# ViPNet CryptoFile 4.0

Руководство пользователя

ViPNet
Virtual Private Network
infotecs

ФРКЕ.00107-01 34 01



ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

# Содержание

# Введение

# О документе

В данном документе содержатся сведения о назначении и принципе работы программы ViPNet CryptoFile, описание установки программы и возможные сценарии работы с ней.

**Совет.** Также вы можете ознакомиться с видеоруководствами по установке и работе с программой https://www.youtube.com/playlist?list=PLkF9DhEbpZWrU4vKQGLfgLpF-kfvJWYD3.

## Для кого предназначен документ

Данный документ предназначен для пользователей программы ViPNet CryptoFile, которые планируют обмениваться конфиденциальными файлами по открытым каналам связи или с использованием съемных носителей.

## Соглашения документа

Ниже перечислены соглашения, принятые в данном документе для выделения информации.

*Таблица 1. Обозначения, используемые в примечаниях*

| Обозначение | Описание |
|---|---|
|  | **Внимание!** Указывает на обязательное для исполнения или следования действие или информацию. |
|  | **Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию. |
|  | **Совет.** Содержит дополнительную информацию общего характера. |

*Таблица 2. Обозначения, используемые для выделения информации в тексте*

| Обозначение | Описание |
|---|---|
| **Название** | Название элемента интерфейса. Например, заголовок окна, название |

| | |
|---|---|
| | поля, кнопки или клавиши. |
| **Клавиша+Клавиша** | Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу. |
| **Меню > Подменю > Команда** | Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации. |
| `Код` | Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки. |

# О программе

Программа ViPNet CryptoFile предназначена для защиты файлов любых форматов с помощью шифрования (см. «Асимметричное шифрование» на стр. 95) и электронной подписи (см. «Электронная подпись» на стр. 99).

Электронная подпись позволяет проверить личность отправителя файлов и целостность данных, содержащихся в этих файлах. Например, электронная подпись обеспечивает юридическую значимость файлов в системах электронного документооборота.

Шифрование обеспечивает защиту передаваемых файлов от несанкционированного прочтения, например, при обмене секретными документами между двумя организациями по открытым каналам связи.

При подписании или шифровании файлов в программе ViPNet CryptoFile создаются контейнеры с подписанными или зашифрованными файлами. Причем эти контейнеры имеют стандартные расширения `*.sig` (см. «Контейнер *.sig» на стр. 96) и `*.enc` (см. «Контейнер *.enc» на стр. 96), работу с которыми поддерживают другие программы со схожим функционалом. Например, расшифровать файл, зашифрованный вами в программе ViPNet CryptoFile, получатель может с помощью программы стороннего производителя (см. «Совместимость с криптопровайдерами сторонних производителей» на стр. 10), при условии поддержки данной программой алгоритмов шифрования ГОСТ или RSA и при наличии закрытого ключа получателя. Таким образом обеспечивается гибкость применения программы ViPNet CryptoFile в различных организациях, в системах электронного документооборота и для частных нужд пользователей.

## Системные требования

Требования к компьютеру для установки программы ViPNet CryptoFile:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 512 Мбайт (рекомендуется 1 Гбайт).
- Свободное место на жестком диске — не менее 300 Мбайт.
- Операционная система — Microsoft Windows XP SP3 (32-разрядная)/Server 2003 (32-разрядная)/Vista SP2 (32/64-разрядная)/Server 2008 (32/64-разрядная)/Windows 7 (32/64-разрядная)/Server 2008 R2 (64-разрядная).

- При использовании Internet Explorer — версия 6.0 и выше.
- Установленный криптопровайдер ViPNet CSP версии 3.2.10 и выше либо криптопровайдер стороннего производителя (см. «Совместимость с криптопровайдерами сторонних производителей» на стр. 10).

  Подробнее об установке ViPNet CSP см. документ «ViPNet CSP. Руководство пользователя».

**Примечание.** В случае использования ViPNet CSP версии ниже 3.2.10 обновите данное ПО до указанной версии. Если обновление по каким-либо причинам невозможно, обратитесь в службу технической поддержки ОАО «ИнфоТеКС» (см. «Обратная связь» на стр. 12).

Криптопровайдер ViPNet CSP может быть установлен на компьютер отдельно либо в составе ПО ViPNet Client или ViPNet CryptoService версии 3.2.9. В этом случае будет использоваться ViPNet CSP версии 3.2.9, также совместимой с программой ViPNet CryptoFile.

## Совместимость с криптопровайдерами сторонних производителей

Программа ViPNet CryptoFile может использоваться совместно с криптопровайдерами сторонних производителей, которые поддерживают алгоритмы ГОСТ и RSA.

Например, возможна работа с криптопровайдером КриптоПро CSP 3.6, который поддерживает алгоритмы ГОСТ. В этом случае на компьютер пользователя устанавливаются программа ViPNet CryptoFile и данный криптопровайдер, средствами которого происходит установка контейнера ключей и сертификата пользователя, а также дальнейшее выполнение низкоуровневых криптографических операций. Подробнее о работе криптопровайдера КриптоПро CSP см. в документации данного программного продукта.

Также возможно использование встроенных криптопровайдеров операционной системы Microsoft Windows, которые осуществляют работу с алгоритмами RSA, например, если вы хотите зашифровать файл с использованием стандартного сертификата пользователя ОС Windows. В этом случае на компьютер пользователя устанавливается только программа ViPNet CryptoFile, а установка контейнеров ключей и сертификатов и дальнейшее выполнение низкоуровневых криптографических операций производятся стандартными средствами операционной системы. Подробнее о работе встроенных криптопровайдеров см. в документации компании Microsoft http://msdn.microsoft.com/ru-ru/library/windows/desktop/aa386983(v=vs.85).aspx.

## Ограничения незарегистрированной версии программы ViPNet CryptoFile

Программа ViPNet CryptoFile может использоваться бесплатно совместно с программным обеспечением ViPNet (ViPNet CSP, ViPNet Client, ViPNet CryptoService). При использовании с криптопровайдерами сторонних производителей или встроенными криптопровайдерами операционной системы необходима регистрация программы ViPNet CryptoFile (см. «Регистрация ViPNet CryptoFile» на стр. 68).

С незарегистрированной версией программного обеспечения ViPNet CryptoFile вы можете работать по демо-лицензии.

Особенности демо-лицензии:

- Срок действия: 14 дней.
- Функциональных ограничений нет.

По истечении срока действия демо-лицензии запуск незарегистрированной программы невозможен.

## Комплект поставки

В комплект поставки ViPNet CryptoFile входит:

- Установочный файл программы:
  - `setup-x86.msi` — для 32-разрядных операционных систем.
  - `setup-x64.msi` — для 64-разрядных операционных систем.
- Документ «ViPNet CryptoFile. Руководство пользователя» в формате PDF.

# Обратная связь

## Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС». По предложенным ссылкам можно найти ответы на многие вопросы, возникающие в процессе эксплуатации продуктов ViPNet.

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/vpn/.

## Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Электронный адрес службы поддержки: hotline@infotecs.ru.
- Форма запроса по электронной почте в службу поддержки http://www.infotecs.ru/support/request/.
- Форум ОАО «ИнфоТеКС» http://www.infotecs.ru/forum.
- 8 (495) 737-6196 — «горячая линия» службы поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения http://infotecs.ru/products/disclosure.php. Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru.

# Общая информация

# Назначение ViPNet CryptoFile

Программа ViPNet CryptoFile устанавливается на рабочие места пользователей и предназначена для обеспечения безопасности различных файлов, передаваемых по открытым каналам связи или с помощью съемных носителей. Вы можете работать с программой ViPNet CryptoFile как с помощью главного окна программы (см. «Интерфейс программы ViPNet CryptoFile» на стр. 33), так и с использованием контекстного меню Windows (см. «Работа с программой ViPNet CryptoFile с помощью контекстного меню Windows» на стр. 35).

Программа ViPNet CryptoFile позволяет вам:

- Защищать файлы с помощью шифрования и электронной подписи (см. «Подписание и шифрование файла» на стр. 52).

  Электронная подпись удостоверяет личность подписавшего файл, а также подтверждает целостность данных, содержащихся в этом файле (то есть подтверждает, что содержимое файла не изменялось после подписания).

  Шифрование обеспечивает защиту и конфиденциальность данных, содержащихся в файле. Только получатель, с использованием сертификата которого зашифрован файл, сможет расшифровать этот файл и ознакомиться с его содержимым.

  Таким образом, программа ViPNet CryptoFile защищает файл от подделки, а также от получения злоумышленником конфиденциальной информации, содержащейся в данном файле.

  С помощью программы ViPNet CryptoFile вы можете как одновременно подписать и зашифровать файл, так и выполнить только одну из данных операций:

  - Только подписать файл (см. «Подписание файла» на стр. 48), например, если вы хотите передать какой-либо юридически значимый документ, авторство которого необходимо подтвердить.
  - Только зашифровать файл (см. «Шифрование файла» на стр. 50), например, если вы хотите передать секретный файл, подтверждение авторства которого не требуется.

- Расшифровывать полученные файлы (см. «Расшифрование файла» на стр. 55).

  При получении файла, зашифрованного с использованием вашего сертификата открытого ключа, вы можете расшифровать его с помощью программы ViPNet CryptoFile, чтобы ознакомиться с его содержимым. При этом вы можете расшифровывать файлы, зашифрованные как в программе ViPNet CryptoFile, так в других программах, поддерживающих асимметричные алгоритмы шифрования и

стандартное расширение `*.enc` (см. «Контейнер *.enc» на стр. 96) для зашифрованных файлов.

- Проверять электронную подпись файлов (см. «Проверка электронной подписи» на стр. 56).

  При получении какого-либо файла, заверенного электронной подписью, вы можете проверить эту электронную подпись, чтобы подтвердить личность отправителя и удостовериться в целостности полученных данных. При этом можно проверить электронную подпись файлов, подписанных как в программе ViPNet CryptoFile, так в других программах, поддерживающих асимметричные алгоритмы электронной подписи и стандартное расширение `*.sig` (см. «Контейнер *.sig» на стр. 96) для контейнеров с подписью.

  В контейнере `*.sig` совместно с электронной подписью передается также сертификат подписавшего файл. Поэтому для проверки подписи отдельная передача сертификата получателям файла не требуется.

- Добавлять штамп точного времени (см. «Штамп времени» на стр. 98) при заверении файлов электронной подписью.

  При заверении файла электронной подписью вы можете добавить к подписи штамп точного времени. Штамп точного времени подтверждает точное время подписания файла и при возникновении спорных ситуаций позволяет доказать факт существования файла на момент его подписания.

- Архивировать файлы перед шифрованием.

  Архивирование файлов перед шифрованием позволяет объединить несколько файлов в один архив формата ZIP и далее поместить этот архив в один контейнер *.enc (на стр. 96) при шифровании. Данная функция позволяет ускорить работу при отправлении большого количества зашифрованных файлов одному получателю.

- Использовать прикрепленную или открепленную подпись.

  При использовании прикрепленной подписи (см. «Прикрепленная подпись» на стр. 97) электронная подпись и исходный файл совместно помещаются в контейнер с расширением `*.sig` (см. «Контейнер *.sig» на стр. 96). Прикрепленная подпись обеспечивает простоту обмена, копирования и шифрования подписанных файлов (например, в системах электронного документооборота). При этом ознакомиться с содержимым файла смогут только пользователи, на компьютерах которых установлены специальные средства работы с контейнерами `*.sig` (программы ViPNet CryptoFile, ViPNet Деловая почта или программы сторонних производителей со схожим функционалом (например, КриптоАРМ)).

  В случае использования открепленной подписи (см. «Открепленная подпись» на стр. 97) электронная подпись помещается в контейнер `*.sig`, при этом исходный файл в данный контейнер не помещается, а передается другим пользователям

отдельно (для проверки электронной подписи требуется и контейнер с открепленной подписью, и исходный файл). Открепленная подпись позволяет ознакомиться с содержимым исходного файла пользователям, на компьютерах которых не установлены средства работы с контейнерами `*.sig`. Однако в этом случае затрудняется передача, шифрование и другие операции с файлом подписи, так как операции необходимо производить с двумя файлами: исходным файлом и контейнером `*.sig`.

- Создавать отчеты о результатах проверки электронной подписи файла (см. «Формирование отчета о результате проверки электронной подписи» на стр. 66).

  После проверки подписи какого-либо файла с помощью программы ViPNet CryptoFile вы можете сформировать отчет о результатах проверки электронной подписи. Отчет содержит информацию о корректности электронной подписи, времени подписания файла, сертификатах пользователей, подписавших файл, а также о штампе времени, если он был добавлен во время подписания файла. Такой отчет может быть использован при разборе конфликтных ситуаций, возникших при использовании электронной подписи.

- Надежно удалять файлы (см. «Надежное удаление файла» на стр. 63).

  С помощью программы ViPNet CryptoFile вы можете безвозвратно удалять с жесткого диска или съемных носителей файлы, тем самым обеспечив их максимальную защиту от потенциальных попыток восстановления. Например, вы можете из соображений безопасности удалить с жесткого диска строго конфиденциальные файлы, при этом вы можете быть уверены, что данные файлы невозможно будет восстановить какими-либо специальными средствами.

# Принцип работы ViPNet CryptoFile

Программа ViPNet CryptoFile осуществляет формирование и проверку электронной подписи, а также шифрование и расшифрование файлов, при этом для выполнения низкоуровневых криптографических операций программа обращается к криптопровайдеру ViPNet CSP (или криптопровайдеру стороннего производителя).

Программа ViPNet CryptoFile работает на основе асимметричных алгоритмов шифрования, которые используют два математически связанных ключа пользователя:

- Закрытый ключ (на стр. 96) — используется для формирования электронной подписи и расшифрования файлов. Закрытый ключ конфиденциален и не передается другим пользователям.
- Открытый ключ (на стр. 97) — используется для проверки электронной подписи и шифрования файлов. Открытый ключ свободно распространяется среди других пользователей в составе сертификата открытого ключа подписи пользователя (см. «Сертификат открытого ключа подписи пользователя» на стр. 98).

Рассмотрим принцип работы программы ViPNet CryptoFile совместно с криптопровайдером ViPNet CSP на следующих примерах:

- Подписание файла для последующей передачи другому пользователю (на стр. 17).
- Шифрование файла для последующей передачи другому пользователю (на стр. 19).
- Подписание и шифрование файла для последующей передачи другому пользователю (на стр. 20).

## Подписание файла для последующей передачи другому пользователю

Подписание файла и передача его другому пользователю при использовании алгоритмов ГОСТ осуществляются следующим образом:

1. Пользователь (1) добавляет в программу ViPNet CryptoFile файл, который хочет передать пользователю (2).
2. При подписании файла программа ViPNet CryptoFile обращается к криптопровайдеру ViPNet CSP для выполнения низкоуровневых криптографических

операций. Затем программа ViPNet CryptoFile с помощью закрытого ключа пользователя (1) формирует электронную подпись:

- В случае использования прикрепленной подписи исходный файл, сформированная электронная подпись и служебная информация помещаются в контейнер с расширением `*.sig`.
- В случае использования открепленной подписи сформированная электронная подпись и служебная информация помещаются в контейнер `*.sig`. При этом исходный файл в контейнер не помещается, а передается пользователю (2) отдельно (для проверки электронной подписи требуется и контейнер с открепленной подписью, и исходный файл).


*Рисунок 1: Подписание данных файла с помощью ViPNet CryptoFile*

3 Пользователь (1) передает пользователю (2) контейнер с подписанным файлом, например, с помощью электронной почты.

4 Пользователь (2) проверяет электронную подпись с использованием открытого ключа пользователя (1), который входит в состав сертификата подписи.

В результате пользователь (2) сможет ознакомиться с данными, содержащимися в полученном файле, и убедиться в их подлинности.

## Шифрование файла для последующей передачи другому пользователю

Шифрование файла и передача его другому пользователю при использовании алгоритмов ГОСТ осуществляются следующим образом:

1. Пользователь (1) добавляет в программу ViPNet CryptoFile файл, который хочет передать пользователю (2).
2. При шифровании файла программа ViPNet CryptoFile обращается к криптопровайдеру ViPNet CSP для выполнения низкоуровневых криптографических операций. Затем программа ViPNet CryptoFile с помощью открытого ключа пользователя (2) зашифровывает файл и помещает его в контейнер с расширением `*.enc`.

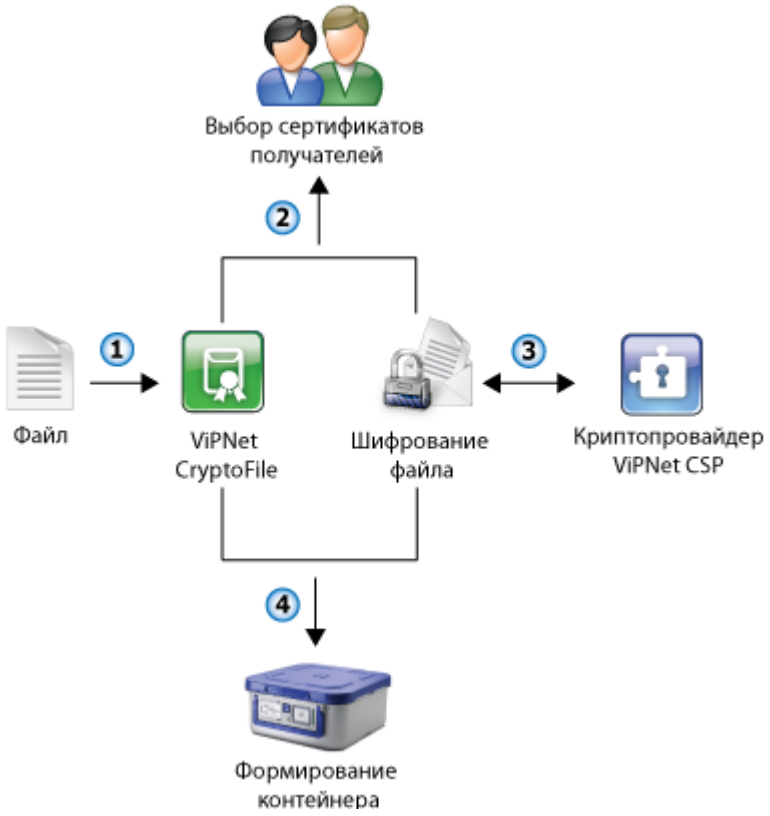


*Рисунок 2: Шифрование данных файла с помощью ViPNet CryptoFile*

3. Пользователь (1) передает пользователю (2) контейнер с зашифрованным файлом, например, с помощью электронной почты.

