



ViPNet CSP 4.4

Руководство пользователя

Версия продукта: 4.4.10

© АО «ИнфоТеКС», 2023

ФРКЕ.00106-09 34 01

Версия продукта 4.4.10

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 АО «ИнфоТеКС».

ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	9
О документе.....	10
Соглашения документа.....	10
О программе	11
Системные требования.....	12
Комплект поставки.....	13
Что нового в версии 4.4.10.....	14
Обратная связь.....	15
 Глава 1. Использование криптографических функций в системах защиты данных	16
Назначение криптопровайдера.....	17
Варианты использования ViPNet CSP	18
Совместимость с ПО других производителей	18
 Глава 2. Установка и запуск программы.....	21
Установка программы	22
Установка из MSI-пакетов.....	Ошибка! Закладка не определена.
Обновление программы	25
Добавление, удаление и восстановление компонентов программы.....	27
Запуск программы.....	29
Подготовка к применению ViPNet CSP	30
 Глава 3. Регистрация ViPNet CSP	31
Зачем нужно регистрировать ViPNet CSP	32
Порядок регистрации	33
Получение кода регистрации	35
Получение кода регистрации через Интернет.....	35
Получение кода регистрации по электронной почте.....	37
Получение кода регистрации по телефону.....	38
Получение кода регистрации через файл	39
Регистрация ViPNet CSP	41
Сохранение регистрационных данных	42
Если конфигурация компьютера изменилась	43
Автоматическая регистрация.....	44

Глава 4. Получение закрытого ключа и сертификата	45
Общая информация о ключах и сертификатах.....	46
Порядок получения закрытого ключа и сертификата.....	48
Создание запроса на сертификат и формирование закрытого ключа.....	49
Глава 5. Установка контейнеров ключей и сертификатов	54
Способы установки закрытого ключа и сертификата	55
Установка контейнера ключей из папки.....	56
Установка контейнера ключей с внешнего устройства.....	59
Добавление сертификата в контейнер ключей.....	60
Установка сертификата в системное хранилище Windows	62
Установка сертификата из файла.....	62
Установка сертификата из контейнера ключей	65
Установка сертификата издателя и списка аннулированных сертификатов	68
Установка и обновление CRL через Интернет.....	70
Глава 6. Операции с контейнерами ключей	71
Просмотр и настройка свойств контейнера ключей.....	72
Смена пароля к контейнеру ключей	72
Удаление сохраненного пароля.....	74
Проверка контейнера ключей.....	74
Настройка прав доступа к контейнеру ключей.....	75
Создание резервной копии контейнера ключей.....	77
Перенос сертификатов и закрытых ключей между компьютерами	78
Экспорт сертификата и закрытого ключа в файл.....	78
Импорт сертификата и закрытого ключа из файла.....	80
Использование ключей подписи пользователя сетевого узла.....	81
Удаление контейнера ключей	82
Глава 7. Работа с внешними устройствами.....	83
Доступ к контейнерам ключей на внешнем устройстве	84
Настройка списка опрашиваемых устройств.....	85
Инициализация устройства	87
Особенности работы с внешними устройствами, на которых установлено более одного апплета.....	89
Смена ПИН-кода	90
Использование датчика случайных чисел	91
Глава 8. Дополнительные настройки ViPNet CSP	93

Настройка регистрации событий криптопровайдера	94
Просмотр событий криптопровайдера в системном журнале	95
Включение аудита доступа к объектам.....	96
Добавление элементов аудита доступа к объектам	97
Глава 9. Использование функций криптопровайдера при разработке программ	99
Настройка проекта для использования функций ViPNet CSP.....	100
Криптографические библиотеки, входящие в состав ViPNet CSP	101
Глава 10. Интеграция ViPNet CSP с центром сертификации на базе Microsoft CA	102
Порядок действий.....	103
Развертывание центра сертификации Microsoft CA.....	104
Глава 11. Электронная подпись в документах Microsoft Office	106
Электронная подпись.....	107
Подписание документов Microsoft Word, Excel и PowerPoint	108
Microsoft Office 2010	108
Microsoft Office 2013	109
Просмотр электронной подписи в Microsoft Word, Excel и PowerPoint	111
Microsoft Office 2010	111
Microsoft Office 2013	112
Удаление электронной подписи в Microsoft Word, Excel и PowerPoint.....	114
Microsoft Office 2010	114
Microsoft Office 2013	114
Видимая строка подписи в документах Microsoft Word и Excel	115
Вставка видимой строки подписи	115
Добавление электронной подписи в строку подписи	116
Глава 12. Электронная подпись и шифрование в Microsoft Outlook	118
Шифрование и подписание документов	119
Порядок организации обмена защищенными сообщениями.....	121
Обмен сертификатами с получателем сообщения	122
Настройка дополнительных параметров электронной подписи и шифрования	124
Добавление электронной подписи к отдельному сообщению	126
Добавление электронной подписи ко всем сообщениям	128
Просмотр электронной подписи сообщения	130
Шифрование сообщений электронной почты.....	131
Шифрование документов и файлов	133
Просмотр зашифрованных сообщений	134

Глава 13. Электронная подпись макросов, форм и баз данных	135
Электронная подпись в Microsoft Office InfoPath	136
Разрешение подписывать форму InfoPath электронной подписью	136
Подписание формы InfoPath	137
Просмотр подписи в форме InfoPath	138
Удаление подписи из формы InfoPath	138
Электронная подпись макросов.....	140
Подписание макросов	140
Проверка подписи макроса	141
Удаление подписи макроса.....	141
Подписание базы данных Microsoft Access	141
 Глава 14. Организация защищенного TLS-соединения	142
TLS-соединение.....	143
Организация доступа к защищенному веб-серверу	144
Настройка серверной части	144
Настройка клиентской части	145
Настройка веб-браузера Internet Explorer для работы по протоколу TLS	146
Проверка доступности веб-узла по защищенному протоколу HTTPS.....	147
 Глава 15. Взаимодействие с ViPNet HSM.....	148
Общие сведения о ViPNet HSM	149
Настройка взаимодействия с ViPNet HSM.....	150
 Глава 16. Региональные настройки.....	150
Региональные настройки в Windows	151
 Приложение А. Возможные неполадки.....	155
Требование обновления Windows при установке ViPNet CSP	155
Не удается запустить ViPNet CSP из-за нарушения целостности файлов программы.....	155
Не удается получить код регистрации через Интернет	156
Проблемы при использовании аппаратного модуля доверенной загрузки «Аккорд-АМДЗ».....	156
Проблемы при использовании устройства типа SafeNet eToken (eToken Aladdin)..	157
Сертификат автоматически некорректно устанавливается в хранилище при подключении внешнего устройства	157
Не удается зашифровать документ.....	158
Адрес электронной почты из сертификата не найден в списке адресов контакта	158

Недопустимый сертификат.....	160
Не удается поставить электронную подпись.....	161
Не найден закрытый ключ, соответствующий сертификату	161
Не удается подписать сообщение электронной почты	161
Не удалось подписать сообщение электронной почты нужным сертификатом.....	161
Невозможно редактировать подписанный документ Microsoft Word или Excel.....	162
Нет соединения с сервером по протоколу TLS	162
На IIS-сервере и веб-клиенте установлены разные версии ViPNet CSP	162
Не установлены сертификаты пользователя, издателя, CRL в нужное хранилище	163
Веб-браузер не настроен на работу по протоколу TLS	165
Требуется перезапуск службы сервера IIS	166
Требуется сохранить пароль к сертификату сервера	166
На компьютере установлен антивирус Kaspersky Internet Security	167
После обновления Windows пропало соединение по протоколу TLS	168
После обновления ViPNet CSP пропало TLS-соединение, организованное с помощью стороннего ПО	168
Не удается подключиться к центру сертификации Microsoft CA по протоколу HTTP	169
При соединении с сервером выводится предупреждение системы безопасности	169
Аварийная остановка ViPNet CSP при одновременном использовании нескольких внешних устройств	171
Не удается подключиться к компьютеру с ViPNet CSP по протоколу RDP.....	172
Проверка целостности файлов программы.....	172
Статистический контроль датчиков случайных чисел программы	173
Восстановление системных файлов и параметров ОС Windows после неудачной установки ViPNet CSP.....	174
Повторная регистрация для устранения неполадок	176
После обновления ViPNet CSP исчезли ранее сохраненные пароли контейнеров ключей	177
Предоставление дополнительной информации о неисправности	178
Приложение В. Внешние устройства	180
Список поддерживаемых внешних устройств.....	181
Алгоритмы и функции, поддерживаемые внешними устройствами	184
Приложение С. История версий	186
Версия 4.4.8.....	186

Версия 4.4.6.....	186
Версия 4.4.4.....	187
Версия 4.4.2.....	187
Версия 4.4.0.....	188
Версия 4.2.11	189
Версия 4.2.10	190
Версия 4.2.9.....	190
Версия 4.2.8.....	191
Версия 4.2.2.....	195
Версия 4.2.0.....	197
Версия 4.1.0.....	197
Версия 4.0.0.....	200
 Приложение D. Термины и сокращения	 205



Введение

О документе	10
О программе	11
Что нового в версии 4.4.10	14
Обратная связь	15

О документе

Документ поможет вам установить, настроить и использовать программу ViPNet CSP (далее — ViPNet CSP). В документе описаны сценарии применения ViPNet CSP для шифрования документов и сообщений электронной почты, подписания и проверки подлинности электронной подписи, организации удаленного доступа к ресурсам по протоколам TLS и взаимодействия с ПАК ViPNet HSM для защищенного хранения ключей и выполнения криптографических операций.

Соглашения документа

Обозначение	Описание
	Внимание! Содержит критически важную информацию
	Примечание. Содержит рекомендательную информацию
	Совет. Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке

О программе

ViPNet CSP — [криптопровайдер](#), обеспечивающий вызов криптографических функций из приложений Microsoft и другого ПО, которое использует интерфейс CryptoAPI 2.0.

С помощью ViPNet CSP вы можете:

- создавать ключи [электронной подписи](#) по ГОСТ Р 34.10-2012;
- формировать электронную подпись по ГОСТ Р 34.10-2012;
- проверять электронную подпись по ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;
- хэшировать данные по ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012;
- шифровать и использовать имитозащиту данных по ГОСТ 28147-89, ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018 доступен только для ViPNet CNG);
- создавать последовательность случайных и псевдослучайных чисел, сеансовых ключей шифрования;
- проводить аутентификацию и выработку сеансового ключа при передаче данных по протоколу TLS;
- хранить сертификаты открытых ключей непосредственно в контейнерах ключей;
- работать с электронными ключами на [внешних устройствах](#).

ViPNet CSP совместим с криптопровайдерами других производителей при условии реализации ими требований, содержащихся в документах:

- [RFC 4357 «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms»](#);
- [RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax \(CMS\)»](#);
- [RFC 4491 «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure»](#);
- [RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012»](#);
- [П 50.1.111-2016 «Парольная защита ключевой информации»](#);
- [П 50.1.112-2016 «Транспортный ключевой контейнер»](#);
- [П 50.1.113-2016 «Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»](#);
- [П 50.1.114-2016 «Параметры эллиптических кривых для криптографических алгоритмов и протоколов»](#);
- [П 1323565.1.023-2018 «Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов \(CRL\) и запросе на сертификат PKCS#10 инфраструктуры открытых ключей X.509»](#);

- Р 1323565.1.017-2018 «Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»;
- Р 1323565.1.025-2019 «Форматы сообщений, защищенных криптографическими методами»;
- Р 1323565.1.024-2019 «Параметры эллиптических кривых для криптографических алгоритмов и протоколов»;
- Р 1323565.1.020–2020 «Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».

Системные требования

- 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.
- Свободное место на жестком диске — не менее 100 Мбайт.
- Операционная система:
 - Windows 10 — 32/64-разрядная, следующих версий и сборок:
 - версия 1507, сборка 10240,
 - версия 1607, сборка 14393,
 - версия 1809, сборка 17763,
 - версия 21H2, сборка 19044,
 - версия 22H2, сборка 19045;
 - Windows 11 — 64-разрядная, следующих версий и сборок:
 - версия 21H2, сборка 22000,
 - версия 22H2, сборка 22621,
 - версия 23H2, сборка 22631;
 - Windows Server 2016 — 64-разрядная, сборка 14393;
 - Windows Server 2019 — 64-разрядная, сборка 17763;
 - Windows Server 2022 — 64-разрядная, сборка 20348.

Для каждой из указанных сборок должны быть установлены последние пакеты обновлений. Работа ViPNet CSP на компьютерах, работающих под управлением операционных систем других сборок, не гарантируется.

Если локализация ОС отличается от русской, для правильного отображения кириллицы в ViPNet CSP измените [региональные настройки Windows](#).



Примечание. В Windows 10 и Windows Server 2016 не поддерживается организация защищенных подключений по протоколу TLS в браузере Microsoft Edge.

- Используемый браузер — Microsoft Edge (в режиме совместимости с IE11).
- ПО для использования функций ЭП — Microsoft Office версии 2010 или 2013.
- Допускается работа в виртуальных средах:
 - Microsoft Hyper-V;
 - VMware VSphere ESX;
 - VMware Workstation;
 - VMware Player;
 - Oracle VM VirtualBox.

ViPNet CSP поддерживает работу с несколькими типами устройств хранения электронных ключей. Подробную информацию о поддерживаемых внешних устройствах см. в приложении [Внешние устройства](#).

В случае обновления ОС до версии, которая не поддерживается текущей версией ViPNet CSP, отобразится сообщение о несовместимости. В таком случае обновите ViPNet CSP.

Работу с неподдерживаемой версией ОС можно продолжить, но стабильность работы не гарантируется. ViPNet CSP может некорректно определять версию ОС при использовании версий Windows Insider.

Комплект поставки

- Установочный файл ViPNet CSP.
- Документы в формате PDF:
 - ViPNet CSP 4.4. Руководство пользователя,
 - ViPNet CSP 4.4. Быстрый старт,
 - ViPNet CSP. Лицензионные соглашения на компоненты сторонних производителей,
 - Криптографический интерфейс ViPNet CSP 4.4. Руководство разработчика,
 - Криптографический интерфейс ViPNet CNG. Руководство разработчика,
 - ViPNet CSP 4.4. Формуляр.

Что нового в версии 4.4.10

Изменения в предыдущих версиях см. в приложении [История версий](#).

Обзор изменений в версии 4.4.10 по сравнению с 4.4.8:

- **Расширение списка поддерживаемых внешних устройств**

Добавлена совместимость с устройствами ESMART Token 192K.

- **Поддержка обновлений Windows 11**

К поддерживаемым версиям и сборкам Windows 11 добавлены:

- версия 22H2, сборка 22621;
- версия 23H2, сборка 22631.

- **Поддержка новых драйверов для внешних устройств**

Для работы с устройствами JaCarta поддерживается работа с драйвером «Единый Клиент JaCarta 3.0».

- **Изменения в интерфейсе**

В интерфейс 4.4.10 добавлен раздел с контактной информацией.

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телеграм-канал поддержки: t.me/vhd21
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

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

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



1

Использование криптографических функций в системах защиты данных

Назначение криптопровайдера	17
Варианты использования ViPNet CSP	18

Назначение криптопровайдера

Криптопровайдер используется для защиты электронных документов криптографическими методами, например с помощью шифрования или электронной подписи.

ViPNet CSP сертифицирован по требованиям ФСБ России, что позволяет использовать его для защиты сведений ограниченного доступа.



Примечание. Криптопровайдер Microsoft Base Cryptographic Provider, встроенный в Windows, не имеет сертификатов ФСБ России.

