



# ViPNet PKI Client File Unit

Руководство пользователя



© ОАО «ИнфоТеКС», 2020

ФРКЕ.00175-01 34 01

Версия продукта 1.5.1

Этот документ входит в комплект поставки продукта VIPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

VIPNet<sup>®</sup> является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: [infotecs.ru](http://infotecs.ru)

Служба технической поддержки: [hotline@infotecs.ru](mailto:hotline@infotecs.ru)

# Содержание

<b>Введение</b> .....	<b>5</b>
О документе.....	6
Для кого предназначен документ .....	6
Связанные документы.....	6
Соглашения документа.....	7
О программе .....	9
Системные требования.....	9
Обратная связь .....	10
<b>Глава 1. Общая информация</b> .....	<b>11</b>
Назначение .....	12
Требования к сертификатам для заверения электронной подписью и шифрования.....	14
Принцип работы.....	15
Заверение данных электронной подписью .....	15
Шифрование данных .....	16
Заверение электронной подписью и шифрование данных.....	17
<b>Глава 2. Начало работы</b> .....	<b>19</b>
Установка .....	20
Запуск.....	21
Интерфейс .....	22
Работа с программой через контекстное меню Windows .....	23
<b>Глава 3. Подготовка к работе с файлами</b> .....	<b>24</b>
Порядок действий при подготовке к работе .....	25
Подготовка личного сертификата и ключа ЭП .....	26
Получение нового сертификата .....	28
Подготовка файла шаблона в формате JSON .....	30
Подготовка файла шаблона в формате XML .....	30
Установка сертификатов и CRL.....	32
Предупреждающие сообщения .....	35
<b>Глава 4. Использование облачных сервисов ЭП</b> .....	<b>37</b>
Настройка подключения к ПАК ViPNet PKI Service.....	38
Аутентификация на ПАК ViPNet PKI Service.....	40

Смена пароля учетной записи пользователя .....	41
<b>Глава 5. Обеспечение безопасности файлов с помощью электронной подписи и шифрования.....</b>	<b>42</b>
Подтверждение личности отправителя с помощью электронной подписи.....	43
Настройка параметров электронной подписи .....	43
Заверение файла электронной подписью .....	45
Обеспечение безопасности файлов с помощью шифрования .....	48
Настройка параметров шифрования .....	48
Зашифрование файла.....	49
Заверение электронной подписью и зашифрование файла .....	51
<b>Глава 6. Работа с файлами, полученными от других пользователей .....</b>	<b>54</b>
Получение зашифрованных и подписанных файлов .....	55
Расшифрование файла .....	56
Проверка электронной подписи.....	58
<b>Глава 7. Возможные неполадки и способы их устранения.....</b>	<b>62</b>
Требуемый сертификат не отображается в списке сертификатов для подписи.....	63
<b>Приложение А. Глоссарий .....</b>	<b>64</b>



# Введение

О документе	6
О программе	9

# О документе

В данном документе рассматривается назначение и применение программы File Unit, которая входит в состав программного комплекса ViPNet PKI Client File Unit (далее — ViPNet PKI Client). В руководстве описаны основные возможности программы, приведено описание пользовательского интерфейса.

## Для кого предназначен документ

Данный документ предназначен для пользователей ViPNet PKI Client, которые собираются обеспечивать безопасность документов, передаваемых по открытым каналам связи или с использованием съемных носителей.

## Связанные документы

В таблице ниже перечислены документы, входящие в комплект документации ПК ViPNet PKI Client помимо данного документа.

Таблица 1. Связанные документы

Документ	Содержание
ViPNet PKI Client. Общие сведения	Назначение ViPNet PKI Client. Общие сведения об инфраструктуре открытых ключей. Сведения о компонентах комплекса. Сценарии использования компонентов комплекса. Инструкция по развертыванию комплекса.
ViPNet PKI Client. Руководство администратора	Назначение ViPNet PKI Client. Общие сведения об инфраструктуре открытых ключей. Сведения о компонентах комплекса. Сценарии использования компонентов комплекса. Инструкция по развертыванию комплекса. Операции с сертификатами. Настройка параметров электронной подписи и шифрования файлов. Настройка автоматической загрузки CRL.

Документ	Содержание
	<p>Настройка подключения к ПАК ViPNet PKI Service.</p> <p>Настройка подключения к сайтам, использующим TLS ГОСТ.</p> <p>Настройка подключения к туннелируемым ViPNet TLS Gateway ресурсам.</p>
ViPNet PKI Client. Руководство разработчика	<p>Назначение ViPNet PKI Client SDK.</p> <p>Работа с комплектом средств разработки ViPNet PKI Client SDK.</p> <p>Добавление вызова криптографических функций в веб-приложения.</p>
ViPNet CSP. Руководство пользователя	<p>Использование криптографических функций в системах защиты данных.</p> <p>Установка и запуск криптопровайдера ViPNet CSP.</p> <p>Регистрация ViPNet CSP.</p> <p>Получение сертификата и ключа ЭП.</p> <p>Установка контейнеров ключей и сертификатов.</p> <p>Операции с контейнерами ключей.</p>

## Соглашения документа

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

Таблица 2. Обозначения, используемые в примечаниях




Обозначение	Описание
	<b>Внимание!</b> Указывает на обязательное для исполнения или следования действие или информацию.
	<b>Примечание.</b> Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	<b>Совет.</b> Содержит дополнительную информацию общего характера.

Таблица 3. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
<b>Название</b>	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
<b>Клавиша+Клавиша</b>	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
<b>Меню &gt; Подменю &gt; Команда</b>	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 File Unit входит в состав ПК ViPNet PKI Client File Unit и позволяет обеспечить безопасность передаваемых файлов с помощью [шифрования](#) (см. глоссарий, стр. 64) и [электронной подписи](#) (см. глоссарий, стр. 66).

## Системные требования

Требования к компьютеру для работы ViPNet PKI Client:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 2 Гбайт.
- Свободное место на жестком диске — не менее 1 Гбайт.
- Операционная система:
  - Windows 7 — 32/64-разрядная;
  - Windows Server 2008 R2 — 64-разрядная;
  - Windows Server 2012 — 64-разрядная;
  - Windows 8.1 — 32/64-разрядная;
  - Windows Server 2012 R2 — 64-разрядная;
  - Windows Server 2016 — 64-разрядная;
  - Windows Server 2019 — 64-разрядная;
  - Windows 10 — 32/64-разрядная следующих версий и сборок:
    - версия 1803, сборка 17134;
    - версия 1809, сборка 17763;
    - версия 1903, сборка 18362;
    - версия 1909, сборка 18363.

Для операционной системы должны быть установлены последние пакеты обновлений. Работа ViPNet PKI Client на компьютерах, работающих под управлением Windows 10 других версий, не гарантируется.

- Веб-браузер — Internet Explorer 11, Chromium с поддержкой ГОСТ 68.0.3440.84, КриптоПро Фок версии 24 и выше, а также Edge, Google Chrome, Mozilla Firefox, Opera, Яндекс.Браузер, браузер «Спутник» последних версий.
- Программная платформа Microsoft .NET Framework версии 4.5.

# Обратная связь

## Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- [Информация о продуктах ViPNet.](#)
- [Информация о решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

## Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:  
+7 (495) 737-6192,  
8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба технической поддержки: [hotline@infotecs.ru](mailto:hotline@infotecs.ru).  
[Форма для обращения в службу технической поддержки через сайт.](#)  
Консультации по телефону для клиентов с расширенной схемой технической поддержки:  
+7 (495) 737-6196.
- Отдел продаж: [soft@infotecs.ru](mailto:soft@infotecs.ru).

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу [security-notifications@infotecs.ru](mailto:security-notifications@infotecs.ru). Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется [политикой ответственного разглашения](#).

# 1

## Общая информация

Назначение	12
Требования к сертификатам для заверения электронной подписью и шифрования	14
Принцип работы	15

# Назначение

Программа File Unit устанавливается на рабочие места пользователей вместе с другими компонентами ViPNet PKI Client и предназначена для обеспечения безопасности файлов, передаваемых по открытым каналам связи или с помощью съемных носителей. Вы можете работать с программой File Unit как с помощью [главного окна](#) (см. рисунок на стр. 22), так и через контекстное меню Windows (см. [Работа с программой через контекстное меню Windows](#) на стр. 23).

С помощью программы File Unit вы можете:

- Обеспечивать безопасность файлов с помощью шифрования (см. [Зашифрование файла](#) на стр. 49) и заверения электронной подписью (см. [Заверение файла электронной подписью](#) на стр. 45).

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 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 File Unit защищает файл от подделки с помощью электронной подписи, а также от получения злоумышленником конфиденциальной информации, содержащейся в файле, путем шифрования данного файла.

- Работать с зашифрованными файлами, полученными от других пользователей (см. [Расшифрование файла](#) на стр. 56).

При получении файла, зашифрованного с использованием вашего сертификата, вы можете расшифровать его с помощью программы File Unit. При этом вы можете расшифровывать файлы, зашифрованные как с помощью программы File Unit, так и с помощью других программ, поддерживающих [асимметричные алгоритмы шифрования](#) (см. глоссарий, стр. 64) и стандартный формат `*.enc` (см. глоссарий, стр. 66) для зашифрованных файлов.

- Проверять личность отправителя и целостность полученных файлов (см. [Проверка электронной подписи](#) на стр. 58).

При получении какого-либо подписанного файла вы можете проверить его электронную подпись, чтобы подтвердить личность отправителя и удостовериться в целостности полученных данных. При этом можно проверить электронную подпись файлов, подписанных как с помощью программы File Unit, так и с помощью других программ, поддерживающих [асимметричные алгоритмы электронной подписи](#) (см. глоссарий, стр. 64) и стандартный формат `*.sig` (см. глоссарий, стр. 66) для подписанных файлов.

В подписанном файле `*.sig` вместе с электронной подписью передается также сертификат пользователя, подписавшего файл. Поэтому для проверки электронной подписи отдельная передача сертификата получателям файла не требуется.

- Подтверждать точное время заверения файлов электронной подписью (см. [Заверение файла электронной подписью](#) на стр. 45).

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

Для выполнения криптографических операций программа File Unit использует следующие криптографические алгоритмы:

- Алгоритмы формирования и проверки электронной подписи данных ГОСТ Р 34.10-2001 (с вычислением хэш-функции по ГОСТ Р 34.11-94) и ГОСТ Р 34.10-2012 (с вычислением хэш-функции по ГОСТ Р 34.11-2012).
- Алгоритм шифрования информации ГОСТ 28147-89.

# Требования к сертификатам для заверения электронной подписью и шифрования

Для заверения электронной подписью и шифрования файлов сертификаты должны удовлетворять следующим требованиям:

- Сертификат должен быть действителен:
  - Срок действия сертификата не истек.
  - Срок действия ключа ЭП не истек.
  - Сертификат не аннулирован.
  - [Вся цепочка сертификации](#) (см. глоссарий, стр. 66) полна, и все входящие в нее сертификаты удостоверяющих центров действительны.
- Для шифрования сертификаты получателей должны быть установлены в хранилище сертификатов **Другие пользователи** и иметь в поле **Использование ключа** хотя бы одно из назначений: **Шифрование данных**, **Шифрование ключей**, **Согласование ключей**.
- Для заверения файлов электронной подписью ваш сертификат должен быть установлен в хранилище сертификатов Windows текущего пользователя **Личное** и иметь назначение **Цифровая подпись** в поле **Использование ключа**. В случае если запрос на сертификат был создан не с помощью ViPNet PKI Client, должна быть установлена связь между сертификатом и контейнером с ключом ЭП (см. документ «ViPNet CSP. Руководство пользователя», раздел «Установка сертификата в системное хранилище Windows»).



**Внимание!** В случае если ваш сертификат или сертификат получателя не соответствует указанным требованиям, вы не сможете выбрать его для заверения электронной подписью или шифрования.

---

# Принцип работы

Программа File Unit выполняет формирование и проверку электронной подписи, а также шифрование и расшифрование файлов, при этом для выполнения криптографических операций программа обращается к криптопровайдеру ViPNet CSP или ПАК ViPNet PKI Service (требуется лицензия на использование Cloud Unit).

Программа File Unit работает на основе алгоритмов асимметричного шифрования и выработки электронной подписи, которые используют пару связанных между собой асимметричных ключей пользователя:

- Ключ ЭП — используется для формирования электронной подписи и расшифрования файлов. Ключ ЭП конфиденциален и должен храниться в секрете.
- Ключ проверки ЭП — используется для проверки электронной подписи и шифрования файлов. Ключ проверки ЭП свободно распространяется среди других пользователей в составе [сертификата пользователя](#) (см. глоссарий, стр. 65).

---

**Примечание.** В федеральном законе № 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. используются термины:



- Ключ, предназначенный для создания электронной подписи, называется [ключом электронной подписи](#) (см. глоссарий, стр. 65).
- Ключ, предназначенный для проверки подлинности электронной подписи, называется [ключом проверки электронной подписи](#) (см. глоссарий, стр. 64).

