Защита программного обеспечения Комплекса Решений АСКОН от несанкционированного использования

Руководство пользователя

7 мая 2009 года

Содержание

Введение

Система защиты программного обеспечения от несанкционированного использования при помощи технологии HASP SRM компании Aladdin Knowledge Systems Ltd представляет собой программно-аппаратный комплекс, использующий 128-битный криптографический алгоритм в соответствии со стандартом Advanced Encryption Standard (AES).

Глава 1.

Аппаратная защита; общие сведения

1.1. Устройство аппаратной защиты

В стандартную поставку Комплекса входит устройство защиты от несанкционированного использования — ключ аппаратной защиты (рис. 1.1), который устанавливается в разъем USB-порта компьютера. Ключ обладает собственной памятью, в которой хранится информация об оплаченных компонентах Комплекса и условиях их использования.

Аппаратная защита Комплекса от несанкционированного использования обеспечивается применением ключей HASP HL с прошивкой версии 3.21.

Рис. 1.1. Ключи аппаратной защиты

Для обеспечения гибкости условий лицензирования могут быть использованы ключи различных типов (табл. 1.1). Все модели ключей обеспечивают защиту от несанкционированного копирования и использования программ. Отличия между ключами различных типов заключаются в особенностях управления лицензиями, записанными на ключе и объеме памяти, доступной для использования.

Табл. 1.1. Типы ключей аппаратной защиты, используемых в Комплексе

Тип ключа	Описание	Тип поддерживаемых лицензий
HASP HL Pro HASP HL Max	Защита нескольких приложений и их компонентов на локальном компьютере.	▼ Бессрочная, ▼ Компонентоориентированная, ▼ По количеству запусков продукта, ▼ Демонстрационная, ▼ Схема лицензирования, настраиваемая по счетчику запусков.
HASP HL Time	Защита нескольких приложений и их компонентов на локальном компьютере. Содержит встроенные часы реального времени.	▼ Бессрочная, ▼ Компонентоориентированная, ▼ Подписная (оплата обновлений и новых версий), ▼ Арендная (оплата оговоренного времени эксплуатации), ▼ Схема лицензирования, настраиваемая по состоянию встроенных часов.

Табл. 1.1. Типы ключей аппаратной защиты, используемых в Комплексе

Тип ключа	Описание	Тип поддерживаемых лицензий
HASP HL Net	Сетевая защита нескольких приложений и их компонентов.	▼ Бессрочная, ▼ Компонентоориентированная, ▼ Подписная или арендная, ▼ Плавающая (передаваемая между пользователями), ▼ По количеству запусков продукта, ▼ Демонстрационная, ▼ Схема лицензирования, настраиваемая по количеству пользователей и счетчику запусков.
HASP HL NetTime	Сетевая защита нескольких приложений и их компонентов. Содержит встроенные часы реального времени.	▼ Бессрочная, ▼ Компонентоориентированная, ▼ Передаваемая между пользователями, ▼ По количеству запусков продукта, ▼ Демонстрационная, ▼ Схема лицензирования, настраиваемая по количеству пользователей, счетчику запусков и состоянию встроенных часов.

Ключи аппаратной защиты, изготовленные по технологии HASP SRM, за исключением ключей типа HASP HL Max, обратно совместимы с ключами HASP4 и HASP HL, которые использовались для защиты Комплекса предыдущих версий.

Ключи HASP HL могут быть перепрограммированы таким образом, чтобы использовать все возможности новой технологии (см. раздел 2.4. на с. 32).

1.2. Программная реализация системы защиты

При установке Комплекса на каждом рабочем месте автоматически и безусловно устанавливается программа защиты *HASP SRM Run-time Environment*. Она обеспечивает запуск программного обеспечения, защищенного системой HASP SRM и его взаимодействие с ключом защиты во время работы. При установке этой программы автоматически устанавливаются следующие компоненты программного обеспечения HASP SRM.

- Драйвер ключа аппаратной защиты.
- *HASP SRM Admin Control Center* — обеспечивает управление сетевыми лицензиями (см. раздел 2.1. на с. 10).
- *HASP SRM Remote Update System* — обеспечивает обновление лицензий в установленных ключах при изменении лицензионного соглашения (см. раздел 2.3. на с. 29).

1.3. Схема защиты

Система HASP SRM позволяет использовать защищенное программное обеспечение, установленное на локальных компьютерах либо на компьютерах, объединенных в локальную сеть.

Корректной работе защиты HASP SRM может препятствовать сетевой экран (например, Брандмауэр Windows). Если при наличии ключа и лицензии на нем приложения Комплекса не запускаются, необходимо изменить настройки сетевого экрана.

1.3.1. Локальные ключи аппаратной защиты

Для работы защищенного приложения на локальном компьютере могут использоваться локальные ключи следующих типов:

- HASP HL Pro,
- HASP HL Max,
- HASP HL Time.

Один или несколько таких ключей (в соответствии с выбранными условиями лицензирования) входят в комплект поставки отдельного рабочего места.

В памяти локального ключа записаны сведения об оплаченных компонентах и условиях лицензирования.

1.3.2. Сетевые ключи аппаратной защиты

Для использования Комплекса, установленного на компьютерах, объединенных в локальную сеть, достаточно сетевого ключа аппаратной защиты типа HASP HL Net или HASP HL NetTime. В память ключа записаны сведения об оплаченных компонентах, количестве лицензий и условиях лицензирования. Этот ключ подключается к одному из компьютеров локальной сети, на котором установлена программа защиты *HASP SRM Run-time Environment*.

Сетевой ключ входит в комплект поставки нескольких рабочих мест, предназначенных для работы в сети. Он позволяет работать с каждым компонентом Комплекса нескольким пользователям одновременно. Максимальное количество пользователей, одновременно работающих с каждым компонентом, определяется количеством лицензий на этот компонент. Компьютер, на котором установлен сетевой ключ, называется **сервером сетевого ключа**.

На компьютерах, объединенных в сеть, для запуска Комплекса вместе с сетевым ключом могут использоваться и локальные.

1.3.3. Порядок использования защищенного программного обеспечения

При загрузке Комплекса и/или отдельных компонентов выполняется поиск действующих и доступных лицензий на их использование. Первоначально проверяется локальный ключ. Если требуемые лицензии не обнаружены на локальном ключе, автоматически выполняется их поиск на доступных сетевых ключах.

Если лицензии не найдены, Комплекс будет запущен в ознакомительном режиме. В этом режиме обеспечивается полная функциональность Комплекса и всех компонентов в течение 30 календарных дней с момента первого запуска.

Ознакомительный режим является однократным для конкретного компьютера.

Чтобы запустить Комплекс заведомо в ознакомительном режиме, необходимо выполнить следующие действия:

- отключить локальный ключ,
- в настройках *HASP SRM Admin Control Center* отключить возможность использования сетевых ключей (см. раздел 2.2.3. на с. 26).