4 Пользователь (2) извлекает файл из контейнера и расшифровывает его с использованием своего закрытого ключа.

В результате пользователь (2) сможет ознакомиться с секретными данными, содержащимися в полученном файле.

## Подписание и шифрование файла для последующей передачи другому пользователю

Подписание, шифрование файла и передача его другому пользователю при использовании алгоритмов ГОСТ осуществляются следующим образом:

1 Пользователь (1) добавляет в программу ViPNet CryptoFile файл, который хочет передать пользователю (2).

2 При подписании файла программа ViPNet CryptoFile обращается к криптопровайдеру ViPNet CSP для выполнения низкоуровневых криптографических операций. Затем программа ViPNet CryptoFile с помощью закрытого ключа пользователя (1) формирует электронную подпись:

   - В случае использования прикрепленной подписи исходный файл, сформированная электронная подпись и служебная информация помещаются в контейнер с расширением `*.sig`.
   - В случае использования открепленной подписи сформированная электронная подпись и служебная информация помещаются в контейнер `*.sig`. При этом исходный файл в контейнер не помещается.

3 При шифровании файла программа ViPNet CryptoFile обращается к криптопровайдеру ViPNet CSP для выполнения низкоуровневых криптографических операций. Затем программа ViPNet CryptoFile с помощью открытого ключа пользователя (2) зашифровывает файл и помещает его в контейнер с расширением `*.enc`.

   В случае использования открепленной подписи контейнер с подписью `*.sig` не зашифровывается. Чтобы исходный файл и контейнер `*.sig` были зашифрованы помещены в один контейнер `*.enc`, необходимо предварительно поместить их в архив.

4 Пользователь (1) передает пользователю (2) контейнер с зашифрованным и подписанным файлом, например, с помощью электронной почты.

5 Пользователь (2) извлекает файл из контейнера и расшифровывает его с использованием своего закрытого ключа.

6 Пользователь (2) проверяет электронную подпись с использованием открытого ключа пользователя (1), который входит в состав сертификата подписи.

В результате пользователь (2) сможет ознакомиться с данными, содержащимися в полученном файле.

# Требования к сертификатам для работы в программе ViPNet CryptoFile

Для работы в программе ViPNet CryptoFile сертификаты пользователей должны удовлетворять следующим требованиям:

- Сертификат должен быть действителен (срок действия сертификата не истек).
- Для шифрования сертификаты получателей должны иметь назначение **Шифрование данных** в поле **Использование ключа**.
- Для подписи файлов сертификат подписывающего должен иметь назначение **Цифровая подпись** в поле **Использование ключа**.

В случае если сертификат подписывающего или сертификат получателя не содержит требуемые расширения, перед выполнением соответствующей операции (подписание, шифрование или подписание и шифрование) появится сообщение о неправильном использовании сертификата. При этом выполнение операции может быть продолжено. Для этого в окне с сообщением нажмите кнопку **Да**.

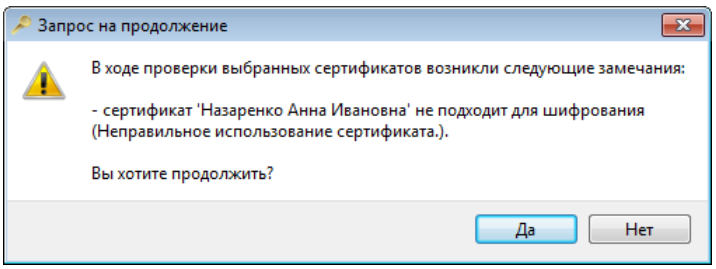


*Рисунок 3: Запрос на продолжение операции*


# Установка программы ViPNet CryptoFile

# Последовательность установки

Программа ViPNet CryptoFile функционирует совместно с криптопровайдером ViPNet CSP или криптопровайдерами сторонних производителей, которые поддерживают алгоритмы ГОСТ и RSA (например, КриптоПро CSP или встроенные криптопровайдеры операционной системы Windows). Также возможно использование ViPNet CryptoFile с ПО ViPNet Client или ViPNet CryptoService, в состав которых входит криптопровайдер ViPNet CSP.

Перед установкой программы ViPNet CryptoFile убедитесь, что у вас имеется:

1. Контейнер ключей (на стр. 97) электронной подписи пользователя. Контейнер ключей содержит закрытый ключ подписи и сертификат открытого ключа подписи (далее также — сертификат).
2. Дистрибутив ключей (на стр. 95) в случае использования ПО ViPNet Client или ViPNet CryptoService.

**Примечание.** Контейнер ключей входит в состав дистрибутива ключей (если пользователь обладает правом подписи). При развертывании дистрибутива ключей происходит автоматическая установка:

- контейнера ключей в криптопровайдер ViPNet CSP;
- сертификата пользователя в системное хранилище.

3. Установочный файл программы ViPNet CryptoFile.

**Совет.** Также вы можете ознакомиться с видеоруководствами по установке и работе с программой https://www.youtube.com/playlist?list=PLkF9DhEbpZWrU4vKQGLfgLpF-kfvJWYD3.

Существует три варианта установки программы ViPNet CryptoFile. Вы можете выбрать один из них в зависимости от того, с каким обязательным программным обеспечением и с использованием каких алгоритмов шифрования вы планируете работать:

- Последовательность установки в случае использования ViPNet CSP или криптопровайдера стороннего производителя (на стр. 25).

- Последовательность установки в случае использования ViPNet Client или ViPNet CryptoService (на стр. 26).
- Последовательность установки в случае использования встроенных криптопровайдеров операционной системы (на стр. 27).

## Последовательность установки в случае использования ViPNet CSP или криптопровайдера стороннего производителя

Для установки программы ViPNet CryptoFile в случае использования ViPNet CSP или криптопровайдера стороннего производителя (алгоритмы шифрования ГОСТ) выполните все действия из приведенного ниже списка.

*Таблица 3. Последовательность установки программы ViPNet CryptoFile*

| | Действие | Примечание |
|---|---|---|
| ☐ | Установите на компьютер криптопровайдер ViPNet CSP или криптопровайдер стороннего производителя | См. документ «ViPNet CSP. Руководство пользователя», глава «Установка и запуск программы».<br>Информацию по установке криптопровайдеров сторонних производителей см. в документации данных программных продуктов. |
| ☐ | Установите контейнер ключей и сертификат открытого ключа пользователя | См. документ «ViPNet CSP. Руководство пользователя», глава «Установка контейнеров и сертификатов».<br>Информацию по установке контейнеров ключей и сертификатов при использовании криптопровайдеров сторонних производителей см. в документации данных программных продуктов. |
| ☐ | Установите на компьютер программу ViPNet CryptoFile | Установка программы ViPNet CryptoFile (на стр. 28) |
| ☐ | В случае использования криптопровайдера стороннего производителя зарегистрируйте программу ViPNet CryptoFile | Регистрация ViPNet CryptoFile (на стр. 68) |
| ☐ | Настройте программу ViPNet CryptoFile | Настройка программы ViPNet CryptoFile (на стр. 39) |

**Совет.** Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

## Последовательность установки в случае использования ViPNet Client или ViPNet CryptoService

Для установки программы ViPNet CryptoFile в случае использования ViPNet Client или ViPNet CryptoService (алгоритмы шифрования ГОСТ) выполните все действия из приведенного ниже списка.

*Таблица 4. Последовательность установки программы ViPNet CryptoFile*

| | Действие | Примечание |
|---|---|---|
| ☐ | Установите на компьютер ПО ViPNet Client или ViPNet CryptoService | См. один из документов:<br>«ViPNet Client Монитор. Руководство пользователя», глава «Установка, обновление и удаление ПО ViPNet Client».<br>«ViPNet CryptoService. Руководство пользователя», глава «Установка, обновление и удаление программы ViPNet CryptoService». |
| ☐ | Установите дистрибутив ключей (на стр. 95) `*.dst` | См. один из документов:<br>«ViPNet Client Монитор. Руководство пользователя», глава «Начало работы с ПО ViPNet Client».<br>«ViPNet CryptoService. Руководство пользователя», глава «Запуск программы и установка ключей». |
| ☐ | Установите на компьютер программу ViPNet CryptoFile | Установка программы ViPNet CryptoFile (на стр. 28) |
| ☐ | Настройте программу ViPNet CryptoFile | Настройка программы ViPNet CryptoFile (на стр. 39) |

**Совет.** Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

## Последовательность установки в случае использования встроенных криптопровайдеров операционной системы

Для установки программы ViPNet CryptoFile в случае использования встроенных криптопровайдеров операционной системы Windows (алгоритмы шифрования RSA) выполните все действия из приведенного ниже списка.

*Таблица 5. Последовательность установки программы ViPNet CryptoFile*

| | Действие | Примечание |
|---|---|---|
| ☐ | Установите контейнер ключей и сертификат открытого ключа пользователя | См. документацию компании Microsoft http://msdn.microsoft.com/ru-ru/library/windows/desktop/aa386983(v=vs.85).aspx |
| ☐ | Установите на компьютер программу ViPNet CryptoFile | Установка программы ViPNet CryptoFile (на стр. 28) |
| ☐ | Зарегистрируйте программу ViPNet CryptoFile | Регистрация ViPNet CryptoFile (на стр. 68) |
| ☐ | Настройте программу ViPNet CryptoFile | Настройка программы ViPNet CryptoFile (на стр. 39) |

**Совет.** Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

# Установка программы ViPNet CryptoFile

Для установки программы ViPNet CryptoFile на компьютер выполните следующие действия:

1. Запустите файл:
   - `setup-x86.msi` — при использовании 32-разрядной операционной системы.
   - `setup-x64.msi` — при использовании 64-разрядной операционной системы.

   Будет запущена программа установки ViPNet CryptoFile.
2. Следуйте указаниям программы установки.
3. По завершении установки нажмите кнопку **Готово**. Программа установки ViPNet CryptoFile будет закрыта.

В результате программа ViPNet CryptoFile будет установлена на компьютер, выполните ее настройку (см. «Настройка программы ViPNet CryptoFile» на стр. 39).

# Обновление и удаление программы ViPNet CryptoFile

Обновление программы ViPNet CryptoFile производится с помощью программы установки ViPNet CryptoFile. Для обновления вам потребуется установочный файл новой версии ViPNet CryptoFile.

Чтобы обновить программу ViPNet CryptoFile, выполните следующие действия:

1. Завершите работу с программой ViPNet CryptoFile (см. «Запуск и завершение работы с программой ViPNet CryptoFile» на стр. 32).
2. Запустите установочный файл новой версии программы ViPNet CryptoFile. Будет запущена программа установки ViPNet CryptoFile.
3. Следуйте указаниям программы установки.
4. По завершении обновления нажмите кнопку **Готово**.
5. Настройте программу ViPNet CryptoFile (см. «Настройка программы ViPNet CryptoFile» на стр. 39).

В результате программа ViPNet CryptoFile будет обновлена до новой версии и готова к работе.

Удаление программы ViPNet CryptoFile производится также с помощью программы установки ViPNet CryptoFile. После удаления программы файлы, с которыми вы работали в ViPNet CryptoFile, могут быть расшифрованы с помощью других программ, поддерживающих асимметричные алгоритмы шифрования ГОСТ или RSA. Поэтому рекомендуется предварительно надежно удалить секретные файлы с компьютера с помощью программы ViPNet CryptoFile.

Чтобы удалить программу ViPNet CryptoFile, выполните следующие действия:

1. При необходимости надежно удалите секретные файлы с компьютера с помощью программы ViPNet CryptoFile (см. «Надежное удаление файла» на стр. 63).
2. Завершите работу с программой ViPNet CryptoFile (см. «Запуск и завершение работы с программой ViPNet CryptoFile» на стр. 32).

3 Запустите установочный файл программы ViPNet CryptoFile. Будет запущена программа установки ViPNet CryptoFile.

4 На первой странице программы установки нажмите кнопку **Далее**.

5 На странице **Изменить, восстановить или удалить программу** нажмите кнопку **Удалить**.

6 На странице **Удаление ViPNet CryptoFile** нажмите кнопку **Удалить**.

7 По завершении удаления нажмите кнопку **Готово**.

В результате программа ViPNet CryptoFile будет удалена с компьютера.

# Начало работы с программой ViPNet CryptoFile

# Запуск и завершение работы с программой ViPNet CryptoFile

Для запуска программы ViPNet CryptoFile:

1. Выполните одно из действий:
   - В меню **Пуск** выберите **Все программы > ViPNet > ViPNet CryptoFile > ViPNet CryptoFile**.
   - Дважды щелкните ярлык  на рабочем столе.

   При этом откроется главное окно программы (см. «Интерфейс программы ViPNet CryptoFile» на стр. 33).
2. Если на компьютере установлен криптопровайдер ViPNet CSP версии ниже 3.2.10, появится сообщение о необходимости обновить ViPNet CSP. В окне с сообщением нажмите кнопку **Продолжить работу**.

Чтобы завершить работу с программой ViPNet CryptoFile, выполните одно из действий:

- В правом верхнем углу окна **ViPNet CryptoFile** нажмите кнопку **Закрыть**  .
- В меню **Файл** выберите пункт **Выход**.
- Нажмите сочетание клавиш **Alt+F4**.

# Интерфейс программы ViPNet CryptoFile

Главное окно программы ViPNet CryptoFile представлено на рисунке ниже.

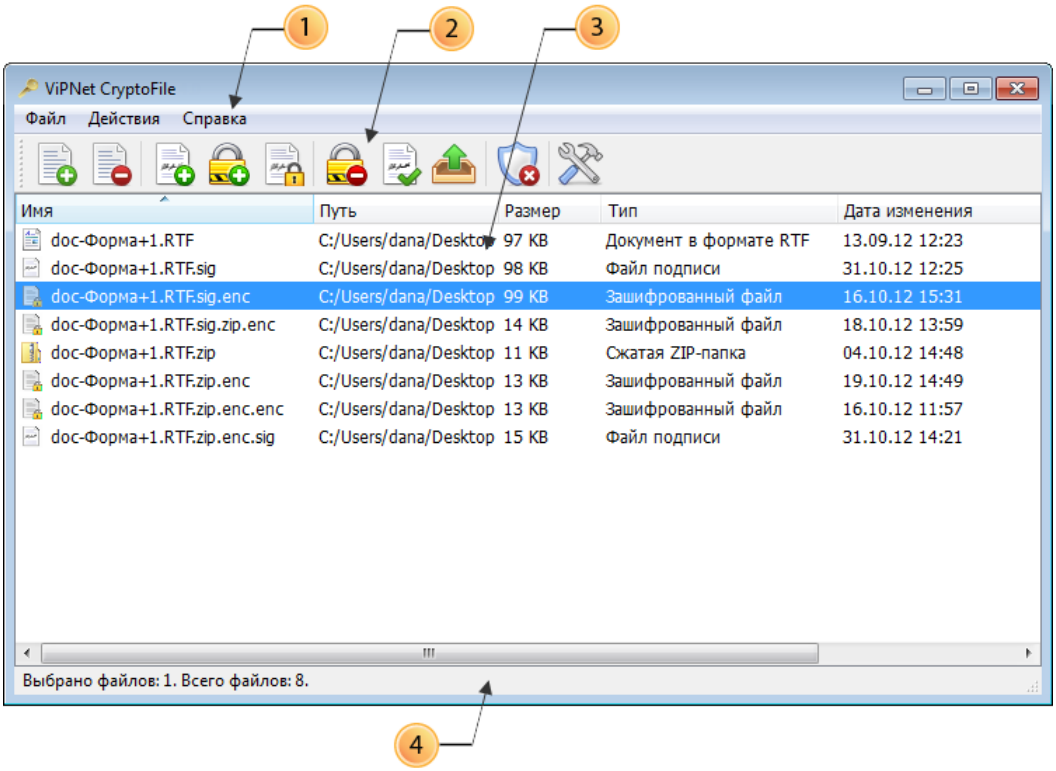


*Рисунок 4: Интерфейс программы ViPNet CryptoFile*

Цифрами на рисунке обозначены:

1. Главное меню программы.
2. Панель инструментов.
3. Панель просмотра. На данной панели отображается список файлов, добавленных в программу ViPNet CryptoFile, а также контейнеры, сформированные в результате подписи или шифрования файлов.

   Контейнеры на панели просмотра обозначаются следующими значками:

   -  — контейнер `*.sig` с прикрепленной подписью и исходным файлом.

-  — контейнер `*.sig` с открепленной подписью.
-  — контейнер `*.enc` с зашифрованным файлом.

В случае использования других программ, схожих по функционалу с ViPNet CryptoFile, вид данных значков может отличаться. Остальные файлы обозначаются значками, соответствующими их формату.

Вы можете отсортировать содержимое списка по любому столбцу таблицы. Для этого щелкните по заголовку нужного столбца.

При удалении, переименовании или перемещении в другую папку файлы на панели просмотра выделяются серым цветом. Для обновления списка файлов нажмите клавишу **F5** или в меню **Файл** выберите пункт **Обновить список файлов**.

**4** Строка состояния. В строке состояния указано общее количество файлов, добавленных в программу, а также количество файлов, которые выбраны для выполнения каких-либо операций (например, шифрования).

# Работа с программой ViPNet CryptoFile с помощью контекстного меню Windows

Вы можете работать с программой ViPNet CryptoFile с помощью контекстного меню Windows без вызова главного окна программы и добавления файлов в нее. Это позволяет ускорить и упростить выполнение основных функций программы ViPNet CryptoFile. Данная функция может быть полезна, если вы выполняете с файлом какие-либо операции средствами операционной системы или других программ (например, копируете файл на съемный носитель или прикрепляете его к электронному письму), и вам понадобилось зашифровать файл, не отвлекаясь на работу с основным окном программы ViPNet CryptoFile.

