Обновление аппаратных ключей

При удаленном программировании электронных ключей, находящихся у конечных пользователей, неизбежно возникают проблемы, связанные с защищенным обменом данными.
Разработчик должен убедиться: во-первых, в том, что конечный пользователь собирается обновить данные именно в том ключе, в котором нужно. Для этой цели в закодированное число-вопрос, генерируемое ключом в начале сессии удаленного программирования, обязательно включается ID ключа, на котором оно сгенерировано.

Во-вторых, разработчику необходимо удостовериться, что число-вопрос является подлинным, то есть конечный пользователь не прислал поддельное или измененное число-вопрос. Для контроля подлинности используется аппаратно реализованная хэш-функция с секретным ключом: HASH64 (для Guardant Sign/Time/Net) или SHA256 (Guardant Code /Code Time). Число-вопрос передается разработчику вместе с результатом вычисления хэш-функции. Имея электронный ключ с тем же алгоритмом, разработчик может убедиться в подлинности числа-вопроса, вычислив хэш-функцию и сравнив ее результат с присланным. Таким образом, реализуется своего рода цифровая электронная подпись данных.

В-третьих, разработчик должен быть уверенным в том, что число-ответ будет передано в электронный ключ конечного пользователя в неизменном виде. Для этого также используется аппаратное вычисление HASH64 (SHA256).

В-четвертых, конечному пользователю вовсе не обязательно знать, какие именно данные передаются. На месте конечного пользователя вполне может оказаться хакер, пытающийся проанализировать протокол удаленного программирования. По этой причине все данные, передаваемые от конечного пользователя разработчику и обратно, в обязательном порядке кодируются симметричным алгоритмом: GSII64 (для Guardant Sign /Time/Net) или AES128 (Guardant Code /Code Time).

Безопасность протокола удаленного программирования Trusted Remote Update обеспечивается именно аппаратной реализацией алгоритмов кодирования и хеширования, а также тем, что секретные ключи этих преобразований в процессе работы не извлекаются из электронного ключа. Все операции, связанные с декодированием и проверкой целостности данных, осуществляются внутри аппаратного устройства. Это исключает возможность компрометации или подмены данных, которые записываются в электронный ключ.

Важно!
Для того чтобы механизм Trusted Remote Update работал, в ключ конечного пользователя на этапе предпродажной подготовки прошиваются секретные пароли удаленного обновления (секретные ключи GSII64 или AES128). Их копии вместе с ID электронных ключей, в которые они были прошиты, обязательно должны сохраняться разработчиком в базе данных, доступ к которой должен иметь только авторизованный персонал.

Обновление памяти ключа широко используется для изменения условий эксплуатации защищенного приложения или/ и его системы защиты, например:

- Продление срока использования программы, защищенной с ограничением времени использования или числа запусков
- Обновление версии программы
- Активация демо-версий
- Увеличение числа лицензий на использование сетевой версии программы
- Расширение функциональности программного комплекса
- Изменение данных или структуры памяти ключа

Возможны два варианта обновления памяти ключа:

- ***Удаленное (дистанционное)*** – обновление данных в ключе, находящемся у удаленного конечного пользователя
- ***Локальное*** – обновление данных в ключе, подсоединенномк компьютеру разработчика защищенного приложения

Зависимость обновления от подвида используемого образа

Процедура обновления памяти ключа зависит от того, в каком виде хранится образ обновляемого ключа – как прошивка, шаблон или файл *.nsd:

Вариант обновления	**Подвид образа**			
	Файл *.nsd	**Шаблон из БД**	**Прошивка из БД GrdUtil**	
Удаленное	Полное обновление содержимого памяти удаленного ключа при помощи операции **Ключ | Начать удаленное обновление ключа**		Полное обновление памяти	**Возможный тип обновления**
			Частичное обновление памяти	
			Операции активации/деактивации	
			Обновление времени деактивации алгоритма (для Guardant Time)	

Локальное	Полная перезапись содержимого памяти ключа, подсоединенного к локальному компьютеру, при помощи операции **Ключ | Записать образ в ключ**	Полное обновление памяти	
		Частичное обновление памяти	
		Операции активации/деактивации	
		Обновление времени деактивации алгоритма (для ключей с RTC)	

Удаленное обновление

Процесс удаленного (дистанционного) программирования ключей Guardant состоит из следующих этапов:

№	Этап	Кто выполняет
1	Создание запроса на обновление	Конечный пользователь по санкции разработчика
2	Создание дампа обновления	Разработчик после получения запроса на обновление от конечного пользователя
3	Обновление памяти ключа	Конечный пользователь после получения от разработчика дампа обновления
3a	Передача разработчику кода-подтверждения	Конечный пользователь после обновления памяти ключа
4	Завершение дистанционного обновления	Разработчик после получения кода-подтверждения от конечного пользователя

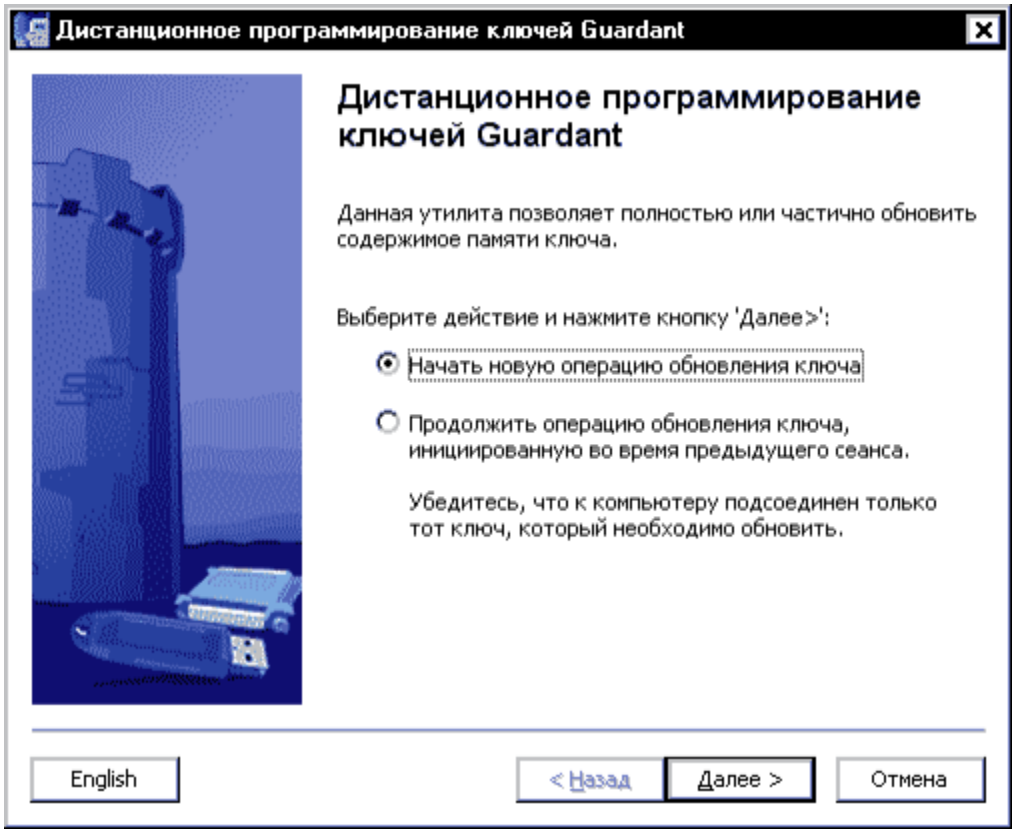
Далее детально рассматривается каждый этап.

1. Создание запроса на обновление

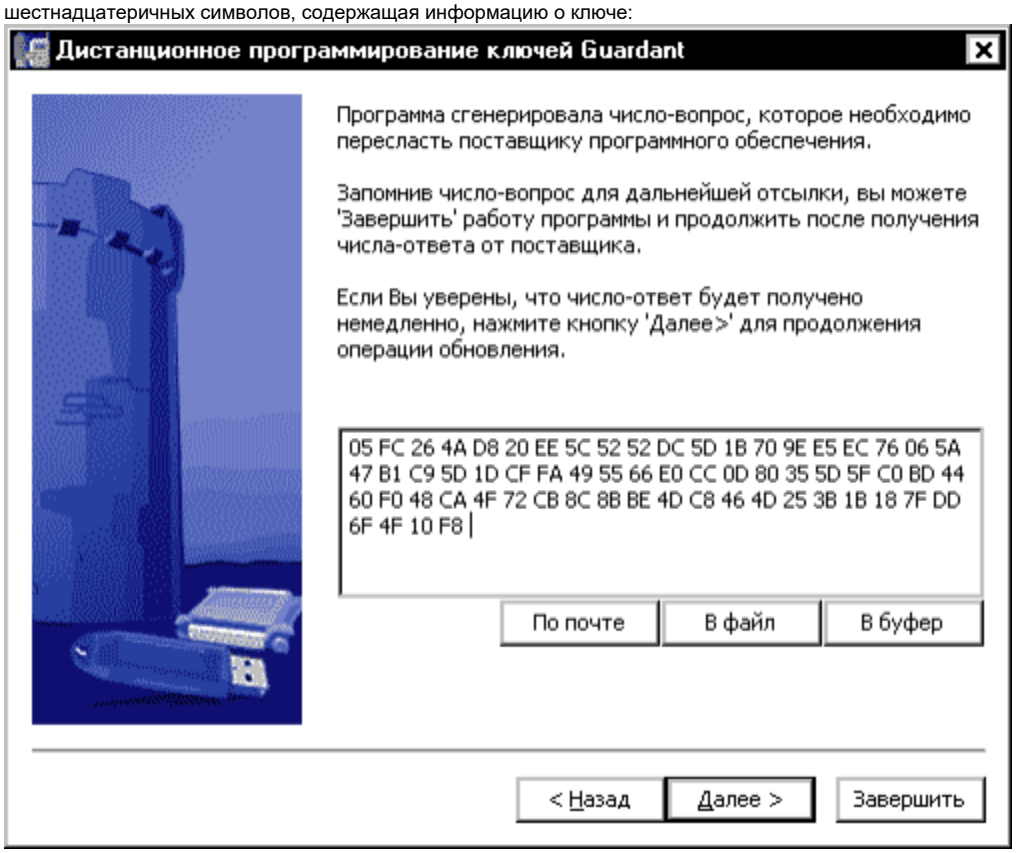
Конечный пользователь по санкции разработчика генерирует запрос на обновление (число-вопрос) при помощи специальной утилиты и передает его разработчику по любому каналу связи.

