Инструкция по установке, настройке и использованию ViPNet CryptoFile

Листов 17

ИнфоТеКС Интернет Траст
2023 г.

Оглавление

I. Введение

✓ Документ предназначен для пользователей, осуществляющих установку и настройку **ПО ViPNet CryptoFile** для выполнения над отдельными файлами криптографических операций - шифрования/расшифрования и создания/проверки электронной подписи.

✓ **ViPNet CryptoFile** не является самостоятельным средством шифрования и электронной подписи, для обеспечения выполнения криптографических операций на компьютере должно быть предварительно установлено средство криптографической защиты информации (СКЗИ) ViPNet CSP или КриптоПро CSP.

✓ **С 1 января 2022 года получить квалифицированный сертификат электронной подписи руководителя юридического лица или индивидуального предпринимателя можно только в государственных удостоверяющих центрах (ФНС, Федеральной казначейство, Центральный банк РФ)[1]. В УЦ ИИТ можно получить сертификат на физическое лицо, сотрудника ЮЛ или доверенное лицо ИП.**

✓ В удостоверяющем центре АО «ИнфоТеКС Интернет Траст» (далее – УЦ ИИТ) срок действия ключей и сертификата ЭП установлен равным 1 году.

✓ При необходимости произвести плановую (скорое истечение срока действия ЭП) или внеплановую (изменение учетных данных владельца ЭП, потеря доступа к ключевому носителю, потеря ключевого носителя и т.д.) смену ЭП необходимо повторно прибыть в УЦ ИИТ по согласованию с менеджером АО «ИнфоТеКС Интернет Траст».

✓ Для правильной работы необходимо выполнить все пункты данного руководства в указанной последовательности.

✓ **Необходимо обращать особое внимание на примечания помеченные знаком .**

Внимание! Вид окон может отличаться в зависимости от используемой операционной системы.
В примерах использовалась операционная система Windows 10.

Всю необходимую документацию по услугам нашей компании вы можете загрузить на нашем сайте www.iitrust.ru раздел «Поддержка», кнопка «Пользовательская документация»

[1] Согласно изменениям в 63-ФЗ «Об электронной подписи».

II. Получение и установка ViPNet CryptoFile

1. Загрузите дистрибутив ПО ViPNet CryptoFile по ссылке: https://iitrust.ru/downloads/cryptofile/vipnet_cryptofile.zip
2. Запустите установку ViPNet CryptoFile из файла **ViPNet_CryptoFile_X.X_(X.XXXXX).exe**. Далее следуйте инструкциям мастера установки.

➡ ***Лицензия на использование ViPNet CryptoFile не требуется при совместном использовании ПО ViPNet CryptoFile с криптопровайдером ViPNet CSP, в том числе входящим в состав ViPNet Client, ViPNet PKI Client. Также ViPNet CryptoFile может работать совместно с криптопровайдерами сторонних производителей в рамках демонстрационного режима (в течение 14 дней).***

III. Настройка ViPNet CryptoFile

A. *Добавление электронной подписи*

1. Запустите ***ViPNet CryptoFile***. Для того, чтобы добавить ваш сертификат перейдите на вкладку ***«Файл»***, затем выберите ***«Настройки…»***. В разделе ***«Подпись - Использовать сертификат»*** нажмите на кнопку ***«Задать»***, из списка сертификатов укажите необходимый сертификат, полученный в УЦ ИИТ, и нажмите ***«ОК»*** (Рисунки 4-5). Если в дальнейшем необходимо сменить сертификат для подписи, нажмите ***«Изменить»*** и выберите новый.

