A KASPERSKY LAB'S COMPANY

INFOWATCH

CryptoStorage 2.1

Руководство пользователя

CRYPTOSTORAGE 2.1

Руководство пользователя

Тел. +7 (495) 229-00-22 • Факс +7 (495) 229-00-22
http://www.infowatch.ru

Дата редакции: сентябрь 2011 года

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

InfoWatch CryptoStorage (далее InfoWatch CryptoStorage или Система) – система криптографической защиты конфиденциальной информации, хранящейся на персональном компьютере, от несанкционированного доступа.

Это руководство описывает использование InfoWatch CryptoStorage.

Аудитория

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows.

Структура руководства

В состав руководства входят следующие разделы:

- *Глава 1. Введение в InfoWatch CryptoStorage (стр. 8).*

  Содержит общие сведения об InfoWatch CryptoStorage (назначение, состав, типы защищаемых объектов).

- *Глава 2. Установка InfoWatch CryptoStorage (стр. 12).*

  В разделе описывается установка InfoWatch CryptoStorage.

- *Глава 3 Интерфейс Системы (стр. 17).*

  Содержит описание интерфейса Системы.

- *Глава 4. Защита данных. Работа с защищенными объектами (стр. 19).*

  В разделе описываются различные способы защиты данных, предлагаемые системой InfoWatch CryptoStorage (особенности различных типов защиты, алгоритмы работы). Содержит описание правил работы с защищенными объектами, сведения по администрированию защищенных объектов.

- *Глава 5. Конфигурирование подсистем (стр. 50).*

  Описывает настройку подсистем InfoWatch CryptoStorage.

- *Глава 6. Удаление InfoWatch CryptoStorage (стр. 52).*

  Описывает процедуру удаления, содержит инструкции по подготовке защищенных объектов к удалению Системы.

- *Приложение А. Пользовательское лицензионное соглашение (стр. 53).*

  Условия использования продукта на основе лицензионного соглашения.

- *Приложение В. Лицензия на библиотеку Windows Installer XML (WIX) (стр. 57*

  Текст лицензии на библиотеку Windows Installer XML (WiX) 3.0.

Условные обозначения

Для наглядности в тексте документации используются различные стили оформления. Области применения стилей указаны в таблице 1.

Таблица 1. Стили оформления

Стиль оформления	Область применения	Пример
Полужирный шрифт	Названия элементов графического пользовательского интерфейса (кнопки, команды меню и пр.)	В меню **Пуск** выберите пункт **Все программы ► InfoWatch CryptoStorage ► Утилита восстановления дисков**.
Курсив	При описании таблиц, в примерах, описаниях – названия и значения атрибутов объектов	Не включайте в состав пароля наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, такие как: *qwerty*, *123456789*, *qazxsw* и т. п.
`Шрифт Courier New (10 пт)`	Имена файлов, значения параметров; примеры настроек конфигурационных файлов, командных строк, тексты программ.	Запустите установочный файл `CryptoStorage_RU_VVVV.msi`.

Техническая поддержка пользователей

Новые версии программного продукта InfoWatch CryptoStorage и документации можно найти на сайте компании www.infowatch.ru по адресу: www.cryptostorage.ru.

Для решения возникающих вопросов при работе с Системой пользователи лицензионных версий программного продукта могут обращаться за поддержкой по адресу: support@infowatch.ru.

ГЛАВА 1. ВВЕДЕНИЕ В INFOWATCH CRYPTOSTORAGE

В данном разделе содержится следующая информация:

1.1. Основные сведения об InfoWatch CryptoStorage

Система предназначена для защиты конфиденциальной информации пользователя от несанкционированного доступа и предотвращения утечки данных при сохранении операционной системой служебной информации на диске или неполного уничтожения файлов пользователя.

Для защиты информации применяется механизм **прозрачного шифрования**.

Прозрачное шифрование – это механизм, при котором информация хранится в защищенном объекте исключительно в зашифрованном виде. Работа с защищенным объектом осуществляется таким образом, что при обращении к данным они автоматически расшифровываются в оперативной памяти, а при записи – снова зашифровываются.

В качестве алгоритма шифрования используется алгоритм AES. Этот алгоритм одобрен международным криптографическим сообществом и является стандартом в криптографии. AES утвержден Национальным Институтом Стандартов и Технологий США (Standards and Technology (NIST) Federal Information Processing Standards (FIPS) PUB 197 26.11.2001).

Криптографический ключ генерируется на основании пароля пользователя. В связи с этим на длину этого пароля могут быть наложены ограничения, обусловленные местными законодательными требованиями.

Ниже перечислены основные функции Системы.

Защита данных

Система предоставляет возможность:

- создавать отдельные защищенные папки в файловой системе NTFS для размещения конфиденциальной информации;
- создавать виртуальные защищенные диски (защищенные контейнеры) для размещения конфиденциальной информации.
- защитить всю информацию на логических разделах жесткого диска, включая системные и загрузочные, на Flash-накопителях, USB устройствах хранения и прочих устройствах класса Mass Storage;

Защита системного диска обеспечивает конфиденциальность:

- содержимого оперативной памяти, сохраняемого на диске при переходе в спящий (hibernate) режим;
- данных файла дампа памяти (crash dump), сохраняемого на диске в экстренных ситуациях;
- информации из временных файлов и файлов подкачки.

Работа с защищенными данными.

Системой обеспечивается:

- разграничение доступа к защищенной информации на основе паролей пользователей;
- многопользовательский доступ к защищаемой информации;
- возможность размещения одних защищенных объектов внутри других с произвольной глубиной вложенности;
- предотвращение случайного или умышленного уничтожения защищенных объектов посредством ограничения доступа к этим объектам;
- работа с защищенными контейнерами и папками, расположенными как на компьютере пользователя, так и на ресурсах локальной сети;
- возможность переноса защищенных объектов вместе с физическим носителем, на котором объекты расположены, на другой компьютер, на котором также установлена Система. При этом возможность работы с объектами не утрачивается;
- гарантированное удаление файлов и папок.

1.2. Компоненты InfoWatch CryptoStorage

Компоненты, входящие в состав InfoWatch CryptoStorage, перечислены в таблице 2.

Таблица 2. Компоненты InfoWatch CryptoStorage

Компонент	Назначение компонента
Компоненты, встроенные в оболочку (Shell) Проводника	Создание защищенных объектов, работа с защищенными данными, снятие защиты, гарантированное удаление файлов и папок.
Программа управления «Конфигуратор CryptoStorage»	Настройка подсистем InfoWatch CryptoStorage, настройка параметров создания и подключения защищенных объектов. Работа с лицензиями, активация
Утилита восстановления дисков	Удаление защищенных разделов на диске, использование которых невозможно. Восстановление метаданных защищённых разделов в случае повреждения
Справка InfoWatch CryptoStorage Help	Файл подсказки в формате .CHM

1.3. Защищенные объекты

Под **защищенными объектами** понимаются любые объекты, предназначенные для хранения данных, которые защищены средствами InfoWatch CryptoStorage.

Защищенные объекты бывают следующих типов.

- **Защищенная папка** представляет собой специальную папку в файловой системе NTFS, которую пользователь создает средствами InfoWatch CryptoStorage на своем компьютере или в сетевой папке. После подключения папки средствами InfoWatch CryptoStorage появляется возможность работы с ней, как с обычной папкой NTFS.
- **Защищенный контейнер** представляет собой специальный файл, который пользователь создает средствами InfoWatch CryptoStorage на своем компьютере или в сетевой папке. После подключения контейнера средствами InfoWatch CryptoStorage появляется возможность работы с ним, как с виртуальным логическим диском. Кроме этого, файлы-контейнеры можно копировать, записывать на CD и DVD, отправлять по почте, переносить на другой компьютер, с установленной Системой. При этом возможность подключения контейнеров не утрачивается.
- **Защищенный раздел (диск)** получается путем преобразования (шифрования) средствами InfoWatch CryptoStorage существующего логического раздела жесткого диска с размещенными на

нем данными. В том числе возможна защита, системных и/или загрузочных разделов и устройств класса Mass Storage (Flash-накопители, USB устройства хранения и пр.). После подключения защищенного раздела средствами InfoWatch CryptoStorage появляется возможность работы с ним, как с обычным разделом.

> **Важная информация!**
>
> После создания защищенного объекта, все данные, помещаемые в него, будут автоматически защищены. При копировании данных из защищенного объекта в незащищенную область данные размещаются в незащищенной области в открытом (незащищенном) виде.

1.4. Права доступа к защищенным объектам

Для предотвращения несанкционированных действий доступ к защищенным объектам осуществляется только после авторизации пользователя.

Для авторизации пользователю необходимо ввести пароль доступа к данному объекту.

> **Примечание:**
>
> Если пользователь ввел пароль неверно, то после сообщения Системы об отказе в доступе отобразится подсказка к паролю, - если при определении пароля пользователь задал подсказку к паролю.

В Системе существуют две роли для работы с защищенными объектами: **владелец** и **пользователь**:

- **Владелец защищенного объекта** – это пользователь, имеющий право на выполнение любых действий над этим объектом. Владелец защищенного объекта назначается при установке защиты на объект (или при создании защищенного объекта). У каждого защищенного объекта может быть только один владелец.
- **Пользователь защищенного объекта** – это любой пользователь, которого владелец включил в список доступа к защищенному объекту. В отличие от владельца, пользователь имеет ограниченный набор прав на работу с защищенным объектом.

В таблице 3 перечислены права на выполнение различных действий по управлению защищенными объектами для владельцев и пользователей (наличие или отсутствие права на выполнение определенного действия отмечено знаками «+» и «–» соответственно).

Таблица 3. Права пользователей и владельцев объектов

Действие над защищенным объектом	Владелец защищенного объекта	Пользователь защищенного объекта
Подключение/ отключение	+	+
Работа с объектом (чтение, копирование, архивирование, удаление и т. п.)	+	+
Гарантированное удаление папки или файла **Примечание**: Гарантированное удаление незащищенных папок может выполнять любой пользователь компьютера, на котором установлена Система	+	+
Просмотр информации о защищенном объекте	+	–
Изменение списка доступа (добавление/удаление пользователей защищенного объекта)	+	–
Переустановка/снятие защиты	+	–
Изменение собственных параметров авторизации	+	+

1.5. Рекомендации по составлению паролей. Использование подсказок к паролям

Доступ ко всем защищенным объектам осуществляется только после прохождения авторизации. Одним из обязательных параметров авторизации является пароль. При составлении паролей рекомендуется придерживаться следующих правил:

- пароль должен содержать не менее восьми символов;
- в состав пароля могут входить цифры, латинские буквы, пробелы и специальные символы («**.**», «**,**», «**?**», «**!**», «**<**», «**>**». «**”**» и др.);
- рекомендуется составлять пароль из смешанного набора цифровых и буквенных (прописных и строчных) символов.

Не включайте в состав пароля:

- общеупотребительные слова и устойчивые словосочетания;
- наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, такие как: *qwerty*, *123456789*, *qazxsw* и т. п.
- персональные данные: имена и фамилии, адреса, номера паспортов, страховых свидетельств и т. п.
- также не рекомендуется повторно использовать пароли, созданные для доступа к другим программам (электронная почта, базы данных и пр.).

> **Важная информация!**
>
> В случае утраты всех паролей доступа к защищенному объекту восстановить содержимое объекта невозможно!

Возможно использование подсказок к паролям. Подсказка – это символьная строка в специальном, для нее отведенном поле, которая может быть задана пользователем на этапе задания пароля. Если подсказка задана, то при неправильном введении пароля Система отказывает в доступе к объекту и отображает подсказку. Подсказка может содержать некую информацию, помогающую пользователю вспомнить пароль.

> **Важная информация!**
>
> При задании подсказки к паролю помните, что эта подсказка будет отображаться любому пользователю при попытке подключения объекта. Поэтому подсказка не должна содержать явных указаний на пароль.

ГЛАВА 2. УСТАНОВКА INFOWATCH CRYPTOSTORAGE

В данном разделе содержится следующая информация:

2.1. Требования к аппаратному и программному обеспечению

Для работы InfoWatch CryptoStorage необходимо соответствие компьютера следующим аппаратным и программным требованиям.

Аппаратные требования:

- процессор Intel Celeron 1 ГГц или выше;
- 256 МБ свободной оперативной памяти;
- 10 МБ свободного дискового пространства для установки приложения.

Программные требования:

- Одна из следующих операционных систем:
  - Microsoft Windows XP Service Pack 3;
  - Microsoft Windows Vista Service Pack 2;
  - Microsoft Windows 7;
  - Microsoft Windows 2003 Server;
  - Microsoft Windows 2008;
  - Microsoft Windows 2008 R2;
  - Microsoft Windows Home Server;
  - Microsoft Windows Small Business Server 2011 Essentials и Standard.

Для систем, поддерживающих платформы x86 и x64, Система поддерживает работу в обоих вариантах.

2.2. Описание установки

> **Важная информация!**
>
> Для установки InfoWatch CryptoStorage требуются права локального администратора на компьютере.

Программа установки выполнена в виде мастера. Каждое окно содержит набор кнопок для управления процессом установки. Их назначение:

- **Далее** – принять действие и перейти к следующему шагу процедуры установки.
- **Назад** – вернуться на предыдущий шаг установки.
- **Отмена** – отказаться от установки.

Ниже приведено пошаговое описание процедуры установки Системы.

Шаг 1. Начало установки

Вставьте диск с дистрибутивом InfoWatch CryptoStorage в дисковод для компакт-дисков или самостоятельно запустите установочный файл `CryptoStorage_RU_VVVV.msi`.

В названии установочного файла `VVVV` – версия программного продукта.

> **Примечание:**
>
> Новую версию программного продукта InfoWatch CryptoStorage вы можете получить по адресу: www.cryptostorage.ru.

После этого на экран будет выведено окно приветствия мастера установки InfoWatch CryptoStorage.

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 2. Заключение лицензионного соглашения.

Ознакомьтесь с текстом лицензионного соглашения. Для продолжения установки вам необходимо принять предложенные условия лицензионного соглашения и нажать кнопку **Далее**. Текст лицензионного соглашения приведен в разделе Приложение А на стр. 53.

Шаг 3. Выбор каталога для установки

На данном шаге указывается путь к каталогу, в который будет установлен InfoWatch CryptoStorage.

Вы можете указать другой каталог, нажав на кнопку **Изменить…**, и выбрав его в стандартном окне выбора каталога, или введя путь к каталогу в соответствующем поле ввода.

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 4. Завершение установки

После перехода к окну **Программа готова к установке** нажмите на кнопку **Установить**, чтобы начать установку InfoWatch CryptoStorage.

Следуйте дальнейшим указаниям мастера установки, чтобы завершить установку InfoWatch CryptoStorage.

Шаг 5. Активирование продукта

По окончании установки вам будет предложено активировать продукт. Вы можете выбрать один из следующих вариантов:

- Активировать ознакомительную версию на 30 дней.
- Активировать полную версию.

Для активации полной версии требуется получить и установить лицензию по коду активации. Порядок получения и установки лицензии по коду активации приведен в п. 2.3 на стр. 14. После выбора типа активации нажмите на кнопку **Далее**.

Для корректного завершения установки необходимо перезагрузить компьютер. На экран будет выведено соответствующее уведомление.

> **Важная информация!**
>
> Не отключайте питание во время перезагрузки (когда завершается работа Microsoft Windows). Это может привести к ошибке при загрузке операционной системы.
>
> Если это произойдет, то при загрузке операционной системы нажмите клавишу **F8**. Далее из меню загрузки выберите команду **Загрузка последней удачной конфигурации**. После этого заново установите InfoWatch CryptoStorage.

2.3. Управление лицензиями

Для полнофункциональной работы InfoWatch CryptoStorage требуется получить и зарегистрировать коммерческую лицензию.

> **Примечание:**
>
> Активация ознакомительной (Trial) лицензии позволяет в течение 30 дней использовать все возможности InfoWatch CryptoStorage с ограниченной длиной пароля – 1 символ.

По истечении срока действия ознакомительной лицензии, у вас сохранится возможность работы с уже созданными (защищенными) объектами: расшифровывать и получать доступ к информации. Однако, вы не сможете создавать новые защищенные объекты, изменять списки доступа, переустанавливать защиту и получать техническую поддержку.

Чтобы зарегистрировать полученную коммерческую лицензию:

1. Запустите программу управления InfoWatch CryptoStorage, выбрав в меню **Пуск** пункт **Все программы ► InfoWatch CryptoStorage ► Конфигурация CryptoStorage**.
2. В открывшемся окне нажмите кнопку **Лицензии**. На экран будет выведено диалоговое окно **Лицензии** (см. рис. 1).

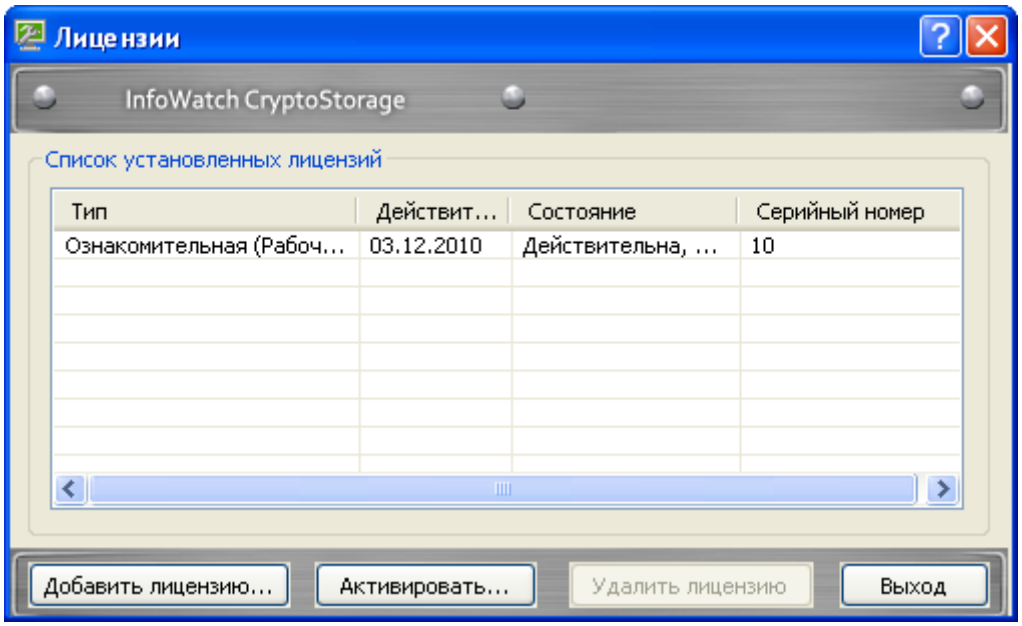

Рисунок 1. Лицензии

В окне представлен список установленных лицензий, где для каждой лицензии указан ее тип, серийный номер, текущее состояние и срок действия.

