

ЗАО «СЕРВЕР-ЦЕНТР»

Криптоменеджер

Версия 2.0

Инструкция пользователя.





690106, г.Владивосток, ул.Нерчинская 10, оф. 315
2007 год.

Инструкция пользователя файлового криптоменеджера.

1. Общие сведения

Программа предназначена для шифрования, дешифрования, создания и проверки электронной цифровой подписи (ЭЦП) файлов любых типов в соответствии со стандартами Windows PKI, PKCS#7, X.509 с помощью любого криптопровайдера, работающего в интерфейсе Windows Crypto API 2.0, с использованием стандартных цифровых сертификатов пользователя в Windows.

Результатом работы являются файлы криптографических сообщений формата PKCS#7 текстовой (Base64), либо бинарной кодировки. Программа определяет и создает следующие типы файлов:

-  *.p7e – Файл отдельной ЭЦП
-  *.p7k – Зашифрованный файл
-  *.p7r – Файл с присоединенной ЭЦП
-  *.p7z – Подписанный и зашифрованный файл

Реализованы следующие режимы работы:

- Шифрование файла, в т.ч. многоадресное
- Подпись файла в двух режимах: присоединенном и отсоединенном
- Добавление подписи к подписанному сообщению.
- Последовательные подпись и шифрование файлов (подпись только в присоединенном режиме)

Операции с файлами можно производить не только из окна криптоменеджера, но и прямо из проводника Windows, из контекстного меню правой клавиши мыши.

Сертификаты для подписи и шифрования файлов должны быть установлены в хранилище «Личные» текущего пользователя системы. Другие хранилища сертификатов для данной версии программы недоступны.

2. Системные требования.

- Windows 98 и выше
- Windows NT 4.0 SP5 и выше
- Windows 2000
- Windows XP

- Internet Explorer 5.0 и выше

3. Установка программы.

Процедура установки программы проста. Запустите файл установки cryptosetup.exe с правами администратора. Следуйте подсказкам инсталлятора.

4. Режим контекстного меню

4.1 Шифрование и постановка ЭЦП.

Откройте **Проводник**, выберите нужный файл и щелкните по нему правой кнопкой мыши. Появится контекстное меню. В меню имеются пункты: «**Зашифровать**», «**Подписать**», «**Подписать и зашифровать**». Выберите в контекстном меню нужный пункт, и криптоменеджер начнет требуемую операцию.