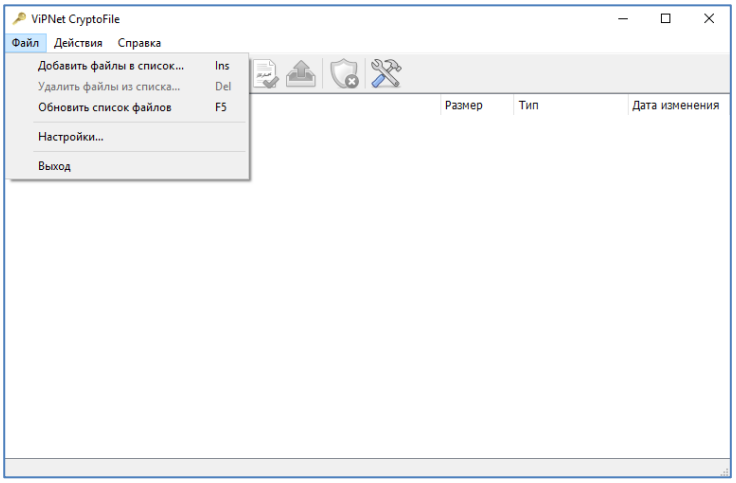

Рисунок 4

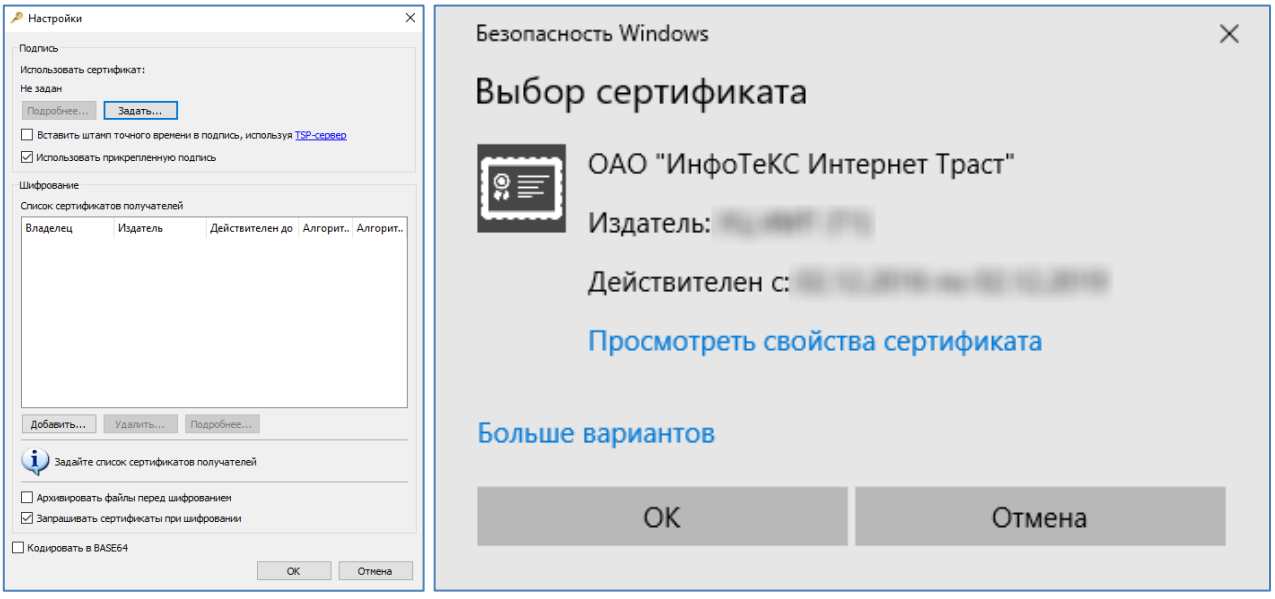

Рисунок 5

Б. Добавление метки штампа времени

Для обеспечения возможности проверки действительности электронной подписи в электронном документе в течение длительного времени используется **метка доверенного времени**, которая, в соответствии с 63-ФЗ, представляет из себя достоверную информацию в электронной форме **о дате и времени подписания электронного документа электронной подписью**, создаваемую и проверяемую доверенной третьей стороной, удостоверяющим центром или оператором информационной системы и полученную в момент подписания электронного документа электронной подписью в установленном уполномоченным федеральным органом порядке.

Для того, чтобы добавить метку штампа времени запустите ***ViPNet CryptoFile***, нажмите на вкладку ***«Файл»***, затем выберите ***«Настройки…»***. В разделе ***«Подпись - Использовать сертификат»*** установите галку ***Вставить штамп точного времени на подпись, используя TSP-сервер***, укажите адрес *http://cades.iitrust.ru:8777/tsp*[2] и нажмите на кнопку ***«ОК»*** (Рисунки 6-8).

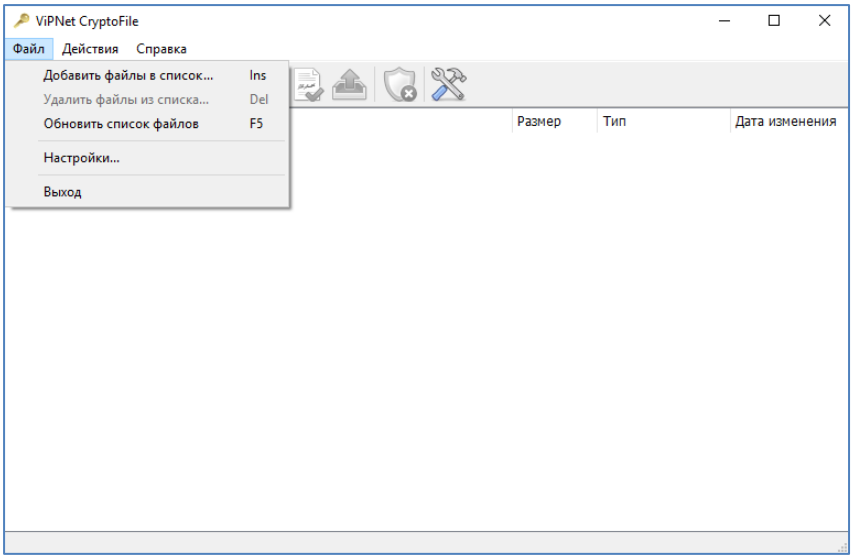

Рисунок 6

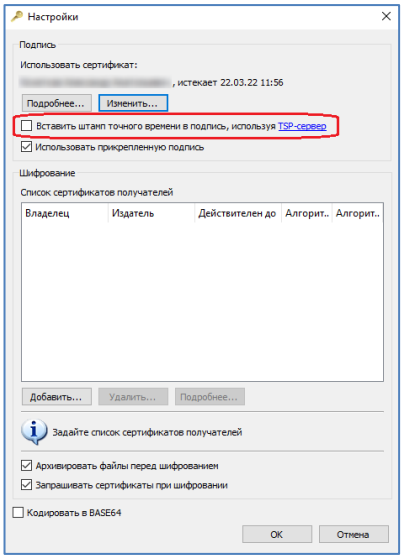

Рисунок 7

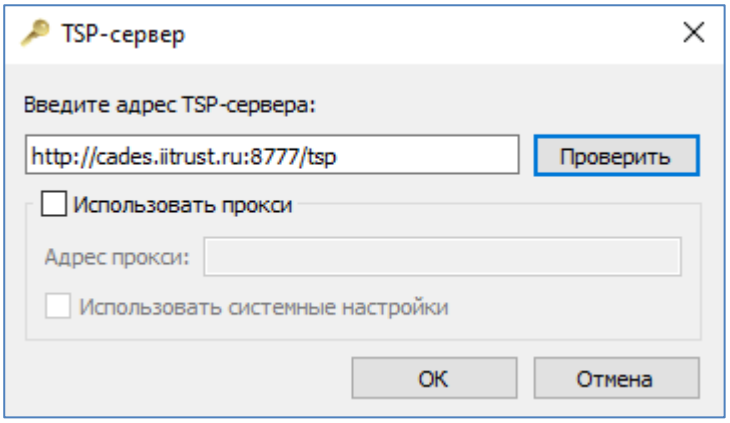

Рисунок 8

На портале уполномоченного федерального органа в области использования электронной подписи вы можете самостоятельно осуществить проверку подлинности и соответствие на квалифицированность сертификата электронной подписи согласно №63-ФЗ от 06.04.2011 «Об электронной подписи», а также проверку присоединенной и отсоединенной электронной подписи, включая штамп времени. Процесс

[2] Можно указать и другие адреса, например, адрес TSP-сервера УЦ ФНС http://pki.tax.gov.ru/tsp/tsp.srf

проверки ЭП описан в инструкции: **Проверка на подтверждение подлинности квалифицированной электронной подписи**

B. Настройте список сертификатов получателей зашифрованных файлов

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если вам необходимо зашифровать файлы.

1. Для настройки списка сертификатов получателей необходимо сначала установить сертификаты получателей в хранилище сертификатов[3].
2. Откройте сертификат получателя двойным щелчком левой клавиши мыши и нажмите клавишу ***«Установить сертификат»*** (Рисунок 9).