---

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

- [Заверение данных электронной подписью](#) (на стр. 15).
- [Шифрование данных](#) (на стр. 16).
- [Заверение электронной подписью и шифрование данных](#) (на стр. 17).

## Заверение данных электронной подписью

Заверение файла электронной подписью и передача его другому пользователю происходит следующим образом:

- 1 Пользователь **A** в программе File Unit инициирует заверение файла электронной подписью, который хочет передать пользователю **B**.
- 2 При заверении файла электронной подписью программа File Unit обращается к криптопровайдеру ViPNet CSP для формирования электронной подписи с помощью закрытого ключа пользователя **A**. Затем программа File Unit формирует файл с расширением `*.sig`, содержимое которого зависит от того, какой тип электронной подписи использует пользователь **A**:

- В случае использования **прикрепленной подписи** (см. глоссарий, стр. 65) в файл `<имя_файла>.sig` помещаются исходный файл, сформированная электронная подпись и служебная информация.

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 файлами `*.sig` (программы File Unit, ViPNet Деловая почта или программы сторонних производителей со схожим функционалом, например КриптоАРМ).

- В случае использования **открепленной подписи** (см. глоссарий, стр. 65) в файл `<имя_файла>.detached.sig` помещаются сформированная электронная подпись и служебная информация. При этом исходный файл передается пользователю **В** отдельно (для проверки электронной подписи требуется и файл с открепленной подписью, и исходный файл).

Открепленная подпись позволяет ознакомиться с содержимым исходного файла пользователям, на компьютерах которых не установлены средства работы с файлами `*.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 файлом `<имя_файла>.detached.sig`.

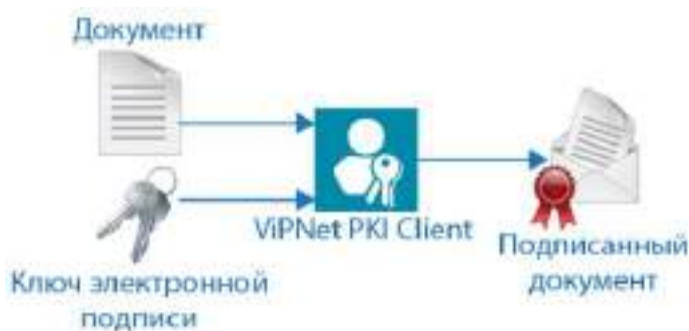


Рисунок 1. Заверение документа электронной подписью с помощью программы File Unit

- 3 Пользователь **А** передает пользователю **В** файл с расширением `*.sig` и исходный файл (если была выбрана открепленная подпись), например, с помощью электронной почты.
- 4 Пользователь **В** проверяет электронную подпись с использованием открытого ключа пользователя **А**, который входит в состав сертификата подписи.

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

## Шифрование данных

Шифрование файла и передача его другому пользователю происходит следующим образом:

- 1 Отправитель в программе File Unit инициирует шифрование файла, который хочет передать нескольким получателям.



- 2 Отправитель из хранилища сертификатов выбирает сертификат одного или нескольких получателей, которым собирается передать зашифрованный файл.
- 3 При шифровании файла программа File Unit обращается к криптопровайдеру ViPNet CSP для шифрования файла с помощью открытых ключей выбранных получателей. В результате программа File Unit формирует зашифрованный файл с расширением \*.enc.



Рисунок 2. Шифрование документа с помощью программы File Unit

- 4 Отправитель передает получателям зашифрованный файл, например, с помощью электронной почты.
- 5 Получатели расшифровывают файл с использованием своих закрытых ключей.

В результате получатели смогут ознакомиться с конфиденциальными данными, содержащимися в полученном файле.

## Заверение электронной подписью и шифрование данных

Заверение электронной подписью и шифрование файла с использованием алгоритмов ГОСТ и передача его одному или нескольким пользователям осуществляются следующим образом:

- 1 Отправитель в программе File Unit инициирует заверение электронной подписью и шифрование файла, который хочет передать другим пользователям (получателям).
- 2 При заверении файла электронной подписью программа File Unit обращается к криптопровайдеру ViPNet CSP для формирования электронной подписи с помощью закрытого ключа отправителя. Затем программа File Unit формирует файл с расширением \*.sig:
  - В случае использования прикрепленной подписи в файл <имя\_файла>.sig помещаются исходный файл, сформированная электронная подпись и служебная информация.
  - В случае использования открепленной подписи в файл <имя\_файла>.detached.sig помещаются сформированная электронная подпись и служебная информация. При этом исходный файл не помещается в файл <имя\_файла>.detached.sig.
- 3 Отправитель из хранилища сертификатов выбирает сертификат одного или нескольких получателей, которым собирается передать зашифрованный и подписанный файл.

- 4 При шифровании файла программа File Unit обращается к криптопровайдеру ViPNet CSP для шифрования файла с помощью открытых ключей выбранных получателей. В результате программа File Unit формирует зашифрованный файл с расширением \*.enc.
- 5 Отправитель передает получателям файл с зашифрованными и подписанными данными, например, с помощью электронной почты.
- 6 Получатели расшифровывают файл с использованием своих закрытых ключей.
- 7 Получатели проверяют электронную подпись с использованием открытого ключа отправителя, который входит в состав сертификата подписи.

В результате получатели смогут ознакомиться с данными, которые содержатся в полученном файле.

# 2

## Начало работы

Установка	20
Запуск	21
Интерфейс	22
Работа с программой через контекстное меню Windows	23

# Установка



Программа File Unit входит в состав ViPNet PKI Client, она устанавливается в процессе развертывания этого комплекса.

Для установки ViPNet PKI Client следуйте рекомендациям, приведенным в документе «ViPNet PKI Client. Руководство администратора» в разделе «Установка и обновление».

# Запуск

Чтобы запустить программу File Unit, в меню **Пуск** выберите **ViPNet > File Unit**.

Чтобы перейти к настройкам компонентов ViPNet PKI Client, выполните одно из действий:

- В **основном окне программы File Unit** (см. рисунок на стр. 22) нажмите кнопку  **Настройки**.
- В меню **Пуск** выберите **ViPNet > Настройки ViPNet PKI Client**.
- Дважды щелкните ярлык  на рабочем столе.

# Интерфейс

Главное окно программы File Unit представлено на рисунке ниже.

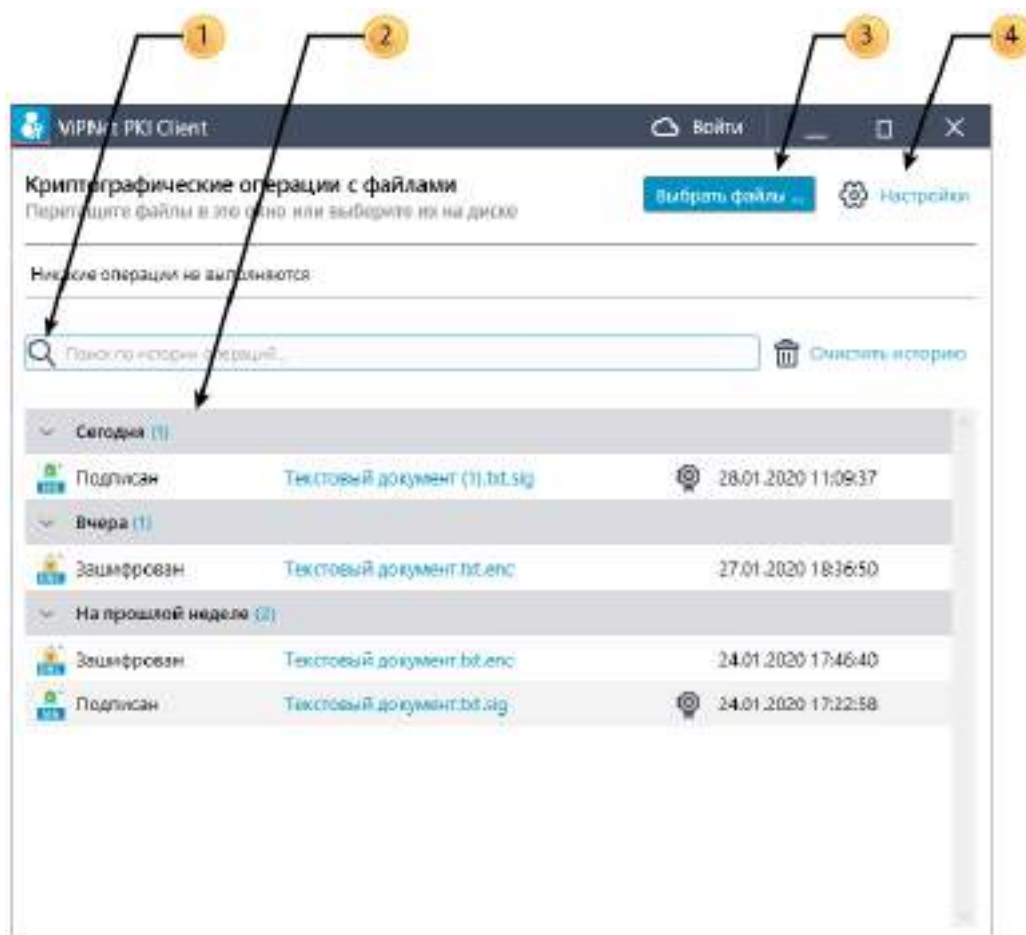


Рисунок 3. Интерфейс программы File Unit

Цифрами на рисунке обозначены:

- 1 Строка поиска файлов.
- 2 Область истории операций с файлами.
- 3 Кнопка выбора файлов для выполнения криптографических операций.
- 4 Кнопка настройки.

# Работа с программой через контекстное меню Windows

Вы можете работать с программой File Unit через контекстное меню Windows без вызова [главного окна программы](#) (см. рисунок на стр. 22). Данная функция может быть полезна, если вы работаете с файлом в Проводнике Windows и вам понадобилось зашифровать файл, не отвлекаясь на работу с главным окном программы File Unit.

С помощью контекстного меню Windows вы можете:

- Зашифровать файл (см. [Зашифрование файла](#) на стр. 49).
- Заверить файл электронной подписью (см. [Заверение файла электронной подписью](#) на стр. 45).
- Одновременно заверить электронной подписью и зашифровать файл (см. [Заверение электронной подписью и зашифрование файла](#) на стр. 51).
- Расшифровать файл (см. [Расшифрование файла](#) на стр. 56).
- Проверить электронную подпись файла (см. [Проверка электронной подписи](#) на стр. 58).



**Примечание.** Прежде чем начать работать с программой File Unit через контекстное меню Windows, выполните предварительные настройки (см. [Подготовка к работе с файлами](#) на стр. 24).

---

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

- 1 В проводнике Windows выберите нужный файл (или несколько файлов) и щелкните его правой кнопкой мыши.
- 2 В контекстном меню выберите **ViPNet PKI Client** и нужную операцию.

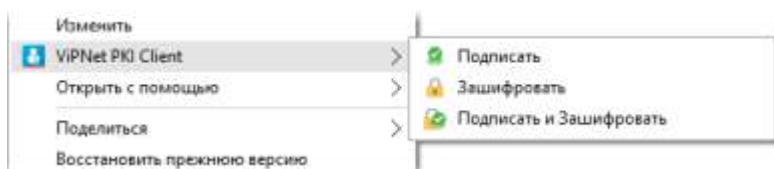


Рисунок 4. Работа с программой с помощью контекстного меню

В результате будет выполнена выбранная операция. Во время выполнения операции следуйте указаниям, описанным в соответствующих разделах глав: [Обеспечение безопасности файлов с помощью электронной подписи и шифрования](#) (на стр. 42) и [Работа с файлами, полученными от других пользователей](#) (на стр. 54).

# 3

## Подготовка к работе с файлами

Порядок действий при подготовке к работе	25
Подготовка личного сертификата и ключа ЭП	26
Получение нового сертификата	28
Установка сертификатов и CRL	32
Предупреждающие сообщения	35



# Порядок действий при подготовке к работе

Таблица 4. Порядок действий

Действие
<input type="checkbox"/> Подготовьте личный сертификат и ключ ЭП (на стр. 26)
<input type="checkbox"/> Установите сертификаты издателей и CRL в хранилище сертификатов (на стр. 32)
<input type="checkbox"/> Настройте параметры электронной подписи (на стр. 43)
<input type="checkbox"/> Настройте параметры шифрования файлов (на стр. 48)

# Подготовка личного сертификата и ключа ЭП

## У меня нет сертификата и ключа ЭП

- 1 Создайте запрос на сертификат (см. [Получение нового сертификата](#) на стр. 28).
- 2 Передайте запрос в УЦ и получите личный сертификат, сертификат издателя и CRL, а если ваш УЦ не является корневым, все сертификаты издателей из цепочки сертификации и соответствующие CRL.
- 3 [Установите личный сертификат в хранилище сертификатов Windows](#) (на стр. 32).

