Guardant®

Система защиты от компьютерного пиратства

Эффективная
защита приложений

Урок 4: дистанционное обновление памяти ключа

Содержание

Общее описание технологии 3

Используемые термины и обозначения 3

Протокол удаленного обновления 4

Доверенное удаленное обновление 5

Шаг 0. Подготовка пароля удаленного обновления 5

Шаг 1. Создание запроса на обновление 6

Шаг 2. Создание дампа обновления 7

Шаг 3. Обновление памяти ключа 9

Шаг 4. Завершение удаленного обновления 10

Заключение 11

Дополнительные источники информации 12

WWW: http://www.guardant.ru 12

Служба технической поддержки: 12

Общее описание технологии

Технология безопасного удаленного обновления предназначена для **обновления памяти ключа**, находящегося у **конечного пользователя** защищенной программы, без передачи электронного ключа разработчику.

Обновление памяти ключа может быть полезно при необходимости:

- Продления срока использования приложения, ограниченного по времени использования или числу запусков
- Активации демо-версии приложения
- Увеличения числа доступных лицензий сетевого приложения
- Обновления версии программы (с изменением архитектуры защиты)
- Покупки конечным пользователем другого защищенного приложения разработчика – для записи новой лицензии в ключ

Основное достоинство технологии заключается в том, что информация, предназначенная для дистанционного обновления памяти ключа, передаваемая от разработчика конечному пользователю, декодируется и обрабатывается только **внутри электронного ключа**.

Для выполнения процедуры удаленного обновления разработчику необходимы:

- Установленный комплект разработчика
- Любой экземпляр электронного ключа **той же модели**, что и у пользователя
- **Пароль удаленного обновления**, записанный в ключ конечного пользователя в момент его последней прошивки.

Пользователю достаточно иметь утилиту **GrdTRU.exe**, распространяемую в составе дистрибутива защищенного приложения.

В рамках данного урока будет приведен протокол процедуры удаленного обновления ключа, а также будут подробно описаны действия, совершаемые сторонами в процессе удаленного обновления памяти ключа.

Используемые термины и обозначения

Доверенное удаленное обновление (**Trusted Remote Update, TRU**) – технология безопасного удаленного обновления памяти электронного ключа, исключающая возможность компрометации и/или фальсификации данных.

Мастер-ключ – любой экземпляр электронного ключа определенной модели, используемый на стороне разработчика для проведения процедуры удаленного обновления.

Пароль удаленного обновления – секретный ключ, используемый для шифрования данных обновления.

Протокол удаленного обновления

Процесс удаленного (дистанционного) программирования ключей Guardant состоит из 4 этапов и выглядит следующим образом:

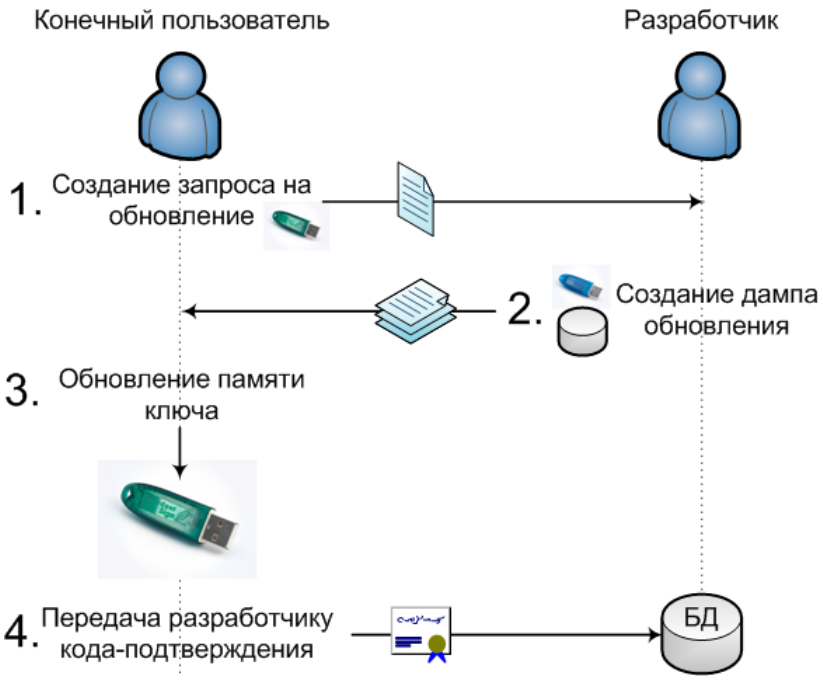


Схема 1. Протокол доверенного удаленного обновления

На 1-м этапе пользователь защищенного приложения генерирует **запрос на обновление памяти** электронного ключа и обращается к разработчику за новой лицензией.

