

Модуль генерации ключей
Руководство пользователя

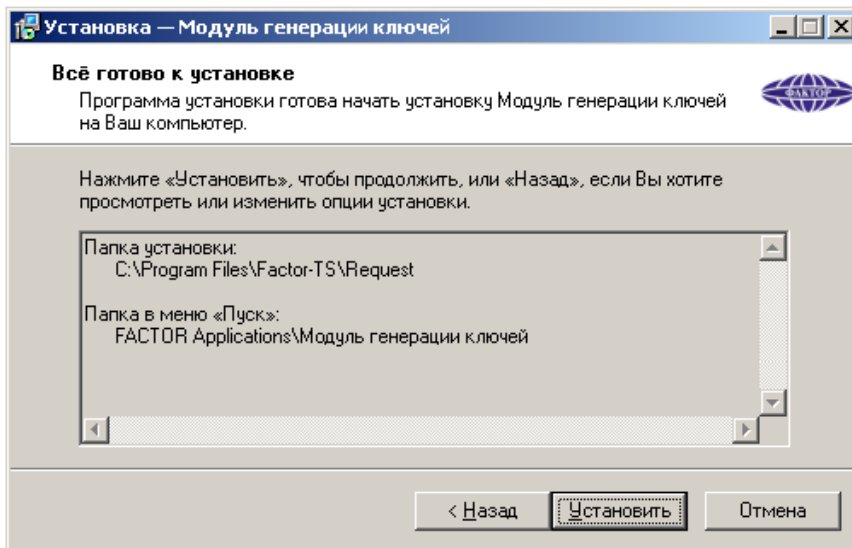
НКБГ.501430.772И6

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
103-18/08	24.03.08			

Содержание

1	Общие сведения.....	3
1.1	Наименование программы.....	3
1.2	Назначение программы МГК.....	3
2	Условия применения программы МГК.....	4
2.1	Требования к оборудованию и операционной среде.....	4
2.2	Ключевые носители.....	4
2.3	Установка ПО МГК.....	4
2.3.1	Установка основного ПО.....	5
2.3.2	Установка дополнительного ПО.....	7
3	Описание задачи.....	9
3.1	Генерация ключей и запросов на сертификаты.....	9
3.1.1	Заполнение формы с исходными данными.....	10
3.1.2	Инициализация ПКДСЧ.....	11
3.1.3	Выбор носителя.....	12
3.1.4	Генерация ключевой пары и запроса на сертификат.....	14
4	Входные и выходные данные.....	15
4.1	Входные данные.....	15
4.1.1	Состав файла инициализации.....	15
4.2	Выходные данные.....	16
	Приложение. Список терминов.....	17

Первое применение					
Справ. №					
Подпись и дата					
Име. № дубл.					
Взам. инв. №					
Подпись и дата	24.03.08				
Име. № подл.	103-18/08				
Изм	Лист	№ документа	Подпись	Дата	
Разработ.	Шпичко			24.03.08	Модуль генерации ключей Руководство пользователя
Проверил	Зенкевич			24.03.08	
Т.контр.	Ветчинкин			24.03.08	
Н.контр.	Кондарь			24.03.08	
Утвердил	Новиков			24.03.08	
НКБГ.501430.772И6					
					Литера
					Лист
					Листов
					0
					2
					18
					ООО «Фактор-ТС»



После нажатия кнопки **Установить** будет выполнена инсталляция.

В состав программного обеспечения **МГК** входят:

- программа генерации ключей и запросов на сертификат **request.exe**;
- программа проверки целостности ПО **CheckWin** и файл **checksum.txt**;
- программа удаления модуля генерации ключей **Uninstall Модуль генерации ключей**;
- конфигурационный файл **request.ini**;
- библиотеки программных модулей (***.dll**).

По окончании инсталляции будет выдано окно с запросом на запуск программы проверки контрольных сумм.