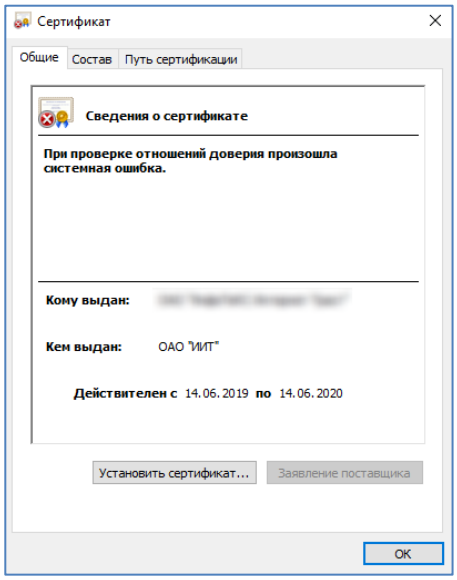

Рисунок 9

3. В появившемся окне ***«Мастера импорта сертификатов»*** (Рисунок 10) нажмите клавишу ***«Далее»*** и в следующем окне выберите опцию ***«Поместить все сертификаты в следующее хранилище»***, затем нажмите кнопку ***«Обзор»*** (Рисунок 10).

[3] Предварительно необходимо получить сертификат ключа проверки ЭП получателя в электронном виде в формате **xxxxxx.cer** и сохранить его на своем компьютере.

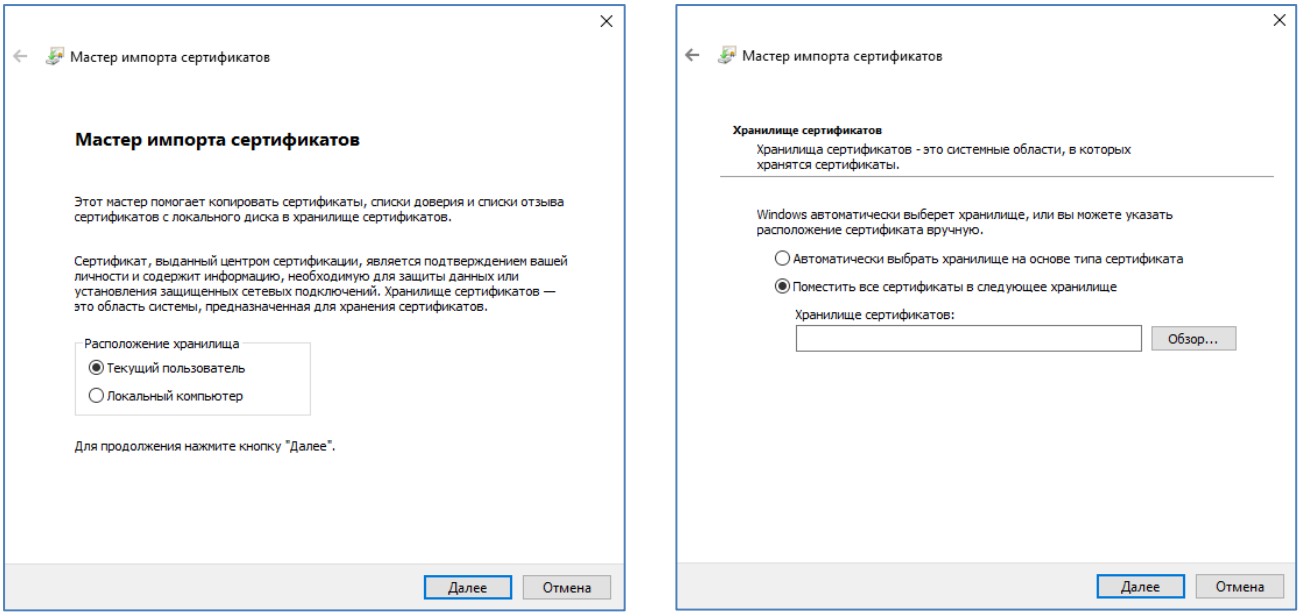

Рисунок 10

4. Выберите хранилище сертификатов ***«Другие пользователи»*** и нажмите ***«ОК»***. В окне Мастера импорта сертификатов нажмите клавишу ***«Далее»***. Завершите работу Мастера импорта сертификатов путем нажатия клавиши ***«Готово»*** (Рисунок 11).

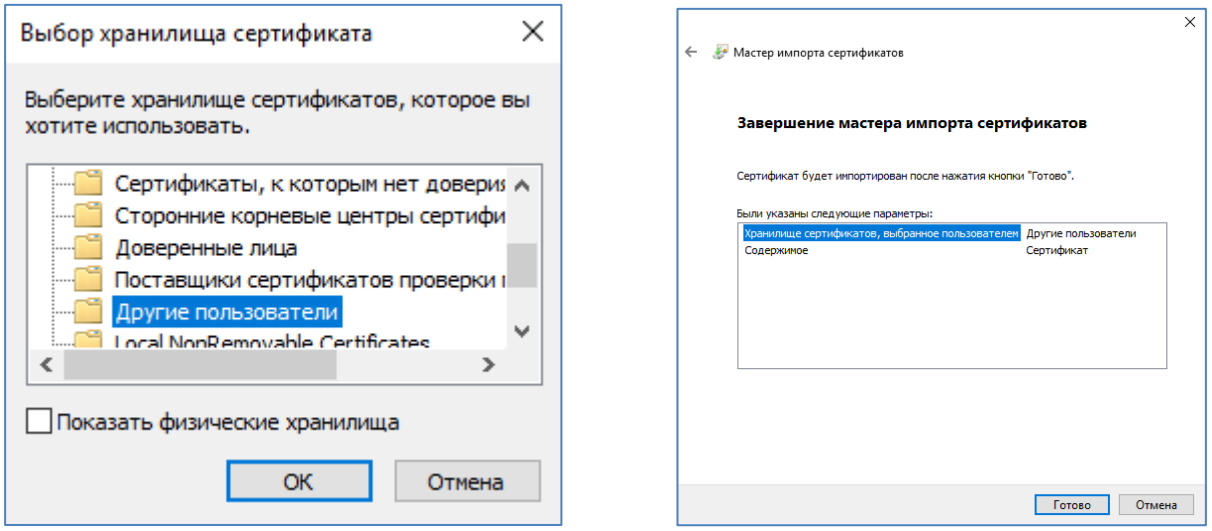

Рисунок 11

5. При успешном завершении работы ***«Мастер импорта сертификатов»*** выдаст соответствующее уведомление. Нажмите на кнопку ***«ОК»*** (Рисунок 12).