С помощью контекстного меню Windows вы можете:

- Заверить файл электронной подписью (см. «Подписание файла» на стр. 48).
- Зашифровать файл (см. «Шифрование файла» на стр. 50).
- Одновременно подписать и зашифровать файл (см. «Подписание и шифрование файла» на стр. 52).
- Проверить электронную подпись файла (см. «Проверка электронной подписи» на стр. 56).
- Расшифровать файл (см. «Расшифрование файла» на стр. 55).
- Извлечь файл из контейнера и одновременно проверить его электронную подпись (см. «Извлечение файла из контейнера» на стр. 59).
- Надежно удалить файл (см. «Надежное удаление файла» на стр. 63).
- Просмотреть или изменить настройки программы ViPNet CryptoFile (см. «Настройка программы ViPNet CryptoFile» на стр. 39).

Чтобы выполнить одно из перечисленных выше действий с помощью контекстного меню Windows:

1. В проводнике Windows выберите нужный файл (или несколько файлов) и щелкните по нему правой кнопкой мыши.

2. В контекстном меню выберите **ViPNet CryptoFile**, затем щелкните нужный пункт.

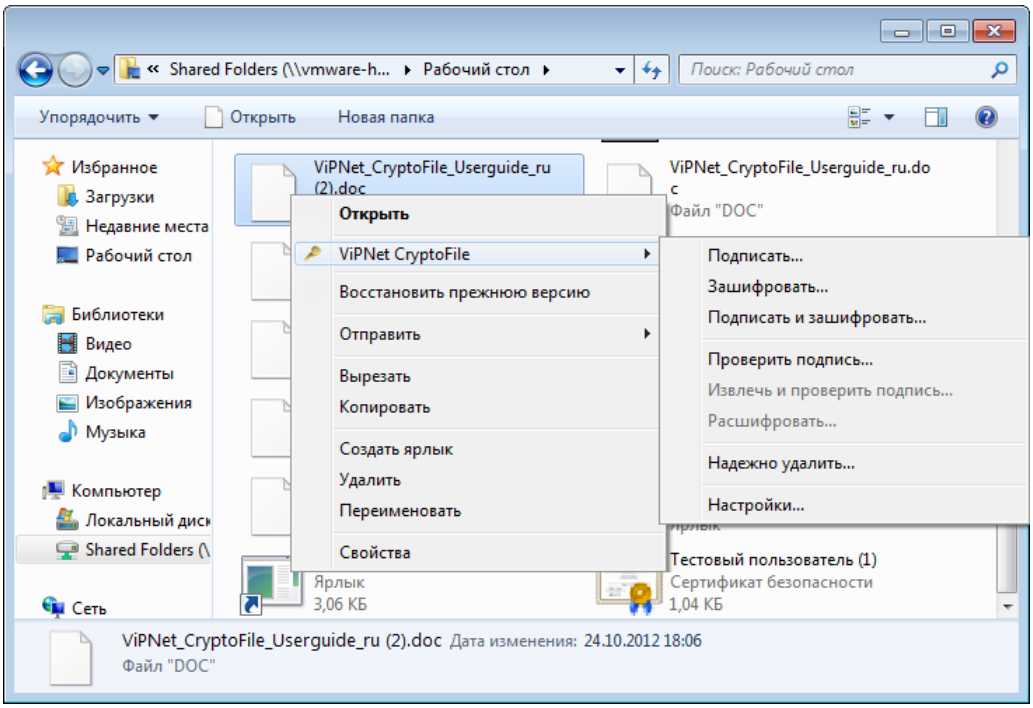


*Рисунок 5: Работа с программой с помощью контекстного меню*

В результате будет выполнена выбранная операция (например, зашифрование файла). Во время выполнения операции следуйте указаниям, описанным в соответствующих разделах главы Работа с программой ViPNet CryptoFile (на стр. 45).

# Установка сертификатов получателей в системное хранилище

Для возможности обмена зашифрованными файлами с другими пользователями предварительно следует обменяться сертификатами открытого ключа подписи с данными пользователями, а затем установить их сертификаты в системное хранилище. Также рекомендуется установить в системное хранилище сертификаты и списки отозванных сертификатов (СОС) администраторов, издавших сертификаты получателей. Таким образом будет установлена цепочка доверия для сертификатов получателей.

Чтобы установить сертификат или СОС в системное хранилище, выполните следующие действия:

1. Откройте папку, содержащую полученный сертификат или СОС. Щелкните правой кнопкой мыши файл сертификата или СОС и выберите пункт **Установить сертификат** или **Установить список отзыва (CRL)**. Будет запущен **Мастер импорта сертификатов**, следуйте его указаниям.
2. На странице **Хранилище сертификатов** выполните следующие действия:
   - **2.1** Установите переключатель в положение **Поместить все сертификаты в следующее хранилище**.
   - **2.2** С помощью кнопки **Обзор** укажите хранилище:
     - **Доверенные корневые центры сертификации** — для установки сертификатов администраторов.
     - **Промежуточные центры сертификации** — для установки СОС.
     - **Другие пользователи** — для установки сертификатов получателей.

     После выбора хранилища нажмите кнопку **OK**.
   - **2.3** Нажмите кнопку **Далее**.

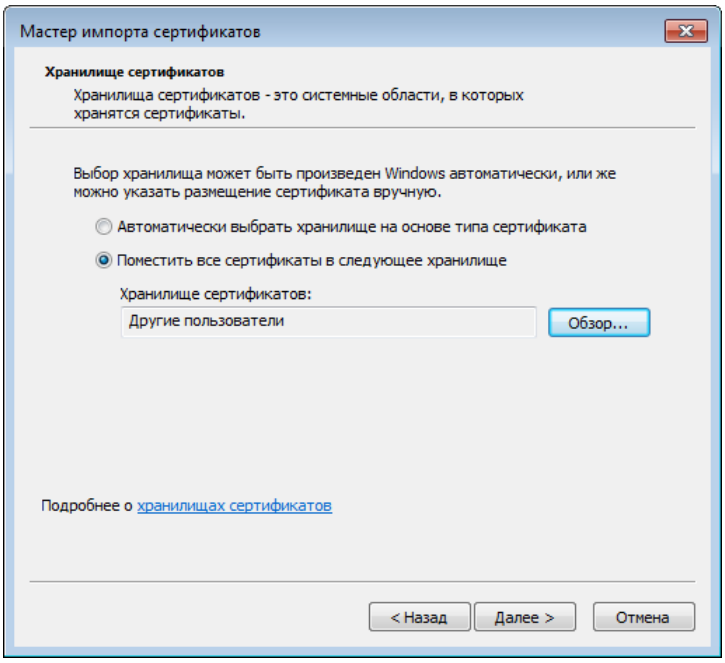


*Рисунок 6: Выбор хранилища сертификатов*

3 На странице **Завершение мастера импорта сертификатов** нажмите кнопку **Готово**.

В результате сертификат или СОС будет добавлен в системное хранилище. Все сертификаты получателей, добавленные в хранилище, будут отображаться в окне **Выбор сертификата** при добавлении сертификатов в список получателей для шифрования файлов (см. «Настройка списка получателей файлов, зашифрованных с помощью программы ViPNet CryptoFile» на стр. 42).

# Настройка программы ViPNet CryptoFile

Перед началом работы с программой ViPNet CryptoFile для возможности подписания и шифрования файлов выполните следующие действия:

- Задайте сертификат пользователя для подписи файлов (см. «Задание сертификата пользователя для подписи файлов» на стр. 39).
- Настройте список получателей файлов, зашифрованных с помощью программы ViPNet CryptoFile (см. «Настройка списка получателей файлов, зашифрованных с помощью программы ViPNet CryptoFile» на стр. 42).
- Настройте подключение к службе штампов времени в случае использования данной функции (см. «Настройка подключения к службе штампов времени (TSP-серверу)» на стр. 43).

## Задание сертификата пользователя для подписи файлов

Для подписания файлов с помощью программы ViPNet CryptoFile вам понадобится сертификат открытого ключа подписи и соответствующий ему закрытый ключ. Сертификат должен быть предварительно установлен в системное хранилище.

Чтобы настроить параметры подписания файлов, в программе ViPNet CryptoFile выполните следующие действия:

1. В главном окне программы выполните одно из действий:
   - На панели инструментов нажмите кнопку **Настройки**  .
   - В меню **Файл** выберите пункт **Настройки**.
2. В окне **Настройки** в группе **Подпись** нажмите кнопку **Задать**, чтобы задать сертификат пользователя, с помощью которого будет производиться подпись файлов.

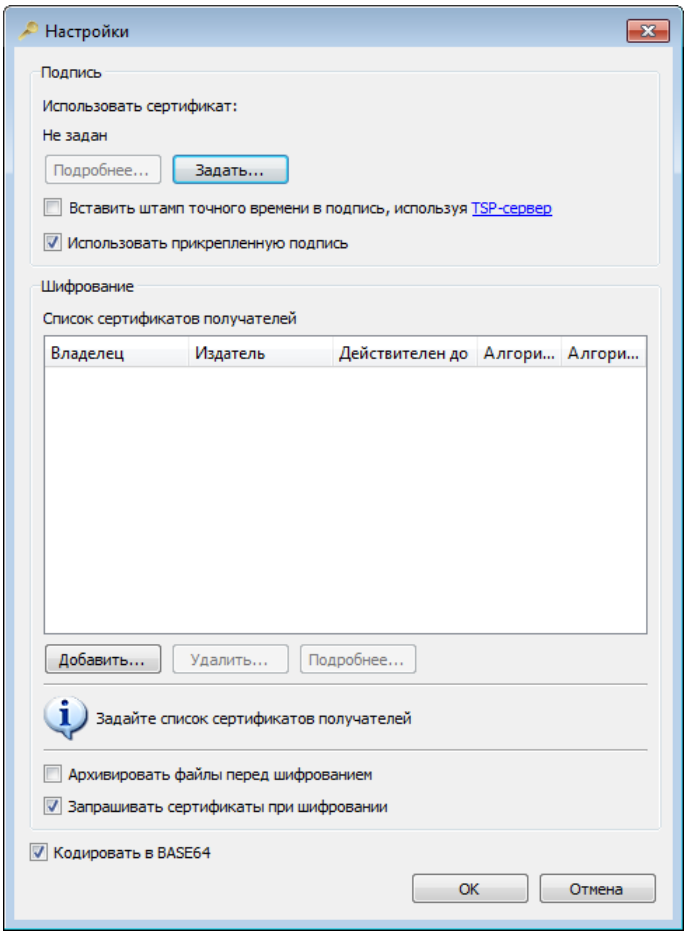


*Рисунок 7: Задание сертификата для подписи файлов*

**3** В окне **Безопасность Windows** выберите нужный сертификат и нажмите кнопку **OK**.

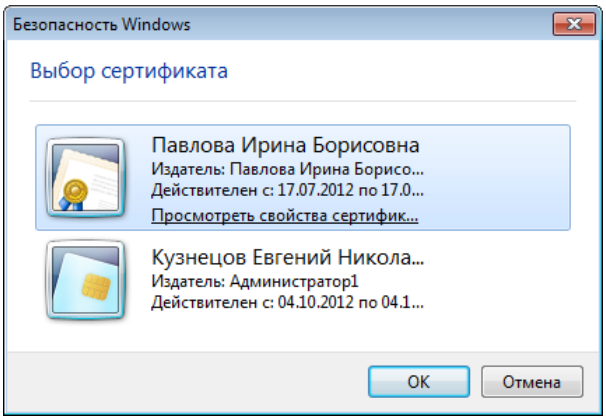


*Рисунок 8: Выбор сертификата*

4 В окне **Настройки** в группе **Подпись** отобразится информация о заданном сертификате. При этом кнопку **Задать** заменится кнопкой **Изменить**.

Для просмотра подробной информации об используемом сертификате в группе **Подпись** нажмите кнопку **Подробнее**.

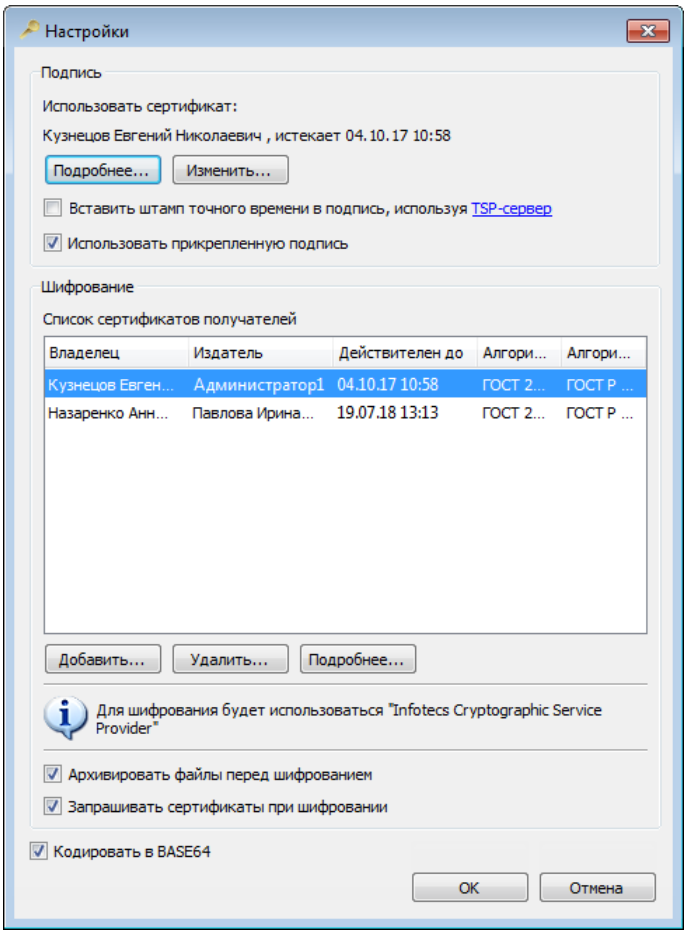


*Рисунок 9: Настройки программы ViPNet CryptoFile*

5 Для использования прикрепленной подписи установите флажок **Использовать прикрепленную подпись**. Для использования открепленной подписи снимите данный флажок (см. «Назначение ViPNet CryptoFile» на стр. 14).

6 При желании для формируемых контейнеров `*.sig` вы можете использовать кодировку Base64, которая широко используется при передаче файлов через Интернет, в том числе по электронной почте. Рекомендуется применять кодировку Base64 в случае использования откреплённой подписи. Чтобы включить кодирование в Base64, установите флажок **Кодировать в BASE64**.

7 Нажмите кнопку **OK**.

В результате параметры подписи будут настроены, и вы сможете заверять файлы электронной подписью с помощью программы ViPNet CryptoFile (см. «Подписание файла» на стр. 48).

## Настройка списка получателей файлов, зашифрованных с помощью программы ViPNet CryptoFile

Для шифрования файлов с помощью программы ViPNet CryptoFile вам понадобятся сертификаты получателей файлов, которые необходимо предварительно установить в системное хранилище, а затем добавить в список получателей при настройке программы.

Чтобы настроить параметры шифрования файлов, выполните следующие действия:

1. Обменяйтесь сертификатами с пользователями, которым хотите передавать конфиденциальные файлы, например, с помощью электронной почты или съемных носителей.
2. Полученные сертификаты установите в системное хранилище (см. «Установка сертификатов получателей в системное хранилище» на стр. 37).
3. В главном окне программы ViPNet CryptoFile выполните одно из действий:
   - На панели инструментов нажмите кнопку **Настройки**  .
   - В меню **Файл** выберите пункт **Настройки**.
4. В окне **Настройки** (см. рисунок на стр. 41) в группе **Шифрование** нажмите кнопку **Добавить**.
5. В появившемся окне **Выбор сертификата** будут отображены сертификаты получателей, которые ранее были установлены в системное хранилище.

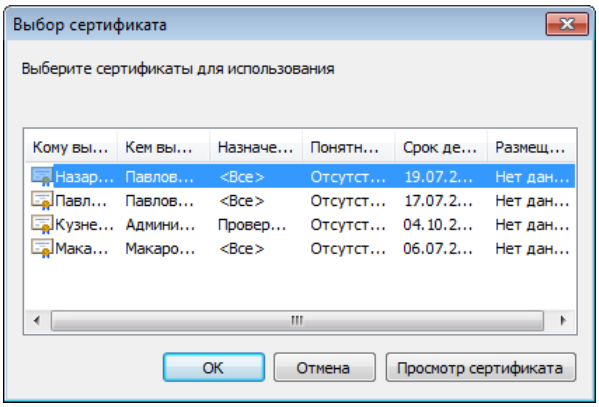


*Рисунок 10: Выбор сертификатов получателей*

Выберите сертификаты, которые хотите добавить в список сертификатов получателей, и нажмите кнопку **OK**. При этом выбранные сертификаты отобразятся в списке сертификатов получателей.

При необходимости вы можете удалить сертификаты из списка сертификатов получателей. Для этого в группе **Шифрование** нажмите кнопку **Удалить.**

Для просмотра подробной информации о каком-либо из сертификатов получателей в группе **Шифрование** нажмите кнопку **Подробнее**.

6 Для архивирования файлов перед шифрованием установите флажок **Архивировать файлы перед шифрованием**.

7 Если вы хотите изменять список сертификатов получателей непосредственно перед шифрованием файлов, установите флажок **Запрашивать сертификаты при шифровании**. В данном случае при шифровании каждого файла будет появляться окно **Сертификаты получателей** (см. рисунок на стр. 51), в котором вы сможете изменить список сертификатов получателей.

8 Нажмите кнопку **OK**.

В результате параметры шифрования файлов будут настроены, и вы сможете зашифровывать файлы с помощью программы ViPNet CryptoFile (см. «Шифрование файла» на стр. 50).

## Настройка подключения к службе штампов времени (TSP-серверу)

С помощью программы ViPNet CryptoFile вы можете добавлять штамп точного времени при подписании файлов. Штамп времени удостоверяет точное время подписи файла. Для добавления штампа времени при подписании файла программа ViPNet CryptoFile обращается к службе штампов времени (см. «TSP-сервер (служба штампов времени)» на стр. 95), поэтому настройте подключение к службе штампов времени следующим образом:

1 В главном окне программы выполните одно из действий:

- На панели инструментов нажмите кнопку **Настройки**  .
- В меню **Файл** выберите пункт **Настройки**.

