

ЕВФРАТ

Н а с т р о й к а Э Ц П
Руководство пользователя

Содержание

ВВЕДЕНИЕ	3
i. Программа Настройка ЭЦП	3
ii. Необходимые сведения	3
iii. Условные обозначения.....	4
1. НАСТРОЙКА КРИПТОСИСТЕМЫ	5
1.1. Установка и запуск программы Настройка ЭЦП.....	5
1.2. Настройка на уровне системного администратора	6
1.3. Настройка на уровне администратора системы ЕВФРАТ	7
1.3.1. Тактика настройки криптосистемы.....	8
1.3.2. Настройка и публикация описания параметров криптосистемы	9
1.3.3. Просмотр опубликованных открытых ключей пользователей	11
1.4. Настройка на уровне пользователя системы ЕВФРАТ	12
1.4.1. Получение описания параметров криптосистемы с сервера.....	13
1.4.2. Формирование новой ключевой пары	15
1.5. Некоторые специальные вопросы.....	16
1.5.1. Особенности, связанные со сменой криптопровайдера или изменением параметров криптосистемы.....	17
1.5.2. Особенности, связанные с восстановлением базы данных ЕВФРАТ из резервной копии.....	17
1.5.3. Работа с несколькими серверами	17
1.5.4. ЭЦП и документы Microsoft Word.....	18
1.5.5. ЭЦП и архивные документы	18
2. СЛОВАРЬ ТЕРМИНОВ	19

Введение

і. Программа Настройка ЭЦП

В состав системы **ЕВФРАТ** включена собственная криптографическая система (далее — *криптосистема*; значения терминов приведены в конце данного документа в разделе 1.2 «Словарь терминов»). Криптосистема позволяет устанавливать *подлинность* электронных документов, зарегистрированных в системе **ЕВФРАТ**. Под подлинностью документа понимается его неизменность и авторство. Подлинность документа устанавливается на основании проверки *электронно-цифровой подписи* (далее — *ЭЦП*), которая проставляется пользователем с помощью средств криптосистемы. ЭЦП может быть сформирована для любого электронного документа, содержащего присоединенные файлы.

Программа **Настройка ЭЦП** предназначена для настройки параметров встроенной в **ЕВФРАТ** криптосистемы.

іі. Необходимые сведения

Проверка подлинности документов, зарегистрированных в системе **ЕВФРАТ**, основана на использовании электронно-цифровой подписи. ЭЦП может быть сформирована для любого электронного документа, содержащего присоединенные файлы, с сохранением уникальных признаков подписавшего документ пользователя.

Электронно-цифровая подпись (ЭЦП) — это последовательность символов, позволяющая установить, что исходный текст не был изменен с тех пор, как его подписал (сформировал ЭЦП этого текста) указанный человек. Подчеркнем, что с точки зрения применяемых алгоритмов и принятой логики работы в системе **ЕВФРАТ** ЭЦП не является выражением отношения пользователя, подписавшего документ, к содержанию документа (согласен или не согласен). ЭЦП — это средство проверки неизменности документа. Пользователь, поставивший в электронном документе свою ЭЦП, подтверждает этим, что видел документ именно таким.

В системе **ЕВФРАТ** один и тот же документ может быть подписан несколькими пользователями. Впоследствии как пользователь, подписавший документ, так и другие пользователи могут проверить каждую из ЭЦП документа. В результате проверки выясняется, верна подпись или неверна. Первое означает, что документ не изменялся и его подписал именно тот сотрудник, имя которого указано в системе. Второе означает, что документ был изменен либо был подписан не тем сотрудником, имя которого указано в системе.

Рассмотрим некоторые специальные понятия. ЭЦП создается путем преобразования текста электронного документа. Само преобразование, а также ряд других действий, выполняемых встроенной в **ЕВФРАТ** криптосистемой, осуществляются специальными программными модулями — *криптопровайдерами*. При формировании ЭЦП используются алгоритмы *хэширования* и *несимметричного шифрования* данных.

Метод несимметричного шифрования характеризуется тем, что шифрование и дешифровка текста производятся с помощью разных ключей, составляющих ключевую пару или, другими словами, пару «*закрытый-открытый ключ*». Названия ключей «закрытый» и «открытый» отражают тот факт, что закрытый ключ, принадлежащий

какому-либо пользователю, сохраняется в тайне. Тогда как соответствующий ему открытый ключ распространяется среди пользователей, проверяющих ЭЦП.

Фактически при формировании ЭЦП производится шифрование *хэша* документа закрытым ключом пользователя. При проверке ЭЦП происходит следующее: создается хэш проверяемой версии документа; хэш подписанной версии документа расшифровывается открытым ключом подписавшего пользователя; два полученных хэша сравниваются, — в результате устанавливается, был ли изменен исходный текст с тех пор, как в нем поставлена ЭЦП.




Для работы криптосистемы необходима тождественность следующих параметров на компьютерах всех пользователей системы **ЕВФРАТ**:

- используемого криптопровайдера;
- алгоритма *симметричного шифрования* (для работы с ЭЦП не используется);
- алгоритма хэширования;
- длин ключей (открытого и закрытого ключей, используемых в алгоритме несимметричного шифрования).

iii. Условные обозначения

В данном документе используются условные обозначения, приведенные в таблице 1.

Таблица 1. Условные обозначения

Обозначение	Смысл
Выберите в меню Файл ...	Заголовки окон, названия пунктов меню и других элементов пользовательского интерфейса.
Нажмите комбинацию клавиш CTRL+O	Обозначения клавиш, комбинаций клавиш.
Введите с клавиатуры значение 15.	Строки, вводимые пользователем с клавиатуры, отображаемые на экране, а также листинги, команды, имена файлов и каталогов.
Для того чтобы посмотреть протокол:	Описание действий, выполняемых пользователем.
1. Перейдите на вкладку Просмотр ...	
 Заметьте...	Замечание.
 Вот хороший совет...	Совет по работе с программой
 Осторожно!...	Предостережение о возможных ошибках.