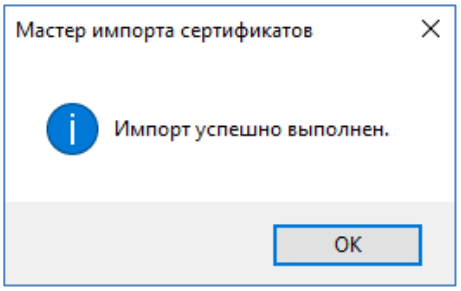

Рисунок 12

Г. Добавление сертификатов получателей в список

1. Запустите ***ViPNet CryptoFile***. Для того, чтобы добавить Ваш сертификат перейдите на вкладку ***«Файл»***, затем выберите ***«Настройки…»***, в разделе ***«Шифрование»*** нажмите клавишу ***«Добавить»*** (Рисунок 13).

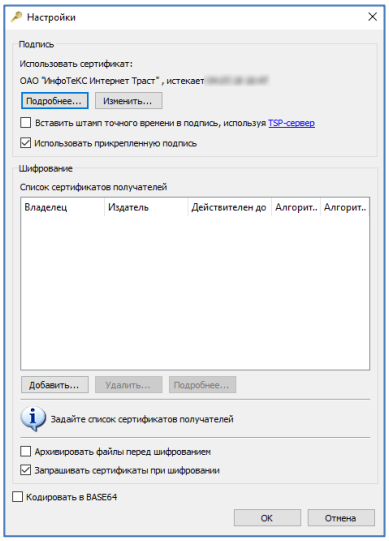

Рисунок 13

2. В окне Выбора сертификатов укажите необходимый сертификат получателя и нажмите ***«ОК»*** (Рисунок 14).

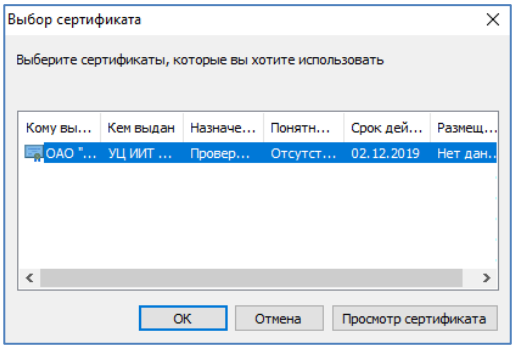

Рисунок 14

3. Выбранный сертификат получателя появится в списке (Рисунок 15)

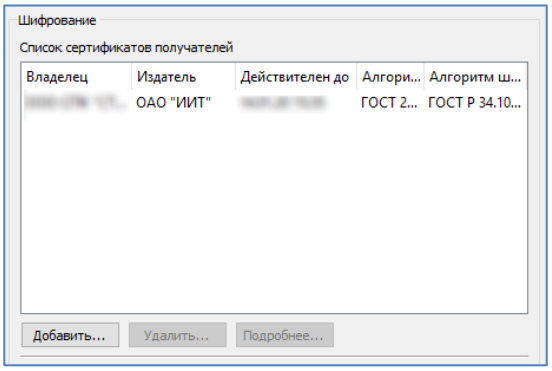

Рисунок 15

4. На этом настройка списка сертификатов получателей завершается. При необходимости включения в список сертификатов иных получателей, повторите действия.

IV. Работа с ViPNet CryptoFile

Работу с ViPNet CryptoFile можно условно разделить на следующие основные сценарии:

А. Электронная подпись файлов.
Б. Электронная подпись файлов двумя ЭП.
В. Проверка электронной подписи в полученных файлах.
Г. Подписывание и шифрование файлов.
Д. Расшифрование и проверка подписи в полученных зашифрованных файлах.

А. Электронная подпись файлов.

В окне ***ViPNet CryptoFile*** нажмите на кнопку ***«Добавить файлы в список»***, либо на вкладку ***«Файл» -> «Добавить файлы в список»***, в окне выберите файл, который необходимо подписать, и нажмите ***«Открыть»*** (Рисунок 16).

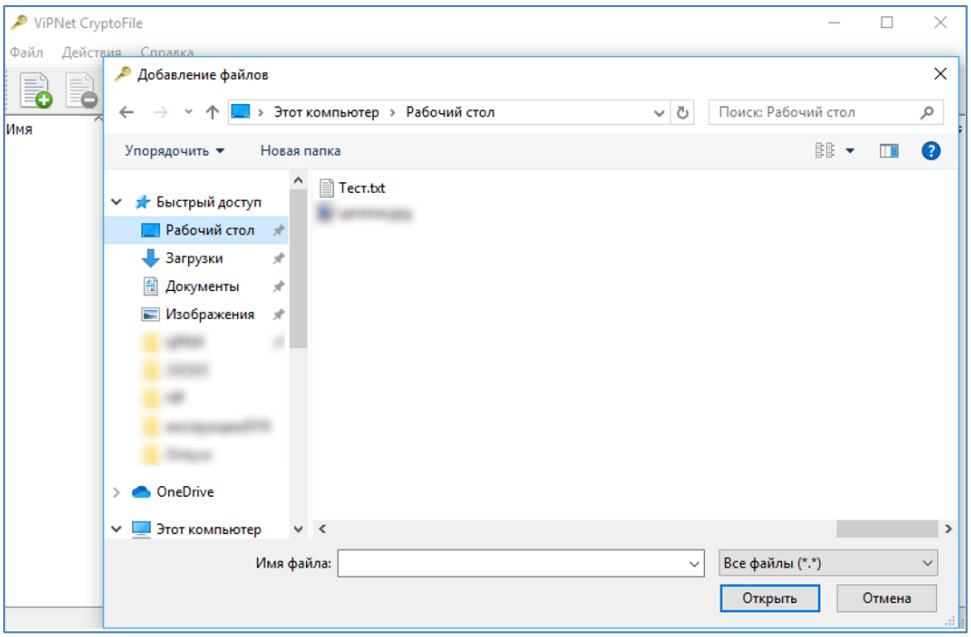

Рисунок 16

Выделите в списке необходимый файл, и нажмите на кнопку ***«Подписать»***, либо нажмите на файл правой кнопкой мыши и выберите пункт ***«Подписать»*** (Рисунок 17).