Криптопровайдер ViPNet CSP предназначен для:

- Авторизации и обеспечения подлинности документов в процессе защищенного документооборота. Для этого используются алгоритмы создания электронной подписи по ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 и проверки электронной подписи по ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Обеспечения конфиденциальности и контроля целостности информации путем ее шифрования и имитозащиты по ГОСТ 28147-89.
- Обеспечения аутентичности и конфиденциальности передачи информации с помощью протокола TLS.

Варианты использования ViPNet CSP

С помощью ViPNet CSP вы можете:

- подписывать сообщения Microsoft Outlook;;
- зашифровывать сообщения Microsoft Outlook и вложенные файлы;;
- создавать и проверять электронную подпись в приложениях Microsoft Office;
- подписывать формы Microsoft Office InfoPath;
- подписывать макросы в программах Microsoft Word, Excel, Outlook, PowerPoint, Access, Publisher и Visio;
- устанавливать защищенные веб-соединения TLS, используя сервер IIS и браузер Microsoft Internet Explorer;
- выполнять криптографические функции в системах электронного документооборота Docsvision и ViPNet ЭДО;
- выполнять криптографические операции для работы службы сертификатов Active Directory.

Совместимость с ПО других производителей

ViPNet CSP можно установить на одном компьютере с криптопровайдером другого производителя, однако при этом некоторые функции программы могут быть недоступны (см. [Варианты использования ViPNet CSP](#)).

Пример настройки ViPNet CSP для работы с криптопровайдером другого производителя описан ниже и применим для всех криптопровайдеров, использующих алгоритмы ГОСТ.

Совместимость с ПО КриптоПро CSP

Сертификаты, созданные в удостоверяющем центре КриптоПро по запросу из ViPNet CSP, могут использоваться криптопровайдером ViPNet CSP.

Сертификаты, созданные с помощью программы ViPNet Удостоверяющий и ключевой центр по запросу из КриптоПро CSP, могут использоваться криптопровайдером КриптоПро CSP.



Внимание! Контейнеры ключей, созданные с помощью криптопровайдера ViPNet CSP, невозможно использовать в КриптоПро CSP. Для работы с ними в КриптоПро CSP экспортируйте и импортируйте их через файл *.pfx.

Использование криптопровайдера ViPNet CSP

- 1 Убедитесь, что компонент ПО КриптоПро CSP «Совместимость с продуктами Microsoft» не установлен на компьютере.
- 2 В ViPNet CSP в разделе **Дополнительно** выберите **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.

Чтобы после установки ViPNet CSP вернуть приоритет КриптоПРО CSP, выполните его восстановление или переустановку (например для работы ПО Citrix).

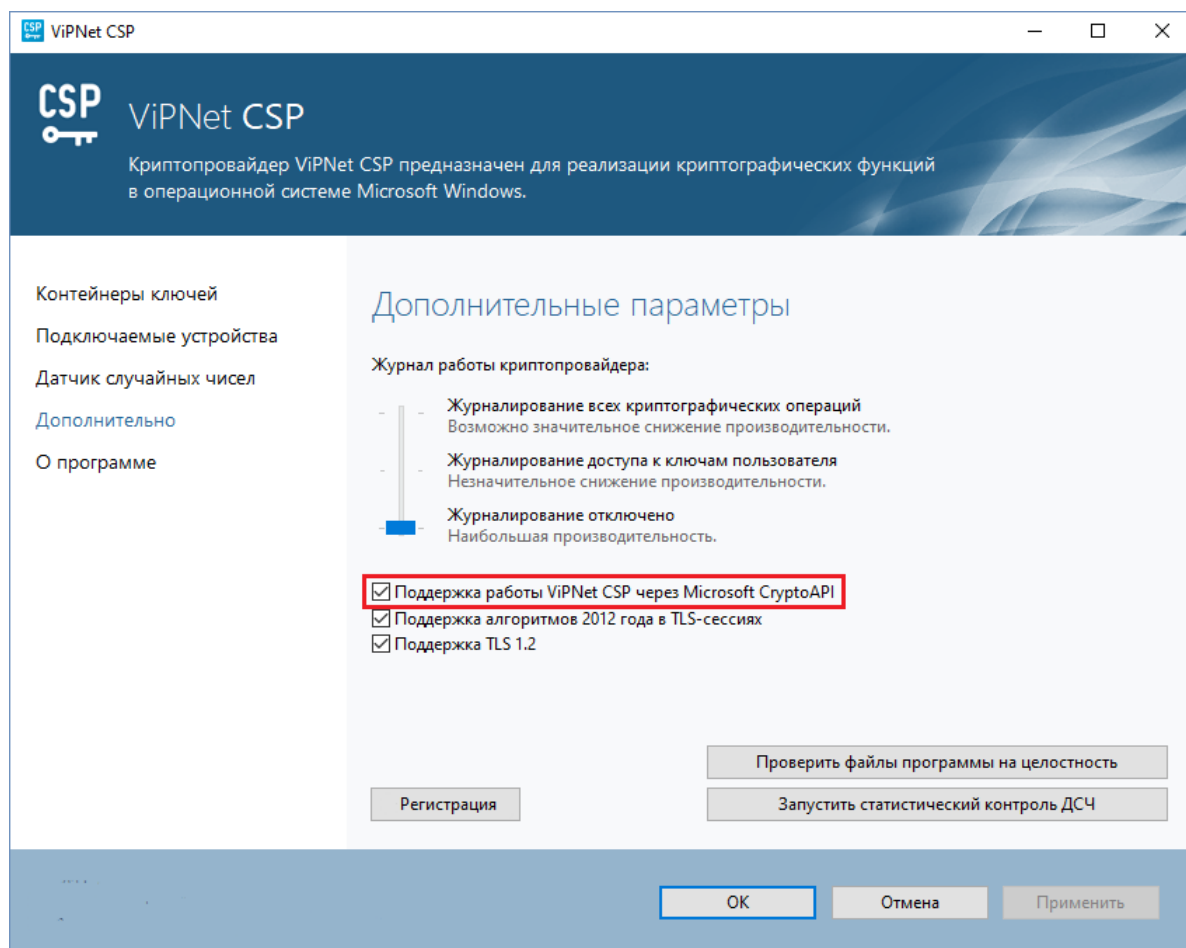


Рисунок 1. Использование ViPNet CSP при одновременной работе с криптопровайдером КриптоПро CSP

Использование криптопровайдера КриптоПро CSP

- 1 В ViPNet CSP в разделе **Дополнительно** снимите флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.

Внимание! Не устанавливайте на компьютер компонент ПО КриптоПро CSP «Совместимость с продуктами Microsoft», если в ViPNet CSP установлен флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.



Несоблюдение этого шага перед установкой компонента может привести к нестабильной работе отдельных программ или операционной системы в целом (вплоть до невозможности её загрузки).

Для возможности восстановления ОС в случае сбоя, создайте контрольную точку восстановления.

- 2 Убедитесь, что компонент КриптоПро CSP «Совместимость с продуктами Microsoft» установлен на компьютере.
- 3 Повторно установите или восстановите КриптоПро CSP.
- 4 Для использования электронной подписи в Microsoft Office установите программу КриптоПро Office Signature.

По умолчанию после установки ViPNet CSP на компьютер с уже установленным ПО КриптоПро CSP флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** снят. В этом случае криптографические операции продолжают выполняться с помощью криптопровайдера КриптоПро CSP.

Если на вашем компьютере установлены ViPNet CSP и ПО КриптоПро CSP и вы хотите удалить ViPNet CSP, то для сохранения работоспособности ОС:

- 1 Удалите ViPNet CSP (см. [Добавление, удаление и восстановление компонентов программы](#)) и не перезагружайте компьютер.
- 2 Запустите установочный файл КриптоПро CSP и восстановите компоненты ПО.
- 3 Перезагрузите компьютер.

Если на вашем компьютере установлены ViPNet CSP и ПО КриптоПро CSP и вы хотите удалить ПО КриптоПро CSP, то для сохранения работоспособности ОС:

- 1 Удалите КриптоПро CSP и не перезагружайте компьютер.
- 2 Запустите установочный файл ViPNet CSP и восстановите компоненты программы (см. [Добавление, удаление и восстановление компонентов программы](#)).
- 3 Перезагрузите компьютер.

2

Установка и запуск программы

Установка программы	22
Установка из MSI-пакетов	24
Обновление программы	25
Добавление, удаление и восстановление компонентов программы	27
Запуск программы	29
Подготовка к применению ViPNet CSP	30

Установка программы



Примечание. Для установки ViPNet CSP необходимы права администратора операционной системы.

Если ViPNet CSP входит в состав ПО ViPNet, она устанавливается автоматически вместе с этим ПО.

Чтобы установить ViPNet CSP отдельно:

- 1 Запустите установочный файл .
- 2 Ознакомьтесь с условиями лицензионного соглашения. Выберите **Я принимаю это соглашение** и нажмите **Продолжить**.
- 3 Выберите **Автоматически перезагрузить компьютер после завершения** для автоматической перезагрузки компьютера после завершения установки.
- 4 Чтобы установить программу с настройками по умолчанию, нажмите **Установить сейчас**.
- 5 Чтобы изменить параметры установки, нажмите **Настроить**.

5.1 На вкладке **Выбор компонентов** укажите компоненты программы, которые хотите установить:

- **Корневые сертификаты** — установка корневых сертификатов Головного удостоверяющего центра и Национального удостоверяющего центра, необходимых для обеспечения TLS-соединения.
- **Панель управления ViPNet CSP** — установка исполняемых файлов ViPNet CSP. При его отключении установятся только библиотеки криптопровайдера, используемые для разработки программ.
- **Эмуляция КриптоПРО CSP** — добавление поддержки совместной работы ViPNet CSP с продуктами КриптоПРО. Например, для работы с КриптоПро ЭЦП Browser plug-in, необходимого для корректного функционирования [ФГИС «Аршин»](#).
- **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** — добавление функций для использования криптопровайдера ViPNet CSP в сторонних приложениях, например в приложениях Microsoft Office. Компонент включен по умолчанию при отдельной установке ViPNet CSP и отключен при установке ViPNet CSP в составе другого ПО ViPNet.
- **Поддержка протокола TLS** — добавление функций для [организации защищенное соединение по протоколу TLS](#).

5.2 На вкладке **Папка установки** укажите путь к папке установки программы на компьютере.

5.3 На вкладке **Информация о пользователе** укажите имя пользователя и название организации.

5.4 На вкладке **Меню «Пуск»** укажите имя папки для установки программы и выберите **Создать ярлыки на рабочем столе**.

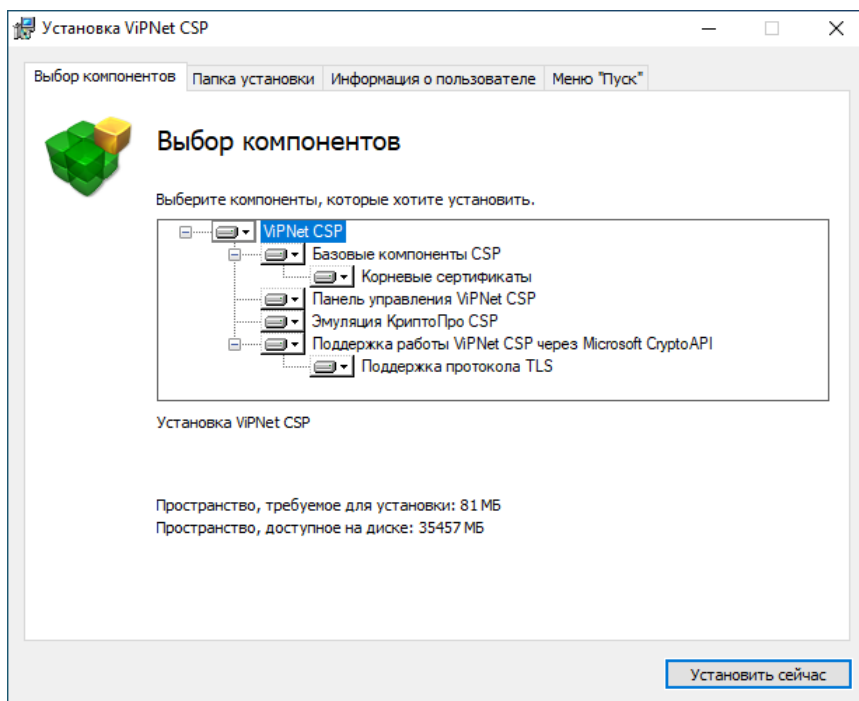


Рисунок 2. Настройка параметров установки ViPNet CSP

- 6 Чтобы начать установку, нажмите **Установить сейчас**.
- 7 Если ранее вы выбрали **Автоматически перезагрузить компьютер после завершения**, по окончании установки компьютер перезагрузится автоматически. Иначе программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите **Да**.

В процессе установки также будет создана точка восстановления системных файлов и параметров.

Примечание. Использование точек восстановления не поддерживается на серверных операционных системах Windows.

Если в настройках вашей операционной системы отключена функция создания точек восстановления, программа установки ViPNet CSP автоматически включит эту функцию.



В процессе установки ViPNet CSP обращается к системным функциям Windows, чтобы создать точку восстановления системных файлов и параметров. В зависимости от настроек восстановления системы, Windows может отменить создание точки восстановления (например, если такая точка в этот день уже создавалась).

Установка из MSI-пакетов

ViPNet CSP может быть установлена из командной строки Windows с указанием ряда стандартных параметров установщика Windows.



Внимание! При установке ViPNet CSP с помощью командной строки на компьютер с неподдерживаемой сборкой Windows процесс установки может быть прекращен без появления окна с уведомлением.

Таблица 1. Параметры режима установки

Параметр	Описание
/qn	Установка без демонстрации интерфейса (Silent mode).
/qb! /qr	Установка с минимальным интерфейсом (на экране выводятся только стандартный индикатор прогресса и информационные сообщения).
/qf	Установка с полным интерфейсом (по умолчанию).

Таблица 2. Параметры перезагрузки

Параметр	Описание
/norestart	Отключение перезагрузки после завершения установки.
/promptrestart	Вывод диалогового окна с запросом на перезагрузку. Данный параметр не действует в сочетании с параметром /qn.
/forcerestart	Перезагрузка компьютера после установки и принудительное закрытие других приложений без сохранения открытых файлов. Данный параметр действует только в сочетании с параметром /qn.

Пример команды установки в «тихом» режиме без автоматической перезагрузки:

```
ViPNet_CSP_RUS_<ver>.exe /qn /norestart
```

где <ver> — версия и номер сборки ViPNet CSP. После выполнения этой команды необходимо будет выполнить перезагрузку вручную.



Примечание. При установке ViPNet CSP с использованием командной строки точка восстановления Windows не создается.

Обновление программы



Внимание! При обновлении с любой несертифицированной версии ViPNet CSP на текущую для сохранения работоспособности TLS-соединений рекомендуется удалить старую версию программы, а затем установить новую.

- 1 Запустите установочный файл  более новой версии ViPNet CSP.
- 2 Чтобы после завершения обновления компьютер перезагрузился автоматически, выберите **Автоматически перезагрузить компьютер после завершения**.
- 3 Нажмите **Начать обновление**.