Важно!
1. Процедура дистанционного обновления современных ключей Guardant требует наличия у конечного пользователя утилиты **GrdTRU.exe**. Этот файл должен входить в комплект поставки защищенного приложения.
2. Процедура дистанционного обновления устаревших ключей Guardant Stealth II/Net II, Guardant Stealth/Net и Guardant Fidus требует наличия у конечного пользователя утилиты **GsRemote.exe**. Этот файл должен входить в комплект поставки защищенного приложения.
3. Для успешного запуска клиентской утилиты удаленного обновления к порту компьютера должен быть подсоединен ключ с кодами доступа разработчика.
4. Если у конечного пользователя установлено несколько защищенных программ одного разработчика, то в порту необходимо оставить только тот ключ, который требует обновления.
5. Информацию, касающуюся работы с клиентской утилитой, рекомендуется включать в инструкцию для конечного пользователя. Клиентская утилита удаленного программирования выполнена в виде мастера, состоящего из нескольких страниц. Переход между страницами осуществляется при помощи кнопок **[Далее]** и **[Назад]**, расположенных в нижней части диалога.

1. После первого запуска утилиты на экране появится страница, на которой необходимо выбрать пункт **Начать новую операцию обновления ключа**:



2. На следующей странице отобразится сгенерированный ***запрос на обновление*** (число-вопрос) – последовательность шестнадцатеричных символов, содержащая информацию о ключе:



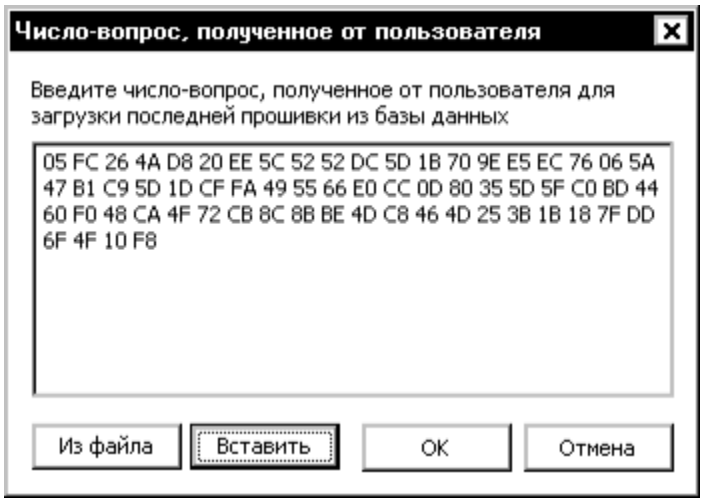
Запрос на обновление необходимо сохранить в файле (кнопка **[В файл]**), скопировать с помощью кнопки **[В буфер]** или сразу сформировать почтовое сообщение для разработчика приложения (кнопка **[По почте]**).
Работу утилиты можно завершить (кнопка **[Завершить]**) до получения дампа-ответа от разработчика.

2. Создание дампа обновления

После получения запроса на обновление разработчик формирует ***дамп обновления*** и отправляет его конечному пользователю.

Важно!
1. Во время операции обновления к порту компьютера должен быть подсоединен ключ той же модели, что и обновляемый.
2. Обновление современных ключей Guardant выполняется по технологии **Доверенного удаленного обновления** (см. пункт **Доверенное удаленное обновление**). Согласно этой технологии должен быть заранее задан пароль удаленного обновления, который вместе с данными образа записывается в ключ перед продажей конечному пользователю, а также сохраняется в прошивке.

1. Перед началом процедуры получения дампа обновления загрузите в Редактор маску, которая будет использована для обновления удаленного ключа, и произведите в ней необходимые изменения.
Для обновления может использоваться шаблон или файл образа,а также прошивка.
Если удаленное обновление выполняется на основе прошивки, то при большом количестве прошивок бывает сложно найти нужную.
Чтобы автоматически загрузить в Редактор образа последнюю прошивку для удаленного ключа, выполните команду **База данных | Образ по числу-вопросу**.
Введите в окно появившегося диалога запрос на обновление, полученный от конечного пользователя (кнопка **[Из файла]** или **[Вставить]**):



После нажатия кнопки **[OK]** актуальная прошивка для удаленного ключа будет автоматически найдена по ID удаленного ключа и загружена в Редактор образа.
Внесите необходимые изменения в прошивку и начните процедуру создания дампа обновления.

Важно!
Если в ходе редактирования шаблона образа или прошивки меняется их структура^*^ Под изменением структуры понимается удаление / добавление полей, а также редактирование содержимого полей, защищенных аппаратными запретами, то для продолжения процесса обновления необходимо сохранить отредактированную маску в базе. Т. о. создается новый шаблон – с уникальным именем и/или версией, и обновление проводится уже на его основе.

2. Чтобы создать дамп обновления, выполните команду **Ключ | Обновить ключ**.
На экране появится диалог **Обновление памяти ключа**, который реализован в виде мастера, состоящего из нескольких страниц. Переход между страницами происходит при помощи кнопок **[Далее]** и **[Назад]**, расположенных в нижней части диалога:

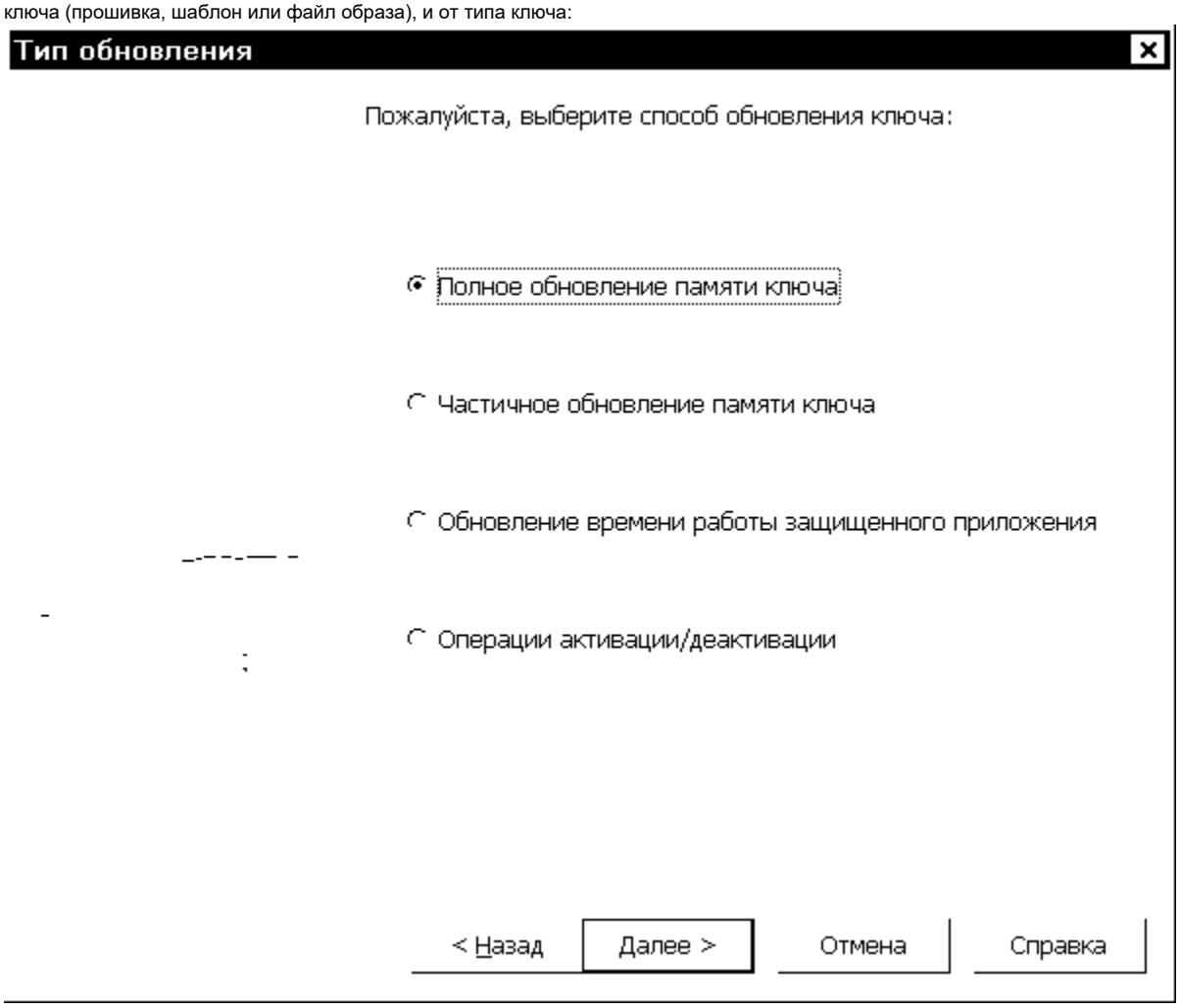
а) Выберите с помощью переключателя пункт **Клиент прислал число-вопрос на обновление удаленного ключа*** При обновлении файлом или шаблоном маски этот пункт является единственно доступным и введите полученный запрос на обновление в поле. Для ввода воспользуйтесь кнопкой:

- **[Вставить]**, если число-вопрос находится в буфере обмена
- **[Из файла]**, если число-вопрос хранится в текстовом файле

После этого в поле ID ключа появится значение идентификатора ключа, извлеченное из запроса на обновление.

Важно!
Если при обновлении от прошивки была успешно выполнена команда **База данных | Загрузить прошивку по числу-вопросу**, то запрос на обновление заносится в поле автоматически, а значение ID не выводится.