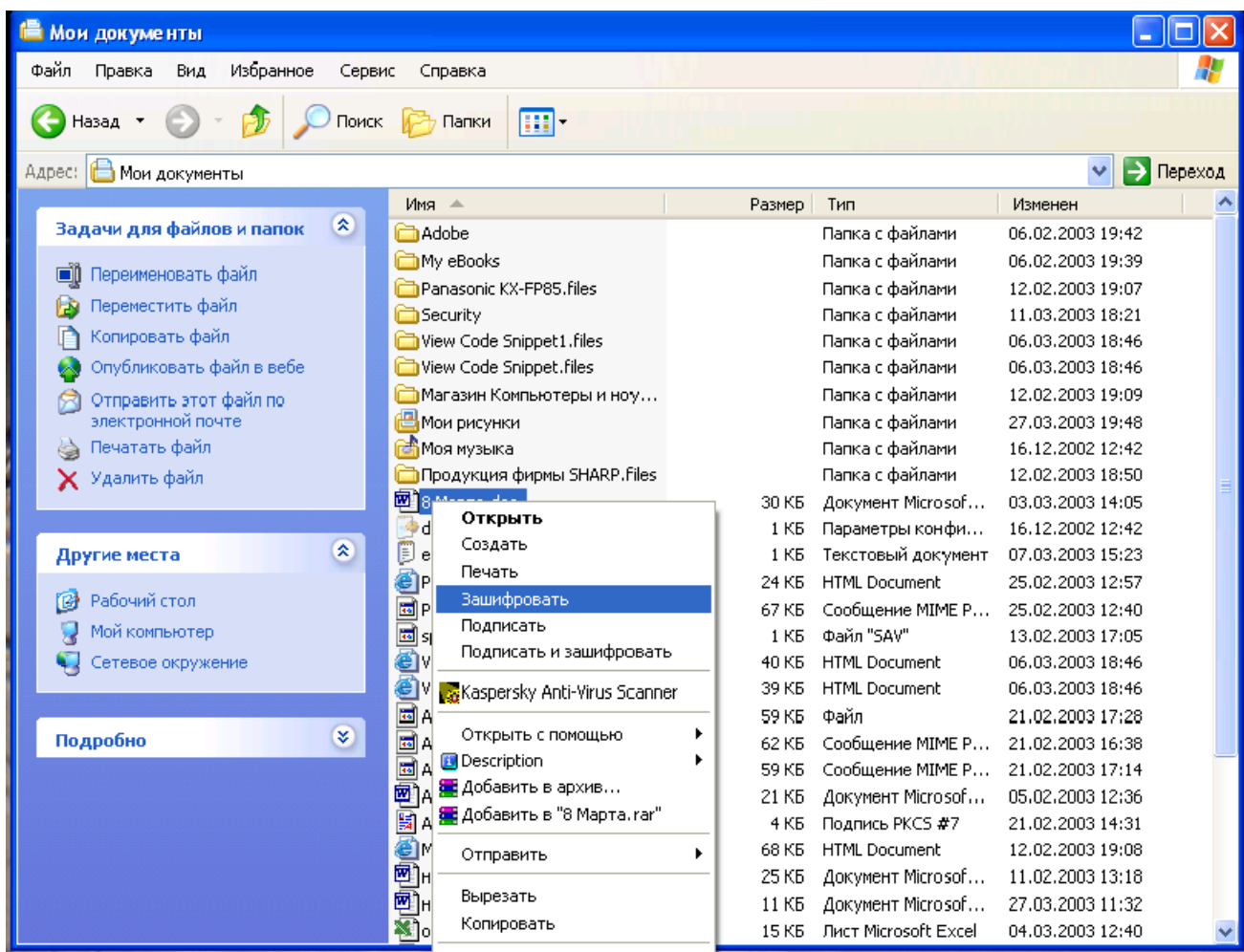


рис.1 Вызов шифрования через контекстное меню проводника.

Если был выбран пункт «**Подписать**», то программа спросит Вас: желаете ли вы присоединить электронно-цифровую подпись к файлу:

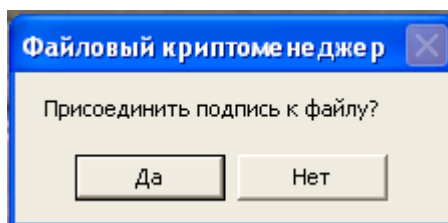


рис.2 Запрос на присоединение ЭЦП к файлу

При положительном ответе криптоменеджер присоединит ЭЦП к содержимому файла, в противном случае он создаст ЭЦП в отдельном файле.

Затем криптоменеджер предложит выбрать сертификаты для создания ЭЦП либо шифрования файлов.