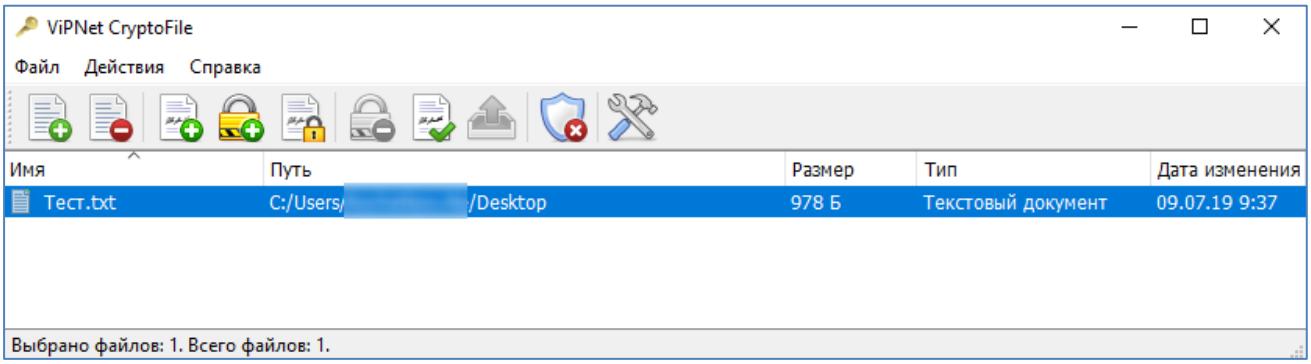

Рисунок 17

При необходимости введите ПИН-код к устройству хранения ключей или пароль и нажмите ***«ОК»***. Убедитесь в успешном завершении операции и нажмите ***«Закрыть»*** (Рисунок 18).

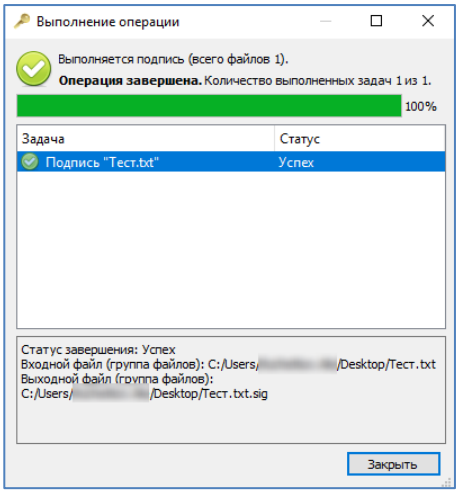

Рисунок 18

Согласитесь с предложением добавить подписанный файл к основному списку (Рисунок 19). В результате подписанный файл ***.sig*** будет сохранен в папке, в которой хранится и исходный файл документа, а также появится в списке ViPNet CryptoFile (Рисунок 19).

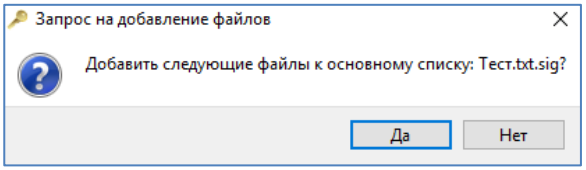

Рисунок 19

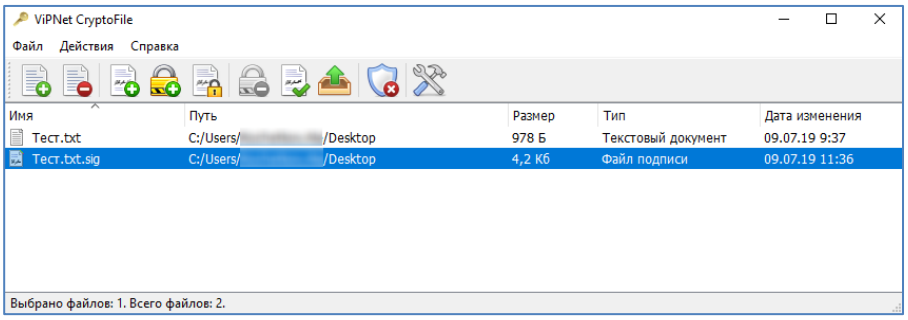

Рисунок 20

В случае необходимости формирования открепленной электронной подписи, с получением файла открепленной подписи *.sig, в окне ***«Настройки»*** необходимо снять флаг ***«Использовать прикрепленную подпись»*** и нажать «***ОК»*** (Рисунок 21).

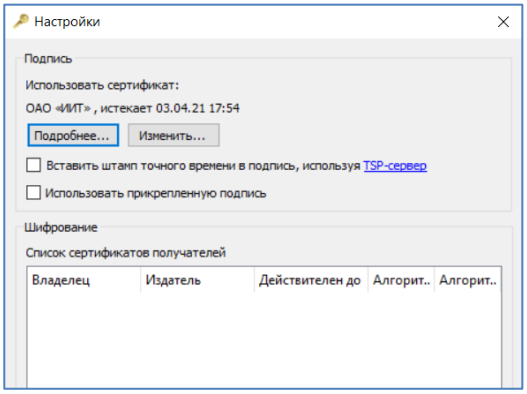

Рисунок 21

Б. Электронная подпись файлов двумя ЭП.

В случае необходимости подписать файл второй электронной подписью, необходимо зайти в настройки ViPNet Cryptofile, перейти на вкладку ***«Файл»***, затем выбрать ***«Настройки…»***. В разделе ***«Подпись - Использовать сертификат»*** нажать на кнопку ***«Изменить…»*** и из списка сертификатов указать другой сертификат (Рисунки 4-5).

В случае необходимости формирования прикрепленной электронной подписи выбрать **ПОДПИСАННЫЙ ФАЙЛ**, в данном примере **Тест.txt.sig** и нажать на кнопку ***«Подписать»***. В результате новый подписанный файл ****.sig*** будет сохранен в папке, в которой хранится и исходный файл документа, а также появится в списке ViPNet CryproFile. В нашем примере **Тест.txt.sig.sig** (Рисунок 22). Для того чтобы убедиться в том, что данный файл подписан двумя электронными подписями, проверьте его. Подробное описание приводится в пункте В на странице 14.