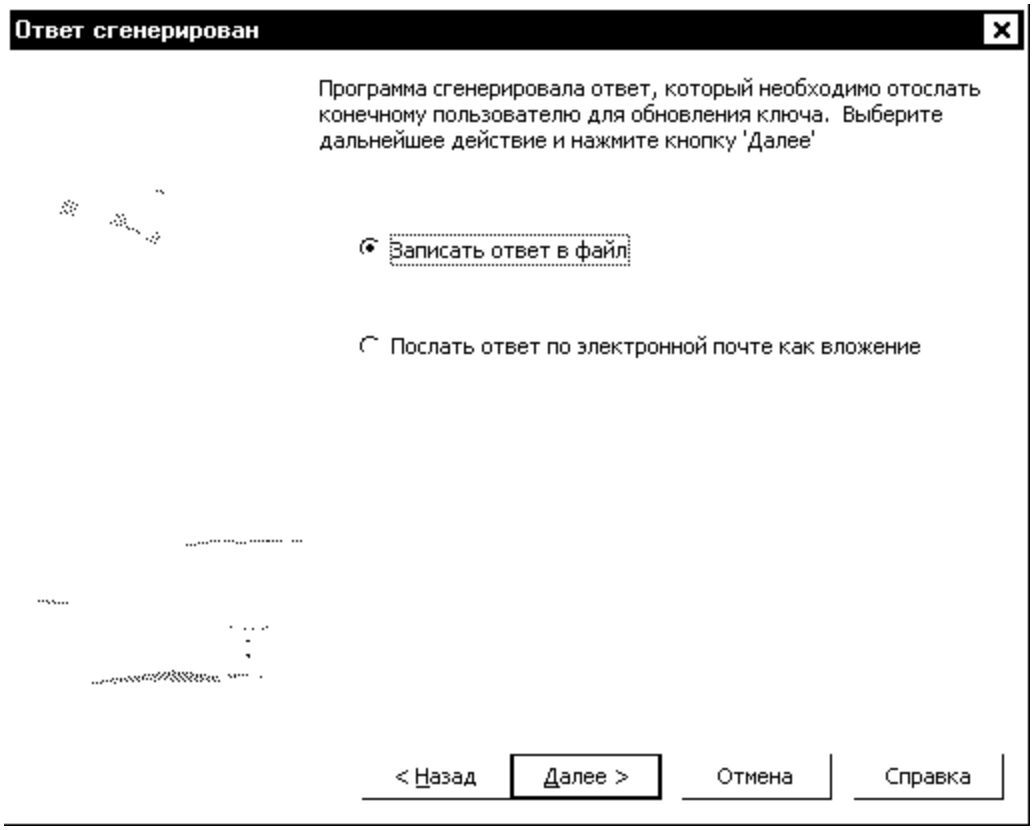
б) После нажатия кнопки **[Далее]** на экране появится страница **Тип обновления** с селектором выбора. Состояние селектора (доступные варианты обновления) зависит от разновидности образа, на основе которого выполняется перепрограммирование ключа (прошивка, шаблон или файл образа), и от типа ключа:



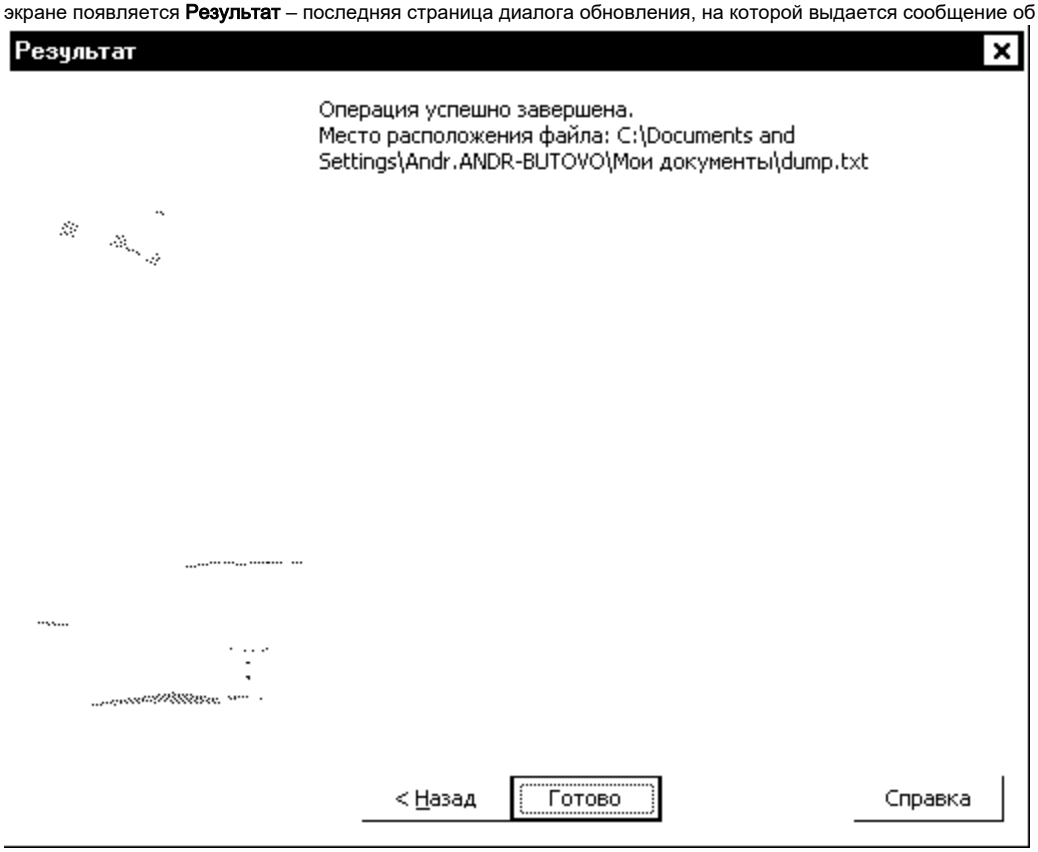
Выберите нужный пункт обновления и нажмите на кнопку **[Далее]**. Следующие несколько страниц служат для задания параметров обновления. Подробно о каждом из вариантов обновления см. далее в разделе **Тип обновления**.

Важно!
Во многих случаях удобно использовать следующую схему получения дампа обновления: заранее произвести в маске необходимые изменения, а затем, в ходе выполнения диалога **Дистанционное обновление** выбрать пункт **Полное обновление памяти ключа**.

в) После определения параметров обновления на экране появится страница **Ответ сгенерирован**, позволяющая выбрать способ дальнейшей обработки полученного дампа:



г) После нажатия кнопки **[Далее]** дамп сохраняется в файле или прикрепляется к почтовому сообщению в качестве вложения. На экране появляется **Результат** – последняя страница диалога обновления, на которой выдается сообщение об итоге операции:

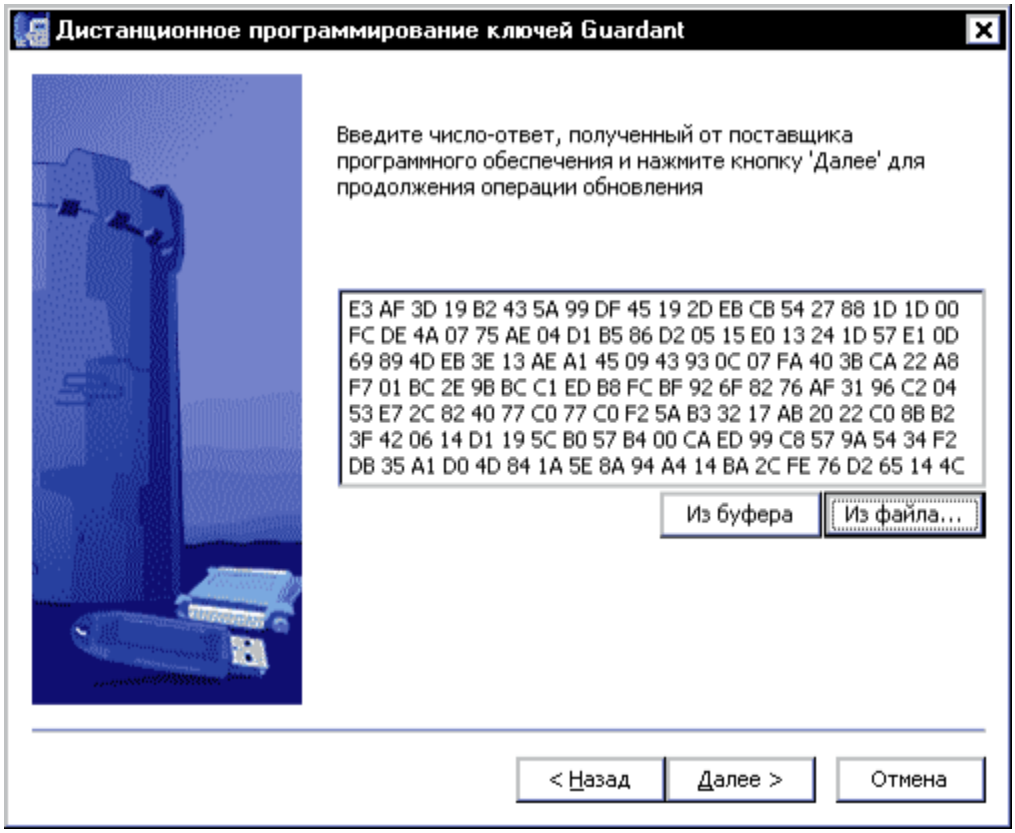


Если используется база данных, то после создания дампа обновления GrdUtil.exe фиксирует факт прошивки удаленного ключа и присваивает этой операции статус незавершенной. Т. е. к списку прошивок образа с указанными параметрами добавляется новая прошивка, а в столбце **Признак завершенности** для нее указывается – ***В процессе*** (см. раздел **Прошивки**).
Сгенерированный дамп обновления необходимо передать конечному пользователю.