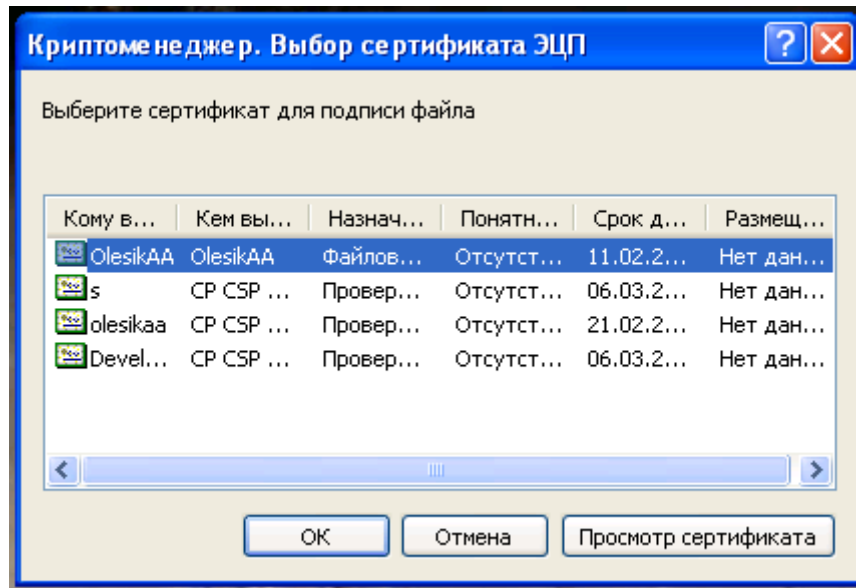


рис.3 Окно выбора сертификатов для создания подписи файла

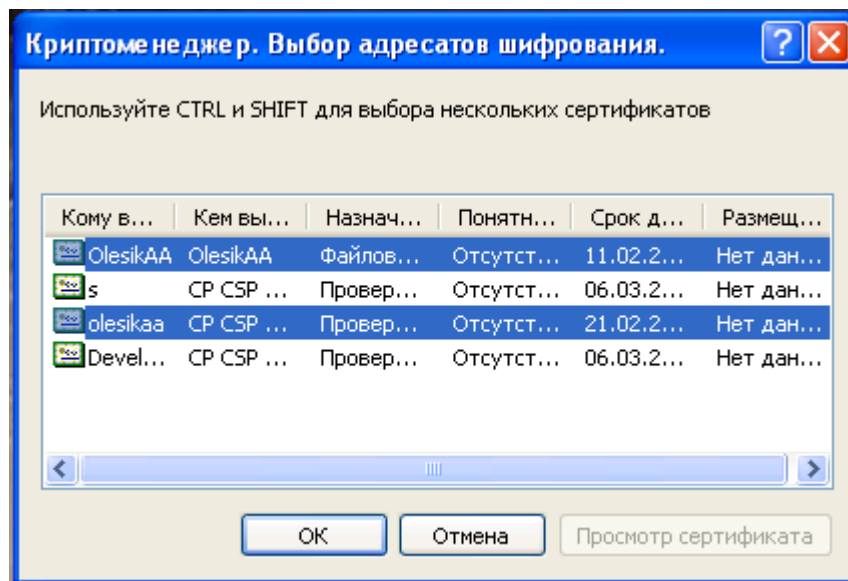


рис.4 Окно выбора сертификатов адресатов шифрования (выбрано 2 сертификата шифрования)

Выберите свой сертификат для создания ЭЦП (требуется наличие закрытого ключа) в первом случае, либо сертификаты тех, кому адресован зашифрованный файл во втором. При выборе сертификатов адресатов шифрования есть возможность назначить несколько адресатов шифрования, при этом файл сможет расшифровать любой из владельцев закрытого ключа хотя бы от одного из назначенных сертификатов. Для выбора нескольких сертификатов необходимо использовать клавиши CTRL или SHIFT аналогично их использованию для выбора нескольких файлов в **Проводнике** (необходимо выбирать сертификаты мышью, удерживая нажатой одну из этих клавиш). Двойным щелчком по нужному пункту, либо

нажатием на клавишу **Просмотр сертификата**, можно более подробно просмотреть свойства интересующего сертификата.

Если был выбран пункт «**Подписать и зашифровать**», то покажется сначала окно выбора сертификатов подписи, а затем сертификатов шифрования.