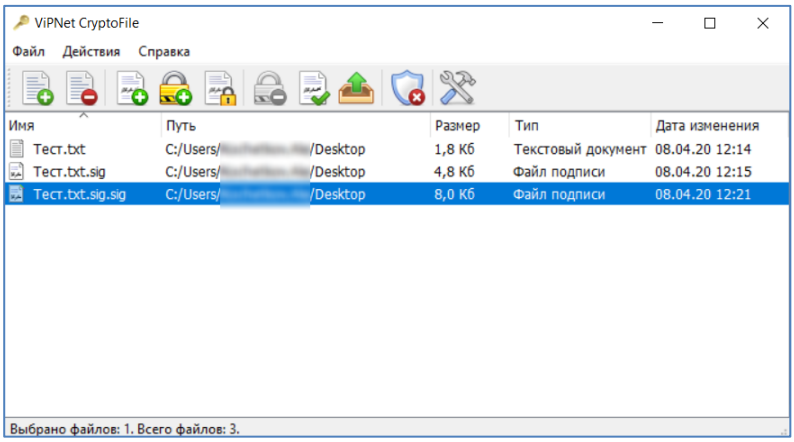

Рисунок 22

В случае необходимости формирования открепленной электронной подписи необходимо проверить настройки ViPNet Cryptofile (Рисунок 21), затем указать **ИСХОДНЫЙ ФАЙЛ**, в данном примере **Тест.txt** и нажать на кнопку ***«Подписать»***. Появится информационное окно ***«Запрос действия с существующим файлом»***. Необходимо нажать на кнопку ***«Добавить подпись»*** (Рисунок 23).

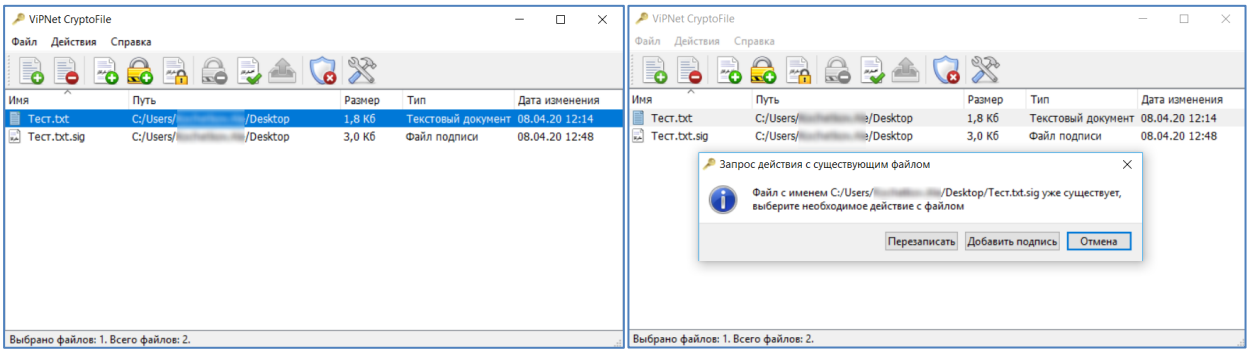

Рисунок 23

В результате новый подписанный файл ****.sig*** будет сохранен в папке, в которой хранится и исходный файл документа, а также появится в списке ViPNet CryproFile. В нашем примере **Тест.txt.sig** (Рисунок 24). Для того чтобы убедиться в том, что данный файл подписан двумя электронными подписями, проверьте его. Подробное описание приводится в пункте В на странице 14.

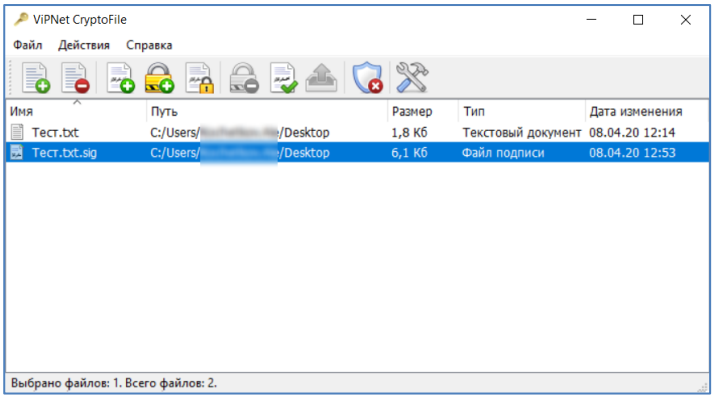

Рисунок 24

В. Проверка электронной подписи в полученных файлах

При получении подписанного ЭП файла (файл в формате *.sig) добавьте, по аналогии с предыдущим пунктом (Рисунок 16), файл подписи *.sig в список ViPNet CryptoFile, выберите его в окне ViPNet CryptoFile и нажмите ***«Проверить подпись»*** (названия кнопок отображаются при наведении курсора) (Рисунок 25).

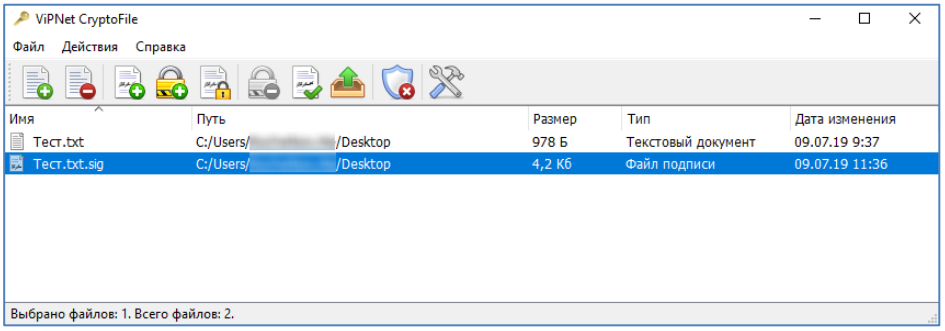

Рисунок 25

Обратите внимание! При проверке откреплённой подписи сам целевой файл должен лежать в одной папке с файлом подписи *.sig и иметь то же название, что и файл подписи до расширения .sig. Другими словами, при получении файлов сохраняйте их в одной папке и ничего не меняйте, как в названиях файлов, так и в их содержимом.

Убедитесь в правильности ЭП и действительности сертификата, и закройте окно проверки ЭП (Рисунок 26).

