС и комплекса **«Гриф»**, а также необходимыми практическими навыками. В процессе штатного функционирования комплекса учетная запись системного администратора не используется.

В обязанности администраторов КСЗ, которых может быть несколько, входит управление учетными записями пользователей, защищенными информационными ресурсами и доступом к ним. За каждым администратором КСЗ могут быть закреплены полномочия на:

- регистрацию, удаление и управление атрибутами учетных записей пользователей, в т.ч. генерация носителей данных аутентификации пользователей, включение и отключение учетных записей обычных пользователей (не администраторов)
- управление правами доступа к защищенным каталогам и содержащимся в них файлам со стороны пользователей;
- управление правами доступа к защищенным каталогам и содержащимся в них файлам со стороны программ (технологическими схемами, см. п. 3.8);
- установка разрешений на использование прикладного ПО;
- управление уровнями конфиденциальности;
- управление квотами на использование дискового пространства.
- управление использованием зарегистрированных съемных носителей ИсОД.

При этом на действия администраторов КСЗ накладываются следующие ограничения:

- администраторы могут назначать права доступа к защищенным каталогам и содержащимся в них файлам только другим пользователям, при назначении прав себе учетная запись отключается и ее необходимо активировать администратору безопасности;
- администраторы могут менять свои административные полномочия, но при этом учетная запись отключается и ее необходимо активировать администратору безопасности;
- изменения атрибутов других администраторов (прав доступа и административных полномочий) вступает в силу только после санкции администратора безопасности и активизации соответствующей учетной записи.

Администратор КСЗ должен обладать знаниями и навыками по эксплуатации средств комплекса **«Гриф»**, достаточными для выполнения указанных выше обязанностей. Глубокого знания особенностей ОС от него не требуется.

В обязанности администраторов безопасности входит осуществление контроля (с использованием соответствующих средств комплекса, позволяющих выполнять анализ и обработку зарегистрированной информации о критичных для безопасности событиях) за соблюдением пользователями АС установленных правил доступа к ИсОД.

Администратор безопасности должен обладать минимальными знаниями и навыками по эксплуатации средств комплекса **«Гриф»**, достаточными для выполнения указанных выше обязанностей. Знания особенностей ОС от него не требуется.

В случае необходимости (при малой численности персонала) одно и то же лицо может совмещать различные административные обязанности, т.е. иметь учетные записи, соответствующие различным ролям, и использовать при этом один носитель данных аутентификации.

Далее в данном документе при описании возможностей комплекса **«Гриф»** под администратором понимается пользователь, имеющий соответствующие полномочия на выполнение действий, о которых идет речь.

3.3 РАЗГРАНИЧЕНИЕ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К КАТАЛОГАМ И ФАЙЛАМ

В соответствии с ПБ, реализуемой комплексом **«Гриф»**, защищаемыми объектами являются каталоги несъемных логических дисков и содержащиеся в них файлы.

Разграничение доступа пользователей к каталогам и содержащимся в них файлам реализовано в соответствии с принципами политики административного управления доступом. В отличие от политики доверительного управления доступом, реализуемой штатными средствами защиты ОС семейства Windows, при которой назначать права доступа пользователей к защищенным информационным ресурсам могут пользователи, являющиеся владельцами соответствующих информационных ресурсов (например, пользователь, создавший файл с ИсОД), реализация политики административного управления доступом к защищаемой информации предполагает, что назначать права доступа пользователей к защищенным информационным ресурсам могут только специально уполномоченные пользователи (администраторы).

При этом все разделы жесткого диска (логические диски), на которых создаются защищенные каталоги, должны быть отформатированы в файловой системе NTFS.

При создании и регистрации в БД комплекса защищенного каталога администратор указывает его уровень конфиденциальности. Уровень конфиденциальности каталога не может быть изменен. Незащищенные каталоги считаются по умолчанию открытыми (не имеющими уровня конфиденциальности) и доступ к ним разрешен всем пользователям.

Для каждого каталога администратор может установить список доступа, в котором перечислены пользователи, имеющие права доступа к данному каталогу и содержащимся в нем файлам (и подкаталогам), и разрешенные для этих пользователей виды доступа (только по чтению или по чтению и модификации).

Если уровень допуска пользователя (также задаваемый администратором) ниже, чем уровень конфиденциальности защищенного каталога, пользователь не сможет получить доступ к каталогу и содержащимся в нем файлам.

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

- «КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ»;
- «ДСП»;
- «СЕКРЕТНО»;
- «СОВ.СЕКРЕТНО»;
- «ОСОБОЙ ВАЖНОСТИ».

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

Каждому пользователю, который имеет соответствующий уровень допуска, администратор может предоставить права доступа к защищенному каталогу и содержащимся в нем файлам по чтению или по чтению и модификации. Пользователи имеют только те права доступа к защищенным каталогам и содержащимся в нем файлам, а значит и к содержащейся в них ИсОД, которые явно определены администратором. В отличие от стандартной политики, реализуемой ОС Windows, пользователь не может предоставить другим пользователям доступ к созданным им файлам – новые файлы наследуют права доступа, заданные администратором для каталога.

Защита распространяется на всю ветвь дерева, начиная с указанного в БД комплекса защищенного каталога, включая его подкаталоги и содержащиеся в них файлы. Поэтому, не допускается указывать в качестве нового защищенного каталога каталог, который является подкаталогом уже защищенного каталога. Комплекс запрещает выполнять переименование и удаление защищенного каталога и тех каталогов, которые его содержат, вплоть до находящегося в корне логического диска.

Доступ по записи к каталогам, в которых хранятся файлы ПО комплекса, разрешен только системному администратору с использованием ПО комплекса (программы АРМ администратора КСЗ). Доступ по записи к каталогам ОС разрешен только всем администраторам.

При попытке пользователя получить запрещенный вид доступа (например, удалить файл в каталоге, к которому разрешен доступ только по чтению) доступ блокируется и в протоколах аудита регистрируется попытка НСД. При этом приложению, с помощью которого осуществлялась попытка доступа, возвращается соответствующий код возврата, интерпретируемый как нарушение установленных прав доступа. При получении такого кода возврата интерактивные приложения (например, «Проводник»), как правило, выводят на экран соответствующее сообщение (рис. 1).