2-й этап происходит на стороне разработчика и включает поиск маски, записанной в ключ пользователя, ее модификацию и генерацию **дампа обновления** памяти для удаленного ключа, а также пересылку дампа конечному пользователю.

3-й этап представляет собой непосредственное обновление памяти ключа (применение дампа обновления), в результате которого пользователь получает **код подтверждения** завершения операции обновления.

4-й этап заключается в получении от пользователя кода подтверждения и фиксировании успешного **статуса завершения** операции в базе прошивок.

Безопасность обмена обеспечивается паролем удаленного обновления, записываемого в ключ и сохраняемого в БД прошивок в момент записи маски в ключ. Таким образом, обмен может происходить по открытому каналу связи.

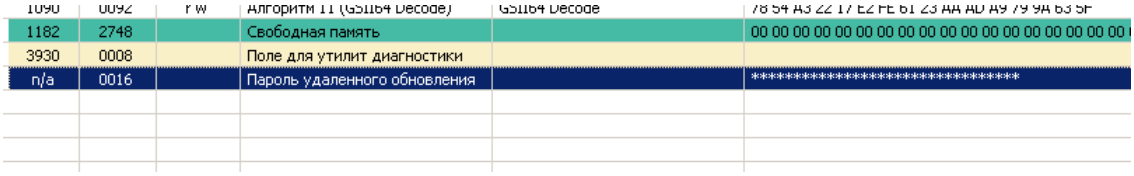
Удаленное обновление

На примере двух электронных ключей Guardant Time рассмотрим подробнее весь цикл удаленного обновления памяти ключа.

Шаг 0. Подготовка пароля удаленного обновления

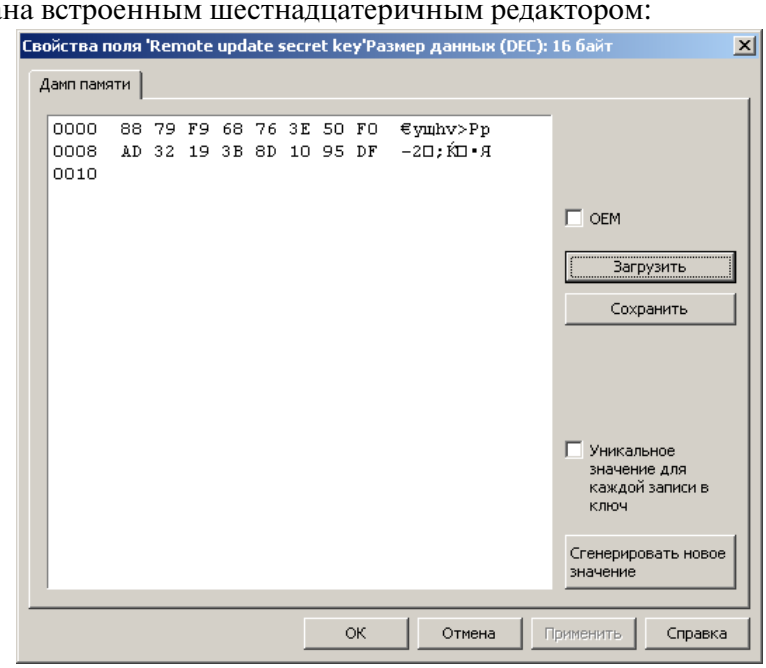
Пароль удаленного обновления записывается в ключ при программировании на этапе предпродажной подготовки. Запись происходит в момент полной инициализации памяти ключа, после чего пароль располагается в неадресуемой области и не может быть считан.

Установить значение пароля удаленного обновления можно при помощи Утилиты программирования ключей. Он отображается непосредственно после полей специального назначения:



При создании новой маски утилита программирования автоматически генерирует **случайное значение** пароля. Чтобы отредактировать значение пароля удаленного обновления, необходимо загрузить (или создать) нужную маску, выделить поле **Пароль удаленного обновления** и выполнить команду меню **Редактировать | Свойства поля**.