Если при последующих запусках Комплекса ключ не найден или на нем нет лицензии на Комплекс и/или запускаемые компоненты, или исчерпано количество лицензий на сетевом ключе, или исчерпан лимит времени на ключе со встроенными часами (HASP HL NetTime или HASP HL Time), то Комплекс не запускается.

В процессе работы Комплекс периодически проверяет наличие локального или сетевого ключа аппаратной защиты и определяет, разрешено ли использование загруженных в данный момент компонентов. Проверка ключа выполняется в фоновом режиме, практически не задерживая работу пользователя.

Если при выполнении такой проверки ключ не обнаружен, или произошел сбой при обращении к нему, или исчерпан лимит времени на ключе со встроенными часами, на экране появится предупреждающее сообщение о завершении работы Комплекса.

После нажатия кнопки **OK** в этом сообщении окно Комплекса будет закрыто.

После нажатия кнопки **Отмена** будет выполнена повторная проверка ключа.

1.4. Установка системы защиты Комплекса

Установка системы защиты Комплекса на компьютер включает в себя два этапа:

- установку программного обеспечения системы HASP SRM, обеспечивающего работу защищенного приложения,
- установку ключа аппаратной защиты в USB-порт компьютера.

Программное обеспечение системы защиты *HASP SRM Run-Time Environment* автоматически и безусловно устанавливается на компьютер во время установки Комплекса.

На время установки Комплекса рекомендуется выключать антивирусные программы и сетевые экраны, например, Брандмауэр Windows.

Ключ аппаратной защиты необходимо вставить в свободный разъем USB-порта после установки программного обеспечения.

Никаких дополнительных действий выполнять не нужно, так как Комплекс автоматически проверяет, установлен ли ключ на компьютере.

Глава 2.

Использование программного обеспечения системы защиты

2.1. Управление лицензиями при сетевом использовании Комплекса

При установке *HASP SRM Run-time Environment* на каждом компьютере устанавливается менеджер лицензий *HASP License Manager*. Он позволяет управлять лицензиями при сетевом использовании Комплекса и его компонентов. Для доступа к менеджеру лицензий и управлению ими используется программа *Admin Control Center* (далее ACC), входящая в состав *HASP SRM Run-time Environment*.

Умолчательная конфигурация ACC обеспечивает доступ ко всем командам программы и изменениям ее настроек. Программа ACC, запущенная на любом компьютере сети, обеспечивает управление Менеджерами лицензий всех компьютеров. Рекомендуется разграничить доступ пользователей к ресурсам ACC, установленных на их компьютерах.

2.1.1. Запуск Admin Control Center

Способы запуска

В общем случае, чтобы запустить ACC, необходимо в окне браузера (Internet Explorer, Opera, и т.п.) ввести доменное имя или IP-адрес компьютера с установленным менеджером лицензий, номер порта 1947 (например, *http://10.3.1.37:1947* или *http://LM_server:1947*) и перейти по этому адресу.

Порт 1947 должен быть открыт, иначе использование ACC будет невозможно.

Чтобы получить доступ к менеджеру лицензий на удаленном компьютере, необходимо выполнение следующих условий:

- в настройках ACC удаленного компьютера должен быть разрешен доступ удаленных пользователей (см. раздел 2.2.4. на с. 28),
- для изменения настроек ACC удаленного компьютера необходимо знать пароль на доступ к ACC этого компьютера (см. раздел *Парольная защита ACC* на с. 24).

Чтобы получить доступ к менеджеру лицензий на локальном компьютере, содержание адресной строки должно быть следующим: *http://localhost:1947*.

Использование языковых шаблонов

Оригинальным языком интерфейса ACC является английский. В комплект поставки входит шаблон, обеспечивающий использование интерфейса и справочной системы на русском языке.

Подробная информация об использовании шаблонов для локализации ACC содержится в документации на сайте разработчика программы.

Использование адресной строки вида *http://<имя сервера>:1947* приведет к запуску англоязычной версии ACC.

Чтобы запустить ACC с использованием русскоязычного интерфейса, необходимо в адресной строке указать имя папки, в которой сохранен шаблон русского языка. Таким образом адресная строка для запуска русскоязычной версии ACC должна иметь вид

http://<имя сервера>:1947/ACCRUS.

Однако даже при использовании русскоязычного интерфейса ACC могут возникнуть ситуации, когда при выполнении команды программы, переходах между ее вкладками и т.п. интерфейс переключится на английский язык. Это связано со способом русификации, который используется разработчиком программы защиты.

Последующее описание интерфейса ACC приводится для обоих вариантов используемого интерфейса — русского и английского. Английский вариант имени команды приводится в скобках.

2.1.2. Интерфейс ACC

После запуска ACC на экране появится окно умолчательного браузера, в котором открыта страница программы. На рисунке 2.1 показано окно Internet Explorer после запуска ACC. Вызвана команда **Ключи HASP (HASP Keys)**

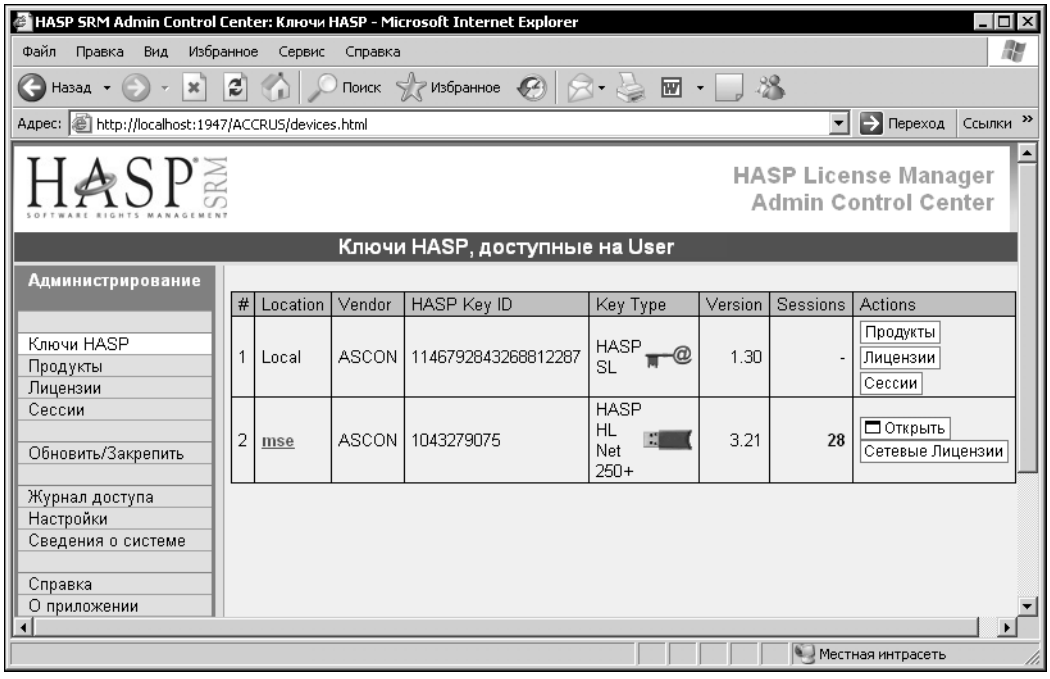


Рис. 2.1. Окно Internet Explorer

В левой части страницы представлено меню команд ACC. Описание команд приведено в табл. 2.1. Эти команды относятся к Менеджеру лицензий компьютера, сетевое имя или IP-адрес которого показан в строке заголовка ACC (далее упоминается как *текущий компьютер*). После вызова команды в окне браузера появляется новая вкладка, элементы управления которой позволяют выполнять дополнительные действия, связанные с этой командой.