Выбрав сертификаты, нажмите в окне их выбора кнопку **ОК**. Криптоменеджер передаст управление криптопровайдеру, которым был сгенерирован выбранный Вами сертификат, и он произведет выбранные Вами криптографические операции, возможно выдав несколько окон запросов. После этого появится окно для сохранения файла результата. Оно может выглядеть примерно так:

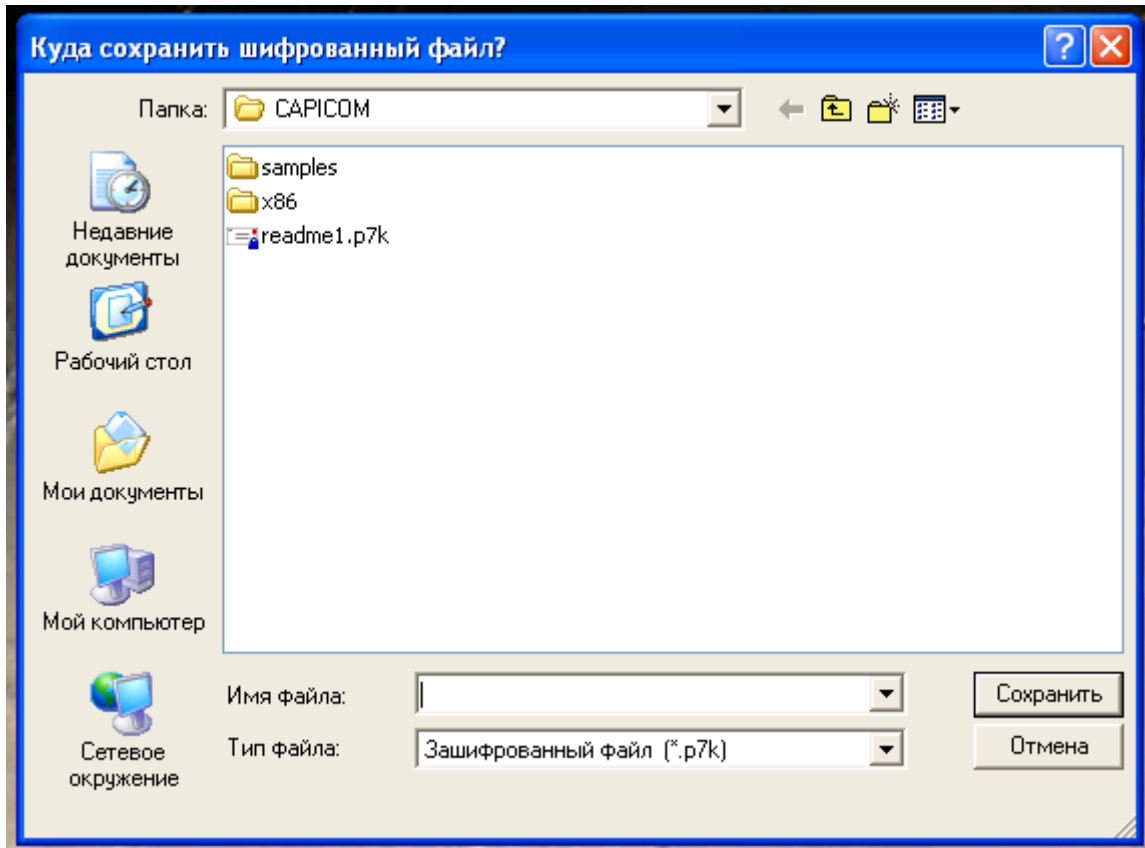


рис.5 Окно сохранения результата работы криптоменеджера

По умолчанию в окне будет установлен тот тип файла, который соответствует полученному результату. Рекомендуется не менять тип файла: при этом для сохраненного файла будут доступны корректные операции дешифрования и проверки ЭЦП из контекстного меню проводника по событию открытия подписанного либо зашифрованного файла. В противном случае эти операции можно будет корректно произвести только из окна Криптоменеджера.

Файл будет сохранен в той кодировке, которая была установлена в окне Криптоменеджера. Подробнее об этом смотрите в гл.5.

4.2 Добавление подписи к уже существующим файлам.