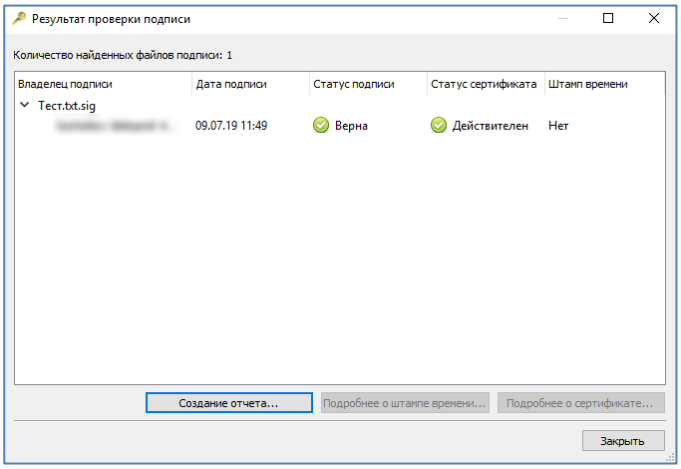

Рисунок 26

Если после проверки ЭП в полученном документе (если прикрепленная подпись) Вам необходимо получить исходный файл для последующей обработки, при проверке подписи вместо ***«Проверить***

подпись» выбирайте операцию ***«Извлечь и проверить подпись»***. В этом случае после выполнения операции проверки ЭП исходный (извлеченный) файл будет сохранен в той же папке, что и подписанный файл.

Г. Электронная подпись и шифрование файлов.

В окне ViPNet CryptoFile нажмите кнопку ***«Добавить файлы в список»***, в диалоговом окне выберите файл, который необходимо подписать и зашифровать, и нажмите ***«Открыть»***. Выделите в списке ViPNet CryptoFile появившийся файл, нажмите ***«Подписать и зашифровать»*** (Рисунок 27).

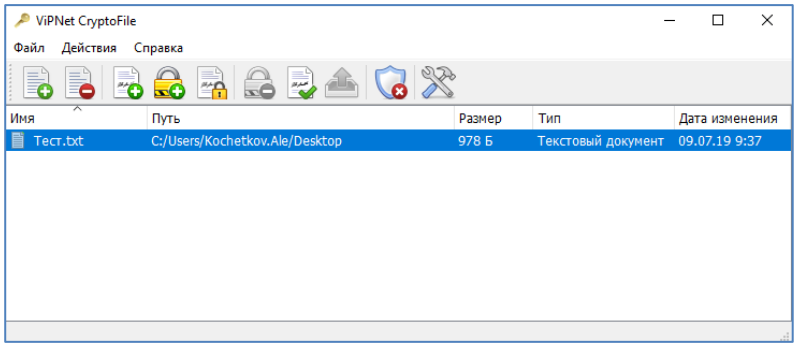

Рисунок 27

Выберите сертификаты получателей зашифрованного файла и нажмите ***«ОК»***.
В случае необходимости архивирования файлов перед шифрованием, установите флаг ***«Архивировать файлы перед шифрованием»*** (Рисунок 28).

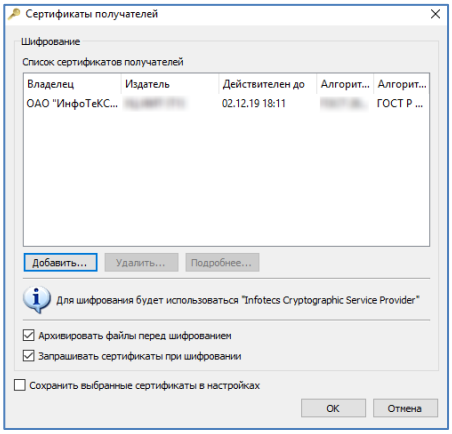

Рисунок 28

При необходимости введите ПИН-код или пароль. Убедитесь в успешном завершении всех операций и нажмите ***«Закрыть»*** (Рисунок 29).

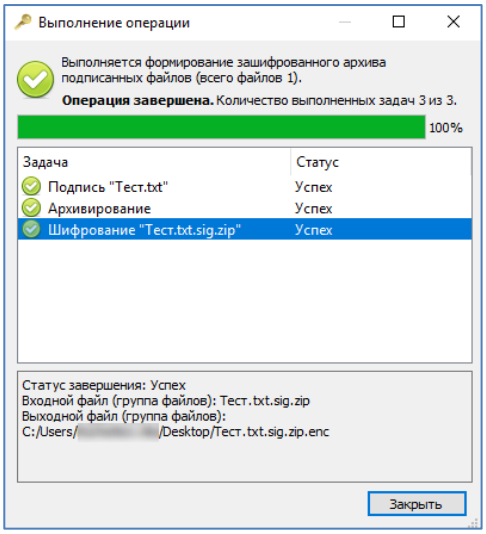

Рисунок 29

Согласитесь с предложением добавить подписанный файл к основному списку. В результате подписанный файл ***.sig.enc** (или ***.sig.zip.enc**, в случае архивирования файла перед шифрованием) будет сохранен в папке, в которой хранится и исходный файл документа, а также появится в списке ViPNet CryptoFile (Рисунок 30).

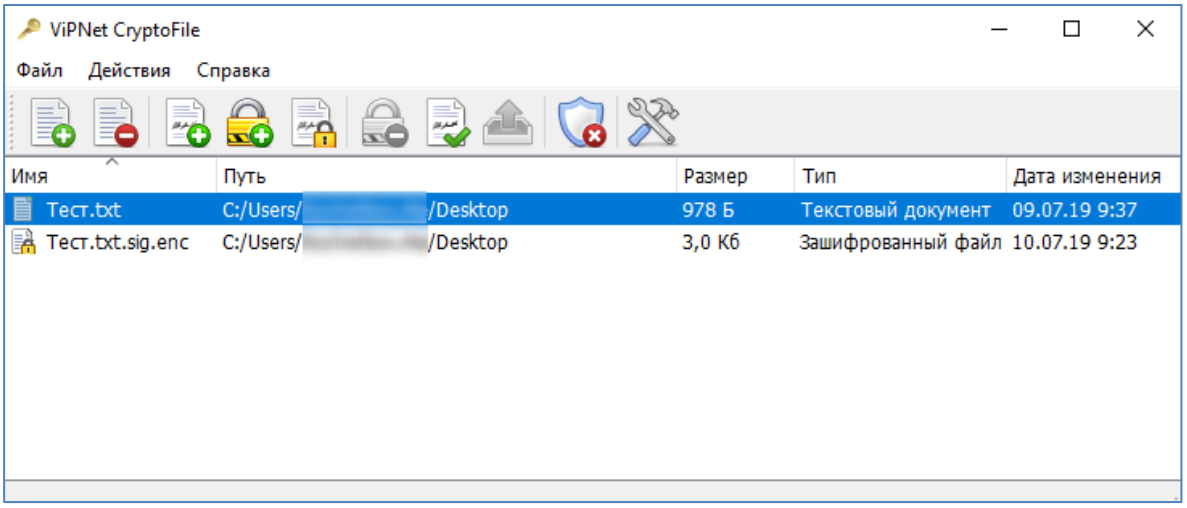

Рисунок 30

Д. Расшифрование и проверка электронной подписи в полученных файлах.