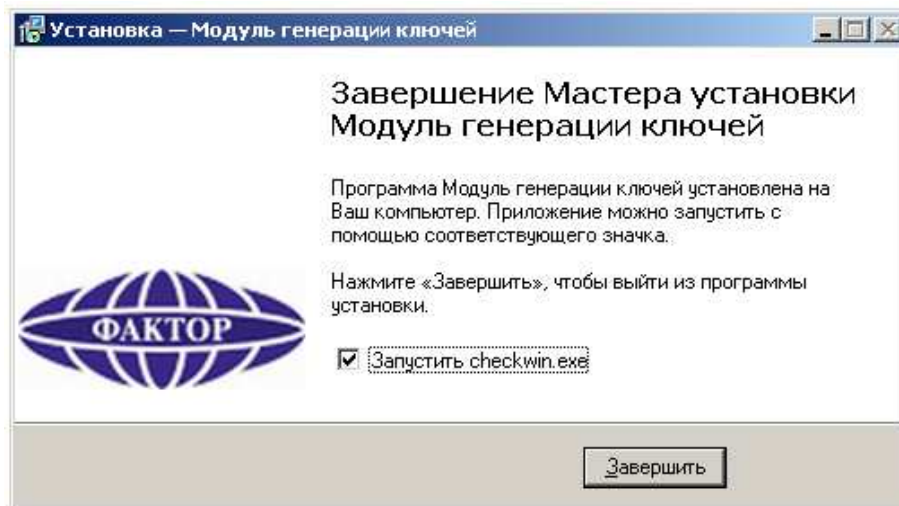


Рис. 1

Проверка целостности полученного программного обеспечения после установки ПО **МГК** на компьютер является обязательной. Кроме того, следует периодически выполнять проверку контрольных сумм в процессе эксплуатации ПО **МГК**. Периодичность проверки

Ине. № подл.	103-18/08
Подпись и дата	24.03.08
Взам. инв. №	
Ине. № дубл.	
Подпись и дата	

Изм	Лист	№ документа	Подпись	Дата	НКБГ.501430.772И6	Лист
						6

целостности ПО **МГК** зависит от условий эксплуатации и определяется политикой безопасности эксплуатирующей организации.

Для проверки целостности ПО служит программа **CheckWin** и файл **checksum.txt**, входящие в состав ПО **МГК**.

Файл **checksum.txt** содержит список файлов программного обеспечения, подлежащих обязательной проверке, вместе с эталонными значениями контрольных сумм. Содержимое файла **checksum.txt** приведено в Формуляре на изделие **МГК**.

Пользователь должен путем просмотра содержимого файла **checksum.txt** сверить значения контрольных сумм данного файла с эталонными значениями, содержащимися в Формуляре. И только убедившись в их идентичности, приступить к дальнейшей проверке.

Запустить программу **CheckWin** (на этапе инсталляции установить флажок **Запустить CheckWin** в окне на Рис. 1 и нажать кнопку **Завершить**). Программа вычислит контрольные суммы файлов, приведенных в списке, сравнит их с эталонными значениями и выведет на экран список проверенных файлов вместе со значениями контрольных сумм.

Если суммы совпадут, то программа выдаст сообщение, что контрольные суммы проверены успешно.

Если будет обнаружено несоответствие, то программа укажет файл, для которого имеет место ошибка контрольной суммы. В этом случае требуется обязательная замена программного обеспечения.

2.3.2 Установка дополнительного ПО

Если предполагается работа с носителями eToken и ruToken, на ПЭВМ пользователя должно быть установлено ПО поддержки (драйверы) этих носителей.

Для удобства пользователей мы включили в дистрибутивный пакет **МГК** ПО драйверов устройств eToken и ruToken. Им можно воспользоваться, если требуемое ПО на ПЭВМ не установлено.

Примечание. ООО «Фактор-ТС» не является разработчиком ПО поддержки носителей eToken и ruToken, а только обеспечивает возможность их использования в качестве ключевых носителей.

ПО поддержки носителей EToken и RuToken располагается в директории **Redist**:

rtDrivers.x86.v.2.15.01.148.exe - инсталляционный файл ruToken;

RTE_3.66.msi - инсталляционный файл eToken;

RTE_3.66.RUI.msi - русификатор для eToken.

Ине. № подл.	103-18/08
Подпись и дата	24.03.08
Взам. инв. №	
Ине. № дубл.	
Подпись и дата	

Изм	Лист	№ документа	Подпись	Дата	НКБГ.501430.772И6	Лист
						7

Установка драйверов носителей ruToken - запустить инсталляционный файл **rtDrives.x86.2.15.01.148.exe**. В процессе установки необходимо пройти через последовательность шагов, которые сопровождаются комментариями и являются стандартными для установки ПО в операционной системе WINDOWS.