При щелчке правой кнопкой мыши на файлы ЭЦП (*.p7e и *.p7p), в выпадающем контекстном меню вместо пункта «Подписать» появляется пункт «Добавить подпись к существующим». При работе с файлом отдельной подписи программа сначала попросит определить местонахождение файла, которому соответствует эта подпись.

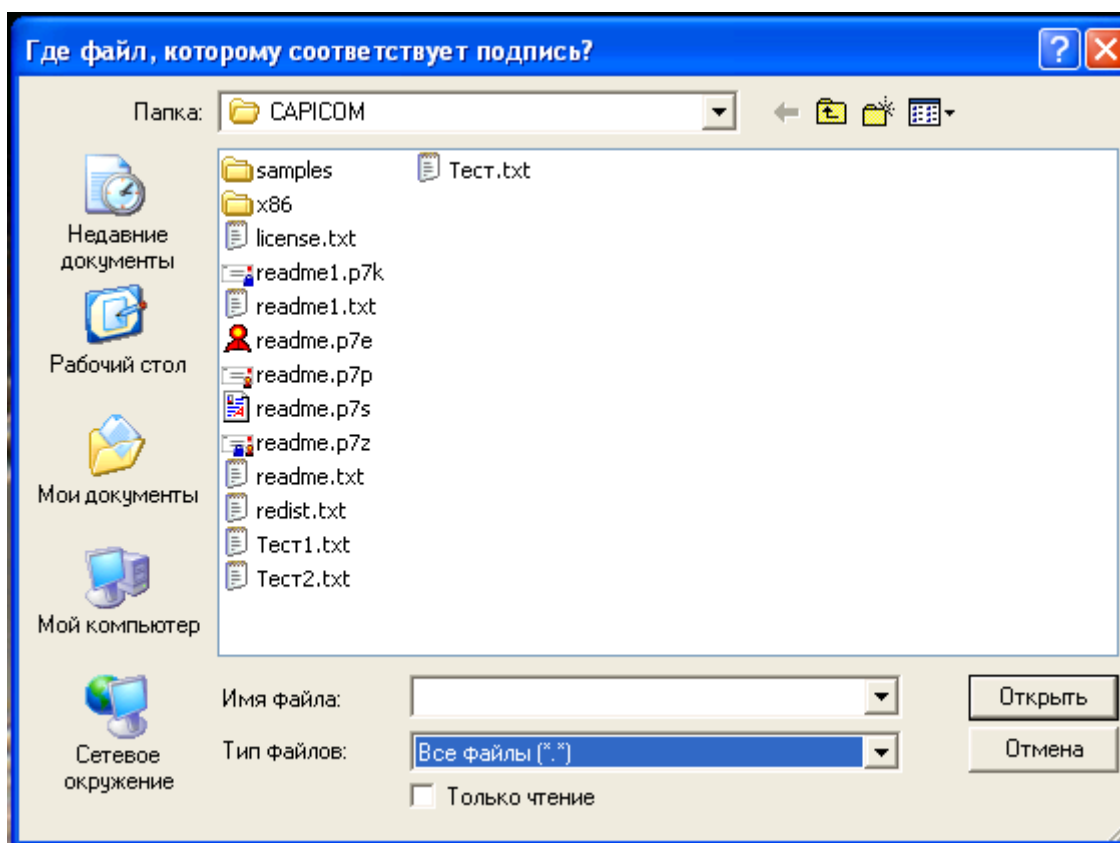


рис.6 Запрос о местонахождении файла, подписанного отдельной ЭЦП

Перед добавлением подписи криптоменеджер проверяет достоверность уже имеющихся ЭЦП и блокирует добавление новой ЭЦП, если старые подписи недостоверны.

4.3 Дешифрование и проверка ЭЦП

В режиме проводника данные операции доступны только для файлов поддерживаемых Криптоменеджером типов (*.p7e, *.p7k, *.p7p, *.p7z). Для этого необходимо в проводнике дважды щелкнуть по таким файлам, как при их открытии.