Табл. 2.1. Описание команд Admin Control Center

Имя команды	Назначение команды
Ключи HASP (HASP Keys)	Отображает список сетевых и локальных ключей аппаратной защиты, доступных в сети.
Продукты (Products)	Отображает список всех приложений, доступных в сети при помощи всех Менеджеров лицензий.
Лицензии (Features)	Отображает следующие сведения: ▼ список компонентов Комплекса, лицензированных для каждого ключа, включая сетевые и локальные ключи, ▼ условия лицензирования компонентов, ▼ количество пользователей, использующих каждый компонент.
Сессии (Sessions)	Отображает сессии клиентов на текущем компьютере, как локальных, так и подключенных к Менеджеру лицензий на этом компьютере по сети. При необходимости сессии могут быть завершены принудительно.
Обновить/ Закрепить (Update/Attach)	Позволяет обновить лицензию на ключе (см. также раздел 2.3. на с. 29).
Журнал доступа (Access Log)	Отображает журнал истории подключений к Менеджеру лицензий на текущем компьютере. Журнал может сохраняться в текстовом файле *access.log*, который автоматически создается в той же папке, что и файл настроек ACC *hasplm.ini*. Полный путь к этому файлу отображается в нижней части вкладки браузера на странице настройки ACC (см. раздел 2.2. на с. 20).
Настройки (Configuration)	Позволяет настроить параметры использования ACC на текущем компьютере, например, доступ пользователей к управлению ACC, доступ к удаленному Менеджеру лицензий с текущего компьютера, доступ удаленных пользователей к Менеджеру лицензий текущего компьютера, формат создаваемых файлов журнала отчета (см. раздел 2.2. на с. 20).
Сведения о системе (Diagnostics)	Позволяет просмотреть сведения о текущем Менеджере лицензий и подготовить отчет для службы технической поддержки.

Табл. 2.1. Описание команд Admin Control Center

Имя команды	Назначение команды
Справка (Help)	Обеспечивает доступ к справочной системе ACC.
О приложении (About)	Предоставляет сведения о версии Менеджера лицензий и содержит ссылку на сайт базы знаний разработчика системы HASP SRM.

В правом нижнем углу страницы каждой команды находится ссылка для вызова раздела справочной системы ACC, связанного с этой страницей.

2.1.3. Просмотр списка ключей, доступных в сети

Чтобы просмотреть список сетевых и локальных ключей аппаратной защиты, подключенных к компьютерам сети, вызовите команду **Ключи HASP** (**HASP Keys**). В окне браузера появится страница **Ключи HASP, доступные на** (**HASP Keys available on**) **<имя текущего компьютера>**.

На этой странице отображается таблица, содержащая сведения о ключах. Описание элементов таблицы приведено в табл. 2.2.

Табл. 2.2. Таблица списка ключей, доступных в сети

Имя колонки	Содержание колонки
Location	Имя компьютера, к которому подключен ключ. Если ключ подключен к текущему компьютеру, его имя будет показано как *Local*. Имя удаленного компьютера является ссылкой. После перехода по этой ссылке текущим становится этот компьютер. ACC этого компьютера будет открыто на новой вкладке. В настройках ACC удаленного компьютера должен быть разрешен доступ удаленных пользователей (см. раздел 2.2.4. на с. 28).
Vendor	Код поставщика программного обеспечения.
HASP Key ID	Уникальный идентификатор ключа.
Key Type	Обозначение типа ключа аппаратной защиты и его уменьшенное изображение.
Version	Номер версии прошивки ключа.
Sessions	Количество открытых сеансов доступа (сессий) для ключа.

Табл. 2.2. Таблица списка ключей, доступных в сети

Имя колонки	Содержание колонки
Actions	Команды, обеспечивающие доступ к дополнительным сведениям о ключе. Набор команд зависит от того, является ли ключ сетевым или локальным. ▼ **Сессии** (**Sessions**) — позволяет открыть вкладку, содержащую информацию о сессиях для этого ключа. ▼ **Лицензии** (**Features**) — позволяет открыть вкладку, содержащую информацию о компонентах приложения, лицензии для которых записаны на этом ключе. Доступна для локального ключа текущего компьютера. ▼ **Мигать/Не мигать** (**Blink on/off**) — позволяет управлять мерцанием светодиода ключа, позволяя идентифицировать его. ▼ **Открыть** (**Browse**) — позволяет просмотреть все компоненты приложения для заданного сетевого ключа. Менеджер лицензий, установленный на компьютере, к которому подключен этот ключ, будет открыт на новой вкладке браузера. Доступ к удаленному менеджеру лицензий возможен, если в его настройках разрешен доступ удаленных пользователей (см. раздел 2.2.4. на с. 28). ▼ **Сетевые лицензии** (**Net Features**) — позволяет просмотреть компоненты приложения для заданного сетевого ключа, доступные для текущего компьютера.

В списке доступных локальных и сетевых ключей аппаратной защиты первым показан локальный ключ программной защиты. Этот ключ обеспечивает работу Комплекса и отдельных компонентов в течение ознакомительного периода. Команда **Лицензии** (**Features**) позволяет просмотреть следующие сведения об этом периоде:

- состояние (запущена работа в ознакомительном периоде или нет, возможна работа в ознакомительном режиме или срок его действия истек),
- дату и время начала и окончания.

2.1.4. Просмотр полного списка приложений, доступных для текущего компьютера в сети

Чтобы просмотреть список приложений, вызовите команду **Продукты** (**Products**). В окне браузера появится страница **Продукты, доступные на** (**Products available on**) **<имя текущего компьютера>**.

На этой странице отображается таблица, содержащая обозначения приложений, относящихся ко всем Менеджерам лицензий в сети. Описание элементов таблицы приведено в табл. 2.3.

Табл. 2.3. Таблица списка приложений, доступных для текущего компьютера в сети

Имя колонки	Содержание колонки
Product Name	Имя приложения, определенное поставщиком.
Vendor	Код поставщика программного обеспечения.
Location	Имя компьютера, к которому подключен ключ для данного компонента. Если ключ подключен к текущему компьютеру, его имя будет показано как *Local*.
Actions	Команды, обеспечивающие доступ к дополнительным сведениям о приложении. ▼ **Лицензии** (**Features**) — позволяет открыть страницу **Лицензии на** (**Features on**) **<имя текущего компьютера>**, отображающую список компонентов приложения.