3. Нажмите кнопку **Добавить лицензию**.
4. В открывшемся диалоговом окне укажите путь к файлу с лицензией и нажмите кнопку **Открыть**.

> **Примечание:**
>
> Добавляемая лицензия должна быть выдана тому же пользователю, что и остальные лицензии в списке, в противном случае добавление лицензии невозможно.

Чтобы удалить ненужную лицензию из списка, выделите ее и нажмите кнопку **Удалить лицензию**.

> **Примечание:**
>
> Ознакомительная (Trial) лицензия не может быть удалена из списка установленных лицензий.

> **Важная информация!**
>
> Не удаляйте из списка действующую коммерческую лицензию, поскольку в этом случае возможности продукта будут ограничены так же, как после окончания действия ознакомительной лицензии.

Для получения и установки лицензии по коду активации, нажмите на кнопку **Активировать**. Порядок активации лицензии по коду рассматривается в п. 2.4 на стр. 15.

После окончания редактирования списка установленных лицензий закройте окно **Лицензии**, нажав кнопку **Выход**.

2.4. Получение и установка лицензии по коду активации

Использование кода активации для получения и установки лицензии возможно как на этапе инсталляции продукта, так и после – при осуществлении управления лицензиями (см. п. 2.3 на стр. 14).

> **Важная информация!**
>
> Чтобы получить лицензию по коду активации, компьютер должен иметь выход в Интернет для обращения на сервис лицензий InfoWatch.

Чтобы получить лицензию по коду активации и установить её:

1. Запустите программу управления InfoWatch CryptoStorage, выбрав в меню **Пуск** пункт **Все программы ► InfoWatch CryptoStorage ► Конфигурация CryptoStorage**.
2. В открывшемся окне нажмите кнопку **Лицензии**.
3. В диалоговом окне **Лицензии** нажмите кнопку **Активировать**. На экран будет выведено диалоговое окно **Активация продукта** (см. рис. 2).

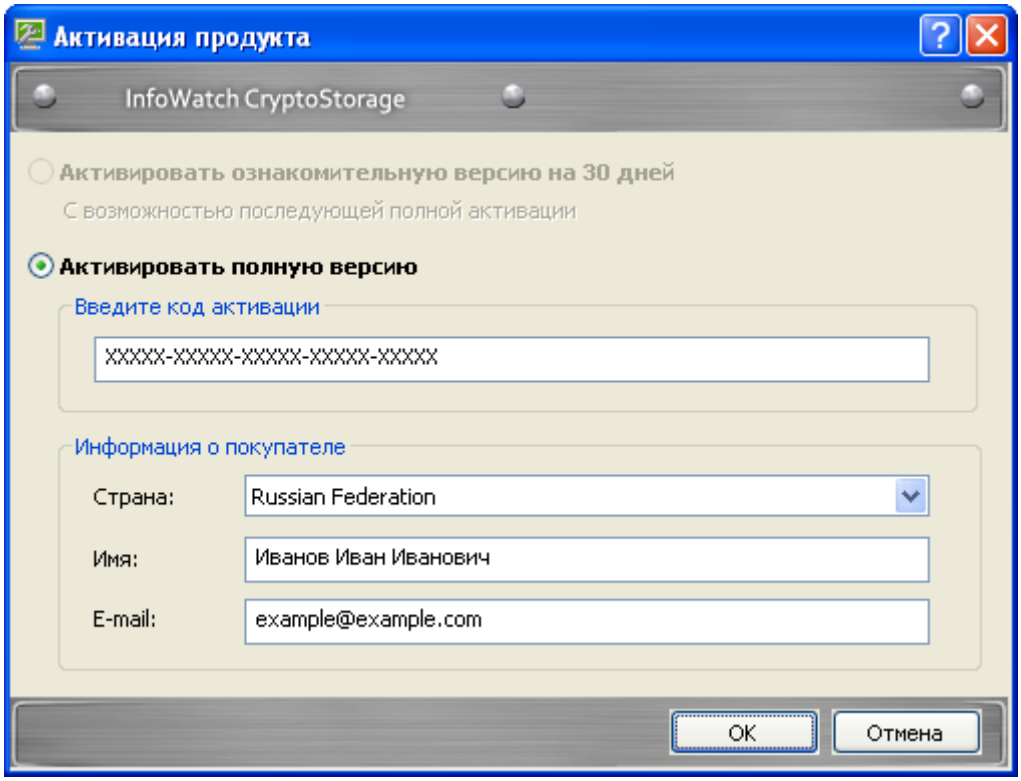

Рисунок 2. Активация продукта

4. Укажите следующую информацию:
   - **Код активации**, состоящий из пяти частей. Каждая часть кода содержит пять символов. В состав кода входят цифры (кроме 0) и заглавные буквы латинского алфавита.

- В области информации о покупателе вы можете указать свою страну проживания, имя и электронный почтовый адрес.

5. Нажмите кнопку **OK**.

Дальнейшие операции по получению и установке лицензии будут выполнены автоматически.

> **Важная информация!**
>
> На каждый код активации выдается только одна лицензия. Не разглашайте код активации своего продукта.

Полученный файл лицензии скопируйте на другой физический жесткий диск или съемный носитель. Эта копия может потребоваться для восстановления системы после сбоя.

2.5. Обновление версии продукта

Новую версию программного продукта InfoWatch CryptoStorage пользователи могут получить по адресу: www.cryptostorage.ru.

Для обновления версии продукта запустите программу установки новой версии.

> **Примечание:**
>
> Более поздняя версия продукта не может быть обновлена на раннюю версию. Для такой замены требуется вначале удалить установленную версию продукта (см. Глава 6 на стр. 52).

ГЛАВА 3. ИНТЕРФЕЙС СИСТЕМЫ

В данном разделе содержится следующая информация:

- *Меню InfoWatch CryptoStorage (п. 3.1 на стр. 17).*
- *Конфигурация InfoWatch CryptoStorage (п. 3.2 на стр. 17).*

3.1. Меню InfoWatch CryptoStorage

Доступ к функциям Системы осуществляется через контекстное меню проводника Microsoft Windows.

Чтобы открыть меню InfoWatch CryptoStorage:

1. Выделите нужный объект (папку, контейнер, логический диск или съемный носитель) и щелкните правой кнопкой мыши.

   После этого на экране раскроется контекстное меню выделенного объекта.

2. В раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage**.

   Данный пункт меню содержит подменю, состав которого зависит от типа объекта и от наличия/отсутствия защиты для данного объекта (см. рис. 3).

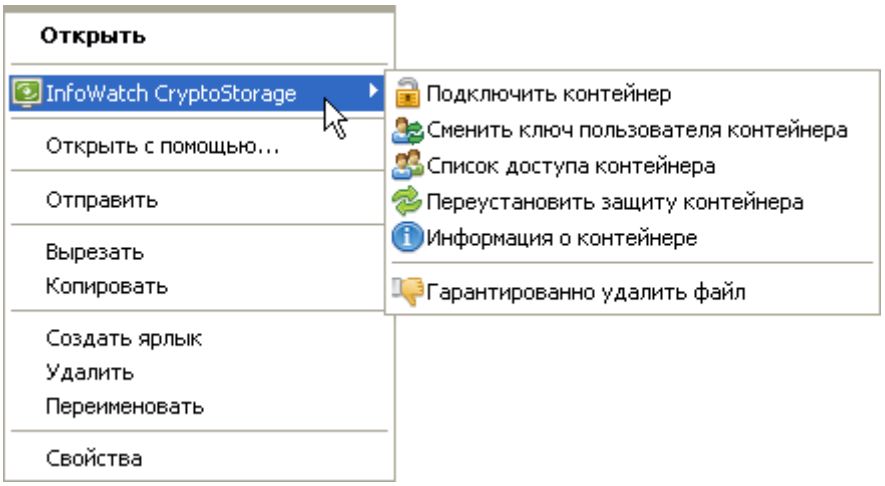

Рисунок 3. Контекстное меню защищенного объекта

Чтобы создать защищенную папку или контейнер,

щелкните правой кнопкой мыши в любом свободном месте открытой папки или рабочего стола и в раскрывшемся контекстном меню выберите команду **Создать ► Папка InfoWatch CryptoStorage** или **Создать ► Контейнер InfoWatch CryptoStorage**.

3.2. Конфигурация InfoWatch CryptoStorage

Чтобы запустить программу управления InfoWatch CryptoStorage,

в меню **Пуск** выберите пункт **Все программы ► InfoWatch CryptoStorage ► Конфигурация CryptoStorage**.

В результате появится окно программы управления (рис. 4).

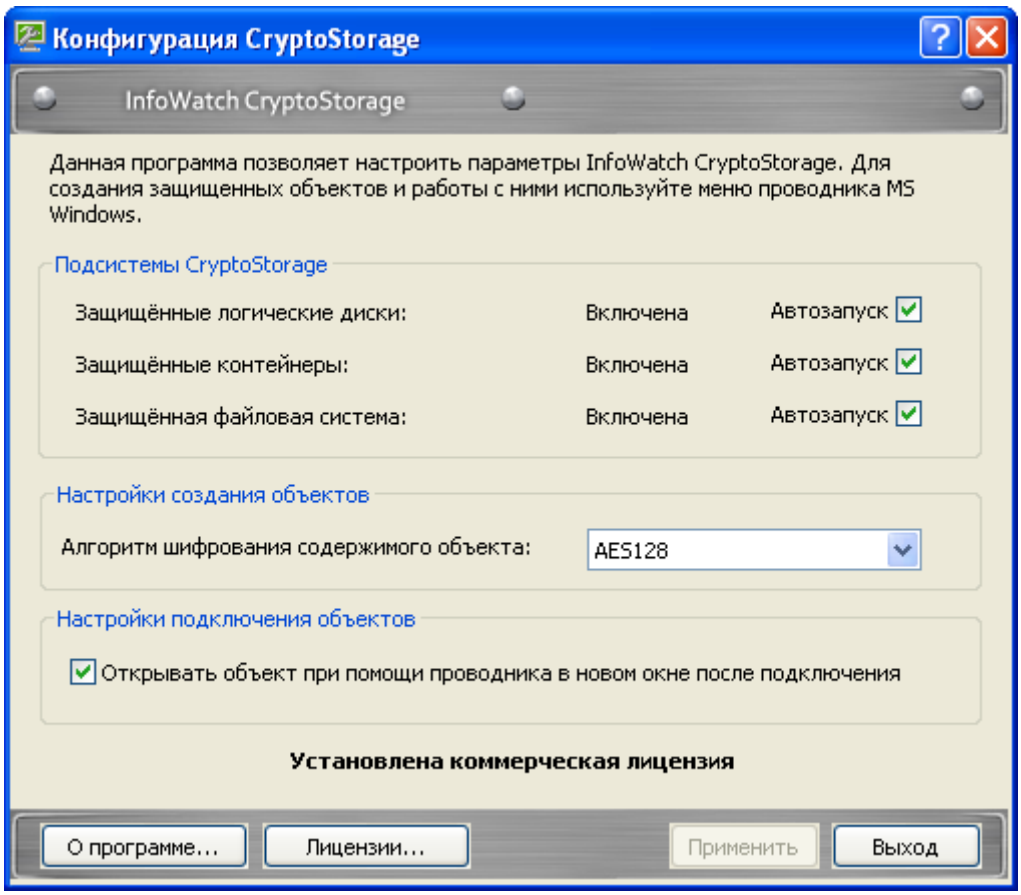

Рисунок 4. Окно программы управления

Программа позволяет выполнять следующие операции:

- Конфигурирование подсистем (см. Глава 5 на стр. 50);
- Выбор алгоритма шифрования содержимого защищаемых объектов;
- Возможность открытия объекта после подключения в отдельном окне с помощью Проводника;
- Работа с лицензиями, активация (см. п. 2.3 на стр. 14).

ГЛАВА 4. ЗАЩИТА ДАННЫХ. РАБОТА С ЗАЩИЩЕННЫМИ ОБЪЕКТАМИ

Данная глава описывает работу со следующими защищенными объектами:

- *Защищенные папки (см. п. 4.1 на стр. 19);*
- *Защищенные логические разделы жесткого диска и съемные носители (см. п. 4.2 на стр. 28);*
- *Защищенные контейнеры (см. п. 4.3 на стр. 38).*

Также в главе описаны следующие возможности при работе с защищенными объектами:

- *Гарантированное удаление защищенных и незащищенных объектов (см. п. 4.4 на стр. 49).*

4.1. Работа с защищенными папками

В данном разделе содержится следующая информация:

- *Особенности защиты папок (п. 4.1.1 на стр. 19).*
- *Создание защищенной папки (п. 4.1.2 на стр. 20).*
- *Правила работы с защищенными папками (п. 4.1.3 на стр. 21).*
- *Подключение защищенной папки (п. 4.1.4 на стр. 22).*
- *Просмотр информации о защищенной папке (п. 4.1.5 на стр. 22).*
- *Отключение защищенной папки (п. 4.1.6 на стр. 23).*
- *Управление доступом к защищенным папкам (п. 4.1.7 на стр. 23).*
- *Переустановка защиты на папку (п. 4.1.8 на стр. 27).*
- *Смена параметров пользователя для доступа к защищенной папке (п. 4.1.9 на стр. 28).*

4.1.1. Особенности защиты папок

Условия создания защищенной папки:

- Работа с защищенными папками возможна, если на компьютере с установленной InfoWatch CryptoStorage запущена подсистема *Защищенные папки* (информацию о порядке отключения и включения подсистем см. Глава 5 на стр. 50). По умолчанию подсистема запущена.
- Устройство (жесткий диск или съемный носитель), на котором создается защищенная папка, не должно быть защищено от записи. Пользователь, создающий защищенную папку, должен иметь права на создание папки
- Защищенная папка может быть создана только в файловой системе NTFS.
- Защищенная папка не может быть создана в защищенной папке InfoWatch CryptoStorage или в папке, защищенной EFS (шифрующей файловой системой, входящей в состав операционной системы Microsoft Windows).
- Длина полного имени папки не превышает 255 символов.

Возможна работа с защищенными папками внутри локальной сети Microsoft Windows. Для этого на удаленном компьютере, где физически хранится информация, не должна быть запущена подсистема *Защищенные папки* (о подсистеме см. Глава 5 на стр. 50), а папки должны храниться на томе с файловой системой NTFS.

4.1.2. Создание защищенной папки

> **Важная информация!**
>
> Перед началом работы ознакомьтесь с особенностями создания защищенных папок, описанными в п. 4.1.1 на стр. 19.

Защищенную папку можно создать на жестком диске или на съемном носителе. Кроме того, защищенная папка может быть создана внутри другого защищенного объекта (логического диска или защищенного контейнера).

> **Примечание:**
>
> Если папка создается внутри другого защищенного объекта, то перед созданием папки необходимо подключить этот объект.

Чтобы создать защищенную папку:

1. Щелкните правой кнопкой мыши в любом свободном месте открытой папки или рабочего стола и в раскрывшемся контекстном меню выберите команду **Создать ► Папка InfoWatch CryptoStorage**.

   Появится диалоговое окно **Создание защищенной папки** (рис. 5).

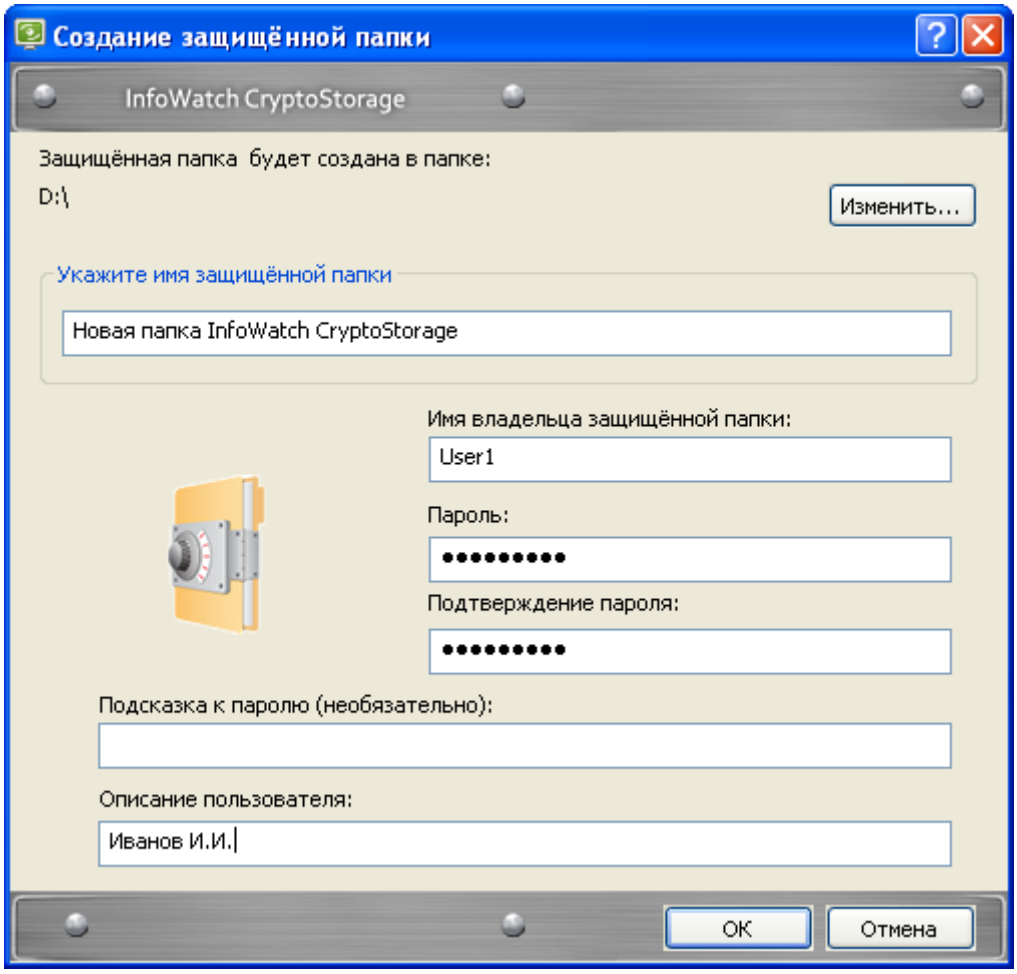

Рисунок 5. Создание защищенной папки

2. Укажите параметры создаваемой защищенной папки:

   - **Защищенная папка будет создана в папке**. По умолчанию указывается папка, в которой было вызвано контекстное меню. Чтобы указать другую папку, нажмите на кнопку **Изменить** и выберите необходимую папку в стандартном окне Проводника.
   - **Укажите имя защищенной папки**. В процессе работы вы можете изменять имена защищенных папок средствами операционной системы.

