

Система шифрования данных для крупных корпораций

Корпоративные системы информационной безопасности должны обеспечивать защиту конфиденциальных данных как внутри, так и за пределами корпоративной сети. Сегодня эта задача чрезвычайно актуальна в связи с широким использованием – особенно в среде топ-менеджмента – портативных компьютеров – ноутбуков и других переносных носителей информации, работать с которыми можно и вне офиса.

Парольная защита, представляемая средствами операционной системы, не может обеспечить должный уровень безопасности, так как незашифрованные данные с жесткого диска утерянного или украденного ноутбука с легкостью могут быть прочитаны.

Разработанный компанией InfoWatch продукт – InfoWatch CryptoStorage Enterprise – осуществляет шифрование данных и позволяет предотвратить несанкционированное использование конфиденциальной информации как внутри, так и за пределами корпоративной сети.

Продукт обеспечивает:

- защиту конфиденциальной информации, хранящейся на рабочих станциях и серверах;
- снижение финансовых, юридических и иных рисков, связанных с утерей данных;
- соответствие требованиям регулирующих органов к хранению персональных данных.

«Более 70% финансовых потерь в 2008 году было вызвано нарушениями информационной безопасности внутри компаний и последующей утратой конфиденциальных данных»

Ponemon Institute

Функциональные возможности решения

Защита различных типов объектов

InfoWatch CryptoStorage Enterprise обеспечивает шифрование:

- отдельных файлов и папок,
- логических дисков, включая системные и загрузочные области,
- съёмных носителей (USB-накопители, Flash-диски, карты памяти для мобильных устройств и т.п.).

Продукт позволяет создавать защищенные хранилища данных (специализированные файлы-контейнеры).

Шифрование данных производится в прозрачном режиме: при обращении к данным они автоматически расшифровываются в оперативной памяти компьютера, а при сохранении – зашифровываются. Продукт позволяет защитить содержимое оперативной памяти, например, Hibernate File, создаваемый системой при переходе в «спящий» режим, или Windows Crash Dump Files, создаваемые при возникновении фатальной ошибки.

Преимущества решения

- Продукт отечественного разработчика, который отвечает требованиям российского законодательства (лицензии ФСБ на разработку, распространение и обслуживание криптографических средств, поддержка ГОСТ 28147-89)
- Доступная цена без скрытых расходов: вся функциональность решения доступна в рамках единого модуля
- Легкость внедрения и эксплуатации: масштабируемость, интеграция с Active Directory, гибкие настройки и высокая надежность защиты
- Удобство для пользователей: возможность работы с защищенными данными вне корпоративной сети и высокая производительность при операциях шифрования/расшифровки

Надежное разграничение доступа к защищенным объектам

Перед началом работы с защищаемыми данными в обязательном порядке осуществляется авторизация пользователя. Доступ к защищенному объекту возможен по паролю или секретному ключу. Для хранения секретных ключей могут использоваться любые носители. Если защита установлена на загрузочный или системный раздел диска, авторизация проводится еще до загрузки операционной системы. Система поддерживает двухфакторную аутентификацию пользователей с помощью электронных ключей USB eToken/USB ruToken.

Стойкие алгоритмы шифрования

В InfoWatch CryptoStorage Enterprise используется на выбор либо стойкий современный алгоритм шифрования AES или российский алгоритм шифрования ГОСТ 28147-89.

Защита сетевых ресурсов

InfoWatch CryptoStorage Enterprise позволяет устанавливать защиту на данные, которые находятся на другом компьютере в рамках локальной сети. Таким образом, можно создать систему централизованного хранения информации, нуждающейся в защите, с организацией к ней многопользовательского иерархического доступа. Продукт предусматривает возможность установки дополнительной защиты на отдельные папки и файлы внутри уже защищенных объектов. Глубина вложенности при этом не ограничена

Интеграция с корпоративным каталогом

Интеграция с Microsoft Active Directory позволяет напрямую выбирать пользователей или группы пользователей из корпоративного каталога и применять к ним корпоративные политики безопасности. Решение позволяет централизованно устанавливать клиентскую часть InfoWatch CryptoStorage Enterprise посредством политик Microsoft Active Directory.

Настройка политик безопасности

Установка и настройка InfoWatch CryptoStorage Enterprise осуществляется централизованно с помощью консоли удаленного администрирования. Централизованное применение политик, позволяет определить правила работы с конфиденциальной информацией для каждого пользователя. С помощью решения можно задать параметры использования защищенных объектов, такие как время работы и разрешенные действия над защищенными объектами. Система ролей пользователей обеспечивает безопасный многопользовательский доступ к данным.

Системные требования

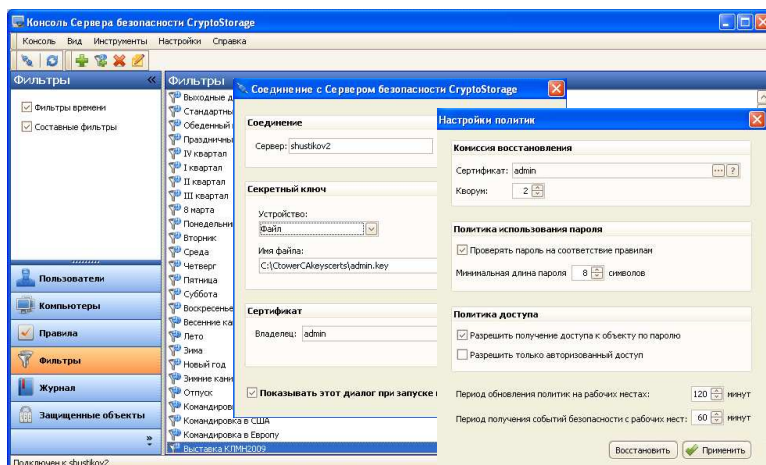
- **Клиент:** ОС - MS Windows (2000, 2000 Server, XP, 2003, Vista). **Аппаратные требования:** Celeron 1GHz и выше, RAM 256Mb, свободное дисковое пространство - 30Mb
- **Сервер:** MS Windows (2000 Server, XP, 2003, Vista). **Аппаратные требования:** Pentium-4 3 GHz, RAM – 1Gb, свободное место на диске 50 Mb

Гарантированное удаление данных

При обычном удалении файлов средствами MS Windows, их содержимое остается на диске. После такого удаления файл можно восстановить с помощью специальных утилит. InfoWatch CryptoStorage Enterprise позволяет удалять данные с диска без возможности обратного восстановления.

Восстановление доступа к конфиденциальной информации

В случае утраты ключа доступ к защищенному объекту возможен благодаря специальной функции решения - комиссии восстановления. Эта функция позволяет восстановить доступ к защищенному объекту с использованием ключей уполномоченных пользователей решения.



Анализ активности

С помощью InfoWatch CryptoStorage Enterprise администратор решения может создавать подробные отчеты, проводить анализ действий пользователей с конфиденциальной информацией с учетом таких параметров, как временной интервал, конкретный пользователь или компьютер, тип защищенного объекта и вид операции с данными.

Контакты:

тел.: +7 495 22 900 22

Российская Федерация, 123458, Москва, проезд №607, дом 30, офис 507

www.infowatch.ru
sales@infowatch.ru