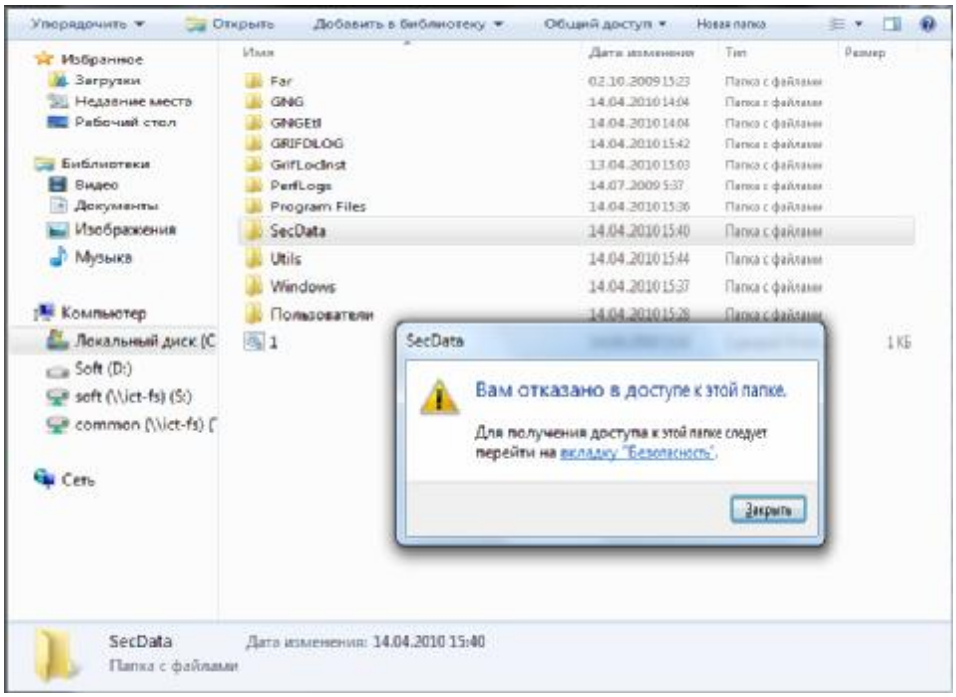


Рис.1. Сообщение «Проводника» об отсутствии прав доступа

3.4 УПРАВЛЕНИЕ ПОТОКАМИ ИНФОРМАЦИИ

Комплекс поддерживает возможность управления потоками информации, т.е.комплекс следит за тем, чтобы процессы, у которых есть открытые для чтения файлы, содержащиеся в защищенных каталогах, не могли открыть для записи файлы, содержащиеся в незащищенных (открытых или общих) каталогах или каталогах с меньшим уровнем конфиденциальности. Данная функция, 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 препятствует снижению уровня конфиденциальности ИсОД.

3.5 КОНТРОЛЬ ЗА ВЫВОДОМ ИНФОРМАЦИИ НА ПЕЧАТЬ

Администраторы КСЗ имеют возможность явным образом указать, кому из пользователей разрешен вывод информации на печать.

Кроме того, в комплексе введены дополнительные ограничения на выполнение операций печати. Пользователь, который имеет полномочия на выполнение операций печати, может реализовать их либо с помощью специальной утилиты комплекса (Программа печати комплекса **«Гриф»**), которая ведет углубленное протоколирование выполненных операций, либо с помощью доверенных (технологических) программ, указанных администратором КСЗ.

Все факты вывода информации на устройство печати фиксируются в протоколах аудита с указанием даты/времени, имени пользователя, атрибутов приложения и имени файла, который печатался. Содержание заносимой в протокол информации соответствует приведенному на рис. 2.

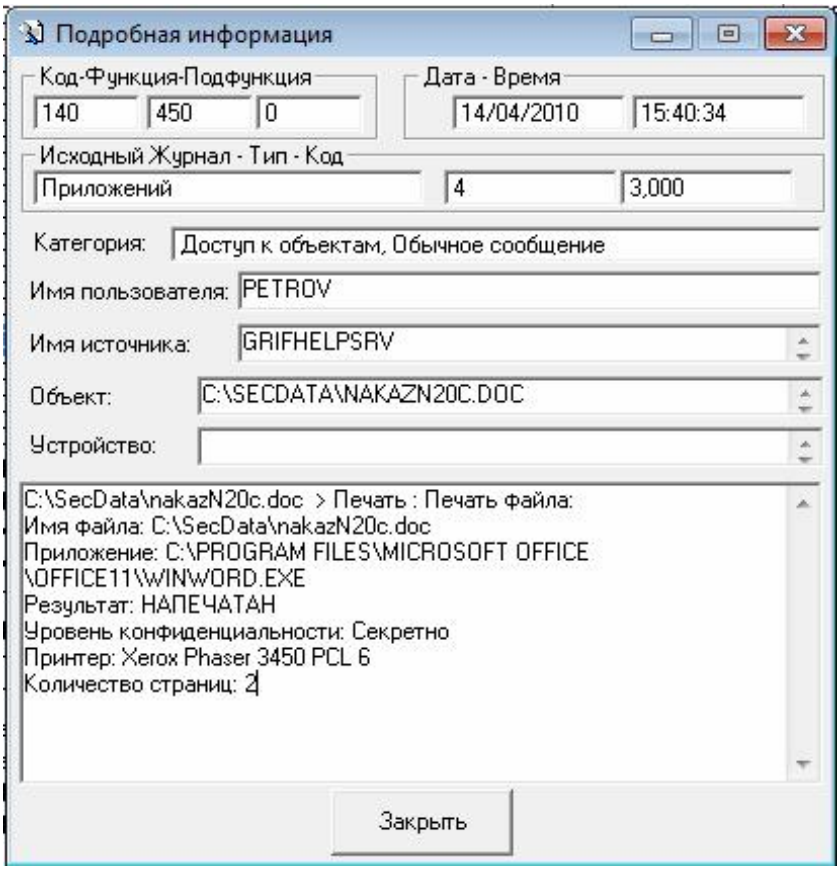


Рис.2. Диалог просмотра сообщения в протоколе аудита о выполненной операции печати

При выводе на печать документов в формате "Office Open XML" (поддерживается в средствах пакета MS Office 2007 и выше или аналогичных) комплекс позволяет выполнить автоматическое маркирование печатных листов документов согласно требований действующих нормативных документов в области охраны государственной тайны.

3.6 КОНТРОЛЬ ЗА ЭКСПОРТОМ/ ИМПОРТОМ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СЪЕМНЫХ НОСИТЕЛЕЙ

Все съемные носители (жесткие диски, подключаемые через USB-интерфейс, дискеты, flash-drive, CD-ROM, DVD-ROM и т.п.) рассматриваются как устройства импорта / экспорта. Администраторы КСЗ имеют возможность явным образом указать, кому из пользователей разрешен доступ к таким устройствам по чтению (импорт) или по чтению / записи (импорт / экспорт).