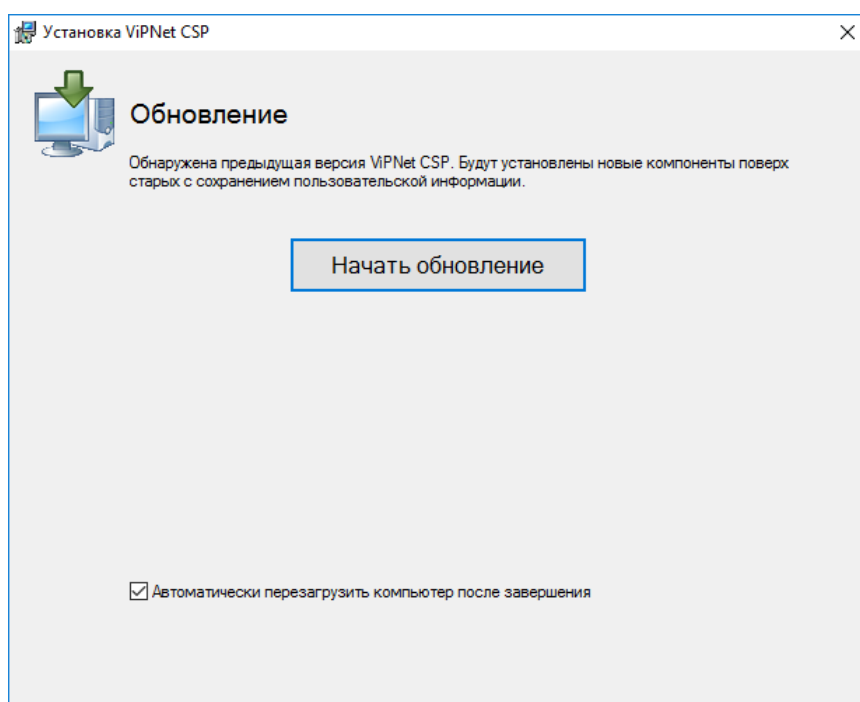


Рисунок 3. Обновление программы ViPNet CSP

- 4 Если появится окно с предупреждением, что права доступа к папке хранения ключей компьютера заданы неверно, нажмите **Да**.
- 5 Дождитесь завершения обновления программы.
- 6 Если ранее вы выбрали **Автоматически перезагрузить компьютер после завершения**, по окончании установки компьютер перезагрузится автоматически. Иначе программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите **Да**.

В процессе обновления также будет создана точка восстановления системных файлов и параметров.

Примечание. Использование точек восстановления не поддерживается на серверных операционных системах Windows.



Если в настройках вашей операционной системы отключена функция создания точек восстановления, программа установки ViPNet CSP автоматически включит эту функцию.

В процессе обновления ViPNet CSP обращается к системным функциям Windows, чтобы создать точку восстановления системных файлов и параметров. В зависимости от настроек восстановления системы, Windows может отменить создание точки восстановления (например, если такая точка в этот день уже создавалась).

Добавление, удаление и восстановление компонентов программы



Внимание! Если ViPNet CSP был установлен в составе другого ПО, то удаляйте ViPNet CSP через удаление этого ПО.

Для установки или удаления компонентов ViPNet CSP, а также восстановления программы:

- 1 Запустите программу установки ViPNet CSP одним из способов:
 - запустите установочный файл ;
 - выберите **Пуск > Параметры > Приложения > ViPNet CSP** и нажмите **Изменить**;
 - в меню **Пуск** начните вводить «ViPNet CSP» и выберите **Установка ViPNet CSP**.
- 2 В окне **Изменение установленных компонентов**:
 - для установки или удаления компонентов выберите **Добавить или удалить компоненты**;
 - для восстановления компонентов программы выберите **Восстановить**;
 - для удаления всех компонентов программы выберите **Удалить все компоненты**.

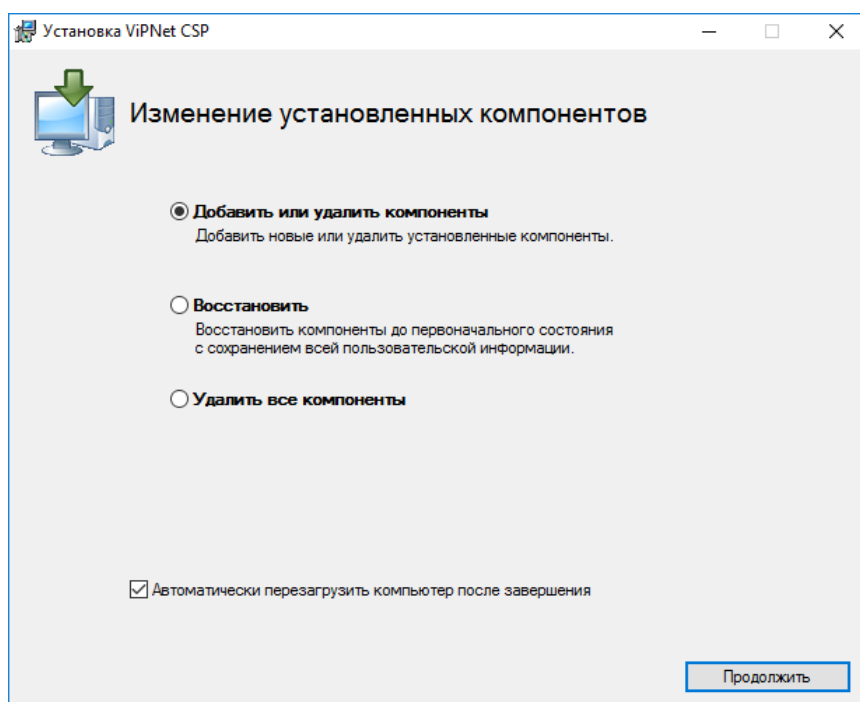


Рисунок 4. Изменение установленных компонентов

- 3 Чтобы отменить автоматическую перезагрузку компьютера после завершения установки, снимите флажок **Автоматически перезагрузить компьютер после завершения**. Затем нажмите **Продолжить**.
- 4 После выбора в окне **Изменение установленных компонентов**:
 - если вы устанавливаете или удаляете компоненты программы, выберите среди компонентов те, которые хотите удалить или добавить. Затем нажмите **Продолжить**.
 - если вы удаляете все компоненты вместе со всеми файлами, созданными в программе и сохраненными в каталогах по умолчанию, в окне **Удаление продукта** выберите **Удалить пользовательские данные** и нажмите **Удалить**.
- 5 Дождитесь завершения установки (восстановления, удаления) компонентов программы.
- 6 Если ранее вы выбрали **Автоматически перезагрузить компьютер после завершения**, по окончании установки компьютер перезагрузится автоматически. Иначе программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите **Да**.



Примечание. При добавлении или удалении компонентов, а также при восстановлении программы точка восстановления Windows не создается.

Запуск программы

Для запуска ViPNet CSP:

- дважды щёлкните ярлык программы на рабочем столе (если при установке был установлен флаг **Создать ярлыки компонентов на рабочем столе**);
- в меню **Пуск** выберите **ViPNet > ViPNet CSP**.



Примечание. Во время установки положение программы в меню **Пуск** или в списке приложений могло быть изменено.

Если вы установили ViPNet CSP в составе другого ПО ViPNet, отдельной регистрации программы не требуется. Если вы установили ViPNet CSP отдельно, при первом запуске откроется окно **ViPNet CSP** с предложением зарегистрировать программу. Вы можете перейти к [регистрации программы](#) либо начать работу с демо-версией программы.

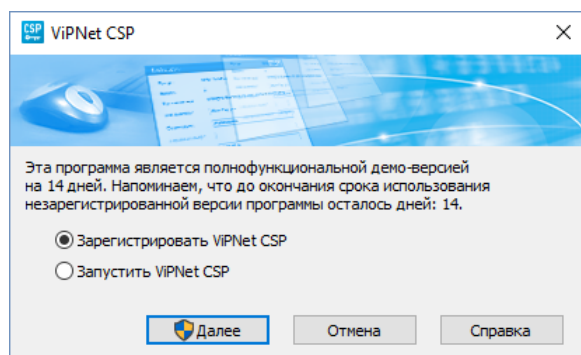


Рисунок 5. Вызов мастера регистрации



Внимание! После обновления ViPNet CSP или изменения физической конфигурации компьютера может понадобиться повторная регистрация.

После запуска программы откроется главное окно ViPNet CSP. Начните работу с программой с [установки контейнера ключей и сертификата](#).

Подготовка к применению ViPNet CSP

Для использования ViPNet CSP, установленного в составе другого ПО ViPNet, в сторонних приложениях:

- 1 Запустите установочный файл ViPNet CSP .
- 2 Добавьте компонент **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.
- 3 Запустите ViPNet CSP и убедитесь, что после установки в разделе **Дополнительно** установлен флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.

3

Регистрация ViPNet CSP

Зачем нужно регистрировать ViPNet CSP	32
Порядок регистрации	33
Получение кода регистрации	35
Регистрация ViPNet CSP	41
Автоматическая регистрация	44

Зачем нужно регистрировать ViPNet CSP

После установки ViPNet CSP на компьютер программа работает в демо-режиме: в течение двух недель вы можете использовать все функции ViPNet CSP. Чтобы затем продолжить работать с полнофункциональной версией программы, зарегистрируйте ViPNet CSP. Вы можете выполнить регистрацию в любой момент.

Вы можете зарегистрировать программу в автоматическом режиме (см. [Автоматическая регистрация](#)).

Порядок регистрации



Примечание. Если программа ViPNet CSP повторно установлена на компьютер, на котором она уже была зарегистрирована, вы можете использовать регистрационные данные, сохраненные в файле *.brg.

Если вы обновили конфигурацию компьютера, на котором будете использовать ViPNet CSP, ознакомьтесь с разделом [Если конфигурация компьютера изменилась](#).

Чтобы зарегистрировать ViPNet CSP:

1 Запустите ViPNet CSP.

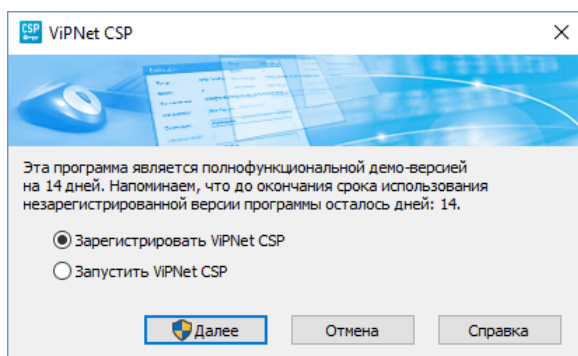


Рисунок 6. Вызов мастера регистрации

2 Выберите **Зарегистрировать ViPNet CSP** и нажмите **Далее**. Будет запущен мастер **Регистрация ViPNet CSP**.

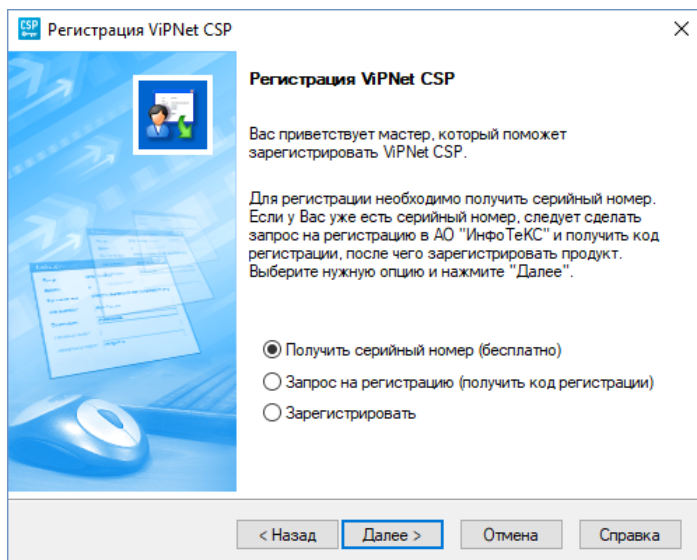


Рисунок 7. Первый шаг регистрации

3 Выполните одно из действий:



Примечание. Серийный номер выдаётся при загрузке ViPNet CSP с веб-страницы АО «ИнфоТеКС».

- Если у вас нет серийного номера и кода регистрации, выберите **Получить серийный номер (бесплатно)**. После регистрации на веб-странице ИнфоТеКС вы получите серийный номер по электронной почте.
- Если у вас есть серийный номер и нет кода регистрации, выберите **Запрос на регистрацию (получить код регистрации)** (см. [Получение кода регистрации](#)).
- Если у вас есть серийный номер и код регистрации, выберите **Зарегистрировать** (см. [Регистрация ViPNet CSP](#)).

Получение кода регистрации

- 1 На странице **Регистрация ViPNet CSP** выберите **Запрос на регистрацию (получить код регистрации)** и нажмите **Далее**.
- 2 На странице **Способ запроса на регистрацию** выберите подходящий способ:
 - Через Интернет (online).
 - По электронной почте.
 - По телефону.
 - Через файл.

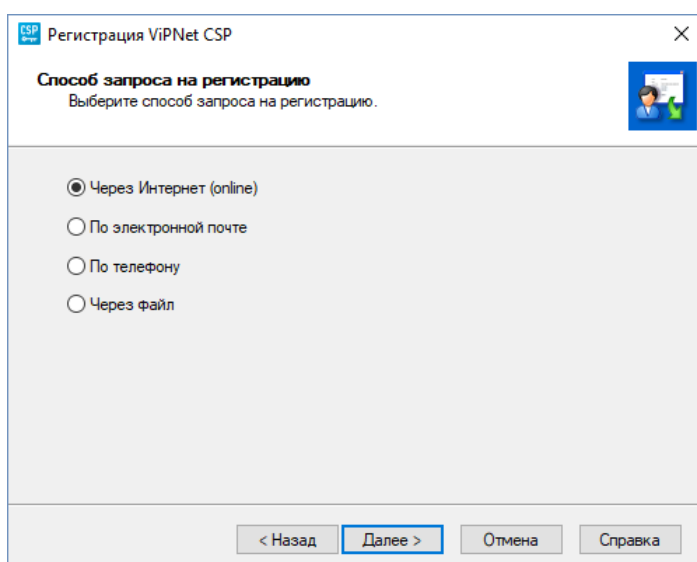


Рисунок 8. Выбор типа запроса на регистрацию

- 3 Нажмите **Далее**.

Получение кода регистрации через Интернет



Внимание! Для данного способа получения кода регистрации подключите компьютер к интернету.

Если вы выбрали способ регистрации **Через Интернет (online)**:

- 1 Введите серийный номер.



Примечание. Серийный номер выдается при загрузке ViPNet CSP с веб-страницы АО «ИнфоТеКС».

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

Рисунок 9. Ввод регистрационных данных

- 2 В поле **Пользователь** введите имя.
- 3 Введите название организации.
- 4 Введите адрес электронной почты.



Внимание! Мы не продаем и не распространяем ваши персональные данные. ИнфоТеКС ответственно подходит к защите ваших данных и принимает все меры для предотвращения несанкционированного доступа или разглашения данных, которые вы нам предоставляете.

- 5 Нажмите **Далее**.

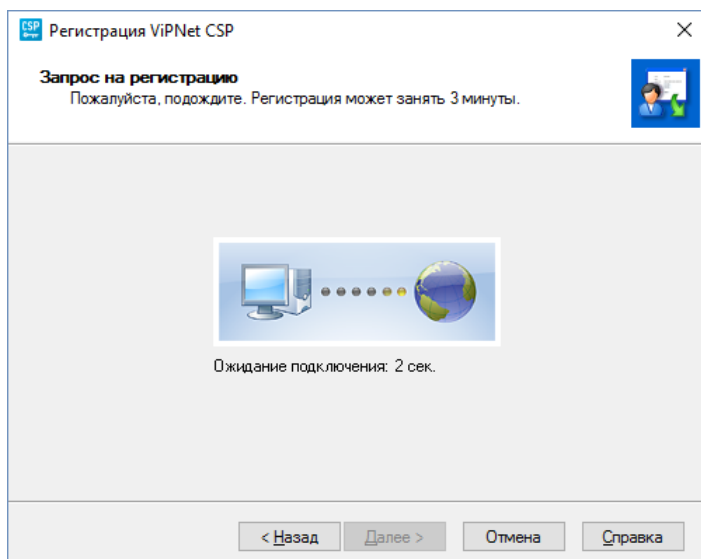


Рисунок 10. Регистрация через Интернет

Если не удалось подключиться к серверу ИнфоТеКСа в течение 3 минут, попробуйте устранить неполадку — см. [Не удается получить код регистрации через Интернет](#).