Установка драйверов носителей eToken выполняется в следующей последовательности.

Запустить файла **RTE_3.66.msi**. В появившемся на экране окне (Рис. 2) нажать кнопку **Next**. В следующем окне (Рис. 3) включить переключатель **I accept the license agreement** и нажать кнопку **Next**.



Рис. 2



Рис. 3

В появившемся окне (Рис. 4) нажатием кнопки **Next** запустить процесс инсталляции. После завершения установки драйверов на экран выводится окно (Рис. 5), в котором надо нажать кнопку **Finish**.



Рис. 4



Рис. 5

Далее для русификации установленного ПО драйверов носителей eToken надо запустить файл **RTE_3.66.RUI.msi**. В процессе установки необходимо следовать инструкциям, которые сопровождаются комментариями и являются стандартными для установки ПО в операционной системе WINDOWS.

По окончании установки драйверов следует подтвердить запрос на перезагрузку системы.

Ине. № подл.	103-18/08
Подпись и дата	24.03.08
Взам. инв. №	
Ине. № дубл.	
Подпись и дата	

Изм	Лист	№ документа	Подпись	Дата	НКБГ.501430.772И6	Лист
						8

3 Описание задачи

3.1 Генерация ключей и запросов на сертификаты

Генерация ключей и запросов на сертификаты может выполняться каждым участником криптосистемы на своем рабочем месте или специально назначенным для этих работ оператором в зависимости от принятого в организации регламента.

После запуска программы **Модуль генерации ключей** на экран будет выведено главное окно с формой, содержащей исходные данные, необходимые для формирования ключей (Рис. 6).

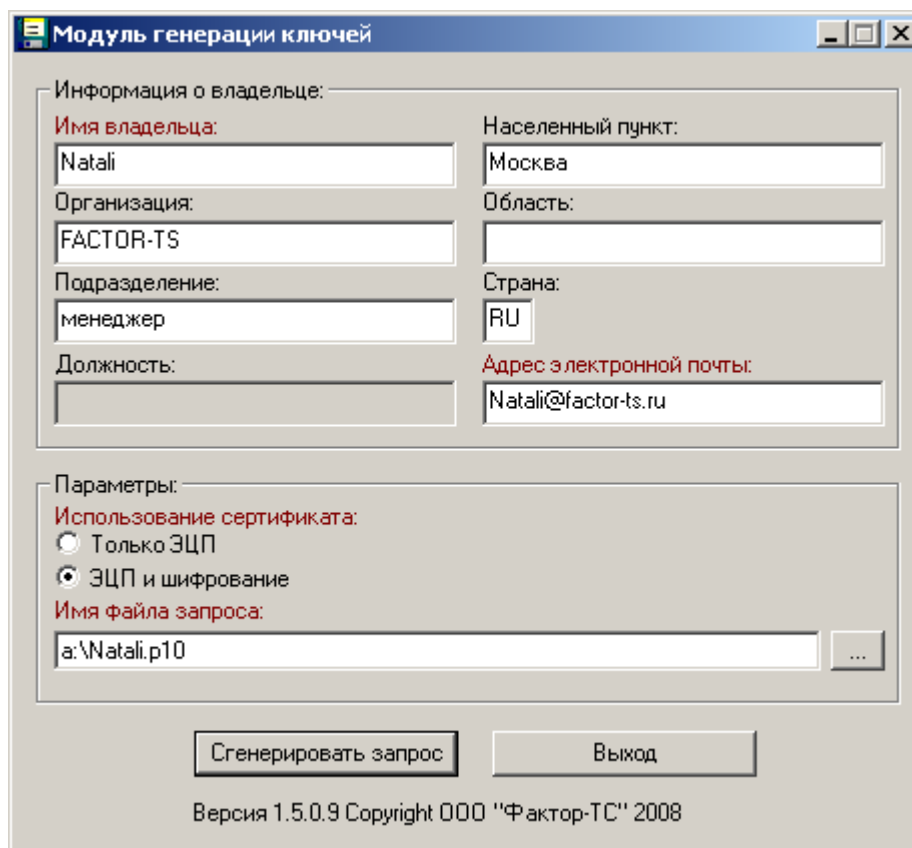


Рис. 6

Передвижение по полям и нажатие кнопок в окне **Модуль генерации ключей** можно выполнять с помощью мыши, а также с помощью клавиш <Tab> (движение вниз) и <Shift+Tab> (движение вверх); нажатие выбранной кнопки выполняется клавишей <Enter>.