В комплексе введены ограничения на выполнение экспорта. Пользователь, который имеет полномочия на выполнение операций экспорта информации, может реализовать их либо с помощью специальной утилиты комплекса (Программа экспорта данных комплекса **«Гриф»**), которая ведет углубленное протоколирование выполненных операций, либо с помощью доверенных (технологических) программ, указанных администратором КСЗ.

Кроме этого, дополнительные ограничения на выполнение операций импорта и экспорта вводятся при использовании режима регистрации съемных носителей, допускающих многократное считывание/ запись информации (дискеты, flash-drive и т.п.). В этом случае администратор КСЗ может зарегистрировать в БД комплекса съемные носители, предварительно поставленные на учет в режимно-секретном органе, и

разрешить определенным пользователям выполнение операций импорта / экспорта только с использованием таких носителей.

Все операции с файлами, находящимися на устройствах импорта / экспорта фиксируются в протоколах аудита с указанием даты / времени, имени пользователя, атрибутов приложения и имени файла.

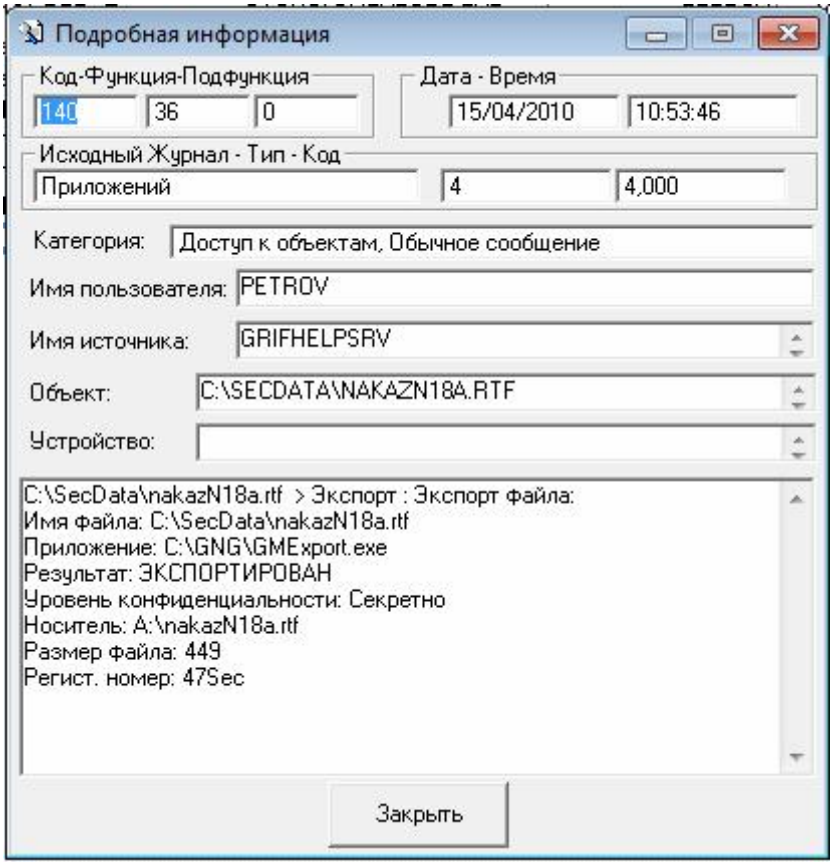


Рис.3. Диалог просмотра сообщения в протоколе аудита о выполненной операции экспорта на зарегистрированный съемный носитель

3.7 ГАРАНТИРОВАННОЕ УДАЛЕНИЕ ИНФОРМАЦИИ

В комплексе реализовано гарантированное удаление 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 услуги препятствует проведению атак типа "сбор мусора".

Гарантированное удаление информации реализуется также при удалении файлов со съемных носителей с использованием программы экспорта данных комплекса **«Гриф»**.

3.8 РАЗГРАНИЧЕНИЕ ДОСТУПА ПРИКЛАДНЫХ ПРОГРАММ К КАТАЛОГАМ И ФАЙЛАМ

В комплексе реализовано разграничение доступа к ресурсам (защищенным каталогам и содержащимся в них файлам) со стороны запускаемых пользователем процессов, что

позволяет обеспечить защиту ИсОД от случайного удаления, модификации и соблюсти технологию ее обработки.

Данная функция реализуется путем создания ТС. ТС представляет собой список защищенных каталогов данных и каталогов, содержащих файлы программ, которым разрешена модификация этих данных. Если каталог данных входит в ТС, то, даже если пользователь имеет права доступа к файлам данных, содержащимся в этом каталоге, он сможет осуществить доступ к данным с целью их модификации только с помощью определенных программ.

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

3.9 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРИКЛАДНОГО ПО

Реализация контроля целостности прикладного ПО преследует сразу несколько целей:

- во-первых, это препятствует распространению вирусов, а значит нарушению целостности программных средств ОС, ПО комплекса и обрабатываемой информации;
- во-вторых, это позволяет избежать утечки ИсОД за счет использования недокументированных возможностей ПО, 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, которое по определению не выполняет никаких действий, которые могли бы привести к отключению или преодолению средств защиты, что позволяет выполнить требования более высоких уровней услуги "целостность КСЗ".

При использовании контроля целостности ПО для тех программ, которые разрешены к использованию на данном рабочем месте, рассчитываются и сохраняются эталонные значения кодов контроля целостности (ККЦ). При запуске каждой программы комплекс заново рассчитывает ее ККЦ и сравнивает полученное значение с эталоном. Попытки запуска программ, целостность которых нарушена или ККЦ для которых не рассчитаны, блокируются и регистрируются в протоколах аудита как попытка НСД.

3.10 КОНТРОЛЬ ЗА ИСПОЛЬЗОВАНИЕМ ДИСКОВОГО ПРОСТРАНСТВА

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

3.11 БЛОКИРОВКА 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 осуществляется пользователем, например, в случае необходимости покинуть на время рабочее место. Для разблокирования компьютера пользователю необходимо предъявить свой носитель данных аутентификации и ввести пароль.

3.12 КОНТРОЛЬ ЦЕЛОСТНОСТИ И САМОТЕСТИРОВАНИЕ КОМПЛЕКСА

Каждый раз в процессе старта комплекс осуществляет контроль целостности своего ПО и тестирование его базовых механизмов.

В случае обнаружения нарушения целостности пользователю выдается соответствующее сообщение и дальнейшая работа блокируется. В такой ситуации необходимо вмешательство системного администратора для восстановления целостности или переинсталляции комплекса.

Контроль целостности комплекса может выполняться также по желанию администратора с использованием соответствующих функций программы АРМ администратора КСЗ.