Если соединение с сервером установлено, попытка регистрации может оказаться неудачной в случае возникновения ошибок:

- Предоставленные вами данные оказались неверными. В этом случае отобразится сообщение с предложением проверить введенную информацию.
В окне сообщения нажмите **ОК**, и вы вернетесь на страницу **Регистрационные данные**.
- Введенный серийный номер уже зарегистрирован. В этом случае отобразится сообщение с предложением бесплатно получить другой серийный номер.

Перейдите по ссылке, содержащейся в сообщении, и сделайте запрос на получение серийного номера.

Если регистрация прошла успешно, откроется страница **Регистрация ViPNet CSP успешно завершена**. На этой странице приведена рекомендация, как безопасно сохранить ваши регистрационные данные.

6 Нажмите **Готово**.

Получение кода регистрации по электронной почте



Внимание! Для данного способа получения кода регистрации подключите компьютер к интернету.

Если вы выбрали способ регистрации **По электронной почте**:

- 1 Введите регистрационные данные, как описано в разделе [Получение кода регистрации через Интернет](#).
- 2 Нажмите **Далее**.
- 3 В вашем почтовом клиенте будет создано письмо с указанными регистрационными данными. Не изменяя это письмо, отправьте его по адресу reg@infotecs.ru.

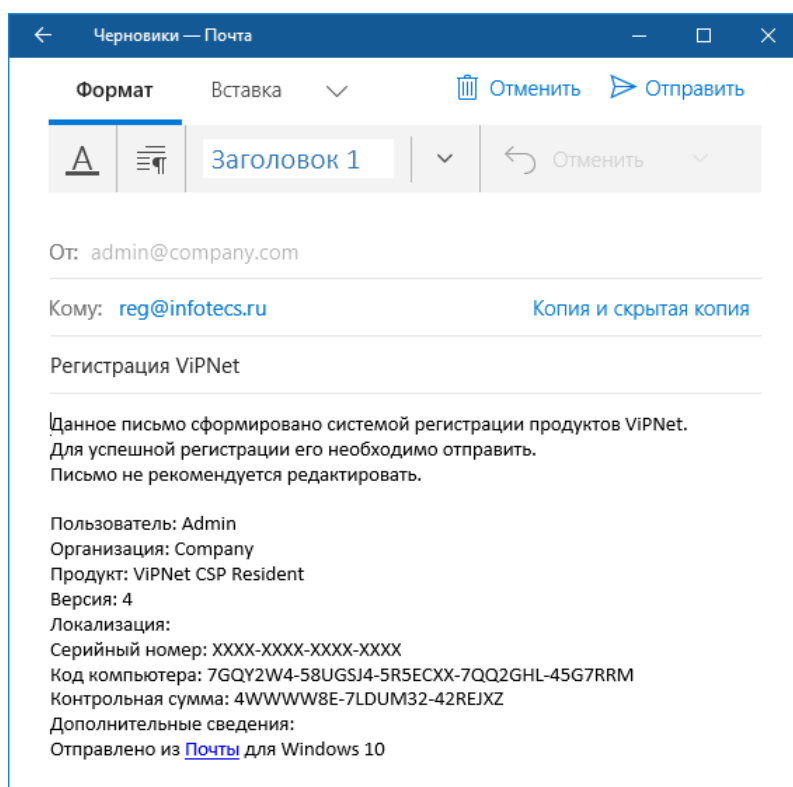


Рисунок 11. Отправка запроса кода регистрации по электронной почте

- 4 После проверки регистрационных данных вы получите код регистрации по электронной почте. Используйте его для регистрации программы (см. [Регистрация ViPNet CSP](#)).



Внимание! Если вы не получили код регистрации в течение нескольких дней, повторно отправьте запрос по электронной почте. Если вы снова не получили ответ, обратитесь в ИнфоТеКС.

Получение кода регистрации по телефону

Если вы выбрали способ регистрации **По телефону**:

- 1 Позвоните в ИнфоТеКС по телефону, приведенному в верхней части окна, и сообщите регистрационные данные. Вам сообщат код регистрации.
- 2 Нажмите **Далее**.

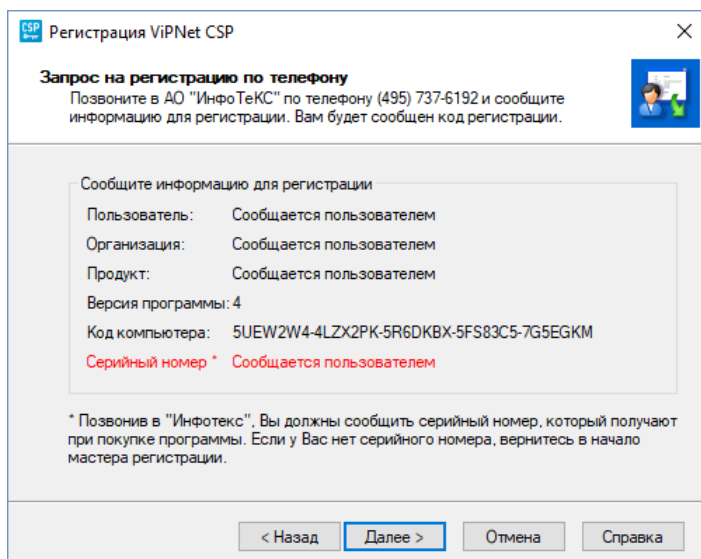


Рисунок 12. Регистрация по телефону

- 3 Введите серийный номер и код регистрации, затем нажмите **Далее** и сохраните регистрационные данные.
- 4 Нажмите **Готово**.

Получение кода регистрации через файл

- 1 Введите все данные, как описано в разделе [Получение кода регистрации через Интернет](#). Нажмите **Далее**.
- 2 На странице **Сохранение регистрационных данных** нажмите **Обзор** и укажите папку, в которой будет сохранен файл с регистрационными данными. Нажмите **Далее**.

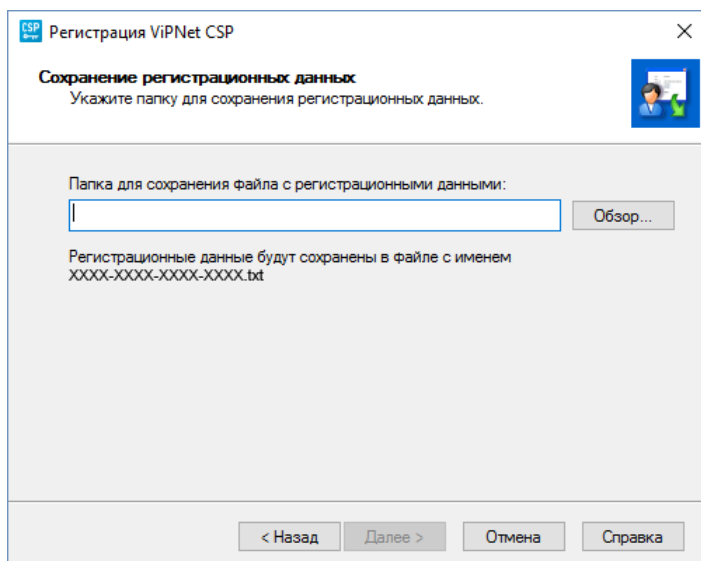


Рисунок 13. Сохранение регистрационных данных

Регистрационные данные будут сохранены в текстовом файле, имя которого совпадает с вашим серийным номером: <серийный номер>.txt.

3 Нажмите **Готово**.

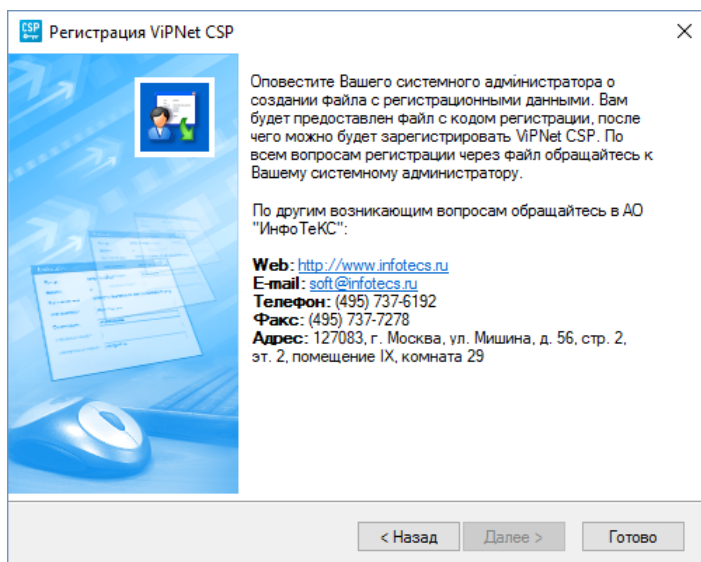


Рисунок 14. Данные для регистрации через файл сохранены

- 4 Отправьте файл с регистрационными данными, на адрес электронной почты reg@infotecs.ru. В теме сообщения укажите «ViPNet Registration Using File».
- 5 После обработки запроса АО «ИнфоТеКС» вы получите сообщение, в котором содержится код регистрации.
- 6 Получив код регистрации, зарегистрируйте свою копию ViPNet CSP (см. [Регистрация ViPNet CSP](#)).

Регистрация ViPNet CSP

Получив код регистрации, введите его и зарегистрируйте ViPNet CSP:

- 1 Запустите мастер **Регистрация ViPNet CSP** (см. [Порядок регистрации](#)).
- 2 Выберите **Зарегистрировать** и нажмите **Далее**.
- 3 Введите серийный номер и нажмите **Далее**.

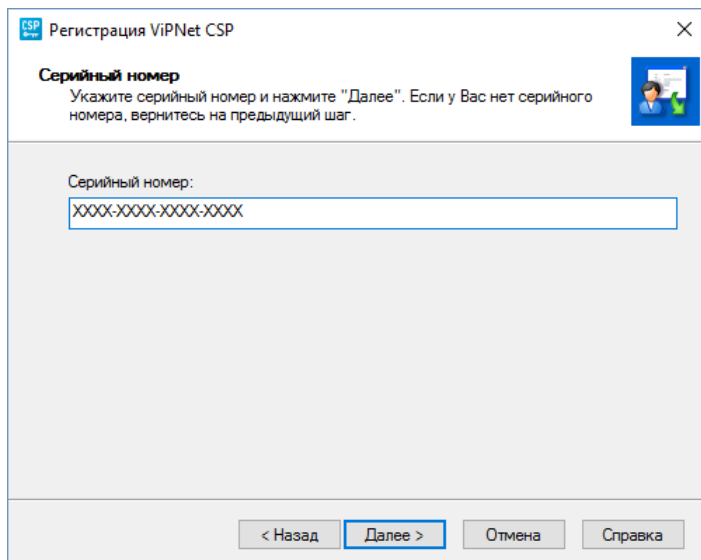


Рисунок 15. Ввод серийного номера

- 4 На странице **Код регистрации** выполните одно из действий:
 - Если вы запрашивали код регистрации через Интернет, по электронной почте или по телефону, выберите **Обычная регистрация** и введите код регистрации.
 - Если вы запрашивали код регистрации через файл, выберите **Регистрация через файл**, затем нажмите **Обзор** и укажите путь к файлу, содержащему код регистрации.

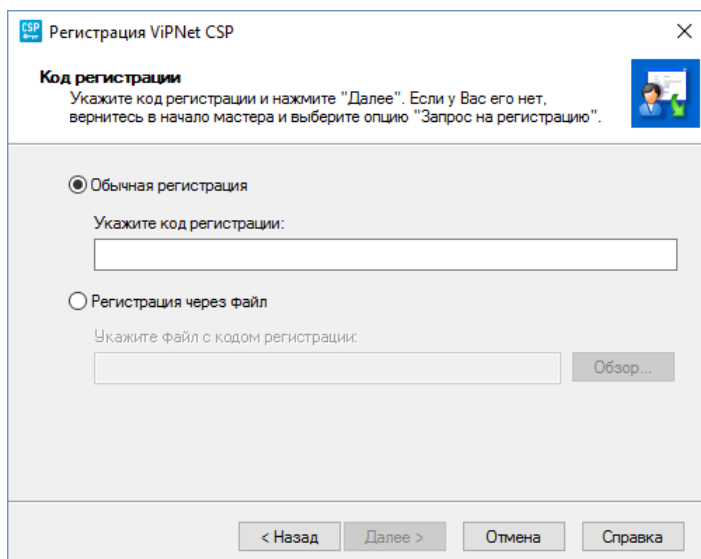


Рисунок 16. Ввод кода регистрации

5 Нажмите **Далее**.

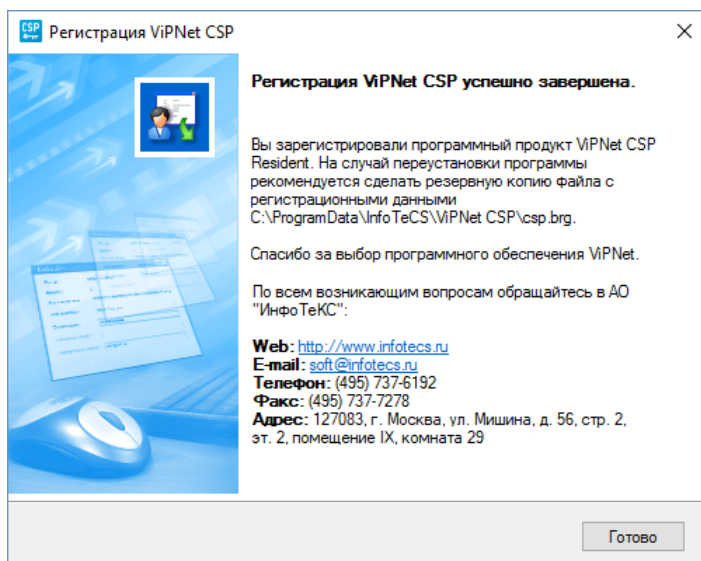


Рисунок 17. Завершение регистрации

6 Нажмите **Готово**.

7 Сохраните регистрационные данные.

Сохранение регистрационных данных

После регистрации программы регистрационные данные сохраняются в файле *.brg и протоколе регистрации reginfo.txt (по умолчанию в папке C:\ProgramData\InfoTeCS\ViPNet CSP). Эти файлы можно использовать для ускоренной регистрации программы, например, если вы переустановили программу в другую папку на том же компьютере или повторно установили программу на компьютер после форматирования жесткого диска.

Для ускоренной регистрации ViPNet CSP с использованием файла *.brg:

- 1 Завершите работу с программой.
- 2 Поместите файл *.brg в папку установки программы.
- 3 Запустите программу. Если регистрационные данные верны и конфигурация компьютера не изменилась, программа будет автоматически зарегистрирована.

Если файл *.brg потерян, вручную зарегистрируйте ViPNet CSP с использованием данных из протокола регистрации `reginfo.txt` (см. [Регистрация ViPNet CSP](#)).

Если конфигурация компьютера изменилась

При изменении конфигурации компьютера:

- Если изменения незначительны, повторная регистрация программы не потребуется. Откроется сообщение, что создан новый файл *.brg. Скопируйте его в надежное место.
- Если изменения значительны (заменена большая часть комплектующих), повторно зарегистрируйте программу.