## У меня есть сертификат и ключ ЭП в папке на диске

- 1 С помощью криптопровайдера ViPNet CSP установите контейнер ключей (см. документ «ViPNet CSP. Руководство пользователя» в разделе «Установка контейнера ключей из папки»).
- 2 Установите сертификат в хранилище сертификатов Windows текущего пользователя **Личное** с указанием расположения контейнера ключей (см. в документе «ViPNet CSP. Руководство пользователя» раздел «Установка сертификата в системное хранилище Windows»).

## У меня есть сертификат и ключ ЭП на внешнем устройстве (токене)

- 1 Подключите внешнее устройство к компьютеру.




**Примечание.** При подключении устройств семейства Rutoken, JaCarta и ESMART Token появится соответствующее уведомление, а в настройках ViPNet PKI Client появится раздел



**Подключено устройств.**

---

- 2 Выполните одно из действий:

- Для устройств семейства Rutoken, JaCarta, ESMART Token — перейдите в раздел  **Подключено устройств**, щелкните сертификат правой кнопкой мыши и выберите **Установить сертификат**.
- Для других устройств — с помощью криптопровайдера ViPNet CSP установите контейнер ключей и сертификат в хранилище сертификатов Windows текущего пользователя **Личное** (см. документ «ViPNet CSP. Руководство пользователя» в разделе «Установка контейнера ключей с внешнего устройства»).

## У меня есть сертификат и ключ ЭП на ПАК ViPNet PKI Service

- 1 Настройте подключение к ПАК ViPNet PKI Service (см. [Настройка подключения к ПАК ViPNet PKI Service](#) на стр. 38).

- 2 Пройдите аутентификацию с помощью вашей учетной записи пользователя. Сертификат появится в списке сертификатов **Облачные**.



**Примечание.** Если в вашей учетной записи на ПАК ViPNet PKI Service нет сертификата или вам нужно обновить существующий, создайте запрос на сертификат с помощью шаблона **Облачный** (см. [Получение нового сертификата](#) на стр. 28) и [установите его на ПАК ViPNet PKI Service](#) (на стр. 32).



---

# Получение нового сертификата

Чтобы выполнять криптографические операции, вам необходимо иметь контейнер ключей и сертификат. Сертификат издается удостоверяющим центром по вашему запросу, в котором указываются необходимые данные. Контейнер ключей и сертификат могут храниться в папке на диске, внешнем устройстве (токене) или на ПАК ViPNet PKI Service.

Чтобы создать запрос на сертификат:

1 Выполните одно из действий:

- [Перейдите в настройки ViPNet PKI Client](#) (на стр. 21), выберите раздел  Сертификаты и нажмите  Создать запрос.
- В меню Пуск выберите ViPNet PKI Client > Создание запроса на сертификат.

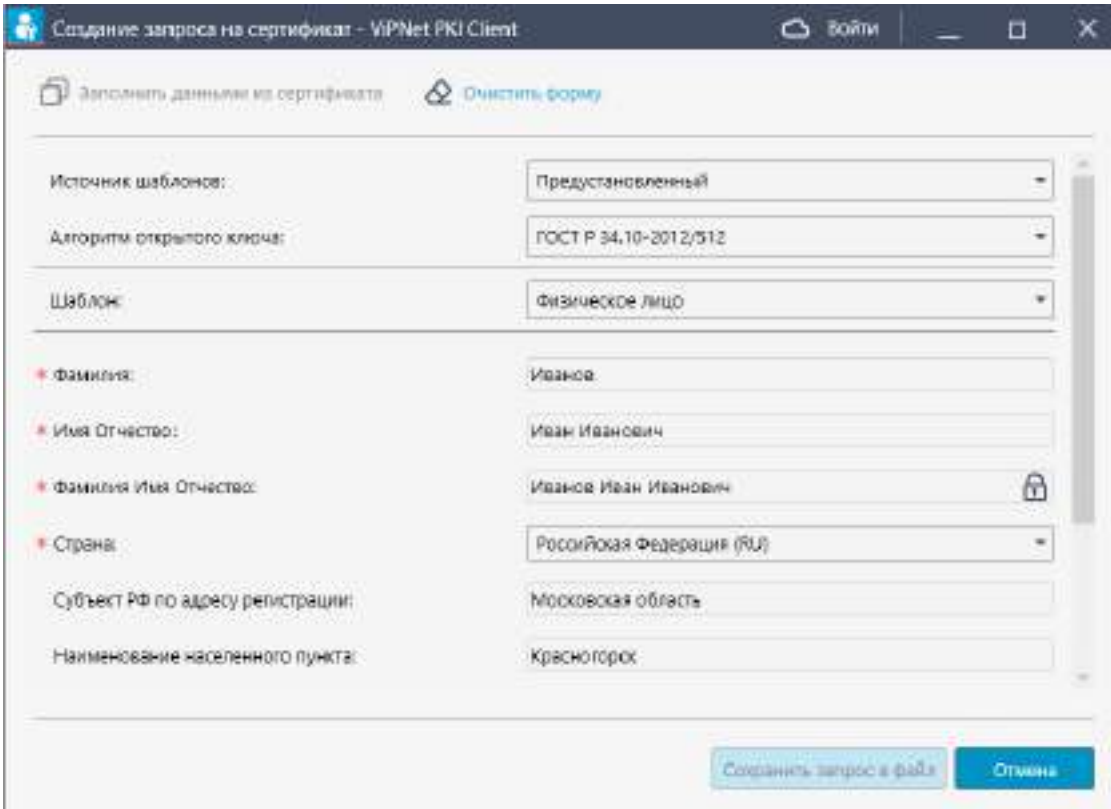



Рисунок 5. Создание запроса на сертификат



**Примечание.** Если у вас есть сертификат, вы можете создать запрос на его основе. Для этого нажмите  Заполнить данными из сертификата и выберите сертификат для автоматического заполнения полей. Если нужно, измените информацию в полях запроса вручную.

2 Выберите **Источник шаблонов**:

- **Предустановленный.** Содержит добавленные по умолчанию шаблоны. Выберите, если нужно сохранить контейнер ключей на диске или внешнем устройстве.
- **Пользовательский.** Выберите, если в вашей организации требуется, чтобы в поле сертификата **Субъект (Subject)** присутствовали только определенные атрибуты. Подготовьте файл в формате JSON (см. [Подготовка файла шаблона в формате JSON](#) на стр. 30) или XML (см. [Подготовка файла шаблона в формате XML](#) на стр. 30), задайте в нем нужные атрибуты и загрузите в окно создания запроса на сертификат. При создании запроса контейнер ключей можно будет сохранить на диске или внешнем устройстве.
- **Облачный.** Требуется [настройка подключения к ПАК ViPNet PKI Service](#) (на стр. 38) и авторизация на нем. Содержит шаблоны, добавленные на ViPNet PKI Service. Выберите, если требуется сохранить контейнер ключей на ПАК ViPNet PKI Service.

3 Выберите **Алгоритм открытого ключа** или оставьте значение по умолчанию.

4 Выберите **Шаблон** сертификата и **Назначение сертификата** (если на предыдущем шаге вы выбрали **Облачный**). **Шаблон** содержит разное количество и наименование атрибутов, которые попадут в поле сертификата **Субъект (Subject)**. **Назначение сертификата** содержит разное количество идентификаторов (OID), которые попадут в поле сертификата **Улучшенный ключ**.

5 Заполните поля и нажмите **Сохранить запрос в файл**.

6 Укажите имя и папку для сохранения файла запроса и нажмите **Сохранить**.

7 Если контейнер ключей был сохранен не на ViPNet PKI Service (**Облачный**), в окне **ViPNet CSP — инициализация контейнера ключей**:

- Укажите имя и место для сохранения [контейнера ключей](#) (см. глоссарий, стр. 65).
- Задайте пароль для работы с контейнером ключей. Чтобы в дальнейшем не вводить пароль, установите флажок **Сохранить пароль**.

8 В окне **Электронная рулетка** отобразится процесс инициализации генератора случайных чисел. Следуйте указаниям в этом окне.

9 В окне сообщения об успешном создании файла запроса на сертификат выполните одно из действий:

- Перейдите в папку с запросом.
- Создайте еще один запрос.
- Закройте окно.

10 Передайте запрос в УЦ и получите личный сертификат, сертификат издателя и CRL, а если ваш УЦ не является корневым, все сертификаты издателей из цепочки сертификации и соответствующие CRL.

После получения сертификата установите его в хранилище Windows или на ПАК ViPNet PKI Service (см. [Установка сертификатов и CRL](#) на стр. 32).

# Подготовка файла шаблона в формате JSON

Атрибуты, которые будут добавлены в поле **Субъект (Subject)**, могут быть заданы с помощью файла шаблона в формате \*.json.

Файл шаблона в формате JSON должен иметь вид:

```
[
  {
    "FieldName": "Название параметра",
    "FieldValue": "Значение по умолчанию",
    "FieldAttribute": "Атрибут",
    "ValidationRegExp": "Ограничение",
    "ValidationErrorText": "Текст ошибки"
  },
  ...
  {
    "FieldName": "Название параметра",
    "FieldValue": "Значение по умолчанию",
    "FieldAttribute": "Атрибут",
    "ValidationRegExp": "Ограничение",
    "ValidationErrorText": "Текст ошибки"
  }
]
```

Где:

- `FieldName` — название атрибута, отображаемое в списке **Поля сертификата**.
- `FieldValue` — значение атрибута, заданное по умолчанию.
- `FieldAttribute` — атрибут поля сертификата **Субъект (Subject)** в соответствии со [стандартом X.509](#), например, SN — фамилия владельца, O — компания и так далее.
- `ValidationRegExp` — ограничение на ввод данных с помощью регулярных выражений, например, `^\d*$` — возможен ввод только цифр (неограниченное количество).
- `ValidationErrorText` — текст ошибки при несоответствии введенного значения регулярному выражению.

# Подготовка файла шаблона в формате XML

Список атрибутов, которые будут добавлены в поле **Субъект (Subject)**, могут быть заданы с помощью файла шаблона в формате \*.xml.

Файл шаблона должен иметь вид:

```
<?xml version="1.0" encoding="utf-8"?>
<RequestTemplate>
  <Field attribute="Атрибут" name="Название параметра" value="Значение по умолчанию"
  validationRegExp="Ограничение" validationErrorText="Текст ошибки"/>
</RequestTemplate>
```

```
...  
<Field attribute="Атрибут" name="Название параметра" value="Значение по умолчанию"  
validationRegExp="Ограничение" validationErrorText="Текст ошибки"/>  
</RequestTemplate>
```

Где:

- `attribute` — атрибут поля сертификата **Субъект (Subject)** в соответствии со [стандартом X.509](#), например, SN — фамилия владельца, O — компания и так далее.
- `name` — название атрибута, отображаемое в списке **Поля сертификата**.
- `value` — значение атрибута, заданное по умолчанию.
- `validationRegExp` — ограничение на ввод данных с помощью регулярных выражений, например, `^\d*$` — возможен ввод только цифр (неограниченное количество).
- `validationErrorText` — текст ошибки при несоответствии введенного значения регулярному выражению.

# Установка сертификатов и CRL

Указанным способом устанавливайте только те личные сертификаты, запрос на которые был создан в ViPNet PKI Client (см. [Получение нового сертификата](#) на стр. 28). Если вы получали сертификат иным способом, следуйте указаниям раздела [Подготовка личного сертификата](#) (на стр. 26).

ViPNet PKI Client также поддерживает работу с файлами формата PKSC#7. Установка сертификатов из таких файлов осуществляется аналогично. Если файл формата PKSC#7 помимо сертификатов содержит CRL, они также могут быть установлены в хранилище сертификатов Windows.

Чтобы установить сертификаты и (или) CRL:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 21).



**Примечание.** Чтобы установить сертификаты издателей и CRL в хранилище сертификатов Windows локального компьютера, запустите настройки ViPNet PKI Client от имени администратора.

- 2 В разделе **Сертификаты** выполните одно из действий:

- Перетащите файлы сертификатов и (или) CRL на панель просмотра.






**Примечание.** При запуске настроек ViPNet PKI Client от имени администратора данный способ недоступен.

- Нажмите **Добавить сертификат или CRL**, укажите путь к файлам сертификатов и (или) CRL.


- 3 В окне **Добавление сертификатов** отображается список устанавливаемых сертификатов и CRL. В этом списке:

- **Личный** — личные сертификаты, запрос на которые был создан в программе ViPNet PKI Client или ViPNet CSP, а контейнер ключей сохранен на диске или внешнем устройстве (токене). Сертификаты будут установлены в хранилище сертификатов Windows текущего пользователя **Личное**. Если нужно установить сертификат в контейнер ключей, установите соответствующий флажок, введите пароль контейнера ключей или ПИН-код внешнего устройства и нажмите **Ввести**.
- **Издатель** — сертификаты удостоверяющих центров. Корневые сертификаты устанавливаются в хранилище **Доверенные корневые центры сертификации**, промежуточные — **Промежуточные центры сертификации**.
- **Другой** — сертификаты получателей. Устанавливаются в хранилище **Другие пользователи**.