1. Настройка криптосистемы

Обеспечение работы встроенной в **ЕВФРАТ** криптосистемы происходит на трех уровнях:

- на уровне системного администратора.
- на уровне администратора системы **ЕВФРАТ**.
- на уровне пользователя системы **ЕВФРАТ**.

Такое разделение условно. Вполне вероятно, что пользователи системы **ЕВФРАТ** сочтут целесообразным, чтобы настройку на уровне пользователя также осуществлял администратор системы **ЕВФРАТ**.

1.1. Установка и запуск программы Настройка ЭЦП

Настройка криптосистемы осуществляется с помощью программы **Настройка ЭЦП**, которая устанавливается в составе программного продукта **ЕВФРАТ Клиент**, см. «Руководство по установке системы».

Чтобы запустить программу Настройка ЭЦП:

1. Убедитесь, что модуль **Сервер ЕВФРАТ** запущен. Если это не так, запустите его.
2. Запустите программу **Настройка ЭЦП** через меню *Windows: Пуск* → **Программы** → **ЕВФРАТ** → **Настройка ЭЦП**.
3. В появившемся диалоговом окне **Соединение с сервером** (рис. 1) укажите свое системное имя и пароль.



Доступ к программе **Настройка ЭЦП** имеют все пользователи, зарегистрированные в системе **ЕВФРАТ**.

Соединение с сервером

Имя
Admin2003

Пароль
xxxx

Сервер:номер порта
Server2003:17170

ОК Отмена

Рис. 1. Запуск программы Настройка ЭЦП

4. В поле **Сервер:номер порта** укажите имя сервера, состоящее из сетевого имени компьютера, на котором работает модуль **Сервер ЕВФРАТ**, и номера порта.
5. Нажмите на кнопку **ОК**. Если все поля заполнены правильно, откроется окно программы **Настройка ЭЦП**. Если при вводе имени пользователя, пароля или

сетевого имени сервера была допущена ошибка, на экран будет выведено сообщение о невозможности подключения к серверу и запуска программы.

6. Если на данном компьютере криптосистема еще не настроена, появится ряд сообщений. Пропустите их, нажимая на кнопку **ОК**.



Если в меню *Windows*: **Пуск** → **Программы** отсутствует пункт **ЕВФРАТ** или далее отсутствует подпункт **Настройка ЭЦП**, то, возможно, компонент **Настройка ЭЦП** не установлен. В этом случае воспользуйтесь программой установки **ЕВФРАТ Клиент**.

1.2. Настройка на уровне системного администратора

Системный администратор обеспечивает установку одинаковых криптопровайдеров на всех компьютерах, где предполагается применять ЭЦП для зарегистрированных в системе **ЕВФРАТ** документов. Допустимо использование криптопровайдеров, входящих в стандартную комплектацию операционной системы. Чтобы выяснить, какие из них установлены на компьютерах пользователей, воспользуйтесь документацией по операционным системам *Windows* или средствами программы **Настройка ЭЦП**.

Чтобы определить, какие криптопровайдеры уже установлены на компьютере пользователя:

1. Запустите программу **Настройка ЭЦП** под именем администратора системы **ЕВФРАТ** (см. п. 1.1).
2. Перейдите на вкладку **Настройка параметров сервера** (см. рис. 2).