2 В окне **Настройки** (см. рисунок на стр. 41) в группе **Подпись** выполните следующие действия:

**2.1** Установите флажок **Вставить штамп точного времени в подпись, используя TSP-сервер**.

**2.2** Щелкните по ссылке **TSP-сервер** и в появившемся окне в поле **Введите адрес TSP-сервера** укажите URL-адрес TSP-сервера. Для проверки соединения с указанным TSP-сервером нажмите кнопку **Проверить**.

**2.3** Если при подключении к службе штампов времени используется прокси-сервер, установите флажок **Использовать прокси** и укажите параметры подключения к прокси-серверу (IP-адрес и порт подключения к прокси-серверу в формате `<IP-адрес>:<порт>`).

Также вы можете воспользоваться системными настройками подключения к прокси-серверу, указанными в веб-браузере, который используется по умолчанию. Для этого установите флажок **Использовать системные настройки**.

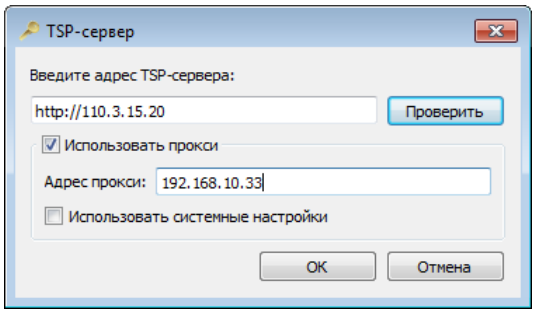


*Рисунок 11: Настройка подключения к TSP-серверу*

**2.4** Нажмите кнопку **OK**.

В результате ко всем подписываемым файлам будет добавляться штамп точного времени. В случае если при подписании файла соединение с TSP-сервером будет отсутствовать, электронная подпись не будет сформирована, и в окне **Выполнение операции** (см. рисунок на стр. 50) будет отображена информация об ошибке. В этом случае дождитесь установления соединения с TSP-сервером либо отключите использование службы штампов времени. Для этого в окне **Настройки** снимите флажок **Вставить штамп точного времени в подпись, используя TSP-сервер**.

# Работа с программой ViPNet CryptoFile

# Добавление файлов в программу ViPNet CryptoFile

Перед началом работы с файлом следует добавить его в программу ViPNet CryptoFile. Для этого выполните следующие действия:

1. В главном окне программы выполните одно из действий:
   - На панели инструментов нажмите кнопку **Добавить файлы в список**  .
   - В меню **Файл** выберите пункт **Добавить файлы в список**.
   - Щелкните правой кнопкой мыши по панели просмотра и выберите пункт **Добавить файлы в список**.
2. В появившемся окне выберите файл (или несколько файлов), который хотите добавить в программу, и нажмите кнопку **Открыть**.

**Примечание.** Также для добавления файлов в программу вы можете перетащить их в главное окно программы, удерживая нажатой левую кнопку мыши.

В результате файл будет добавлен в программу, его название отобразится в списке файлов на панели просмотра.

# Подготовка файлов к передаче другим пользователям

При отправке конфиденциальных файлов другим пользователям по открытым каналам с помощью программы ViPNet CryptoFile вы можете защитить их от прочтения или подмены злоумышленниками. Для этого используются электронная подпись и асимметричное шифрование.

В контейнер `*.sig` с электронной подписью (прикрепленной или открепленной) помещается также сертификат пользователя, подписавшего файл. Поэтому отдельная передача вашего сертификата получателям файла не требуется.

Чтобы подготовить файл к передаче другим пользователям, выполните следующие действия:

1. Получите и установите в системное хранилище сертификаты пользователей, которым планируете передавать файлы (см. «Установка сертификатов получателей в системное хранилище» на стр. 37). С использованием данных сертификатов будет производится шифрование файлов.
2. Добавьте файл в программу ViPNet CryptoFile (см. «Добавление файлов в программу ViPNet CryptoFile» на стр. 46) либо воспользуйтесь контекстным меню Windows (см. «Работа с программой ViPNet CryptoFile с помощью контекстного меню Windows» на стр. 35).
3. Заверьте файл электронной подписью и зашифруйте его (см. «Подписание и шифрование файла» на стр. 52). Вы также можете выполнить только одну из данных операций:
   - Вы можете только подписать файл (см. «Подписание файла» на стр. 48), например, если вы хотите передать какой-либо юридически значимый документ, авторство которого необходимо подтвердить.
   - Вы можете только зашифровать файл (см. «Шифрование файла» на стр. 50), например, если вы хотите передать секретный файл, подтверждение авторства которого не требуется.
4. При необходимости передайте файл другим пользователям для добавления их электронных подписей (см. «Добавление электронных подписей к ранее подписанному файлу» на стр. 65).

5 По завершении подготовки передайте файл получателям любым удобным способом, например, по электронной почте.

6 При необходимости удалите файл из программы ViPNet CryptoFile (см. «Удаление файлов из программы ViPNet CryptoFile» на стр. 62).

7 Если из соображений безопасности вам нужно надежно удалить файл с вашего компьютера, выполните указания раздела Надежное удаление файла (на стр. 63).

---

**Совет.** Также вы можете ознакомиться с видеоруководствами по установке и работе с программой https://www.youtube.com/playlist?list=PLkF9DhEbpZWrU4vKQGLfgLpF-kfvJWYD3.

---

## Подписание файла

С помощью программы ViPNet CryptoFile вы можете заверить файл своей электронной подписью, которая подтверждает личность отправителя файла и целостность содержащихся в нем данных. Для этого выполните следующие действия:

1 В главном окне программы на панели просмотра выберите файл, который хотите подписать, и выполните одно из действий:

- На панели инструментов нажмите кнопку **Подписать**  .
- В меню **Действия** выберите пункт **Подписать**.
- Щелкните правой кнопкой мыши по выделенному файлу и выберите пункт **Подписать**.

2 Если ваш сертификат не имеет назначение **Цифровая подпись** в поле **Использование ключа**, появится сообщение о неправильном использовании сертификата. Для продолжения операции нажмите кнопку **Да**.

3 Если при подписании файла вы используете открепленную подпись, и ранее файл уже был подписан другим пользователем, то в появившемся окне выбора действия с существующим контейнером `*.sig` нажмите кнопку **Добавить подпись**.

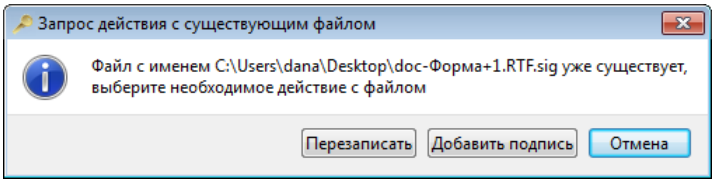


*Рисунок 12: Выбор действия с существующим файлом*

4 В окне **ViPNet CSP — пароль контейнера ключей** введите пароль доступа к контейнеру ключей и нажмите кнопку **OK**.

Если контейнер ключей хранится на внешнем устройстве, подключите это устройство к компьютеру и введите ПИН-код. Для использования внешнего устройства необходимо предварительно установить на компьютер драйверы данного устройства. Подробная информация об использовании внешних устройств хранения данных см. в приложении Информация о внешних устройствах хранения данных (на стр. 90).

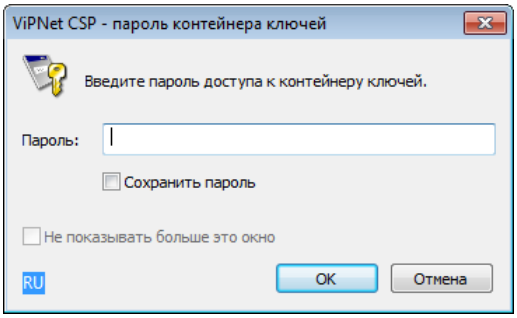


*Рисунок 13: Ввод пароля доступа к контейнеру ключей или ПИН-кода внешнего устройства*

---

**Примечание.** При использовании криптопровайдеров сторонних производителей интерфейс окна ввода пароля к контейнеру ключей имеет другой вид.

В случае использования встроенных криптопровайдеров операционной системы пароль к контейнеру ключей вводить не требуется.

---

5 В окне **Выполнение операции** будет отображаться процесс подписания файла. По завершении выполнения данной операции нажмите кнопку **Закрыть**.

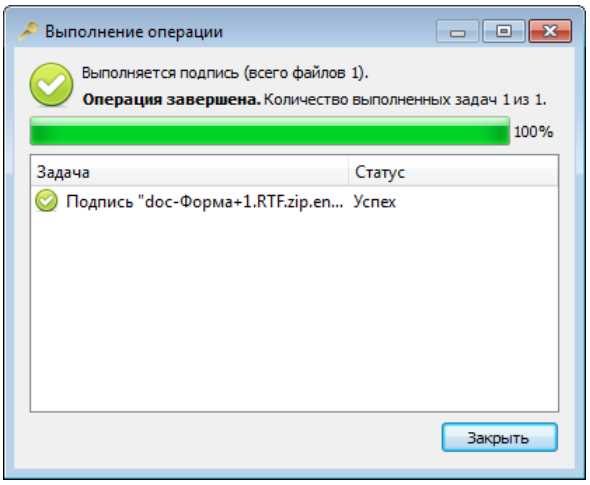


*Рисунок 14: Процесс подписания файла*

В результате файл будет заверен вашей электронной подписью и вместе с вашим сертификатом помещен в контейнер с расширением `*.sig`. Сформированный контейнер находится в той же папке, что и исходный файл. Чтобы открыть данную папку, в программе ViPNet CryptoFile щелкните правой кнопкой мыши по нужному файлу и выберите пункт **Открыть папку с файлом**.

## Шифрование файла

С помощью программы ViPNet CryptoFile вы можете зашифровать добавленный файл с использованием сертификатов получателей (одного или нескольких). Содержимое зашифрованного файла конфиденциально, и только получатель сможет ознакомиться с ним, расшифровав файл с использованием своего закрытого ключа. Если файл зашифрован с использованием нескольких сертификатов получателей, то все получатели смогут расшифровать его.

Для шифрования файла выполните следующие действия:

1. В главном окне программы на панели просмотра выберите файл, который хотите зашифровать, и выполните одно из действий:
   - На панели инструментов нажмите кнопку **Зашифровать**  .
   - В меню **Действия** выберите пункт **Зашифровать**.
   - Щелкните правой кнопкой мыши по выделенному файлу и выберите пункт **Зашифровать**.

2 Если ранее в окне **Настройки** (см. рисунок на стр. 41) был установлен флажок **Запрашивать сертификаты при шифровании**, появится окно **Сертификаты получателей**, в котором при необходимости вы можете изменить список сертификатов получателей с помощью кнопок **Добавить** и **Удалить**. Если же данный флажок не был установлен, то файл будет зашифрован с использованием сертификатов получателей, заданных ранее при настройке программы (см. «Настройка списка получателей файлов, зашифрованных с помощью программы ViPNet CryptoFile» на стр. 42).

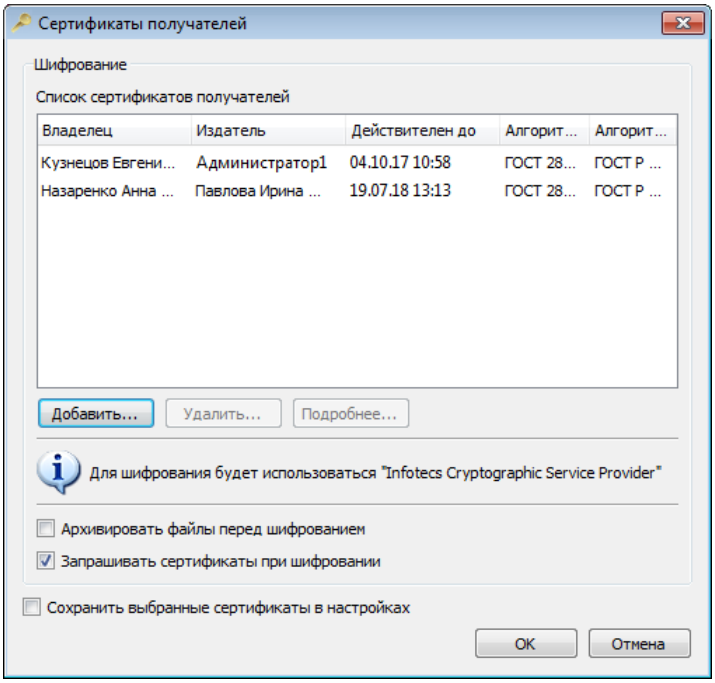


*Рисунок 15: Изменение списка сертификатов получателей*

3 Если какие-либо сертификаты получателей не имеют назначение **Шифрование данных** в поле **Использование ключа**, появится сообщение о неправильном использовании сертификатов. Для продолжения операции нажмите кнопку **Да**.

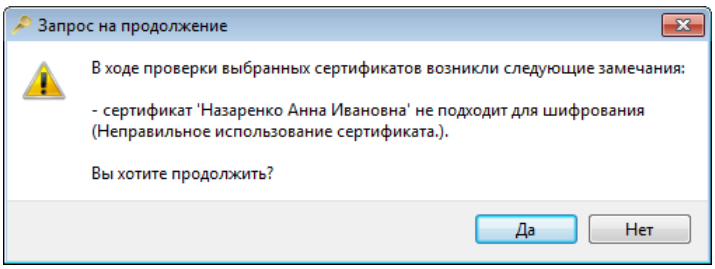


*Рисунок 16: Запрос на продолжение операции*

4 В окне **Выполнение операции** (см. рисунок на стр. 50) будет отображаться процесс шифрования файла. По окончании выполнения данной операции нажмите кнопку **Закрыть**.

В результате зашифрованный файл будет помещен в контейнер с расширением `*.enc` в ту же папку, в которой находится исходный файл. Чтобы открыть данную папку, в программе ViPNet CryptoFile щелкните правой кнопкой мыши по нужному файлу и выберите пункт **Открыть папку с файлом**.

## Подписание и шифрование файла

При необходимости вы можете одновременно заверить файл электронной подписью и зашифровать его, если хотите не только подтвердить личность отправителя, но и обеспечить конфиденциальность содержимого файла. Данная операция позволяет сэкономить время за счет одновременного шифрования и подписания файла.

Чтобы подписать и зашифровать файл, выполните следующие действия:

1 В главном окне программы на панели просмотра выберите файл, который хотите подписать и зашифровать, и выполните одно из действий:

- На панели инструментов нажмите кнопку **Подписать и зашифровать**  .
- В меню **Действия** выберите пункт **Подписать и зашифровать**.
- Щелкните правой кнопкой мыши по выделенному файлу и выберите пункт **Подписать и зашифровать**.

2 Если ранее в окне **Настройки** (см. рисунок на стр. 41) был установлен флажок **Запрашивать сертификаты при шифровании**, появится окно **Сертификаты получателей** (см. рисунок на стр. 42). В появившемся окне при необходимости измените список сертификатов получателей, с использованием которых будет зашифрован файл. Если же данный флажок не был установлен, то файл будет зашифрован с использованием сертификатов получателей, заданных ранее при настройке программы (см. «Настройка списка получателей файлов, зашифрованных с помощью программы ViPNet CryptoFile» на стр. 42).

   Затем нажмите кнопку **OK**.

3 Если ваш сертификат или какие-либо сертификаты получателей не имеют назначение **Цифровая подпись** или **Шифрование данных** в поле **Использование ключа**, появится сообщение о неправильном использовании сертификатов. Для продолжения операции нажмите кнопку **Да**.

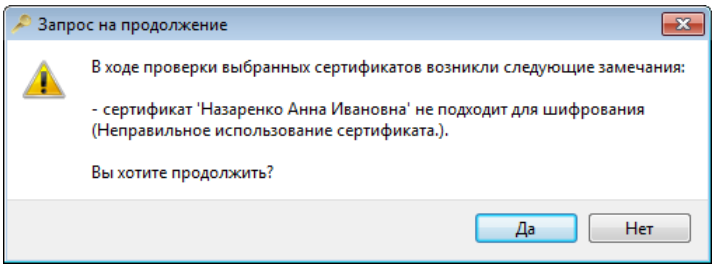


*Рисунок 17: Запрос на продолжение операции*

4 Если при подписании файла вы используете открепленную подпись, и ранее файл уже был подписан другим пользователем, то в появившемся окне выбора действия с существующим контейнером `*.sig` нажмите кнопку **Добавить подпись**.

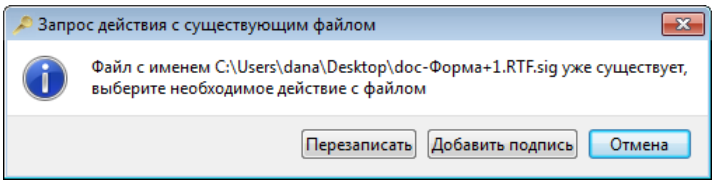


*Рисунок 18: Выбор действия с существующим файлом*

5 В окне **ViPNet CSP — пароль контейнера ключей** (см. рисунок на стр. 49) введите пароль доступа к контейнеру ключей и нажмите кнопку **OK**.

Если контейнер ключей хранится на внешнем устройстве, подключите это устройство к компьютеру и введите ПИН-код.

---

**Примечание.** При использовании криптопровайдеров сторонних производителей интерфейс окна ввода пароля к контейнеру ключей имеет другой вид.

В случае использования встроенных криптопровайдеров операционной системы пароль к контейнеру ключей вводить не требуется.

---

6 В окне **Выполнение операции** (см. рисунок на стр. 50) будет отображаться процесс подписания и шифрования файла. По завершении выполнения данной операции нажмите кнопку **Закрыть**.

В результате файл будет заверен электронной подписью и зашифрован. При этом файл будет помещен в контейнер `*.enc` в ту же папку, в которой находится исходный файл, и вы сможете передать его получателю. Чтобы открыть данную папку, в программе ViPNet CryptoFile щелкните правой кнопкой мыши по нужному файлу и выберите пункт **Открыть папку с файлом**. В случае использования открепленной подписи передайте получателю также контейнер с подписью `*.sig`.