Процесс генерации ключевой пары и запроса на сертификат разбит на несколько этапов.

1. Заполнение формы с исходными данными: ввод идентификационных данных о владельце сертификата, выбор необходимых значений параметров для сертификата и указание месторасположения файла, который будет содержать запрос на сертификат.

Име. № подл.	103-18/08
Подпись и дата	24.03.08
Взам. име. №	
Име. № дубл.	
Подпись и дата	

Изм	Лист	№ документа	Подпись	Дата	НКБГ.501430.772И6	Лист
						9

2. Инициализация программно-клавиатурного датчика случайных чисел (ПКДСЧ) и выбор съемного ключевого носителя для записи закрытого ключа вместе с дополнительной информацией.
3. Собственно работа **МГК** по генерации ключевой пары и формированию запроса на сертификат, записи закрытого ключа и дополнительной информации на выбранный съемный носитель и запись запроса на сертификат в указанное на первом этапе место.

3.1.1 Заполнение формы с исходными данными

Группа параметров под заголовком **Информация о владельце** (Рис. 6) задает основную информацию о владельце сертификата.

Группа имеет два обязательных для заполнения поля (их название выводится красным цветом):


- **Имя владельца** - имя участника криптосистемы - владельца сертификата;
- **Адрес электронной почты** - адрес электронной почты владельца сертификата; в качестве адреса электронной почты должен быть указан реальный работающий адрес, который необходим как для контактов участников информационного обмена с владельцем сертификата, так и для работы с почтовыми агентами **DiPost**.

В поле **Страна** вводится стандартное сокращение страны проживания владельца сертификата (значение по умолчанию **RU** – Россия).

Группа под заголовком **Параметры** (Рис. 6).

Переключатель **Использование сертификата** – в зависимости от выбранного значения переключателя тот сертификат, который будет выпущен Удостоверяющим центром по запросу пользователя, сможет поддерживать:

- **Только ЭЦП** - только одну криптографическую функцию – «Формирование ЭЦП»;
- **ЭЦП и шифрование** – две криптографические функции – «Формирование ЭЦП» и «Шифрование».

Имя файла запроса – в поле должно быть занесено имя файла (с указанием полного пути доступа), в который будет записан сгенерированный запрос на сертификат. Файл можно выбрать при помощи кнопки обзора файловой системы компьютера  (кнопка справа от поля с именем файла).

В частности, для размещения файла можно указать тот же съемный носитель, который предназначен для хранения закрытого ключа (см. ниже, раздел 3.1.3, стр. 12).

Име. № подл.	103-18/08
Подпись и дата	24.03.08
Взам. инв. №	
Име. № дубл.	
Подпись и дата	

Изм	Лист	№ документа	Подпись	Дата	НКБГ.501430.772И6	Лист
						10

Примечание. Рекомендованное расширение имени данного файла - **p10**, оно добавляется автоматически.

МГК не позволит продолжить работу, если обязательные поля не будут заполнены – выдается предупреждающее сообщение и предоставляется возможность ввести нужные параметры.

Набор полей, обязательных и необязательных для заполнения, а также доступных и заблокированных, может определяться администратором Удостоверяющего Центра на основе собственной политики выдачи сертификатов. Соответствующая информация должна быть занесена пользователем **МГК** в конфигурационный файл **request.ini**, помещенный в директорию установки программы.

3.1.2 Инициализация ПКДСЧ

После того как будут заполнены все поля, необходимо в окне **Модуль генерации ключей** (Рис. 6) нажать кнопку **Сгенерировать запрос**.

Программа предложит выполнить инициализацию программно-клавиатурного датчика случайных чисел (ПКДСЧ). Следуя инструкции по инициализации ПКДСЧ (Рис. 7), необходимо тридцать один раз либо устанавливать курсор мыши на маленькое желтое окно, появляющееся в различных местах экрана, и нажимать левую кнопку мыши, либо вводить с клавиатуры указанный в желтом окне символ (с учетом регистра!).