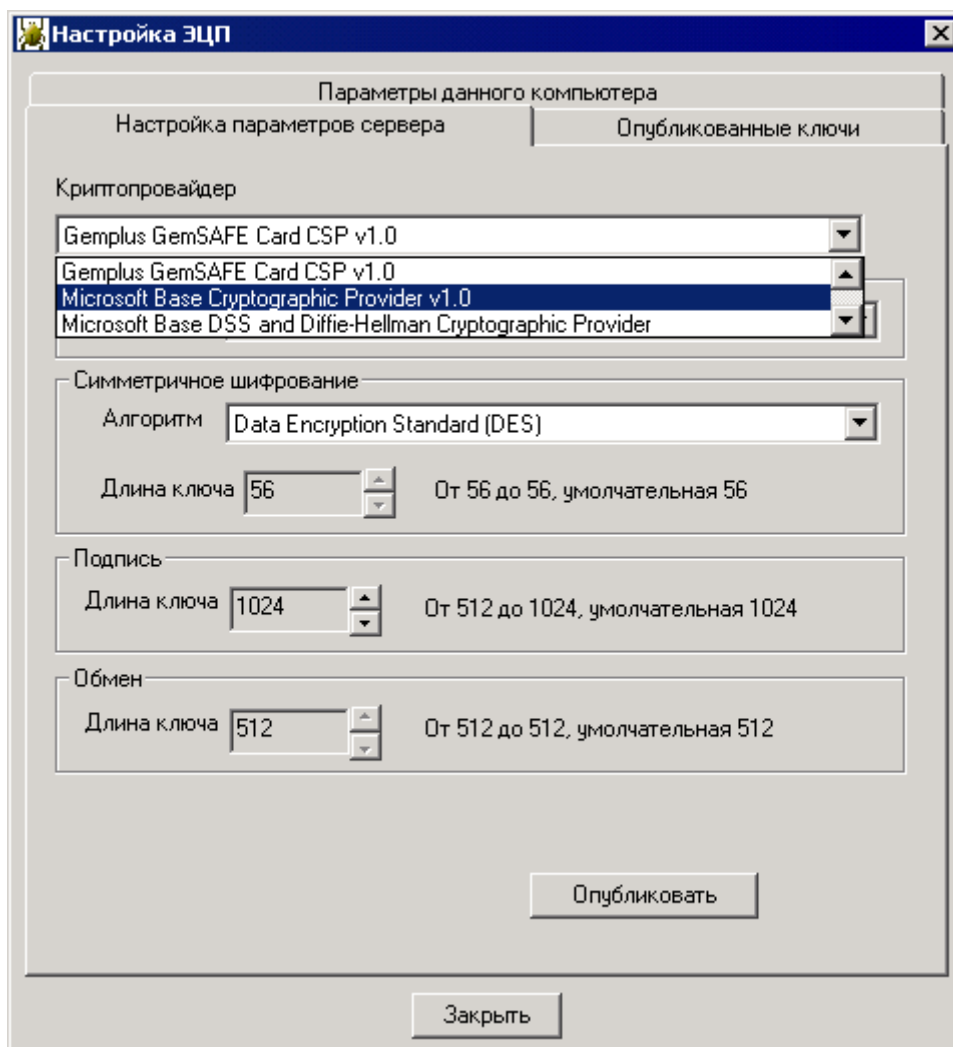


Рис. 2 Список установленных на компьютере криптопровайдеров

3. Просмотрите раскрывающийся список **Криптопровайдер**. В нем перечислены криптопровайдеры, установленные на данном компьютере.
4. Таким же образом просмотрите списки установленных криптопровайдеров на компьютерах других пользователей системы **ЕВФРАТ**.

При необходимости, дополнительно установите криптопровайдеры на компьютеры пользователей. В этом случае обратитесь к специальной литературе по криптографической защите данных в компьютерных сетях или к специалистам фирм, имеющих лицензии на производство криптографических средств защиты.

1.3. Настройка на уровне администратора системы ЕВФРАТ

После запуска программы **Настройка ЭЦП** (см. п. 1.1) перейдите на вкладку **Настройка параметров сервера** (рис. 3). На этой вкладке осуществляется настройка криптосистемы. Следует отметить, что криптосистема, включенная в состав **ЕВФРАТ**, предназначена для выполнения целого комплекса функций: формирования и проверки ЭЦП, шифрования электронных документов, шифрования трафика между клиентским рабочим местом и сервером. Для пользователей текущей версии системы **ЕВФРАТ** доступны только функции формирования и проверки ЭЦП.

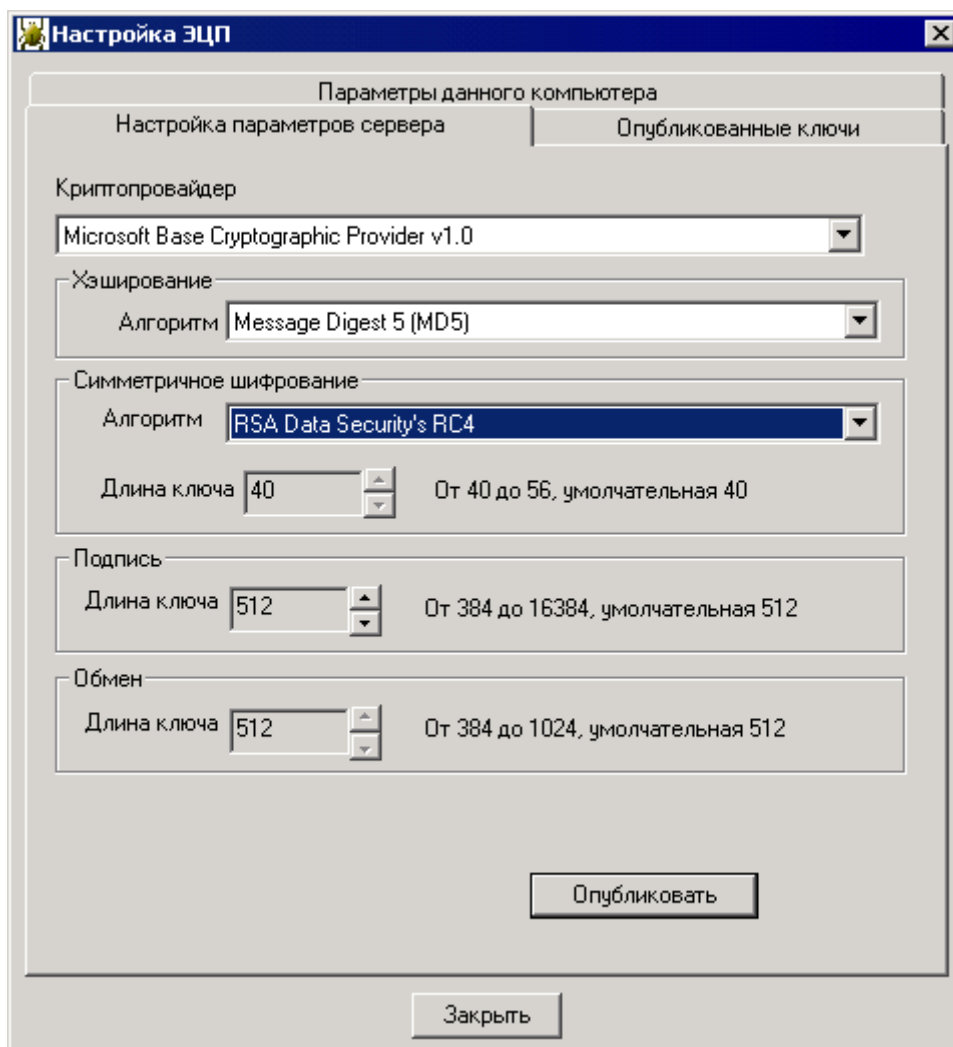


Рис. 3. Настройка параметров сервера

Чтобы настроить криптосистему для формирования ЭЦП в документах, на вкладке **Настройка параметров сервера** (рис. 3) следует заполнить следующие поля:

- **Криптопровайдер** — криптопровайдер из числа установленных на компьютере, который будет использоваться для формирования ЭЦП;
- **Алгоритм** (в группе элементов **Хэширование**) — алгоритм хэширования, используемый при формировании ЭЦП;
- **Длина ключа** (в группе элементов **Подпись**) — длина генерируемых ключей (открытого и закрытого) в битах.

Дополнительно следует заполнить группу полей **Симметричное шифрование**, хотя эти настройки и не используются непосредственно при формировании ЭЦП.