-  **CRL** — списки аннулированных сертификатов. Устанавливаются в хранилище **Промежуточные центры сертификации**.
-  **Облачный** — сертификаты, контейнеры ключей которых сохранены на ПАК ViPNet PKI Service. Такие сертификаты будут установлены на ПАК ViPNet PKI Service (потребуется авторизация).
- сертификаты и CRL с истекшим сроком действия или имеющие недействительную цифровую подпись отмечаются значком  и не будут установлены в хранилище сертификатов.

При необходимости вы можете:

- Посмотреть подробную информацию об устанавливаемых сертификатах и CRL, для этого щелкните имя владельца сертификата или CRL.
- Удалить сертификат или CRL из списка, для этого щелкните значок  (появляется при наведении курсора на строку сертификата или CRL).

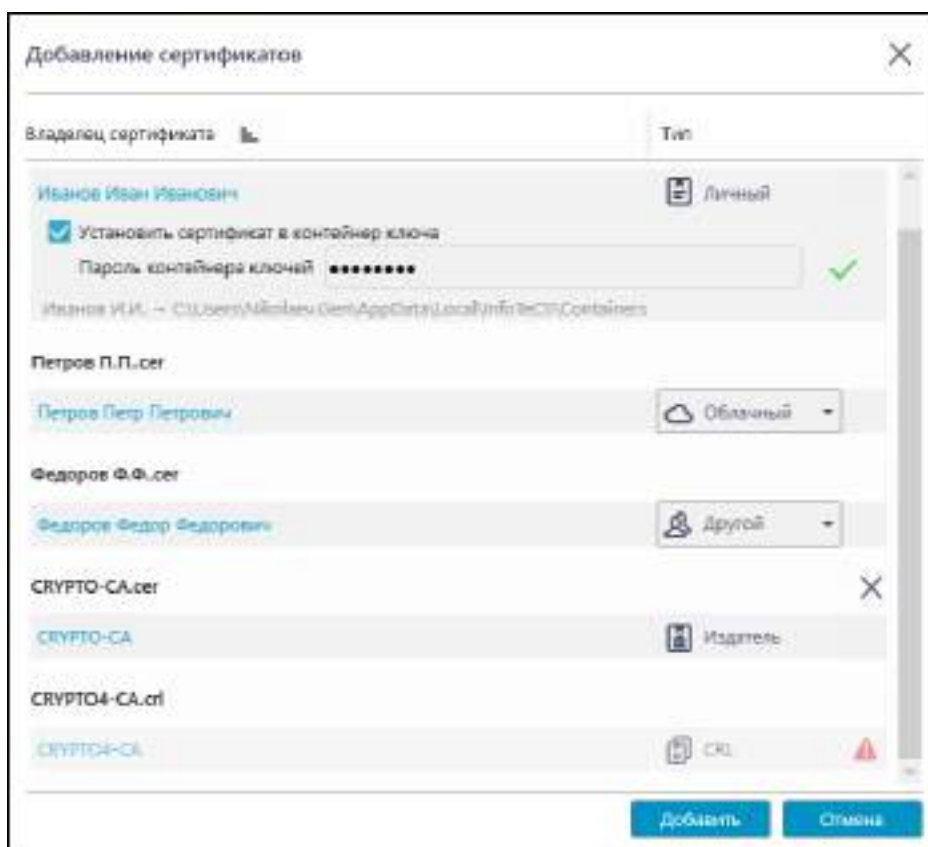





Рисунок 6. Установка сертификатов и CRL

- 4 В окне **Добавление сертификатов** нажмите **Добавить**, а затем **Заккрыть**.

Если вы работаете не под учетной записью администратора ОС Windows, то при установке сертификата издателя откроется окно **Предупреждение о безопасности**, в котором вам будет предложено установить сертификат издателя. Чтобы установить сертификат, нажмите **Да**.

Результат установки отмечается значком напротив каждого установленного сертификата и CRL:

- o  — установка выполнена успешно;
- o  — во время установки произошла ошибка;
- o  — сертификат или CRL уже установлен в системное хранилище.




**Примечание.** Если после установки сертификата в строке имени владельца сертификата появится предупреждающее сообщение, наведите курсор на значок , просмотрите более подробные сведения об ошибках и устраните их (см. [Предупреждающие сообщения](#) на стр. 35).



Рисунок 7. Просмотр предупреждающих сообщений

## Установка с помощью контекстного меню Windows

Вы можете устанавливать сертификаты и CRL с помощью контекстного меню Windows без вызова окна **Настройки - ViPNet PKI Client**. Установленные таким способом сертификаты появятся в ViPNet PKI Client.



**Примечание.** Если вы работаете не под учетной записью администратора ОС Windows, то при установке сертификата издателя он будет установлен в системное хранилище текущего пользователя, то есть будет доступен только текущему пользователю.

Для установки сертификатов или CRL с помощью контекстного меню Windows выделите их, щелкните правой кнопкой мыши и выберите **ViPNet PKI Client > Установить сертификат/список отзыва**.

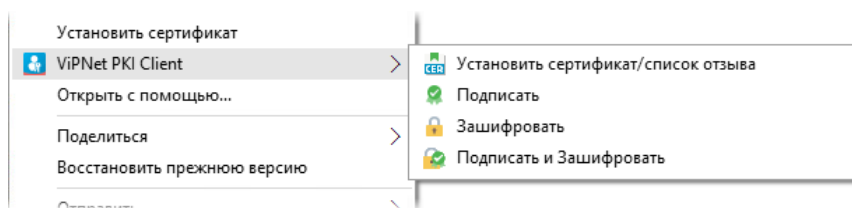


Рисунок 8. Установка сертификатов и CRL с помощью контекстного меню Windows



# Предупреждающие сообщения

Предупреждающие сообщения предназначены для информирования пользователя о невозможности использования установленных сертификатов для выполнения криптографических операций (заверения электронной подписью, шифрования, расшифрования).

Во время установки сертификатов ViPNet PKI Client выполняет проверку сертификатов на соответствие следующим требованиям:

- Срок действия сертификата не истек.
- Сертификат не находится в списке аннулированных сертификатов доверенного удостоверяющего центра.
- [Цепочка сертификации](#) (см. глоссарий, стр. 66) полна, и все входящие в нее сертификаты удостоверяющих центров действительны.

Вы можете выполнить проверку установленных сертификатов вручную. Для этого:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 21) и выберите раздел  **Сертификаты**.
- 2 На панели инструментов нажмите .

В случае если устанавливаемый сертификат не соответствует указанным требованиям, в строке имя владельца сертификата появится [предупреждающее сообщение](#) (см. рисунок на стр. 34):

- **Цепочка сертификации неполная**

В хранилище установлены не все сертификаты, образующие [цепочку сертификации](#) (см. глоссарий, стр. 66).

При появлении установите в хранилище все сертификаты, образующие цепочку сертификации (см. [Установка сертификатов и CRL](#) на стр. 32).

- **Сертификат отозван**

Сертификат или один из сертификатов, образующих цепочку сертификации, аннулирован.

При появлении получите новый сертификат (см. [Получение нового сертификата](#) на стр. 28) и установите его в хранилище (см. [Установка сертификатов и CRL](#) на стр. 32).

- **Сертификат в цепочке содержит недействительную ЭП**

Сертификат или один из сертификатов, образующих цепочку сертификации, искажен.

При появлении переустановите все сертификаты, образующие цепочку сертификации.

- **Срок действия ключа ЭП истек**

Истек срок действия ключа ЭП.

При появлении выполните одно из действий:

- Если вы устанавливаете личный сертификат, получите новый сертификат (см. [Получение нового сертификата](#) на стр. 28) и установите его в хранилище (см. [Установка сертификатов и CRL](#) на стр. 32).
- Если вы устанавливаете сертификат получателя, запросите у получателя новый сертификат.
- **Статус отзыва сертификата не проверен**

Появляется в следующих случаях:

- В хранилище сертификатов не установлен CRL.
- В хранилище сертификатов установлен CRL с истекшим сроком действия.
- Электронная подпись CRL неверна.

При появлении [установите актуальный CRL в хранилище сертификатов](#) (на стр. 32).

# 4

## Использование облачных сервисов ЭП

Настройка подключения к ПАК ViPNet PKI Service	38
Аутентификация на ПАК ViPNet PKI Service	40
Смена пароля учетной записи пользователя	41


# Настройка подключения к ПАК ViPNet PKI Service

Если в вашей компании используется ПАК ViPNet PKI Service, настройте подключение к нему. Это позволит:

- создавать запросы на сертификаты (см. [Получение нового сертификата](#) на стр. 28), используя шаблоны сертификатов ПАК ViPNet PKI Service, при этом ключ ЭП будет сохранен на ПАК ViPNet PKI Service;
- [устанавливать личные сертификаты на ПАК ViPNet PKI Service](#) (на стр. 32), если ключ ЭП хранится на ПАК ViPNet PKI Service;
- использовать сертификаты и ключи ЭП, хранящиеся на ПАК ViPNet PKI Service, для заверения электронной подписью, проверки электронной подписи и расшифрования файлов.

Для выполнения операций потребуется аутентификация на ViPNet PKI Service под учетной записью пользователя. Для заверения электронной подписью также потребуется действительный сертификат и ключ ЭП, установленные на ПАК ViPNet PKI Service.

Чтобы настроить подключение к ПАК ViPNet PKI Service:

- 1 У администратора ПАК ViPNet PKI Service получите данные подключения (адрес и порт).
- 2 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 21) и выберите раздел  **Облачные сервисы**.

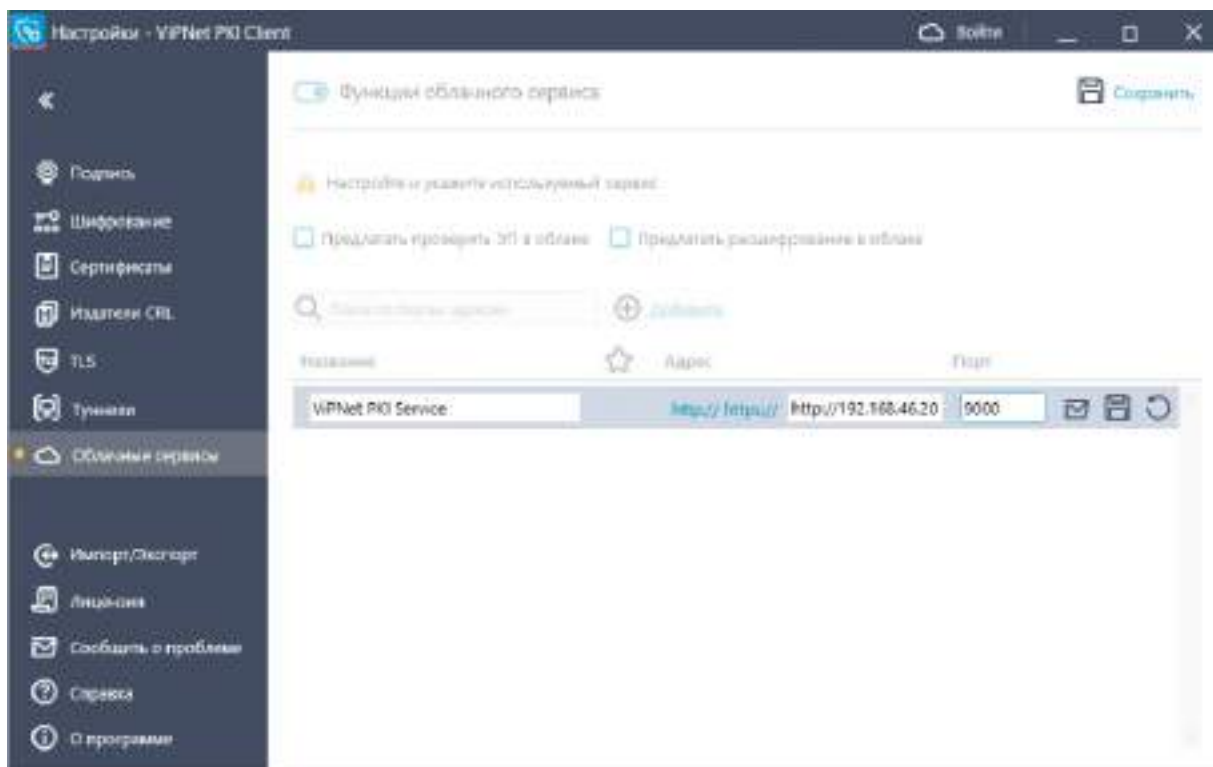






Рисунок 9. Настройка подключения к облачному сервису ЭП (ViPNet PKI Service)

- 3 Включите функции облачного сервиса с помощью переключателя, если они отключены.
- 4 Нажмите  **Добавить** и укажите:
  - Название облачного сервиса.
  - Адрес ПАК ViPNet PKI Service и порт для подключения пользователей — 9000.
  - Нажмите , чтобы проверить соединение с ПАК ViPNet PKI Service.
  - Нажмите .
- 5 Установите флажок **Предлагать проверять ЭП в облаке** — ViPNet PKI Client будет предлагать проверить подпись на ПАК ViPNet PKI Service, если при проверке подписи не удалось проверить сертификат подписанта с помощью сертификатов, установленных в хранилище сертификатов Windows.
- 6 Установите флажок **Предлагать расшифрование в облаке** — ViPNet PKI Client будет предлагать расшифровать файл на ПАК ViPNet PKI Service, если подходящий для расшифрования сертификат не найден в хранилище сертификатов Windows.
- 7 В верхней части окна нажмите  **Сохранить**.

