Защита конфиденциальной информации и государственной тайны

СКЗИ «М-506А-XP»

Средство криптографической защиты информации **«М-506А-XP»** – это программно-аппаратный комплекс, предназначенный для защиты информации от несанкционированного доступа в локальных вычислительных сетях, функционирующих под управлением ОС MS Windows 2000, MS Windows XP и MS Windows 2003.

Легитимная защита

СКЗИ М-506А-XP сертифицировано ФСБ России и может применяться для защиты конфиденциальной информации, а также сведений, составляющих государственную тайну.

Ключевые возможности и преимущества

Шифрование сетевого трафика	реализовано в соответствии с ГОСТ 28147-89
Комплексная защита информации на рабочих станциях и серверах	доверенная загрузка, разграничение доступа к устройствам, контроль целостности программ и данных, контроль аппаратной конфигурации компьютера, гарантированное уничтожение данных, электронно-цифровая подпись и прозрачное шифрование файлов.
Удобство управления комплексом	централизованное управление настройками безопасности защищаемых компьютеров, средства управления безопасностью интегрированы со встроенными средствами управления ОС.
Оперативный контроль безопасности	регистрация событий на рабочих станциях, контроль действий сотрудников и администраторов, удобный механизм отчетов.
Надежность и масштабируемость	клиент-серверная архитектура с возможностью масштабирования контура управления повышает надежность системы и позволяет эффективно распределять нагрузку.

Механизмы защиты информации

Идентификация и аутентификация
Осуществляется с помощью средств аппаратной поддержки при входе пользователя в систему. В качестве устройств ввода идентификационных признаков могут быть использованы iButton или eToken R2/Pro.

Защита от загрузки с внешних носителей
С помощью средств аппаратной поддержки можно запретить обычному пользователю загрузку ОС с внешних съемных носителей.

Разграничение доступа к устройствам
Обеспечивается разграничение доступа к устройствам с целью предотвращения несанкционированного копирования информации с защищаемого компьютера.

Полномочное управление доступом
Управление доступом пользователей к конфиденциальной информации осуществляется на основе категорий конфиденциальности и прав допуска пользователей.

Контроль печати
Осуществляется контроль вывода конфиденциальной информации на печать, с возможностью маркировки листов в соответствии с принятыми в организации стандартами.

Замкнутая программная среда
Для каждого пользователя компьютера формируется определенный перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей.

Контроль целостности программ и данных
Контроль целостности и защита от модификации файлов, каталогов, элементов системного реестра и секторов дисков.

Прозрачное шифрование файлов
Шифрование производится по алгоритму ГОСТ 28147-89. Управление шифрованием файлов и доступ к зашифрованным файлам осуществляется на уровне каталога.

Гарантированное уничтожение данных
Путем записи случайной последовательности на место удаленной информации в освобождаемую область диска.

Контроль аппаратной конфигурации
Система контролирует аппаратную конфигурацию компьютера и позволяет блокировать его в случае обнаружения изменений.

Электронно-цифровая подпись файлов
Функция электронно-цифровой подписи (ЭЦП) реализована в соответствии с ГОСТ Р34.10-2001 и позволяет организовать обмен электронными документами внутри ЛВС, проверяя подлинность передаваемых и принимаемых документов.

Шифрование сетевого трафика
Функция криптографической защиты всего сетевого трафика, циркулирующего между всеми защищаемыми компьютерами ЛВС. Данная функция реализована в соответствии с ГОСТ 28147-89 и позволяет исключить возможность перехвата информации, которой обмениваются между собой серверы и рабочие станции локальной сети.

Архитектура комплекса

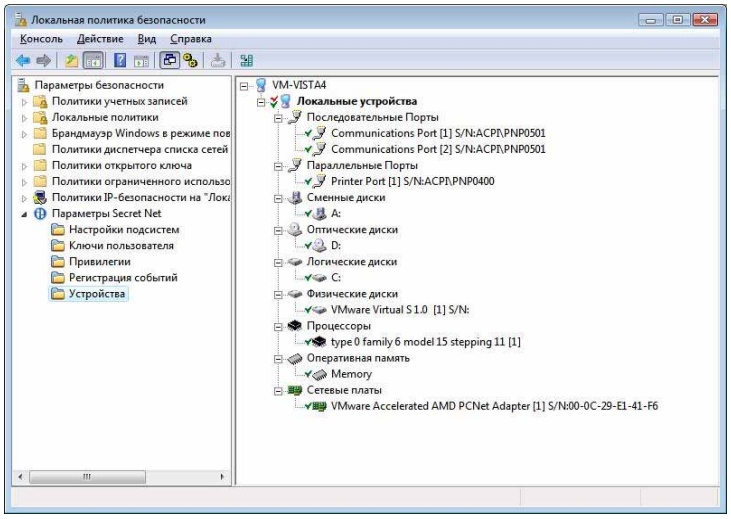
СКЗИ М-506А-XP создано на основе системы **Secret Net 5.0** – одного из самых распространенных сертифицированных средств защиты информации от несанкционированного доступа, дополненного механизмами шифрования сетевого трафика, прозрачного шифрования файлов и ЭЦП.

В качестве хранилища информации о настройках безопасности используется Active Directory (AD). Для нужд централизованного управления схема AD расширяется с помощью специального модуля из состава ПО **Secret Net** – создаются новые объекты и изменяются параметры существующих.

Управление безопасностью

Система централизованного управления безопасностью **М-506А-XP**, интегрирована в Microsoft Active Directory и служит для настройки защитных механизмов и изменения прав пользователей.

Настройки выполняются для отдельных компьютеров и пользователей, а также для их групп. Для этого используются стандартные средства управления операционной системы, такие как групповая политика и шаблоны безопасности.



Сервер безопасности
Производит сбор и хранение журналов событий рабочих станций и обеспечивает выдачу команд оперативного управления (блокировку рабочей станции при выявлении попытки НСД).

Система мониторинга «Монитор»
Отображает информацию о состоянии рабочих станций, дает возможность отслеживать какие компьютеры сети в данный момент включены, какие пользователи на них работают (как локально, так и в терминальном режиме), а также позволяет выдавать на защищаемые рабочие станции команды оперативного управления.

СЗИ Secret Net 5.0
Устанавливается на все защищаемые компьютеры. Защищает ресурсы компьютера и регистрирует события. Каждый компьютер оснащается средствами аппаратной поддержки (для идентификации пользователей и защиты от внештатной загрузки ОС).

Станция управления ключами
Выполняет функции создания ключей шифрования и изготовления ключевых носителей. Устанавливается на автономный компьютер.

Оперативный контроль

СКЗИ М-506А-XP немедленно сообщает администратору безопасности о фактах и попытках НСД и позволяет своевременно реагировать на подобные события. **М-506А-XP** позволяет контролировать:

Действия сотрудников в ИС
Система защиты позволяет контролировать действия пользователя на рабочей станции сети в реальном режиме времени, блокировать работу пользователя или выключить компьютер;

Действия привилегированных пользователей
Реализована регистрация управляющих действий администраторов разных уровней;

Потоки информации
СКЗИ М-506А-XP обеспечивает доступ пользователей к информационным ресурсам в соответствии с уровнем допуска сотрудника к информации и позволяет контролировать создание, перемещение и удаление информационного ресурса, содержащего конфиденциальную информацию.

СКЗИ «М-506А-XP»

127018, г.Москва, а/я 55
Тел./факс (495) 980-2345
E-mail: market@infosec.ru, http://www.infosec.ru