- Параметры, которые будут использоваться владельцем для доступа к защищенному контейнеру: **Имя владельца защищенной папки**, **Пароль**, **Подтверждение пароля, Подсказка к паролю**. Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.
- **Описание пользователя**. Данное описание будет отображаться в списке доступа к объекту (подробнее см. п. 4.1.7.2 на стр. 24), и дальнейшему изменению не подлежит.

3. Нажмите на кнопку **OK**.

В результате будет создана защищенная папка. После создания она находится в подключенном состоянии и готова к использованию.

4.1.3. Правила работы с защищенными папками

При работе с защищенными папками необходимо учитывать следующее:

- Все файлы и папки, находящиеся внутри защищенной папки, зашифрованы и являются защищенными.
- Выполнение любых действий (чтение, запись, переименование, архивирование, удаление и т. п.) непосредственно над защищенной папкой возможно только после подключения этой папки.
- Подключенная папка доступна всем пользователям и программам, которые могут работать с компьютером локально от имени подключившего. Доступ к защищенным папкам по сети запрещен Системой.

> **Примечание:**
>
> Рекомендуется отключать защищенную папку сразу после того, как работа с ней завершена.

- Копии или перемещенные файлы и папки имеют защиту только тех объектов, в которых находятся.

> **Примечание:**
>
> Копии или перемещенные файлы и папки, находящиеся в незащищенных Системой объектах, незащищены.

- Система не позволяет выполнять непосредственно с защищенными папками и их содержимым следующие действия: удаление в корзину, перемещение в рамках одного логического диска файлов и папок, содержащих файлы.

> **Примечание:**
>
> При попытке переместить в рамках одного логического диска защищённую папку, содержащую файлы, исходная папка останется без изменений. В Windows XP и Windows 2003 по месту перемещения будет создана пустая папка с именем исходной и имеющая защиту того объекта, в котором она находится.
>
> Некоторые файловые менеджеры, например Total Commander, при перемещении файлов и папок в рамках одного логического диска могут использовать копирование с последующим удалением исходных объектов. В этом случае перемещение возможно, и перемещенные файлы и папки получают защиту тех объектов, в которых находятся.

- В рамках одного логического диска можно перемещать незащищенные папки, содержащие защищенные подпапки, со всем содержимым в незащищенные папки. В этом случае для перемещения не требуется подключение объектов, и все свойства защищенных объектов сохраняются.
- Может быть выполнено перемещение в корзину незащищенной папки, содержащей защищенные подпапки, если все защищенные объекты в папке подключены.

> **Примечание:**
>
> Перемещенную таким образом в корзину защищенную папку можно удалить или восстановить. Если не проводилась перезагрузка компьютера (Shut Down) или завершение сеанса (Log Off), то при восстановлении все защищенные объекты этой папки будут подключены. В операционных системах Windows XP и Windows 2003 после перезагрузки компьютера или завершения сеанса помещенную в корзину папку удалить невозможно: возможно только восстановление. Total Commander не может выполнить перемещения в корзину такой папки.

4.1.4. Подключение защищенной папки

Работа (чтение, запись, переименование, копирование, удаление и т. д.) с защищенной папкой становится возможна только при условии, что она подключена.

Чтобы подключить папку:

1. Щелкните правой кнопкой мыши по защищенной папке и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Подключить папку**.
2. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** для доступа к защищенной папке
3. Нажмите на кнопку **OK**.

4.1.5. Просмотр информации о защищенной папке

Просмотр информации о защищенной папке доступен только её владельцу.

Чтобы просмотреть свойства защищенной папки:

1. Щелкните правой кнопкой мыши по защищенной папке, сведения о которой нужно просмотреть, и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Информация о защищенной папке**.
2. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенной папки. Затем нажмите на кнопку **OK**.

В результате на экран будет выведено диалоговое окно, содержащее информацию о выбранной защищенной папке (рис. 6).

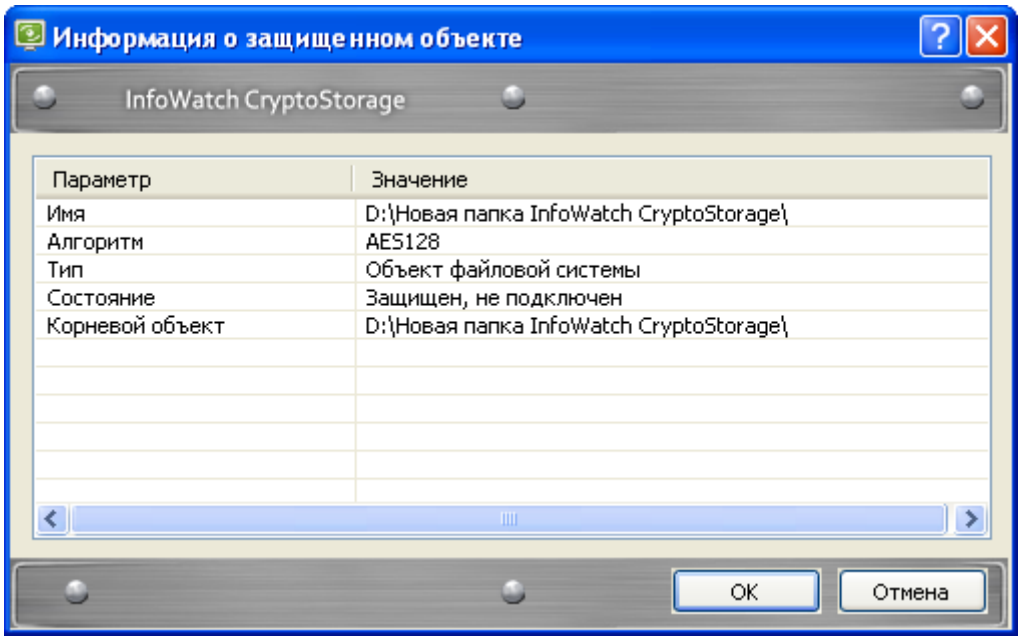

Рисунок 6. Просмотр информации о защищенной папке

Атрибуты защищенной папки перечислены в таблице 4.

Таблица 4. Атрибуты защищенной папки

Атрибут	Описание
Имя	Полное имя объекта
Алгоритм	Тип защиты
Тип	Тип защищенного объекта – объект файловой системы
Состояние	Состояние защиты объекта
Корневой объект	Полное имя объекта, являющегося родительским для данного объекта (для объектов верхнего уровня выводится имя объекта)

4.1.6. Отключение защищенной папки

После отключения защищенная папка переводится в состояние, при котором дальнейшая работа с ней невозможна до следующего подключения.

> **Важная информация!**
>
> Приложения могут сохранять доступ к данным до завершения всех операций над этими данными даже после отключения. Поэтому отключение необходимо выполнять только после сохранения всех изменений и завершения работы с папкой

Чтобы отключить защищенную папку,

щелкните правой кнопкой мыши по папке, работу с которой нужно завершить, и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Отключить папку**.

Если работа производится с несколькими защищенными объектами одновременно, то на отключение всех объектов потребуется некоторое время. Однако в ряде случаев могут возникнуть экстренные ситуации, когда требуется отключить все защищенные объекты одновременно. С этой целью можно выполнить перезагрузку компьютера (предварительно сохранив сделанные изменения). После перезагрузки компьютера все защищенные объекты будут отключены. Можно отключить все защищенные папки, выполнив завершение сеанса (Log Off).

4.1.7. Управление доступом к защищенным папкам

В системе InfoWatch CryptoStorage предусмотрен многопользовательский доступ к объектам.

Каждый защищенный объект имеет свой список доступа. После создания защищенного объекта в списке доступа содержится информация только о владельце защищенного объекта (имя владельца объекта отмечено буквой (O)).

Владелец защищенного объекта может редактировать список доступа, добавляя/удаляя пользователей.

Подключить защищенный объект могут:

- владелец этого объекта;
- пользователи, включенные владельцем в список доступа.

Доступ к содержимому защищенной папки имеет только тот, кто его подключил.

При организации доступа к защищенным папкам необходимо учитывать следующее:

- Для управления списками доступа защищенной папки и её подпапок, она должна быть подключена владельцем.
- Папка, создаваемая внутри защищенной папки, наследует все свойства родительской папки. После создания вложенной папки можно отредактировать список доступа, унаследованный от родительской папки.

- Пользователь, добавляемый в список доступа вложенной папки, автоматически добавляется в список доступа родительской папки.

Информация по работе со списком доступа содержится в подразделах:

- *Иерархия доступа (п. 4.1.7.1 на стр. 24).*
- *Просмотр списка доступа (п. 4.1.7.2 на стр. 24).*
- *Добавление нового пользователя (п. 4.1.7.3 на стр. 25).*
- *Добавление существующего пользователя (п. 4.1.7.4 на стр. 26).*
- *Удаление пользователя из списка доступа (п. 4.1.7.5 на стр. 27).*

4.1.7.1. Иерархия доступа

В защищенной папке каждая подпапка имеет свой список доступа. Структура списков доступа в защищенной папке организована так, что пользователи, допущенные к внутренней папке, обязательно имеют доступ и к внешней папке. При этом две папки, расположенные внутри одной и той же папки, могут иметь разные списки доступа. В результате корневая защищенная папка имеет максимально полный список доступа: в нем присутствует любой пользователь, допущенный хотя бы к одной внутренней папке.

Таким образом, можно создавать иерархическую структуру доступа и предоставлять пользователю доступ ко всем его подпапкам при подключении корневой защищенной папки.

Иерархическая структура доступа на основе защищенных папок (по сравнению со структурой из вложенных друг в друга защищенных объектов) имеет следующие преимущества:

- Доступ к вложенной подпапке в защищенной папке не требует отдельного подключения ее и всех предшествующих подпапок.
- Скорость доступа к подпапке не зависит от глубины ее расположения, в то время как переход к работе с вложенным защищенным объектом связан с дополнительными затратами времени и ресурсов.

При копировании папки в защищенную папку, скопированная папка и все ее подпапки получают список доступа, равный списку доступа той подпапки, куда они скопированы.

4.1.7.2. Просмотр списка доступа

Чтобы открыть список доступа к защищенной папке:

1. Подключите необходимую защищенную папку (см. п. 4.1.4 на стр. 22).
2. Щелкните правой кнопкой мыши по защищенной папке и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Список доступа папки**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенной папки. Затем нажмите на кнопку **OK**.

В результате на экран будет выведено диалоговое окно с информацией о пользователях, имеющих доступ к защищенной папке (см. рис. 7).

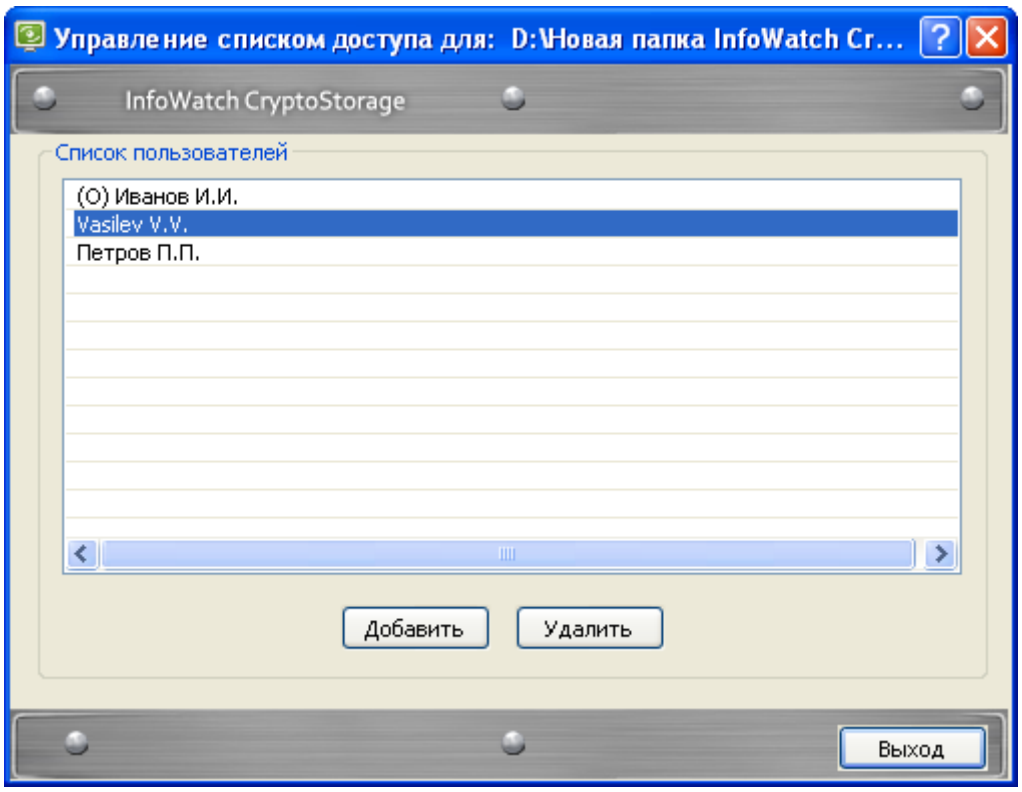

Рисунок 7. Список пользователей, имеющих доступ к защищенной папке

Первоначально в список доступа включен только владелец объекта. В процессе работы можно редактировать список доступа путем добавления/удаления пользователей.

4.1.7.3. Добавление нового пользователя

Чтобы добавить нового пользователя в список доступа к защищенной папке или к подпапке в защищенной папке:

1. Откройте список доступа к защищенной папке или подпапке в защищенной папке (п. 4.1.7.2 на стр. 24).
2. В диалоговом окне списка доступа нажмите на кнопку **Добавить**.

   На экран будет выведено диалоговое окно выбора добавляемого пользователя (см. рис. 8).

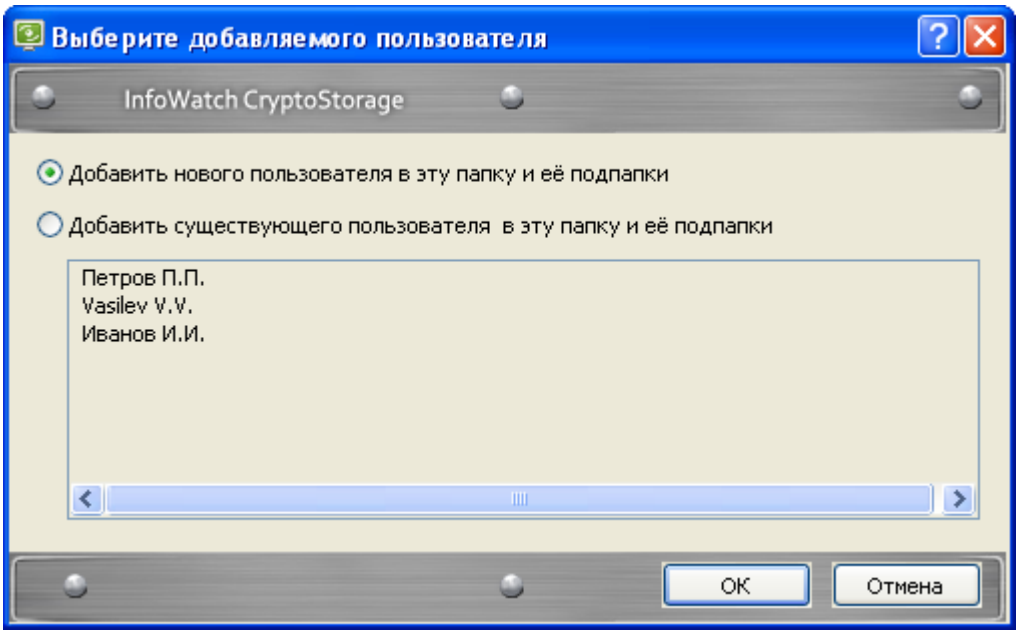

Рисунок 8. Добавление пользователя в список доступа

3. Установите флажок в поле **Добавить нового пользователя…** и нажмите на кнопку **OK**.
4. В открывшемся диалоговом окне укажите параметры для доступа нового пользователя к защищенной папке:
   - **Имя пользователя**.
   - **Пароль**, **Подтверждение пароля, Подсказка к паролю**. Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.
   - **Описание пользователя**. Данное описание будет отображаться в списке доступа к объекту (подробнее см. п. 4.1.7.2 на стр. 24), и дальнейшему изменению не подлежит.
5. Нажмите на кнопку **OK**.

В результате новый пользователь будет добавлен в список доступа к указанной подпапке и всем ее подпапкам, а также ко всем папкам, лежащим на пути из корневой папки к указанной.

4.1.7.4. Добавление существующего пользователя

При определении списка доступа к подпапке защищенной папки вы можете добавлять в него пользователей, которые уже допущены к корневой защищенной папке.

Чтобы разрешить пользователю доступ к подпапке защищенной папки:

1. Откройте список доступа к данной подпапке защищенной папки (см. п. 4.1.7.2 на стр. 24).
2. В диалоговом окне списка доступа нажмите на кнопку **Добавить**.

   После этого на экран будет выведено диалоговое окно выбора добавляемого пользователя (см. рис. 9).