В появившемся диалоге **Свойства поля** представлена последовательность из 16 байт. Она может быть отредактирована встроенным шестнадцатеричным редактором:

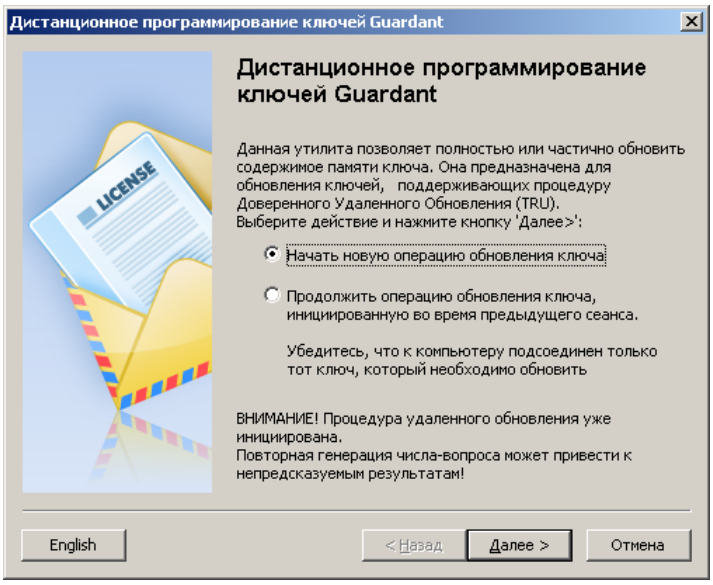


Шаг 1. Создание запроса на обновление

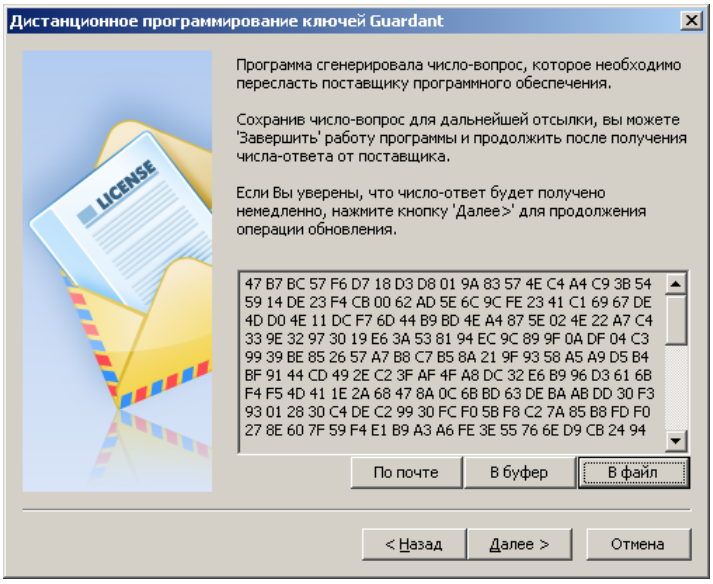
Рассмотрим ситуацию, когда после передачи конечному пользователю ключа и приложения, ограниченного по числу запусков, клиент покупает у разработчика полную версию программы плюс набор расширений, лицензируемых отдельно.

Таким образом, в ключе пользователя необходимо снять ограничение по числу запусков алгоритма, соответствующего лицензии приложения, а также добавить алгоритм, соответствующий лицензии на новые модули.

Конечный пользователь – с санкции разработчика – при помощи специальной утилиты (**GrdTRU.exe**) начинает процесс удаленного обновления:



Происходит генерация запроса на обновление памяти ключа (т. н. **числа-вопроса**). Созданный запрос пользователь должен передать разработчику:



В окне диалога предложены три варианта сохранения запроса. При нажатии кнопки **[По почте]** будет автоматически сформировано письмо, во вложении которого будет содержаться файл с запросом. Кнопки **[В файл]** и **[В буфер]** позволяют, соответственно, сохранить запрос в виде файла, или сохранить его в буфер.

Сохраним запрос в файл. Имя файла, предлагаемое по умолчанию, имеет название вида **question_ID_DATE.txt**. После сохранения числа-вопроса работу утилиты можно завершить (кнопка **[Завершить/Отмена]**).

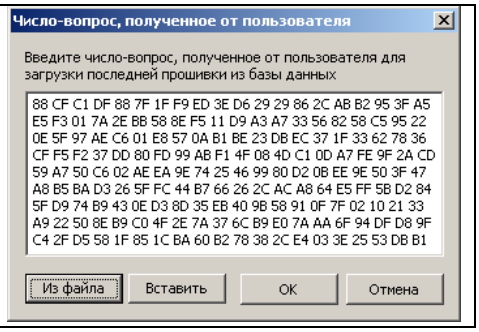
Примечание

В случае генерации пользователем нескольких запросов на обновление действителен будет последний. Обновление памяти ключа может быть выполнено только на нем.