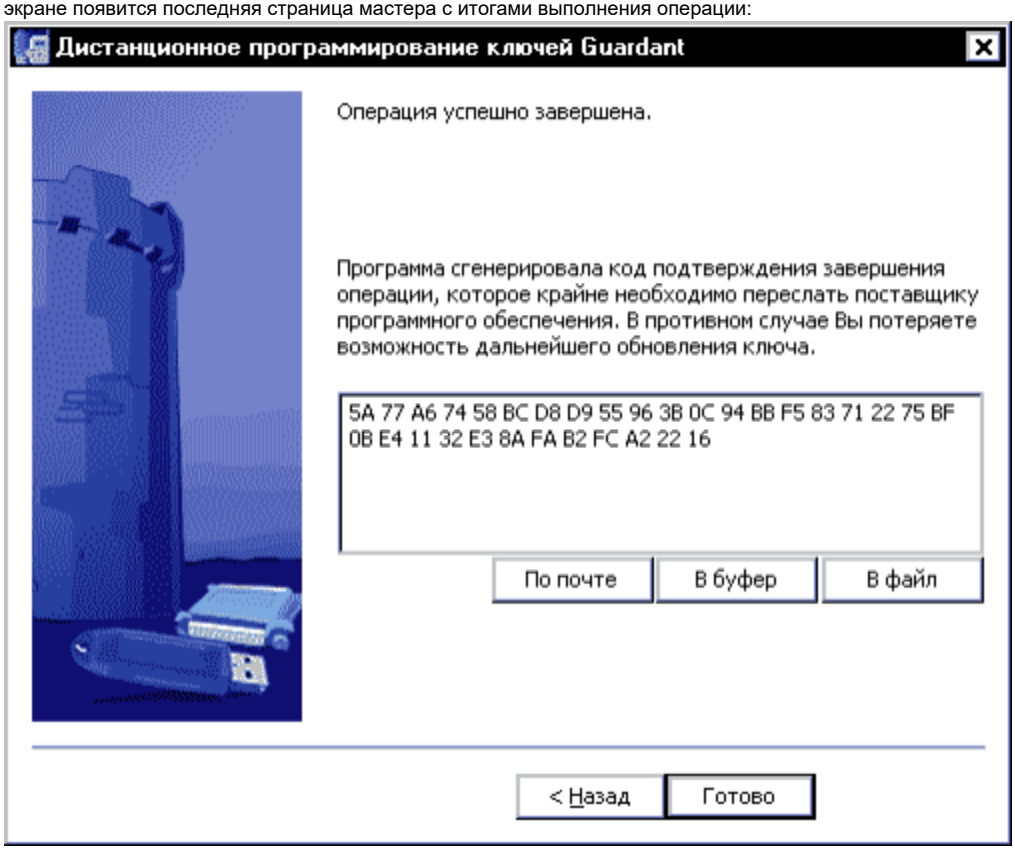
3. Обновление памяти ключа

После получения дампа обновления конечный пользователь может перепрограммировать память ключа.

Важно!
1. Данные обновления передаются в закодированном виде и могут быть использованы только один раз
2. При генерировании данных обновления и прошивке их в ключ выполняется ряд проверок параметров ключа (ID, Общий код и некоторые другие). Этим исключается возможность подмены перепрограммируемого ключа
Необходимо снова запустить клиентскую утилиту, с помощью селектора-переключателя выбрать пункт **Обработать число-ответ..** и нажать на кнопку **[Далее]**.
На экране появится страница мастера, содержащая поле для ввода и отображения дампа обновления. Ввод дампа происходит при помощи одной из кнопок: **[Из буфера]** или **[Из файла…]**:



После ввода дампа и нажатия на кнопку **[Далее]** будет произведена операция по обновлению памяти ключа присланными данными. Затем на экране появится последняя страница мастера с итогами выполнения операции:



Важно!
Последующие этапы необходимы в случае, когда обновление ключа происходит по факту прошивки или шаблона образа. Если же обновление выполнялось на основе данных файла образа, то шаг 3 является завершающим этапом обновления.

3. Передача разработчику кода-подтверждения

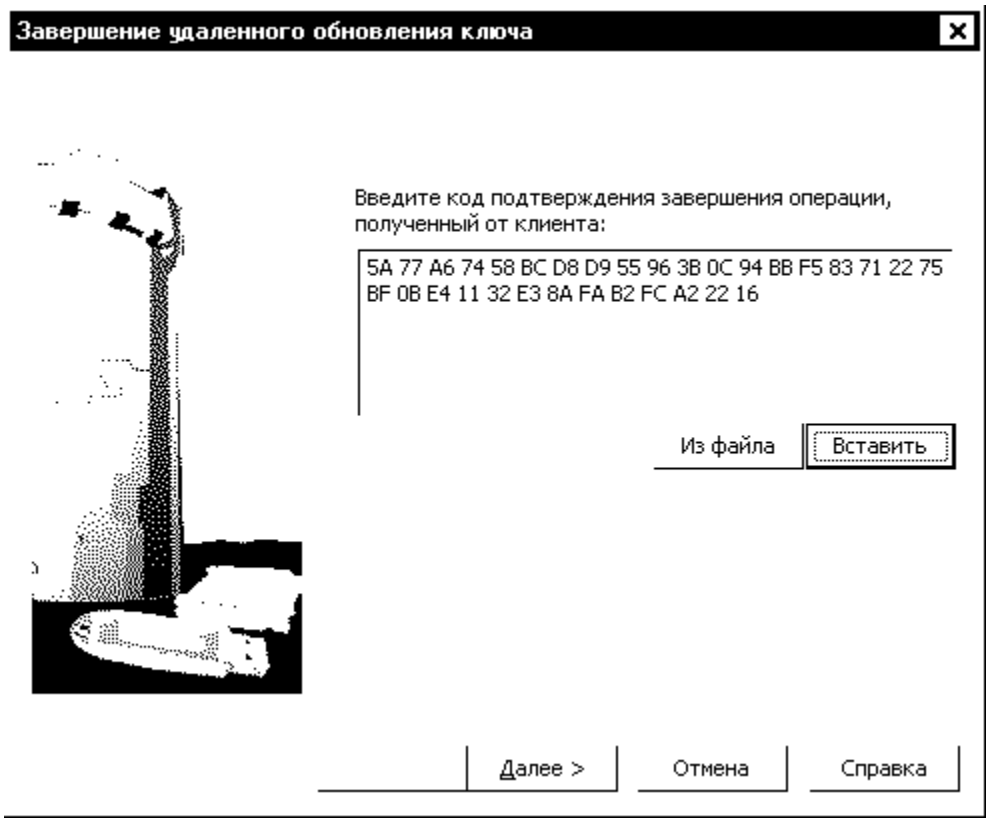
В процессе обновления памяти ключа клиентская утилита выдаст финальный ***код-подтверждение***, содержащий информацию о результате обновления (успешно/неудачно). Код-подтверждение необходимо сохранить в файле (кнопка **[В файл]**) или скопировать с помощью кнопки **[В буфер]** и передать разработчику приложения любым удобным способом.

4. Завершение удаленного обновления

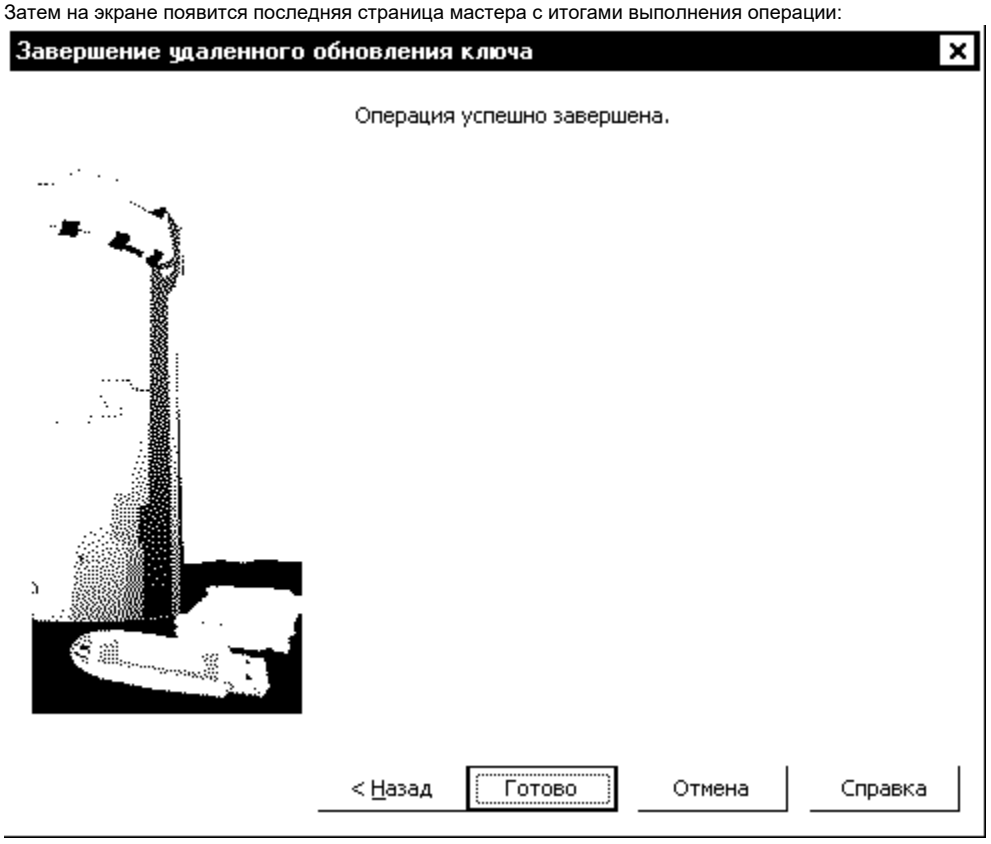
После получения кода-подтверждения разработчику необходимо завершить обновление: занести в базу данных информацию об итогах состоявшегося обновления.
Чтобы завершить процедуру удаленного обновления ключа, выполните команду **Ключ | Завершить удаленное обновление**.

Важно!
Завершение удаленного обновления не требует загрузки обрабатываемой прошивки в Редактор образа.

В появившемся диалоге **Завершение удаленного обновления ключа** введите код-подтверждение, полученный от конечного пользователя:



После ввода кода-подтверждения и нажатия на кнопку **[Далее]** будет произведена операция по завершению процедуры удаленного обновления. Затем на экране появится последняя страница мастера с итогами выполнения операции:



В случае успеха операции факт прошивки удаленного ключа получает статус завершенного. Признак завершенности для этой прошивки меняется на ***Завершен*** (См. раздел **Прошивки**).

Доверенное удаленное обновление

В современных ключах Guardant используется ***Доверенное удаленное обновление*** (Trusted Remote Update). Основное достоинство этой технологии заключается в том, что вся информация, предназначенная для дистанционного обновления, декодируется и обрабатывается только внутри электронного ключа.
Доверенное удаленное обновление – технология безопасного удаленного обновления памяти электронного ключа, исключающая возможность компрометации и/или фальсификации данных. Идеология Доверенного удаленного обновления гарантирует, что однажды записанная в электронный ключ информация не может быть записана в него повторно, а данные, сгенерированные для одного ключа, не подойдут для другого.