Дополнительно для обеспечения целостности комплекса ограничивается доступ к каталогу, в котором содержатся файлы ПО комплекса, и параметрам настройки ОС по записи. Доступ по записи к каталогу, в котором содержатся файлы ПО комплекса, системный администратор может получить только через программу АРМ администратора КСЗ, которая позволяет модифицировать файлы ПО и БД комплекса только имеющим соответствующие полномочия пользователям и в соответствии с установленными правилами.

3.13 ВОССТАНОВЛЕНИЕ ФУНКЦИОНИРОВАНИЯ КОМПЛЕКСА ПОСЛЕ СБОЕВ

В случае обнаружения в процессе самотестирования при старте нарушения работоспособности комплекса, нарушения целостности ПО или БД комплекса пользователю выдается соответствующее сообщение и дальнейшая работа блокируется. В такой ситуации необходимо вмешательство системного администратора, который имеет возможность восстановить ПО или БД комплекса из резервной копии.

При работе с программой АРМ администратора КСЗ администратор КСЗ имеет возможность выполнять откат неудачно завершившихся операций, связанных с регистрации в БД комплекса защищенных каталогов и создании ТС.

3.14 РЕГИСТРАЦИЯ СОБЫТИЙ

Средства комплекса обеспечивают регистрацию в протоколах аудита таких событий, имеющих отношение к безопасности:

- факты регистрации и удаления или попытки регистрации и удаления учетных записей пользователей;
- факты регистрации/ удаления защищенных ресурсов (установки/ снятия защиты);
- факты назначения/ изменения прав доступа пользователей к защищенным ресурсам;
- факты изменения данных идентификации и аутентификации пользователей;
- факты входа пользователя в ОС и завершение работы пользователя (выход);
- факты доступа пользователя к защищенным каталогам и файлам;
- факты нарушения установленных прав доступа;
- изменение состояния БД комплекса и программных средств КСЗ:
- факты или попытки вывода файлов с ИсОД на печать;
- факты или попытки импорта файлов со съемных носителей;
- факты или попытки экспорта файлов с ИсОД на съемные носители;
- факты нарушения целостности или работоспособности средств комплекса;
- факты перезагрузки, выключения ПЭВМ и другие системные события;
- запуск и завершение технологических и привилегированных программ, в том числе входящих в состав комплекса.

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.

Просмотр и углубленная обработка протоколов аудита (фильтрация по заданным критериям, поиск) осуществляется администраторами с помощью программы АРМ анализа данных аудита. При работе с программой АРМ анализа данных аудита администраторы безопасности имеют доступ ко всем функциям программы АРМ, включая просмотр всех данных аудита, работу с архивами и изменение настроек программы АРМ. Системный администратор и администраторы КСЗ имеют полномочия по работе с данными аудита за исключением просмотра информации о доступе к файлам с ИсОД, которая заносится в журнал безопасности ОС. Они не могут менять настройки аудита комплекса или работать с архивами.

Для упрощения выполнения администраторами контроля за соблюдением пользователями АС установленных правил доступа к ИсОД в программе АРМ анализа данных аудита, кроме фильтрации и поиска событий, зарегистрированных в протоколах аудита, реализована возможность генерации следующих отчетов:

- сводный отчет по работе пользователей с ИсОД (рис. 4), в который выводится информация, отражающая результаты выполненных пользователями операций с файлами, содержащими ИсОД, за определенный период времени, а именно: время и количество операций открытия, чтения, модификации файлов; время и количество операций удаления файлов; время и количество операций печати файлов; время и количество операций записи файлов на устройства экспорта; время и количество операций чтения файлов с устройств импорта;