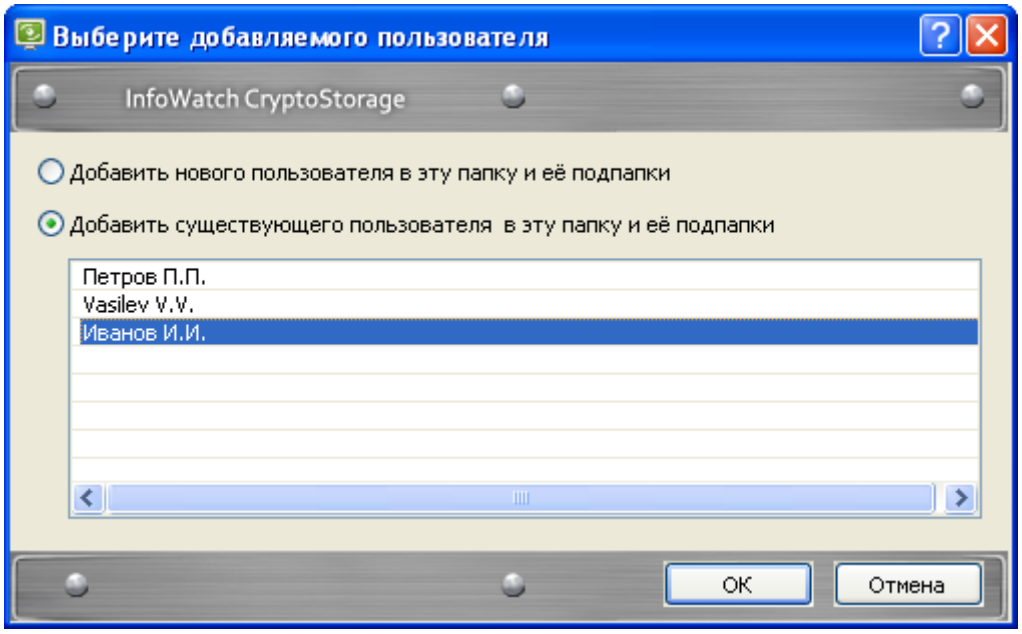

Рисунок 9. Выбор пользователя, добавляемого в список доступа

3. Установите флажок в поле **Добавить существующего пользователя…**, затем из списка пользователей, имеющих доступ к корневой защищенной папке, выберите имя пользователя, которому нужно дать доступ к подпапке, и нажмите на кнопку **OK**.

В результате выбранный пользователь будет добавлен в список доступа к указанной подпапке и всем ее подпапкам, а также ко всем папкам, лежащим на пути из корневой папки к указанной.

В ходе добавления пользователя в списки доступа к защищенной папке может возникнуть необходимость прервать этот процесс или процедура может быть прервана вследствие нештатной ситуации (например, при неожиданном отключении компьютера). В этом случае для завершения добавления пользователя повторите описанные выше действия. Присутствие пользователя в списке доступа рассматриваемой папки значения не имеет: пользователь мог не попасть в списки доступа всех ее подпапок.

4.1.7.5. Удаление пользователя из списка доступа

> **Важная информация!**
>
> Пользователь, удаленный из списка доступа к родительской защищенной папке, теряет доступ ко всем вложенным подпапкам.

Чтобы удалить пользователя из списка доступа к подпапке в защищенной папке:

1. Откройте список доступа к данной защищенной подпапке (см. п. 4.1.7.2 на стр. 24).
2. В списке доступа к защищенному объекту (см. рис. 7) выделите имя пользователя, которого нужно удалить из списка.
3. Нажмите на кнопку **Удалить**.

После выполнения этой операции рекомендуется переустановить защиту на объект.

В ходе добавления пользователя в списки доступа к защищенной папке может возникнуть необходимость прервать этот процесс или процедура может быть прервана вследствие нештатной ситуации (например, при неожиданном отключении компьютера). В этом случае пользователь будет удален лишь из части защищенной папки. Чтобы завершить удаление пользователя, который продолжает оставаться в списке доступа, повторите процедуру его удаления из списка доступа для данной папки.

4.1.8. Переустановка защиты на папку

Переустановку защиты рекомендуется проводить в случае возможной компрометации внутренней ключевой информации защищенного объекта: например, после удаления пользователя из списка доступа. В результате переустановки защиты объект перешифровывается на новом ключе, что делает невозможным доступ к объекту по скомпрометированной ключевой информации.

При переустановке защиты на корневую защищённую папку возможна замена криптографического алгоритма: алгоритм заменится на выбранный в программе Конфигурации (см. п. 3.2 на стр. 17). При переустановке защиты на подпапку, замены алгоритма не производится: он остаётся таким же, как и на всей защищенной папке.

Переустановка защиты на папку выполняется владельцем объекта.

> **Важная информация!**
>
> Не работайте с защищенной папкой в процессе переустановки защиты: на используемых папках переустановка защиты не осуществляется.

Чтобы переустановить защиту на папку:

1. Щелкните правой кнопкой мыши по защищенной папке и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Переустановить защиту папки**.
2. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

Начнется процесс переустановки защиты на папку. Работать в это время с защищенной папкой или её содержимым нельзя.

> **Примечание:**
>
> Если в ходе переустановки защиты на папку возникнет необходимость прервать этот процесс (для этого нажмите на кнопку **Стоп** в диалоговом окне, где отображается процесс переустановки защиты), или переустановка будет прервана вследствие нештатной ситуации (например, при неожиданном отключении компьютера), то содержимое защищенной папки может частично оставаться зашифрованным на старом ключе. Для полного перешифрования содержимого папки на новом ключе необходимо повторить процедуру переустановки защиты на папку.

По окончании переустановки защиты папка останется защищенной и подключенной, и с ней можно будет работать.

4.1.9. Смена параметров пользователя для доступа к защищенной папке

Параметры доступа состоят из имени и пароля пользователя. Описание пользователя изменению не подлежит.

Чтобы изменить параметры доступа к защищенной папке:

1. Подключите необходимую защищенную папку (см. п. 4.1.4 на стр. 22).
2. Щелкните правой кнопкой мыши по подключенной папке и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Сменить ключ пользователя папки**.
3. В открывшемся диалоговом окне укажите текущие параметры авторизации, необходимые для доступа к защищенной папке: **Имя пользователя** и **Пароль**. Затем нажмите на кнопку **OK**.
4. В открывшемся диалоговом окне с настройками новых параметров авторизации укажите новые значения для параметров **Имя пользователя**, **Новый пароль** и **Подтверждение пароля**. Затем нажмите на кнопку **OK**.

> **Примечание:**
>
> Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.

В результате параметры доступа к защищенной папке будут изменены, но описание пользователя останется прежним. Новые параметры доступа вступят в силу при следующем подключении папки.

4.2. Работа с защищенными контейнерами

В данном разделе содержится следующая информация:

4.2.1. Создание контейнера

Контейнеры можно создавать на жестком диске, на съемном носителе или на локальных сетевых ресурсах. Кроме того защищенный контейнер может быть создан внутри другого защищенного объекта (логического диска, съемного устройства, папки, защищенного контейнера).

Ограничения на создание защищенных контейнеров:

- Работа с защищенными контейнерами возможна, только если на компьютере с установленной системой InfoWatch CryptoStorage запущена подсистема *Защищенные контейнеры*.
- Устройство (жесткий диск или съемный носитель), на котором создается защищенный контейнер, не должно быть защищено от записи.
- Пользователь, создающий контейнер, должен иметь права на создание файлов.

- Если контейнер создается внутри другого защищенного объекта, то перед созданием контейнера необходимо подключить этот объект.
- Создание защищенных контейнеров на CD/DVD-дисках не поддерживается. Однако эти носители могут использоваться для размещения готовых защищенных контейнеров.

Чтобы создать контейнер:

1. Откройте папку (на жестком диске или съемном носителе), в которой нужно создать защищенный контейнер.
2. Щелкните правой кнопкой мыши в любом свободном месте открытой папки или рабочего стола и в раскрывшемся контекстном меню выберите команду **Создать ► Контейнер InfoWatch CryptoStorage**.

   На экран будет выведено диалоговое окно **Создание защищенного контейнера** (см. рис. 10).

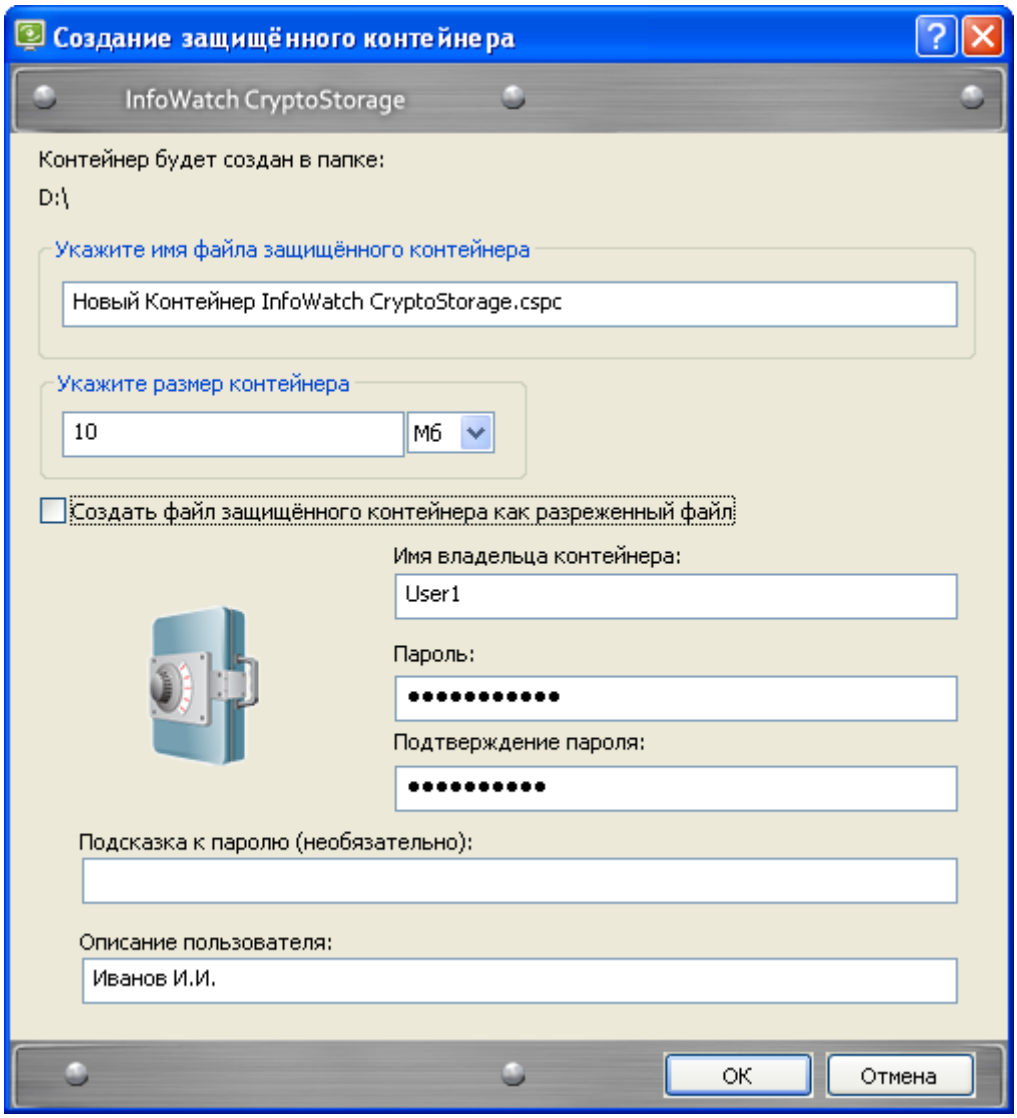

Рисунок 10. Создание защищенного контейнера

3. Укажите параметры создаваемого защищенного контейнера:
   - **Укажите имя файла защищенного контейнера**. Имя и расширение файла защищенного контейнера.

     По умолчанию имя файла контейнера имеет расширение `.cspc` (при установке InfoWatch CryptoStorage файлы с таким расширением регистрируются в операционной системе как контейнеры InfoWatch CryptoStorage). В операционной системе такие файлы отображаются значком .

     Если вместо `.cspc` указать расширение, незарегистрированное в операционной системе, то файл контейнера будет отображаться, как файл неизвестного формата.

> **Примечание:**
>
> Контейнеры, файлы которых имеют расширение `.cspc`, можно подключать, дважды щелкнув на названии файла левой кнопкой мыши (см. п. 4.2.5 на стр. 31).
>
> В процессе работы вы можете изменять имена и расширения файлов контейнеров средствами операционной системы.

- **Укажите размер контейнера**. Размер контейнера может быть задан в мегабайтах или гигабайтах. Выберите единицу измерения и укажите необходимый размер.

> **Важная информация!**
>
> Если контейнер планируется форматировать для файловой системы NTFS (независимо от файловой системы диска, на котором создается контейнер), то размер файла такого контейнера должен составлять не менее 12Мб.

Если файл контейнера создается на томе с файловой системой NTFS, то вы можете выбрать разреженный тип файла контейнера.

> **Примечание:**
>
> Если файл контейнера создается как разреженный, то его размер на диске (см. свойства файла в проводнике Microsoft Windows) увеличивается по мере заполнения. Создание файла такого типа помогает экономить дисковое пространство. Копии разреженного файла этим свойством не обладают и имеют максимальный заданный размер. Информацию о работе с контейнерами, размер файлов которых увеличивается по мере заполнения, см. п. 4.2.6 на стр. 32.

- Параметры, которые будут использоваться владельцем для доступа к защищенному контейнеру: **Имя владельца контейнера**, **Пароль**, **Подтверждение пароля, Подсказка к паролю**. Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.
- **Описание пользователя**. Информация о владельце создаваемого контейнера. Данное описание будет отображаться в списке доступа к объекту (подробнее см. п. 4.2.9.1 на стр. 34).

4. Когда все необходимые параметры будут заданы, нажмите на кнопку **OK**.

После того, как защищенный контейнер будет создан, вам будет предложено подключить его (см. п. 4.2.5 на стр. 31) и отформатировать (см. п. 4.2.6 на стр. 32).

4.2.2. Подготовка контейнера к работе

Для подготовки контейнера к работе необходимо:

1. Подключить контейнер как логический диск (см. п. 4.2.5 на стр. 31).
2. Отформатировать логический диск, к которому подключен защищенный контейнер (см. п. 4.2.6 на стр. 32).

4.2.3. Защита от удаления контейнера

Поскольку защищенный контейнер представляет собой обычный файл, он может быть удален любым пользователем. Предотвратить несанкционированное удаление защищенного контейнера можно, поместив файл контейнера в защищенную папку или на защищенный логический диск.

> **Важная информация!**
>
> Данный вид защиты действует только на компьютере с установленной системой InfoWatch CryptoStorage.

4.2.4. Правила работы с защищенными контейнерами

Выполнение любых действий над содержимым защищенного контейнера возможно только после подключения.

> **Важная информация!**
>
> Подключение и работа с защищенными контейнерами возможны, только если на компьютере с установленной системой InfoWatch CryptoStorage запущена подсистема *Защищенные контейнеры*.

При работе с защищенным контейнером необходимо учитывать, что все файлы и папки, находящиеся внутри защищенного контейнера, зашифрованы и являются защищенными. Однако перемещение таких объектов за пределы контейнера приводит к снятию защиты.

4.2.5. Подключение контейнера

Работа с защищенным контейнером возможна только после подключения.

Чтобы подключить защищенный контейнер:

1. Выделите защищенный контейнер.
2. Щелкните правой кнопкой мыши по выделенному контейнеру и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Подключить контейнер**.

   Если файл контейнера имеет расширение `.cspc` (отображается значком), то вы можете подключить контейнер, дважды щелкнув по нему левой кнопкой мыши.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** пользователя защищенного контейнера. Затем нажмите **OK**.

   На экран будет выведено диалоговое окно **Подключение контейнера** (см. рис. 11).

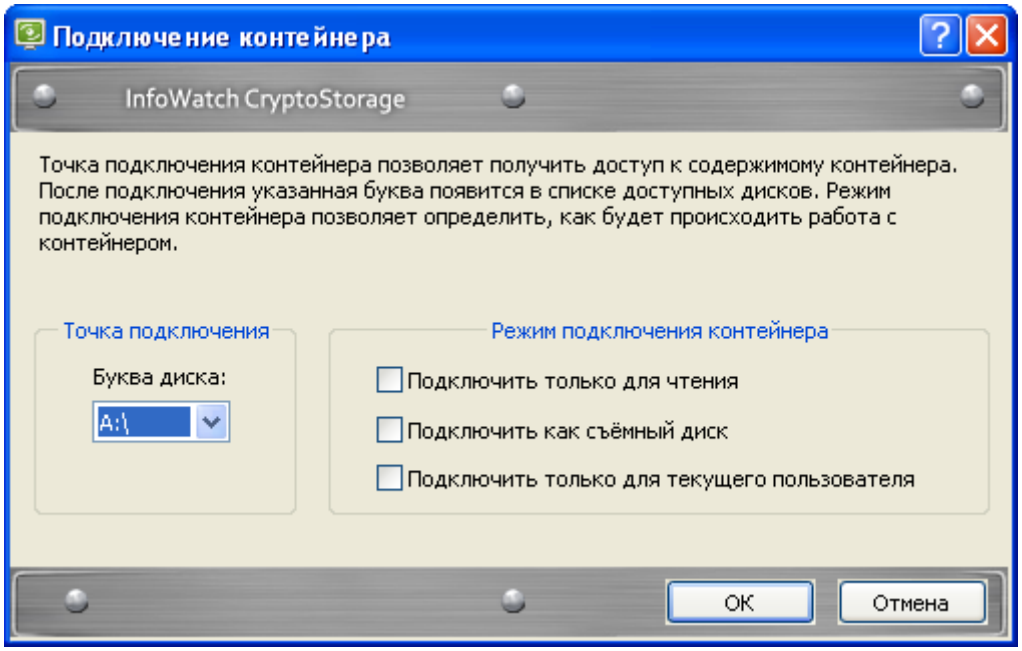

Рисунок 11. Подключение защищенного контейнера

4. В открывшемся диалоговом окне укажите параметры подключения:
   - **Точка подключения**. Выберите любую незанятую букву логического диска. После подключения содержимое контейнера будет открыто на логическом диске с этой буквой.
   - **Режим подключения**:
     - **Подключить только для чтения**. Если флажок в данном поле установлен, все содержимое защищенного контейнера доступно только для чтения. Запись и удаление данных не выполняется.