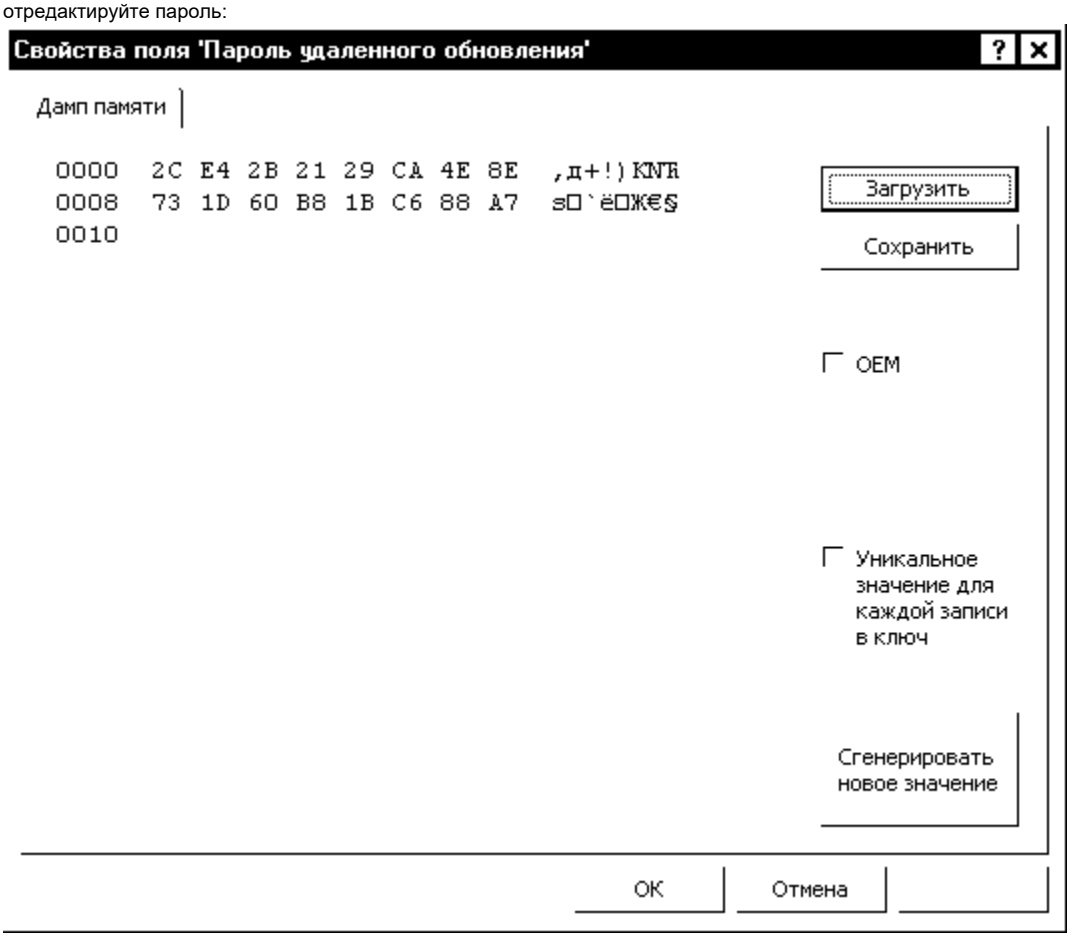
Важно!
Процедура Доверенного удаленного обновления предполагает использование уникальных данных, в частности, пароля удаленного обновления, для каждого ключа. Поэтому настоятельно рекомендуется использовать режим базы данных для регистрации и сохранения уникальной информации. В противном случае, процедура удаленного обновления будет затруднена, или вовсе невозможна.

Пароль удаленного обновления

Пароль удаленного обновления – это 16-байтовая последовательность шестнадцатеричных символов, которая используется в процедуре Доверенного удаленного обновления для преобразования данных обновления. Пароль удаленного обновления может быть, как одинаковым для партии ключей, так и уникальным для каждого ключа.

Важно!
Для успешного выполнения Доверенного удаленного обновления пароль, содержащийся в удаленном ключе, должен совпадать с паролем, хранящимся в прошивке для этого ключа.
Пароль удаленного обновления содержится в неадресуемом, доступном для редактирования поле, которое расположено в образах современных ключей Guardant сразу после области полей специального назначения.
Для задания пароля удаленного обновления из приложения служит операция ***GrdTRU_SetKey***.

Чтобы просмотреть/ отредактировать пароль удаленного обновления, загрузите нужную маску, выделите поле **Пароль удаленного обновления** и выполните команду меню **Редактировать | Свойства поля**.
В появившемся диалоге **Свойства поля Пароль удаленного обновления**, который представляет собой шестнадцатеричный редактор, отредактируйте пароль:



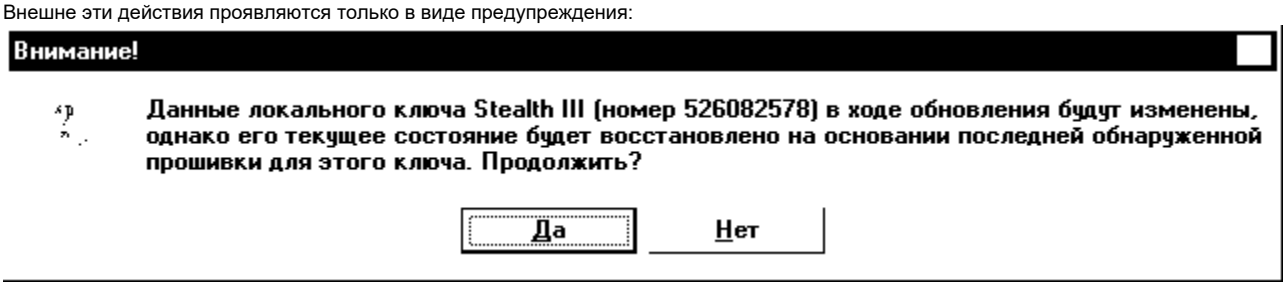
По умолчанию **GrdUtil.exe** автоматически формирует пароль удаленного обновления. При необходимости его можно изменить, сформировав пароль самостоятельно, путем ввода нового значения непосредственно в окне редактора, или автоматически создать новый пароль (кнопка **[Сгенерировать новое значение]**).
Диалог также позволяет определить, будет ли использоваться уникальный или постоянный пароль. Если флаг **Уникальное значение для каждой записи в ключ** установлен, то при каждой операции прошивки в ключ значение пароля автоматически меняется на новую случайную последовательность. Т. о. каждый ключ получает уникальный пароль на обновление, хранящийся в памяти ключа и в его прошивке.
Элементы управления диалога **Пароль удаленного обновления**:

Элемент интерфейса	Назначение
Окно шестнадцатеричного редактора	Ввести значение пароля удаленного обновления
Кнопка **[Сгенерировать новое значение]**	Заменить текущее значение пароля новой случайной последовательностью
Флаг **Уникальное значение для каждой записи в ключ**	Использовать уникальный/ постоянный пароль. По умолчанию используется постоянный пароль – флаг не установлен.
Флаг **OEM**	Выбрать Windows- / DOS-кодировку. По умолчанию используется Windows-кодировка (ANSI) – опция OEM отключена
Кнопка **[Загрузить]**	Загрузить дамп из файла с расширением *.dmp
Кнопка **[Сохранить]**	Сохранить дамп в файле с расширением *.dmp

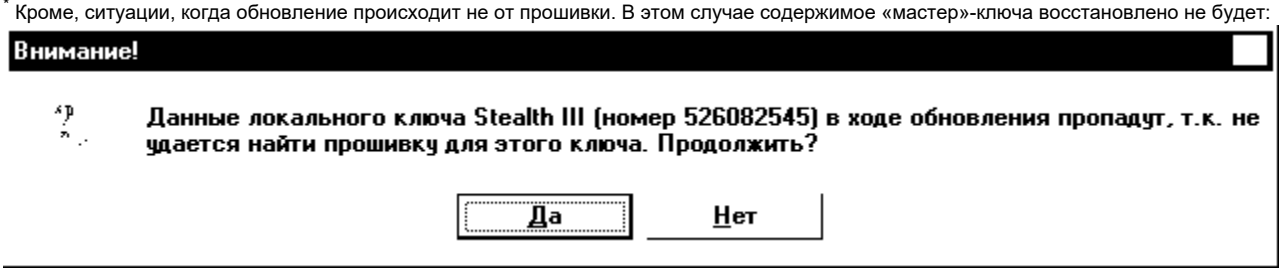
После ввода данных нажмите на кнопку **[Применить]** и закройте диалог.