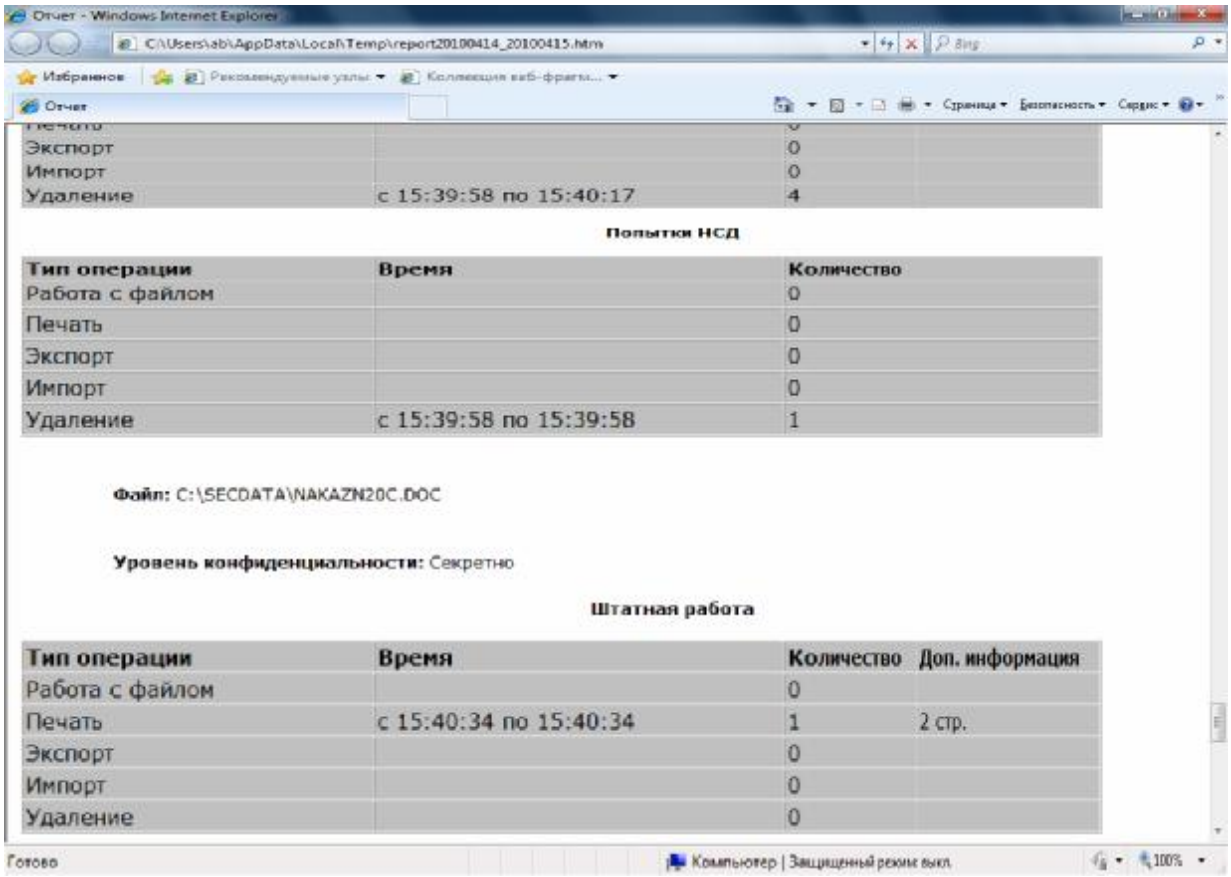
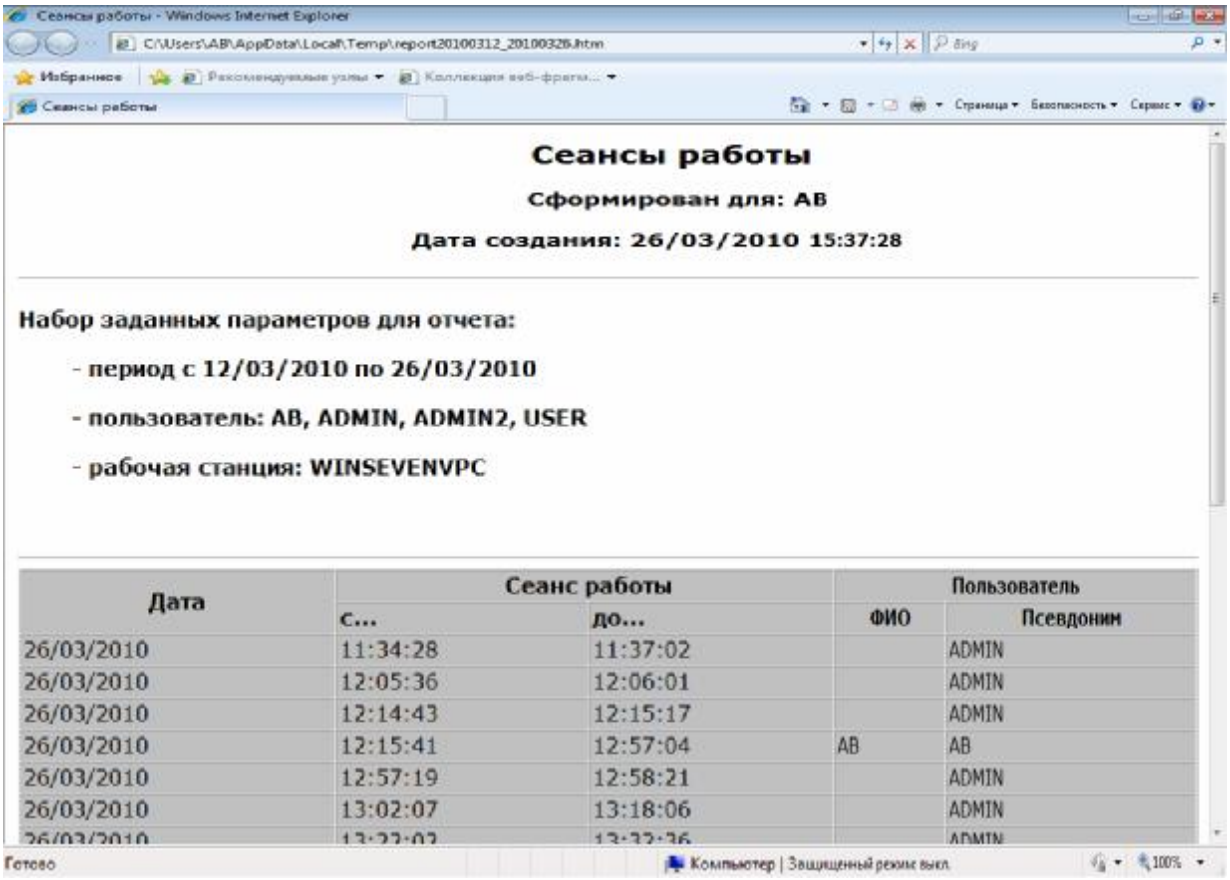


Рис. 4. Сводный отчет по работе пользователей с ИсОД

- сводный отчет о сеансах работы пользователей (рис.5), в который выводится информация о сеансах работы пользователей, а именно: ФИО и псевдоним пользователя, и инициировавшего сеанс работы; дата/ время начала/ завершения сеанса работы;
- сводный отчет по пользователям (рис. 6), в который выводится информация, отражающая результаты выполненных пользователями операций с файлами, содержащимися в защищенных каталогах, за определенный период времени, а именно: имя файла, содержащегося в защищенном каталоге; уровень конфиденциальности (гриф информации), содержащейся в защищенном каталоге; информация о наличии зарегистрированных сообщений о попытках НСД к файлу; информация о наличии зарегистрированных сообщений о штатной работе с файлом; информация о наличии зарегистрированных сообщений о выводе содержимого файла на печать; информация о наличии зарегистрированных сообщений о выводе содержимого файла на устройства экспорта (съемные носители); информация о наличии зарегистрированных сообщений о вводе содержимого файла с устройств импорта (съемных носителей); информация о наличии зарегистрированных сообщений об удалении файла;



Сеансы работы - Windows Internet Explorer

C:\Users\AB\AppData\Local\Temp\report20100312_20100326.htm

Избранное | Рекомендуемые узлы | Коллекция веб-фрагм...