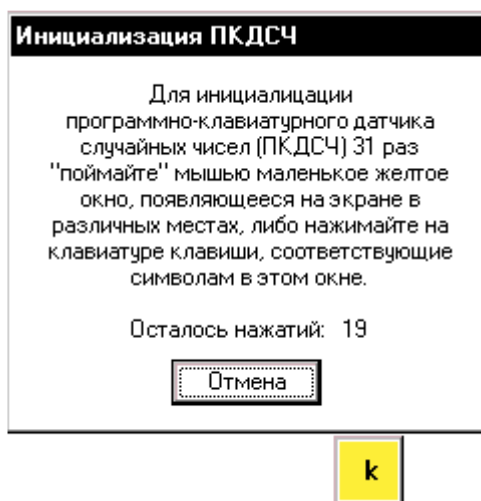


Рис. 7

В поле **Осталось нажатий** (Рис. 7) отображается, сколько нажатий осталось сделать пользователю до завершения процесса инициализации ПКДСЧ. До тех пор пока инициализация не будет закончена, генерация ключевой пары и запроса на сертификат не начнется.

Примечание. Следует быть внимательным, поскольку маленькое желтое окошко может появиться на значительном расстоянии от окна **Инициализация ПКДСЧ**.

Ине. № подл.	103-18/08
Подпись и дата	24.03.08
Взам. инв. №	
Ине. № дубл.	
Подпись и дата	

Изм	Лист	№ документа	Подпись	Дата	НКБГ.501430.772И6	Лист
						11

1. Если выбран носитель eToken или ruToken, на экран выводится окно (Рис. 9) для ввода пароля (пароль устанавливает производитель носителя, в дальнейшем пользователь пароль может изменить).

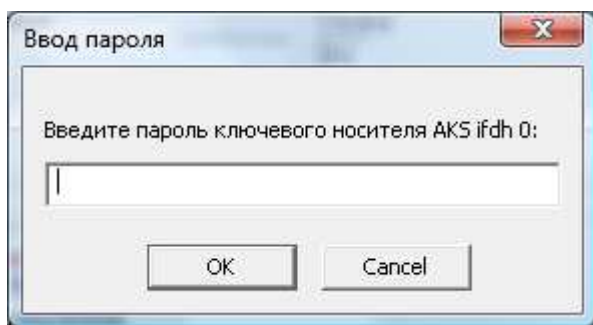


Рис. 9

Следует ввести пароль и нажать кнопку **OK**. При вводе ошибочного пароля на экран будет выведено сообщение об ошибке, процедура генерации заканчивается и на экране активизируется главное окно (Рис. 6).

При нажатии кнопки **Cancel** программа выдаст сообщение о том, что операция генерации ключевого носителя прервана, и вернется в главное окно.

2. При выборе носителя НГМД или Flash-памяти будет выдан запрос, позволяющий установить пароль на ключевой носитель (Рис. 10). Пароль устанавливать не обязательно.

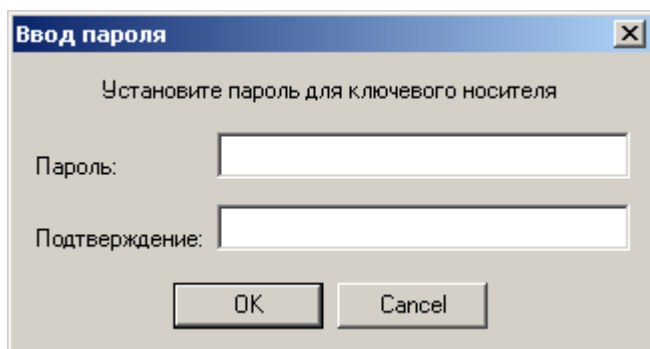


Рис. 10

Если пароль будет установлен, то система будет требовать ввода этого пароля каждый раз при обращении к ключевому носителю. В дальнейшем пароль *НЕЛЬЗЯ* ни заменить, ни отменить.

Вне зависимости от того, будете Вы устанавливать пароль на ключевой носитель или нет, для продолжения работы из последнего окна (Рис. 10) необходимо выходить нажатием кнопки **OK**.

При нажатии кнопки **Cancel** программа выдает сообщение о том, что операция генерации ключевого носителя прервана оператором и вернется на главное окно.