# Аутентификация на ПАК ViPNet PKI Service

Для обращения к ПАК ViPNet PKI Service потребуется ввести логин и пароль пользователя. Окно аутентификации будет появляться:

- При выполнении операций с помощью сертификатов и ключей ЭП, хранящихся на ПАК ViPNet PKI Service.
- При просмотре и выборе сертификатов, хранящихся на ПАК ViPNet Service, для подписи.
- При создании запроса на сертификат с помощью шаблона **Облачный**.

Для первой аутентификации используется разовый пароль, который нужно сменить на постоянный.



**Примечание.** По требованиям безопасности срок действия постоянного пароля составляет 6 месяцев (по истечении система направит запрос на смену пароля), а продолжительность сессии — 10 минут.




---

Если вы забыли пароль, обратитесь к администратору ПАК ViPNet PKI Service и получите новый разовый пароль.



# Смена пароля учетной записи пользователя

Я знаю свой пароль и хочу его сменить

- 1 Перейдите в настройки ViPNet PKI Client (на стр. 21), в разделе  **Облачные сервисы** выберите **Используемый сервис**.
- 2 На панели заголовка нажмите  **Войти**.
- 3 Введите ваши учетные данные и нажмите  **Сменить пароль**.
- 4 Введите и повторите новый пароль и нажмите **Изменить**.

Я забыл пароль и хочу получить новый

Обратитесь к администратору ПАК ViPNet PKI Service и получите разовый пароль. При первой аутентификации его нужно будет изменить.

# 5

## Обеспечение безопасности файлов с помощью электронной подписи и шифрования

Подтверждение личности отправителя с помощью электронной подписи	43
Обеспечение безопасности файлов с помощью шифрования	48
Заверение электронной подписью и зашифрование файла	51

# Подтверждение личности отправителя с помощью электронной подписи

Данные, передаваемые по открытым каналам связи, могут быть повреждены или подменены злоумышленником. Чтобы избежать искажения данных посторонними лицами, в ViPNet PKI Client реализован механизм электронной подписи. Электронная подпись позволяет:



- Определить лицо, подписавшее документ.
- Обнаружить факт искажения данных, содержащихся в документе, произошедший после момента заверения электронной подписью.

Чтобы заверить документ своей электронной подписью:

- 1 [Убедитесь, что у вас есть сертификат и соответствующий ключ ЭП](#) (на стр. 26).
- 2 Если ваш сертификат установлен в хранилище сертификатов Windows, проверьте, что в хранилище также [установлены сертификаты издателей и соответствующие CRL](#) (на стр. 32).
- 3 Настройте параметры электронной подписи (см. [Настройка параметров электронной подписи](#) на стр. 43).
- 4 Заверьте файл электронной подписью (см. [Заверение файла электронной подписью](#) на стр. 45).
- 5 Передайте подписанный файл получателям любым удобным способом.

## Настройка параметров электронной подписи

Настройте параметры электронной подписи, которые будут использоваться по умолчанию в программах File Unit и Web Unit. Для этого:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 21).
- 2 В разделе  **Подпись** нажмите  **Выберите сертификат**.
- 3 Выберите сертификат и нажмите **Выбрать**.

Отобразится информация о выбранном сертификате. Для просмотра подробной информации об используемом сертификате щелкните имя владельца сертификата.

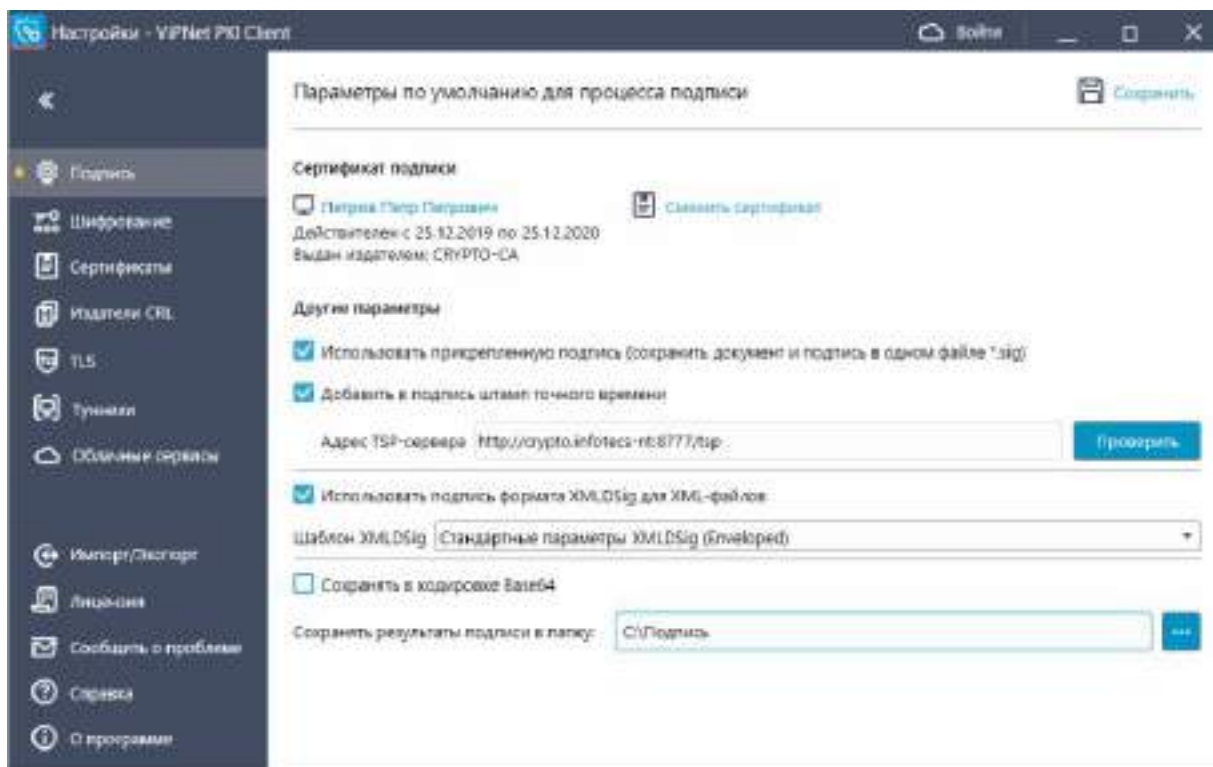


Рисунок 10. Настройка параметров электронной подписи


- 4 Чтобы сохранять подпись **отдельно от подписываемого файла** (см. глоссарий, стр. 65), снимите флажок **Использовать прикрепленную подпись (сохранить документ и подпись в одном файле \*.sig)**. По умолчанию подпись прикрепляется к подписываемому файлу.
- 5 Чтобы использовать подпись формата **XMLDSig** (см. глоссарий, стр. 64) для XML-файлов, установите соответствующий флажок и выберите шаблон. По умолчанию в настройки добавлен шаблон с параметрами:
  - Подписывается весь XML-документ, подпись помещается в корневой тег.
  - Алгоритм каноникализации — <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>.
  - Алгоритм трансформации — <http://www.w3.org/2000/09/xmlsig#enveloped-signature>.
 Если этот шаблон не подходит, создайте свой и импортируйте его в настройки.
- 6 Чтобы сохранять файл подписи в кодировке Base64, установите соответствующий флажок.
- 7 Чтобы добавлять к электронной подписи подтверждение точного времени заверения файла, настройте подключение к службе **штампов времени** (см. глоссарий, стр. 66). Для этого:
  - 7.1 Установите флажок **Добавить в подпись штамп точного времени**.
  - 7.2 В поле **Адрес TSP-сервера** укажите URL-адрес **TSP-сервера** (см. глоссарий, стр. 64) в формате `http://<IP-адрес или доменное имя>:<порт>/`. Для проверки соединения с указанным TSP-сервером нажмите **Проверить**. Поддерживаются протоколы HTTP и HTTPS.

---

**Внимание!** Чтобы использовать указанный TSP-сервер при заверении электронной подписью с помощью сертификата и ключа ЭП, хранящегося на ПАК ViPNet PKI Service:



- На ПАК ViPNet PKI Service должен быть установлен сертификат издателя и CRL, выпустивший сертификат TSP-сервера, а если сертификат издателя не является корневым, все сертификаты из цепочки сертификации.
  - ПАК ViPNet PKI Service должен иметь доступ к TSP-серверу.
- 

8 С помощью кнопки  укажите папку для сохранения подписанных файлов.

9 Нажмите  **Сохранить**.

## Заверение файла электронной подписью

---



**Примечание.** Вы можете заверять файлы электронной подписью, используя контекстное меню Windows (см. [Работа с программой через контекстное меню Windows](#) на стр. 23).

---

С помощью программы File Unit вы можете заверить файл своей электронной подписью, которая удостоверяет личность отправителя файла и целостность содержащихся в нем данных. Для этого:

- 1 В [главном окне программы](#) (см. рисунок на стр. 22) выполните одно из действий:
    - Нажмите **Выбрать файлы** и выберите один или несколько файлов.
    - Перетащите файлы в главное окно программы.
- 



**Примечание.** Чтобы открыть документ, который вы собираетесь заверить электронной подписью, щелкните название этого документа в разделе **Выбранные файлы**.

---

- 2 В разделе **Доступные операции** установите флажок **Подписать сертификатом**.  
Станут доступны настройки параметров электронной подписи.

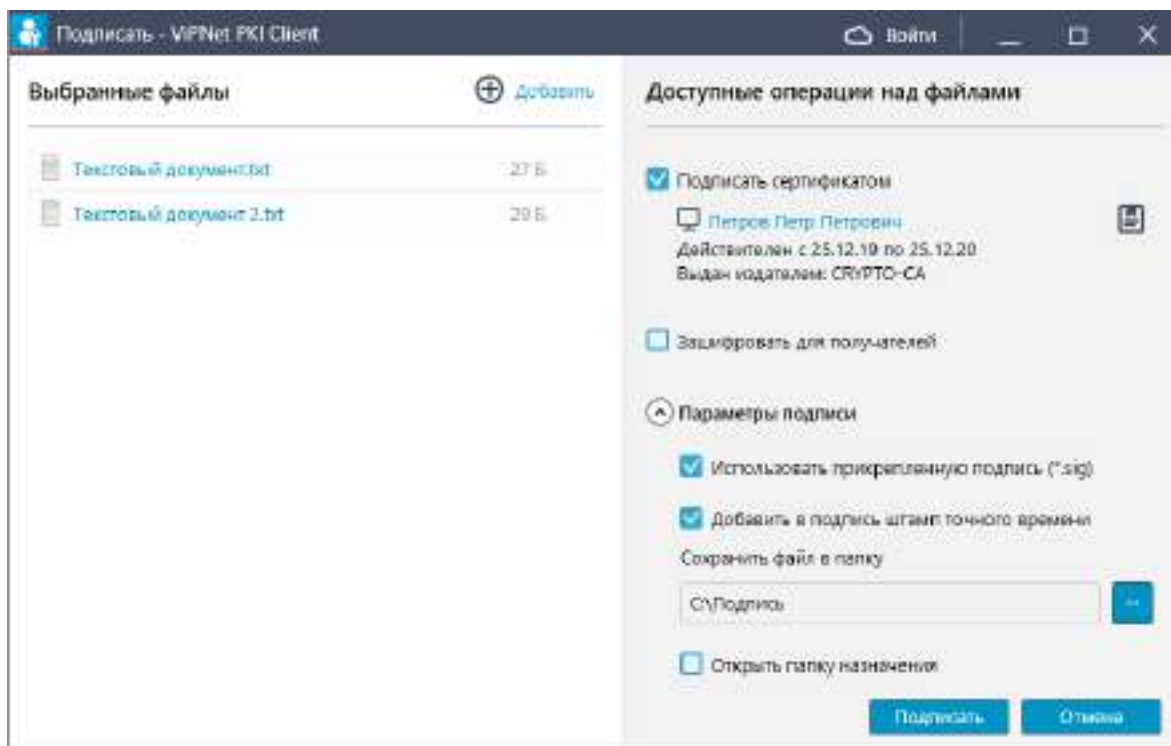


Рисунок 11. Заверение файла электронной подписью

- 3 Если необходимо, измените параметры электронной подписи и нажмите **Подписать**.
- 4 В окне ввода пароля, в зависимости от места хранения вашего контейнера ключей, введите:
  - Пароль контейнера ключей — папка на диске.
  - ПИН-код внешнего устройства — внешнее устройство.
  - Логин и пароль учетной записи пользователя — ПАК ViPNet PKI Service.