2.1.5. Просмотр списка компонентов приложения

Чтобы просмотреть список компонентов приложения, лицензированных на ключах, доступных в сети, вызовите команду **Лицензии** (**Features**). В окне браузера появится страница **Лицензии, доступные на** (**Features available on**) **<имя текущего компьютера>**.

На этой странице отображается таблица, содержащая сведения о компонентах приложения, лицензированных на каждом из ключей (сетевых и локальных), доступных в сети. В таблице приводятся сведения об условиях лицензирования и текущем использовании компонентов. Описание элементов таблицы приведено в табл. 2.4.

Табл. 2.4. Таблица списка компонентов приложения, лицензированных на ключах, доступных в сети

Имя колонки	Содержание колонки
Vendor ID	Код поставщика программного обеспечения.
HASP Key ID	Уникальный идентификатор ключа.
Feature ID	Уникальный идентификационный номер и наименование компонента приложения, установленное поставщиком.
Location	Имя компьютера, к которому подключен ключ. Если ключ подключен к текущему компьютеру, его имя будет показано как *Local*.

Табл. 2.4. Таблица списка компонентов приложения, лицензированных на ключах, доступных в сети

Имя колонки	Содержание колонки
Access	Тип компьютеров, для которых разрешен доступ к использованию компонента. Возможными вариантами являются следующие: ▼ *Loc* — доступ разрешен только для локального компьютера, ▼ *Net* — доступ разрешен для удаленных компьютеров по сети, ▼ *Disp* — доступ разрешен для удаленных компьютеров с использованием терминального сервера (в Комплексе не используется).
Count	Способ подсчета количества использований компонента. Возможными вариантами являются следующие: ▼ *Process* — все запросы доступа к использованию одного процесса считаются одним доступом, ▼ *Station* — все запросы доступа к использованию одного компьютера считаются одним доступом, ▼ *Login* — в подсчет количества использований компонента включаются все запросы к использованию.
Logins	Количество пользователей, использующих компонент приложения в текущий момент времени.
Limit	Максимально возможное количество пользователей, которые могут одновременно использовать компонент.
Detached	В настоящее время не используется.
Restrictions	Ограничения, связанные с использованием компонента приложения на данном ключе. Например, *Expired* — истек срок действия лицензии на ключе со встроенными часами реального времени.
Sessions	Количество текущих сеансов доступа к ключу.
Actions	Команды, обеспечивающие доступ к дополнительным сведениям о приложении. ▼ **Сессии** (**Sessions**) — позволяет открыть страницу **Сессии на** (**Sessions on**) **<имя текущего компьютера>**, содержащую сведения о сеансах доступа к конкретному компоненту приложения.

2.1.6. Просмотр списка сеансов доступа к защищенным продуктам и управление сеансами

Чтобы просмотреть список сеансов доступа, необходимо вызвать команду **Сессии** (**Sessions**). В окне браузера откроется страница **Сессии на** (**Sessions on**) **<имя текущего компьютера>**.

На этой странице отображается таблица, содержащая сведения о всех сеансах доступа локальных и удаленных пользователей к текущему компьютеру. Элементы управления, расположенные на странице, обеспечивают просмотр сведений о сеансах доступа и позволяют прерывать их. Описание элементов таблицы приведено в табл. 2.5.

Табл. 2.5. Таблица списка сеансов доступа к текущему компьютеру

Имя колонки	Содержание колонки
ID	Уникальный идентификатор сессии.
HASP Key ID	Уникальный идентификатор ключа.
Location	Имя или IP-адрес компьютера, к которому подключен ключ. Если ключ подключен к текущему компьютеру, его имя будет показано как *Local*.
Feature ID	Уникальный идентификационный номер и наименование компонента приложения, установленное поставщиком.
Address	IP-адрес компьютера, с которого выполнен доступ или *Local*, если доступ выполнен с локального компьютера.
User	Имя пользователя, использующего компонент приложения.
Machine	Сетевое имя компьютера, с которого используется компонент приложения, и идентификатор процесса, открывшего сеанс доступа.
Login Time	Время начала сеанса доступа к компоненту приложения.
Timeout	Оставшееся время использования лицензии (сеанса доступа). По истечении указанного промежутка времени сеанс доступа к компоненту приложения будет автоматически прерван. На экране появится предупреждающее сообщение об этом. Максимальная длительность использования лицензии составляет 12 часов.
Actions	Команды, обеспечивающие доступ к дополнительным сведениям о приложении. ▼ **Отключить** (**Disconnect**) — позволяет прервать сеанс доступа текущего пользователя к текущему компоненту приложения (отключить пользователя от лицензии). Для выполнения команды необходимо знать пароль доступа к ACC компьютера, к которому подключен ключ аппаратной защиты (см. раздел *Парольная защита ACC* на с. 24).

2.1.7. Просмотр журнала истории подключений к Менеджеру лицензий на текущем компьютере

Чтобы просмотреть журнал истории подключений, необходимо вызвать команду **Журнал доступа** (**Access Log**). В окне браузера появится страница **Журнал доступа для** (**Access Log for**) **<имя текущего компьютера>**.

На этой странице отображается таблица, содержащая сведения о сеансах доступа локальных и удаленных пользователей к Менеджеру лицензий текущего компьютера. По умолчанию в таблице показаны крайние 20 записей. Кнопки **20**, **100** и **1000** позволяют выбрать количество отображаемых записей на странице.

Каждая запись журнала по умолчанию содержит следующие сведения:

- дату и время формирования записи,
- IP адрес и порт пользователя,
- идентификатор пользователя,
- метод доступа,
- URL ресурса, к которому адресован запрос,
- используемую функцию,
- параметры функции,
- значение, возвращаемое функцией.

Умолчательный шаблон журнала может быть изменен на вкладке **Общие настройки** (**Basic Settings**) страницы настройки ACC (см. раздел *Шаблон журнала учета* на с. 22).

Если на вкладке **Общие настройки** (**Basic Settings**) страницы конфигурации ACC включена опция **Вести журнал доступа** (**Write an Access Log File**), журнал истории подключений сохраняется в текстовом файле *access.log*. Файл автоматически создается в той же папке, что и файл настроек ACC *hasplm.ini*. Полный путь к этому файлу отображается в нижней части вкладки браузера на странице настройки ACC (см. раздел 2.2. на с. 20). По умолчанию указанные файлы сохраняются в папке *C:\Program Files\Common Files\Aladdin Shared\HASP*.

2.1.8. Просмотр сведений о текущем Менеджере лицензий

Чтобы просмотреть сведения о текущем Менеджере лицензий, необходимо вызвать команду **Сведения о системе** (**Diagnostics**). В окне браузера появится страница **Сведения по HASP License Manager на** (**Diagnostics for HASP License Manager on**) **<имя текущего компьютера>**.