> **Примечание:**
>
> Данный флажок необходимо установить, если файл защищенного контейнера будет одновременно подключаться на нескольких компьютерах.

Флажок устанавливается автоматически и не может быть снят, если контейнер уже подключен в режиме «*только для чтения*» другим пользователем, или файл контейнера имеет атрибут **Только чтение**.

- **Подключить как съемный диск**. По умолчанию точкой монтирования защищенного контейнера является съемный диск (отображается в списке съемных дисков в окне **Мой компьютер**). Однако если флажок в данном поле не установлен, то защищенный контейнер будет смонтирован как фиксированный диск (отображается в списке жестких дисков в окне **Мой компьютер**).
- **Подключить только для текущего пользователя**. Если флажок в данном поле установлен, то диск, в который подключен контейнер, будет виден только в сеансе подключившего пользователя и не будет доступен из сети. Подключение для текущего пользователя возможно только если контейнер подключен как съемный диск.

При подключении созданного, но ещё не отформатированного контейнера выбор режима подключения недоступен.

5. Когда все параметры будут заданы, нажмите на кнопку **OK**.

При подключении созданного, но ещё не отформатированного, контейнера вам будет предложено произвести форматирование (см. п. 4.2.6 на стр. 32).

4.2.6. Форматирование контейнера

> **Важная информация!**
>
> В процессе форматирования диска, к которому подключен защищенный контейнер, все данные, хранящиеся в этом контейнере, будут уничтожены.

Форматирование защищенного контейнера выполняется стандартными средствами операционной системы Microsoft Windows. При настройке параметров форматирования необходимо учитывать следующее:

- Для форматирования контейнера его необходимо подключить как логический диск (см. п. 4.2.5 на стр. 31). Режим **Подключить только для текущего пользователя** должен быть отключён.
- При полном форматировании файл защищенного контейнера будет иметь размер, указанный в процессе создания этого контейнера.
- При быстром форматировании и выборе файловой системы FAT, файл защищенного контейнера всегда принимает минимальный размер, который будет увеличиваться по мере заполнения контейнера, что позволяет экономить свободное дисковое пространство.
- Если при быстром форматировании контейнера выбирается файловая система NTFS, то для минимизации занимаемого дискового пространства он должен быть создан как разреженный файл (см. п. 4.2.1 на стр. 28). Иначе, даже при быстром форматировании размер файла контейнера будет равен максимальному, указанному в процессе создания.

> **Примечание:**
>
> При любом форматировании размер логического диска, в который подключается защищенный контейнер, всегда равен размеру, выбранному при создании этого контейнера; изменяется только размер самого файла контейнера.

4.2.7. Просмотр информации о защищенном контейнере

Просмотр информации о защищенном контейнере доступен только его владельцу.

Чтобы просмотреть свойства защищенного контейнера:

1. Выделите необходимый защищенный контейнер либо диск, к которому он подключен.
2. Щелкните правой кнопкой мыши по выделенному объекту и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Информация о контейнере**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

В результате на экран будет выведено диалоговое окно, содержащее информацию о выбранном защищенном контейнере (рис. 12).

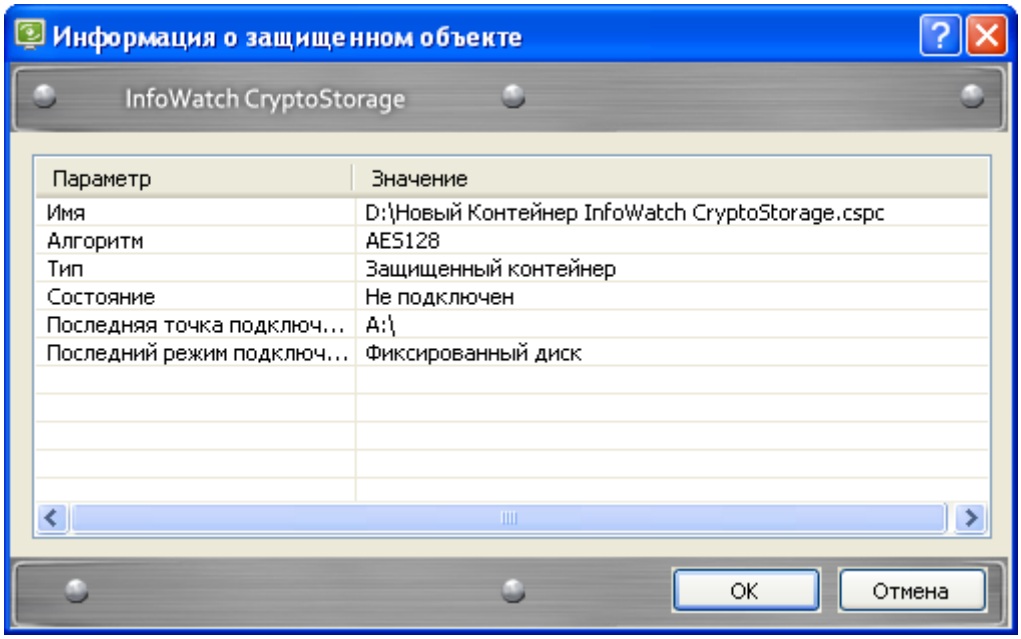

Рисунок 12. Просмотр информации о защищенном контейнере

Атрибуты защищенного контейнера перечислены в таблице 5.

Таблица 5. Атрибуты защищенного контейнера

Атрибут	Описание
Имя	Полное имя объекта
Алгоритм	Тип защиты
Тип	Тип защищенного объекта – защищенный контейнер
Состояние	Состояние защиты объекта
Последняя/Текущая точка подключения	Папка или диск, к которому был подключен контейнер в последний раз или подключен в настоящее время
Последний режим подключения	Параметры, подключения, выбранные при последнем подключении.

4.2.8. Отключение контейнера

Перед отключением защищенного контейнера необходимо завершить работу со всеми содержащимися в нем объектами (файлами, папками, вложенными защищенными контейнерами).

Если вы подключили тома в папки контейнера, то перед отключением контейнера необходимо отключить тома, подключенные в папки контейнера. В противном случае после отключения контейнера вы не сможете получить доступ к этим томам через данные точки подключения.

Чтобы отключить защищенный контейнер:

1. Выделите диск, к которому подключен защищенный контейнер, либо файл защищенного контейнера.
2. Щелкните правой кнопкой мыши по выделенному контейнеру или диску и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Отключить контейнер**.

Если работа производится с несколькими защищенными объектами одновременно, то на отключение всех объектов потребуется некоторое время. Однако в ряде случаев могут возникнуть экстренные ситуации, когда требуется отключить все защищенные объекты одновременно. С этой целью можно выполнить перезагрузку компьютера (предварительно сохранив сделанные изменения). После перезагрузки компьютера все защищенные контейнеры будут отключены.

4.2.9. Управление доступом к защищенным контейнерам

В системе InfoWatch CryptoStorage предусмотрен многопользовательский доступ к объектам. Каждый защищенный объект имеет свой список доступа. Подключить защищенный объект может только владелец этого объекта и пользователи, включенные владельцем в список доступа.

Владелец защищенного контейнера может (после подключения контейнера) редактировать список доступа, добавляя/удаляя пользователей.

Внутри защищенного контейнера могут быть размещены папки или другие контейнеры, на которых также установлена защита. При организации доступа к таким объектам нужно учитывать, что доступ к вложенному защищенному объекту осуществляется по списку доступа, назначенного именно этому объекту.

Если контейнер подключён (но не в режиме *Подключить только для текущего пользователя*), то доступ к его содержимому может быть предоставлен средствами операционной системы другим пользователям, не включенным в список доступа.

Если необходимо предоставить доступ ко вложенным защищенным объектам для нескольких пользователей независимо друг от друга, то все эти пользователи должны быть включены в список доступа защищенного контейнера, содержащего необходимые вложенные защищенные объекты.

Информация по работе со списком доступа содержится в подразделах:

- *Просмотр списка доступа (п. 4.2.9.1 на стр. 34).*
- *Добавление пользователя в список доступа (п. 4.2.9.2 на стр. 35).*
- *Удаление пользователя из списка доступа (п. 4.2.9.3 на стр. 35).*

4.2.9.1. Просмотр списка доступа

Чтобы открыть список доступа к защищенному контейнеру:

1. Выделите нужный защищенный контейнер.
2. Щелкните правой кнопкой мыши по выделенному контейнеру и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Список доступа контейнера**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного контейнера. Затем нажмите на кнопку **OK**.

В результате на экран будет выведено диалоговое окно с информацией о пользователях, имеющих доступ к защищенному контейнеру (см. рис. 13).

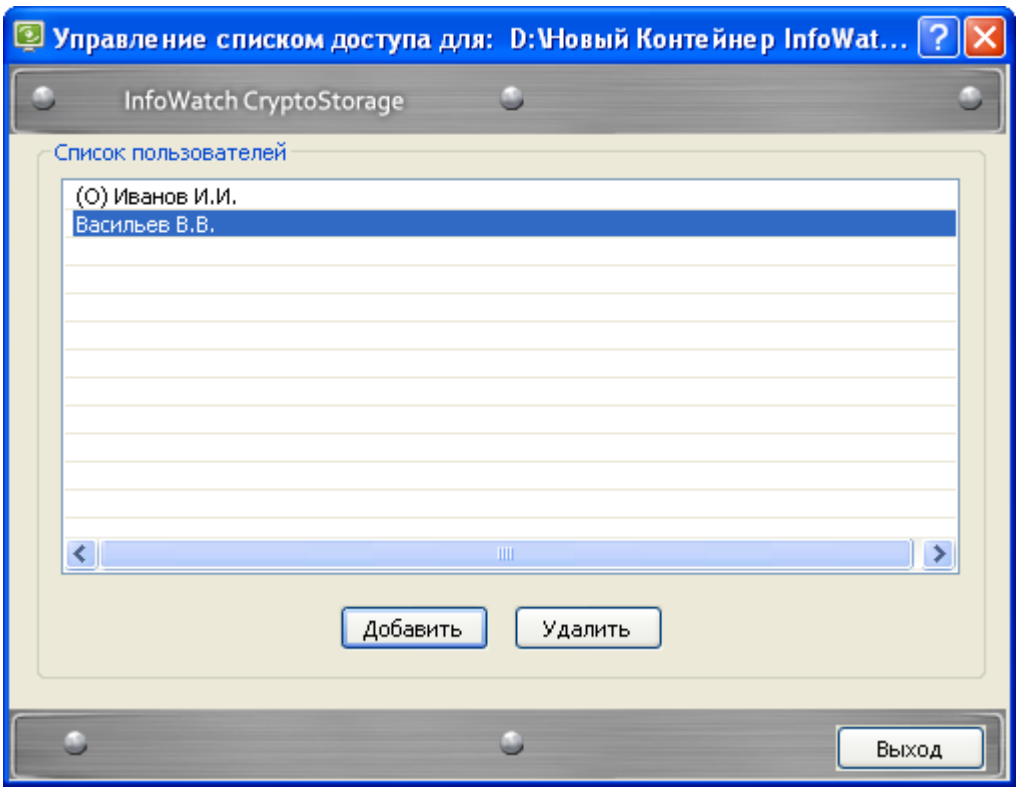

Рисунок 13. Список пользователей, имеющих доступ к защищенному контейнеру

Первоначально в список доступа включен только владелец объекта (имя владельца объекта отмечено буквой (О)). В процессе работы можно редактировать список доступа, добавляя и удаляя пользователей.

4.2.9.2. Добавление пользователя в список доступа

Чтобы добавить пользователя в список доступа:

1. Откройте список доступа к защищенному контейнеру (п. 4.2.9.1 на стр. 34).
2. В диалоговом окне списка доступа нажмите на кнопку **Добавить**.
3. В открывшемся диалоговом окне укажите параметры для доступа нового пользователя к защищенному контейнеру:
   - **Имя пользователя**.
   - **Пароль**, **Подтверждение пароля, Подсказка к паролю**. Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.
   - **Описание пользователя**. Данное описание будет отображаться в списке доступа к объекту (подробнее см. п. 4.2.9.1 на стр. 34), и дальнейшему изменению не подлежит.
4. Нажмите на кнопку **OK**.

В результате новый пользователь будет добавлен в список доступа к защищенному контейнеру.

4.2.9.3. Удаление пользователя из списка доступа

Чтобы удалить пользователя из списка доступа:

1. Откройте список доступа к защищенному контейнеру (п. 4.2.9.1 на стр. 34).
2. В списке доступа к защищенному контейнеру выделите имя пользователя, которого нужно удалить из списка.
3. Нажмите на кнопку **Удалить**.

После удаления пользователя из списка доступа рекомендуется переустановить защиту на контейнер.

4.2.10. Переустановка защиты на контейнер

Переустановку защиты может выполнять только владелец защищенного контейнера.

Данная операция осуществляется, только если защищенный контейнер находится в отключенном состоянии. Об отключении защищенных контейнеров см. п. 4.2.8 на стр. 34.

При переустановке защиты возможна замена криптографического алгоритма: алгоритм заменится на выбранный в программе Конфигурации (см. п. 3.2 на стр. 17).

Чтобы переустановить защиту на защищенный контейнер:

1. Выделите защищенный контейнер, для которого нужно выполнить переустановку защиты.
2. Щелкните правой кнопкой мыши по выделенному защищенному контейнеру и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Переустановить защиту контейнера**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного контейнера. Затем нажмите на кнопку **OK**.

После этого начнется процесс переустановки защиты. В этот период подключить защищенный контейнер нельзя.

При необходимости можно прервать процесс установки защиты (см. п. 4.2.10.1 на стр. 36). В дальнейшем переустановка защиты может быть продолжена (см. п. 4.2.10.2 на стр. 37). Кроме того, возможно отказаться от переустановки защиты и вернуться к предыдущему состоянию (см. п. 4.2.10.3 на стр. 37).

Переустановку защиты рекомендуется проводить в случае возможной компрометации внутренней ключевой информации защищенного объекта. Типовым случаем возможной компрометации внутренней ключевой информации является удаление пользователя из списка доступа. Удаленный пользователь был допущен к внутренней ключевой информации, следовательно, у него может быть возможность воспользоваться этой информацией для доступа к объекту, даже после исключения из списка. Переустановка защиты изменяет внутреннюю ключевую информацию (объект перешифровывается на новом ключе) и делает невозможным доступ к объекту по скомпрометированной ключевой информации.

> **Примечание:**
>
> Если переустановка защиты производилась на контейнер, размер которого увеличивался по мере заполнения, после переустановки защиты размер контейнера будет максимально заданный. Отказ от переустановки защиты и возврат в исходное состояние не уменьшат размер контейнера.

4.2.10.1. Прерывание переустановки защиты

В ходе переустановки защиты на защищенный контейнер может возникнуть необходимость прервать этот процесс или переустановка может быть прервана вследствие нештатной ситуации (например, при неожиданном отключении компьютера). Впоследствии прерванная процедура может быть возобновлена.

Прерывание процесса переустановки защиты на защищенный контейнер выполняется его владельцем.

Чтобы прервать переустановку защиты на защищенном контейнере:

1. Выполните одно из следующих действий:
   - Нажмите на кнопку **Стоп** в диалоговом окне, в котором отображается процесс переустановки защиты.
   - Выделите файл, являющийся защищенным контейнером, на котором выполняется процедура переустановки защиты.
   - Щелкните правой кнопкой мыши по выделенному файлу и в раскрывшемся контекстном меню выберите **InfoWatch CryptoStorage ► Остановить**.
2. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного контейнера. Затем нажмите на кнопку **OK**.

После этого переустановка защиты будет прервана. В этом состоянии с защищенным контейнером можно выполнять только операции возобновления переустановки защиты (см. п. 4.2.10.2 на стр. 37) и возврата к предшествующему состоянию защиты (см. п. 4.2.10.3 на стр. 37).

4.2.10.2. Возобновление переустановки защиты

После прерывания процесса переустановки защиты на защищенном контейнере работать с ним нельзя, необходимо либо завершить переустановку защиты, либо вернуться к предшествующему состоянию защиты.

Возобновление процесса переустановки защиты выполняется владельцем защищенного контейнера.

Чтобы возобновить переустановку защиты на защищенный контейнер:

1. Выделите файл, являющийся защищенным контейнером, на котором прервана процедура переустановки защиты.
2. Щелкните правой кнопкой мыши по выделенному файлу и в раскрывшемся контекстном меню выберите **InfoWatch CryptoStorage ► Продолжить**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

После этого процесс переустановки защиты будет продолжен. В этот период работать с защищенным контейнером нельзя.

4.2.10.3. Возврат к предшествующему состоянию защиты

После прерывания процесса переустановки защиты на защищенном контейнере работать с ним нельзя. Необходимо либо завершить переустановку защиты, либо вернуться к предшествующему состоянию защиты.

Возврат к предшествующему состоянию защиты выполняется владельцем защищенного контейнера.

Чтобы вернуться к предшествующему состоянию защиты защищенного контейнера:

1. Выделите файл, являющийся защищенным контейнером, на котором прервана процедура переустановки защиты.
2. Щелкните правой кнопкой мыши по выделенному файлу и в раскрывшемся контекстном меню выберите **InfoWatch CryptoStorage ► Откатить**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

После этого начнется процесс возврата к предшествующему состоянию защиты защищенного контейнера. В этот период работать с защищенным контейнером нельзя.

4.2.11. Смена параметров пользователя для доступа к защищенному контейнеру

Параметры доступа состоят из имени и пароля пользователя. Описание пользователя изменению не подлежит.

Чтобы изменить параметры доступа к защищенному контейнеру:

1. Щелкните правой кнопкой мыши по файлу контейнера и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Сменить ключ пользователя контейнера**.
2. В открывшемся диалоговом окне укажите текущие параметры авторизации, необходимые для доступа к защищенному контейнеру: **Имя пользователя** и **Пароль**. Затем нажмите на кнопку **OK**.
3. В открывшемся диалоговом окне с настройками новых параметров авторизации укажите новые значения для параметров **Имя пользователя**, **Новый пароль** и **Подтверждение пароля**. Затем нажмите на кнопку **OK**.