1.3.1. Тактика настройки криптосистемы

При настройке ЭЦП администратор системы **ЕВФРАТ** выполняет следующие действия:

1. Запускает программу **Настройка ЭЦП** под именем администратора системы **ЕВФРАТ**.
2. В программе **Настройка ЭЦП** формирует описание параметров криптосистемы (администратор выбирает криптопровайдер, алгоритм хэширования и длину

открытого и закрытого ключей; дополнительно выбирает алгоритм симметричного шифрования и длину ключа для этого алгоритма).

3. Публикует описание параметров криптосистемы на сервере. (Каждый из пользователей, которые желают подписывать электронные документы с помощью ЭЦП или проверять ЭЦП других пользователей, формирует собственную ключевую пару средствами программы **Настройка ЭЦП** (см. п. 1.4). Чтобы обеспечить тождественность параметров криптосистемы на всех компьютерах, пользователи получают описание параметров криптосистемы с сервера. Следовательно, параметры предварительно должны быть опубликованы на сервере.)
4. В случае неудачной публикации, формирует и публикует другой набор параметров криптосистемы.

1.3.2. Настройка и публикация описания параметров криптосистемы

Администратор системы **ЕВФРАТ** осуществляет подбор параметров криптосистемы исходя из двух принципов:

1. Выбранный криптопровайдер установлен на компьютерах всех пользователей.
2. Выбранное сочетание параметров должно успешно публиковаться на сервере ЕВФРАТ.

При публикации описания параметров ЭЦП производится тестирование работы криптосистемы с произведенными настройками. Тестирование проходит на компьютере администратора системы **ЕВФРАТ**. При тестировании выполняется набор стандартных действий криптосистемы. В случае неудачного прохождения теста публикация не производится и администратору следует сформировать и опубликовать другой набор параметров. Причиной неудачного прохождения теста может являться, например, тот факт, что выбранному криптопровайдеру для хранения закрытых ключей пользователей требуется дополнительное оборудование. В этом случае обращайтесь к документации, прилагаемой к данному криптопровайдеру, или используйте другой криптопровайдер.



Отметим, что хорошие результаты дает выбор криптопровайдера *Microsoft Base Cryptographic Provider v1.0* в сочетании с алгоритмом хэширования *Message Digest 5 (MD5)* и алгоритмом симметричного шифрования *RSA Data Security RC4* с длинами ключей, принятыми по умолчанию (в частности, 512 бит для ЭЦП).

Криптопровайдеры *Microsoft Enhanced Cryptographic Provider v1.0* и *Microsoft Strong Cryptographic Provider* обладают лучшими характеристиками, но менее распространены.

Для остальных криптопровайдеров настоятельно рекомендуется изучить прилагаемую к ним документацию, чтобы определить их пригодность в предполагаемых условиях работы.

Чтобы настроить параметры ЭЦП и опубликовать на сервере их описание:

1. Запустите программу **Настройка ЭЦП** под именем администратора системы **ЕВФРАТ** (см. п. 1.1).
2. Перейдите на вкладку **Настройка параметров сервера** (см. рис. 3).
3. Выберите криптопровайдера из раскрывающегося списка **Криптопровайдер**.

4. В группе элементов **Хэширование** укажите алгоритм хэширования, выбрав его из раскрывающегося списка.
5. В группе элементов **Подпись** укажите длину ключа (это длина открытого и закрытого ключей в ключевой паре).



При выборе длины ключа следует иметь в виду, что увеличение длины ключа приводит к увеличению стойкости шифра (т. е., в случае ЭЦП, усложняет ее подделку) и замедлению процессов шифрования/дешифровки (процессов формирования и проверки ЭЦП). Для достижения оптимально эффективной работы криптосистемы следует обратиться к специальной литературе по криптографической защите данных в компьютерных сетях или к специалистам фирм, имеющих лицензии на производство криптографических средств защиты.

1. Опубликуйте на сервере описание параметров криптосистемы. Для этого нажмите на кнопку **Опубликовать** в нижней части вкладки **Настройка параметров сервера**.
2. Если тестирование описания параметров криптосистемы прошло успешно, появится предупреждение, представленное на рис. 4.

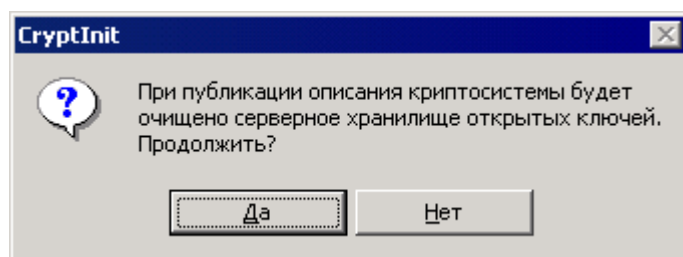


Рис. 4. Предупреждение при публикации описания параметров криптосистемы



Внимательно отнеситесь к этому предупреждению. После публикации нового описания параметров криптосистемы серверное хранилище открытых ключей будет очищено и потребуются заново создать пары «закрытый-открытый ключ» для всех пользователей.

3. Нажмите на кнопку **Да**, чтобы продолжить публикацию нового описания параметров криптосистемы.

1.3.3. Просмотр опубликованных открытых ключей пользователей

Программа **Настройка ЭЦП** позволяет администраторам системы **ЕВФРАТ** просматривать информацию об опубликованных на сервере открытых ключах пользователей. Такая информация может потребоваться в нескольких случаях:

- для определения даты, когда последний раз была сформирована ключевая пара выбранного пользователя. На основании этих сведений администратор принимает решение о формировании новой ключевой пары для пользователя (по общим правилам работы с криптосистемой следует заново формировать ключевые пары для работы с ЭЦП не реже одного раза в год);
- для получения сведений обо всех версиях открытых ключей пользователей и времени создания этих версий. Эта информация используется администратором, если у пользователя возникают проблемы с постановкой или проверкой ЭЦП. Таким способом можно выяснить, была ли вообще сформирована ключевая пара у данного пользователя и хранится ли на сервере открытый ключ для проверки ЭЦП, поставленной этим пользователем.