На этой странице отображается таблица, содержащая сведения о Менеджере лицензий. Описание элементов таблицы приведено в табл. 2.6.

Табл. 2.6. Таблица сведений о Менеджере лицензий

Имя колонки	Содержание колонки
HASP License Manager Version	Версия текущего Менеджера лицензий.

Табл. 2.6. Таблица сведений о Менеджере лицензий

Имя колонки	Содержание колонки
Имя компьютера (Computer Name)	Имя компьютера, на котором установлен Менеджер лицензий, и идентификатор процесса (PID).
Операционная система (Host Operating System)	Наименование и версия операционной системы компьютера, на котором запущен Менеджер лицензий.
Протоколы (LM Protocols)	▼ Текущий протокол, используемый Менеджером лицензий. Возможными вариантами значений являются *IPv4* (только IPv4) или *IPv4*, *IPv6* (IPv4 и IPv6). ▼ IP-адрес текущего менеджера лицензий.
Продолжительность работы (Uptime)	Длительность текущего сеанса доступа к Менеджеру лицензий.
Шаблоны (Template Sets)	Список доступных шаблонов интерфейса ACC.
Текущее использование (Current Usage)	Сведения о текущем использовании Менеджера лицензий: ▼ **подключений** (**logins**) — количество захваченных лицензий, ▼ **сессий** (**sessions**) — количество текущих сеансов доступа к Менеджеру лицензий, ▼ **соединений** (**connections**) — количество текущих сетевых соединений из общего количества доступных.
Запросы на подключение (Login Requests)	Количество полученных лицензий у текущего Менеджера лицензий с момента его запуска.
Запросы (Requests)	Количество запросов к Менеджеру лицензий с момента его запуска.
Объем данных (Data Volume)	Количество принятых и переданных этим сервером байт информации с момента запуска Менеджера лицензий.
Ошибки (Errors)	Суммарное количество ошибок, связанное с ключом или передачей на этом сервере с момента запуска Менеджера лицензий.
Потоки (Client Threads)	Количество одновременно протекающих подпроцессов, открытых Менеджером лицензий.
Драйверы (Run-time)	Список запущенных компонентов системы HASP SRM с указанием их версий.

Табл. 2.6. Таблица сведений о Менеджере лицензий

Имя колонки	Содержание колонки
Создать отчет (Generate Report)	Кнопка позволяет создать диагностический отчет в формате HTML. Отчет содержит детальную информацию о системе, на которой запущен конкретный экземпляр Менеджера лицензий, использовании лицензий и другие сведения, которые могут быть использованы в диагностических целях. Отчет следует использовать при обращении в службу технической поддержки.

2.2. Настройка ACC

Настройки ACC позволяют определить следующие параметры:

- права доступа пользователей к сетевым ресурсам системы защиты,
- параметры доступа к удаленным Менеджерам лицензий,
- права доступа пользователей сетевых компьютеров к управлению Менеджером лицензий текущего компьютера.

Чтобы выполнить настройки, необходимо вызвать команду **Настройки** (**Configuration**). В окне браузера появится страница **Настройки для HASP License Manager на** (**Configuration for HASP License Manager on**) **<имя текущего компьютера>**.

На вкладках этой страницы сгруппированы элементы управления, позволяющие выполнить настройку. Названия вкладок соответствуют типу настроек.

Для выполнения настроек ACC необходимо ввести пароль администратора, если он был ранее задан (см. раздел *Парольная защита ACC* на с. 24).

Настройки ACC сохраняются в файле *hasplm.ini*, который создается автоматически при первом изменении умолчательных настроек. Полный путь к файлу отображается в нижней части вкладки браузера.

2.2.1. Общие настройки ACC; вкладка Общие настройки (Basic Settings)

Общие настройки ACC

Общие настройки ACC включают в себя задание имени компьютера, ACC которого настраивается, параметры формирования журналов отчетов и настройку парольной защиты. Описание элементов управления вкладки приведено в табл. 2.7.

Табл. 2.7. Элементы управления вкладки **Общие настройки** (**Basic Settings**)

Имя элемента управления	Описание
Имя компьютера (Machine Name)	Сетевое имя компьютера, для ACC которого выполняются настройки.
Разрешить удаленный доступ к ACC (Allow Remote Access to ACC)	Опция позволяет управлять доступом удаленных пользователей к ACC компьютера, имя которого задано в поле **Имя компьютера** (**Machine Name**). По умолчанию опция отключена.
Время обновления страницы (Display Refresh Time)	Период обновления информации на вкладках ACC в секундах.
Записей на странице (Table Rows per Page)	Количество строк в таблицах, отображаемых на каждой странице вкладки. Значение может изменяться в пределах от 5 до 100.
Вести Журнал доступа (Write an Access Log File)	Опция позволяет управлять созданием файла журнала учета доступа к Менеджеру лицензий. Если опция включена, становятся доступными следующие опции, позволяющие управлять содержанием журнала: ▼ **Включить локальные запросы** (**Include Local Requests**), ▼ **Включить удаленные запросы** (**Include Remote Requests**), ▼ **Включить административные запросы** (**Include Administration Requests**).
Включить локальные запросы (Include Local Requests)	Опция позволяет добавлять в журнал сведения о сеансах доступа пользователей локального компьютера к компонентам приложения, лицензированным на ключе, подключенном к этому компьютеру.
Включить удаленные запросы (Include Remote Requests)	Опция позволяет добавлять в журнал сведения о сеансах доступа пользователей сетевых компьютеров к компонентам приложения, лицензированным на ключе, подключенном к текущему компьютеру.

Табл. 2.7. Элементы управления вкладки **Общие настройки** (**Basic Settings**)

Имя элемента управления	Описание
Включить административные запросы (Include Administration Requests)	Опция позволяет добавлять в журнал сведения о сеансах доступа к Менеджеру лицензий при помощи ACC.
Вести Журнал ошибок (Write an Error Log File)	Опция позволяет управлять созданием журнала ошибок.
Вести Журнал процессов (Write a Process ID (.pid) File)	Опция позволяет создавать файл идентификаторов процессов.

Шаблон журнала учета

Команда **Редактировать параметры Журнала** (**Edit Log Parameters**) позволяет изменить шаблон журнала учета доступа к Менеджеру лицензий.

После вызова команды **Редактировать параметры Журнала** (**Edit Log Parameters**) в окне браузера появляется страница **Редактирование параметров журнала** (**Edit Log Parameters**). Поле в верхней части страницы содержит текущий набор обозначений элементов шаблона. Содержимое поля представлено в текстовом формате. Обозначения элементов являются зарезервированными словами. Они помещаются между фигурными скобками. Для пояснения элементов журнала можно добавлять к ним комментарии. Обозначения элементов можно редактировать как обычный текст или с использованием содержимого поля **Доступные тэги для журнала:** (**Available tags for log:**).