Автоматическая регистрация



Внимание! Для данного способа получения кода регистрации подключите компьютер к интернету.

Чтобы зарегистрировать программу автоматически:

- 1 Подготовьте файл регистрации `reginfo.txt` с серийным номером, полученным при загрузке программы. Файл `reginfo.txt` должен иметь вид:

Serial Number: XXXX-XXXX-XXXX-XXXX

E-mail: email@company.com

User name: <ФИО пользователя>

Company: <Название компании>



Примечание. Поля `User name` и `Company` необязательные.

- 2 Запустите командную строку с правами администратора и перейдите в папку установки ViPNet CSP.
- 3 Выполните команду:
 - o `csp_settings_app.exe -SilentRegSnFile reginfo.txt` — для регистрации в полностью автоматическом режиме (без графического интерфейса);
 - o `csp_settings_app.exe -RegSnFile reginfo.txt` — для регистрации с оповещением об успешном завершении регистрации.

4

Получение закрытого ключа и сертификата

Общая информация о ключах и сертификатах	46
Порядок получения закрытого ключа и сертификата	48
Создание запроса на сертификат и формирование закрытого ключа	49

Общая информация о ключах и сертификатах

Для шифрования документов и использования электронной подписи используется пара взаимосвязанных ключей — закрытый и открытый ключ.

Закрытый ключ создается в удостоверяющем центре (далее — УЦ) или самим пользователем и хранится в контейнере ключей на диске или внешнем устройстве.

Открытый ключ создается в УЦ и помещается в сертификат пользователя. Сертификат выпускается в УЦ по запросу пользователя (см. [Получение закрытого ключа и сертификата](#)) или, в некоторых случаях, по инициативе УЦ. Запрос на выдачу или обновление сертификата пользователя вы можете создать с помощью программного обеспечения ViPNet Client, ViPNet PKI Client или программы **Создание запроса на сертификат** (см. [Порядок получения закрытого ключа и сертификата](#)), установленной вместе с ViPNet CSP.

Подлинность и действительность сертификата пользователя проверяются с помощью цепочки [сертификатов издателя](#) и [списка аннулированных сертификатов \(CRL\)](#).

При организации защищенного документооборота приложение (например, программа из состава Microsoft Office, служба сервера IIS) обращается к криптопровайдеру, передавая ему параметры сертификатов и местоположение закрытого ключа. Чтобы обеспечить приложениям доступ к сертификатам, установите в хранилище Windows:

- Сертификат пользователя и закрытый ключ пользователя с помощью ViPNet CSP (см. [Установка контейнеров ключей и сертификатов](#)).
- Сертификат издателя и [списки аннулированных сертификатов \(CRL\)](#) стандартными средствами Windows (см. [Установка сертификата издателя и списка аннулированных сертификатов](#)).

ViPNet CSP позволяет устанавливать закрытые ключи и сертификаты открытого ключа:

- Путем добавления контейнера, содержащего закрытый ключ и сертификат. Контейнер может находиться в папке на диске (см. [Установка контейнера ключей из папки](#)) или на внешнем устройстве (см. [Установка контейнера ключей с внешнего устройства](#)).
- Путем установки сертификата и сопоставления ему закрытого ключа из контейнера ключей в папке на диске или внешнем устройстве (см. [Добавление сертификата в контейнер ключей](#)).

Сертификат может находиться отдельно от закрытого ключа в тех случаях, когда сертификат создается по запросу пользователя. Сертификат и закрытый ключ находятся в одном контейнере, когда их выдаёт УЦ.

Формат файла контейнера ключей зависит от криптопровайдера, который его создал.



Внимание! Контейнеры ключей, созданные с помощью криптопровайдера ViPNet CSP, невозможно использовать в КриптоПро CSP. Для работы с ними в КриптоПро CSP экспортируйте и импортируйте их через файл *.pfx.

Контейнеры ключей ViPNet CSP могут храниться на компьютере в одной из двух папок:

- Папка хранения ключей текущего пользователя — папка, к содержимому которой имеют доступ только текущий пользователь и администратор ОС:

`C:\Users\<Имя пользователя>\AppData\Local\InfoTeCS\Containers.`

- Папка хранения ключей компьютера — папка, к содержимому которой имеет доступ только администратор операционной системы:

`C:\ProgramData\InfoTeCS\Containers.`



Внимание! Для соответствия рекомендациям [Технического комитета по стандартизации \(ТК 26\) «Криптографическая защита информации»](#) изменен формат контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012.

Контейнеры ключей, созданные в ViPNet CSP 4.1 с помощью ГОСТ 34.10-2012, более не поддерживаются.

Файлы сертификатов создаются УЦ в форматах:

- Файл формата X.509, содержащий только сертификат (файлы с расширениями .cer, .crt).
 - Файл формата PKCS#7 — для хранения зашифрованных и подписанных сообщений вместе с соответствующими сертификатами. Файл также может использоваться для передачи наборов сертификатов и списков CRL (файлы с расширениями .spc, .p7b, .p7s).
 - Файл формата PKCS#12 — для передачи зашифрованных на пароле закрытых ключей и сертификатов (файлы с расширениями .pfx, .p12). Файлы формата PKCS#12 создаются в соответствии с рекомендациями Технического комитета по стандартизации (ТК 26) «Криптографическая защита информации».
-



Примечание. Не поддерживаются файлы формата PKCS#12, не соответствующие рекомендациям ТК 26 (например, файлы, созданные с помощью ПО компании «КриптоПро»).

В ViPNet CSP можно использовать неограниченное количество сертификатов и контейнеров ключей. Поэтому при подписании документа необходимо выбрать, каким ключом он будет подписан.

Порядок получения закрытого ключа и сертификата

Порядок получения и ввода в действие сертификата и закрытого ключа определяется регламентом работы вашего УЦ. Прежде чем формировать запрос на создание сертификата, уточните в УЦ, принимаются ли запросы, сформированные с помощью программы **Создание запроса на сертификат** из состава ViPNet CSP.

Чтобы получить и подготовить к работе сертификат:

- 1 Создайте закрытый ключ и файл запроса на сертификат в программе **Создание запроса на сертификат** (см. [Создание запроса на сертификат и формирование закрытого ключа](#)).
- 2 Сохраните контейнер закрытого ключа на диске или внешнем устройстве.
- 3 Передайте файл запроса в УЦ и получите сертификат.
- 4 [Установите сертификат в контейнер ключей](#).
- 5 [Установите в системное хранилище сертификат](#), а также [сертификаты издателей](#) и [списки CRL](#).

Создание запроса на сертификат и формирование закрытого ключа



Внимание! Если требуется сохранить запрос на сертификат и контейнер ключей на внешнем устройстве, убедитесь, что это устройство подключено к компьютеру.

Для создания запроса на новый сертификат или обновления уже существующего:

- 1 В меню **Пуск** выберите **ViPNet > Создание запроса на сертификат**.
- 2 Выберите одно из действий:
 - **Запросить новый сертификат** — для создания запроса на новый сертификат.
 - **Запросить обновление действующего сертификата** — для обновления уже имеющегося.

При создании запроса на обновление сертификата:

- Выберите сертификат для обновления, и нажмите **ОК**.
- Чтобы выбрать другой сертификат или просмотреть выбранный сертификат, нажмите **Выбрать сертификат** или **Свойства сертификата**.
- Укажите новые параметры сертификата и данные о владельце или оставьте реквизиты предыдущего сертификата.

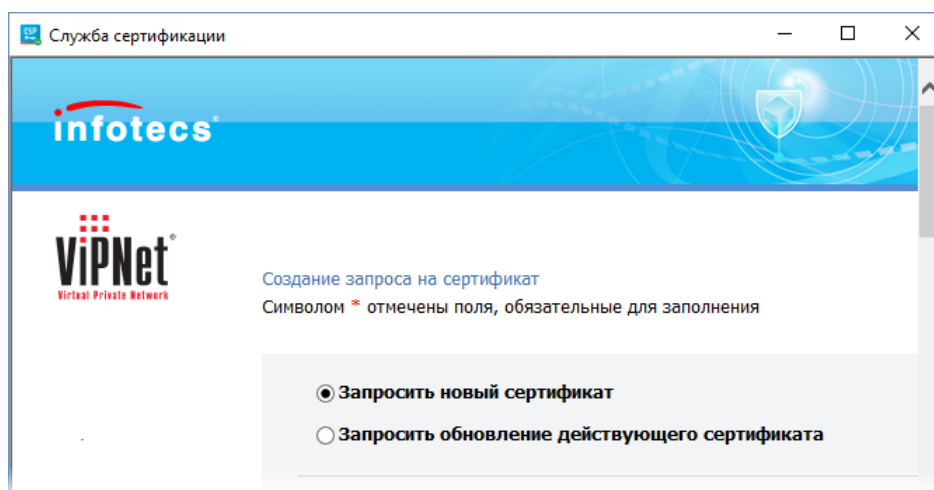


Рисунок 18. Выбор типа запроса на сертификат

- 3 В разделе **Параметры сертификата**:
 - В списке **Криптопровайдер** выберите криптопровайдер, с помощью которого вы хотите создать закрытый и открытый ключи.
 - В списке **Назначение** выберите действия, которые планируете выполнять с помощью сертификата:

- **Подпись** (по умолчанию), если создаете ключ и сертификат только для подписания сообщений и документов электронной подписью.
 - **Подпись и шифрование**, если создаете ключ и сертификат для шифрования сообщений и их защиты с помощью электронной подписи.
 - **Шифрование**, если создаете ключ и сертификат только для шифрования сообщений электронной почты и документов.
- В списке **Шаблон сертификата** выберите один из вариантов:
- **Веб-сервер** — чтобы создать запрос на сертификат для веб-сервера IIS.
 - **Квалифицированный ViPNet CSP** (по умолчанию) — чтобы создать запрос на [квалифицированный сертификат](#), в котором нужно указать атрибуты:
 - ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя),
 - СНИЛС (страховой номер индивидуального лицевого счета),
 - ИНН (идентификационный номер налогоплательщика),
 - ОГРН (основной государственный регистрационный номер).
 - **Квалифицированный лично** — запрос, аналогичный **Квалифицированному ViPNet CSP**. Предназначен для личного получения сертификата, соответствующего приказу ФСБ № 795 от 27 декабря 2011 г.
 - **Отчетность** — чтобы создать запрос на сертификат, с помощью которого можно подписывать документы для сдачи бухгалтерской отчетности.
 - **Стандартный** — чтобы создать запрос на сертификат без определенных требований.

Если у вас есть другие шаблоны сертификатов, можете выбрать один из них.

- Для экспорта закрытого ключа вместе с полученным сертификатом в файл формата PKCS#12 (см. [Экспорт сертификата и закрытого ключа в файл](#)), выберите **Экспортируемый**.
 - Чтобы контейнер ключей к запросу на сертификат был создан в папке хранения ключей компьютера, выберите **Системный**, иначе контейнер ключей будет создан в папке хранения ключей текущего пользователя (см. [Общая информация о ключах и сертификатах](#)).
- 4** В разделе **Данные о владельце сертификата** укажите персональные данные лица, для которого создаётся запрос на сертификат.

Данные о владельце сертификата:

Для физ. лиц: имя (ФИО); для юр. лиц: наименование организации*	АО «ИнфоТекС»
Имя и отчество владельца сертификата*	Иван Иванович
Фамилия владельца сертификата*	Иванов
Адрес электронной почты	ivanov@company.com
Организация	АО «ИнфоТекС»
Подразделение	

Рисунок 19. Указание данных о владельце сертификата

- 5 Если сертификат планируется использовать для подписания сообщений электронной почты программы Microsoft Outlook, укажите адрес электронной почты.
- 6 В разделе **Сохранение запроса в файл** нажмите **Обзор** и укажите место и имя файла для сохранения файла запроса.



Совет. Чтобы облегчить поиск вашего запроса, включите в имя файла фамилию и инициалы владельца сертификата.

- 7 Нажмите **Сформировать запрос**. Эта кнопка появляется после заполнения всех обязательных полей.
- 8 В окне **ViPNet CSP - инициализация контейнера ключей** укажите:
 - Имя контейнера ключей или оставьте значение по умолчанию.
 - Место размещения контейнера ключей. Для этого выберите **Папка на диске** или **Выберите устройство**.

В зависимости от места размещения контейнера ключей в запрос будет добавлено расширение со следующей информацией:

- При размещении контейнера ключей в папке на диске — с информацией о том, что срок действия закрытого ключа — 1 год.
- При размещении контейнера ключей на устройстве с аппаратной поддержкой алгоритмов ГОСТ — с информацией о том, что срок действия закрытого ключа — 3 года.
- При размещении контейнера ключей в ПАК ViPNet HSM (см. [Взаимодействие с ViPNet HSM](#)) — с информацией о том, что срок действия закрытого ключа — 5 лет.

Нажмите **ОК**.



Примечание. В ряде случаев появление окна **ViPNet - инициализация контейнера ключей** может происходить с запозданием. Дождитесь появления этого окна.

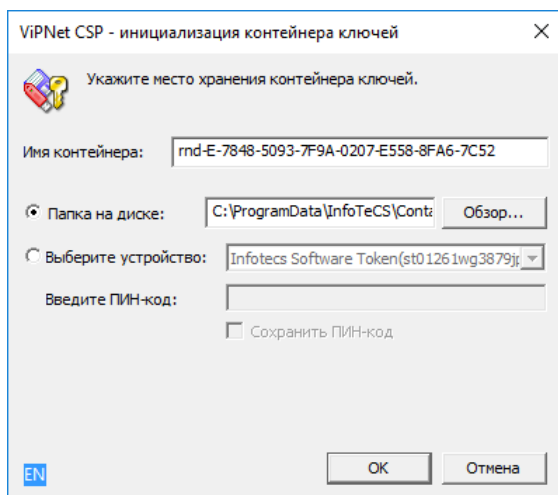


Рисунок 20. Создание контейнера ключей

- 9 В окне **ViPNet CSP - пароль контейнера ключей** задайте пароль доступа к контейнеру ключей. Чтобы повторно не вводить пароль при последующих обращениях к контейнеру ключей в Windows, выберите **Сохранить пароль**. Нажмите **OK**.



Внимание! Запрещается вводить пароль при помощи операций копирования и вставки через буфер обмена.

Сохранение пароля к контейнеру ключей ведет к снижению уровня безопасности.

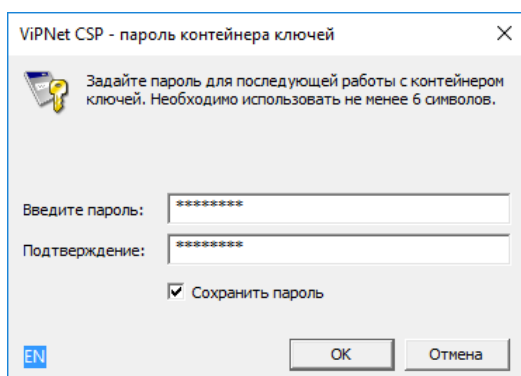


Рисунок 21. Задание пароля доступа к контейнеру ключей

- 10 Появится **электронная рулетка**, если она еще не запускалась в текущем сеансе работы программы. Поводите курсором в окне **Электронная рулетка**.

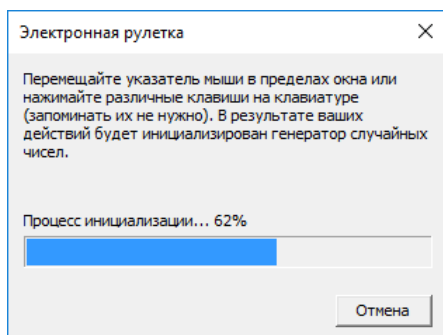


Рисунок 22. Электронная рулетка



Примечание. Электронная рулетка может не появиться, если в ViPNet CSP в разделе **Датчик случайных чисел** используемым датчиком указан датчик отличный от биологического.