Особенности процедуры Доверенного удаленного обновления

Процедура Доверенного удаленного обновления при использовании GrdUtil.exe практически не отличается от обычного удаленного обновления (см. раздел Удаленное обновление), за исключением нескольких деталей:
При выполнении команды **Ключ | Начать удаленное обновление ключа** GrdUtil.exe автоматически записывает в память «мастер»-ключа, подсоединенного к порту, специальные алгоритмы. Эти алгоритмы участвуют в обработке запроса на обновление и кодировании данных обновления, используя пароль, хранящийся в прошивке обновляемого ключа.
После того, как дамп обновления сформирован, содержимое «мастер»-ключа автоматически восстанавливается путем записи в ключ последней прошивки для этого ключа.
Внешне эти действия проявляются только в виде предупреждения:



Если удаленное обновление выполняется без использования базы данных, на основе файла образа, то запрос на обновление не будет декодирован при несовпадении паролей удаленного обновления в файле образа и в удаленном ключе!!!
* Кроме, ситуации, когда обновление происходит не от прошивки. В этом случае содержимое «мастер»-ключа восстановлено не будет:



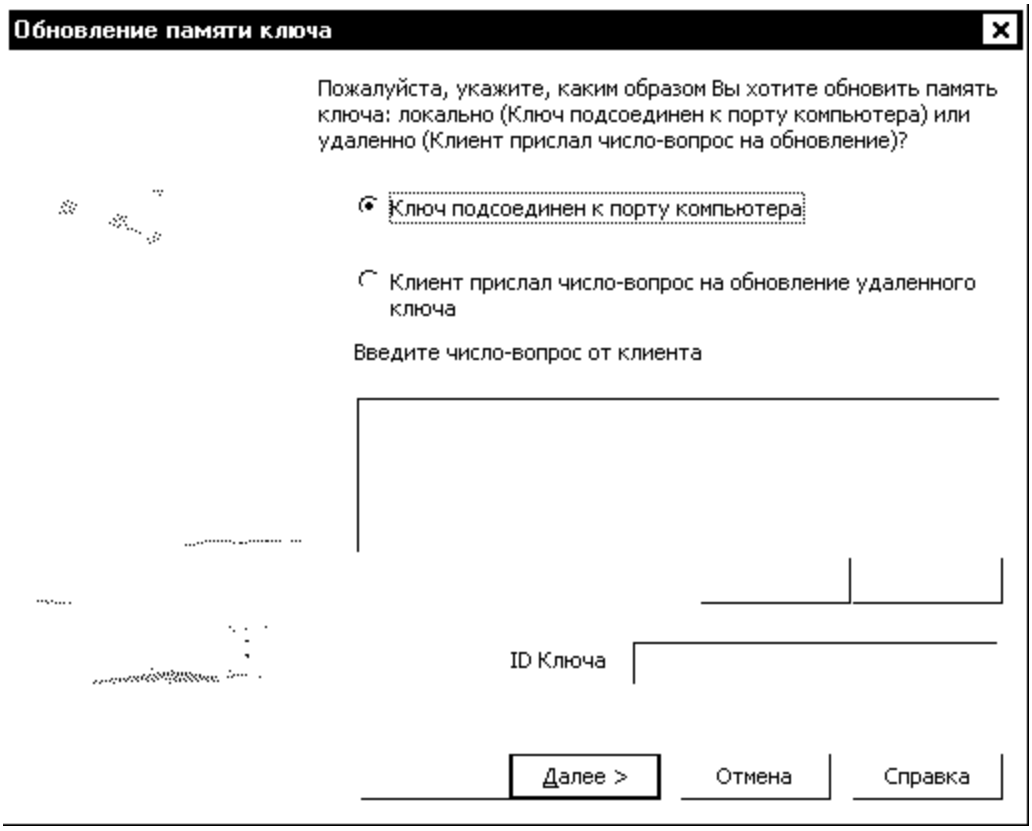
Локальное обновление

Локальное обновление памяти ключа подразумевает перепрограммирование памяти ключа, подсоединенного к порту компьютера, на котором установлен Комплект разработчика.
Чтобы обновить память локального ключа, выполните команду меню **Ключ | Начать удаленное обновление ключа**, либо **Ключ | Записать образ в ключ**. Причем первая команда будет доступна только в случае, когда используется прошивка ключа, а не шаблон или файл образа.
Особенности способов локального обновления:

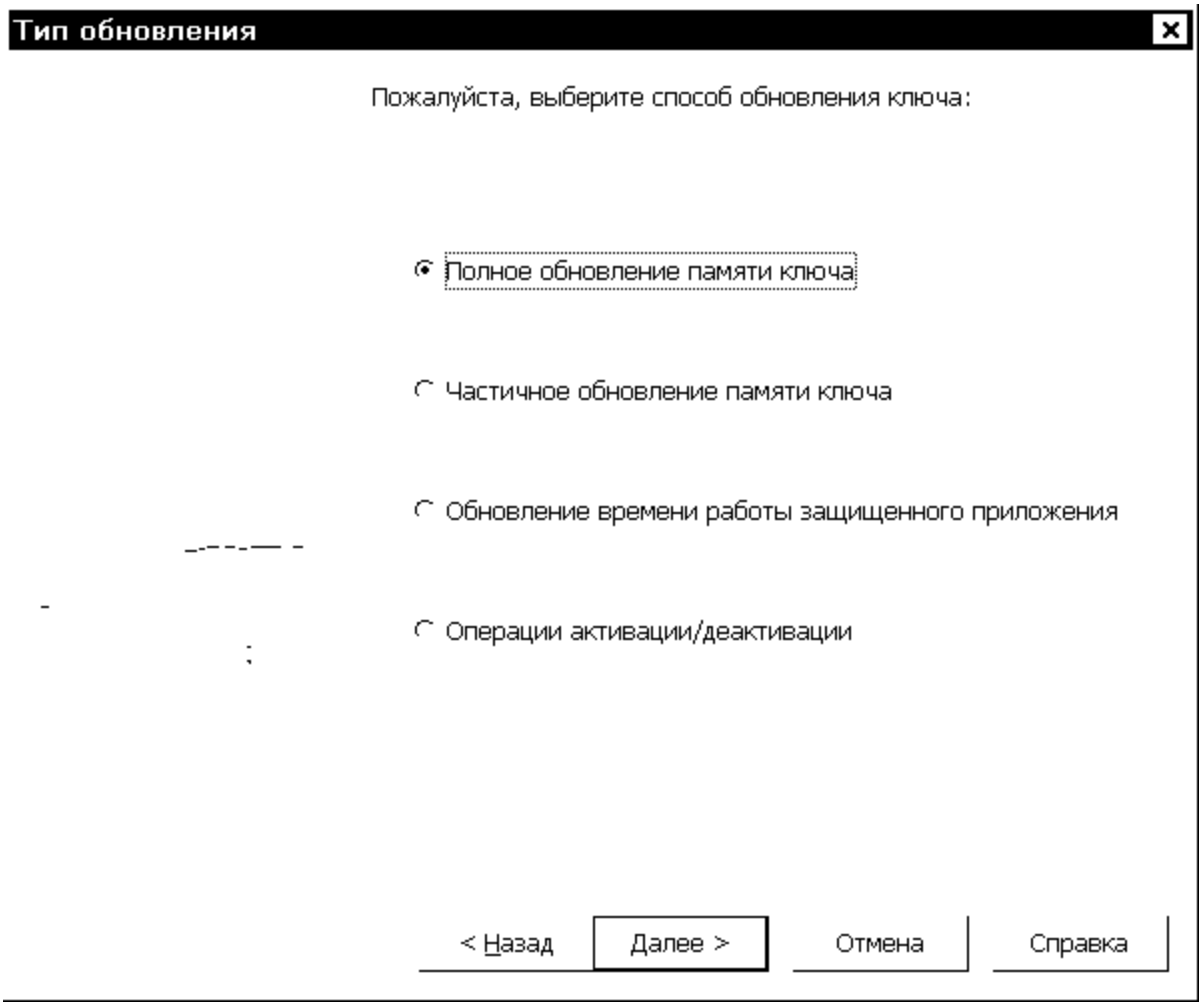
Способ обновления	**Особенности**
Команда **Ключ	Начать удаленное обновление ключа**	Способ доступен только при обновлении от прошивки, т.е. предварительно нужно загрузить образ из имеющейся в базе данных прошивки. Позволяет выбрать тип обновления: полная перезаписьили изменение содержимого отдельных полей
Команда **Ключ	Записать образ в ключ**	Происходит полная перезапись содержимого памяти ключа данными текущего образа

Локальное обновление командой Ключ | Начать удаленное обновление ключа

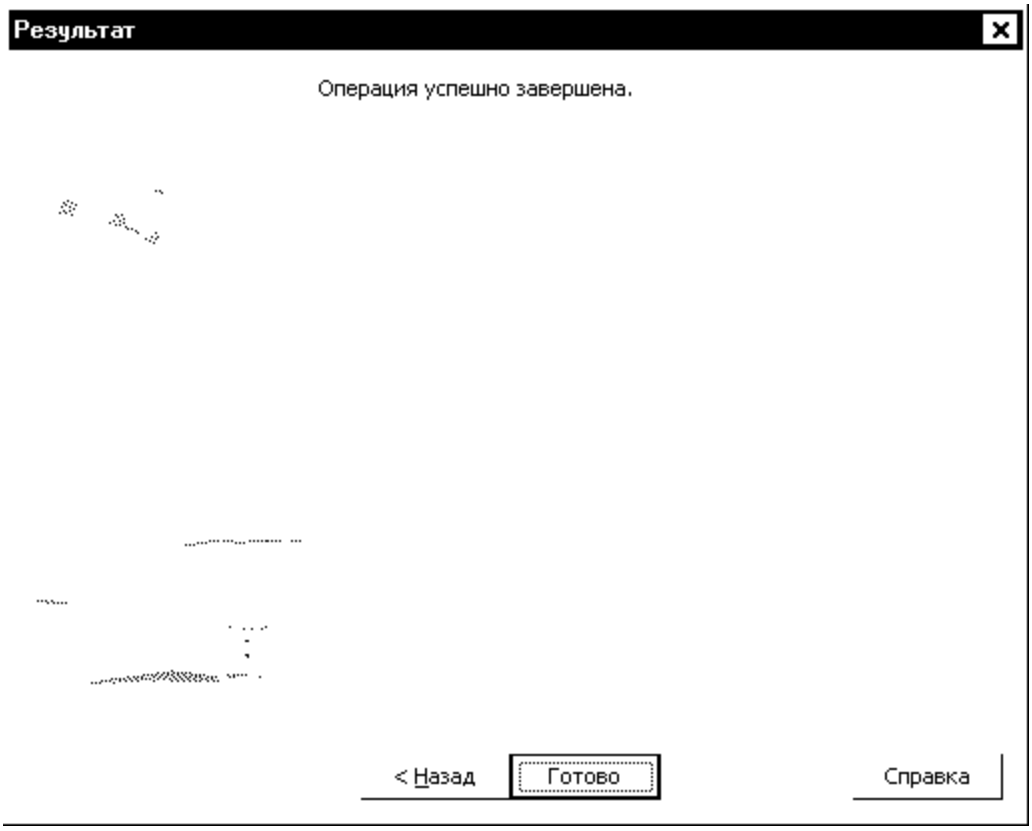
Практическая необходимость в локальном обновлении путем выполнения команды **Ключ | Начать удаленное обновление ключа** возникает, когда требуется сохранить в ключе «наработанные» данные (счетчики алгоритмов, к примеру), т. е. произвести изменение содержимого отдельных полей, не затрагивая остальные поля. В остальных случаях, проще отредактировать данные нужной прошивки или шаблона образа и выполнить команду **Ключ | Записать образ в ключ**.
После выполнения команды **Ключ | Начать удаленное обновление ключа** на экране появляется диалог **Обновление памяти ключа**, который реализован в виде мастера, состоящего из нескольких страниц. Переход между страницами происходит при помощи кнопок **[Далее]**и **[Назад]**, расположенных в нижней части диалогового окна.