> **Примечание:**
>
> Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.

В результате параметры доступа к защищенному контейнеру будут изменены, но описание пользователя останется прежним. Новые параметры доступа вступят в силу при следующем подключении контейнера.

4.3. Работа с защищенными жесткими дисками и съемными носителями

В данном разделе содержится следующая информация:

4.3.1. Особенности защиты жестких дисков и съемных носителей

Защита может быть установлена на логические разделы жесткого диска (в том числе системные и загрузочные) и другие устройства класса Mass Storage.

Защищенные логические разделы жесткого диска и защищенные съемные носители имеют следующие особенности:

- Если защита устанавливается на логический раздел, являющийся системным и/или загрузочным, то авторизация для доступа к защищенному разделу будет выполняться до загрузки операционной системы (подробнее см. п. 4.3.4 на стр. 41).
- Установка защиты InfoWatch CryptoStorage на системный раздел жесткого диска обеспечивает защиту файла аварийного дампа памяти (crash dump), а также содержимого оперативной памяти, сохраняемого на системном диске при переходе в спящий (hibernate) режим. Защита системного раздела позволит предотвратить утечку конфиденциальных данных через служебную информацию, сохраняемую на жестком диске.
- Работа с защищенным диском или съемным носителем возможна, если на компьютере с установленной системой InfoWatch CryptoStorage запущена подсистема *Защищенные логические диски* (см. Глава 5 на стр. 50). Если данная подсистема отключена, то доступ к информации в расшифрованном виде на защищенном диске или съемном носителе невозможен. Операционная система отображает такой раздел как неформатированный или содержащий некоторые ошибки. Если на компьютере защищен системный и/или загрузочный раздел жесткого диска, то конфигуратор системы не позволяет отключить подсистему *Защищенные логические диски*.
- Не рекомендуется защищать системные и загрузочные диски с помощью InfoWatch CryptoStorage на компьютерах с несколькими операционными системами и при этом защищать разделы дисков, необходимые для загрузки установленных операционных систем.
- Данные Системы обо всех защищенных логических разделах физических носителей (физического жесткого диска, Flash-накопителя, и т.д.), находятся в корневых каталогах логических разделов физических носителей в файлах `iwcs.bin`. В случае форматирования логического раздела, со-

держащего `iwcs.bin`, или в случае удаления, замещения, или повреждения `iwcs.bin` доступ к защищенным логическим разделам физического носителя может быть утрачен. Не рекомендуется форматировать разделы содержащие файл iwcs.bin или удалять этот файл. Если на компьютере с установленной системой InfoWatch CryptoStorage запущена подсистема *Защищенные логические диски* (см. Глава 5 на стр. 50), то Система защищает файл `iwcs.bin` от удаления и изменения. Поэтому, при наличии защищенных логических разделов, не рекомендуется отключать подсистему *Защищенные логические диски*.

- Чтобы снизить риск потери доступа к зашифрованным данным, при включенной подсистеме *Защищенные логические диски* и наличии хотя бы одного защищенного раздела физического диска, блокируется доступ на запись в загрузочный сектор этого диска (кроме изменения данных о размере разделов). Для предоставления доступа к загрузочному сектору снимите защиту со всех разделов данного физического диска.

Ограничения на защиту логических разделов жесткого диска и съемных носителей:

- Установка защиты на логические разделы жестких дисков и съемных носителей возможна только если выполнены все нижеперечисленные условия:
  - соответствующее устройство имеет размер сектора 512 байт (стандартный размер сектора для большинства устройств подобного типа);
  - раздел не является динамическим;
  - диск является локальным (защита сетевых дисков не поддерживается);
  - на защищаемый раздел разрешена запись.
- Начать установку защиты на съемный диск можно только при условии, что съемный диск не используется никакими программами. В процессе установки защиты использование съемного диска возможно.
- Защита логического раздела жесткого диска, на котором установлена система InfoWatch CryptoStorage, допускается только при условии, что этот раздел является системным и/или загрузочным.
- В Windows 7 при физическом подключении защищенных съемных носителей операционная система сообщает, что носитель не форматирован, и доступа к нему не предоставляет до тех пор, пока носитель не будет подключен средствами Системы (см. п. 4.3.5 на стр. 42).
- В Системе не поддерживается непосредственная защита CD/DVD-дисков. Однако они могут использоваться для размещения защищенных контейнеров (см. п. 4.2 на стр. 28).

4.3.2. Особенности использования утилит для работы с жесткими дисками

Некоторые утилиты предоставляют возможность изменять размеры логических разделов на жестком диске. Не изменяйте размеры логических разделов жесткого диска, защищенных средствами InfoWatch CryptoStorage. Это может привести к потере данных.

При необходимости выполнить такую операцию снимите защиту с защищенных логических разделов, выполните перераспределение свободного пространства, а затем установите защиту вновь.

4.3.3. Установка защиты на жесткий диск или съемный носитель

> **Важная информация!**
>
> Перед началом работы ознакомьтесь с особенностями защиты логических разделов жесткого диска и съемных устройств (см. п. 4.3.1 на стр. 38).

Установка защиты на логические разделы жестких дисков и съемные носители выполняется в фоновом режиме. Поэтому в процессе установки защиты можно продолжать работу с устройством.

При необходимости процесс установки защиты может быть прерван (см. п. 4.3.3.1 на стр. 40). Затем возможно либо продолжить установку защиты (см. п. 4.3.3.2 на стр. 41), либо отказаться от защиты объекта (см. п. 4.3.3.3 на стр. 41).

> **Примечание:**
>
> Переход компьютера в ждущий/спящий режим приводит к тому, что установка защиты будет автоматически прервана. После выхода из ждущего/спящего режима установку защиты можно продолжить или отказаться от нее.

Чтобы установить защиту на логический раздел жесткого диска или на съемный носитель:

1. Откройте папку **Мой компьютер**.
2. Щелкните правой кнопкой мыши по объекту (логическому разделу жесткого диска или съемному носителю), на который нужно установить защиту, и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Установить защиту на диск**.
3. В открывшемся диалоговом окне укажите параметры, которые будут использоваться владельцем для доступа к защищенному объекту:
   - **Имя пользователя**
   - **Пароль**, **Подтверждение пароля, Подсказка к паролю**. Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.
   - **Описание пользователя**. Информация о владельце защищаемого объекта. Данное описание будет отображаться в списке доступа к объекту (подробнее см. п. 4.3.8.1 на стр. 44).

   Когда все необходимые параметры будут заданы, нажмите на кнопку **OK**.

После этого выполняется установка защиты на объект. С этого момента логический диск (съемный носитель) становится защищенным объектом.

> **Важная информация!**
>
> Если защита установлена на системный и/или загрузочный диск, то для загрузки операционной системы необходимо пройти авторизацию (подробнее см. п. 4.3.4 на стр. 41). Авторизация выполняется каждый раз при включении или перезагрузке компьютера, а также при выходе из спящего (hibernate) режима.

4.3.3.1. Прерывание установки защиты

В ходе установки защиты может возникнуть необходимость прервать этот процесс или защита может быть прервана вследствие нештатной ситуации (например, при неожиданном отключении компьютера). В дальнейшем можно возобновить установку защиты.

> **Важная информация!**
>
> Логический диск (съемный носитель) является защищенным объектом вне зависимости от того, установлена ли защита полностью или частично. Поэтому даже если установка защиты была прервана, работа с этим диском (съемным устройством) возможна только после подключения (прохождения авторизации). При этом если установка защиты не завершена, часть информации в разделе находится в незашифрованном виде.

Чтобы прервать установку защиты:

1. Выполните одно из следующих действий:
   - Нажмите на кнопку **Стоп** в диалоговом окне, где отображается прогресс установки защиты.
   - Щелкните правой кнопкой мыши по объекту и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Остановить обработку диска**.
2. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

После этого установка защиты будет прервана. Защищенный диск (съемное устройство) остается в подключенном состоянии, и работу с ним можно продолжать.

4.3.3.2. Возобновление установки защиты

Надежная защита объекта обеспечивается только после завершения операции по установке защиты. Если установка защиты была прервана по каким-либо причинам, то часть содержимого остается незашифрованной. Продолжить установку защиты можно с помощью специальной функции.

Возобновление процесса установки защиты выполняется владельцем защищенного логического диска (съемного носителя).

Чтобы возобновить установку защиты:

1. Подключите защищенный объект (см. п. 4.3.5 на стр. 42).
2. Щелкните правой кнопкой мыши по объекту и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Продолжение установки защиты диска**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

После этого процесс установки защиты будет продолжен. Защищенный диск (съемное устройство) остается в подключенном состоянии, и работу с ним можно продолжать.

4.3.3.3. Возврат к незащищенному состоянию

Если установка защиты была прервана, можно отказаться от установки защиты и вернуться к незащищенному состоянию.

Это действие выполняется владельцем защищенного логического диска (съемного носителя).

Чтобы отказаться от установки защиты и вернуться к незащищенному состоянию:

1. Подключите защищенный объект, защита которого была прервана (см. п. 4.3.5 на стр. 42).
2. Щелкните правой кнопкой мыши по объекту и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Отмена установки защиты диска**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

После этого начнется процесс возврата к незащищенному состоянию. Защищенный диск (съемное устройство) остается в подключенном состоянии, и работу с ним можно продолжать.

4.3.4. Загрузка с защищенного системного и/или загрузочного диска

Если системный и/или загрузочный диск защищен средствами InfoWatch CryptoStorage, то загрузка операционной системы, установленной на этом диске, возможна только после подключения защищенного диска. Для подключения защищенного диска необходимо пройти авторизацию, которая выполняется до загрузки операционной системы.

Чтобы подключить защищенный системный и/или загрузочный диск, укажите следующие параметры:

- **Login**. Имя пользователя.
- **Password**. Пароль пользователя.

> **Примечание:**
>
> Для ввода имени и пароля вы можете воспользоваться виртуальной клавиатурой (см. инструкции на экране). Рекомендуется воспользоваться этой возможностью в случае не QWERTY-клавиатуры.

> **Важная информация!**
>
> Если на вашем компьютере системный и загрузочный разделы находятся на разных логических дисках и оба раздела защищены, необходимо подключить каждый из этих разделов.

После этого выполняется авторизация пользователя. Если авторизация пройдена успешно, выполняется загрузка операционной системы, установленной на защищенном диске.

> **Примечание:**
>
> Если в процессе авторизации были введены неверные данные, на экран компьютера будет выведено предупреждение о том, что авторизация невозможна, подсказка соответствующая введенному имени пользователя (если такая имеется), и предложение повторить процедуру авторизации.

4.3.5. Подключение защищенных жестких дисков и съемных носителей

Работа (чтение, запись, переименование, копирование, удаление и т. д.) с любым защищенным объектом становится возможна только при условии, что этот объект подключен.

Чтобы подключить логический раздел жесткого диска или съемный носитель:

1. Щелкните правой кнопкой мыши по защищенному объекту и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Подключить диск**.
2. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** пользователя защищенного объекта. Затем нажмите на кнопку **OK**.

Подключенный объект незащищен и доступен всем пользователям, которые могут работать с компьютером. Поэтому необходимо отключать защищенный объект сразу после того, как работа с этим объектом завершена.

4.3.6. Просмотр информации о защищенном жестком диске или съемном носителе

Просмотр информации о защищенном объекте доступен только владельцу защищенного объекта.

Чтобы просмотреть свойства защищенного объекта:

1. Щелкните правой кнопкой мыши по объекту и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Информация о диске**.
2. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

В результате на экран будет выведено диалоговое окно, содержащее информацию о выбранном защищенном объекте (рис. 14).

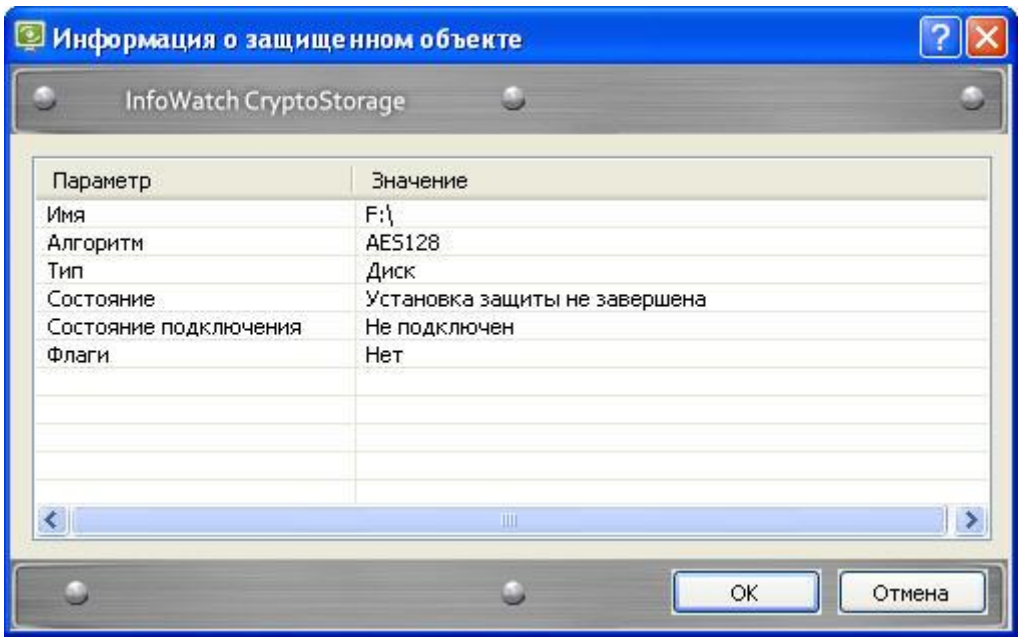

Рисунок 14. Просмотр информации о защищенном жестком диске или съемном носителе

Атрибуты защищенных объектов перечислены в таблице 6.

Таблица 6. Атрибуты защищенных жестких дисков и съемных носителей

Атрибут защищенного объекта	Пояснения
Имя	Полное имя объекта
Алгоритм	Тип защиты
Тип	Тип защищенного объекта - диск
Состояние	Состояние защиты объекта
Состояние подключения	Состояние подключения объекта: подключен или нет
Флаги	Параметры диска

4.3.7. Отключение защищенных разделов жестких дисков и съемных носителей

После отключения защищенный объект переводится в состояние, при котором дальнейшая работа с ним невозможна до следующего подключения.

> **Важная информация!**
>
> Отключение необходимо выполнять только после сохранения всех изменений и завершения работы с объектом.

Чтобы отключить защищенный объект,

щелкните правой кнопкой мыши по объекту и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Отключить диск**.

Если работа производится с несколькими защищенными объектами одновременно, то на отключение всех объектов потребуется некоторое время. Однако в ряде случаев могут возникнуть экстренные ситуации, когда требуется отключить все защищенные объекты одновременно. С этой целью можно выполнить перезагрузку компьютера (предварительно сохранив сделанные изменения). После перезагрузки компьютера все защищенные объекты будут отключены.

4.3.8. Управление доступом к защищенному жесткому диску или съемному носителю

В системе InfoWatch CryptoStorage предусмотрен многопользовательский доступ к объектам. Каждый защищенный объект имеет свой список доступа. Подключить защищенный объект может только владелец этого объекта и пользователи, включенные владельцем в список доступа. Владелец защищенного объекта может редактировать список доступа, добавляя/удаляя пользователей.

После подключения защищенного логического диска или съемного носителя доступ к его содержимому может быть предоставлен средствами операционной системы другим пользователям, не включенным в список доступа.

Внутри защищенного раздела жесткого диска или съемного носителя могут быть размещены папки или другие контейнеры, на которых также установлена защита. При организации доступа к таким объектам нужно учитывать, что доступ к вложенному защищенному объекту осуществляется по списку доступа, назначенного именно этому объекту.

Если необходимо предоставить доступ ко вложенным защищенным объектам для нескольких пользователей независимо друг от друга, то все эти пользователи должны быть включены в список доступа защищенного раздела жесткого диска или съемного носителя содержащего необходимые вложенные защищенные объекты.

Доступ к файлам и папкам, расположенным на защищенном логическом диске или съемном носителе, осуществляется по списку доступа, имеющемуся у этого диска (съемного носителя).

Информация по работе со списком доступа содержится в подразделах:

- *Просмотр списка доступа (п. 4.3.8.1 на стр. 44).*
- *Добавление пользователя в список доступа (п. 4.3.8.2 на стр. 45).*
- *Удаление пользователя из списка доступа (п. 4.3.8.3 на стр. 45).*

4.3.8.1. Просмотр списка доступа

Чтобы открыть список доступа к защищенному логическому диску или съемному носителю:

1. Щелкните правой кнопкой мыши по необходимому объекту и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Список доступа диска**.
2. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

В результате на экран будет выведено диалоговое окно с информацией о пользователях, имеющих доступ к защищенному объекту (см. рис. 15).

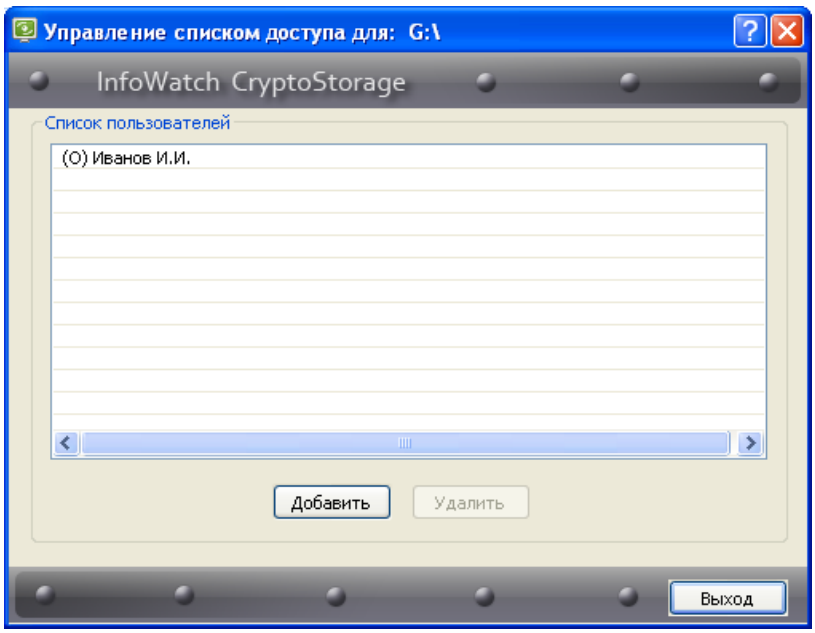

Рисунок 15. Список пользователей, имеющих доступ к защищенному диску

Первоначально в список доступа включен только владелец объекта. В процессе работы можно редактировать список доступа путем добавления/удаления пользователей.