Сеансы работы

Страница | Безопасность | Сервис

Сеансы работы

Сформирован для: AB

Дата создания: 26/03/2010 15:37:28

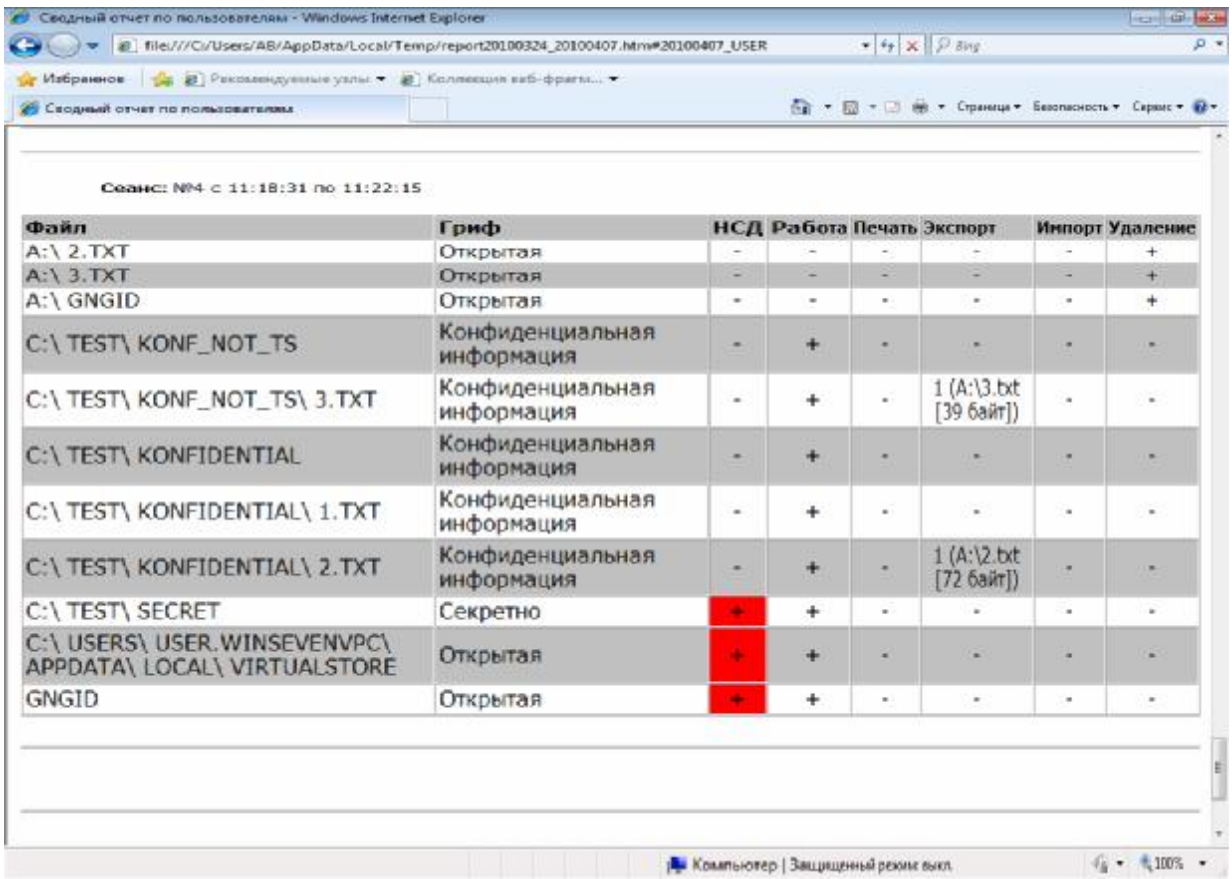
Набор заданных параметров для отчета:

- **период с 12/03/2010 по 26/03/2010**
- **пользователь: AB, ADMIN, ADMIN2, USER**
- **рабочая станция: WINSEVENVPC**

Дата	Сеанс работы		Пользователь	
	с...	до...	ФИО	Псевдоним
26/03/2010	11:34:28	11:37:02		ADMIN
26/03/2010	12:05:36	12:06:01		ADMIN
26/03/2010	12:14:43	12:15:17		ADMIN
26/03/2010	12:15:41	12:57:04	AB	AB
26/03/2010	12:57:19	12:58:21		ADMIN
26/03/2010	13:02:07	13:18:06		ADMIN
26/03/2010	13:22:02	13:32:26		ADMIN

Готово | Компьютер | Защищенный режим выкл. | 100%

Рис. 5. Диалог просмотра сводного отчета о сеансах работы пользователей



Сводный отчет по пользователям - Windows Internet Explorer

file:///C:/Users/AB/AppData/Local/Temp/report20100324_20100407.htm#20100407_USER

Избранное | Рекомендуемые узлы | Коллекция веб-фрагм...