В случае проверки отдельной ЭЦП Криптоменеджер выдаст запрос о местонахождении подписанного ей файла (см. выше).

Если подпись верна, то высветится следующее окошко:

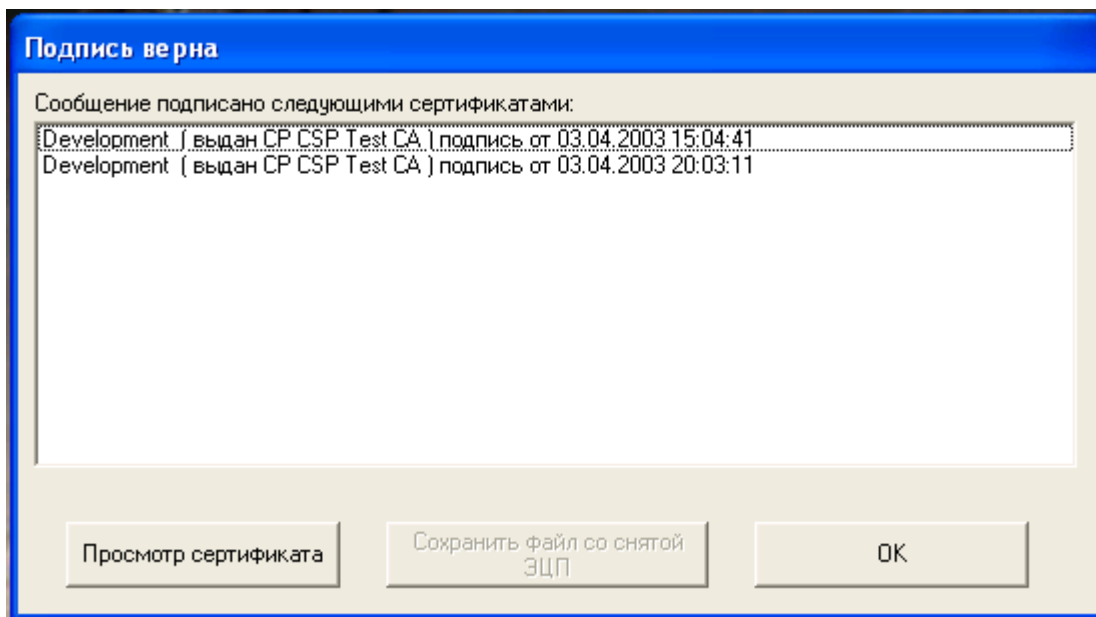


рис.7 Сообщение о подлинности ЭЦП

Двойным щелчком по строчке подписи, либо нажатием кнопки **«Просмотр сертификата»** можно просмотреть сертификаты подписей.

Если проверялся файл с присоединенной подписью, то нажатием на кнопку **«Сохранить файл со снятой ЭЦП»** можно сохранить этот файл в первоначальном виде уже без ЭЦП.

В случае если ЭЦП была неверна, либо не удалось установить подлинность сертификата подписанта, высветится сообщение об ошибке типа такого:

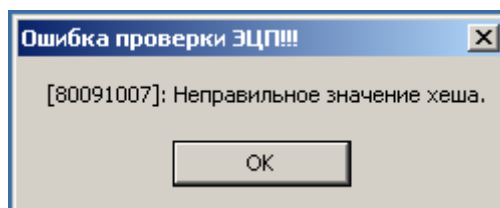


Рис. 5 Сообщение о неудаче проверки ЭЦП

5. Режим окна Криптоменеджера.

5.1 Общий порядок работы.

Откройте файл crypto.exe в установочной директории (C:\Program Files\Crypto). На экране высветится окно режима шифрования и постановки ЭЦП.