Выберите с помощью переключателя пункт **Ключ подсоединенк порту компьютера** и перейдите на следующую страницу.
На экране появится страница **Тип обновления** с селектором выбора. Состояние селектора (доступные варианты обновления) зависит от типа ключа:



Выберите нужный пункт обновления и нажмите на кнопку **[Далее]**. Следующие несколько страниц служат для задания параметров обновления и работы с редактором сценария. Подробно о каждом из вариантов обновления см. далее в разделе **Тип обновления**.
Последняя страница диалога локального обновления называется **Результат**, она отображает сообщение о результате операции:



После нажатия кнопки **[Готово]** обновление завершается, и **GrdUtil.exe** фиксирует в базе данных факт прошивки локального ключа.

Тип обновления памяти ключа

При удаленном или локальном обновлении памяти ключа по факту прошивки доступны следующие варианты обновления:

Тип обновления	**Характеристика**
Полное обновление памяти ключа	Перезапись всего содержимого памяти ключа данными текущего образа
Частичное обновление памяти ключа	Перезапись содержимого полей памяти ключа, не защищенных аппаратным запретом на запись. Можно обновить только одно поле за процедуру обновления
Операции активации/деактивации	Активация, деактивация или перезапись выбранного участка защищенной ячейки, алгоритма или таблицы лицензий.
Изменение времени деактивации алгоритма(для ключей с RTC)	Продление времени работы приложения, защищенного ключом с часами реального времени в режиме лицензирования **Установить время деактивации**

Полное обновление памяти ключа

При полном обновлении памяти ключа происходит перезапись всей памяти ключа данными выбранного образа.
Полное обновление выполняется в тех случаях, когда не требуется сохранения каких-либо «наработанных» данных в ключе, а также когда этот вариант обновления является единственно возможным – при обновлении от файла или шаблона образа.
Чтобы полностью обновить память ключа, выполните команду **Ключ | Начать удаленное обновление ключа**. На экране появится диалог мастера обновления.
Список страниц мастера обновления при полном обновлении памяти ключа:

№	**Страница**	**Действия разработчика**
1	Обновление памяти	Выберите удаленное или локальное обновление.При удаленном обновлении введите в поле запросна обновление от конечного пользователя

2	Тип обновления	Выберите пункт **Полное обновление памяти ключа**
3	Результат	Проконтролируйте результаты работы мастера обновления

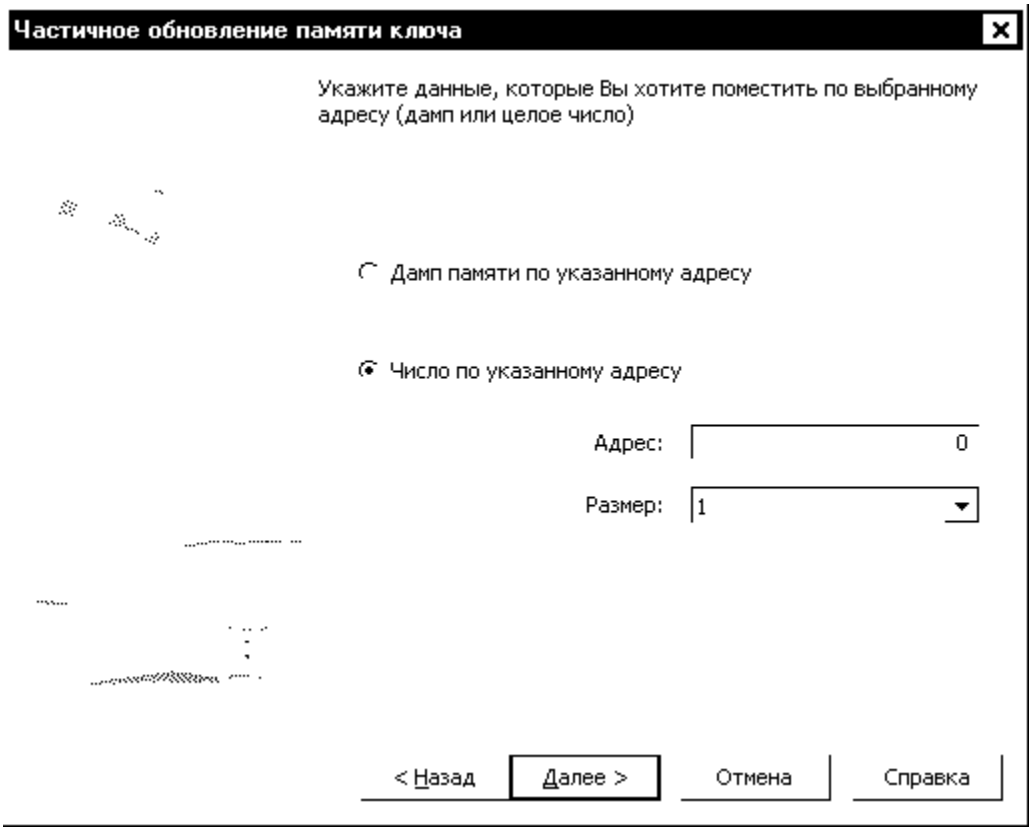
Частичное обновление памяти ключа

Вариант **Частичное обновление памяти ключа** служит для обновления участков памяти, которые не защищены аппаратными запретами на запись. Причем при удаленном обновлении современных ключей Guardant можно обновить только один участок памяти.
Частичное обновление памяти актуально для тех ситуаций, когда необходимо сохранить «наработанную» в ключе информацию (поля счетчиков), и полное обновление памяти неприемлемо. Частично обновить память можно только при обновлении от прошивки, сохраненной в базе данных.
Чтобы обновить участок памяти ключа, не защищенный аппаратным запретом на запись, выполните команду **Ключ | Начать удаленное обновление ключа**. На экране появится диалог мастера обновления.
Список страниц мастера обновления при частичном обновлении памяти ключа:

№	Страница	Действия разработчика
1	Обновление памяти	Выберите удаленное или локальное обновление. При удаленном обновлении введите в поле запрос на обновление от конечного пользователя
2	Тип обновления	Выберите пункт **Частичное обновление памяти ключа**
3	Частичное обновление памяти ключа	Укажите тип данных, адрес и размер участка памяти, содержимое которого необходимо обновить (см. скриншот и описание после таблицы)
4	Частичное обновление памяти ключа	Введите данные обновления.Скриншот и описание интерфейса страницы совпадаютс диалогом редактирования свойств соответствующих полей (см. раздел **Дампы, целые числа, строки и счетчики**)
5	Результат	Проконтролируйте результаты работы мастера обновления

Страница «Частичное обновление памяти ключа»

На странице **Частичное обновление памяти ключа** укажите тип данных, адрес и размер участка памяти, содержимое которого необходимо обновить:



Важно!
Поля памяти, которые необходимо обновить, должны быть предварительно созданы в Редакторе образа.

Элементы управления страницы **Частичное обновление памяти ключа**:

Элемент интерфейса	**Описание**
Переключатель **Дамп памяти / Число**	Выбрать тип данных обновления: дамп или целое число
Поле **Адрес**	Указать адрес, начиная с которого будут записаны данныеобновления. Этот адрес не должен быть защищен аппаратным запретом на запись
Поле/список **Размер**	Указать размер данных обновления, в байтах.Возможные значения: для дампа памяти – произвольныйразмер, для поля – 1, 2, 4

Обновление счетчика GP (времени работы приложения)

Важно!
Устаревший режим обновления, изменяющий значение счетчика GP. Этот режим не подходит для обновления чистого времени работы приложений, использующих счетчик алгоритма (опция автозащиты /DTA).

Для обновления времени работы приложений, защищенных в указанном режиме (версия автозащиты 5.3 и выше) необходимо использовать **Полное обновление памяти ключа**.
Чтобы увеличить значение счетчика GP, выполните команду **Ключ | Начать удаленное обновление ключа**. На экране появится диалог мастера обновления.

Операции активации/деактивации

Для современных ключей Guardant существует специальный режим управления статусом защищенных ячеек и обновления их содержимого. Его достоинство заключается в возможности управлять состоянием защищенной ячейки (активировать/деактивировать) и изменять ее содержимое (читать/перезаписывать), не затрагивая остальную память.
Режим изменения содержимого и статуса защищенной ячейки доступен только при обновлении от прошивки, сохраненной в базе данных.

Важно!
1. Обновлять можно только те защищенные ячейки, для которых перед записью прошивки в ключ был включен хотя бы один из сервисов: активация, деактивация или запись данных.
2. Для обновления доступны только ранее включенные сервисы ячейки.
3. За сеанс удаленного обновления можно выполнить только по одной операцииактивации, деактивации и записи данных, если ранее эти сервисы были включены.
Чтобы обновить участок памяти ключа, защищенный аппаратным запретом на запись, выполните команду **Ключ | Начать удаленное обновление ключа**. На экране появится диалог мастера обновления.