Если для сохранения контейнера выбрано устройство с аппаратной поддержкой алгоритмов ГОСТ, электронная рулетка также не появится, так как в этом случае формирование закрытого ключа происходит средствами этого устройства.

- 11 После уведомления об успешном создании файла запроса на сертификат нажмите **ОК**.
- 12 После создания файла запроса окно **Служба сертификации** можно закрыть.

5

Установка контейнеров ключей и сертификатов

Способы установки закрытого ключа и сертификата	55
Установка контейнера ключей из папки	56
Установка контейнера ключей с внешнего устройства	59
Добавление сертификата в контейнер ключей	60
Установка сертификата в системное хранилище Windows	62
Установка сертификата издателя и списка аннулированных сертификатов	68

Способы установки закрытого ключа и сертификата



Внимание! Для соответствия рекомендациям [Технического комитета по стандартизации \(ТК 26\) «Криптографическая защита информации»](#) изменен формат контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012.

Контейнеры ключей, созданные в ViPNet CSP 4.1 с помощью ГОСТ 34.10-2012, более не поддерживаются.

Чтобы использовать закрытый ключ и сертификат:

1 Установите контейнер ключей:

- Если закрытый ключ и сертификат находятся в одном контейнере, и этот контейнер размещен в папке на диске, см. раздел [Установка контейнера ключей из папки](#).
- Если закрытый ключ и сертификат находятся в одном контейнере, и этот контейнер размещен на внешнем устройстве, см. раздел [Установка контейнера ключей с внешнего устройства](#).
- Если сертификат издан в удостоверяющем центре по запросу, и в результате имеется контейнер ключей и отдельный файл сертификата, см. раздел [Установка сертификата в контейнер ключей](#) (см. [Добавление сертификата в контейнер ключей](#)).

2 Установите сертификат в системное хранилище (см. [Установка сертификата в системное хранилище Windows](#)).

3 Установите сертификаты издателей и список аннулированных сертификатов (CRL) в системное хранилище (см. [Установка сертификата издателя и списка аннулированных сертификатов](#)).



Внимание! При работе с контейнерами запрещается вводить пароль при помощи операций копирования и вставки через буфер обмена.

Установка контейнера ключей из папки

Для установки в программу контейнера ключей, созданного в удостоверяющем центре или программе «Создание запроса на сертификат» (см. [Порядок получения закрытого ключа и сертификата](#)), скопируйте его в одну из папок хранения контейнеров ключей (см. [Общая информация о ключах и сертификатах](#)). После этого в ViPNet CSP в разделе **Контейнеры ключей** этот контейнер ключей появится автоматически.

Если контейнер ключей сохранен в другой папке или на USB-носителе:

- 1 В ViPNet CSP в разделе **Контейнеры ключей** нажмите **Добавить контейнер**.

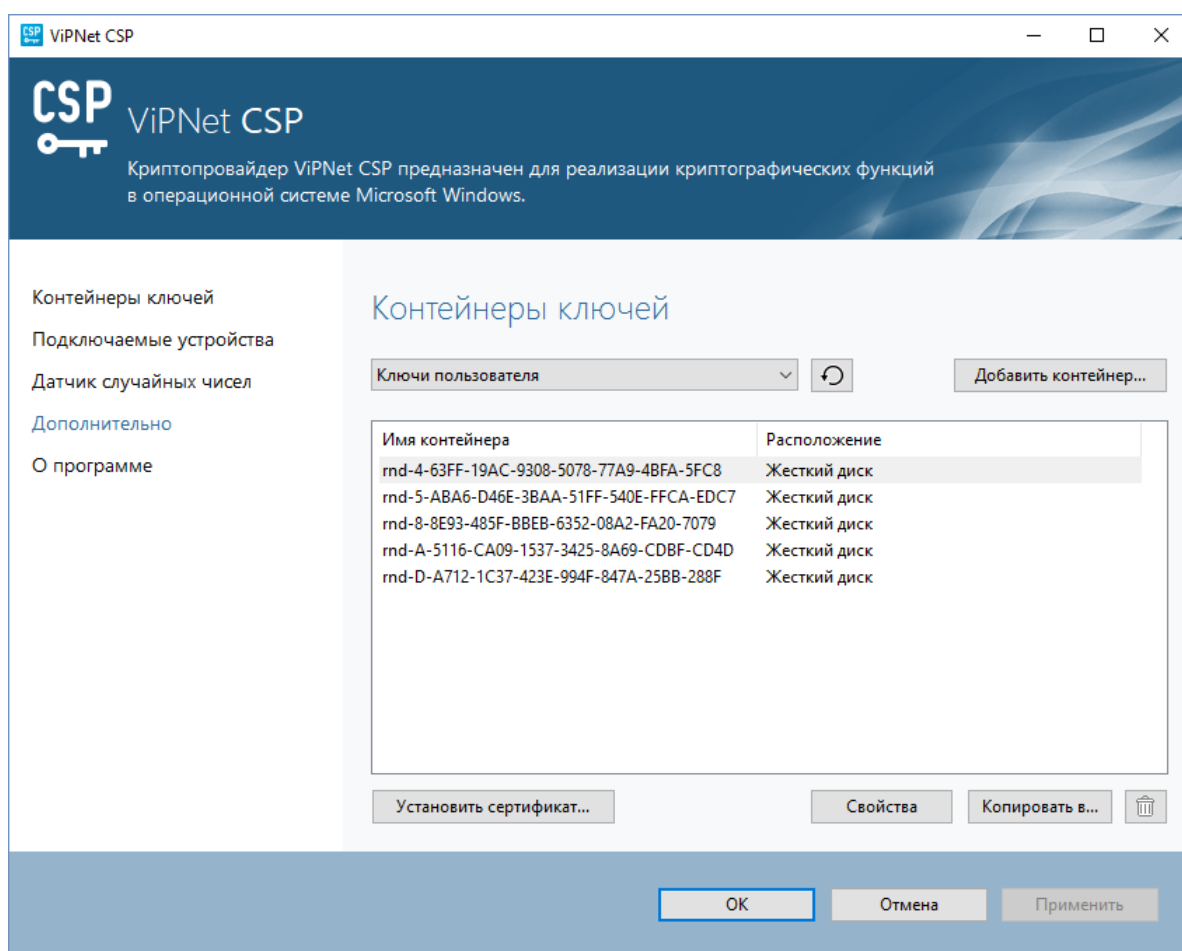


Рисунок 23. Управление контейнерами ключей

- 2 В окне ViPNet CSP - инициализация контейнера ключей нажмите **Обзор**.
 - Если контейнер ключей хранится на жестком диске, в окне **Обзор папок** укажите путь к папке, содержащей контейнер.



Примечание. Полный путь к контейнеру ключей (например, D:\Folder1\Container1) не должен превышать 259 символов.

- Если контейнер ключей хранится на USB-носителе, в окне **Обзор папок** укажите этот съемный диск. В поле **Папка на диске** автоматически будет подставлен путь, например E:\Infotecs\Containers.



Внимание! На USB-носителе контейнер ключей обязательно должен находиться в папке Infotecs\Containers.

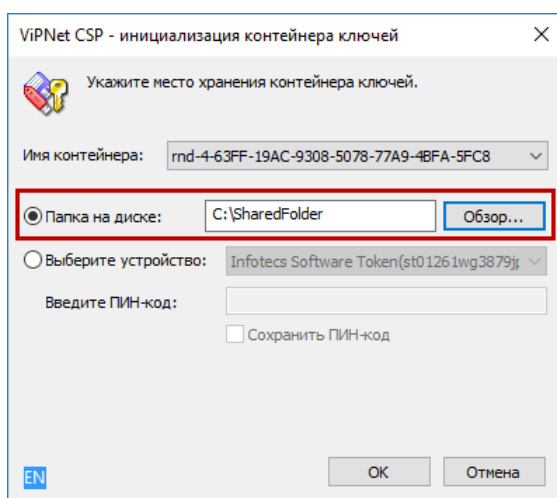


Рисунок 24. Установка контейнера ключей из папки

- 3 В списке **Имя контейнера** выберите файл контейнера ключей или оставьте значение по умолчанию.
- 4 Нажмите **ОК**. В окне **Контейнер ключей** появится сообщение об успешном добавлении контейнера ключей и предложение установить сертификат в системное хранилище.

Для работы с сертификатами их необходимо установить в хранилище текущего пользователя.



Внимание! Если ViPNet CSP установлена на сервере и используется для организации защищенных соединений TLS, сертификат необходимо устанавливать в хранилище локального компьютера вручную (см. [Установка сертификата из контейнера ключей](#)).

В окне **Контейнер ключей** выполните одно из следующих действий:

- Чтобы автоматически установить сертификат в системное хранилище, нажмите **Да**.
- Если сертификаты устанавливать не требуется (или установка будет происходить вручную), нажмите **Нет**.
- Для просмотра списка сертификатов в контейнере ключей нажмите **Сертификаты**.

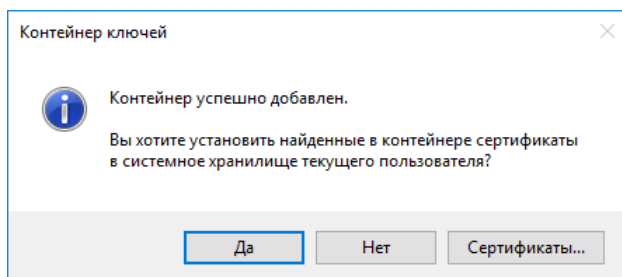


Рисунок 25. Установка сертификатов из контейнера ключей в системное хранилище

- 5 После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров ключей появится добавленный контейнер ключей.



Примечание. Вы можете установить сертификаты из контейнера ключей вручную в окне настройки свойств контейнера (см. [Установка сертификата из контейнера ключей](#)).

После добавления контейнера ключей [установите сертификат издателя и список CRL](#) и приступайте к выполнению криптографических операций.

Установка контейнера ключей с внешнего устройства



Внимание! Для доступа к контейнерам ключей, хранящимся на внешнем устройстве, на компьютере с ViPNet CSP предварительно должно быть установлено необходимое программное обеспечение, а также выполнены условия для работы с устройством, указанные в его руководстве.

При подключении внешнего устройства к компьютеру с ViPNet CSP контейнеры ключей, записанные на этом устройстве, устанавливаются в программу автоматически. Чтобы просмотреть контейнеры ключей, хранящиеся на подключенном внешнем устройстве:

- 1 Перейдите в раздел **Контейнеры ключей**.
- 2 Вверху в списке выберите название подключенного внешнего устройства. В окне отобразятся контейнеры ключей, находящиеся на внешнем устройстве.



Совет. После извлечения и повторной установки внешнего устройства для

обновления списка контейнеров в разделе **Контейнеры ключей** нажмите .

- 3 Выберите необходимый контейнер ключей из списка и установите сертификат из контейнера в системное хранилище (см. [Установка сертификата из контейнера ключей](#)).

Добавление сертификата в контейнер ключей

При создании запроса на сертификат формируется контейнер, содержащий закрытый ключ. По запросу в удостоверяющем центре издается сертификат, соответствующий этому закрытому ключу.

Чтобы использовать сертификат, полученный из удостоверяющего центра, для формирования электронной подписи и других целей, сертификат нужно установить в контейнер с соответствующим закрытым ключом.

Чтобы установить сертификат в контейнер ключей:

- 1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** выберите контейнер ключей, в который требуется установить сертификат.

Примечание. [Папку хранения контейнеров ключей](#), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:



- чтобы отобразить в списке контейнеры ключей, находящиеся в папке хранения ключей текущего пользователя, выберите **Ключи пользователя**;
- чтобы отобразить контейнеры ключей, находящиеся в папке хранения ключей компьютера, выберите **Ключи компьютера**;
- чтобы отобразить контейнеры ключей, находящиеся на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при запуске ViPNet CSP с правами администратора и наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. [Общая информация о ключах и сертификатах](#)).

- 2 Нажмите **Свойства** либо дважды щелкните контейнер ключей.
- 3 В окне **Свойства контейнера ключей** нажмите **Добавить сертификат из файла**.

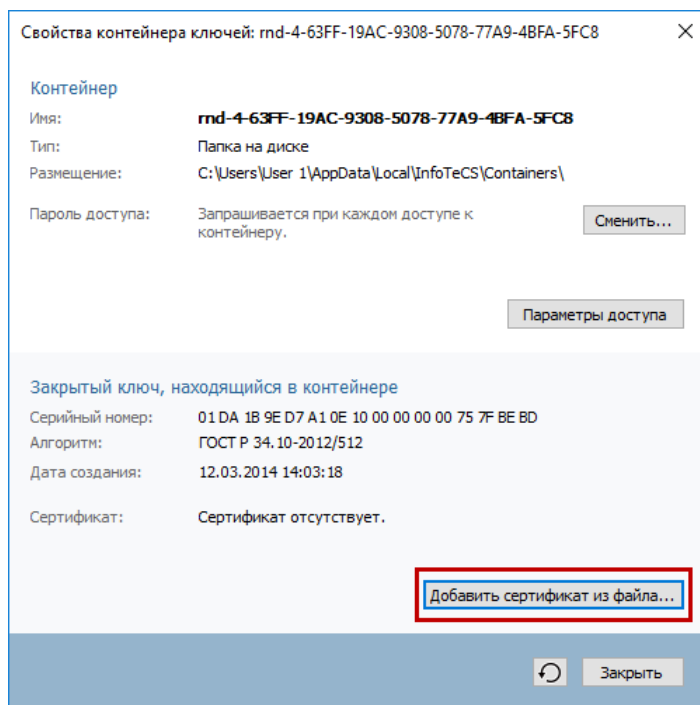


Рисунок 26. Добавление сертификата в контейнер ключей

- 4 В окне **Открыть** укажите файл сертификата, который соответствует закрытому ключу в контейнере, и нажмите **Открыть**. Если указан верный сертификат, он будет добавлен в контейнер, в противном случае появится сообщение «Сертификат не соответствует закрытому ключу в контейнере».

Установка сертификата в системное хранилище Windows

Чтобы использовать сертификат в различных приложениях, следует установить его в одно из следующих хранилищ сертификатов Windows:

- Хранилище текущего пользователя (Current User), раздел **Личное** > **Сертификаты** — сертификат следует установить в это хранилище в целях шифрования, расшифрования, создания и проверки электронной подписи файлов, а также для доступа к защищенным ресурсам через веб-браузер.
- Хранилище компьютера (Local Machine), раздел **Личное** > **Сертификаты** — сертификат следует установить в это хранилище при использовании ViPNet CSP на веб-сервере для организации доступа к защищенным ресурсам. Также в хранилище компьютера следует устанавливать сертификаты, которые будут использоваться службами данного компьютера.

Вы можете установить сертификат в системное хранилище Windows одним из следующих способов:

- Если сертификат еще не установлен в контейнер ключей, содержащий соответствующий закрытый ключ, в окне **ViPNet CSP** перейдите в раздел **Контейнеры ключей** и нажмите **Установить сертификат** (см. [Установка сертификата из файла](#)).
- Если сертификат уже установлен в контейнер ключей, установите сертификат в системное хранилище с помощью окна свойств контейнера ключей (см. [Установка сертификата из контейнера ключей](#)).

Установка сертификата из файла



Примечание. Для установки сертификата необходимы права администратора.