Поле **Доступные тэги для журнала:** (**Available tags for log:**) содержит обозначения и краткие описания доступных элементов шаблона. Чтобы добавить элемент в шаблон, выделите его мышью и вызовите команду **Добавить** (**Add**). Обозначение элемента будет добавлено в конец списка.

Команда **Назад на страницу "Настройки"** (**Back to Configuration**) позволяет завершить редактирование шаблона и вернуться на страницу конфигурации.

Пример сформированного шаблона журнала приведен на рис. 2.2.

Рис. 2.2. Пример сформированного шаблона

В соответствии с этим шаблоном каждая запись журнала будет содержать следующие сведения:

- дату и время записи,
- идентификатор ключа, лицензия которого используется,
- идентификатор пользователя,
- длительность сеанса использования лицензии,
- идентификатор компонента,
- тип запроса, например, получение лицензии (LOGIN), освобождение лицензии (LOGOUT).
- IP-адрес сервера лицензий,
- код результата выполнения запроса.

Элемент **newline** обеспечивает перевод строки в журнале.

Код результата выполнения запроса может быть использован при анализе возможных неудач при выполнении запросов. Например, значение кода, равное *0*, соответствует успешному выполнению запроса. Значение кода, равное *7*, возвращается в случае, если ключ аппаратной защиты не найден. Полное описание кодов приведено в разделе *API Status Codes* документа *Software Protection and Licensing Guide*. Этот документ сохранен в файле *HASP_SRM_Guide.pdf* и входит в комплект документации системы защиты.

Фрагмент файла журнала, сформированного по шаблону (рис. 2.2), приведен ниже.

2009-01-23 11:30:00 HASP ID:1086818230 ID пользователя:Test@Tester Длительность сессии: 0 days 0 hours 0 minutes 0 seconds ID компонента:120 тип запроса:LOGIN IP сервера лицензий: 127.0.0.1 Код результата:0

2009-01-23 11:31:54 HASP ID:1086818230 ID пользователя:Test@Tester Длительность сессии: 0 days 0 hours 1 minutes 54 seconds ID компонента:120 тип запроса:LOGOUT IP сервера лицензий: 10.3.1.2 Код результата:0

Помимо записей, содержащих сведения об использовании лицензий пользователями, журнал отчета содержит большое количество других сведений. Для удобства анализа журнала целесообразно обеспечить фильтрацию его содержания, например, средствами текстового редактора.

Парольная защита ACC

Команда **Изменить пароль** (**Change Password**) позволяет задать пароль ACC.

При использовании программного обеспечения HASP SRM паролем защищаются следующие действия:

- отключение пользователя от лицензии (см. раздел 2.1.6. на с. 16),
- изменение конфигурации ACC.

Чтобы задать пароль, необходимо вызвать команду **Изменить пароль** (**Change Password**). В окне браузера появится вкладка **Сменить пароль** (**Change Password**). В поле **Текущий пароль Администратора** (**Current Admin Password**) необходимо ввести текущий пароль.

По умолчанию пароль не задан. При первом задании пароля следует оставить поле **Текущий пароль Администратора** (**Current Admin Password**) пустым.

В поле **Новый пароль Администратора** (**New Admin Password**) необходимо ввести новый пароль и повторно ввести его в поле **Подтверждение пароля** (**Re-enter new Admin Password**). После задания нового пароля необходимо вызвать команду **Применить** (**Submit**). Чтобы отказаться от изменений, вызовите команду **Отмена** (**Cancel**).

Вкладка задания пароля будет закрыта. Активной станет вкладка **Общие настройки** (**Basic Settings**).

Прежний пароль продолжает действовать в течение сеанса работы браузера. Чтобы изменения вступили в силу, необходимо перезапустить браузер.

Чтобы изменения настроек, выполненные на вкладке **Общие настройки** (**Basic Settings**), вступили в силу, вызовите команду **Применить** (**Submit**). Команда **По умолчанию** (**Set Defaults**) позволяет вернуть все настройки к умолчательным значениям.

Действие команды **По умолчанию** (**Set Defaults**) не распространяется на установленный пароль.

2.2.2. Настройка доступа пользователей к Менеджеру лицензий; вкладка Пользователи (Users)

Настройки, выполняемые на вкладке **Пользователи** (**Users**), позволяют явно указать имена пользователей, которым разрешен или запрещен доступ к Менеджерам лицензий, и имена компьютеров, на которых установлены Менеджеры лицензий, к которым выполняются попытки доступа.

Описание элементов управления вкладки приведено в табл. 2.8.

Табл. 2.8. Элементы управления вкладки **Пользователи** (**Users**)

Имя элемента управления	Описание
Ограничения пользователей (User Restrictions)	Поле позволяет задать правила разрешений/ограничений, применяемые при попытках доступа к Менеджеру лицензий со стороны пользователей.

Правила имеют следующий формат:

<restricrion>=[username]@[hostname]

Описание параметров приведено в табл. 2.9.

Табл. 2.9. Элементы правил разграничения доступа

Обозначение параметра	Наименование	Возможные значения	Описание
restriction	Тип ограничения	allow	разрешено
		deny	запрещено
hostname	Имя или IP-адрес компьютера	10.3.1.27, test-2	
		all	все компьютеры сети
		none	ни один компьютер сети
username	Имя пользователя	User1, testuser	
		all	все пользователи сети
		none	ни один из пользователей

Параметры *hostname* и *username* являются необязательными. Отсутствие параметра при вводе строки соответствует его значению, равному *all*.

Например, если задать правило вида *allow=[username]*, то доступ к Менеджеру лицензий для пользователя *[username]* будет разрешен вне зависимости от того, на каком компьютере в сети установлен Менеджер лицензий.

Если при вводе строка задана в виде *allow=[username]*, то после подтверждения изменений конфигурации командой **Применить** (**Submit**) она будет преобразована к виду *allow=[username]@all*.

Аналогично, если задать строку вида *allow=@[hostname]*, то доступ к Менеджеру лицензий, установленному на компьютере *[hostname]*, будет разрешен вне зависимости от того, какой пользователь выполняет доступ.

Если при вводе строка задана в виде *allow=@[hostname]*, то после подтверждения изменений конфигурации командой **Применить** (**Submit**) она будет преобразована к виду *allow=all@[hostname]*.

Каждое правило должно быть записано в отдельной строке. Правила обрабатываются по порядку следования сверху вниз. Обработка правил прекращается после нахождения первого соответствия условий.

Примеры обработки правил приведены в табл. 2.10. Предполагается, что все правила записаны в поле **Ограничения пользователей** (**User Restriction**) в том порядке, в котором они расположены в таблице.