Список страниц мастера обновления в режиме **Операции активации / деактивации**:

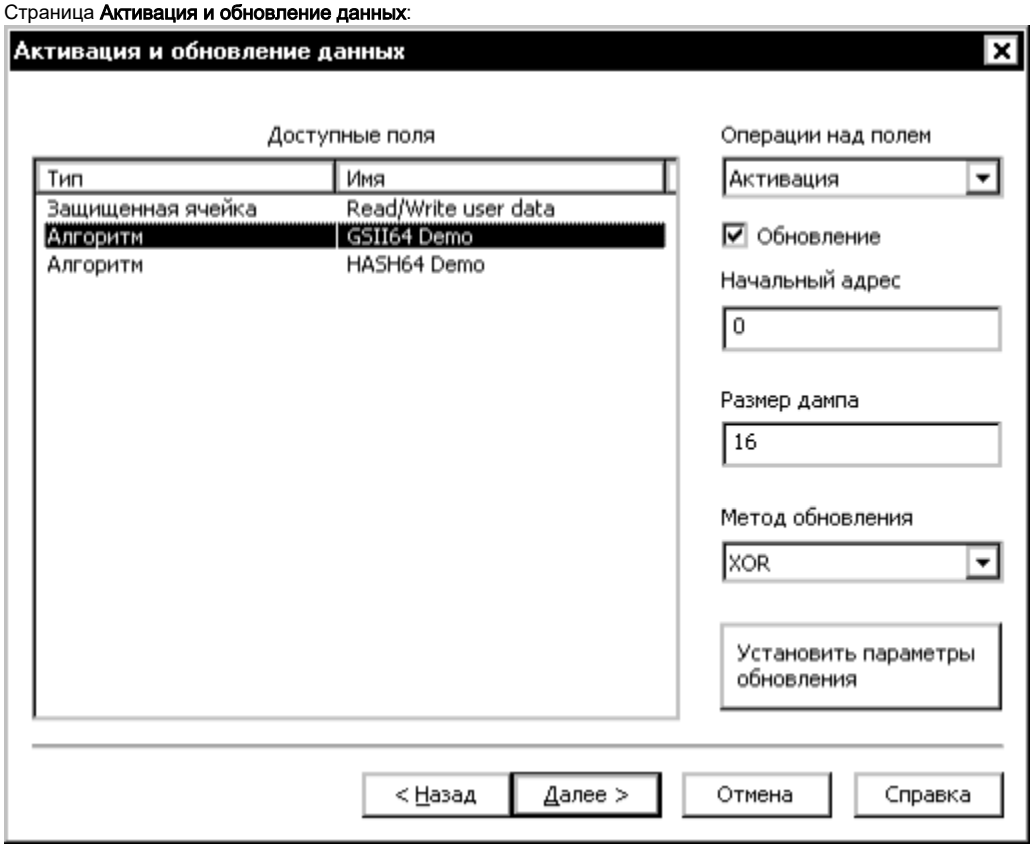
№	Страница	Действия разработчика
1	Обновление памяти	Выберите удаленное или локальное обновление. При удаленном обновлении введите в поле запрос на обновление от конечного пользователя
2	Тип обновления	Выберите пункт **Операции активации/ деактивации**
3	Активацияи обновление данных	Выберите защищенную ячейку, аппаратный алгоритм или таблицу лицензий и задайте для нее необходимые операции (см. скриншот и описание после таблицы)
4	Результат	Проконтролируйте результаты работы мастера обновления

Страница «Активация и обновление данных»

На странице **Активация и обновление данных** выберите защищенную ячейку, аппаратный алгоритм или таблицу лицензий и задайте для нее необходимые операции:

Возможные операции	Описание
Активация	Операция выполняется над ячейкой, находящейся в неактивном состоянии. Для успешного выполнения операции ячейка должна иметь ранее включенный сервис **Активация**.
Деактивация	Операция выполняется над ячейкой, находящейся в активном состоянии. Для успешного выполнения операции ячейка должна иметь ранее включенный сервис **Деактивация**.
Обновление участка защищенной ячейки	Операция выполняется над ячейкой, находящейся в активном состоянии. Для успешного выполнения операции ячейка должна иметь ранее включенный сервис **Обновление данных**. При выполнении операции происходит перезапись выбранного участка ячейки: 1) методом исключающего ИЛИ, 2) методом полного замещения содержимого

Страница **Активация и обновление данных**:



Элементы управления диалога **Активация и обновления данных**:

Элемент интерфейса		**Назначение**
Окно **Доступные поля**		Перечень защищенных ячеек, над которыми можно проводить операции обновления. Чтобы задать операции для поля, выделите его в списке
Список **Операции над полем**	Нет	Не использовать **Операции активации/ деактивации**
	Активация	Активировать ячейку
	Деактивация	Деактивировать ячейку
Флаг **Обновление**		Установить флаг,чтобы использовать операцию обновления ячейки
Поле **Начальный адрес, байтов**		Задать смещение относительно начала обновляемой ячейки
Поле **Размер дампа, байтов**		Задать размер обновляемого участка ячейки
Список **Метод обновления**	**MOV**	Выполнить полное замещение содержимого участка ячейки на данные обновления
	XOR	Выполнить операцию исключающего ИЛИнад содержимым участка ячейки
Кнопка **[Установить параметры обновления]**		Ввести данные обновленияв шестнадцатеричном виде

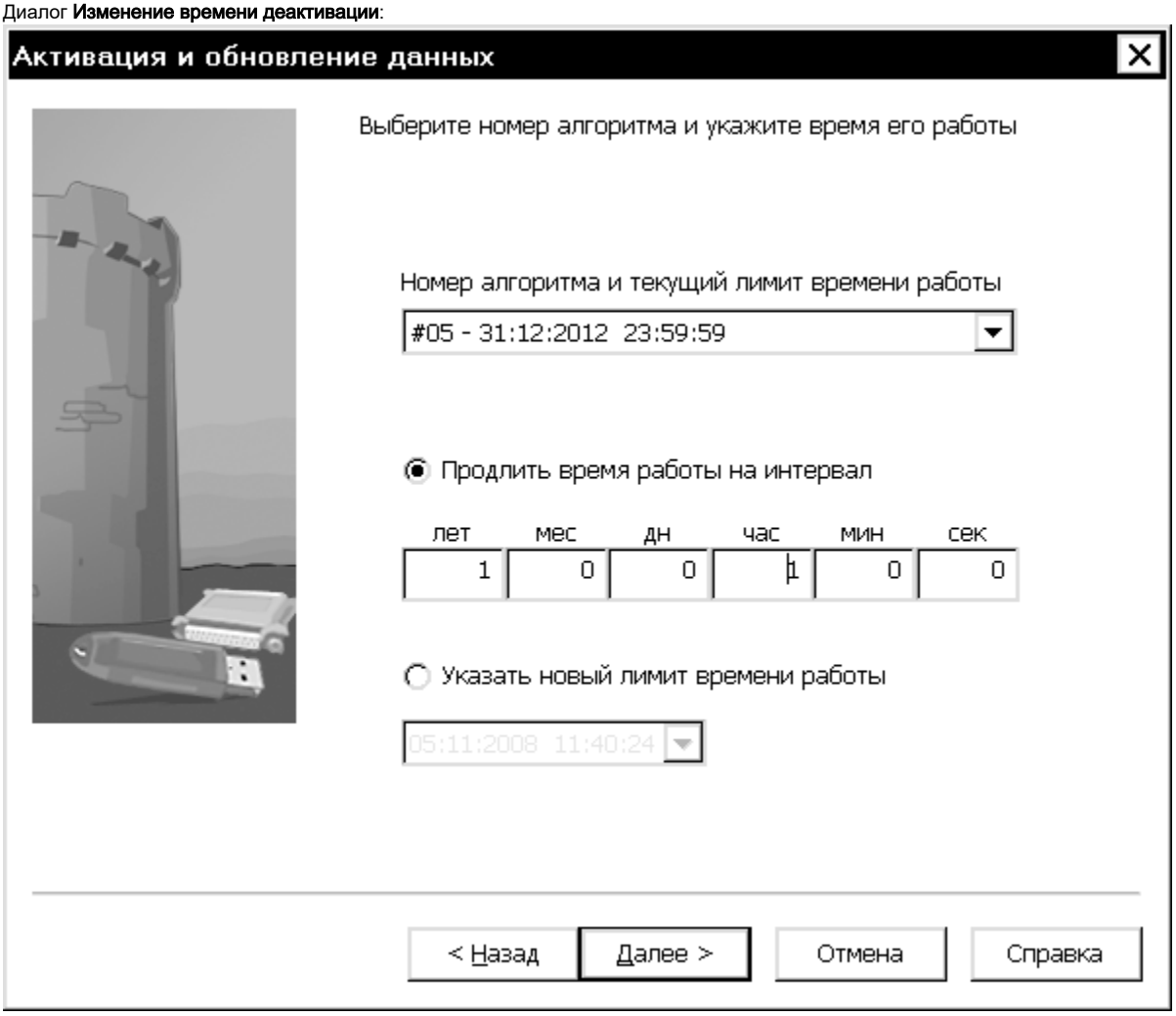
Изменить время деактивации алгоритма. Технология Time

Данный вариант предназначен для ситуаций, когда необходимо продлить срок работы приложения, защищенного ключом Guardant Time в режиме лицензирования **Деактивировать алгоритм по наступлению указанной даты**.
Его достоинство заключается в возможности продлевать время работы приложения, не затрагивая остальную память.
Чтобы изменить время деактивации аппаратного алгоритма в ключе с RTC, выполните команду **Ключ | Начать удаленное обновление ключа**. На экране появится диалог мастера обновления.
Список страниц мастера обновления в режиме **Изменить время деактивации алгоритма**:

№	Страница	Действия разработчика
1	Обновление памяти	Выберите удаленное или локальное обновление. При удаленном обновлении введите в поле запрос на обновление от конечного пользователя
2	Тип обновления	Выберите пункт **Изменить время деактивации алгоритма**
3	Изменение времени деактивации	Выберите аппаратный алгоритм и задайте новое время деактивации (см. скриншот и описание после таблицы)
4	Ответ сгенерирован	Выберите вариант сохранения дампа обновления
5	Результат	Проконтролируйте результаты работы мастера обновления

Страница «Изменение времени деактивации»

На странице **Изменение времени деактивации** выберите аппаратный алгоритм, который нуждается в изменении срока деактивации, и укажите для него новый лимит времени работы или интервал работоспособности.
Диалог **Изменение времени деактивации**:



Элементы управления диалога **Изменение времени деактивации**:

Элемент интерфейса	Назначение

Разворачивающийся список **Номер алгоритма и текущий лимит времени работы**	Выбрать из списка аппаратный алгоритм, для которого необходимо изменить срок деактивации
Переключатель **Продлить время работы на интервал**	Выбрать вариант, при котором деактивация откладывается на заданный интервал
Поле для ввода нового интервала	Задать интервал работоспособности
Переключатель **Указать новый лимит времени работы**	Выбрать вариант, при котором задается календарная дата новой деактивации
Комбинированное поле/календарь	Задать новую дату деактивации