Чтобы просмотреть список опубликованных на сервере открытых ключей выбранного пользователя:

1. Запустите программу **Настройка ЭЦП** под именем администратора системы **ЕВФРАТ** (см. п. 1.1).
2. Перейдите на вкладку **Опубликованные ключи** (см. рис. 5).
3. Нажмите на кнопку **Выбор пользователя**. Откроется стандартное диалоговое окно системы **ЕВФРАТ — Выбор пользователя**.
4. Выделите интересующего пользователя и нажмите на кнопку **Выбрать**. На вкладке **Опубликованные ключи** отобразятся фамилия, инициалы пользователя, а также список его открытых ключей, опубликованных на сервере. Список ключей разбит на две колонки: дата, когда ключ был опубликован на сервере, а также версия этого ключа.

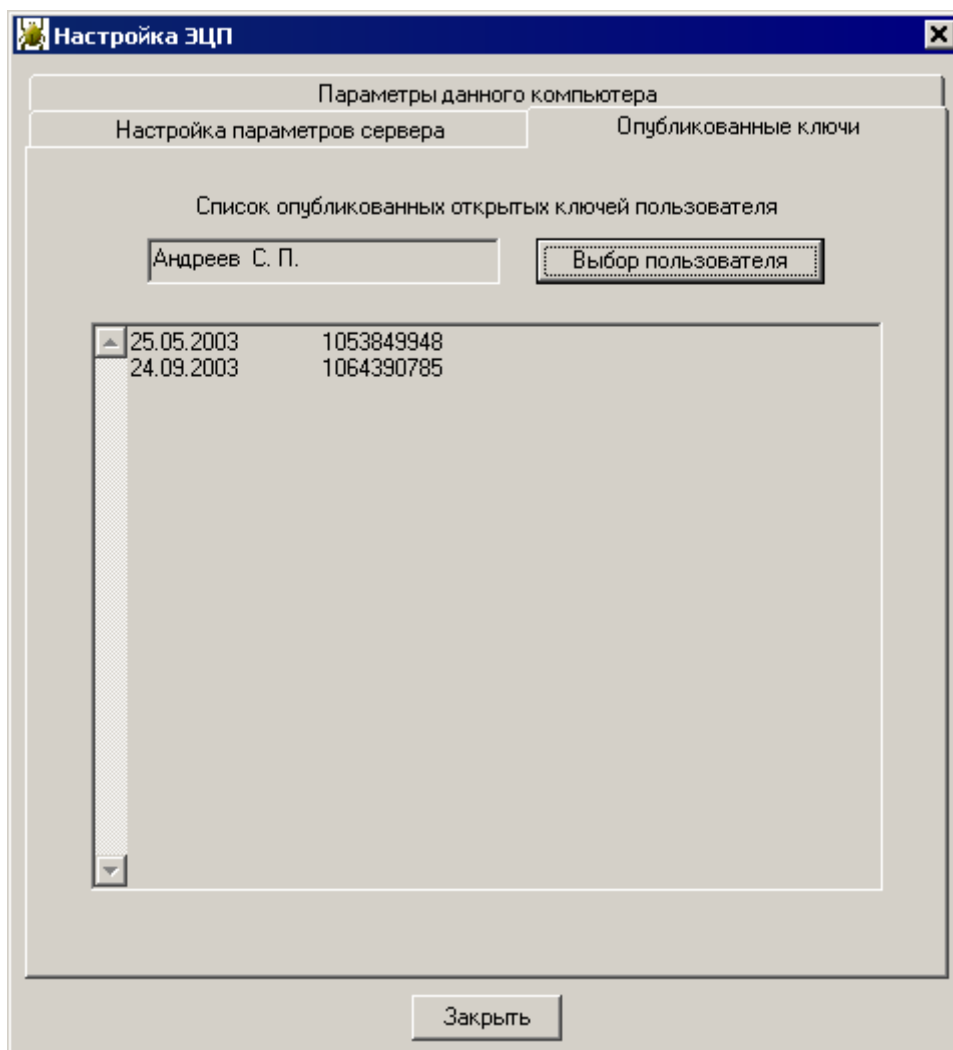


Рис. 5. Просмотр опубликованных на сервере открытых ключей пользователей

1.4. Настройка на уровне пользователя системы ЕВФРАТ

Каждый пользователь, желающий ставить или проверять ЭЦП в электронных документах системы **ЕВФРАТ**, заводит собственную ключевую пару (пару «закрытый-открытый ключ»).

Закрытый ключ используется при формировании ЭЦП. Этот ключ недоступен другим пользователям и хранится на компьютере своего владельца, что обеспечивается криптопровайдером. С другой стороны, для того чтобы остальные пользователи могли проверить ЭЦП пользователя, подписавшего документ, им должен быть доступен его открытый ключ. В этих целях открытые ключи сразу же после формирования ключевой пары автоматически публикуются на сервере ЕВФРАТ.

Ключевые пары для всех пользователей следует формировать после того, как на компьютерах пользователей установлены тождественные параметры криптосистемы. В этих целях пользователи вместо самостоятельной настройки криптосистемы получают описание параметров с сервера ЕВФРАТ.

Настройка криптосистемы на уровне пользователя системы **ЕВФРАТ** проходит в два этапа:

1. Получение описания параметров криптосистемы с сервера.
2. Формирование ключевой пары.

1.4.1. Получение описания параметров криптосистемы с сервера

Для работы криптосистемы необходима тождественность параметров криптосистемы на компьютерах всех пользователей системы **ЕВФРАТ**. В этих целях все пользователи получают описание параметров криптосистемы с сервера ЕВФРАТ.

Чтобы настроить параметры криптосистемы на компьютере пользователя:

1. На компьютере пользователя, для которого следует настроить параметры криптосистемы, запустите программу **Настройка ЭЦП**. При этом подключение к серверу ЕВФРАТ следует осуществить под именем этого пользователя (см. п. 1.1).