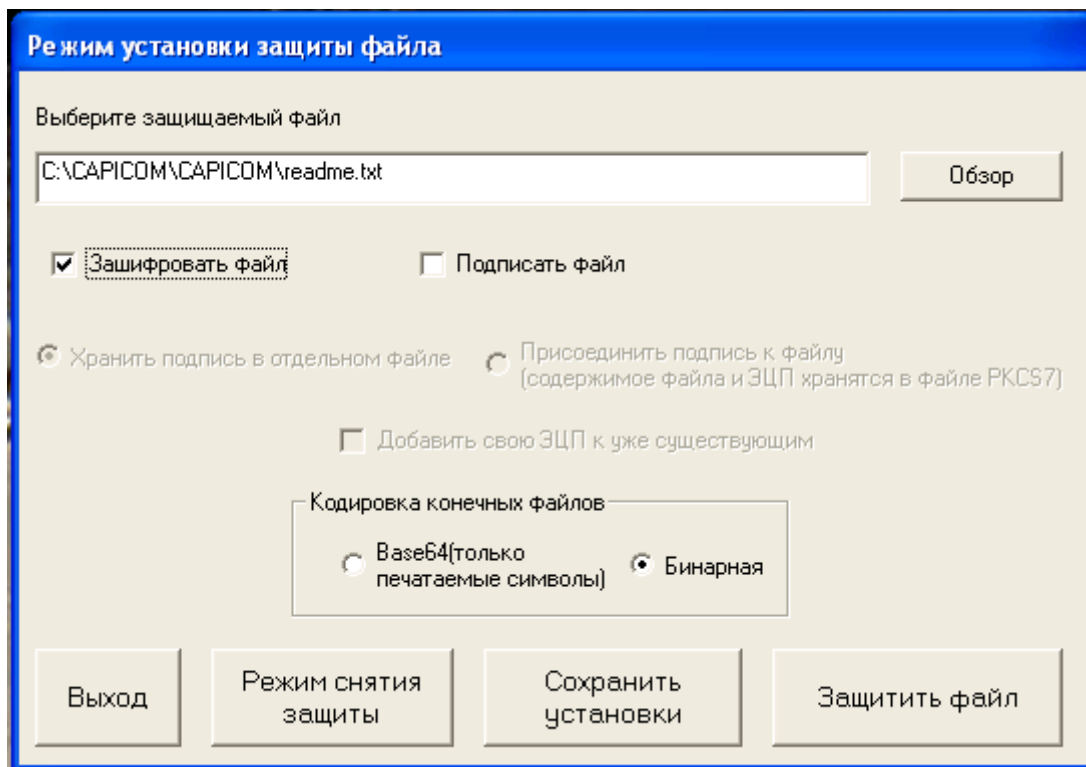


рис.8 Режим шифрования и постановки ЭЦП окна Криптоменеджера

1. Выберите файл, с которым будете работать
2. Установите галочками и переключателями нужный режим работы. Если все необходимые исходные данные введены, то активируется кнопка «**Защитить файл**».
3. Нажмите на кнопку «**Защитить файл**». При этом будут произведены заданные Вами действия.

При нажатии кнопки «**Выход**» происходит закрытие программы. При нажатии кнопки «**Режим снятия защиты**» произойдет переход в окно проверки ЭЦП и дешифрования файлов.

Нажатие на кнопку «**Сохранить установки**» сохранит текущий выбор кодировки конечных файлов по умолчанию. В режиме окна, впрочем, выбором соответствующего пункта можно устанавливать кодировку для любого конкретного файла, однако режим контекстного меню проводника всегда использует сохраненные из окна Криптоменеджера установки по умолчанию.

При передаче конечных файлов по некоторым линиям связи требуется, чтобы они содержали только печатаемые символы. В этом случае требуется выбор кодировки Base64. В остальных случаях рекомендуется выбирать бинарную кодировку. Она хоть и содержит непечатаемые символы, зато занимает заметно меньше места на диске.

При выборе в режиме проверки ЭЦП и дешифрования файла, программа сама предлагает необходимую для них расстановку управляющих элементов.