# Обработка файлов, полученных от других пользователей

При получении файлов, имеющих стандартные расширения `*.sig` и `*.enc`, от других пользователей вы можете ознакомиться с помощью программы ViPNet CryptoFile с их содержимым и проверить авторство.

В контейнеры `*.sig` с электронной подписью (прикрепленной или открепленной) помещается также сертификаты отправителей, подписавших файлы. Поэтому для проверки подписи отдельно получать сертификаты других пользователей не требуется.

Чтобы ознакомиться с содержимым полученного файла, выполните следующие действия:

1. Добавьте файл в программу ViPNet CryptoFile (см. «Добавление файлов в программу ViPNet CryptoFile» на стр. 46) либо воспользуйтесь контекстным меню Windows (см. «Работа с программой ViPNet CryptoFile с помощью контекстного меню Windows» на стр. 35).

2. По расширению файла определите, какие операции были применены к нему перед отправкой: подписание, шифрование или одновременное подписание и шифрование. От этого зависит выбор операции, с помощью которой вы сможете ознакомиться с содержимым файла:

   - Если файл зашифрован, то есть имеет расширение `*.enc`, расшифруйте его (см. «Расшифрование файла» на стр. 55). При этом файл будет извлечен из контейнера `*.enc`.
   - Если файл был заверен электронной подписью, то есть имеет расширение `*.sig`, проверьте корректность данной подписи и извлеките файл из контейнера `*.sig` (см. «Извлечение файла из контейнера» на стр. 59).
   - Если вам не нужно извлекать файл из контейнера *.sig (например, была использована открепленная подпись (на стр. 97) и исходный файл не входит в данный контейнер), просто проверьте электронную подпись файла (см. «Проверка электронной подписи» на стр. 56).
   - Если файл подписан и зашифрован электронной подписью, то есть имеет расширение `*.sig.enc` (или другое расширение, представляющее собой сочетание расширений `*.enc`, `*.sig`, а также `*.zip` (см. «Выполнение групповых операций в программе ViPNet CryptoFile» на стр. 86)), то выполните операции расшифрования, проверки подписи и извлечения из контейнера в порядке, соответствующем последовательному раскрытию контейнеров.

Например, чтобы ознакомиться с содержимым контейнера `*.sig.zip.enc`, выполните последовательно операции: расшифрование, извлечение из контейнера. При извлечении из контейнера будет также проверена электронная подпись файла.

Также вы можете извлечь содержимое контейнера `*.sig.zip.enc` быстрее, выполнив операцию извлечения из контейнера. При этом файл будет расшифрован и извлечен из контейнера `*.enc` и архива `*.zip`, а также будет проверена электронная подпись файла.

3 При необходимости сформируйте отчет о результате проверки электронной подписи (см. «Формирование отчета о результате проверки электронной подписи» на стр. 66).

4 После прочтения при необходимости удалите файл из программы ViPNet CryptoFile (см. «Удаление файлов из программы ViPNet CryptoFile» на стр. 62).

5 Если из соображений безопасности вам нужно надежно удалить файл с вашего компьютера, выполните указания раздела Надежное удаление файла (на стр. 63).

---

**Совет.** Также вы можете ознакомиться с видеоруководствами по установке и работе с программой https://www.youtube.com/playlist?list=PLkF9DhEbpZWrU4vKQGLfgLpF-kfvJWYD3.

---

## Расшифрование файла

С помощью программы ViPNet CryptoFile вы можете расшифровать файл, полученный от другого пользователя и зашифрованный с использованием вашего сертификата. Для этого выполните следующие действия:

1 На панели просмотра выберите нужный файл (или несколько файлов) и выполните одно из действий:

- На панели инструментов нажмите кнопку **Расшифровать**  .
- В меню **Действия** выберите пункт **Расшифровать**.
- Щелкните правой кнопкой мыши по выделенному файлу и выберите пункт **Расшифровать**.

2 В окне **ViPNet CSP — пароль контейнера ключей** (см. рисунок на стр. 49) введите пароль доступа к контейнеру ключей вашей электронной подписи и нажмите кнопку **OK**.

Если контейнер ключей хранится на внешнем устройстве, подключите это устройство к компьютеру и введите ПИН-код.

**Примечание.** При использовании криптопровайдеров сторонних производителей интерфейс окна ввода пароля к контейнеру ключей имеет другой вид.

В случае использования встроенных криптопровайдеров операционной системы пароль к контейнеру ключей вводить не требуется.

3 В окне **Выполнение операции** (см. рисунок на стр. 50) будет отображаться процесс расшифрования файла. По окончании выполнения данной операции нажмите кнопку **Закрыть**.

В результате файл будет расшифрован и помещен в ту же папку, в которой находится контейнер с зашифрованным файлом. Теперь вы можете ознакомиться с содержимым данного файла.

Чтобы открыть папку, содержащую расшифрованный файл, в программе ViPNet CryptoFile щелкните правой кнопкой мыши по нужному файлу и выберите пункт **Открыть папку с файлом**.

## Проверка электронной подписи

С помощью программы ViPNet CryptoFile вы можете проверить электронную подпись файла, полученного от другого пользователя. Для этого выполните следующие действия:

1 На панели просмотра выберите нужный файл (или несколько файлов) и выполните одно из действий:

- На панели инструментов нажмите кнопку **Проверить подпись**  .
- В меню **Действия** выберите пункт **Проверить подпись**.
- Щелкните правой кнопкой мыши по выделенному файлу и выберите пункт **Проверить подпись**.

Если подписанный файл был зашифрован, в окне **ViPNet CSP — пароль контейнера ключей** (см. рисунок на стр. 49) введите пароль доступа к контейнеру ключей и нажмите кнопку **OK**. Если контейнер ключей хранится на внешнем устройстве, подключите это устройство к компьютеру и введите ПИН-код.

**Примечание.** При использовании криптопровайдеров сторонних производителей интерфейс окна ввода пароля к контейнеру ключей имеет другой вид.

В случае использования встроенных криптопровайдеров операционной системы пароль к контейнеру ключей вводить не требуется.

В окне **Выполнение операции** (см. рисунок на стр. 50) будет отображаться процесс расшифрования файла. По завершении выполнения данной операции появится окно **Результат проверки подписи**, в котором будет отображен результат проверки подписи файла.

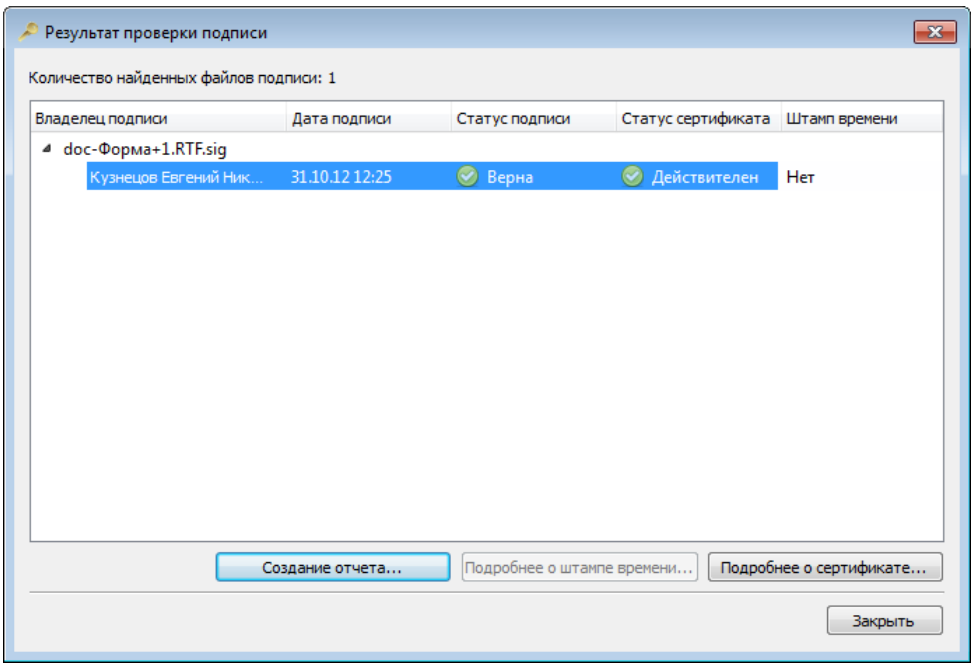


*Рисунок 19: Результат проверки подписи*

2 Чтобы просмотреть информацию о сертификате отправителя файла, в окне **Результат проверки подписи** выберите сертификат нужного пользователя и нажмите кнопку **Подробнее о сертификате**.

В окне **Результат проверки сертификата** будет отображена информация о результате проверки сертификата. Если сертификат недействителен, в поле **Подробнее** будет отображена причина недействительности сертификата.

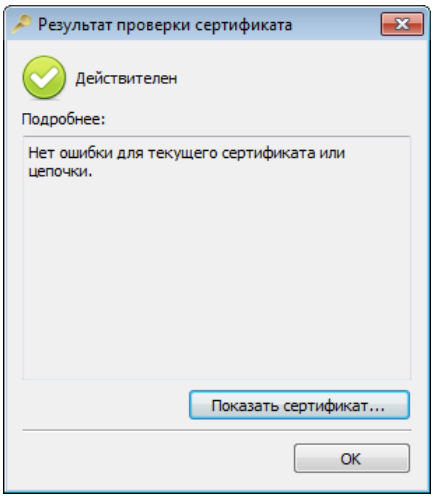


*Рисунок 20: Результат проверки сертификата*

Если вы хотите просмотреть сертификат, нажмите кнопку **Показать сертификат**.

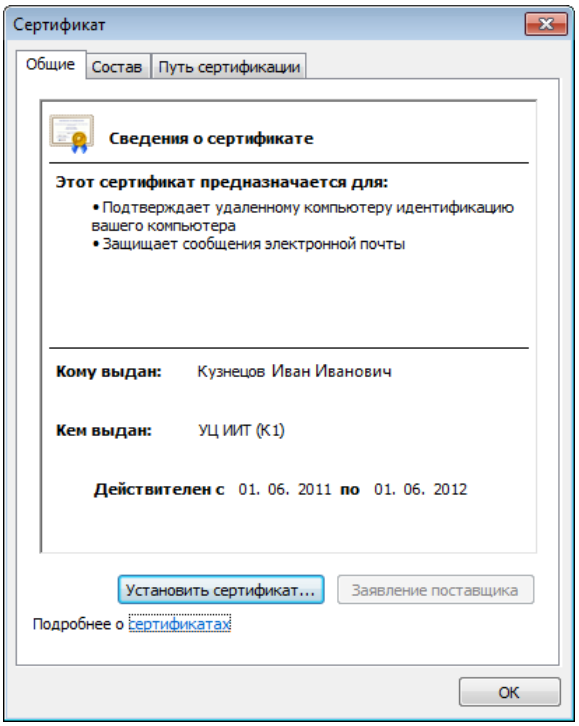


*Рисунок 21: Просмотр сертификата*

**3** Если при подписании файла был добавлен штамп точного времени, вы можете узнать подробности о данном штампе времени. Для этого в окне **Результат проверки подписи** (см. рисунок на стр. 57) выберите сертификат и нажмите кнопку **Подробнее о штампе времени**.

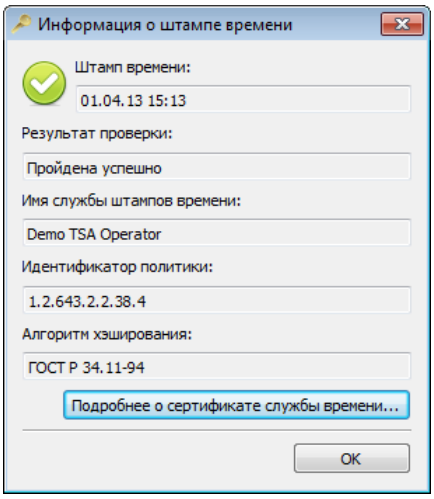


*Рисунок 22: Просмотр информации о штампе времени*

Если вы хотите просмотреть информацию о сертификате службы штампов времени (например, чтобы убедиться в действительности данного сертификата), нажмите кнопку **Подробнее о сертификате службы времени**.

## Извлечение файла из контейнера

С помощью программы ViPNet CryptoFile вы можете извлечь файл из контейнера `*.sig`, `*.enc` или архива `*.zip`, чтобы ознакомиться с его содержимым (например, если вы получили контейнер `*.sig` с подписанным документом и хотите как можно скорее ознакомиться с информацией, содержащейся в нем). При этом будет произведена проверка электронной подписи отправителя данного файла, а также расшифрование файла, если он был зашифрован. Данная функция позволяет сэкономить время за счет одновременного выполнения операций извлечения из контейнера, проверки подписи и расшифрования.

Для извлечения файла из контейнера выполните следующие действия:

1. На панели просмотра выберите нужный файл (или несколько файлов) и выполните одно из действий:

   - На панели инструментов нажмите кнопку **Извлечь и проверить подпись**  .
   - В меню **Действия** выберите пункт **Извлечь и проверить подпись**.
   - Щелкните правой кнопкой мыши по выделенному файлу и выберите пункт **Извлечь и проверить подпись**.

2 Если подписанный файл был зашифрован, в окне **ViPNet CSP — пароль контейнера ключей** (см. рисунок на стр. 49) введите пароль доступа к контейнеру ключей и нажмите кнопку **OK**.

Если контейнер ключей хранится на внешнем устройстве, подключите это устройство к компьютеру и введите ПИН-код.

---

**Примечание.** При использовании криптопровайдеров сторонних производителей интерфейс окна ввода пароля к контейнеру ключей имеет другой вид.

В случае использования встроенных криптопровайдеров операционной системы пароль к контейнеру ключей вводить не требуется.

---

В окне **Выполнение операции** (см. рисунок на стр. 50) будет отображаться процесс расшифрования файла.

3 Если извлекается подписанный файл, то будет выполнена проверка электронной подписи отправителя файла. По завершении выполнения данной операции появится окно **Результат проверки подписи** (см. рисунок на стр. 57), в котором будет отображен результат проверки подписи файла. В данном окне вы можете просмотреть подробную информацию о сертификате отправителя и о штампе точного времени. Для этого выполните действия, описанные в разделе Проверка электронной подписи (на стр. 56).

В результате файл будет извлечен из контейнера и помещен в ту же папку, где находится контейнер. Чтобы открыть данную папку, в программе ViPNet CryptoFile щелкните правой кнопкой мыши по нужному файлу и выберите пункт **Открыть папку с файлом**.


# Дополнительные возможности программы ViPNet CryptoFile

# Удаление файлов из программы ViPNet CryptoFile

Если вы закончили работу с файлом, вы можете удалить его из программы ViPNet CryptoFile (например, если в программе накопилось большое количество файлов, и вам стало трудно ориентироваться в списке файлов). При этом файл не удаляется с жесткого диска или съемного носителя.

Чтобы удалить файл из программы, выполните следующие действия:

1. В главном окне программы на панели просмотра выберите файл (или несколько файлов), который хотите удалить из программы, и выполните одно из действий:
   - На панели инструментов нажмите кнопку **Удалить файлы из списка**  .
   - В меню **Файл** выберите пункт **Удалить файлы из списка**.
   - Щелкните правой кнопкой мыши по выделенному файлу и выберите пункт **Удалить файлы из списка**.
2. В появившемся окне нажмите кнопку **Да** для подтверждения удаления файла. Для отмены удаления файла нажмите кнопку **Нет**.

В результате файл будет удален из программы. Чтобы возобновить работу с удаленным файлом, следует повторно добавить его в программу.

# Надежное удаление файла

С помощью программы ViPNet CryptoFile вы можете удалить какой-либо файл с жесткого диска или съемного носителя без возможности восстановления, например, если из соображений безопасности вы хотите безвозвратно удалить конфиденциальный файл после прочтения. Для этого выполните следующие действия:

1. В главном окне программы на панели просмотра выберите файл (или несколько файлов), который хотите надежно удалить, и выполните одно из действий:
   - На панели инструментов нажмите кнопку **Надежно удалить**  .
   - В меню **Действия** выберите пункт **Надежно удалить**.
   - Щелкните правой кнопкой мыши по выделенному файлу и выберите пункт **Надежно удалить**.
2. В появившемся окне нажмите кнопку **Да** для подтверждения удаления файла. Для отмены удаления файла нажмите кнопку **Нет**.

В результате выбранный файл будет удален с жесткого диска. Восстановление файла, удаленного таким образом, невозможно.

# Работа нескольких пользователей с программой ViPNet CryptoFile

При работе с программой ViPNet CryptoFile вы можете задать другой сертификат пользователя, от лица которого будет производиться подпись файлов. Например, если необходимо заверить файл подписями нескольких пользователей (см. «Добавление электронных подписей к ранее подписанному файлу» на стр. 65), при этом не передавая его на другие компьютеры.

Для смены сертификата текущего пользователя выполните следующие действия:

1. Установите сертификат и контейнер ключей пользователя средствами ViPNet CSP (либо встроенного криптопровайдера или криптопровайдера стороннего производителя). См. документ «ViPNet CSP. Руководство пользователя», глава «Установка контейнеров и сертификатов».
2. В главном окне программы ViPNet CryptoFile выполните одно из действий:
   - На панели инструментов нажмите кнопку **Настройки**  .
   - В меню **Файл** выберите пункт **Настройки**.
3. В окне **Настройки** в группе **Подпись** нажмите кнопку **Изменить**, чтобы задать сертификат другого пользователя, с помощью которого будет производиться подпись файлов.
4. В окне **Безопасность Windows** выберите нужный сертификат и нажмите кнопку **OK**.

   В окне **Настройки** в группе **Подпись** отобразится информация о заданном сертификате.

В результате будет задан нужный сертификат, и его владелец сможет приступить к работе с программой ViPNet CryptoFile (см. «Работа с программой ViPNet CryptoFile» на стр. 45).