Табл. 2.10. Примеры обработки правил разграничения доступа

Правило	Описание обработки правила, выполняемой ACC
deny=User1@seat1	Пользователю *User1* запрещен доступ к Менеджеру лицензий, установленному на компьютере *seat1*.
allow=User1@all	Пользователю *User1* разрешен доступ ко всем компьютерам, за исключением *seat1*. Запрет определяется предыдущим правилом.
allow=User2@all	Пользователю *User2* разрешен доступ ко всем компьютерам.
deny=all@seat2 **deny=all@seat3** **deny=all@seat4**	Всем пользователям запрещен доступ к Менеджерам лицензий, установленным на компьютерах *seat2*, *seat3*, *seat4*, за исключением пользователей *User1* и *User2*. Правила доступа этих пользователей уже обработаны.

Команда **Недавние подключения пользователей** (**Show Recent Users**) позволяет отобразить список пользователей, выполнявших доступ к Менеджерам лицензий последними.

Чтобы изменения настроек, выполненные на этой вкладке, вступили в силу, вызовите команду **Применить** (**Submit**). Команда **Отмена** (**Cancel**) позволяет отказаться от изменений в настройках. Кнопка **По умолчанию** (**Set Defaults**) позволяет вернуть все настройки к умолчательным значениям.

2.2.3. Настройка доступа пользователей к удаленным Менеджерам лицензий; вкладка Доступ к удаленным Менеджерам лицензий (Access to Remote License Managers)

Элементы управления, расположенные на вкладке **Доступ к удаленным Менеджерам лицензий** (**Access to Remote License Managers**), позволяют указать имена компьютеров, с установленными Менеджерами лицензий, к которым может быть выполнен доступ.

Описание элементов управления вкладки приведено в табл. 2.11.

Табл. 2.11. Элементы управления вкладки **Доступ к удаленным Менеджерам лицензий** (**Access to Remote License Managers**)

Имя элемента управления	Описание
Разрешить доступ к удаленным лицензиям (Allow Access to Remote Licenses)	Опция позволяет управлять доступом к Менеджерам лицензий других компьютеров сети с текущего компьютера. По умолчанию включена.
Широковещательный поиск удаленных лицензий (Broadcast Search for Remote Licenses)	Опция позволяет управлять поиском компьютеров с установленными Менеджерами лицензий в сети. Если опция отключена, имена компьютеров, среди которых будет выполнен поиск Менеджеров лицензий, должны быть явно указаны в поле **Определить параметры поиска** (**Specify Search Parameters**). Если опция включена, поиск будет выполняться среди всех компьютеров (широковещательный поиск).
Агрессивный поиск удаленных лицензий (Aggressive Search for Remote Licenses)	Опция позволяет управлять способом поиска компьютеров с установленными Менеджерами лицензий. Если она включена, доступ к удаленным Менеджерам лицензий будет доступным даже в случае невозможности их обнаружения стандартными средства поиска протокола UDP. «Агрессивный» способ поиска уменьшает частоту обновления информации о состоянии системы HASP, однако может позволить обходить файерволы.
Определить параметры поиска (Specify Search Parameters)	Поле позволяет явно указать имена компьютеров, среди которых будет выполнен поиск Менеджеров лицензий. Адреса компьютеров могут быть заданы следующими способами: ▼ IP-адрес компьютера, например, *10.3.1.37*; ▼ сетевое имя компьютера, например, *test-2*; ▼ широковещательный адрес, например, *10.3.1.255*. При использовании протокола *Ipv6* следует записывать адреса в формате этого протокола. Каждый адрес должен располагаться на отдельной строке.

Чтобы изменения настроек, выполненные на этой вкладке, вступили в силу, вызовите команду **Применить** (**Submit**). Команда **Отмена** (**Cancel**) позволяет отказаться от изменений в настройках. Кнопка **По умолчанию** (**Set Defaults**) позволяет вернуть все настройки к умолчательным значениям.

2.2.4. Настройка доступа удаленных пользователей к Менеджеру лицензий текущего компьютера; вкладка Доступ Удаленных клиентов (Access from Remote Clients)

Элементы управления, расположенные на вкладке **Доступ Удаленных клиентов** (**Access from Remote Clients**), позволяют настроить следующие параметры:

- имена компьютеров, пользователям которых разрешен или запрещен доступ к Менеджеру лицензий текущего компьютера,
- правила доступа к Менеджеру лицензий.

Описание элементов управления вкладки приведено в табл. 2.12.

Табл. 2.12. Элементы управления вкладки **Доступ Удаленных клиентов** (**Access from Remote Clients**)

Имя элемента управления	Описание
Разрешить доступ удаленным клиентам (Allow access from Remote Clients)	Опция позволяет управлять доступом удаленных пользователей к Менеджеру лицензий текущего компьютера.
Ограничения доступа (Access Restrictions)	Поле позволяет задать правила разрешений/ограничений, применяемые при попытках доступа к Менеджеру лицензий со стороны пользователей.

Правила имеют следующий формат:

<restricrion>=[item]

Описание параметров приведено в табл. 2.13.

Табл. 2.13. Элементы правил разграничения доступа

Обозначение параметра	Наименование	Возможные значения	Описание
restriction	Тип ограничения	allow	разрешено
		deny	запрещено
item	IP-адрес компьютера или имя компьютера в сети	10.3.1.27 или TEST2	
		all	все компьютеры сети
		none	ни один компьютер сети

Каждое правило должно быть записано в отдельной строке. Правила обрабатываются по порядку следования сверху вниз. Обработка правил прекращается после нахождения первого соответствия условий.

Команда **Недавние подключения клиентов** (**Show Recent Client Access**) позволяет просмотреть список компьютеров, с которых был выполнен доступ к Менеджеру лицензий текущего компьютера за последнее время.

Чтобы изменения настроек, выполненные на этой вкладке, вступили в силу, вызовите команду **Применить** (**Submit**). Команда **Отмена** (**Cancel**) позволяет отказаться от изменений в настройках. Кнопка **По умолчанию** (**Set Defaults**) позволяет вернуть все настройки к умолчательным значениям.

2.3. Дистанционное перепрограммирование ключа аппаратной защиты

Дистанционное перепрограммирование ключа производится с помощью программы системы дистанционного обновления *HASP SRM Remote Update System*.

2.3.1. Общий порядок действий для обновления лицензий

При покупке Комплекса вы получаете сетевые или локальные аппаратные ключи. В памяти ключей содержатся сведения о наборе компонентов Комплекса, которые были оплачены и с которыми, следовательно, разрешено работать пользователю.

В дальнейшем может возникнуть необходимость изменить лицензионные условия, например, приобрести дополнительные компоненты Комплекса и установить их на тот же компьютер, изменить количество лицензий и т.п.

Чтобы изменить лицензионные условия, необходимо выполнить следующие действия.

1. Оформить договор об изменении лицензионных условий.
2. Сформировать файл статуса ключа, содержащий сведения о состоянии лицензий пользователя.
3. Отправить файл статуса в компанию АСКОН по электронной почте.
4. Оплатить добавляемые компоненты.
5. Получить файл ответа из компании АСКОН.
6. Перепрограммировать ключ, записав в его память информацию о вновь приобретенных компонентах.
7. Установить оплаченные компоненты Комплекса.