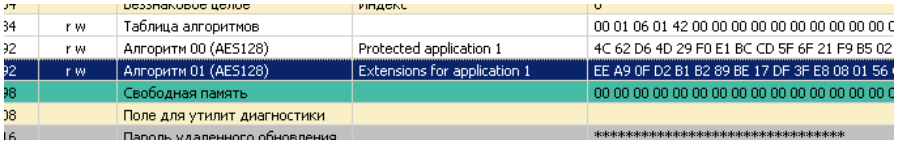
Шаг 2. Создание дампа обновления

Получив запрос на обновление, разработчик формирует дамп обновления и отправляет его конечному пользователю.

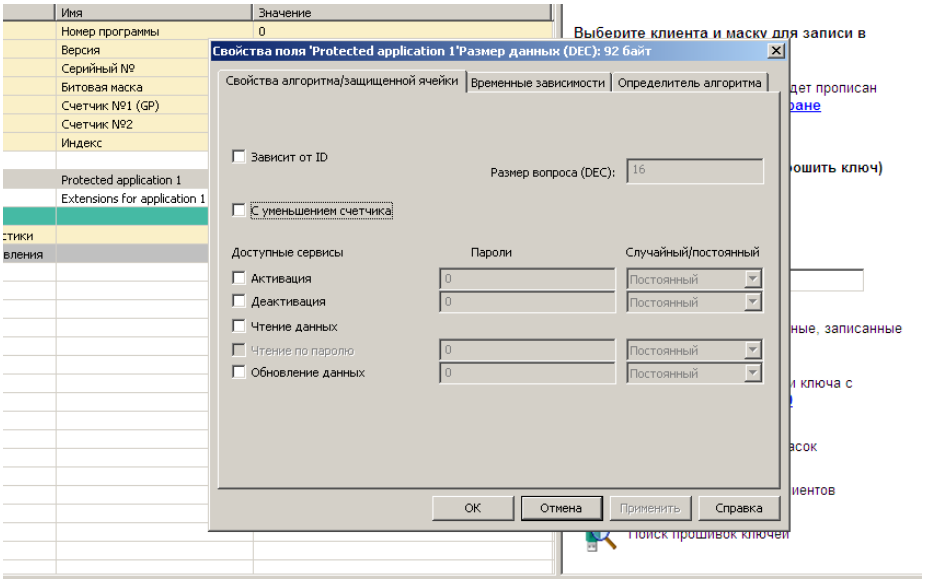
При проведении удаленного обновления памяти ключа важно, чтобы пароль удаленного обновления в ключе пользователя соответствовал паролю удаленного обновления в формируемой маске. Чтобы исключить возможность ошибки рекомендуется загрузить в Редактор маски последнюю прошивку для обновляемого ключа. Для этого необходимо выполнить команду меню **База данных | Загрузить прошивку по числу-вопросу**.

Введите в окно появившегося диалога запрос на обновление, полученный от конечного пользователя. После нажатия на кнопку **[OK]** будет автоматически найдена и загружена в Редактор маски актуальная прошивка для ключа, находящегося у конечного пользователя.	

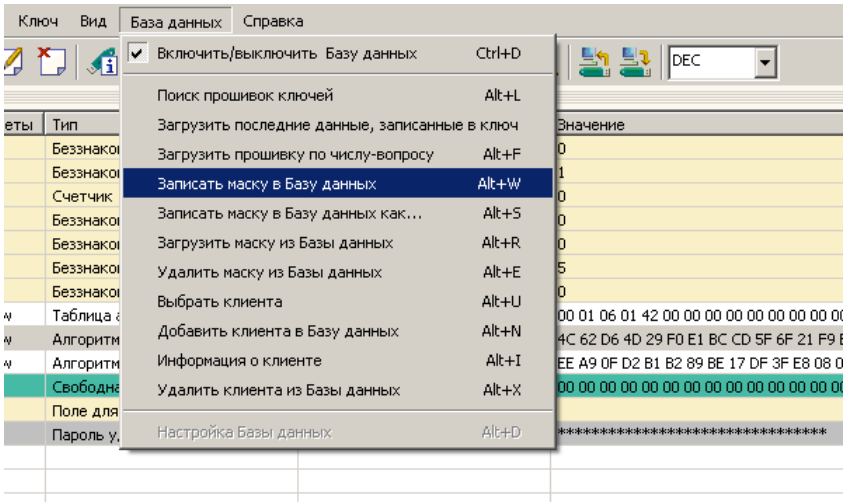
Теперь необходимо внести изменения в найденную прошивку. Добавим в маску аппаратный алгоритм с номером (т. н. **числовым именем**), типом и определителем, соответствующим лицензии на расширения к защищенному приложению:



А также снимем ограничение на число обращений к алгоритму, соответствующему лицензии на само приложение:

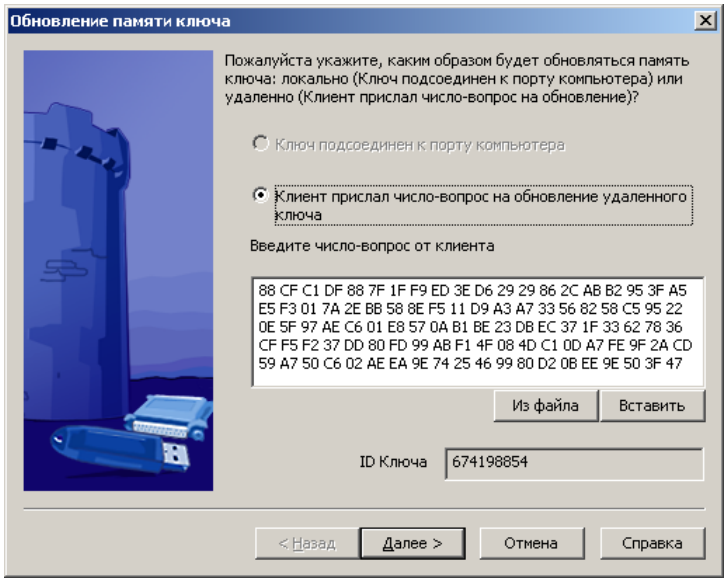


После внесения всех изменений необходимо сохранить маску в базе данных прошивок:



...и продолжить процедуру обновления – создать дамп обновления памяти ключа, выполнив команду **Ключ | Обновление ключа**.

На экране появится диалог Обновление памяти ключа. В нем уже содержится запрос на обновление, присланный пользователем (если маска была загружена в редактор по числу-вопросу) и выведен ID ключа клиента, для которого проводится процедура обновления:

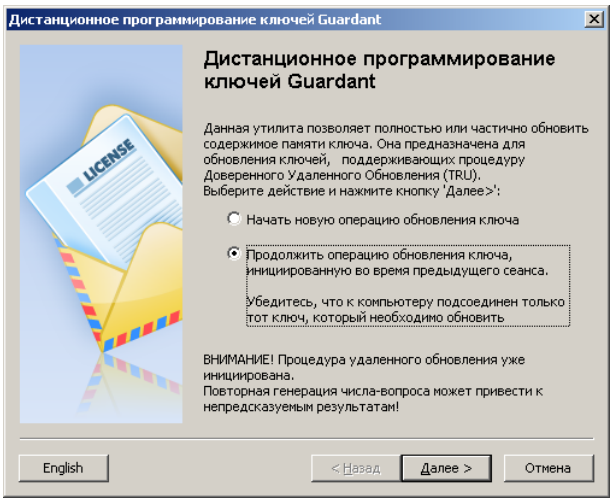


Теперь необходимо подсоединить **мастер-ключ** (любой ключ той же модели, что и обновляемый) к порту и нажать на кнопку **[Далее >]**. При этом в память мастер-ключа будут записаны специальные алгоритмы, участвующие в подготовке данных обновления. Как только дамп обновления будет сформирован, содержимое мастер-ключа автоматически восстановится путем записи в него последней прошивки для этого ключа из БД (при наличии таковой).

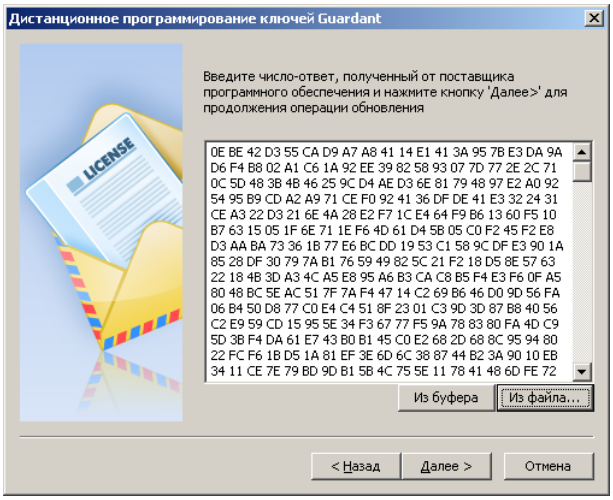
Созданный дамп обновления необходимо передать пользователю. Следует отметить, что дамп обновления будет действителен только для того электронного ключа, запрос на обновление которого использовался.