**Внимание!** Допускается не более десяти попыток ввода пароля. После десяти неудачных попыток ввода пароля программы File Unit, Web Unit и настройки ViPNet PKI Client будут заблокированы на 15 минут. Количество неудачных попыток ввода пароля считается суммарно для всех файлов. То есть, если при попытке заверить электронной подписью 10 и более файлов вы ввели неверный пароль, указанные программы также будут заблокированы. При вводе верного пароля счетчик, который фиксирует неудачные попытки, обнуляется.

- 5 Дождитесь завершения процесса подписания файлов.

В результате будут сформированы и помещены в выбранную папку файлы:

- <имя файла>.sig, если вы использовали прикрепленную подпись;
- <имя файла>.detached.sig, если вы использовали открепленную подпись.

По окончании заверения файлов электронной подписью в области истории операций с файлами появятся соответствующие записи.

- 6 Чтобы открыть папку с файлом подписи (файл с расширением \*.sig) или с исходным файлом, в [главном окне программы](#) (см. рисунок на стр. 22) в области истории операций с файлами щелкните имя файла и в контекстном меню выберите соответствующий пункт.


# Обеспечение безопасности файлов с помощью шифрования


Передаваемые по открытым каналам данные могут быть перехвачены, искажены либо подменены злоумышленниками. Чтобы обеспечить безопасность данных с помощью программы File Unit и передать их другим пользователям:

- 1 Настройте параметры шифрования (см. [Настройка параметров шифрования](#) на стр. 48).
- 2 Зашифруйте файл (см. [Зашифрование файла](#) на стр. 49).
- 3 Передайте файл получателям любым удобным способом.

## Настройка параметров шифрования

Настройте параметры шифрования, которые будут использоваться по умолчанию в программах File Unit и Web Unit. Для этого:

- 1 Обменяйтесь сертификатами с пользователями, которым вы хотите передавать зашифрованные файлы, например, с помощью электронной почты или съемных носителей.
- 2 Установите полученные сертификаты в хранилище (см. [Установка сертификатов и CRL](#) на стр. 32).
- 3 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 21) и выберите раздел  **Шифрование**.
- 4 Чтобы каждый раз при шифровании файлов не приходилось выбирать сертификат получателя, сформируйте список получателей файлов. Для этого:
  - 4.1 В группе **Получатели зашифрованных файлов** нажмите  **Добавить**.
  - 4.2 Выберите сертификат и нажмите **Выбрать**.
  - 4.3 Аналогичным образом добавьте сертификаты других получателей.

Чтобы удалить сертификат получателя из списка, щелкните значок  (появляется при наведении курсора на строку сертификата).



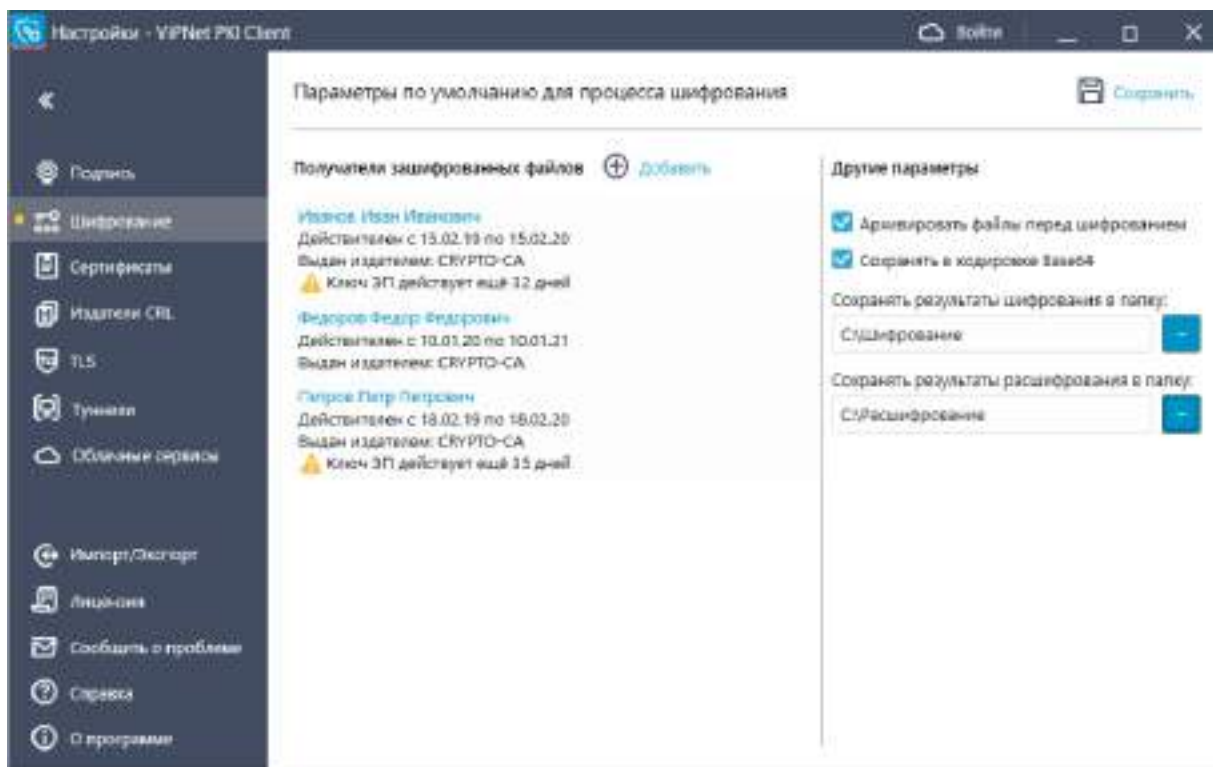




Рисунок 12. Настройка параметров шифрования

- 5 Чтобы перед шифрованием файлы помещались в архив, установите соответствующий флажок.
- 6 Чтобы сохранять зашифрованные файлы в кодировке Base64, установите соответствующий флажок.
- 7 С помощью кнопок  укажите папки для сохранения зашифрованных и расшифрованных файлов.
- 8 Нажмите  **Сохранить**.

В результате будут настроены параметры шифрования файлов.

## Зашифрование файла



**Примечание.** Вы можете зашифровать файлы, используя контекстное меню Windows (см. [Работа с программой через контекстное меню Windows](#) на стр. 23).

С помощью программы File Unit вы можете зашифровать 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 каждый из получателей сможет расшифровать его.

Чтобы зашифровать файл:

- 1 В **главном окне программы** (см. рисунок на стр. 22) выполните одно из действий:
  - Нажмите **Выбрать файлы**. В открывшемся окне выберите один или несколько файлов и нажмите кнопку **Открыть**.
  - Перетащите файлы в главное окно программы.



**Примечание.** Чтобы открыть документ, который вы собираетесь зашифровать, щелкните название этого документа в разделе **Выбранные файлы**.

- 2 В разделе **Доступные операции** установите флажок **Зашифровать для получателей**.  
Станут доступны настройки параметров шифрования.

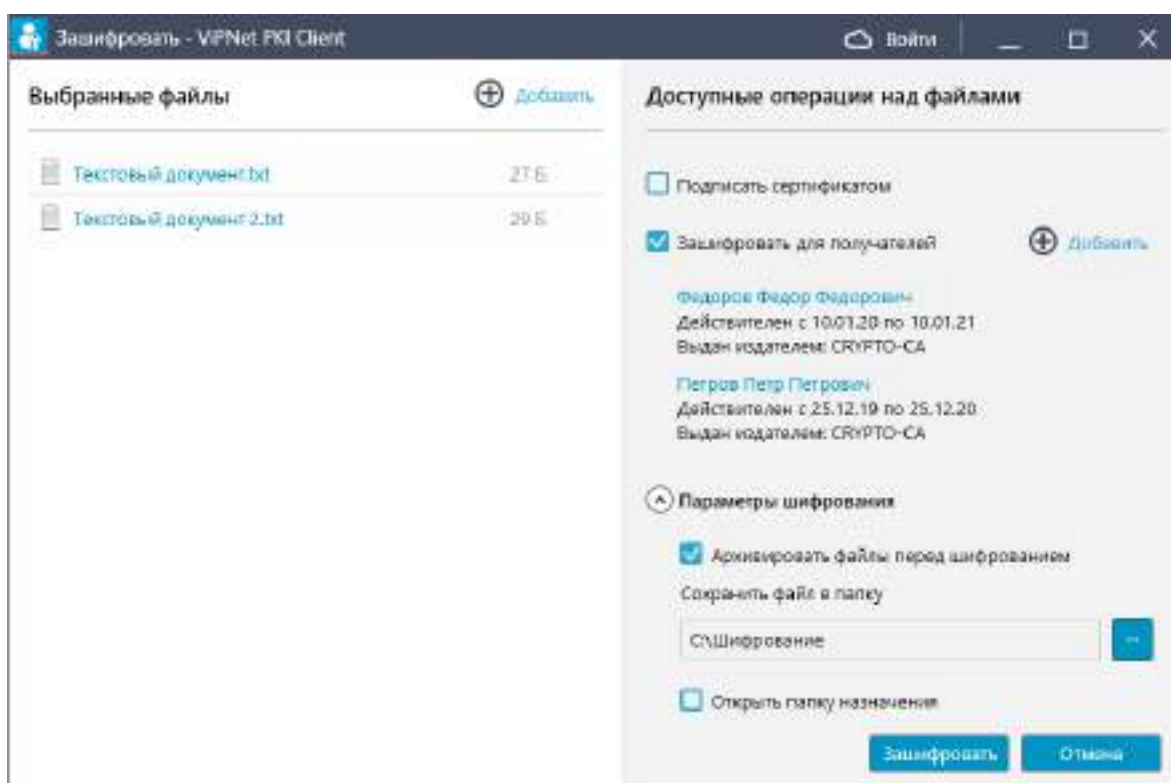


Рисунок 13. Зашифрование файла

- 3 Если необходимо, измените параметры шифрования и нажмите **Зашифровать**.
- 4 Нажмите кнопку **Зашифровать**.
- 5 Дождитесь завершения процесса шифрования.

В результате будут сформированы зашифрованные файлы с расширением \* .enc и помещены в выбранную папку.

- 6 Чтобы открыть папку с зашифрованным или исходным файлом, в **главном окне программы** (см. рисунок на стр. 22) в области истории операций с файлами щелкните имя файла и в контекстном меню выберите соответствующий пункт.

# Заверение электронной подписью и зашифрование файла



**Примечание.** Вы можете заверять электронной подписью и зашифровывать файлы, используя контекстное меню Windows (см. [Работа с программой через контекстное меню Windows](#) на стр. 23).

---

Если вы хотите не только подтвердить личность отправителя, но и обеспечить конфиденциальность содержимого файла, вы можете одновременно заверить файл электронной подписью и зашифровать его.

Чтобы заверить электронной подписью и зашифровать файл:

- 1 [Запустите программу File Unit](#) (на стр. 21).
- 2 В [главном окне программы](#) (см. рисунок на стр. 22) выполните одно из действий:
  - Нажмите **Выбрать файлы** и выберите один или несколько файлов.
  - Перетащите файлы в [главное окно программы](#) (см. рисунок на стр. 22).



**Примечание.** Чтобы открыть документ, который вы собираетесь заверить электронной подписью и зашифровать, щелкните название этого документа в разделе **Выбранные файлы**.

---

- 3 В разделе **Доступные операции** установите флажки **Подписать сертификатом** и **Зашифровать для получателей**.

Станут доступны настройки параметров электронной подписи и шифрования.