Ине. № подл.	103-18/08
Подпись и дата	24.03.08
Взам. инв. №	
Ине. № дубл.	
Подпись и дата	

Ине. № подл.	103-18/08					НКБГ.501430.772И6	Лист
Изм	Лист	№ документа	Подпись	Дата			13

3.1.4 Генерация ключевой пары и запроса на сертификат

После выбора типа носителя программа **МГК** выполняет следующие действия:

- генерирует ключевую пару;
- записывает закрытый ключ с дополнительной информацией на выбранный съемный носитель;
- записывает в указанный файл - **Имя файла запроса** (Рис. 6) - запрос на сертификат, включающий в себя открытый ключ, информацию о выбранном пользователе алгоритме для создания открытого ключа и другую информацию;
- выдает на экран сообщение об успешном формировании запроса на сертификат и возвращается в главное окно (Рис. 6).

Для завершения работы, если требуется сгенерировать только одну ключевую пару (и запрос на сертификат), следует нажать кнопку **Выход** (Рис. 6 **Ошибка! Источник ссылки не найден.**) и выйти из программы.

Для генерирования новой ключевой пары (и нового запроса на сертификат) необходимо внести изменения в поля формы (Рис. 6), при этом необходимо обязательно ввести новое имя файла для размещения запроса на сертификат (иначе прежний запрос на сертификат будет утерян) и нажатием кнопки **Сгенерировать запрос** запустить новый процесс.

При генерации второй и последующих ключевых пар инициализация ПҚДСЧ не требуется. Она необходима только при повторном запуске программы.

Обращаем Ваше внимание! При повторной генерации ключей без изменения данных в полях формы (Рис. 6) полученная ключевая пара будет отличаться от предыдущей.

На одной ключевой носитель можно записать только один закрытый ключ. После выполнения программы **МГК** на ключевом носителе будут размещены три файла (контейнера) с именами, имеющими одинаковую основную часть имени и различные расширения:

<идентификатор_ключа> **.pvt** – закрытый ключ;

<идентификатор_ключа> **.hdr** – дополнительная информация для закрытого ключа,

<идентификатор_ключа> **.nam** – файл ссылки на контейнер закрытого ключа,

где <идентификатор_ключа> – значение, получаемое при помощи ПҚДСЧ.

Кроме того, на этот ключевой носитель можно поместить файл, содержащий запрос на сертификат. Для этого в главном окне ((Рис. 6) в поле **Имя файла запроса** для размещения файла с запросом на сертификат должен быть указан файл на данном носителе.

Име. № подл.	103-18/08	Подпись и дата		Име. № дубл.		Подпись и дата	
Взам. инв. №		Подпись и дата	24.03.08	Име. № дубл.		Подпись и дата	
Изм		Лист		№ документа		Подпись	
Дата		Лист		Дата		Лист	
НКБГ.501430.772И6							14

4.2 Выходные данные

Выходными данными программы являются:

1. Ключевая информация, сгенерированная программой и записанная на ключевой носитель. Состав ключевой информации приведен в разделе 3.1.4 на стр. 14.
2. Запрос на сертификат для сгенерированной пары ключей, записанный либо на ключевой носитель, либо на отдельный магнитный носитель, предназначенный для передачи в Управляющий центр.

После получения сертификата ключи готовы к использованию для получения подписанных ЭЦП файлов (например, программой **DiSignCA**) и/или для шифрования (например, программой **DiPostCA**).

Ине. № подл.	103-18/08	Подпись и дата	24.03.08	Взам. инв. №	Ине. № дубл.	Подпись и дата	НКБГ.501430.772И6					Лист
												16
Изм	Лист	№ документа	Подпись	Дата								

	<ul style="list-style-type: none"> - уведомление владельца сертификата ключа о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа; - предоставляет участникам информационных систем иные услуги, связанные с использованием сертификатов ключей.
Электронная цифровая подпись (ЭЦП)	Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате преобразования информации в соответствии с алгоритмом электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа, а также установить отсутствие искажения информации в электронном документе (предназначенный для подтверждения целостности электронного документа и подлинности его авторства).

Ине. № подл.	103-18/08	Подпись и дата	24.03.08	Взам. инв. №		Ине. № дубл.		Подпись и дата	
Изм	Лист	№ документа	Подпись	Дата	НКБГ.501430.772И6				Лист 18