4.3.8.2. Добавление пользователя в список доступа

Чтобы добавить пользователя в список доступа:

1. Откройте список доступа к защищенному объекту (п. 4.3.8.1 на стр. 44).
2. В диалоговом окне списка доступа нажмите на кнопку **Добавить**.
3. В открывшемся диалоговом окне укажите параметры для доступа нового пользователя к защищенному объекту:
   - **Имя пользователя**.
   - **Пароль**, **Подтверждение пароля, Подсказка к паролю**. Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.
   - **Описание пользователя**. Данное описание будет отображаться в списке доступа к объекту (подробнее см. п. 4.3.8.1 на стр. 44), и дальнейшему изменению не подлежит.
4. Когда все необходимые параметры будут заданы, нажмите на кнопку **OK**.

В результате новый пользователь будет добавлен в список доступа к защищенному объекту.

4.3.8.3. Удаление пользователя из списка доступа

Чтобы удалить пользователя из списка доступа:

1. Откройте список доступа к защищенному объекту (п. 4.3.8.1 на стр. 44).
2. В списке доступа к защищенному объекту выделите имя пользователя, которого нужно удалить из списка.
3. Нажмите на кнопку **Удалить**.

Рекомендуется после выполнения этой операции переустановить защиту на объект.

4.3.9. Переустановка защиты на жесткий диск или съемный носитель

Переустановку защиты рекомендуется проводить в случае возможной компрометации внутренней ключевой информации защищенного объекта. Типовым случаем возможной компрометации внутренней ключевой информации является удаление пользователя из списка доступа (см. п. 4.3.8.3 на стр. 45). Удаленный пользователь был допущен к внутренней ключевой информации, следовательно, у него может быть возможность воспользоваться этой информацией для доступа к объекту, даже после исключения из списка. Переустановка защиты изменяет внутреннюю ключевую информацию (объект перешифровывается на новом ключе) и делает невозможным доступ к объекту по скомпрометированной ключевой информации.

При переустановке защиты возможна замена криптографического алгоритма: алгоритм заменится на выбранный в программе Конфигурации (см. п. 3.2 на стр. 17).

Переустановку защиты выполняет владелец объекта.

Чтобы переустановить защиту на логический раздел жесткого диска или съемный носитель:

1. Подключите объект, для которого нужно выполнить переустановку защиты (см. п. 4.3.5 на стр. 42).
2. Щелкните правой кнопкой мыши по объекту и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Переустановить защиту на диск**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

После этого начнется процесс переустановки защиты. В это время логический диск (съемное устройство) остается защищенным объектом. Он находится в подключенном состоянии, и работу с ним можно продолжать.

При необходимости можно прервать процесс переустановки защиты аналогично прерыванию установки защиты (см. п. 4.3.3.1 на стр. 40).

В дальнейшем переустановку защиты можно возобновить аналогично возобновлению установки защиты (см. п. 4.3.3.2 на стр. 41).

Кроме того, возможно отказаться от переустановки защиты и вернуться к предыдущему состоянию. Процедура отказа от переустановки защиты выполняется аналогично процедуре отказа от установки защиты (см. п. 4.3.3.3 на стр. 41).

4.3.10. Снятие защиты с жесткого диска или съемного носителя

Снять защиту с объекта может только владелец этого объекта.

Чтобы снять защиту с объекта:

1. Подключите объект, с которого нужно снять защиту (см. п. 4.3.5 на стр. 42).
2. Щелкните правой кнопкой мыши по объекту и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Снять защиту с диска**.
3. В открывшемся диалоговом окне введите **Имя пользователя** и **Пароль** владельца защищенного объекта. Затем нажмите на кнопку **OK**.

При необходимости можно прервать процесс снятия защиты аналогично прерыванию установки защиты (см. п. 4.3.3.1 на стр. 40).

В дальнейшем снятие защиты можно будет продолжить аналогично возобновлению установки защиты (см. п. 4.3.3.2 на стр. 41).

Кроме того, возможно отказаться от снятия защиты и вернуться к предыдущему состоянию. Процедура отказа от снятия защиты выполняется аналогично процедуре отказа от установки защиты (см. п. 4.3.3.3 на стр. 41). После отказа от снятия защиты объект будет находиться в защищенном состоянии.

4.3.11. Смена параметров пользователя для доступа к защищенному жесткому диску или съемному носителю

Параметры доступа состоят из имени и пароля пользователя. Описание пользователя изменению не подлежит.

Чтобы изменить параметры доступа к защищенному жесткому диску или съемному носителю:

1. Щелкните правой кнопкой мыши по необходимому объекту и в раскрывшемся контекстном меню выберите пункт **InfoWatch CryptoStorage ► Сменить ключ пользователя диска**.
2. В открывшемся диалоговом окне укажите текущие параметры авторизации, необходимые для доступа к защищенному объекту: **Имя пользователя** и **Пароль**. Затем нажмите на кнопку **OK**.
3. В открывшемся диалоговом окне с настройками новых параметров авторизации укажите новые значения для параметров **Имя пользователя**, **Новый пароль** и **Подтверждение пароля**. Затем нажмите на кнопку **OK**.

> **Примечание:**
>
> Рекомендации по составлению паролей и подсказок к паролям приведены в п. 1.5 на стр. 11.

В результате параметры доступа к защищенному объекту будут изменены, но описание пользователя останется прежним. Новые параметры доступа вступят в силу при следующем подключении объекта.

4.3.12. Утилита восстановления дисков

> **Важная информация!**
>
> Для работы с утилитой восстановления дисков требуются права локального администратора на компьютере.

В состав InfoWatch CryptoStorage входит утилита, позволяющая при работе с защищенными логическими разделами физического диска, Flash-накопителями или другим USB-устройствами хранения данных:

- восстанавливать доступ к перечисленным защищенным объектам в случае частичного повреждения метаданных Системы (загрузочного сектора Системы);
- освобождать пространство, занятое защищенными разделами, когда доступ к ним безвозвратно утрачен.

Потребность в удалении информации о защищенном разделе без снятия защиты может возникнуть в следующих ситуациях:

- Утеряны ключи доступа к защищенному разделу, поэтому подключить его или снять защиту невозможно.
- В отсутствие InfoWatch CryptoStorage с запущенной подсистемой *Защищенные логические диски*, защищенный раздел был отформатирован. Как следствие, все данные с этого раздела пропали, но на диске сохранилась запись Системы о наличии раздела. Получить доступ к такому разделу на компьютере с InfoWatch CryptoStorage и запущенной подсистемой *Защищенные логические диски* можно только после удаления информации о защите. Доступ может потребоваться, например, если после форматирования в раздел были записаны незашифрованные данные.
- Был изменен размер защищенного раздела (см. п. 4.3.3 на стр. 39). Как следствие, возникло рассогласование между учитываемым Системой размером и реально существующим размером защищенного раздела.

Если на компьютере с установленной системой InfoWatch CryptoStorage запущена подсистема *Защищенные логические диски* (см. Глава 5 на стр. 50), то отсутствует доступ к указанным выше защищенным разделам диска. Кроме того, пространство, занимаемое ими на диске, невозможно использовать. Утилита позволяет сделать это пространство снова доступным для использования, в том числе и для InfoWatch CryptoStorage.

Перед началом работы с утилитой обязательно выполните следующие действия:

1. Завершите все операции, связанные с установкой, переустановкой и удалением защиты на всех разделах этого физического диска.
2. Отключите защищенные разделы физического диска, информацию о которых нужно удалить из Системы при помощи утилиты.

> **Важная информация!**
>
> Будьте внимательны при выборе защищённого раздела. После удаления информации Системы о защищенном разделе, расшифровывание данных из этого раздела невозможно. Поэтому, если раздел был зашифрован, он будет выглядеть как неформатированный.

Чтобы сделать доступным для использования пространство на диске, занимаемое защищенным разделом,

1. Запустите утилиту. Для этого в меню **Пуск** выберите пункт **Все программы ► InfoWatch CryptoStorage ► Утилита восстановления дисков**.

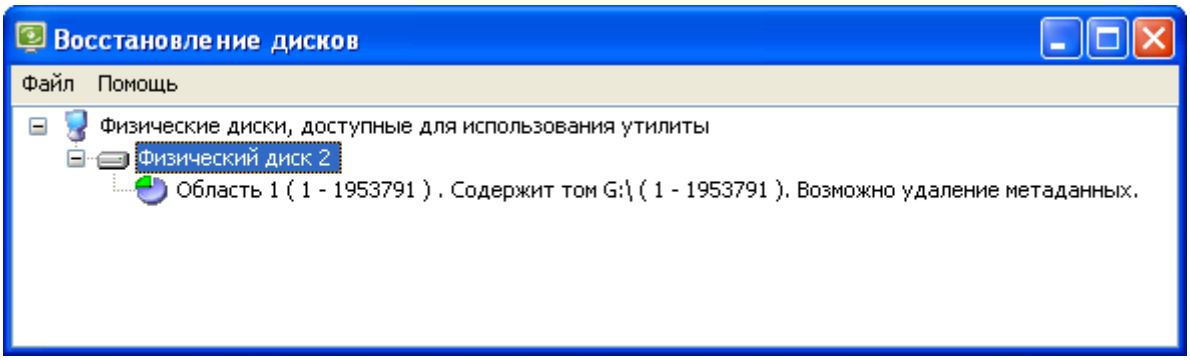

Рисунок 16. Окно утилиты восстановления дисков

2. В окне В**осстановление дисков** выделите защищенный раздел, сведения Системы о котором нужно удалить с диска.
3. Щелкните по выделенному разделу правой кнопкой мыши и в раскрывшемся контекстном меню выберите команду **Удалить информацию о шифрованной области**.

Повреждение метаданных Системы может произойти в результате действия каких-либо программ, изменяющих загрузочный сектор физического диска, например:

- установка или переустановка операционной системы на одном из разделов защищенного физического диска;
- удаление информации о защищённом логическом разделе Системы при помощи утилиты восстановления дисков (см. выше);
- действие какой-либо вредоносной программы.

Защищенные разделы в этом случае выглядят как неформатированные или поврежденные. Для таких разделов, при вызове контекстного меню проводника с помощью правой кнопки мыши, меню InfoWatch CryptoStorage не строится.

Чтобы восстановить возможность доступа к защищённому логическому разделу:

1. Запустите утилиту. Для этого в меню **Пуск** выберите пункт **Все программы ► InfoWatch CryptoStorage ► Утилита восстановления дисков**.

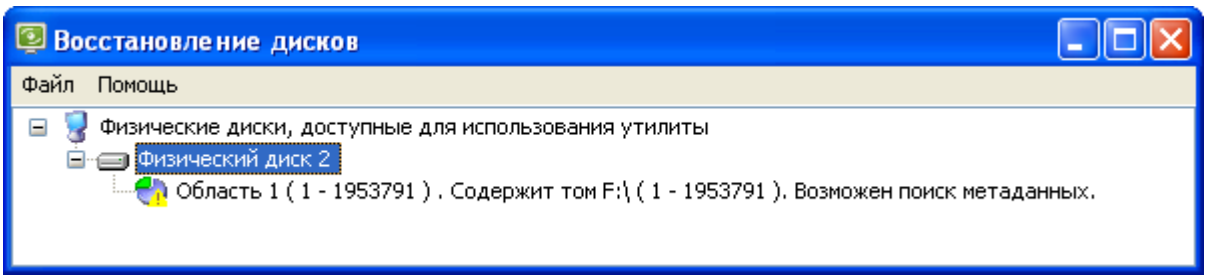

Рисунок 17. Окно утилиты восстановления дисков

2. В окне В**осстановление дисков** выделите защищенный раздел, возможность доступа к которому нужно восстановить на диске.
3. Щелкните по выделенному разделу правой кнопкой мыши и в раскрывшемся контекстном меню выберите команду **Искать метаданные**.

   Утилита проведёт поиск метаданных для выбранного раздела и, в случае успеха, отобразит сообщение с датой создания найденных метаданных.
4. Чтобы восстановить найденные метаданные, в окне сообщения нажмите **Да**. Чтобы продолжить поиск, нажмите **Нет**.

> **Важная информация!**
>
> Доступ к восстановленному защищенному разделу можно получить только после выполнения процедуры подключения защищенного раздела (см. п. 4.3.5 на стр. 42).

4.4. Гарантированное удаление защищенных и незащищенных объектов

Папки и файлы, удаленные обычным способом, могут быть впоследствии восстановлены при помощи специальных утилит. Как следствие информация, хранившаяся в удаленном объекте, станет доступной посторонним лицам. Решить эту проблему можно посредством гарантированного удаления объекта.

Функция гарантированного удаления доступна как для защищенных, так и для незащищенных объектов.

Если на папку установлена защита, то гарантированное удаление возможно только после подключения этой папки.

Гарантированное удаление защищенного контейнера выполняется только если контейнер отключен.

Чтобы удалить папку или файл без возможности последующего восстановления:

1. Выделите объект, который нужно удалить.
2. Щелкните правой кнопкой мыши по выделенному объекту и в раскрывшемся контекстном меню выберите команду **InfoWatch CryptoStorage ► Гарантированно удалить…**.
3. В открывшемся окне запроса об удалении нажмите на кнопку **Да**.

ГЛАВА 5. КОНФИГУРИРОВАНИЕ ПОДСИСТЕМ

В состав InfoWatch CryptoStorage входят три подсистемы, каждая из которых обеспечивает защиту объектов определенного типа. Назначение подсистем приводится в таблице 7.

Таблица 7. Описание подсистем InfoWatch CryptoStorage

Подсистема	Назначение
Защищенные логические диски	Защита логических разделов жесткого диска и съемных носителей
Защищенные контейнеры	Создание защищенных контейнеров, работа с защищенными контейнерами
Защищенная файловая система	Создание защищенных папок, работа с защищенными папками

Для настройки подсистем, входящих в состав InfoWatch CryptoStorage, предназначена программа **Конфигурация CryptoStorage**.

Чтобы открыть окно программы Конфигурация CryptoStorage, в меню **Пуск** выберите пункт **Программы ► InfoWatch CryptoStorage ► Конфигурация CryptoStorage**.

После этого на экран будет выведено окно программы, в котором можно просмотреть информацию о подсистемах InfoWatch CryptoStorage, установленных на вашем компьютере (см. рис. 18).

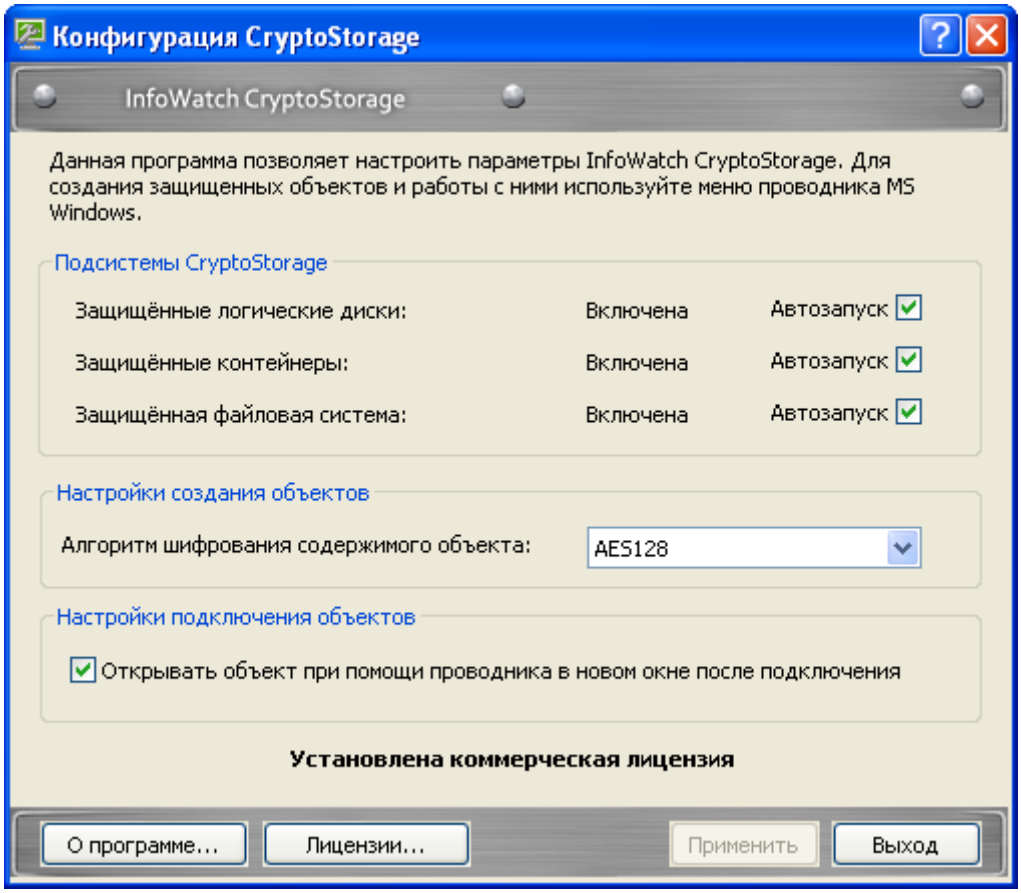

Рисунок 18. Конфигурирование подсистем InfoWatch CryptoStorage

Справа от названия каждой подсистемы расположено поле **Автозапуск**. Флажок, установленный в данном поле, означает, что включен автозапуск подсистемы.