Если сертификат не добавлен в контейнер ключей, для установки сертификата в системное хранилище:

- 1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** нажмите **Установить сертификат**.
- 2 Выберите сертификат на диске (см. [Общая информация о ключах и сертификатах](#)) и нажмите **Далее**.
- 3 Укажите хранилище, в которое будет установлен сертификат (см. [Установка сертификата в системное хранилище Windows](#)).



Примечание. Сертификат будет установлен в выбранное хранилище в раздел **Другие пользователи** > **Сертификаты**.

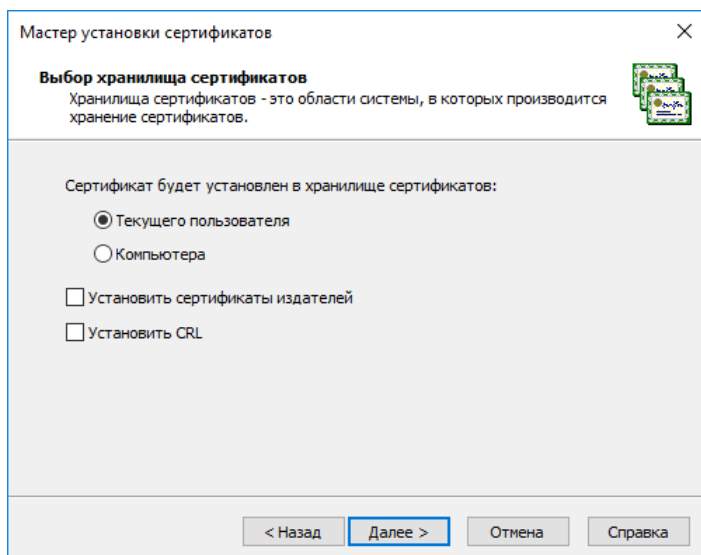


Рисунок 27. Выбор хранилища сертификатов



Примечание. При установке сертификата из файла с расширением *.p7b, *.p7s, *.p12 или *.pfx, в котором также содержатся сертификаты издателей или списки CRL, с помощью соответствующих флажков укажите, следует ли устанавливать эти сертификаты издателей или CRL.

Нажмите **Далее**.

4 Проверьте правильность выбранных параметров.

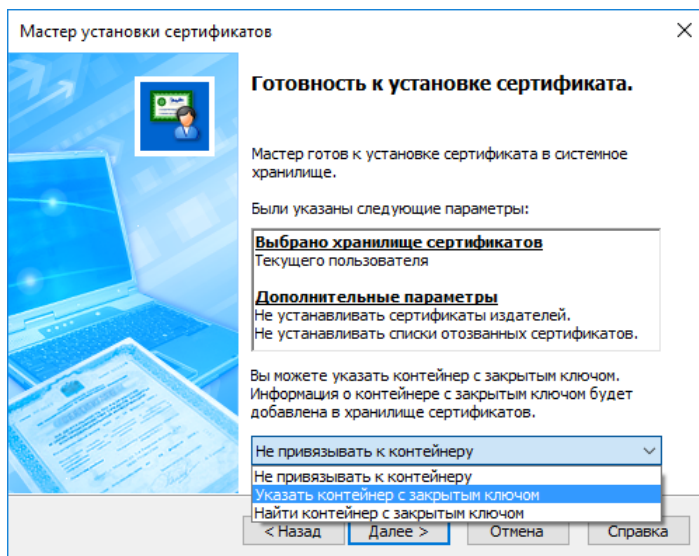


Рисунок 28. Сертификат готов к установке

В списке в нижней части окна выберите одно из действий:

- Если вы хотите позже указать расположение контейнера ключей, соответствующего сертификату, выберите **Не привязывать к контейнеру**. Работа мастера установки сертификата при этом завершается.

- Если вы хотите вручную указать расположение контейнера ключей, соответствующего сертификату, выберите **Указать контейнер с закрытым ключом**.
- Если вы хотите, чтобы программа выбрала подходящий контейнер ключей среди контейнеров, установленных в ViPNet CSP, выберите **Найти контейнер с закрытым ключом**.

Нажмите **Далее**.

- 5 Если вы выбрали **Указать контейнер с закрытым ключом**, в появившемся окне **ViPNet CSP – инициализация контейнера ключей** укажите расположение контейнера ключей: папку на диске (см. [Установка контейнера ключей из папки](#)) либо устройство с указанием его параметров и ПИН-кода (см. [Установка контейнера ключей с внешнего устройства](#)).



Примечание. Перечень поддерживаемых устройств хранения данных и полезная информация об их использовании содержится в приложении [Внешние устройства](#).

Нажмите **ОК**.

- 6 Если вы выбрали **Найти контейнер с закрытым ключом** и программа нашла подходящий контейнер ключей, в окне **ViPNet CSP – инициализация контейнера ключей** нажмите **ОК**.
- 7 В окне подтверждения нажмите **Да**, чтобы добавить сертификат в контейнер ключей, или **Нет**, чтобы оставить сертификат в виде отдельного файла.
- 8 Если на предыдущем шаге вы согласились добавить сертификат в контейнер ключей и нажали **Да**, в появившемся окне **ViPNet CSP – пароль контейнера ключей** в поле **Пароль** введите пароль доступа к контейнеру ключей, после чего нажмите **ОК**.



Примечание. Окно **ViPNet CSP – пароль контейнера ключей** не отображается в том случае, если ранее был сохранен пароль и установлен флажок **Не показывать больше это окно**.

- 9 На странице **Завершение работы мастера установки сертификата** нажмите **Готово**.

Сертификат установлен в выбранное хранилище сертификатов. Если в процессе установки сертификата ему не был сопоставлен закрытый ключ, необходимо установить контейнер с закрытым ключом, соответствующий сертификату (см. [Установка контейнера ключей из папки](#)), а затем установить в него этот сертификат (см. [Добавление сертификата в контейнер ключей](#)).

Если в процессе установки сертификату был сопоставлен закрытый ключ, контейнер с которым ранее не был установлен в ViPNet CSP, этот контейнер появится в списке контейнеров.

Кроме сертификата пользователя для работы с защищенными файлами и организации соединений TLS [установите сертификат издателя и список CRL](#).

Установка сертификата из контейнера ключей



Внимание! Сертификаты из контейнеров ключей в папке хранения ключей текущего пользователя следует устанавливать в хранилище ключей текущего пользователя.

Сертификаты из контейнеров ключей в папке хранения ключей компьютера следует устанавливать в хранилище ключей компьютера.

Для установки сертификата в системное хранилище из контейнера ключей:

- 1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** выберите контейнер ключей, сертификат из которого требуется установить.

Примечание. Папку хранения контейнеров ключей, отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:



- чтобы отобразить в списке контейнеры ключей, находящиеся в папке хранения ключей текущего пользователя, выберите **Ключи пользователя**;
- чтобы отобразить контейнеры ключей, находящиеся в папке хранения ключей компьютера, выберите **Ключи компьютера**;
- чтобы отобразить контейнеры ключей, находящиеся на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при запуске ViPNet CSP с правами администратора и наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. [Общая информация о ключах и сертификатах](#)).

- 2 Нажмите **Свойства** либо дважды щелкните контейнер ключей.
- 3 Если вы хотите установить сертификат в хранилище ключей текущего пользователя (см. [Установка сертификата в системное хранилище Windows](#)), выполните следующие действия:
 - 3.1 В окне **Свойства контейнера ключей** нажмите **Открыть**.

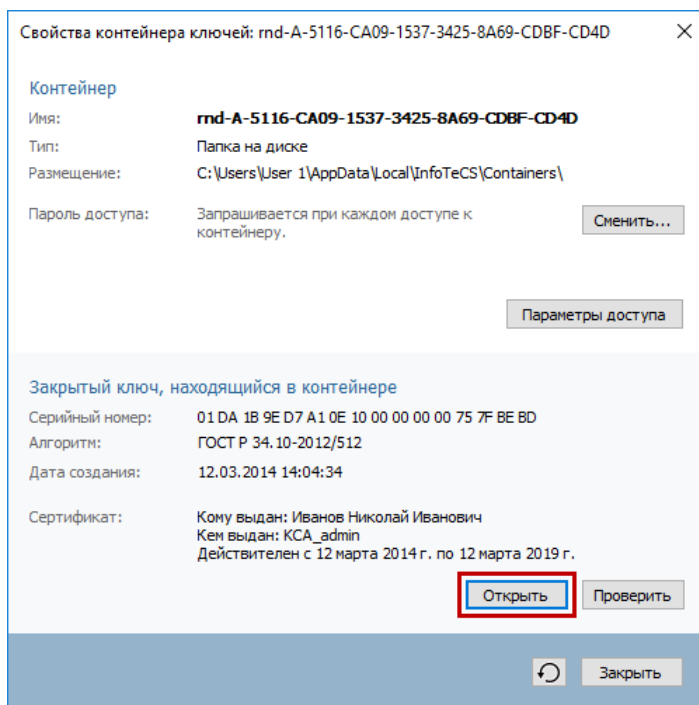


Рисунок 29. Установка сертификата в хранилище ключей текущего пользователя

- 3.2 В окне **Сертификат** на вкладке **Общие** нажмите **Установить сертификат**.
- 3.3 На странице приветствия мастера импорта сертификатов выберите расположение хранилища и нажмите **Далее**.
- 3.4 На странице **Хранилище сертификатов** выберите **Поместить все сертификаты в следующее хранилище** и нажмите **Обзор**.
- 3.5 В окне **Выбор хранилища сертификатов** выберите хранилище **Личное** и нажмите **Далее**.
- 3.6 На странице **Завершение мастера импорта сертификатов** нажмите **Готово**.
- 4 Если вы хотите установить сертификат в хранилище ключей компьютера (см. [Установка сертификата в системное хранилище Windows](#)), в окне **Свойства контейнера ключей** нажмите **Установить в личное хранилище**.

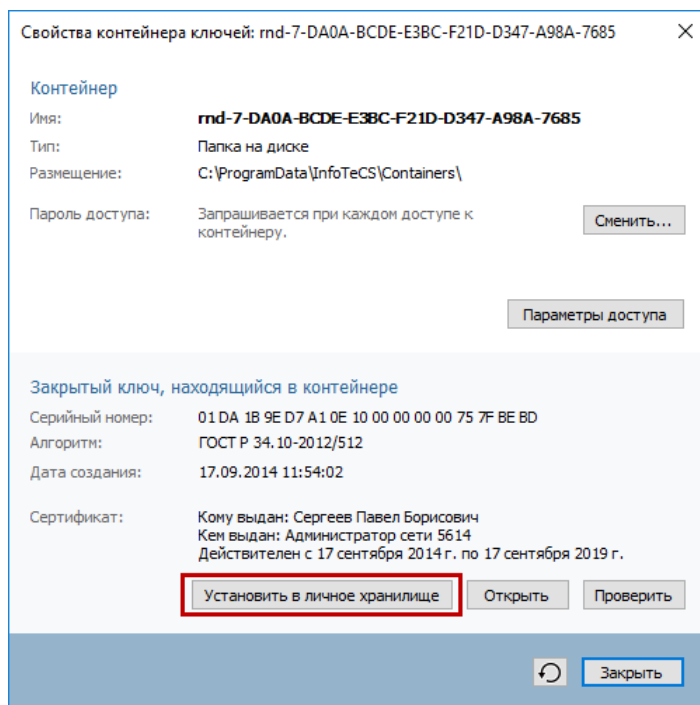


Рисунок 30. Установка сертификата в хранилище ключей компьютера



Примечание. Кнопка **Установить в личное хранилище** отображается только в окне свойств контейнера ключей, находящегося в папке хранения ключей компьютера (см. [Общая информация о ключах и сертификатах](#)).

Кроме сертификата пользователя для работы с защищенными файлами и организации соединений TLS [установите сертификат издателя и список CRL](#).

Установка сертификата издателя и списка аннулированных сертификатов

Для добавления электронной подписи и организации TLS-соединений требуется установить в системное хранилище:

- сертификаты пользователя (см. [Установка сертификата в системное хранилище Windows](#));
- сертификат издателя или цепочку сертификатов издателей;
- список аннулированных сертификатов (CRL).



Примечание. Если в вашем сертификате указан URL-адрес точки распространения списков аннулированных сертификатов и если ваш компьютер подключен к интернету, список CRL устанавливается и обновляется автоматически при просмотре свойств сертификата.

Установка сертификата издателя и списка CRL выполняется средствами операционной системы. Такой способ установки сертификата также необходим, если ПО ViPNet установлено на веб-сервере и используется для организации защищенных соединений TLS.

Для установки сертификата издателя и CRL:

- 1 Нажмите **Win+R** или в меню **Пуск > Выполнить**.
- 2 В поле **Открыть** введите команду `mmc` и нажмите **ОК**.
- 3 В окне консоли управления Microsoft в меню **Файл** выберите **Добавить или удалить оснастку**.
- 4 В окне **Добавление и удаление оснасток** в списке **Доступные оснастки** выберите оснастку **Сертификаты** и нажмите **Добавить**.
- 5 В окне **Оснастка диспетчера сертификатов** выберите один из следующих вариантов:
 - Чтобы установить сертификат издателя или список CRL в хранилище компьютера (см. [Установка сертификата в системное хранилище Windows](#)), выберите вариант **учетной записи компьютера**, нажмите **Далее**, а затем **Готово**.
 - Чтобы установить сертификат издателя или список CRL в хранилище текущего пользователя (см. [Установка сертификата в системное хранилище Windows](#)), выберите вариант **моей учетной записи пользователя** и нажмите **Готово**.
- 6 Нажмите **ОК**.
- 7 На панели навигации консоли управления Microsoft щелкните правой кнопкой мыши хранилище:
 - **Доверенные корневые центры сертификации**, если вы устанавливаете сертификат издателя, являющийся **корневым в цепочке сертификации**.



Примечание. Если сертификат издателя является единственным в [цепочке сертификации](#), он также считается корневым.

- Промежуточные центры сертификации, если вы устанавливаете:
 - список CRL;
 - сертификат издателя, который является промежуточным в [цепочке сертификации](#).

8 В контекстном меню выберите **Все задачи > Импорт**.

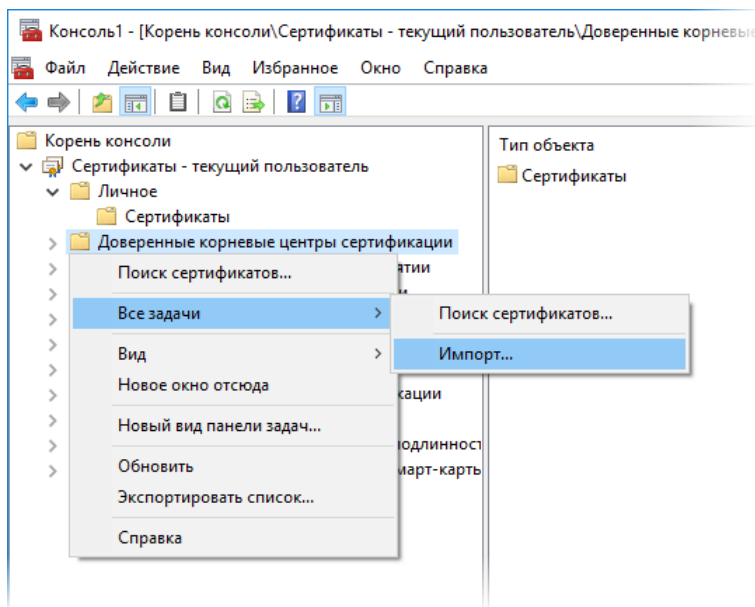


Рисунок 31. Выбор хранилища для сертификата издателя

- 9 На первой странице мастера импорта сертификатов нажмите **Далее**.
- 10 На странице **Мастер импорта сертификатов** выберите файл с сертификатом издателя или списком CRL.
- 11 На странице **Хранилище сертификатов** отобразится выбранное ранее хранилище сертификатов.
- 12 На странице **Завершение мастера импорта сертификатов** нажмите **Готово**.



