

РОСЖЕЛДОР

Федеральное государственное бюджетное образовательное учреждение высшего  
образования

«Ростовский государственный университет путей сообщения»  
(ФГБОУ ВО РГУПС)

Тамбовский техникум железнодорожного транспорта  
(ТаТЖТ – филиал РГУПС)

Обзор программно-аппаратных комплексов защиты информации для  
государственных учреждений. Характеристики, возможности

Подготовил  
студент группы  
ТАКС-311  
Жуков А.С.

Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в сетевые операционные системы.

К сервисам безопасности относятся:

Идентификация и аутентификация;

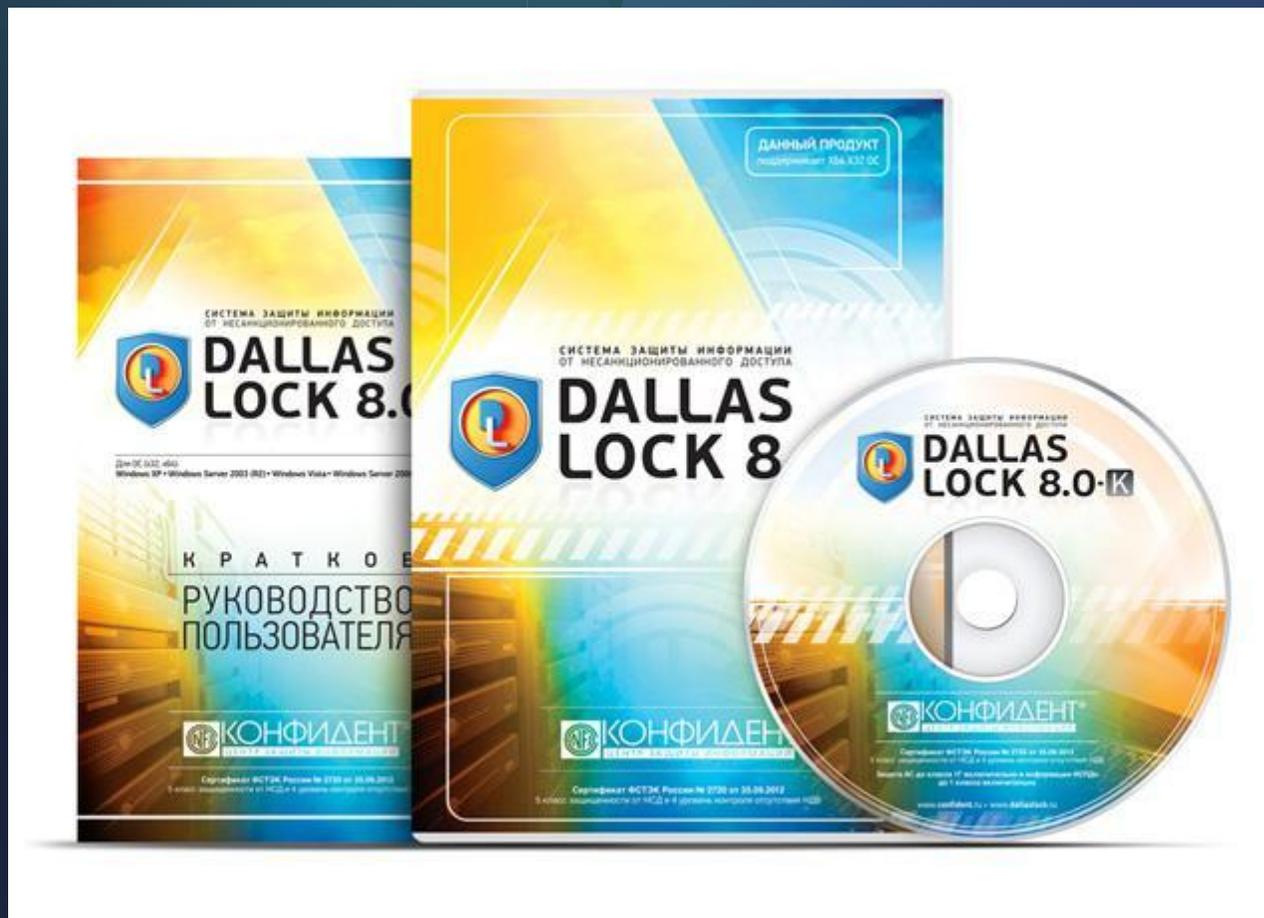
Управление доступом;

Протоколирование и аудит;

Криптография;

Экранирование.

# Система защиты информации от несанкционированного доступа «Dallas Lock»



## СЗИ «Dallas Lock» (разработчик ООО «Конфидент») представляет собой программно-аппаратный комплекс, добавляющий к системе безопасности Windows следующие функциональные возможности:

- 1. Организация доверенной загрузки с возможностью идентификации и аутентификации при помощи электронных идентификаторов Touch Memory;
- 2. Создание замкнутой программной среды для пользователей путем разрешения запуска ограниченного количества прикладных программ и динамических библиотек;
- 3. Реализация мандатной модели разграничения доступа на основе меток конфиденциальности пользователей и защищаемых ресурсов;
- 4. Контроль потоков защищаемой информации;
- 5. Очистка секторов, занимаемых защищаемыми файлами при их удалении, а также очистка памяти, выделяемой прикладным программам;
- 6. Контроль целостности указанных администратором файлов и системных областей диска;
- 7. Аудит доступа к защищаемым ресурсам;
- 8. Защита данных путем криптографического преобразования информации на диске.

# Система защиты информации «Secret NET 5.0-C»



С помощью программных и аппаратных средств «Secret Net 5.0-C» реализуются следующие защитные механизмы:

1. Механизм контроля входа в систему с использованием аппаратных средств.
2. Механизмы разграничения доступа и защиты ресурсов:
  - механизм полномочного разграничения доступа к объектам файловой системы;
  - механизм замкнутой программной среды;
  - механизм шифрования файлов;
  - механизм разграничения доступа к устройствам компьютера;
  - механизм затирания информации, удаляемой с дисков компьютера.
3. Механизмы контроля и регистрации событий:
  - механизм функционального контроля;
  - механизм регистрации событий безопасности;
  - механизм контроля целостности;
  - механизм контроля аппаратной конфигурации компьютера.

# Состав системы Secret NET