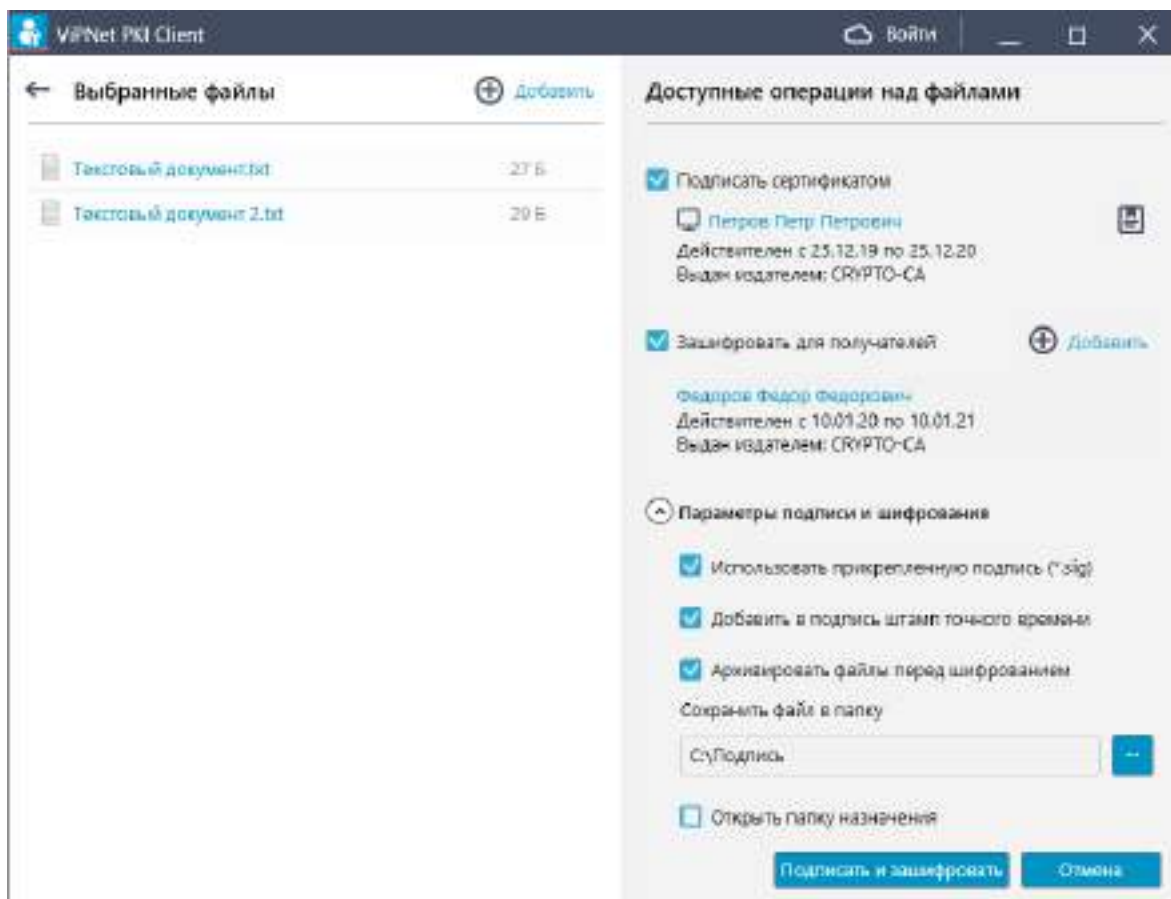


Рисунок 14. Одновременное заверение электронной подписью и шифрование файла

- 4 Если необходимо, измените параметры электронной подписи и шифрования и нажмите **Подписать и зашифровать**.
- 5 В окне ввода пароля, в зависимости от места хранения вашего контейнера ключей, введите:
  - Пароль контейнера ключей — папка на диске.
  - ПИН-код внешнего устройства — внешнее устройство.
  - Логин и пароль учетной записи пользователя — ПАК ViPNet PKI Service.



**Внимание!** Допускается не более десяти попыток ввода пароля. После десяти неудачных попыток ввода пароля программы File Unit, Web Unit и настройки ViPNet PKI Client будут заблокированы на 15 минут. Количество неудачных попыток ввода пароля считается суммарно для всех файлов. То есть, если при попытке заверить электронной подписью и зашифровать десять и более файлов вы ввели неверный пароль, указанные программы также будут заблокированы. При вводе верного пароля счетчик, который фиксирует неудачные попытки, обнуляется.

- 6 Дождитесь завершения процесса заверения электронной подписью и шифрования файлов. В результате будут сформированы и помещены в выбранную папку файлы:
  - <имя файла>.sig.enc, если вы использовали прикрепленную подпись;

- `<имя файла>.detached.sig` и файл электронной подписи `<имя файла>.enc`, если вы использовали открепленную подпись без архивирования файлов перед шифрованием;
  - `<ГТГГММДдчмм>.zip.sig`, если вы использовали открепленную подпись с архивированием файлов перед шифрованием. Файлы электронной подписи и исходные файлы будут содержаться в архиве `*.zip`.
- 7 Чтобы открыть папку с зашифрованным или исходным файлом, в [главном окне программы](#) (см. рисунок на стр. 22) в области истории операций с файлами щелкните имя файла и в контекстном меню выберите соответствующий пункт.

# 6

## Работа с файлами, полученными от других пользователей

Получение зашифрованных и подписанных файлов	55
Расшифрование файла	56
Проверка электронной подписи	58

# Получение зашифрованных и подписанных файлов

При получении файлов, имеющих стандартные расширения \*.sig и \*.enc, от других пользователей с помощью программы File Unit вы можете ознакомиться с их содержимым и удостовериться личность отправителя.

В файлы с расширением \*.sig с электронной подписью ([прикрепленной](#) (см. глоссарий, стр. 65) или [открепленной](#) (см. глоссарий, стр. 65)) помещаются также сертификаты отправителей, подписавших файл. Поэтому для проверки электронной подписи отдельно получать сертификаты других пользователей не требуется.

Чтобы ознакомиться с содержимым полученного файла, по расширению файла определите, какие операции были применены к нему перед отправкой: заверение электронной подписью, шифрование или обе операции. 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. 56).
- Если файл заверен электронной подписью, то есть имеет расширение \*.sig, проверьте электронную подпись (см. [Проверка электронной подписи](#) на стр. 58).
- Если файл заверен электронной подписью и зашифрован, то есть имеет вид <ИМЯ файла>.sig.enc, то выполните расшифрование (см. [Расшифрование файла](#) на стр. 56), а затем проверку электронной подписи (см. [Проверка электронной подписи](#) на стр. 58).

# Расшифрование файла


---



**Примечание.** Вы можете расшифровывать файлы с помощью контекстного меню Windows (см. [Работа с программой через контекстное меню Windows](#) на стр. 23).

---

С помощью программы File Unit вы можете расшифровать полученный от другого пользователя файл, который был зашифрован с использованием вашего сертификата. Для этого:

- 1 В **главном окне программы** (см. рисунок на стр. 22) выполните одно из действий:
    - Нажмите **Выбрать файлы**. Выберите один или несколько файлов с расширением \*.enc.
    - Перетащите файлы с расширением \*.enc в главное окно программы.
  - 2 Щелкните имя файла в разделе **Выбранные файлы**.
  - 3 Если файл зашифрован с помощью нескольких ваших личных сертификатов, в группе **Расшифровать используя сертификат** с помощью кнопки  выберите сертификат для расшифрования.
  - 4 При необходимости измените параметры расшифрования и нажмите **Расшифровать**.
- 



**Примечание.** Если в хранилище сертификатов Windows не найден сертификат для расшифрования и настроено подключение к ПАК ViPNet PKI Service (установлен флажок **Предлагать расшифрование в облаке**), щелкните ссылку **Расшифровать**. ViPNet PKI Client расшифрует файл на ПАК ViPNet PKI Service, если на нем установлен подходящий сертификат.

---



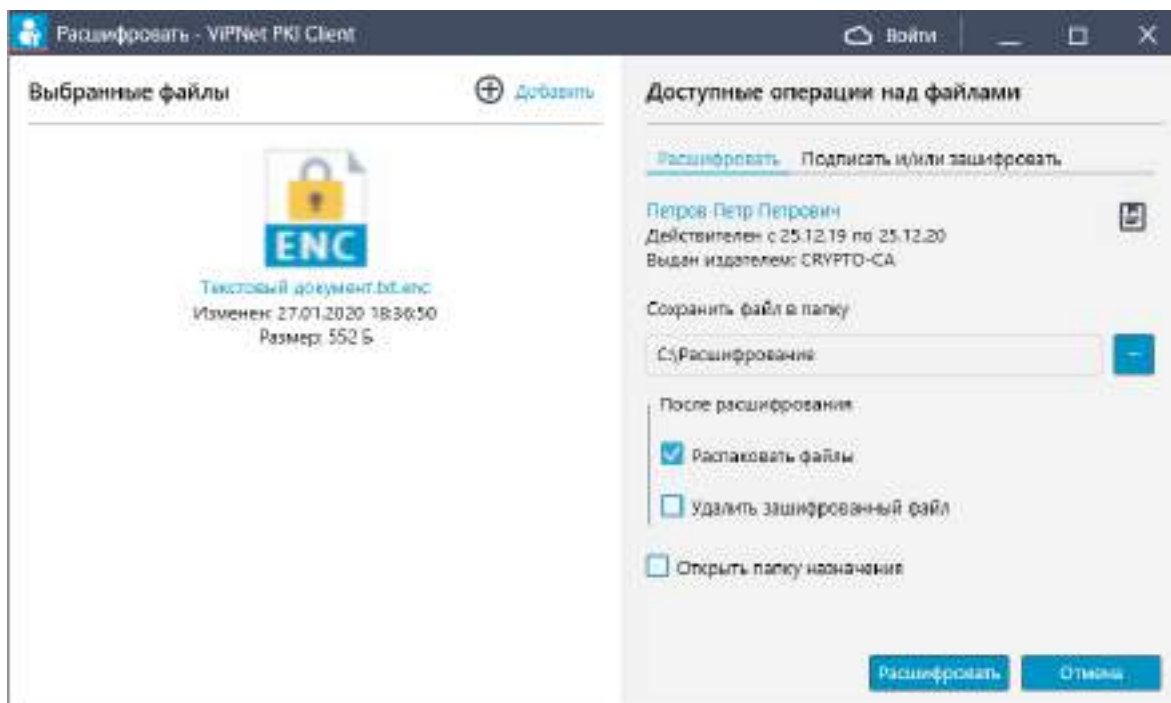


Рисунок 15. Расшифрование файла

- 5 В окне ввода пароля, в зависимости от места хранения вашего контейнера ключей, введите:
  - Пароль контейнера ключей — папка на диске.
  - ПИН-код внешнего устройства — внешнее устройство.



**Внимание!** Допускается не более десяти попыток ввода пароля. После десяти неудачных попыток ввода пароля программы File Unit, Web Unit и настройки VIPNet PKI Client будут заблокированы на 15 минут. Количество неудачных попыток ввода пароля считается суммарно для всех файлов. То есть, если при попытке расшифровать 10 и более файлов вы ввели неверный пароль, указанные программы также будут заблокированы. При вводе верного пароля счетчик, который фиксирует неудачные попытки, обнуляется.

- 6 Выполните шаги 2-5 для остальных зашифрованных файлов.
- 7 Чтобы открыть папку с расшифрованным или исходным файлом, в [главном окне программы](#) (см. рисунок на стр. 22) в области истории операций с файлами щелкните имя файла и в контекстном меню выберите соответствующий пункт.

В результате файл будет расшифрован и помещен в выбранную папку.

# Проверка электронной подписи



**Примечание.** Вы можете проверять электронную подпись, используя контекстное меню Windows (см. [Работа с программой через контекстное меню Windows](#) на стр. 23).

Чтобы проверить электронную подпись файлов, полученных от других пользователей:

- 1 Запустите программу File Unit (на стр. 21).
- 2 В **главном окне программы** (см. рисунок на стр. 22) выполните одно из действий:
  - Нажмите **Выбрать файлы** и выберите один или несколько файлов с расширением \*.sig.
  - Перетащите нужные файлы с расширением \*.sig в главное окно программы.
- 3 В зависимости от количества выбранных файлов и типа электронной подписи:
  - Если вы выбрали один файл с прикрепленной электронной подписью, результат проверки электронной подписи будет отображен в разделе **Выбранные файлы**.

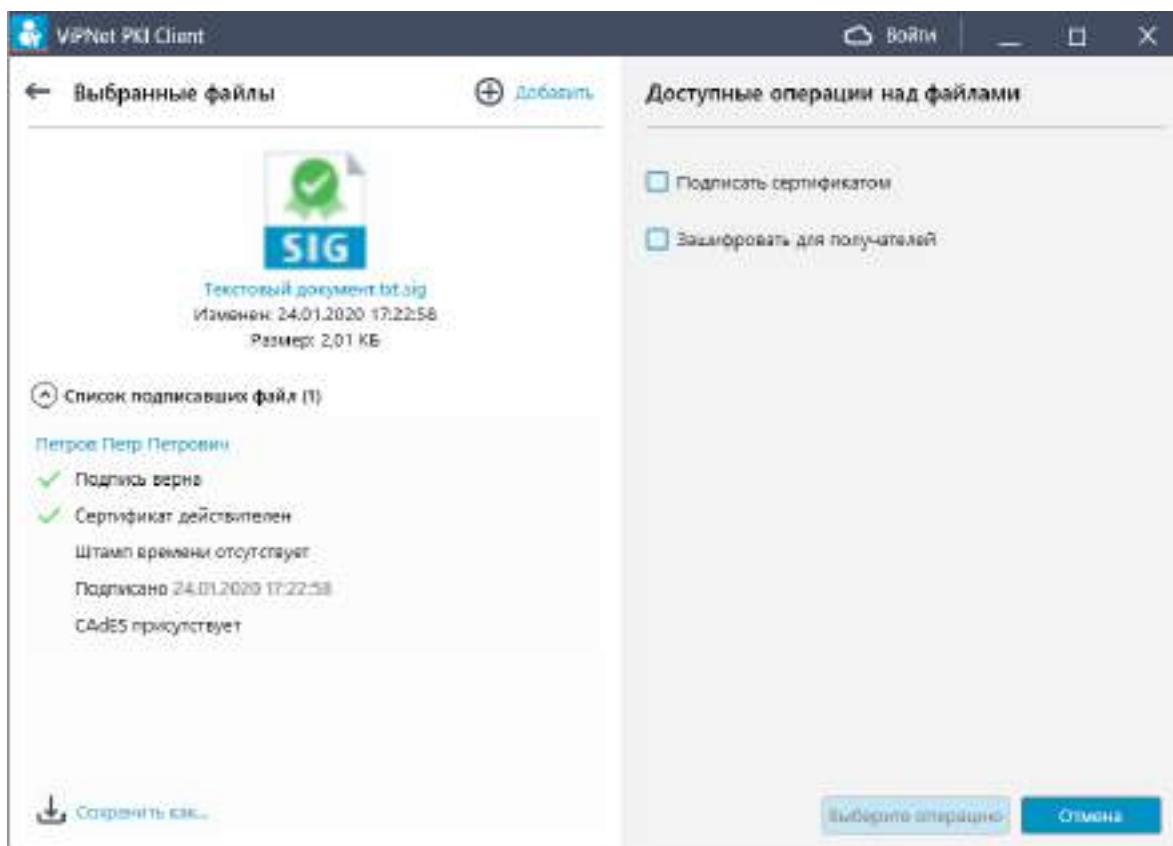


Рисунок 16. Проверка прикрепленной электронной подписи

- Если вы выбрали один файл с открепленной электронной подписью (то есть исходный файл не был помещен совместно с электронной подписью в файл \*.sig), укажите

исходный файл с помощью соответствующей кнопки или перетащите его в выделенную область.