Всегда настраивайте параметры криптосистемы для какого-либо пользователя непосредственно с рабочего компьютера этого пользователя

2. Если пользователь еще не настроил свой компьютер после последней публикации описания параметров, появится ряд сообщений, вызванных отсутствием записей о параметрах криптосистемы. Пропустите их, нажимая на кнопку **ОК**. Откроется окно программы **Настройка ЭЦП** (рис. 6).

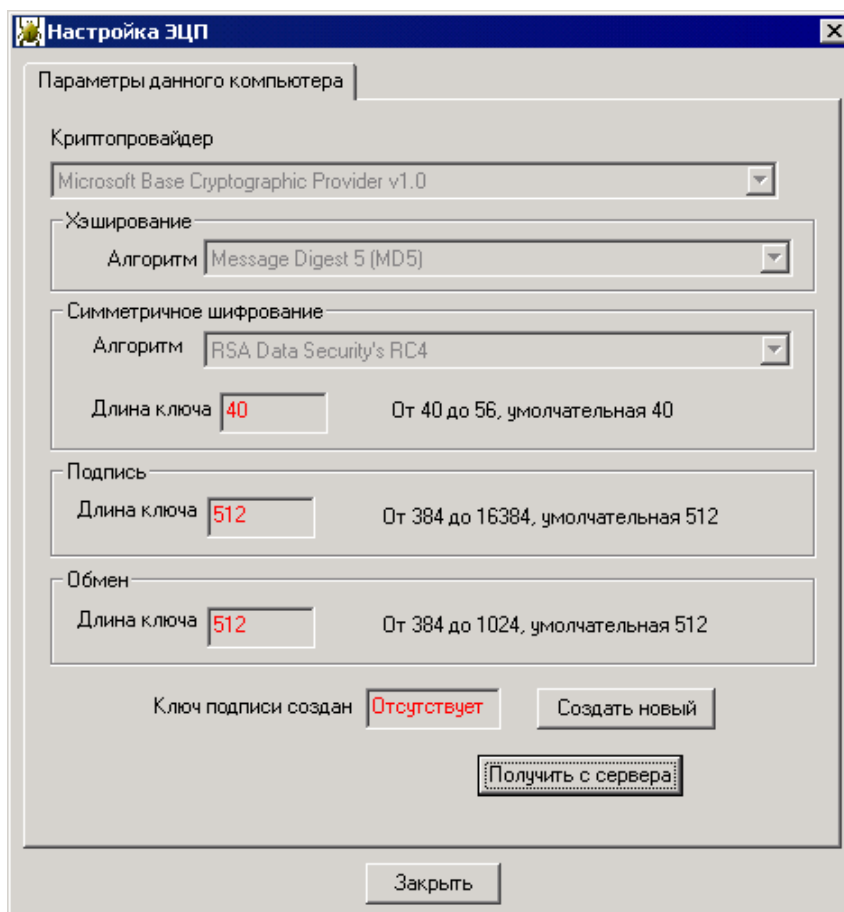


Рис. 6. Настройка параметров компьютера пользователя



Если пользователь не обладает правами администратора, то в открывшемся окне программы **Настройка ЭЦП** расположена только одна вкладка — **Параметры данного компьютера** (см. рис. 6). Если пользователь обладает правами администратора, то окно программы содержит три вкладки (см. рис. 3).

3. На вкладке **Параметры данного компьютера** отображается описание параметров криптосистемы. Чтобы получить описание, нажмите на кнопку **Получить с сервера**.
4. При успешном переносе описания параметров с сервера, нажмите на кнопку **ОК** в появившемся сообщении (рис. 7). После этого цвет значений в полях **Длина ключа** изменится с красного на черный. Это означает, что параметры криптосистемы данного компьютера тождественны параметрам, опубликованным на сервере.



При получении описания также происходит тестирование работы криптосистемы на данном компьютере с параметрами, указанными в описании. Причиной неудачного прохождения теста может являться, например, то, что на компьютере не установлен криптопровайдер, указанный в описании.

5. Приступите к формированию новой ключевой пары согласно п. 1.4.2.

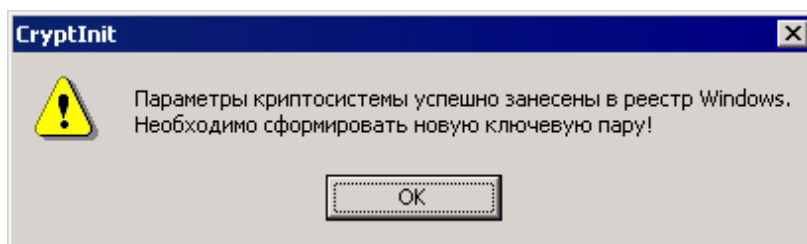


Рис. 7. Сообщение об успешной настройке параметров криптосистемы для данного компьютера

1.4.2. Формирование новой ключевой пары

Чтобы подписывать электронные документы посредством ЭЦП, пользователю системы **ЕВФРАТ** требуется завести собственную ключевую пару (пару «закрытый-открытый ключ»). При этом возможны три основные причины формирования новой ключевой пары:

- первоначальная настройка криптосистемы;
- произошла смена криптопровайдера или параметров шифрования (алгоритмов или длин ключей). То есть на сервере ЕВФРАТ опубликовано новое описание параметров криптосистемы и оно было перенесено на данный компьютер (см. п. 1.4.1);
- плановое обновление ключевой пары. Периодическая замена ключей (не реже одного раза в год) предусматривается общими правилами работы со всеми криптосистемами.

Чтобы сформировать новую ключевую пару:

1. На компьютере пользователя, для которого следует сформировать новую ключевую пару, запустите программу **Настройка ЭЦП**. При этом подключение серверу ЕВФРАТ следует осуществить под именем этого пользователя (см. п. 1.1).
2. На вкладке **Параметры данного компьютера** нажмите на кнопку **Создать новый**.
3. При успешном формировании ключевой пары нажмите на кнопку **ОК** в появившемся сообщении (рис. 8). После этого в поле **Ключ подписи создан** отобразится текущая дата (рис. 9).