Шаг 3. Обновление памяти ключа

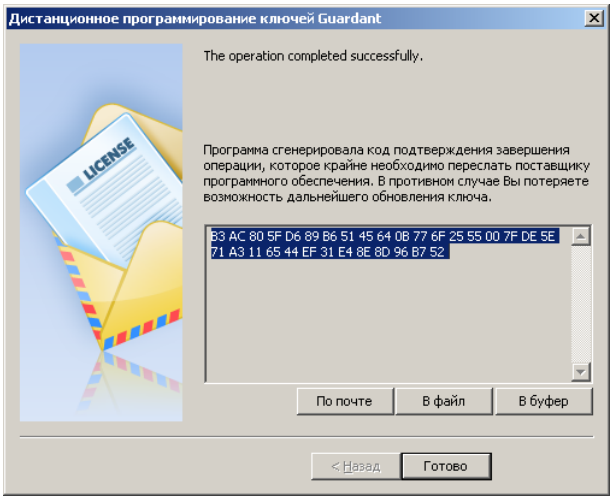
После получения дампа обновления пользователю необходимо снова запустить клиентскую утилиту обновления **GrdTRU**, выбрать пункт **Продолжить операцию обновления ключа** и нажать на кнопку **[Далее]**:



После ввода дампа обновления и нажатия на кнопку **[Далее]** будет произведена операция по обновлению памяти ключа присланными данными.



В случае успешного окончания на экране появится последняя страница мастера с итогами выполнения операции:

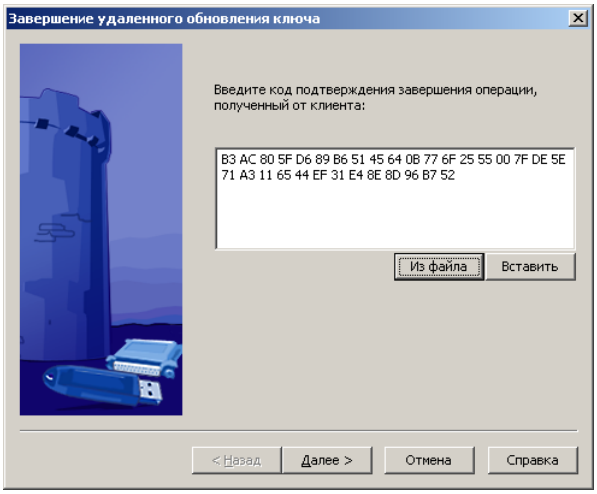


В результате успешного обновления памяти ключа утилита **GrdTRU** выдаст код подтверждения, содержащий информацию о результате обновления. Пользователю следует сохранить его и передать разработчику приложения любым удобным способом.

Шаг 4. Завершение удаленного обновления

После получения кода подтверждения разработчик завершает процедуру обновления, занося в базу данных информацию о результате состоявшегося обновления.

Для этого необходимо выполнить команду меню **Ключ | Завершить удаленное обновление**:



В результате в БД будет добавлена очередная запись о прошивке ключа.

Заключение

В данном уроке был рассмотрен порядок действий, выполняемых при удаленном программировании ключей Guardant.

Инструмент удаленного обновления памяти ключей является одним из основных средств сопровождения защищенных приложений и проведения долгосрочной лицензионной политики.

Не следует забывать о необходимости включения утилиты **GrdTRU.exe** в состав дистрибутива защищенного приложения.

Во избежание несовместимости при проведении удаленного обновления рекомендуется использовать утилиты **GrdTRU** и **GrdUtil** из одной и той же версии комплекта разработчика Guardant.

Дополнительные источники информации

При возникновении вопросов, на которые вам не удалось найти ответа в этом пособии, рекомендуем обратиться к следующим дополнительным источникам информации:

WWW: http://www.guardant.ru

Web-сайт разработчика содержит большой объем справочной информации об электронных ключах Guardant.

Служба технической поддержки:

e-mail: hotline@guardant.ru

тел. +7(495)925-77-90