После установки InfoWatch CryptoStorage все подсистемы настроены на автозапуск. Однако можно изменять параметры автозапуска подсистемы:

- отключить автозапуск, сняв флажок в поле **Автозапуск**;
- включить автозапуск, установив флажок в поле **Автозапуск**.

> **Примечание:**
>
> Настройки, связанные с автозапуском подсистем, вступают в действие только после перезагрузки компьютера.

При отключении автозапуска подсистем необходимо учитывать особенности функционирования подсистем InfoWatch CryptoStorage. В таблице 8 приводится описание последствий отключения для каждой подсистемы.

Таблица 8. Влияние отключаемых подсистем на защиту объектов

Подсистема	Результат отключения подсистемы
Защищенные логические диски	Операционная система идентифицирует защищенные диски как неформатированные устройства. Содержимое зашифровано. Недоступны функции Системы для работы с логическими разделами жесткого диска и съемными носителями **Примечание:** Отключить подсистему при защищенном системном и/или загрузочном диске невозможно
Защищенные контейнеры	Доступ к содержимому защищенных контейнеров невозможен. Содержимое зашифровано. Недоступны функции Системы для работы с защищенными контейнерами
Защищенная файловая система	Защищенные папки и защищенные контейнеры могут быть удалены с вашего компьютера любым пользователем. Содержимое файлов зашифровано, можно просматривать только структуру подпапок. Недоступны функции Системы для работы с защищенными папками

ГЛАВА 6. УДАЛЕНИЕ INFOWATCH CRYPTOSTORAGE

Для защищенных объектов удаление InfoWatch CryptoStorage равносильно отключению всех подсистем (см. Глава 5 на стр. 50):

- Защищенные папки могут быть удалены с вашего компьютера любым пользователем. Содержимое файлов зашифровано, можно просматривать только структуру подпапок.
- Контейнеры остаются в защищенном состоянии, однако работа с ними невозможна, так как отсутствует возможность подключения.
- Защита, установленная на логические разделы жесткого диска и съемные носители, сохраняется. Однако доступ к данным, хранящимся на этих устройствах, становится невозможен, так как отсутствует средство подключения.

> **Важная информация!**
>
> Операционной системой подобные объекты воспринимаются как неформатированные, и при попытке получить доступ к защищенному объекту будет предложено выполнить форматирование. В процессе форматирования объекта будут потеряны все данные. Поэтому, если объект содержит ценную для вас информацию, то необходимо отказаться от форматирования.
>
> Не допускается удаление Системы, если защищен системный и/или загрузочный раздел жесткого диска. Поскольку, в этом случае, загрузка операционной системы и, как следствие, доступ к данным, хранящимся на этом диске, будет невозможен.

Перед удалением Системы необходимо выполнить ряд подготовительных действий:

- Снять защиту с защищенного системного и/или загрузочного раздела, защищенных несистемных логических дисков и съемных носителей.
- Подключить защищенные контейнеры и папки, затем перенести содержимое этих контейнеров и папок на незащищенные жесткие диски или съемные носители.

> **Важная информация!**
>
> Для удаления InfoWatch CryptoStorage требуются права локального администратора на компьютере.

Чтобы удалить InfoWatch CryptoStorage:

1. В меню **Пуск** выберите пункт **Все программы ► InfoWatch CryptoStorage ► Изменение, восстановление или удаление**.

   На экран будет выведено окно приветствия мастера установки InfoWatch CryptoStorage.
2. Для продолжения нажмите на кнопку **Далее**.
3. В окне **Исправление или удаление установленного продукта** нажмите на кнопку **Удалить**.
4. Подтвердите удаление, нажав на кнопку **Удалить**.
5. Чтобы завершить удаление, выполните перезагрузку компьютера.

ПРИЛОЖЕНИЕ А. ПОЛЬЗОВАТЕЛЬСКОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

ЗАО «ИнфоВотч»

Тел./факс:+7(495)229-00-22

Сайт компании: www.infowatch.ru

Служба технической поддержки: support@infowatch.ru

Веб-сайт: www.cryptostorage.ru

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями лицензионного соглашения перед началом работы с программным обеспечением.

Настоящее Пользовательское лицензионное соглашение (далее - Соглашение) является Договором между Вами, физическим или юридическим лицом (далее – Пользователь), правомерно владеющим экземпляром программного обеспечения InfoWatch CryptoStorage 2.x (далее - ПО), и ЗАО «ИнфоВотч» (далее - Правообладатель).

Исключительные права в полном объеме на ПО (исходный текст, объектный код, все иные элементы) и Руководство пользователя в печатном и/или электронном виде принадлежат Правообладателю.

Выбор Пользователем пункта «Я принимаю условия Пользовательского лицензионного соглашения» при установке ПО и нажатии на кнопку «Далее» означает безоговорочное согласие Пользователя с условиями настоящего Соглашения. Если Пользователь не согласен с условиями данного Соглашения, то Пользователь должен прекратить установку ПО.

В случае если Пользователь приобрел ПО на материальном носителе, то вскрытие упаковочного конверта с компакт-диском (нарушение целостности наклейки) означает безоговорочное согласие Пользователя с условиями настоящего Соглашения. Если Пользователь не согласен с условиями данного Соглашения, то Пользователь имеет право вернуть ПО продавшей его организации и получить обратно его полную стоимость.

После вскрытия упаковочного конверта или повреждения наклейки (в случае приобретения ПО на материальном носителе), либо после выбора Пользователем пункта «Я принимаю условия Пользовательского лицензионного соглашения» (при приобретении ПО через Интернет), Пользователь получает простую (неисключительную) лицензию на воспроизведение ПО, ограниченную правом установки (инсталляции), копирования и запуска ПО в соответствии с условиями настоящего Соглашения.

Пользователь имеет право использовать ПО в соответствии с условиями настоящего лицензионного соглашения:

1. ПО предназначено для криптографической защиты конфиденциальной информации, хранящейся на персональном компьютере. ПО призвано избежать несанкционированного доступа к данным, а также обеспечить защиту данных в случае, если носитель, на котором они хранятся, был утерян.
2. ПО имеет следующие функции:
   - защита логических разделов жесткого диска, включая загрузочные и системные разделы, а также USB Mass Storage Device;
   - защита папок и файлов в файловой системе NTFS;
   - реализация защищенных виртуальных дисков посредством специальных файлов-контейнеров;
   - защита crash-dump файлов и файлов подкачки ОС (при защите системного раздела);
   - прозрачный режим работы с защищаемой информацией;
   - многопользовательский доступ к защищаемым данным;
   - авторизация на основе паролей пользователей;
   - иерархический доступ к папкам и файлам внутри защищенной папки;

- защита трафика в сети при работе с удаленными защищенными файлами и папками или файлами-контейнерами;
- поддержка режимов Hibernate и Stand by при работе с защищаемой информацией;
- фоновый режим установки и снятия защиты с логических разделов жестких дисков и USB Mass Storage Device;
- гарантированное удаление файлов;
- защита от несанкционированного уничтожения защищенных файлов и папок, в том числе и от переименования.

3. Количество рабочих станций, защита которых обеспечивается данной версией ПО, и срок использования ПО указаны в файле лицензионного ключа (уникальный электронный файл, необходимый для обеспечения полной функциональности ПО) и представлены в интерфейсе ПО «Конфигурация CryptoStorage» в окне «Лицензии».
4. Коммерческая лицензия - не содержит никаких ограничений по функционалу. Срок действия коммерческой лицензии не ограничен (perpetual license) .

   В случае использования коммерческой лицензии Пользователь имеет право получать:

   - обновления ПО минорных версий CryptoStorage версии 2.x, при этом поведение продукта - это продукт с активной коммерческой лицензией;
   - дубликат файла лицензионного ключа (автоматически - количество попыток регулируется программой лицензирования и может изменяться, по истечению попыток Пользователю необходимо обратиться к Правообладателю).

   В коммерческую лицензию продукта включена годовая техническая поддержка (через веб-сайты Правообладателя).
5. В случае использования ознакомительных версий продукта длина пароля ограничивается одним символом. Ознакомительная лицензия - может быть установлена только однократно. Срок использования ознакомительной лицензии ограничивается периодом в 1 месяц.

   По окончании срока, указанного в файле лицензионного ключа (Пользователь может посмотреть этот срок в интерфейсе ПО «Конфигурация CryptoStorage» в окне «Лицензии») Пользователю автоматически становятся недоступны следующие функции:

   - создание новых защищенных объектов;
   - управление списками доступа к объектам;
   - переустановка защиты объекта.
6. Пользователь CryptoStorage 1.x в любой момент имеет возможность обновиться до версии продукта CryptoStorage 2.x со следующими условиями:

   - переход в активную ознакомительную лицензию CryptoStorage 2.x с уведомлением о том, что он переходит в ознакомительную лицензию (о политике перехода смотреть на сайте Правообладателя в соответствующем разделе), если в хранилище присутствует коммерческая лицензия CryptoStorage 1.x;
   - переход в активную ознакомительную лицензию CryptoStorage 2.x если в хранилище присутствует ознакомительная лицензия CryptoStorage 1.x;
   - в процессе обновления Пользователю предоставляется возможность получить файл лицензии CryptoStorage 2.x по короткому ключу CryptoStorage 1.x или по файлу лицензии CryptoStorage 1.x в неавтоматическом режиме, посредством запроса в специальной форме на сайте Правообладателя в соответствующем разделе.
7. Сервисы, описанные в п.4 настоящего Соглашения, предоставляются при условии установки Пользователем последнего обновления последней версии ПО.
8. Правообладатель не гарантирует Пользователю функциональность ПО в случае, если Пользователь не осуществляет обновления ПО.
9. Пользователь имеет право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра ПО в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Указанная в настоящем

пункте копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

10. При использовании ПО, предназначенного для ознакомительных целей, Пользователь не имеет права продавать (передавать на иных условиях) имеющийся у Пользователя экземпляр ПО другим лицам.
11. Запрещается производить декомпиляцию и/или модификацию ПО.
12. Запрещается сдавать ПО в аренду, прокат или во временное пользование.
13. Запрещается разделять ПО на составляющие части для использования их на разных компьютерах.
14. Запрещается использовать ПО с целью создания данных или кода, предназначенных для использования другими программными продуктами.
15. Не существует никаких других прямо выраженных или подразумеваемых гарантий или условий, в том числе гарантий товарности и пригодности ПО для конкретных целей.
16. Пользователь согласен с тем, что никакое ПО не свободно от ошибок и что рекомендуется регулярно создавать резервные копии своих файлов.
17. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Руководстве Пользователя, а также в случае нарушения Пользователем условий настоящего Соглашения.
18. В МАКСИМАЛЬНОЙ СТЕПЕНИ, ДОПУСКАЕМОЙ ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И/ИЛИ ЕГО ПАРТНЕРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКИЕ-ЛИБО УБЫТКИ И/ИЛИ УЩЕРБ (В ТОМ ЧИСЛЕ УБЫТКИ В СВЯЗИ С НЕДОПОЛУЧЕННОЙ КОММЕРЧЕСКОЙ ПРИБЫЛЬЮ, ПРЕРЫВАНИЕМ ДЕЯТЕЛЬНОСТИ, УТРАТОЙ ИНФОРМАЦИИ ИЛИ ИНОЙ ИМУЩЕСТВЕННЫЙ УЩЕРБ), ВОЗНИКАЮЩИЕ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИЛИ НЕВОЗМОЖНОСТЬЮ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ БЫЛИ УВЕДОМЛЕНЫ О ВОЗМОЖНОМ ВОЗНИКНОВЕНИИ ТАКИХ УБЫТКОВ И/ИЛИ УЩЕРБА. В ЛЮБОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ ПРАВООБЛАДАТЕЛЯ И ЕГО ПАРТНЕРОВ ПО ЛЮБОМУ ИЗ ПОЛОЖЕНИЙ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ОГРАНИЧИВАЕТСЯ СУММОЙ, ФАКТИЧЕСКИ УПЛАЧЕННОЙ ПОЛЬЗОВАТЕЛЕМ ЗА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. НАСТОЯЩИЕ ОГРАНИЧЕНИЯ НЕ МОГУТ БЫТЬ ИСКЛЮЧЕНЫ ИЛИ ОГРАНИЧЕНЫ В СООТВЕТСТВИИ С ПРИМЕНИМЫМ ПРАВОМ.
19. ЗА ИСКЛЮЧЕНИЕМ УСТАНАВЛИВАЕМОЙ В НАСТОЯЩЕМ ПУНКТЕ ОГРАНИЧЕННОЙ ГАРАНТИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ НА ЕГО ИСПОЛЬЗОВАНИЕ ИЛИ ПРОИЗВОДИТЕЛЬНОСТЬ. ЗА ИСКЛЮЧЕНИЕМ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ, СТЕПЕНЬ КОТОРЫХ НЕ МОЖЕТ БЫТЬ ИСКЛЮЧЕНА ИЛИ ОГРАНИЧЕНА ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ (ВЫРАЖАЕМЫХ В ЯВНОЙ ИЛИ В ПОДРАЗУМЕВАЕМОЙ ФОРМЕ) НА ВСЕ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ НЕНАРУШЕНИЕ ПРАВ ТРЕТЬИХ ЛИЦ, КОММЕРЧЕСКОЕ КАЧЕСТВО, ИНТЕГРАЦИЮ ИЛИ ПРИГОДНОСТЬ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ПОЛЬЗОВАТЕЛЬ СОГЛАСЕН С ТЕМ, ЧТО ОН НЕСЕТ ОТВЕТСТВЕННОСТЬ ЗА ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, ЗА УСТАНОВКУ И ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ЗА РЕЗУЛЬТАТЫ, ПОЛУЧЕННЫЕ С ЕГО ПОМОЩЬЮ.
20. Пользователь самостоятельно несет ответственность за неправомерное использование ПО.
21. Пользователь самостоятельно несет ответственность и обеспечивает соблюдение применимого экспортного и импортного законодательства, а также применимых торговых санкций и эмбарго в отношении передачи прав и использования ПО.
22. Правообладатель и/или его Партнеры не несут ответственности за какой-либо ущерб, связанный с использованием или невозможностью использования ПО.
23. Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) Пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду (“ПО с открытым исходным кодом”). Если такая лицензия предусматривает предоставление исходного кода пользователям, которым предоставляется ПО в формате

исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса Правообладателю или сопровождается с продуктом.

24. Данный продукт использует библиотеку Windows Installer XML (WiX) 3.0 Copyright (c) 2005-2008 Microsoft Corporation под лицензией CPL 1.0

Дистрибутив библиотеки: http://sourceforge.net/projects/wix/.

25. ПО, документация, как и все другие объекты авторского права, а также системы, идеи и методы работы, другая информация, которая содержится в ПО, товарные знаки являются объектами интеллектуальной собственности Правообладателя или его Партнеров. Данное Лицензионное соглашение не дает Вам никаких прав на использование объектов интеллектуальной собственности, включая товарные знаки и знаки обслуживания Правообладателя или его Партнеров, за исключением прав, предоставленных настоящим Лицензионным соглашением.
26. Исходный код, код активации и/или лицензионный ключ для ПО являются собственностью Правообладателя.
27. Пользователь не может удалять или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.
28. Настоящее Соглашение и информация включенная в его состав письменной ссылкой (включая ссылки на информацию, содержащуюся на веб сайтах или ссылки на применимые правила), совместно со всеми дополнительными письменными условиями, представляют собой полный объем Соглашения.
29. За нарушение исключительных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством.
30. Права на ПО, а также на торговые марки связанные или включенные в ПО охраняются по всему миру.

ПРИЛОЖЕНИЕ В. ЛИЦЕНЗИЯ НА БИБЛИОТЕКУ WINDOWS INSTALLER XML (WIX)

В этом приложении содержится текст лицензии на библиотеку Windows Installer XML (WiX) 3.0 Copyright (c) 2005-2008 Microsoft Corporation.

> **Примечание:**
>
> Текст лицензии приводится по источнику: http://www.opensource.org/licenses/cpl1.0.php.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLICLICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAMCONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

   "Contribution" means:

   a. in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b. in the case of each subsequent Contributor:

   c. changes to the Program, and

   d. additions to the Program;

   where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

   a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

   b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

   c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights

needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i. effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii. effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii. states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv. states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and as-

sumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

   EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

   If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

   If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

   All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

   Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

   This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

ГЛОССАРИЙ

InfoWatch CryptoStorage

Система, которая предназначена для криптографической защиты конфиденциальной информации, хранящейся на компьютере пользователя или на локальных сетевых ресурсах, от несанкционированного доступа.

Владелец защищенного объекта

Пользователь, который создал защищенный объект и имеет право на его администрирование.

Гарантированное удаление объекта

Функция уничтожения папок, которая не только удаляет имя объекта из файловой системы, но и затирает содержимое удаляемого объекта.

Защита информации

Меры для ограничения доступа к информации пользователей (категорий пользователей).

Защищенный контейнер

Файл специального формата, который отображается Системой как виртуальный логический диск. Сами данные размещаются в файле.

Защищенный объект

Под защищенными объектами понимаются любые объекты, предназначенные для хранения данных, которые защищены средствами InfoWatch CryptoStorage.

Защищенный объект – это специализированный объект (файл-контейнер) или объект хранения данных (логический диск, папка и т.п.), который содержит зашифрованные конфиденциальные данные, снабженные списком доступа.

Конфиденциальные данные

Данные, доступ к которым ограничивается. Конфиденциальные данные становятся доступными только пользователям, которые включены в список доступа к этим данным.

Многопользовательский доступ

Работа с данными, хранящимися в защищенном объекте, пользователей, которые включены в список доступа к этому объекту.

Пароль

Последовательность символов, которая используется для доступа к содержимому защищенного объекта. Пользователь должен хранить свой пароль в тайне.

Пользователь защищенного объекта

Это любой пользователь, которого владелец включил в список доступа к защищенному объекту. Пользователь имеет ограниченный набор прав на работу с защищенным объектом.

Прозрачное шифрование

Механизм, при котором в процессе установки защиты информация шифруется, и хранится в защищенном объекте исключительно в зашифрованном виде. Работа с защищенным объектом осуществляется таким образом, что при обращении к данным они автоматически расшифровываются в оперативной памяти, а при записи – снова зашифровываются.

УКАЗАТЕЛЬ