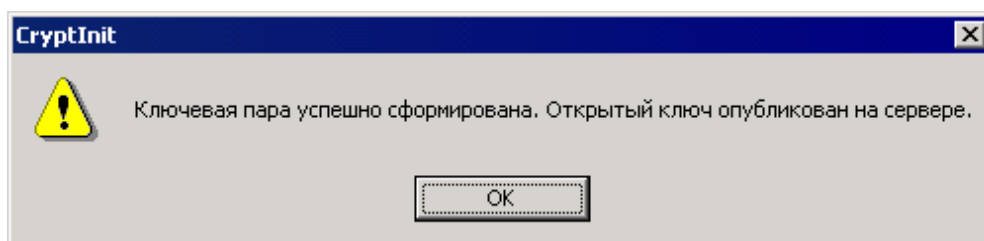


Рис. 8. Сообщение об успешном формировании ключевой пары

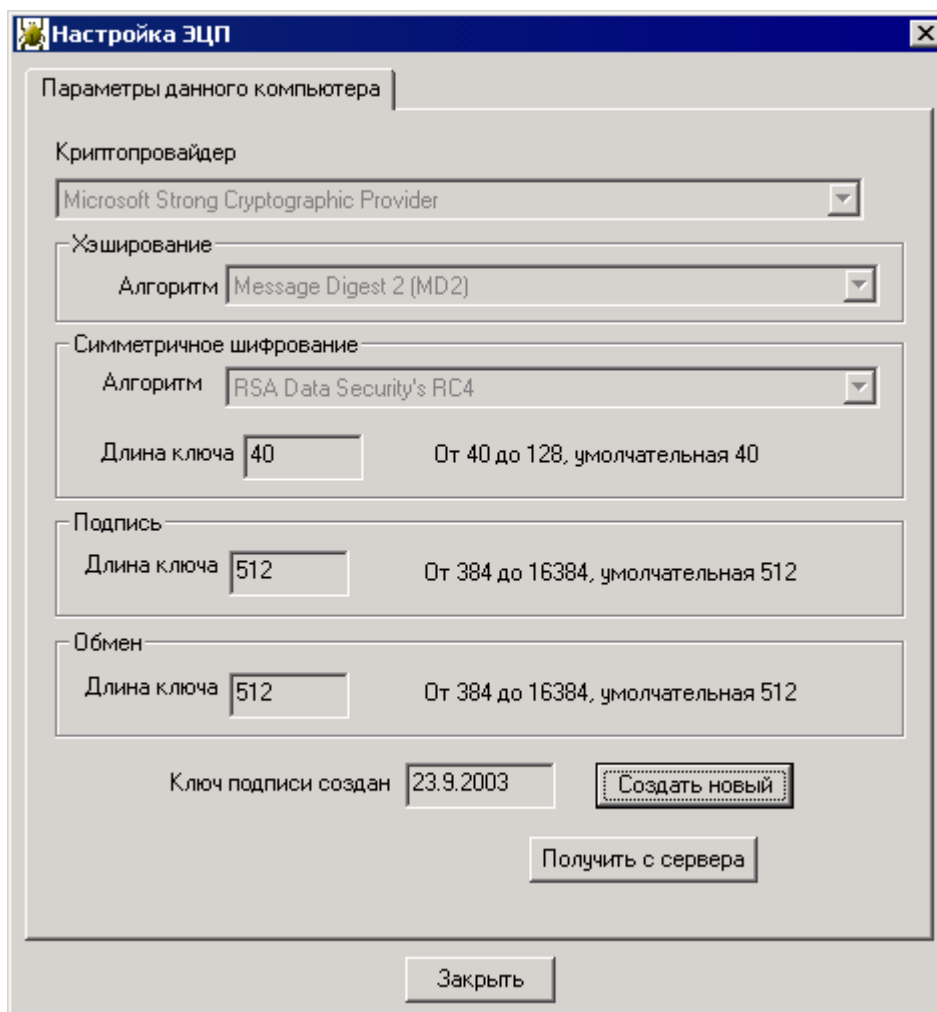


Рис. 9. Успешное формирование новой ключевой пары



Какому-либо пользователю одновременно принадлежит только один закрытый ключ. При создании новой ключевой пары старый закрытый ключ (хранящийся на компьютере пользователя) средствами криптопровайдера заменяется на новый. В свою очередь, старый открытый ключ продолжает храниться на сервере для проверки ЭЦП, поставленных ранее, чем была создана новая ключевая пара (за исключением случаев публикации нового описания параметров криптосистемы, см. п. 1.5.1).



Информация о том, как в системе **ЕВФРАТ** подписывать документы с помощью ЭЦП и проверять ЭЦП, поставленные другими пользователями, приводится в «Учебном пособии для пользователей».

1.5. Некоторые специальные вопросы

В данном разделе рассматриваются некоторые специальные вопросы, которые следует учитывать при работе с криптосистемой, встроенной в **ЕВФРАТ**.

При проверке ЭЦП электронного документа возможны случаи, когда криптосистеме не удаётся определить, верна ЭЦП или неверна. В этом случае результатом диагностики является сообщение: **Не удалось проверить ЭЦП**. Такая ситуация возникает

вследствие ряда причин, для выяснения которых внимательно ознакомьтесь с содержанием данного раздела. Также в разделе рассматриваются другие важные моменты, возникающие при эксплуатации криптосистемы.