# Добавление электронных подписей к ранее подписанному файлу

С помощью программы ViPNet CryptoFile вы можете добавлять свою электронную подпись к подписям других пользователей, содержащимся в контейнере `*.sig`. Например, если необходимо заверить какой-либо юридический документ подписями нескольких пользователей, и затем передать его в другую организацию. Выполнение данной операции возможно только в случае использования открепленной подписи. Для добавления электронной подписи в контейнер `*.sig` выполните следующие действия:

1. Добавьте исходный файл и контейнер `*.sig` в программу ViPNet CryptoFile (см. «Добавление файлов в программу ViPNet CryptoFile» на стр. 46).
2. Заверьте исходный файл электронной подписью (см. «Подписание файла» на стр. 48). Перед этим убедитесь, что в настройках программы снят флажок **Использовать прикрепленную подпись** (см. «Задание сертификата пользователя для подписи файлов» на стр. 39), то есть при подписании будет использоваться открепленная подпись.
3. В появившемся окне выбора действия с существующим контейнером `*.sig` нажмите кнопку **Добавить подпись**.

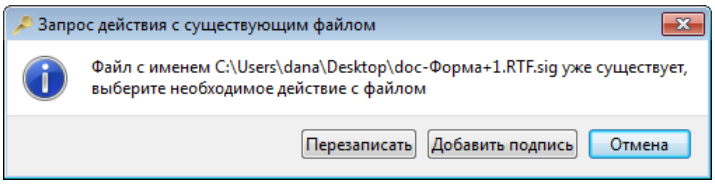


*Рисунок 23: Выбор действия с существующим файлом*

В результате подпись будет добавлена в контейнер `*.sig` с открепленной подписью. Теперь при проверке подписи исходного файла в окне **Результат проверки подписи** (см. рисунок на стр. 57) будут отображаться результаты проверки всех добавленных подписей.

# Формирование отчета о результате проверки электронной подписи

С помощью программы ViPNet CryptoFile вы можете сформировать отчет о результате проверки электронной подписи. Такой отчет содержит информацию о сертификате отправителя файла, времени и корректности подписи, о сертификате службы штампов времени (если к электронной подписи был добавлен штамп времени) и может быть использован при разборе конфликтных ситуаций (например, для подтверждения существования файла в момент подписи).

Чтобы сформировать отчет о результате проверки электронной подписи файла, выполните следующие действия:

1. Выполните проверку электронной подписи файла (см. «Проверка электронной подписи» на стр. 56).
2. В окне **Результат проверки подписи** нажмите кнопку **Создание отчета**. При этом сформированный отчет будет открыт в браузере, который используется по умолчанию.

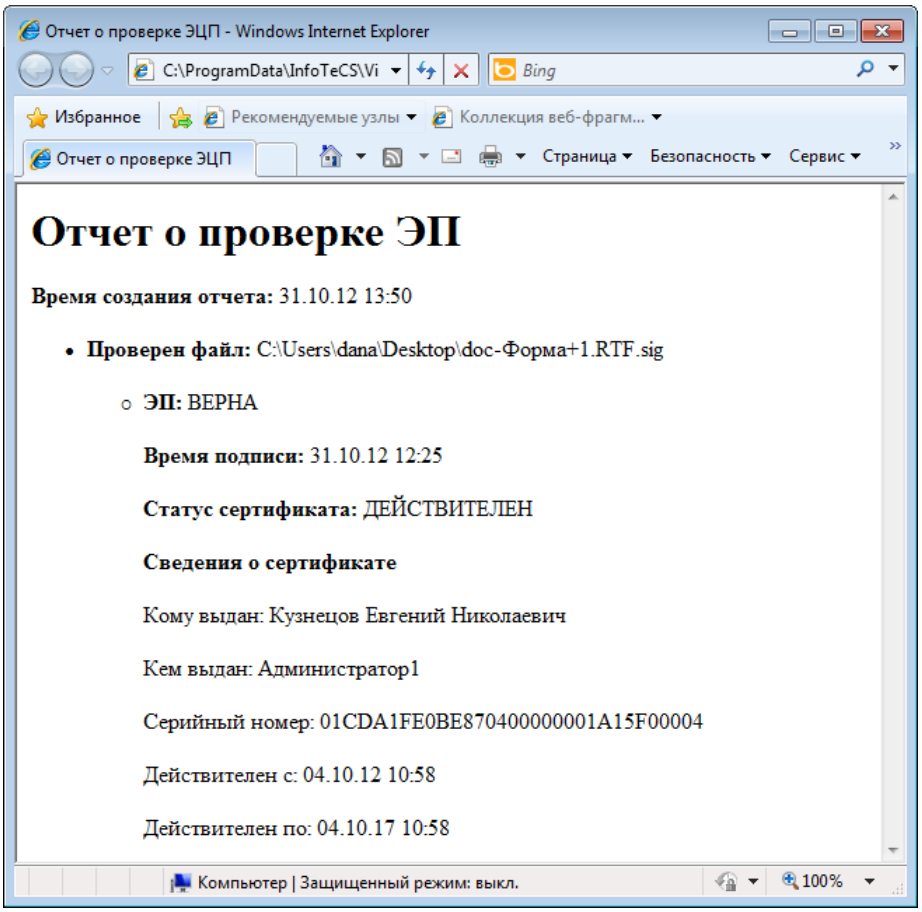


*Рисунок 24: Просмотр отчета о результате проверки электронной подписи*


# Регистрация ViPNet CryptoFile

# Прежде чем регистрировать ViPNet CryptoFile

## Зачем нужно регистрировать ViPNet CryptoFile

В случае использования криптопровайдеров сторонних производителей после установки ViPNet CryptoFile на компьютер программа работает в демо-режиме (см. «Ограничения незарегистрированной версии программы ViPNet CryptoFile» на стр. 11). Зарегистрировать программу ViPNet CryptoFile можно в любой момент, и тогда полнофункциональная версия программы будет доступна неограниченное время.

Мы рекомендуем поступить следующим образом:

- установите ViPNet CryptoFile и пользуйтесь незарегистрированной версией программы, чтобы оценить возможности и преимущества продукта;
- чтобы работать с полной версией, зарегистрируйте вашу копию ViPNet CryptoFile.

Также вы можете бесплатно загрузить, установить и зарегистрировать ПО ViPNet CSP, при этом регистрация программы ViPNet CryptoFile не потребуется. Для этого при запуске незарегистрированной версии программы ViPNet CryptoFile выберите пункт **Открыть страницу загрузки и регистрации ViPNet CSP**.

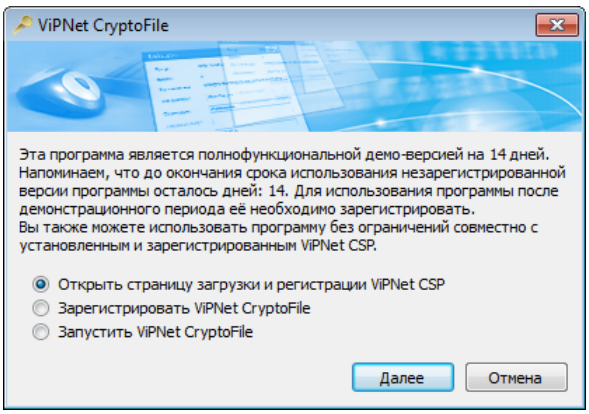


*Рисунок 25: Запуск незарегистрированной версии ViPNet CryptoFile*

## Начало регистрации

Вы можете зарегистрировать ViPNet CryptoFile самостоятельно (обычная регистрация). Для этого следуйте приведенным ниже указаниям.

Если вы системный администратор и хотите одновременно зарегистрировать несколько копий программы, вы можете использовать возможность регистрации через файл, чтобы собрать запросы на регистрацию от всех пользователей, отправить их в одном сообщении электронной почты и получить все регистрационные коды одновременно. Подробнее см. раздел Порядок действий системного администратора при регистрации через файл.

---

**Примечание.** Если программа ViPNet CryptoFile повторно установлена на компьютер, на котором она уже была зарегистрирована, вы можете использовать регистрационные данные, сохраненные в файле `*.brg` (см. «Сохранение регистрационных данных» на стр. 84).

Если вы провели обновление конфигурации компьютера, на котором будете использовать ViPNet CryptoFile, ознакомьтесь с разделом Если конфигурация вашего компьютера изменилась (на стр. 84).

---

Чтобы зарегистрировать ViPNet CryptoFile, выполните следующие действия:

1 В главном окне программы ViPNet CryptoFile в меню **Справка** выберите пункт **Регистрация**. Будет запущен мастер **Регистрация ViPNet CryptoFile**.

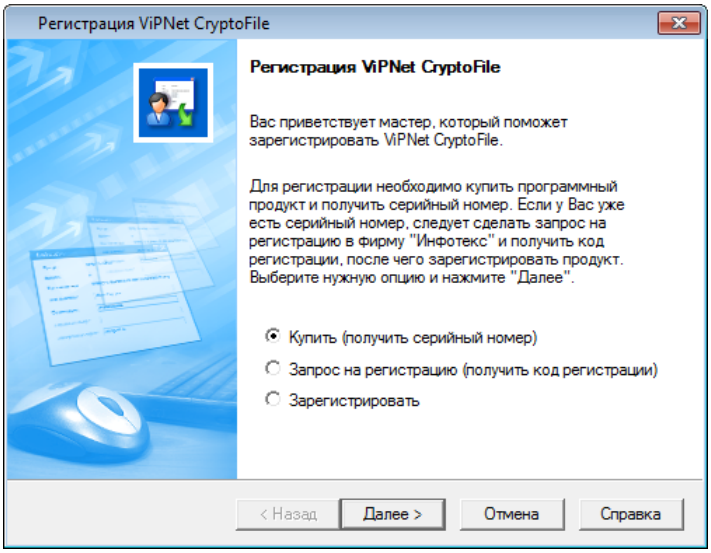


*Рисунок 26: Мастер регистрации ViPNet CryptoFile*

2 Если перед этим:

- вы не приобрели ViPNet CryptoFile, выберите **Купить (получить серийный номер)** (см. «Получение серийного номера» на стр. 72).

**Примечание.** Если вы приобрели программу ViPNet CryptoFile на компакт-диске, у вас уже есть серийный номер (он включен в комплект вместе с компакт-диском) и вы можете перейти к запросу кода регистрации (см. ниже).

- вы уже приобрели ViPNet CryptoFile и имеете серийный номер, выберите **Запрос на регистрацию (получить код регистрации)** (см. «Получение кода регистрации» на стр. 73).

**Примечание.** Если вы сделаете запрос на регистрацию через Интернет, регистрация ViPNet CryptoFile будет проведена автоматически без вашего участия.

- вы уже приобрели ViPNet CryptoFile и получили код регистрации, выберите **Зарегистрировать** (см. «Регистрация ViPNet CryptoFile» на стр. 82).

**3** Нажмите кнопку **Далее**.

# Получение серийного номера

Для получения серийного номера:

1. На странице **Регистрация ViPNet CryptoFile** выберите **Купить (получить серийный номер)** и нажмите кнопку **Далее**.

   В окне вашего браузера откроется страница заказа продуктов ViPNet на сайте компании ОАО «ИнфоТеКС». Приобретите ViPNet CryptoFile через веб-сайт и получите серийный номер по электронной почте.

2. Получив серийный номер, вернитесь на страницу **Регистрация ViPNet CryptoFile** (см. «Начало регистрации» на стр. 70) и сделайте запрос на получение кода регистрации (см. «Получение кода регистрации» на стр. 73).

# Получение кода регистрации

Чтобы запросить код регистрации для ViPNet CryptoFile:

1. На странице **Регистрация ViPNet CryptoFile** выберите **Запрос на регистрацию (получить код регистрации)** и нажмите кнопку **Далее**.
2. На странице **Способ запроса на регистрацию** выберите подходящий для вас способ. Для этого установите переключатель в одно из положений:
   - **Через Интернет (online)** (см. «Получение кода регистрации через Интернет» на стр. 74).
   - **По электронной почте** (см. «Получение кода регистрации по электронной почте» на стр. 76).
   - **По телефону** (см. «Получение кода регистрации по телефону» на стр. 78).
   - **Через файл** (см. «Регистрация через файл» на стр. 79).

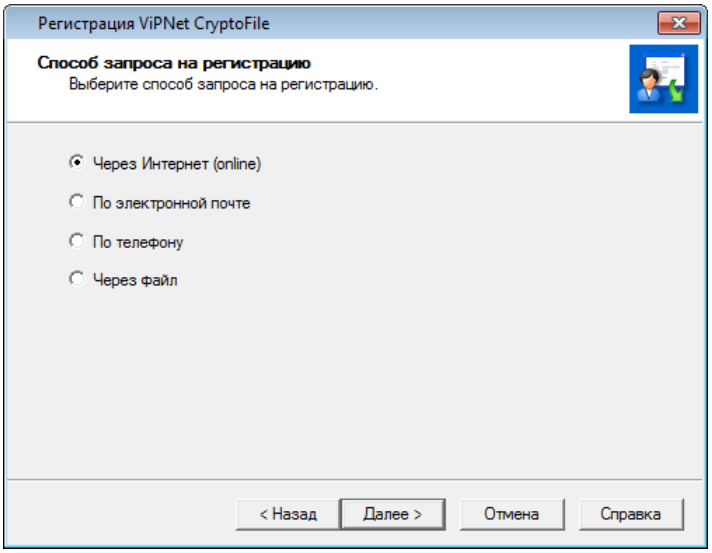


*Рисунок 27: Выбор способа регистрации*

3. Нажмите кнопку **Далее**.

## Получение кода регистрации через Интернет

**Внимание!** Для данного способа регистрации необходим доступ в Интернет.

Если вы выбрали способ регистрации **Через Интернет (online)**, откроется страница **Регистрационные данные**.

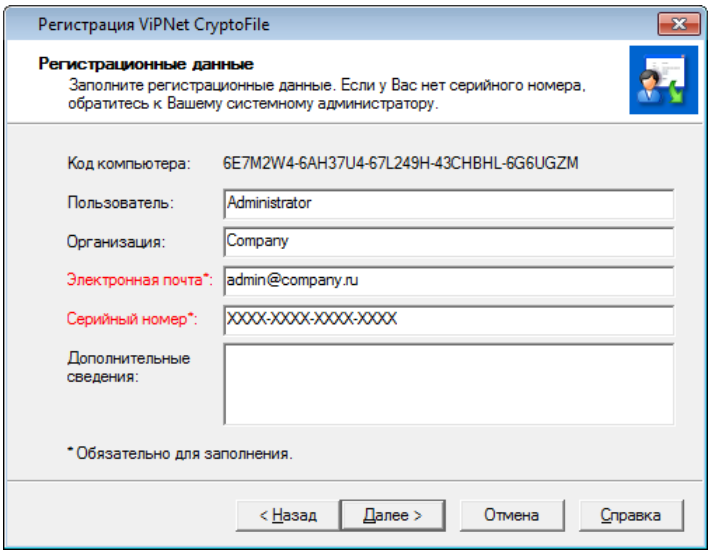


*Рисунок 28: Страница регистрационных данных*

На странице **Регистрационные данные**:

1 В поле **Серийный номер** введите серийный номер.

**Примечание.** Если у вас нет серийного номера, сделайте запрос на его получение (см. «Получение серийного номера» на стр. 72).

Если вы вводили серийный номер раньше, поле **Серийный номер** будет заполнено автоматически.

2 В поле **Пользователь** введите ваше имя. Оно будет использоваться при выпуске лицензии и для обращения к вам. Заполнение этого поля необязательно. По умолчанию в поле **Пользователь** отображается имя, которое вы ввели во время установки ViPNet CryptoFile.

3 В поле **Организация** введите название вашей организации. Заполнение этого поля необязательно. По умолчанию в поле **Организация** отображается название, которое вы ввели во время установки ViPNet CryptoFile.

4 В поле **Электронная почта** введите ваш адрес электронной почты, который будет использован для связи с вами в случае необходимости.

---

**Внимание!** Мы не будем продавать или распространять ваш адрес электронной почты. ОАО «ИнфоТеКС» ответственно подходит к защите вашей личной информации и принимает все меры для предотвращения несанкционированного доступа или разглашения информации, которую вы нам предоставляете.

---

5 В поле **Дополнительные сведения** вы можете указать любую дополнительную информацию. Например, ваши контактные данные, сообщение о возникшей проблеме или пожелания, касающиеся программного обеспечения ViPNet.

В поле **Код компьютера** отображается код, который однозначно идентифицирует ваш компьютер. Вы не можете изменить значение этого поля.

6 Нажмите кнопку **Далее**. Откроется страница, отображающая состояние запроса на регистрацию. На этой странице ведется отсчет времени с начала текущей попытки регистрации. Обратите внимание, что на установление соединения с сервером отводится не более 3-х минут.

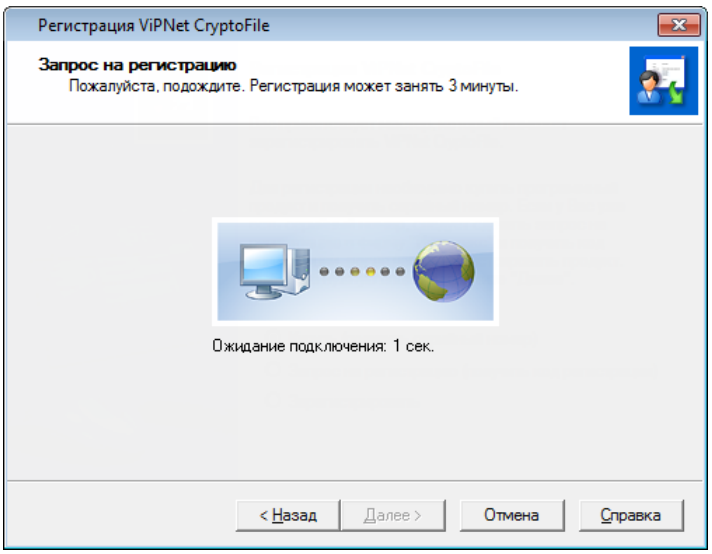


*Рисунок 29: Подключение к серверу*

Если в течение 3-х минут соединение с сервером системы регистрации ОАО «ИнфоТеКС» не было установлено, вы увидите соответствующее сообщение.