Сводный отчет по пользователям

Страница | Безопасность | Сервис

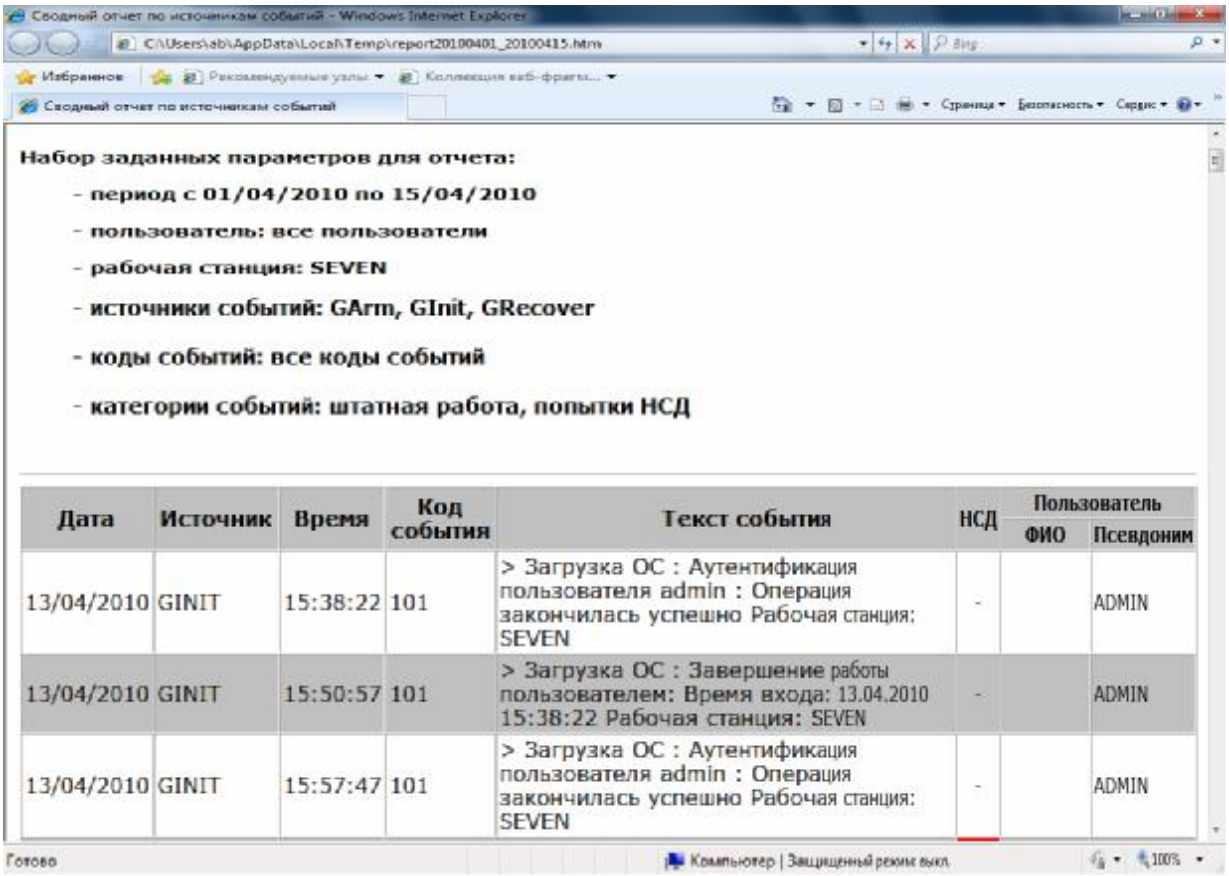
Сеанс: NN4 с 11:18:31 по 11:22:15

Файл	Гриф	НСД	Работа	Печать	Экспорт	Импорт	Удаление
A:\ 2.TXT	Открытая	-	-	-	-	-	+
A:\ 3.TXT	Открытая	-	-	-	-	-	+
A:\ GNGID	Открытая	-	-	-	-	-	+
C:\ TEST\ KONF_NOT_TS	Конфиденциальная информация	-	+	-	-	-	-
C:\ TEST\ KONF_NOT_TS\ 3.TXT	Конфиденциальная информация	-	+	-	1 (A:\3.txt [39 байт])	-	-
C:\ TEST\ KONFIDENTIAL	Конфиденциальная информация	-	+	-	-	-	-
C:\ TEST\ KONFIDENTIAL\ 1.TXT	Конфиденциальная информация	-	+	-	-	-	-
C:\ TEST\ KONFIDENTIAL\ 2.TXT	Конфиденциальная информация	-	+	-	1 (A:\2.txt [72 байт])	-	-
C:\ TEST\ SECRET	Секретно	+	+	-	-	-	-
C:\ USERS\ USER.WINSEVENVPC\ APPDATA\ LOCAL\ VIRTUALSTORE	Открытая	+	+	-	-	-	-
GNGID	Открытая	+	+	-	-	-	-

Компьютер | Защищенный режим выкл. | 100%

Рис. 6. Диалог просмотра сводного отчета по пользователям

- сводный отчет по источникам событий (рис. 7), в который выводится информация, касающаяся событий, зарегистрированных в протоколах аудита определенными (выбранными) источниками (приложениями), а именно: дата/ время регистрации события; имя приложения, выполнившего регистрацию события (являющегося источником события); код и текст сообщения о зарегистрированном событии.



Дата	Источник	Время	Код события	Текст события	НСД	Пользователь	
						ФИО	Псевдоним
13/04/2010	GINIT	15:38:22	101	> Загрузка ОС : Аутентификация пользователя admin : Операция закончилась успешно Рабочая станция: SEVEN	-		ADMIN
13/04/2010	GINIT	15:50:57	101	> Загрузка ОС : Завершение работы пользователем: Время входа: 13.04.2010 15:38:22 Рабочая станция: SEVEN	-		ADMIN
13/04/2010	GINIT	15:57:47	101	> Загрузка ОС : Аутентификация пользователя admin : Операция закончилась успешно Рабочая станция: SEVEN	-		ADMIN

Рис. 7. Диалог просмотра сводного отчета по источникам событий

3.15 ВЕДЕНИЕ АРХИВА ЗАРЕГИСТРИРОВАННЫХ ДАННЫХ АУДИТА

С помощью программы АРМ анализа данных аудита администратор безопасности может создать архивную копию данных аудита. Созданная архивная копия данных аудита может быть, при необходимости, перемещена на съемный носитель для долговременного хранения. При необходимости данные аудита могут быть восстановлены из архивной копии.

4 ВАРИАНТЫ ПРИМЕНЕНИЯ КОМПЛЕКСА

4.1 ПРИМЕНЕНИЕ КОМПЛЕКСА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ВИДЕ ФАЙЛОВ

При использовании комплекса для защиты обрабатываемой в АС с использованием соответствующих ППС информации, представленной в виде файловых объектов, защищаемые ресурсы (файлы с ИсОД) должны размещаться на жестких дисках отдельной ПЭВМ (в случае АС класса «1») или на жестких дисках серверов и рабочих станций АС (в случае АС класса «2») в защищенных средствами комплекса каталогах.

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 КОМПЛЕКСА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ВИДЕ ОБЪЕКТОВ БАЗ ДАННЫХ

При использовании комплекса для защиты обрабатываемой в АС с использованием соответствующих ППС информации, представленной в виде объектов баз данных, защищаемые ресурсы (файлы с содержимым хранилищ данных, в которых содержатся объекты баз данных, содержащие ИсОД) должны размещаться на жестких дисках отдельной ПЭВМ (в случае АС класса «1») или на жестких дисках серверов АС (в случае АС класса «2») в защищенных средствами комплекса каталогах.

Доступ к защищенным каталогам (и, соответственно, сохраняемым в них файлам), должен быть предоставлен только той служебной учетной записи (сервису), под которым функционирует соответствующий сервер системы управления базой данных (СУБД) и, в случае необходимости выполнения операций резервного копирования данных, выполняющим эту операцию пользователям. С целью предотвращения возможности модификации файлов, содержащих защищенные объекты баз данных (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 содержимого хранилищ, содержащими защищенные объекты баз данных (сильносвязанные объекты).

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

- взаимодействие со средствами комплекса (через соответствующий интерфейс, реализуемый интерфейсным модулем взаимодействия с ППС, см. *Модуль взаимодействия с прикладными программными системами. Руководство программиста*) для получения идентификаторов зарегистрированных пользователей ОС и их атрибутов доступа к ИсОД;
- назначение прав доступа к информационным объектам, обрабатываемым в ППС, в соответствии с полученными идентификаторами и атрибутами доступа пользователей к ИсОД, а также согласно установленным для системы требованиям;

- взаимодействие со средствами комплекса (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 ППС, на основании полученных от средств комплекса 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 со средствами комплекса для получения списка и атрибутов доступа защищенных ресурсов ОС (защищенных каталогов файловой системы) через соответствующий интерфейс, реализуемый интерфейсным модулем взаимодействия с ППС;
- контроль соответствия атрибутов доступа (уровня конфиденциальности) защищенных информационных объектов, обрабатываемых в ППС, и атрибутов доступа защищенных каталогов при экспорте информационных объектов из хранилища данных ППС в каталоги файловой системы или импорте информационных объектов из каталогов файловой системы в хранилище данных ППС.

5 УСЛОВИЯ ПОСТАВКИ

5.1 КОМПЛЕКТ ПОСТАВКИ

В комплект поставки входит:

- упаковка;
- паспорт;
- носитель с программным обеспечением комплекса и документацией в электронном виде;
- съемный файловый носитель (устройство Flash Drive) для хранения данных аутентификации системного администратора.

Кроме программы инсталляции комплекса и файлов эксплуатационной документации в электронном виде, носитель с программным обеспечением комплекса и документацией может включать пакеты обновления ПО комплекса (каталоги Patch_xxx). Перед установкой комплекса прочитайте файл _readme, который находится в корневом каталоге диска и содержит описание особенностей конкретного комплекта.