2.3.2. Формирование файла статуса ключа

Формирование файла статуса ключа и перепрограммирование ключа производится с помощью программы *HASP SRM Remote Update System* (далее HASP SRM RUS). Исполняемым файлом программы является *hasprusa.exe*.

Для запуска HASP SRM RUS запустите на выполнение файл *hasprusa.exe*, расположенный в папке *\HASP* главной папки Комплекса.

После запуска программы на экране появляется окно HASP SRM RUS (рис. 2.3).

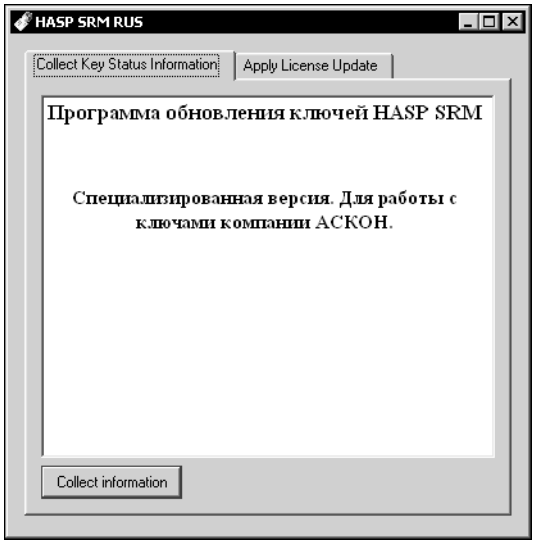


Рис. 2.3. Окно программы обновления лицензий; вкладка сбора сведений

По умолчанию раскрыта вкладка сбора сведений о состоянии лицензий на ключе **Collect Key Status Information**.

Чтобы подготовить файл статуса ключа, выполните следующие действия.

1.Вставьте аппаратный ключ в разъем порта компьютера.

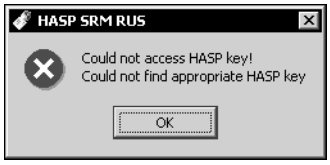
2.Нажмите кнопку **Collect information**.

На экране появится стандартный диалог сохранения файлов Windows. По умолчанию файл статуса ключа имеет расширение *c2v* (от ***c****ustomer to* ***v****endor*).

3.Введите имя файла запроса и закройте диалог.

В окне программы появится сообщение об успешном выполнении операции *Key status retrieved from HASP successfully*. Сформированный файл будет сохранен в указанной папке.

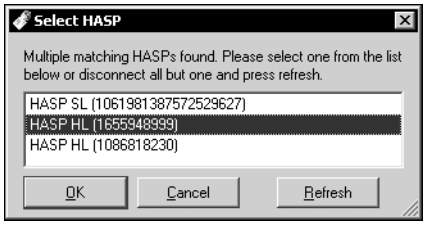
Если при выполнении операции программа не обнаружит ключ, на экране появится предупреждающее сообщение (рис. 2.4).



В этом случае необходимо вставить ключ аппаратной защиты в USB-порт и повторить операцию.

Рис. 2.4.

Если при выполнении операции программа обнаружит несколько ключей, на экране появится диалог **Select HASP** (рис. 2.5).



В этом случае необходимо указать мышью обозначение одного из ключей и нажать кнопку **OK** либо отключить все ключи, кроме нужного, и нажать кнопку **Refresh**.

Рис. 2.5.

Если необходимо обновить лицензии на нескольких ключах, следует выполнить рассмотренные операции для каждого из них поочередно. Для каждого ключа будет сформирован файл статуса.

2.3.3. Отправка файла статуса

Завершив подготовку файлов статуса ключей, отправьте их в компанию АСКОН по электронной почте, сопроводив необходимыми комментариями.

Рекомендуется контактировать с тем офисом, в котором было первоначально приобретено программное обеспечение компании АСКОН. Если вы приобрели Комплекс у регионального дилера, можно выполнить процедуру обновления ключей с его помощью.

2.3.4. Перепрограммирование ключа после получения ответа

После того, как вы оплатите заказанные дополнительные компоненты Комплекса, компания АСКОН вышлет вам файлы, содержащие обновления лицензий.

Файлы обновления могут поставляться в следующих форматах:

- файл с расширением *v2c* (от ***v****endor to* ***c****ustomer*).
- исполняемый файл с расширением *exe*.

Для перепрограммирования ключа с использованием файла с расширением *v2c* выполните следующие действия.

1. Вставьте аппаратный ключ в разъем порта компьютера.
2. Запустите программу HASP SRM RUS и в появившемся на экране окне программы раскройте вкладку обновления лицензий **Apply License Update** (рис. 2.6).

Рис. 2.6. Окно программы обновления лицензий; вкладка обновления лицензии

3. Нажмите кнопку поиска файла обновления **Browse for update file**. На экране появится стандартный диалог открытия файлов Windows.
4. Откройте полученный от компании АСКОН файл обновления.
5. Нажмите кнопку **Apply Update**.

Данные о дополнительных продуктах, содержащиеся в файле обновления лицензии и соответствующие текущему ключу, будут записаны в этот ключ. После успешной записи данных в ключ на экране появляется сообщение об этом.

Если необходимо обновить лицензии на нескольких ключах, следует выполнить рассмотренные операции для каждого из них поочередно.

Если файл обновления предоставлен поставщиком в виде исполняемого файла, имеющего расширение *exe*, для обновления лицензий необходимо запустить этот файл на выполнение. Программа HASP SRM RUS будет запущена автоматически.

2.3.5. Установка компонентов Комплекса

После перепрограммирования ключа аппаратной защиты можно установить компоненты Комплекса, лицензии на которые получены. Для этого выполните следующие действия.

- Запустите Мастер установки Комплекса.
- В окне **Тип обслуживания** выберите вариант **Изменить**.
- В окне **Выборочная установка** укажите необходимые компоненты и завершите установку.

2.4. Обновление прошивки ключа

Прошивка ключей аппаратной защиты HASP HL, полученных от поставщика в комплектах поставки предыдущих версий ПО АСКОН, может быть обновлена до версии 3.21. Эта версия прошивки поддерживает полную функциональность системы защиты HASP SRM. Для обновления прошивки следует использовать программу обновления, исполняемым файлом которой является *FirmwareUpdate.exe*. Этот файл находится в папке *Komplex_2009\support* установочного диска.

Подключите ключ, прошивку которого следует обновить.

Чтобы запустить программу, откройте ее исполняемый файл. На экране появится окно **HASP SRM RUS** (рис 2.7).

Рис. 2.7. Окно программы обновления прошивки

Кнопка **Apply Update** позволяет обновить прошивку ключа аппаратной защиты. После обновления прошивки окно программы следует закрыть.