1.5.1. Особенности, связанные со сменой криптопровайдера или изменением параметров криптосистемы

Во процессе эксплуатации встроенной в **ЕВФРАТ** криптосистемы может потребоваться сменить используемый криптопровайдер или какие-либо параметры шифрования (алгоритмы, длины ключей). В этом случае следует действовать согласно указанной последовательности операций:

1. Установить новое матобеспечение (новый криптопровайдер) на компьютерах всех пользователей, которые будут подписывать документы или проверять ЭЦП других пользователей (см. п. 1.2).
2. В программе **Настройка ЭЦП** внести изменения в текущие настройки криптосистемы, т. е. создать и опубликовать на сервере новое описание параметров криптосистемы (см. п. 1.3).
3. Всем пользователям, которые будут подписывать документы или проверять ЭЦП других пользователей, создать новые ключевые пары (см. п. 1.4). Это связано с тем, что все ранее заведенные ключи пользователей после смены криптопровайдера становятся неверны.



После смены криптопровайдера всем пользователям следует учитывать, что криптосистема не сможет проверить ЭЦП, поставленные ранее (при старом криптопровайдере) из-за отсутствия открытых ключей на сервере. Отсюда следует, что наиболее подходящее время для смены параметров криптосистемы — это период массовой сдачи документов в электронный архив (с помощью программы **Архивариус** системы **ЕВФРАТ**).

1.5.2. Особенности, связанные с восстановлением базы данных ЕВФРАТ из резервной копии

При восстановлении базы данных **ЕВФРАТ** из резервной копии происходит изменение версии базы данных криптосистемы. То есть имеет место ситуация, аналогичная публикации нового описания параметров криптосистемы на сервере. В этом случае всем пользователям, которые будут подписывать документы или проверять ЭЦП других пользователей, следует создать новые ключевые пары (см. п. 1.4).

При попытке проверить ЭЦП, поставленные до восстановления базы данных **ЕВФРАТ** из резервной копии, криптосистема будет выдавать сообщение: **Не удалось проверить ЭЦП**.

1.5.3. Работа с несколькими серверами

Система **ЕВФРАТ** поддерживает работу с несколькими серверами ЕВФРАТ. Тем не менее, нормальная работа криптосистемы обеспечивается только при подключении всех пользователей к одному из серверов ЕВФРАТ. Такой сервер далее будем называть *домашним сервером криптосистемы*. В качестве него выступает сервер ЕВФРАТ, с

которого все пользователи получили описание параметров криптосистемы. Отсюда следует учитывать следующее: в случае соединения пользователя с сервером ЕВФРАТ, не являющимся при этом домашним сервером криптосистемы, криптосистема не инициализируется, подписывать и проверять ЭЦП в документах невозможно.

1.5.4. ЭЦП и документы Microsoft Word

Когда пользователь системы **ЕВФРАТ** ставит в электронном документе свою ЭЦП, фактически подпись формируется для каждого из присоединенных файлов данного документа. При проверке ЭЦП документа криптосистема делает заключение о подлинности ЭЦП пользователя только в случае, если верны все подписи, сформированные для присоединенных файлов. В связи с этим существует особенность, связанная с использованием ЭЦП в присоединенных файлах формата *Microsoft Word* (файлах с расширением **.doc*).

При сохранении файла в формате *Microsoft Word* в нем могут произойти изменения даже в том случае, если пользователь не вносил правок, связанных с изменением текста (или форматирования). Это относится к особенностям функционирования программы *Microsoft Word*. Так как ЭЦП формируется на основании полного содержимого файла, в этом случае при проверке подпись будет признана неверной, как если бы текст, содержащийся в данном файле, был изменен кем-то из пользователей.

Чтобы избежать этого, следуйте рекомендациям:

- избегайте присоединять к электронному документу, зарегистрированному в системе **ЕВФРАТ**, файлы с расширением **.doc*. Предварительно конвертируйте их в файлы текстового формата (**.txt*) или формата **RTF** (**.rtf*).
- если файл с расширением **.doc* уже присоединен к электронному документу, после подписания ЭЦП избегайте применять по отношению к этому файлу команду **Сохранить** программы *Microsoft Word*. То есть, по возможности, осуществляйте только просмотр данного присоединенного файла.

1.5.5. ЭЦП и архивные документы

Документы, зарегистрированные в системе **ЕВФРАТ**, после выведения из активного документооборота могут быть списаны в электронный архив. Для этих целей служит специальный модуль системы **ЕВФРАТ** — программа **Архивариус**. Архивные документы не подлежат никаким изменениям. Поэтому все ЭЦП, которыми подписан тот или иной электронный документ, уничтожаются при списании документа в электронный архив.

2. Словарь терминов

Закрытый ключ — секретная половина ключевой пары, используемая при шифровании (в частности, для формирования ЭЦП).

Криптография — технология и наука защиты сообщений и данных. Криптография обеспечивает для данных конфиденциальность, целостность, проверку подлинности (объекта и источника) и невозможность отрицания автора.

Криптопровайдер («поставщик криптографических услуг») — специализированный программный или программно-аппаратный модуль, содержащий библиотеку криптографических функций со стандартизованным программным интерфейсом. Криптопровайдер отвечает за реализацию функций интерфейса, а также играет роль хранилища для ключей всех типов.

Несимметричное шифрование — метод шифрования, в котором шифрование и дешифровка текста производятся с помощью разных ключей, составляющих ключевую пару или, другими словами, пару *закрытый-открытый ключ*.

Открытый ключ — несекретная половина ключевой пары, используемая при дешифровке (в частности, для проверки ЭЦП).

Симметричное шифрование — метод шифрования, в котором шифрование и дешифровка текста производятся с помощью одного и того же ключа.

Хэш — см. *хэширование*.

Хэширование — алгоритм преобразования текста (представленного в виде двоичной последовательности) в результате которого по исходному тексту формируется некоторая последовательность фиксированной длины (хэш). Алгоритм хэширования построен таким образом, что любое изменение исходного текста обязательно приводит к изменению хэша. Это позволяет выявить факт изменения текста путем сравнения хэшей, а не самих текстов.

Электронно-цифровая подпись — последовательность символов, позволяющая установить, что исходный текст не был изменен с тех пор, как его подписал (сформировал ЭЦП этого текста) указанный человек. Цифровая подпись есть не что иное, как результат *хэширования* исходных данных, зашифрованный закрытым ключом пользователя.