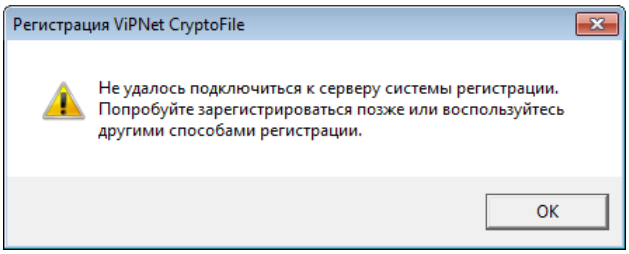


*Рисунок 30: Ошибка подключения*

Если соединение с сервером системы регистрации установлено успешно, но предоставленные вами данные оказались неверными, программа выдаст сообщение об этом.

В окне сообщения нажмите **OK**, и вы вернетесь на страницу **Регистрационные данные**.

Если вам отказано в регистрации, откроется страница **Регистрационные данные**. Проверьте правильность введенного серийного номера и попробуйте зарегистрироваться снова.

Если регистрация прошла успешно, откроется страница **Регистрация ViPNet CryptoFile успешно завершена**. На этой странице дана рекомендация, как безопасно сохранить ваши регистрационные данные (см. «Сохранение регистрационных данных» на стр. 84).

7 Нажмите кнопку **Готово**.

## Получение кода регистрации по электронной почте

**Внимание!** Для данного способа регистрации необходим доступ в Интернет.

Если вы выбрали способ регистрации **По электронной почте**, откроется страница **Регистрационные данные**. На этой странице:

1 Введите все данные, как описано в разделе Получение кода регистрации через Интернет (на стр. 74).

2 Нажмите кнопку **Далее**. В вашей почтовой программе будет создано новое сообщение электронной почты, содержащее указанные вами регистрационные данные. Сообщение будет адресовано на электронный почтовый ящик reg@infotecs.biz.

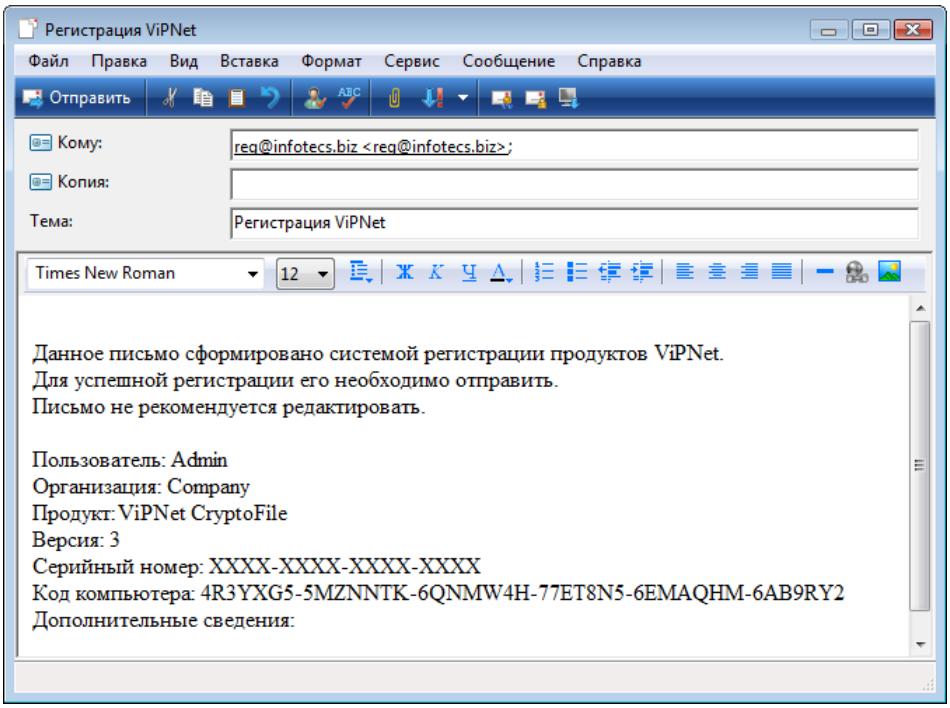


*Рисунок 31: Запрос кода регистрации по электронной почте*

**Внимание!** Мы не рекомендуем редактировать сообщение с регистрационными данными.

3 Для завершения регистрации отправьте это сообщение. После проверки ваших регистрационных данных вы получите код регистрации по электронной почте.

**Внимание!** Если в течение нескольких дней вы не получили ответ от компании «ИнфоТеКС», попытайтесь снова отправить свое сообщение. Для этого повторите все шаги, описанные в данном разделе. Если после этого вам все же не удалось зарегистрировать ViPNet CryptoFile, обратитесь в службу поддержки ОАО «ИнфоТеКС».

4 Получив сообщение с кодом регистрации, зарегистрируйте вашу копию ViPNet CryptoFile (см. «Регистрация ViPNet CryptoFile» на стр. 82).

## Получение кода регистрации по телефону

Если вы выбрали способ регистрации **По телефону**, откроется страница **Запрос на регистрацию по телефону**, содержащая данные, которые вы должны будете сообщить сотруднику ОАО «ИнфоТеКС».

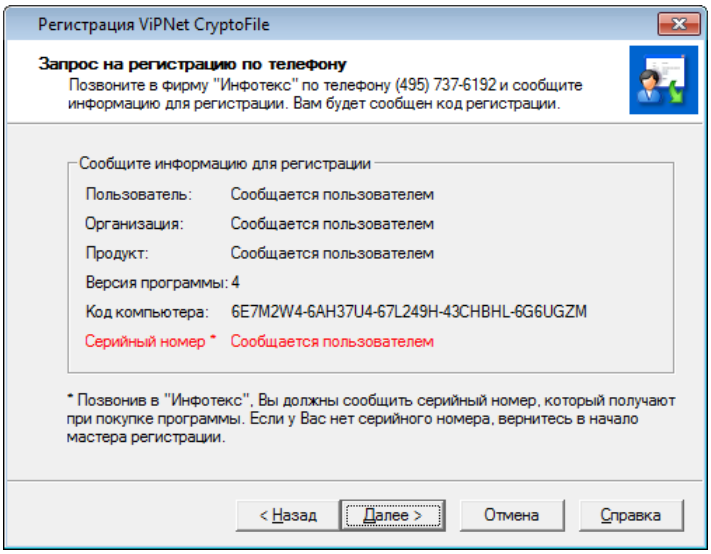


*Рисунок 32: Запрос кода регистрации по телефону*

Выполните следующие действия:

1. Позвоните в ОАО «ИнфоТеКС» по телефону, приведенному в верхней части страницы, и сообщите регистрационную информацию**.** В ответ вам будет сообщен код регистрации.

2. Получив код регистрации, нажмите кнопку **Далее**, откроется страница **Зарегистрировать**.

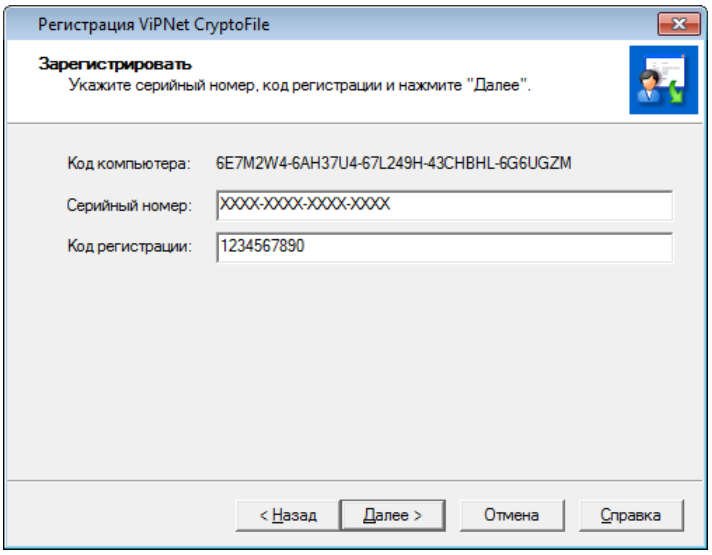


*Рисунок 33: Ввод кода регистрации*

3 На странице **Зарегистрировать** введите ваши серийный номер и код регистрации, затем нажмите кнопку **Далее**.

**Примечание.** Если вы вводили серийный номер раньше, поле **Серийный номер** будет заполнено автоматически.

Если введенные данные верны, откроется страница **Регистрация ViPNet CryptoFile успешно завершена**. На этой странице приведены рекомендации, как безопасно сохранить ваши регистрационные данные (см. «Сохранение регистрационных данных» на стр. 84).

4 Нажмите кнопку **Готово**.

## Регистрация через файл

Смысл регистрации через файл состоит в том, что вы перекладываете ответственность за получение кода регистрации на своего системного администратора. Вам не нужно лично запрашивать код регистрации у компании «ИнфоТеКС». Вместо этого вы должны воспользоваться мастером **Регистрация ViPNet CryptoFile** для формирования файла регистрационных данных и передать файл вашему системному администратору.

**Примечание.** Если требуется провести регистрацию через файл только одной копии программы ViPNet CryptoFile, сначала выполните действия 1–6, описанные в данном разделе, затем выполните действия системного администратора из

раздела Порядок действий системного администратора при регистрации через файл. После этого выполните действие 7 данного раздела, зарегистрировав свою копию ViPNet CryptoFile (см. «Регистрация ViPNet CryptoFile» на стр. 82).

После того как администратор получает регистрационные данные от вас и от других пользователей ViPNet, он запрашивает коды регистрации и сообщает их пользователям. Получив от вашего системного администратора код регистрации, вы можете зарегистрировать ViPNet CryptoFile.

Чтобы воспользоваться регистрацией через файл:

1. На странице **Способ запроса на регистрацию** выберите **Через файл** и нажмите кнопку **Далее**.
2. На странице **Регистрационные данные** введите все данные, как описано в разделе Получение кода регистрации через Интернет (на стр. 74). Нажмите кнопку **Далее**.
3. На странице **Сохранение регистрационных данных** нажмите кнопку **Обзор** и укажите папку, в которой будет сохранен файл с вашими регистрационными данными.

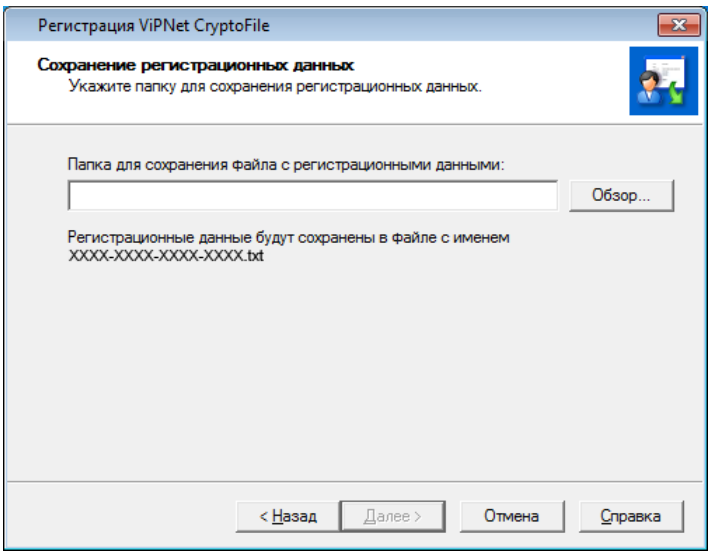


*Рисунок 34: Сохранение данных для групповой регистрации*

4. Указав папку, нажмите кнопку **Далее**. Регистрационные данные будут сохранены в текстовом файле, имя которого совпадает с вашим серийным номером: `<серийный номер>.txt`.

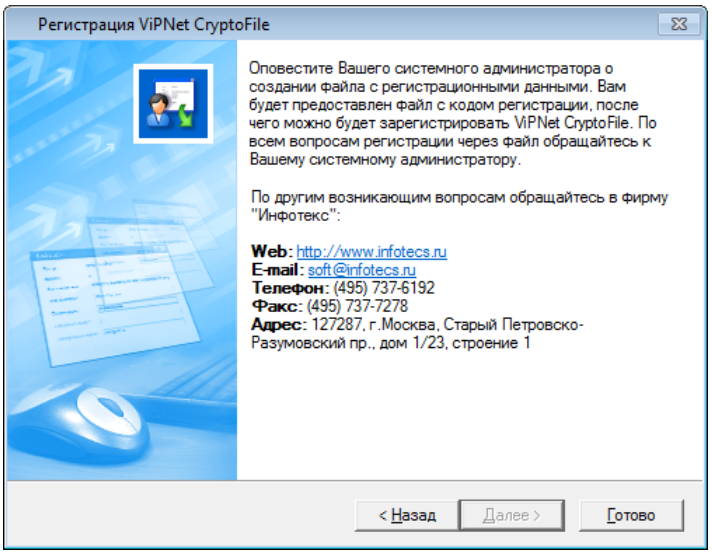


*Рисунок 35: Данные для групповой регистрации сохранены*

5 На следующей странице мастера нажмите кнопку **Готово**.

6 Передайте файл, содержащий регистрационные данные, своему системному администратору.

7 Получив от администратора код регистрации, зарегистрируйте свою копию ViPNet CryptoFile (см. «Регистрация ViPNet CryptoFile» на стр. 82).

# Регистрация ViPNet CryptoFile

Получив от ОАО «ИнфоТеКС» код регистрации, вы можете зарегистрировать вашу копию ViPNet CryptoFile. Для этого:

1 Запустите мастер **Регистрация ViPNet CryptoFile** (см. «Начало регистрации» на стр. 70).

2 На первой странице мастера выберите **Зарегистрировать** и нажмите кнопку **Далее**.

3 На странице **Серийный номер** введите ваш серийный номер и нажмите кнопку **Далее**.

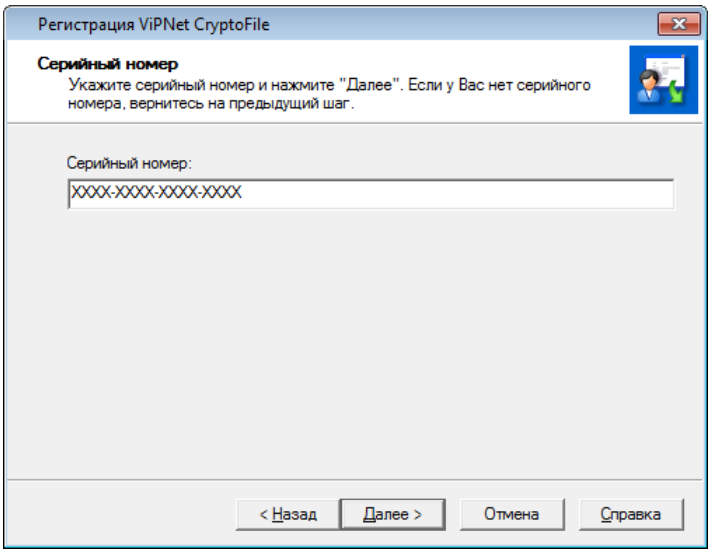


*Рисунок 36: Ввод серийного номера*

**Примечание.** Если вы вводили серийный номер раньше, поле **Серийный номер** будет заполнено автоматически.

4 На странице **Код регистрации**:

- Если вы запрашивали код регистрации лично, выберите **Обычная регистрация** и введите код регистрации.

- Если запрос на регистрацию делал ваш системный администратор, выберите **Регистрация через файл**, затем нажмите кнопку **Обзор** и укажите путь к файлу, содержащему код регистрации.

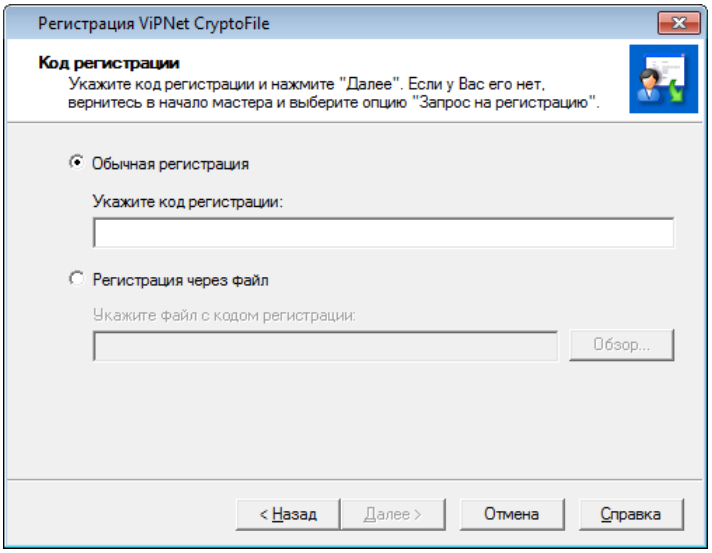


*Рисунок 37: Ввод кода регистрации*

5 Нажмите кнопку **Далее**. Если указанные вами данные верны, откроется страница **Регистрация ViPNet CryptoFile успешно завершена**.

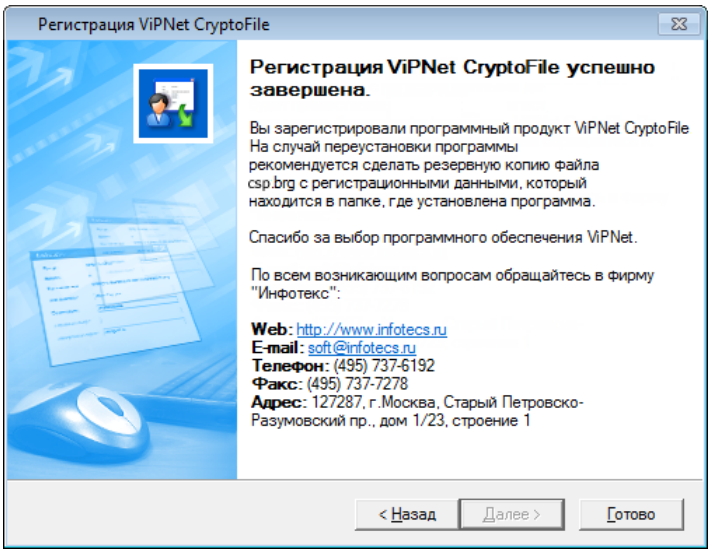


*Рисунок 38: Завершение регистрации ViPNet CryptoFile*

6 Нажмите кнопку **Готово**.