**Примечание.** Если исходный файл и файл подписи расположены в одной папке, проверка электронной подписи произойдет автоматически.

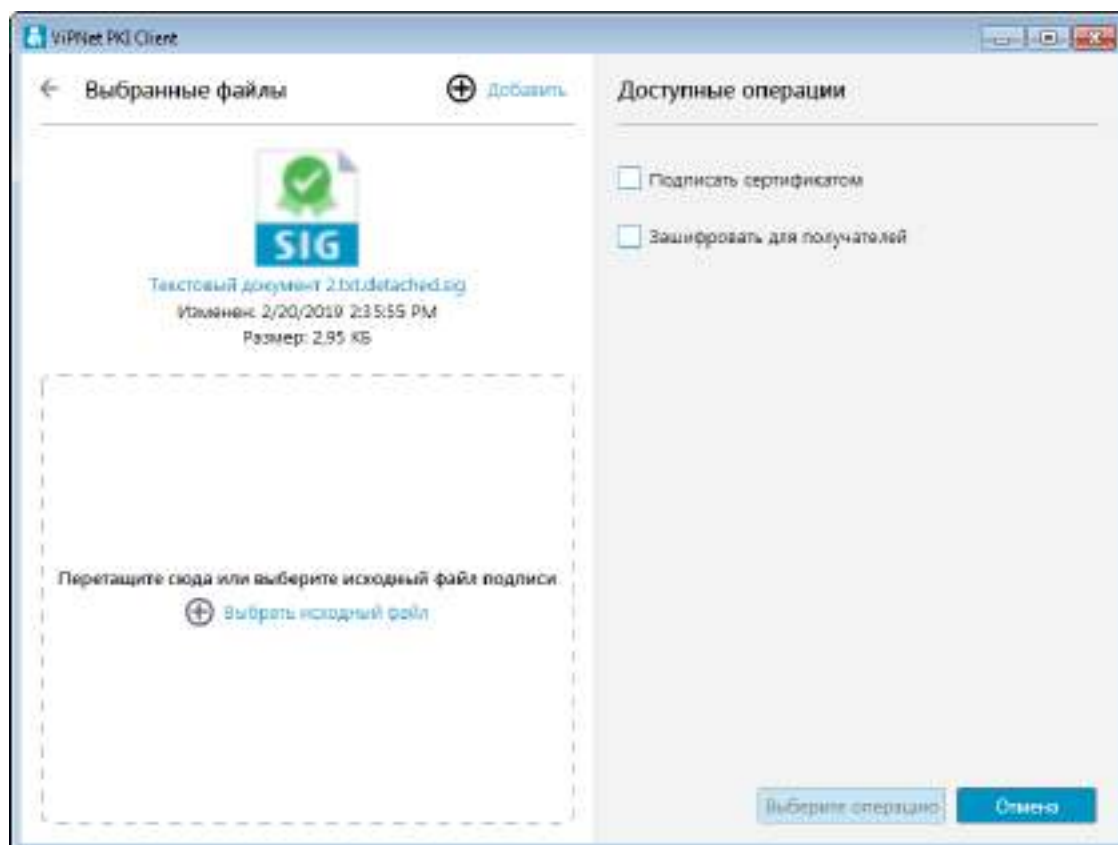



Рисунок 17. Проверка открепленной электронной подписи

- Если вы выбрали несколько файлов, то для проверки электронной подписи щелкните значок  напротив имени файла:
  - Если для заверения файла использовалась прикрепленная электронная подпись. Результат проверки подписи будет отображен в отдельном окне.
  - Если для заверения файла использовалась открепленная электронная подпись, в открывшемся окне укажите исходный файл и нажмите кнопку **Открыть**. Результат проверки подписи также будет отображен в отдельном окне.

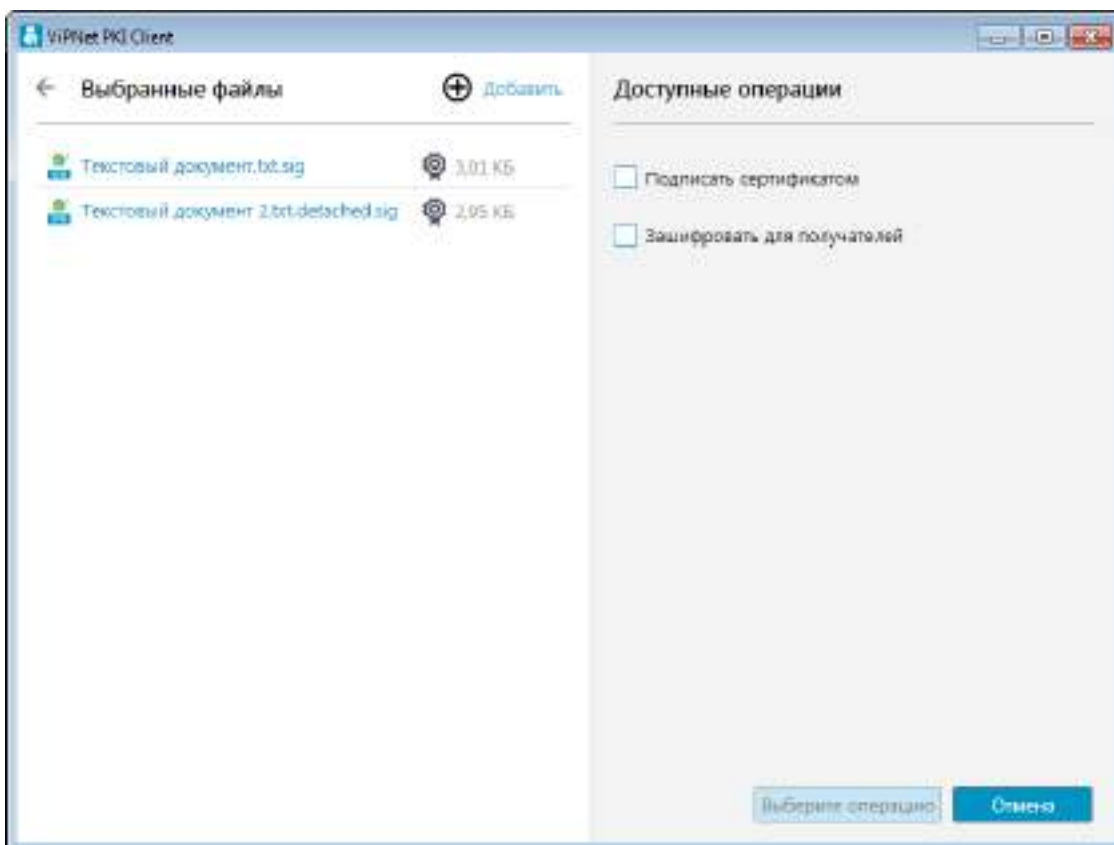


Рисунок 18. Проверка электронной подписи нескольких файлов

4 В окне с результатами проверки подписи:

- Щелкните имя владельца подписи, чтобы просмотреть информацию о его сертификате.
- Если к подписи был добавлен штамп времени, щелкните ссылку **присутствует**, чтобы просмотреть информацию о нем.
- Сохраните исходный файл.
- Если при проверке подписи не удалось проверить сертификат подписанта с помощью сертификатов, установленных в хранилище сертификатов Windows (например, истек CRL издателя), и настроено подключение к ПАК ViPNet PKI Service (установлен флажок **Предлагать проверять ЭП в облаке**), щелкните ссылку **Проверить**. ViPNet PKI Client проверит подпись на ПАК ViPNet PKI Service.

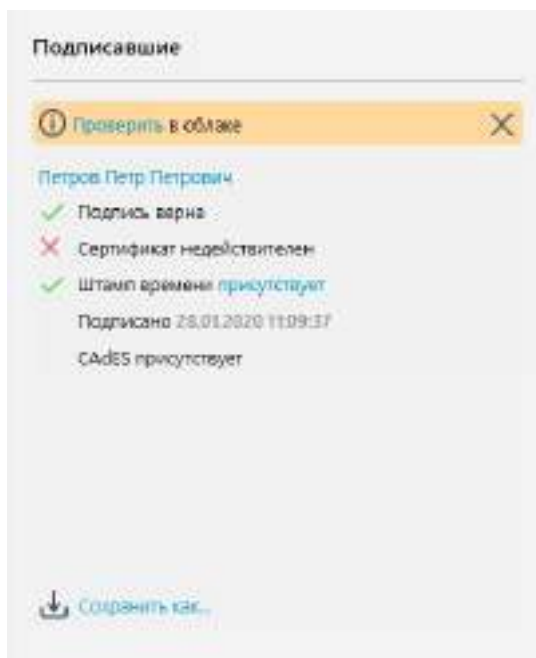


Рисунок 19. Результаты проверки подписи

# 7

## Возможные неполадки и способы их устранения

Требуемый сертификат не отображается в списке сертификатов для подписи

63

# Требуемый сертификат не отображается в списке сертификатов для подписи

При заверении файлов электронной подписью с помощью программы File Unit в окне **Выбор сертификата** нужный сертификат может не отображаться.

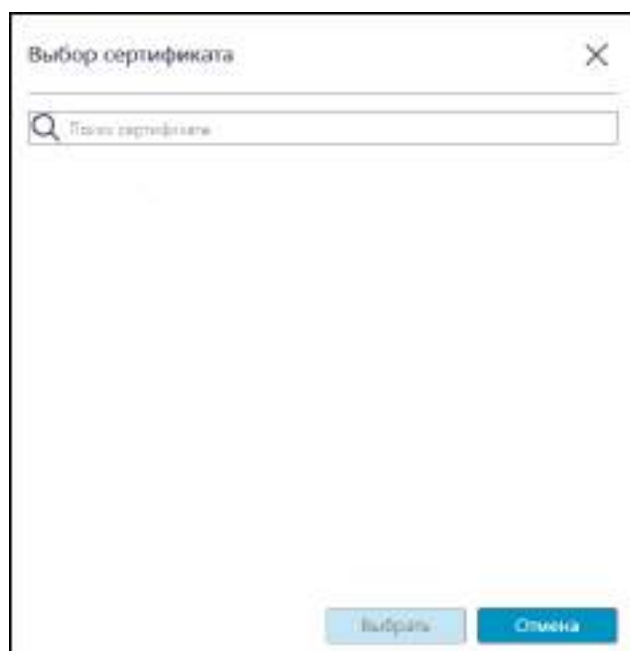


Рисунок 20. Сертификат не отображается в списке сертификатов для подписи

В этом случае нужно проверить, что для сертификата соблюдаются требования, перечисленные в разделе [Требования к сертификатам для заверения электронной подписью и шифрования](#) (на стр. 14).

# А

## Глоссарий

### TSP-сервер (служба штампов времени)

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

### XMLDSig

Формат подписи, позволяющий подписывать не только весь XML-документ, но и его часть, причем разные части XML-документа могут быть подписаны разными пользователями.

### Асимметричное подписание

Система подписания, при которой алгоритмы используют два математически связанных ключа. Закрытый ключ используется для подписи файла, а с помощью открытого ключа и сертификата пользователя подпись подтверждается.

### 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.

### Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.



## Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

## Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

## Открепленная подпись

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

Например, при подписании `file.txt` открепленная 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.

## 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.

## Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

## Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

## Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

## Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

### Файл \*.enc

Файл с расширением \*.enc, который содержит в себе файл, зашифрованный с использованием ключа проверки электронной подписи получателя или нескольких получателей.

### Файл \*.sig

Файл с расширением \*.sig, который содержит в себе электронную подпись, служебную информацию, сертификат ключа проверки электронной подписи, с помощью которого была сформирована данная электронная подпись, а также исходный файл (в случае использования прикрепленной подписи).

## Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

## 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.

## Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.