При получении зашифрованного и подписанного ЭП отправителя файла (файл в формате ***.sig.[zip].enc**) добавьте его в список ViPNet CryptoFile, выберите этот файл в окне ViPNet CryptoFile и нажмите на кнопку ***«Извлечь и проверить подпись»*** (названия кнопок отображаются при наведении курсора) (Рисунок 31).

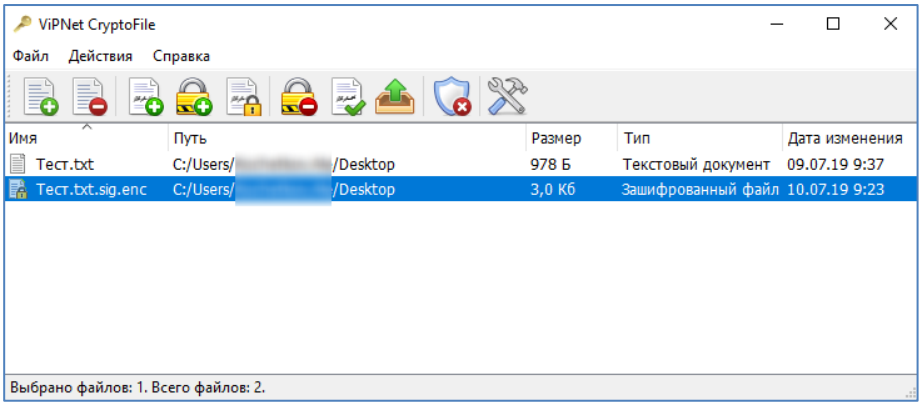

Рисунок 31

Убедитесь в успешном завершении операции и нажмите ***«Закрыть»*** (Рисунок 32).

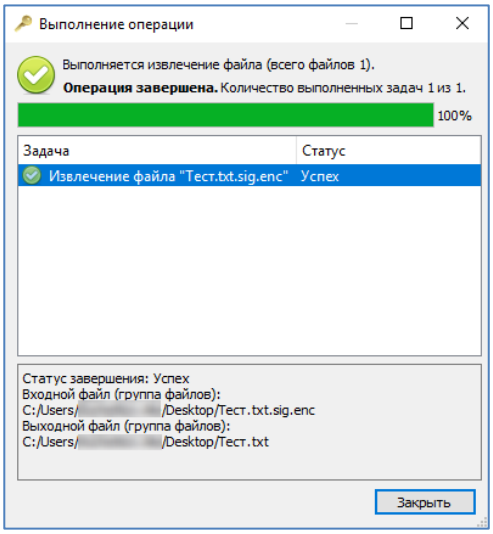

Рисунок 32

Убедитесь в правильности ЭП и действительности сертификата, и закройте окно проверки ЭП (Рисунок 33).

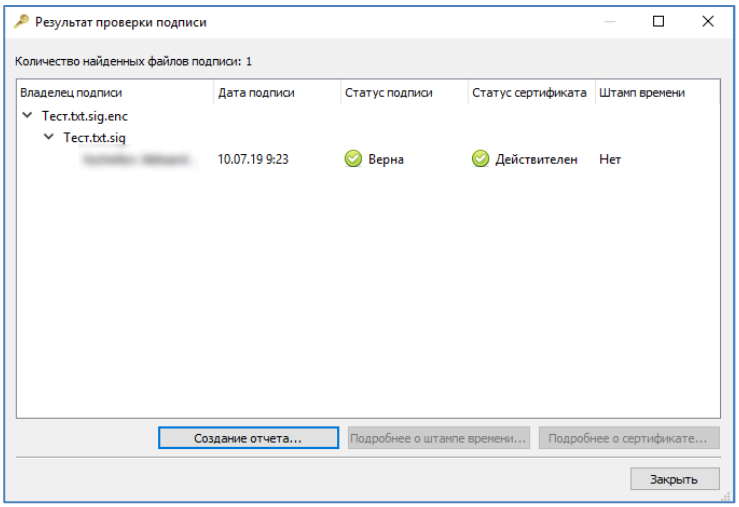

Рисунок 33

На этом процедура расшифрования и проверки подписи файла завершена. Расшифрованный (извлеченный) файл будет сохранен в той же папке, что и зашифрованный файл.

Если ViPNet CryptoFile настроен, то все доступные операции можно выполнить, не запуская ПО, нажав правой кнопкой мыши на оперируемый файл и выбрав необходимые пункты в контекстном меню «ViPNet CryptoFile» Проводника (Рисунок 34).

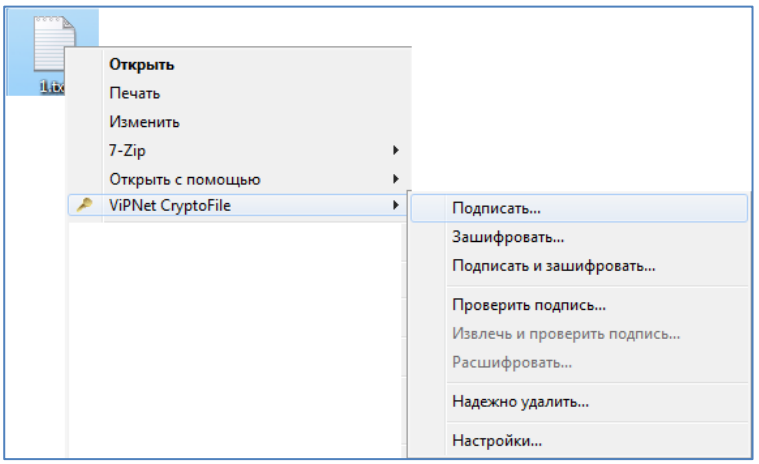

Рисунок 34