7 Сохраните регистрационные данные (см. «Сохранение регистрационных данных» на стр. 84), скопировав в надежное место файл `*.brg`, находящийся в папке установки программы ViPNet CryptoFile.

## Сохранение регистрационных данных

После завершения регистрации программа сохраняет регистрационные данные в файле `*.brg`, который создается в папке:

- `C:\ProgramData\InfoTeCS\ViPNet CryptoFile\`, если используется операционная система Windows Vista, Windows 7, Windows Server 2008, Windows 8 или Windows Server 2012;
- `C:\Documents and Settings\All Users\Application Data\InfoTeCS\ViPNet CryptoFile\`, если используется операционная система Windows XP или Windows Server 2003.

**Примечание.** Имя файла `*.brg` зависит от версии программного обеспечения ViPNet.

Мы рекомендуем скопировать файл регистрационных данных в надежное место, так как он может быть полезен при повторной установке ViPNet CryptoFile (например, если вы хотите переустановить программу в другую папку или снова установить программу после форматирования жесткого диска). В таких случаях следует завершить работу с программой, поместить сохраненный файл `*.brg` в папки, указанные выше, и заново запустить программу. После запуска программа ViPNet CryptoFile будет автоматически зарегистрирована (если регистрационные данные верны и конфигурация компьютера не изменилась).

Данные о регистрации (серийный номер, код компьютера и так далее) также сохраняются в протоколе регистрации `reginfo.txt`, который хранится в папке установки ViPNet CryptoFile. Вы можете использовать содержащиеся в этом файле данные, чтобы вручную зарегистрировать программу после переустановки (например, если файл `*.brg` потерян).

## Если конфигурация вашего компьютера изменилась

Обновление конфигурации компьютера, на котором установлена программа ViPNet CryptoFile, может сказаться на ее работе. Если изменение конфигурации было значительным (вы заменили большую часть комплектующих), необходимо перерегистрировать вашу копию ViPNet CryptoFile (см. «Получение кода регистрации»

на стр. 73). Если изменения в конфигурации были небольшими, вам не нужно снова регистрировать ViPNet CryptoFile.

При первом запуске ViPNet CryptoFile после небольшого обновления конфигурации программа выдаст сообщение о том, что в связи с изменением конфигурации компьютера был создан новый файл `*.brg`. Это значит, что прежний файл регистрационных данных устарел, и вы не можете использовать его для регистрации программы после переустановки.

Скопируйте новый файл `*.brg` в надежное место. Если вы переустановите ViPNet CryptoFile, вам нужно будет скопировать этот файл в папку установки ViPNet CryptoFile, и программа будет зарегистрирована.


# Выполнение групповых операций в программе ViPNet CryptoFile

С помощью программы ViPNet CryptoFile вы можете выполнять операции как с одиночными файлами, так и с группами файлов. При этом в зависимости от настроек программы (см. «Настройка программы ViPNet CryptoFile» на стр. 39) в результате выполнения операций подписания и шифрования могут быть получены различные виды файлов.

В таблице ниже представлены результаты выполнения операций **Подписать**, **Зашифровать** и **Подписать и зашифровать** в зависимости от количества файлов, применения архивирования и использования прикрепленной либо открепленной подписи.

*Таблица 6. Результаты подписания или шифрования файлов*

| Выполняемая операция | Количество обрабатываемых файлов | Архивирование файлов перед шифрованием | Тип подписи | Результат |
|---|---|---|---|---|
| Подписать | 1 | Не используется | Прикрепленная | Контейнер `*.sig` с прикрепленной подписью и исходным файлом |

| Выполняемая операция | Количество обрабатываемых файлов | Архивирование файлов перед шифрованием | Тип подписи | Результат |
|---|---|---|---|---|
| | | Не используется | Открепленная | Контейнер `*.sig` с открепленной подписью (исходный файл в контейнер не входит) |
| | Больше 1 (групповая операция) | Не используется | Прикрепленная | Группа контейнеров `*.sig` с прикрепленными подписями и исходными файлами |
| | | Не используется | Открепленная | Группа контейнеров `*.sig` с открепленными подписями (исходные файлы в контейнеры не входят) |
| Зашифровать | 1 | Нет | Не используется | Контейнер `*.enc` с зашифрованным файлом |
| | | Да | Не используется | Контейнер `*.zip.enc` с зашифрованным архивом, в который был помещен исходный файл |
| | Больше 1 (групповая операция) | Нет | Не используется | Группа контейнеров `*.enc` с зашифрованными файлами |
| | | Да | Не используется | Контейнер `*.zip.enc` с зашифрованным архивом, в который были помещены исходные файлы |
| Подписать и зашифровать | 1 | Нет | Прикрепленная | Контейнер `*.sig.enc`, внутри которого зашифрованный контейнер `*.sig` с прикрепленной подписью и исходным файлом |

| Выполняемая операция | Количество обрабатываемых файлов | Архивирование файлов перед шифрованием | Тип подписи | Результат |
|---|---|---|---|---|
| | | Нет | Открепленная | Контейнер `*.sig` с открепленной подписью и контейнер `*.enc` с зашифрованным исходным файлом |
| | | Да | Прикрепленная | Контейнер `*.sig.zip.enc` с зашифрованным архивом, внутри которого контейнер `*.sig` с прикрепленной подписью и исходным файлом |
| | | Да | Открепленная | Контейнер `*.sig.zip.enc` с зашифрованным архивом, внутри которого исходный файл и контейнер `*.sig` с открепленной подписью |
| | Больше 1 (групповая операция) | Нет | Прикрепленная | Группа контейнеров `*.sig.enc`, в каждом из которых зашифрованный контейнер `*.sig` с прикрепленной подписью и исходным файлом |
| | | Нет | Открепленная | На основе каждого из исходных файлов будет создано по два контейнера: контейнер `*.sig` с открепленной подписью и контейнер `*.enc` с зашифрованным исходным файлом |

| Выполняемая операция | Количество обрабатываемых файлов | Архивирование файлов перед шифрованием | Тип подписи | Результат |
|---|---|---|---|---|
| | | Да | Прикрепленная | Контейнер `*.zip.enc` с зашифрованным архивом, внутри которого группа контейнеров `*.sig` с прикрепленными подписями и исходными файлами |
| | | Да | Открепленная | Контейнер `*.zip.enc` с зашифрованным архивом, внутри которого исходные файлы и группа контейнеров `*.sig` с открепленными подписями |

Обратные операции проверки подписи и расшифрования выполняются в соответствии со следующими правилами:

- Операция **Расшифровать** выполняется только для контейнеров `*.enc` с зашифрованными файлами, архивами или контейнерами.
- Операция **Проверить подпись** выполняется для контейнеров `*.enc` и `*.sig` и архивов, в которых содержатся подписанные файлы. При этом исходные файлы из контейнеров и архивов не извлекаются.
- Операция **Извлечь и проверить подпись** выполняется для контейнеров `*.enc` и `*.sig`, а также для архивов. Если контейнеры или архивы не содержат подписанные файлы, будет производиться только извлечение исходных файлов без проверки электронной подписи.


# Информация о внешних устройствах хранения данных

В ПО ViPNet для записи и считывания персональной информации (паролей, ключей и так далее) имеется возможность использовать различные внешние устройства хранения данных.

**Внимание!** Хранение персональных ключей нескольких пользователей на одном устройстве невозможно. Однако возможно хранение нескольких контейнеров ключей (см. «Контейнер ключей» на стр. 97) на одном устройстве.

Перед записью ключей на устройство убедитесь, что устройство отформатировано.

Ниже в таблице перечислены устройства и ключи, с которыми может работать ПО ViPNet. Приведенная таблица содержит следующие данные:

- в столбце **Тип устройства** представлены все типы устройств считывания, доступные для выбора в ПО ViPNet;
- в столбце **Тип ключа** представлены типы ключей, используемые для данных устройств;
- в столбце **Необходимые условия работы с ключом** описаны необходимые условия и важные моменты для использования каждого ключа;

- в последнем столбце содержится информация о поддержке стандарта PKCS#11.

**Примечание.** Стандарт PKCS#11 (также известный как Cryptoki) — один из стандартов семейства PKCS (Public Key Cryptography Standards — криптографические стандарты открытого ключа), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

*Таблица 7. Поддерживаемые внешние устройства*

| Тип устройства | Тип ключа | Необходимые условия работы с ключом | Поддержка стандарта PKCS#11 |
|---|---|---|---|
| **eToken Aladdin** | **eToken PRO**, персональные электронные ключи, eToken PRO (Java), eToken PRO, смарт-карты eToken PRO (Java), eToken PRO компании «Аладдин Р.Д.» | На компьютере должно быть установлено программное обеспечение PKI Client версии 5.1 и выше.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2.<br>**Примечание:** Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым USB-устройством считывания с карт. | Да |
| **iButton Aladdin** | **iButton (Dallas)**, электронные ключи iButton типа DS1993, DS1994, DS1995 и DS1996 | К компьютеру должно быть подключено устройство считывания.<br>На компьютере должно быть установлено программное обеспечение обмена информации с iButton — 1-Wire Drivers версии 3.20 либо версии 4.0.3.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная).<br>**Примечание:** На ОС Windows XP и Server 2003 совместно с ПО ViPNet может использоваться только ПО 1-Wire Drivers версии 3.20. | Нет |
| **Smartcard Athena** | Смарт-карты с памятью типа I2C | Чтение и запись на смарт-карту осуществляется через считыватель | Нет |

| | | | |
|---|---|---|---|
| | (ASE M4), синхронные смарт-карты с шиной 2/3 и защищенной памятью, удовлетворяющие стандарту ISO7816-3 (ASE MP42) | ASEDrive III PRO-S компании Athena.<br>На компьютере должны быть установлены драйверы версии 2.5.0.0.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная). | |
| **SmartCard RIK** | **Российская интеллектуальная карта** компании «Атлас-Телеком» | Работа с картой ПО ViPNet может производиться через любой PC/SC-совместимый считыватель. | Нет |
| **Shipka** | **ПСКЗИ ШИПКА** компании ОКБ САПР | Перед началом работы с устройством ШИПКА убедитесь, что на компьютере установлено программное обеспечение ACShipka Environment версии не ниже 3.3.2.6.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная). Проведите инициализацию устройства при помощи утилиты производителя «Параметры авторизации». | Да |
| **ruToken** | **Rutoken S**, электронный идентификатор компании «Актив» | На компьютере должны быть установлены драйверы Rutoken версии 2.81.00.0424.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная). | Да |
| **ruToken ECP** | **Rutoken ЭЦП**, электронный идентификатор компании «Актив» | На компьютере должны быть установлены драйверы Rutoken версии 2.81.00.0424.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная).<br>**Примечание**: перенос ключей подписи на данный тип устройств невозможен. | Да |

| | | | |
|---|---|---|---|
| **iButton Accord** | **Аккорд-5MX**, iButton типа DS1993, DS1994, DS1995 и DS1996 | На компьютере должен быть установлен драйвер версии не ниже 3.18.0.0.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32-разрядная), Server 2008 (32-разрядная). | Нет |
| **Siemens CardOS** | **Смарт-карты Siemens** CardOS/M4.01a, CardOS V4.3B, CardOS V4.2B, CardOS V4.2B DI, CardOS V4.2C, CardOS V4.4 | Для работы на компьютере должно быть установлено ПО Siemens CardOS API V5.0 или выше.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 EE SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 SP2 (32/64-разрядная), Windows 7 (32/64-разрядная). | Да |
| **Rosan Mifare** | **Rosan Mifare** | Для работы с устройством необходимо наличие COM-порта.<br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная). | Нет |
| **Mifare Standard4K** | **Mifare 4K** | Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная).<br>Для работы с устройством используется интерфейс подключения USB 2.0 (совместимый с USB 1.1).<br>Карта Mifare 4K поддерживается только через считыватель ACR128. | Нет |
| **eToken GOST** | **eToken ГОСТ Aladdin** | Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная).<br>**Примечание**: устройство поддерживает ГОСТ 34.10-2001; перенос ключей подписи на данный тип устройств невозможен. | Да |

| | | | |
|---|---|---|---|
| **JCDS** | Смарт-карты Gemalto Optelio Contactless D72, KONA 131 72K | На карту должен быть загружен апплет, позволяющий модулю jcpkcs11ds.dll компании «Аладдин Р.Д.» работать с картой.<br><br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2. | Да |
| **JaCarta** | Персональные электронные ключи JaCarta компании «Аладдин Р.Д.» | На компьютере должно быть установлено программное обеспечение JC-Client компании «Аладдин Р.Д.».<br><br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2. | Да |
| **KazToken ECP** | **KAZTOKEN**, электронный идентификатор компании «Цифровой поток» | На компьютере должны быть установлены драйверы ktDrivers.x64.v.2.73.00.04.08 (для 64-разрядной ОС) или ktDrivers.x86.v.2.73.00.04.08.<br><br>Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная).<br><br>**Примечание**: перенос ключей подписи на данный тип устройств невозможен. | Да |

# Глоссарий

## T

**TSP (Time Stamp Protocol)**

Криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определённый момент времени. Подробнее см. RFC 3161 http://tools.ietf.org/html/rfc3161.

**TSP-сервер (служба штампов времени)**

Доверенный субъект инфраструктуры открытых ключей, обладающий точным и надёжным источником времени и оказывающий услуги по созданию штампов времени.

См. также: PKI (Инфраструктура открытых ключей), Штамп времени (на стр. 98).

## A

**Асимметричное шифрование**

Система шифрования, при которой алгоритмы используют два математически связанных ключа. Открытый ключ используется для зашифрования и передается по незащищенному каналу. Закрытый ключ служит для расшифрования.

См. также: Закрытый ключ (на стр. 96), Открытый ключ (на стр. 97), Симметричное шифрование.

## Д

### Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Manager для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

См. также: Сетевой узел ViPNet, Справочники, Файл лицензии, ViPNet Удостоверяющий и ключевой центр (УКЦ).

## З

### Закрытый ключ

Закрытая (секретная) часть пары асимметричных ключей. Служит для создания электронных подписей, которые можно проверять с помощью парного ему открытого ключа, или для расшифрования сообщений, которые были зашифрованы парным ему открытым ключом.

Ключ электронной подписи (см. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи») является закрытым ключом.

См. также: Асимметричное шифрование (на стр. 95), Открытый ключ (на стр. 97), Электронная подпись (на стр. 99).

## К

### Контейнер *.enc

Файл с расширением `*.enc`, который содержит в себе файл или архив, зашифрованный с использованием открытого ключа получателя или нескольких получателей.

См. также: Открытый ключ (на стр. 97).

### Контейнер *.sig

Файл с расширением `*.sig`, который содержит в себе электронную подпись, служебную информацию, исходный файл (в случае использования прикрепленной подписи) и сертификат открытого ключа подписи, с помощью которого была сформирована данная электронная подпись.

См. также: Прикрепленная подпись (на стр. 97), Сертификат открытого ключа подписи пользователя (на стр. 98), Электронная подпись (на стр. 99).

**Контейнер ключей**

Файл, в котором хранятся закрытый ключ и соответствующий ему сертификат открытого ключа.

См. также: Закрытый ключ (на стр. 96), Сертификат открытого ключа подписи пользователя (на стр. 98).

## О

**Откреплённая подпись**

Тип электронной подписи, при использовании которой электронная подпись и служебная информация помещаются в контейнер с расширением `*.sig` отдельно от исходного файла.

Например, при подписании `file.txt` откреплённая электронная подпись помещается в контейнер `file.txt.sig`. Далее для проверки электронной подписи требуется не только данный контейнер, но и исходный файл, который в контейнер `file.txt.sig` не входит.

См. также: Электронная подпись (на стр. 99).

**Открытый ключ**

Последовательность символов, связанная с закрытым ключом определенным математическим соотношением. Открытый ключ доступен любым пользователям информационной системы и предназначен для подтверждения подлинности электронной подписи (или шифрования).

Ключ проверки электронной подписи (см. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи») является открытым ключом.

См. также: Асимметричное шифрование (на стр. 95), Закрытый ключ (на стр. 96), Электронная подпись (на стр. 99).

## П

**Прикрепленная подпись**

Тип электронной подписи, при использовании которой исходный файл, электронная подпись и служебная информация помещаются совместно в один контейнер с расширением `*.sig`.

Например, файл `file.txt` заверяется прикрепленной электронной подписью и помещается в контейнер `file.txt.sig`. Далее для проверки электронной подписи требуется только данный контейнер, который содержит и электронную подпись, и исходный файл.

См. также: Электронная подпись (на стр. 99).

## С

### Сеансовый ключ

Случайный или производный ключ, предназначенный для шифрования одного сообщения.

### Сертификат открытого ключа подписи пользователя

Электронный документ определенного формата, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Сертификат содержит информацию о владельце ключа, открытый ключ, сведения о его назначении и области применения, информацию о выпустившем сертификат удостоверяющем центре, период действия сертификата, а также некоторые дополнительные параметры. В сети ViPNet сертификат создается в программе ViPNet Удостоверяющий и ключевой центр в соответствии со стандартом X.509 v3 и заверяется электронной подписью администратора УКЦ.

В терминологии Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» сертификат открытого ключа подписи пользователя называют «сертификатом ключа проверки электронной подписи».

См. также: Администратор УКЦ, Открытый ключ (на стр. 97), Удостоверяющий центр, Электронная подпись (на стр. 99), ViPNet Удостоверяющий и ключевой центр (УКЦ).

### Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

См. также: Сетевой узел ViPNet.

## Ш

### Штамп времени

Реквизит электронного документа, которым Служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции данного документа. Штамп времени подтверждает точное время создания документа. Также может подтверждать время получения или отправления документа.

В штампе времени указывается следующее: значение хэш-функции документа, на который выдан штамп; идентификатор политики (OID), в соответствии с которой был выдан штамп; время выдачи штампа; точность времени и другие параметры.

См. также: Идентификатор объекта (OID), Электронная подпись (на стр. 99), TSP-сервер (Служба штампов времени) (на стр. 95).

## Э

### Электронная подпись

Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата открытого ключа подписи пользователя, а также установить отсутствие искажения информации в электронном документе.

См. также: Закрытый ключ (на стр. 96), Сертификат открытого ключа подписи пользователя (на стр. 98).


# Указатель