5.2 ТРЕБОВАНИЯ К АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

ПЭВМ, на которой предполагается использовать комплекс, должна функционировать по управлением одной из следующих ОС: Windows XP Professional, Windows Vista (все версии кроме Home Basic, Home Premium, Starter), Windows Server 2008/ 2008 R2, Windows 7 (все версии кроме Home Basic, Home Premium, Starter), Windows 8/ 8.1 (все версии кроме Core и SL), Windows Server 2012/ 2012 R2, без пакетов обновления (ServicePack) или с пакетами обновления.

Требования к конфигурации ПЭВМ для использования комплекса совпадают с требованиями разработчика соответствующей ОС. Для обеспечения возможности использования в качестве носителей данных аутентификации пользователей устройств Touch Memory дополнительными требованиями к конфигурации ПЭВМ являются:

- наличие последовательного порта для обеспечения возможности подключения адаптеров чтения/записи устройств Touch Memory;
- возможность выбора в Setup BIOS значения 2f8 (шестнадцатеричное) в качестве адреса выбранного порта.

Комплекс можно использовать для защиты рабочих станций и серверов локальной вычислительной сети, если эти серверы и рабочие станции не объединены в единый домен и функционируют под управлением указанных выше ОС.

5.3 СОВМЕСТИМОСТЬ С ПРОГРАММНЫМИ СРЕДСТВАМИ

Программные средства комплекса совместимы со средствами, входящими в комплект поставки ОС Windows XP Professional, Windows Vista (все версии кроме Home Basic, Home Premium, Starter), Windows Server 2008/ 2008 R2, Windows 7 (все версии кроме Home Basic, Home Premium, Starter), Windows 8/ 8.1 (все версии кроме Core и SL), Windows Server 2012/ 2012 R2, без пакетов обновления (ServicePack) или с пакетами

обновления, а также с другим системным, инструментальным и прикладным ПО, использующим стандартные интерфейсы указанных ОС.

Комплекс протестирован и может использоваться совместно с такими антивирусными средствами:

- DrWeb версий 5.0, 6.0 и выше;
- **«Антивирус Касперского»** версий 6.0, 7.0 и выше;
- Eset Smart Security (Nod32) версии 4.0 и выше.

Комплекс протестирован и может использоваться совместно с такими серверами систем управления базами данных:

- Microsoft SQL Server;
- Oracle;
- IBM DB2;
- Informix.

Комплекс может быть не совместим с другими средствами защиты от НСД, антивирусным ПО и ПО, работающим с дисками и файлами на низком уровне в обход файловой системы.

Информация о возможных ограничениях установки пакетов обновления ОС (ServicePack и patch) после установки комплекса содержится в файле _readme, который находится в корневом каталоге носителя с программным обеспечением, а также может быть получена в службе технической поддержки (см. п. 4.6).

5.4 СОСТАВ ДОКУМЕНТАЦИИ

В комплект эксплуатационной документации входят:

- описание комплекса;
- руководство по эксплуатации;
- руководство системного администратора;
- руководство администратора КСЗ;
- руководство администратора безопасности;
- руководство пользователя;
- краткое руководство по эксплуатации (быстрый старт);
- руководство программиста по использованию модуля взаимодействия с прикладными программными системами.

«Описание комплекса», «Руководство по эксплуатации» и «Краткое руководство по эксплуатации (быстрый старт)» предназначены для администраторов и среднего руководящего звена организации, использующей комплекс. «Руководство по эксплуатации» содержит рекомендации по использованию комплекса и призвано дать ответы на вопросы, ЧТО необходимо сделать для достижения максимальной эффективности его использования. Кроме того, в «Руководстве по эксплуатации» затрагивается ряд сопутствующих организационно-технических вопросов. «Краткое руководство по эксплуатации (быстрый старт)» содержит минимально необходимые сведения, необходимые для инсталляции комплекса и последующей работы.

Остальные руководства, как следует из их названий, в значительной степени предназначены для определенной категории пользователей, как привилегированных, обладающих правами по управлению комплексом – администраторов, так и не обладающих такими правами – обычных пользователей. Большая часть каждого руководства посвящена рассмотрению того, КАК выполняются те или иные функции, присущие каждой категории пользователей. «Руководство системного администратора» содержит описание средств и порядка инсталляции комплекса. Кроме того, оно содержит описание возможных проблем, конфликтов и ошибок и будет полезно также и администратору КСЗ. «Руководство администратора КСЗ» содержит описание программы автоматизированного рабочего места администратора и необходимо для всех администраторов, в части их касающейся. «Руководство администратора безопасности» содержит описание порядка работы со средствами анализа данных аудита, поэтому, кроме администратора безопасности оно будет полезно также системному администратору и администратору КСЗ. «Руководство пользователя» содержит описание специфики работы обычного пользователя в системе с установленным комплексом **«Гриф»**, в частности, работы с защищенными информационными ресурсами, вывода информации на съемные носители и принтер.

5.5 ПОРЯДОК ПРИОБРЕТЕНИЯ И ЛИЦЕНЗИРОВАНИЯ

Приобретение комплекса осуществляется Заказчиком непосредственно у Разработчика или у его уполномоченных представителей. Лицензирование использования комплекса осуществляется путем выработки Разработчиком регистрационного кода, который высылается Заказчику.

Начальный (ознакомительный) регистрационный код вводится автоматически, в процессе установки комплекса. Начальный (ознакомительный) регистрационный код дает право использования комплекса в течение трех месяцев с момента его установки. В течение этого срока необходимо получить у Разработчика (на основе данных, собранных программой инсталляции) и ввести новый регистрационный код. Наличие полученного от Разработчика регистрационного кода дает Заказчику право на установку и использование комплекса на одной ПЭВМ, функционирующей под одной из указанных выше ОС.

Повторная установка комплекса после выполнения переустановки ОС, вызванной любыми причинами (переход на новую версию, изменение конфигурации аппаратных средств используемой ПЭВМ и т.п.) возможна только на той же ПЭВМ после получения у Разработчика нового регистрационного кода.

5.6 ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Техническая поддержка комплекса включает:

- доступ в on-line режиме к пакетам обновления ПО комплекса на сайте Разработчика www.ict.com.ua с возможностью их установки на ПЭВМ с функционирующим комплексом;
- консультации по вопросам установки и использования комплекса в режиме "горячей линии" по телефону и по электронной почте;
- доступ в on-line режиме к базе данных часто задаваемых вопросов на сайте Разработчика www.ict.com.ua.

5.7 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

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