Внимание! Если система не сможет проверить подлинность сертификата (например, отсутствует подключение к Интернету или узел проверки недоступен), появится окно **Предупреждение системы безопасности**. Чтобы установить сертификат без проверки, нажмите **Да**.

Устанавливайте только те сертификаты, в подлинности которых вы уверены.

- 13 В появившемся окне с сообщением об успешном импорте сертификата нажмите **ОК**. Установка будет завершена.

После этого, если вы уже выполнили установку личного и корневого сертификатов, можно приступить к выполнению криптографических операций (см. [Варианты использования ViPNet CSP](#)).

Установка и обновление CRL через Интернет



Примечание. Предварительно убедитесь, что в вашем сертификате указан URL-адрес точки распространения списков аннулированных сертификатов и ваш компьютер подключен к Интернету.

Чтобы установить или обновить список CRL автоматически:

- 1 В разделе **Контейнеры ключей** выберите контейнер ключей, которому соответствует сертификат, список CRL для которого требуется установить или обновить.

Примечание. [Папку хранения контейнеров ключей](#), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:



- чтобы отобразить в списке контейнеры ключей, находящиеся в папке хранения ключей текущего пользователя, выберите **Ключи пользователя**;
- чтобы отобразить контейнеры ключей, находящиеся в папке хранения ключей компьютера, выберите **Ключи компьютера**;
- чтобы отобразить контейнеры ключей, находящиеся на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при запуске ViPNet CSP с правами администратора и наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. [Общая информация о ключах и сертификатах](#)).

- 2 Нажмите **Свойства** либо дважды щелкните контейнер ключей.
- 3 В окне **Свойства контейнера ключей** нажмите **Открыть**.

Откроется окно со свойствами сертификата. При этом будет выполнено подключение к точке распространения списков CRL:

- Если список CRL не был установлен ранее, он будет загружен и автоматически установлен.
- Если список CRL уже установлен, будет проверена его актуальность, при необходимости он будет автоматически обновлен.

6

Операции с контейнерами ключей

Просмотр и настройка свойств контейнера ключей	72
Создание резервной копии контейнера ключей	77
Перенос сертификатов и закрытых ключей между компьютерами	78
Использование ключей подписи пользователя сетевого узла	81
Удаление контейнера ключей	82

Просмотр и настройка свойств контейнера ключей

Чтобы просмотреть свойства контейнера ключей или изменить его настройки:

- 1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** выберите контейнер.



Примечание. Папку хранения контейнеров ключей, отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:

- чтобы отобразить в списке контейнеры ключей, находящиеся в папке хранения ключей текущего пользователя, выберите **Ключи пользователя**;
- чтобы отобразить контейнеры ключей, находящиеся в папке хранения ключей компьютера, выберите **Ключи компьютера**;
- чтобы отобразить контейнеры ключей, находящиеся на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при запуске ViPNet CSP с правами администратора и наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. [Общая информация о ключах и сертификатах](#)).

- 2 Нажмите **Свойства** либо дважды щелкните контейнер ключей.
- 3 Вы можете:
 - Просмотреть информацию о закрытом ключе и сертификате, которые находятся в контейнере ключей.
 - [Сменить пароль доступа к контейнеру ключей.](#)
 - [Удалить сохраненный пароль доступа к контейнеру ключей.](#)
 - Произвести установку сертификата пользователя.
 - [Настроить права доступа к контейнеру ключей.](#)

Смена пароля к контейнеру ключей

Для смены пароля к контейнеру ключей в папке на диске:

- 1 В окне **Свойства контейнера ключей** нажмите **Сменить**.

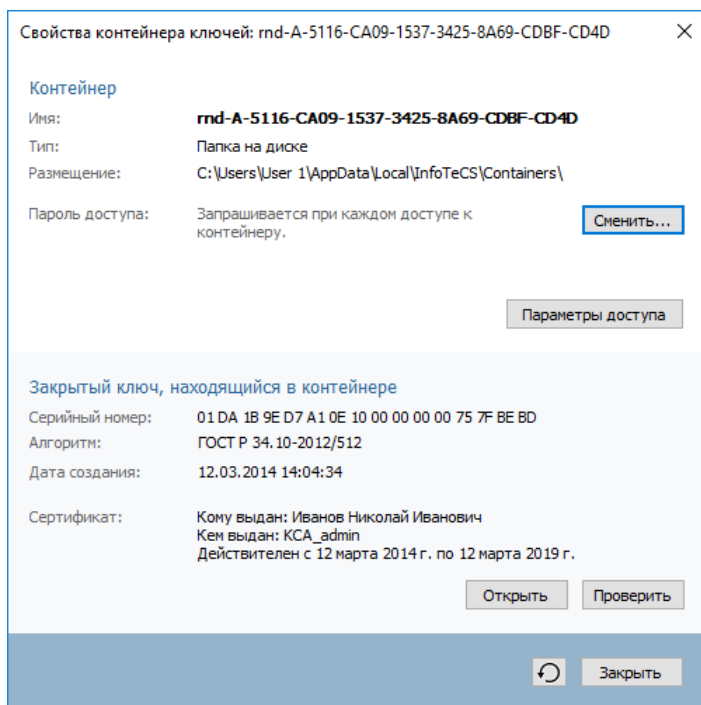


Рисунок 32. Информация о контейнере ключей

- В окне **Пароль** введите текущий пароль доступа к контейнеру ключей и нажмите **ОК**.



Примечание. Если ранее был установлен режим **Сохранить пароль**, то окно **Пароль** не появится.

- В окне **ViPNet CSP - смена пароля контейнера ключей** укажите текущий пароль, задайте и подтвердите новый пароль. Нажмите **ОК**.



Внимание! Запрещается вводить пароль при помощи операций копирования и вставки через буфер обмена.

Чтобы сохранить пароль для последующих обращений к контейнеру ключей, установите флажок **Сохранить пароль**.

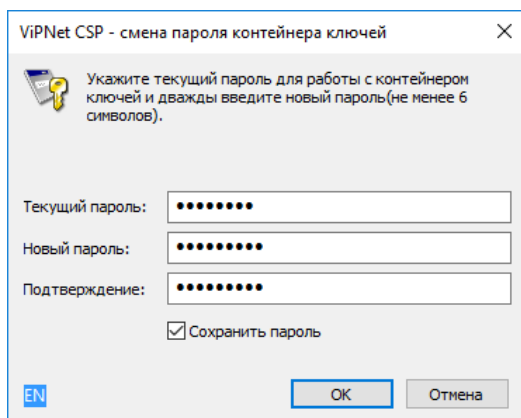


Рисунок 33. Смена пароля доступа к контейнеру ключей



Внимание! Не создавайте пароль длиной в 32 символа и более. Пароли с такой длиной не могут использоваться в текущих версиях приложений ViPNet. Данное ограничение связано с существующим алгоритмом передачи пароля в криптопровайдер. В соответствии с этим алгоритмом длина пароля не должна превышать 31 символ.

Удаление сохраненного пароля

Удаление сохраненного пароля к контейнеру ключей может потребоваться в том случае, если изменились условия эксплуатации пароля или регламент вашей организации, вследствие чего хранение пароля на компьютере стало недопустимым.

Для удаления ранее сохраненного в системе пароля к контейнеру ключей в окне **Свойства контейнера ключей** нажмите **Удалить**.

Теперь пароль необходимо вводить всякий раз при обращении к контейнеру ключей.

Проверка контейнера ключей

Проверка контейнера ключей позволяет убедиться, что файл контейнера не поврежден, хранящиеся в контейнере сертификат и ключ электронной подписи соответствуют друг другу и могут быть использованы для работы с защищенными документами.

Чтобы проверить контейнер ключей:

- 1 В окне **Свойства контейнера ключей** нажмите **Проверить**.
- 2 В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите **ОК**.

Чтобы сохранить пароль для последующих обращений к контейнеру ключей, выберите **Сохранить пароль**.

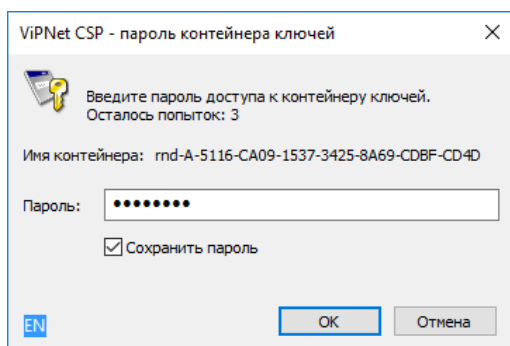


Рисунок 34. Ввод пароля доступа к контейнеру ключей

Далее будет сформирован фрагмент данных, который будет подписан с помощью ключа электронной подписи, после чего будет выполнена проверка электронной подписи с помощью ключа проверки электронной подписи. Так будет проверена пригодность ключа электронной подписи и его соответствие сертификату ключа проверки электронной подписи, хранящемуся в контейнере.

В результате вы получите сообщение с результатом проверки.



Примечание. Проверка возможна только в том случае, если в контейнере ключей есть сертификат, соответствующий ключу электронной подписи.

При проверке ключа электронной подписи проверка действительности сертификата (срок его действия, отсутствие в списках аннулированных сертификатов и прочее) не выполняется.

Настройка прав доступа к контейнеру ключей

С помощью прав доступа вы можете разрешать или запрещать доступ к контейнеру ключей для субъектов безопасности операционной системы Windows (например, учетных записей и групп пользователей). Например, разрешение на доступ к контейнеру ключей для встроенной учетной записи NETWORK SERVICE может потребоваться при настройке сервера IIS (см. [Настройка серверной части](#)).

Для настройки прав доступа к контейнеру ключей:

- 1 В окне **Свойства контейнера ключей** нажмите **Параметры доступа**.
- 2 В окне **Разрешения для группы**:
 - 2.1 В области **Группы и пользователи** выберите учетную запись или группу учетных записей Windows, для которых необходимо задать разрешения.
 - 2.2 В области **Разрешения для группы** задайте разрешения для выбранных учетных записей.
 - 2.3 Нажмите **ОК**.

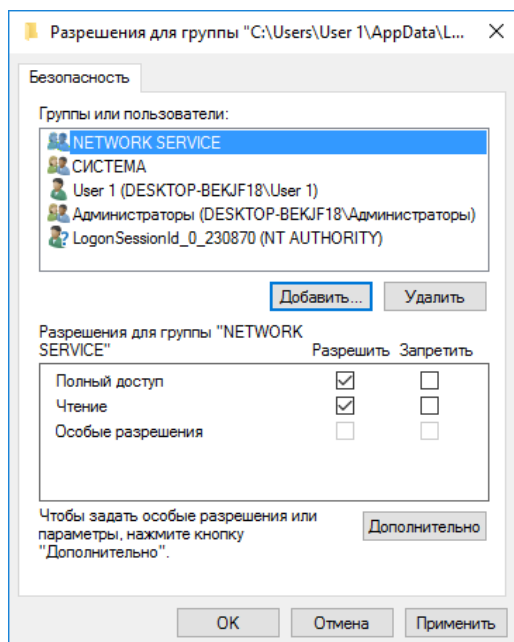


Рисунок 35. Настройка прав доступа к контейнеру ключей

Права доступа для выбранных учетных записей изменены.

Создание резервной копии контейнера ключей

Вы можете скопировать контейнер ключей в папку на диске или на внешнее устройство. Эта функция может быть использована для создания резервной копии контейнера ключей.



Примечание. Копирование контейнера ключей подписи с внешних устройств с аппаратной поддержкой алгоритмов ГОСТ невозможно.

Для копирования контейнера:

- 1 В разделе **Контейнеры ключей** выберите контейнер ключей, который вы хотите скопировать.



Совет. Папку хранения контейнеров ключей, отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна.

- 2 Нажмите **Копировать в**.
- 3 В окне **ViPNet CSP - инициализация контейнера ключей** укажите новое имя для контейнера и место его расположения. Вы можете скопировать контейнер ключей в папку на диске или на внешнее устройство. Нажмите **ОК**.
- 4 В окне **ViPNet CSP - пароль контейнера ключей** введите пароль (или ПИН, если контейнер ключей находится на внешнем устройстве) доступа к контейнеру ключей, копию которого требуется создать.

Чтобы сохранить пароль для последующих обращений к контейнеру ключей, выберите **Сохранить пароль**.

Затем нажмите **ОК**.
- 5 В окне **ViPNet CSP - пароль контейнера ключей** задайте и подтвердите пароль, который будет использоваться для доступа к создаваемой копии контейнера.



Примечание. Сохранение пароля к контейнеру ключей в системе ведет к снижению уровня безопасности.

Копия контейнера ключей появится в списке контейнеров ключей (в папке хранения ключей текущего пользователя) и в указанной папке (либо на устройстве).

Перенос сертификатов и закрытых ключей между компьютерами

Если вы хотите перенести сертификаты или закрытые ключи с компьютера, на котором установлен криптопровайдер ViPNet CSP, на другой компьютер с ViPNet CSP либо на компьютер с криптопровайдером другого производителя:

- 1 На компьютере с ViPNet CSP экспортируйте сертификат отдельно или вместе с закрытым ключом в файл одного из универсальных форматов (см. [Экспорт сертификата и закрытого ключа в файл](#)).
- 2 На компьютере, где вы хотите использовать экспортированный сертификат или сертификат с закрытым ключом, выполните одно из действий:
 - Если на компьютере установлен криптопровайдер ViPNet CSP, импортируйте сертификат или сертификат с закрытым ключом (см. [Импорт сертификата и закрытого ключа из файла](#)).
 - Если на компьютере используется криптопровайдер другого производителя, импортируйте сертификат или сертификат с закрытым ключом, следуя руководству для данного криптопровайдера.

Экспорт сертификата и закрытого ключа в файл

Для переноса сертификатов и закрытых ключей между компьютерами вы можете экспортировать установленные сертификаты и закрытые ключи из контейнера в файлы различных форматов:

- 1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** выберите контейнер ключей, содержащий сертификат, которые вы хотите экспортировать.

Примечание. [Папку хранения контейнеров ключей](#), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:



- чтобы отобразить в списке контейнеры ключей, находящиеся в папке хранения ключей текущего пользователя, выберите **Ключи пользователя**;
- чтобы отобразить контейнеры ключей, находящиеся в папке хранения ключей компьютера, выберите **Ключи компьютера**;
- чтобы отобразить контейнеры ключей, находящиеся на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при запуске ViPNet CSP с правами администратора и наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. [Общая информация о ключах и сертификатах](#)).

- 2 Нажмите **Свойства** либо дважды щелкните контейнер ключей.

- 3 В окне **Свойства контейнера ключей** нажмите **Открыть**.
- 4 В окне **Сертификат** перейдите на вкладку **Состав** и нажмите **Копировать в файл**.
- 5 На странице приветствия мастера экспорта сертификатов нажмите **Далее**.
- 6 На странице **Экспортирование закрытого ключа** укажите, хотите ли вы вместе с сертификатом экспортировать закрытый ключ.



Примечание. Вы можете экспортировать вместе с сертификатом закрытый ключ, только если при формировании запроса на этот сертификат был установлен флажок **Экспортируемый** (см. [Получение закрытого ключа и сертификата](#)).

- 7 На странице **Формат экспортируемого файла** выберите формат для экспорта сертификата и дополнительные параметры экспорта. Формат и параметры должны определяться документами вашей организации.

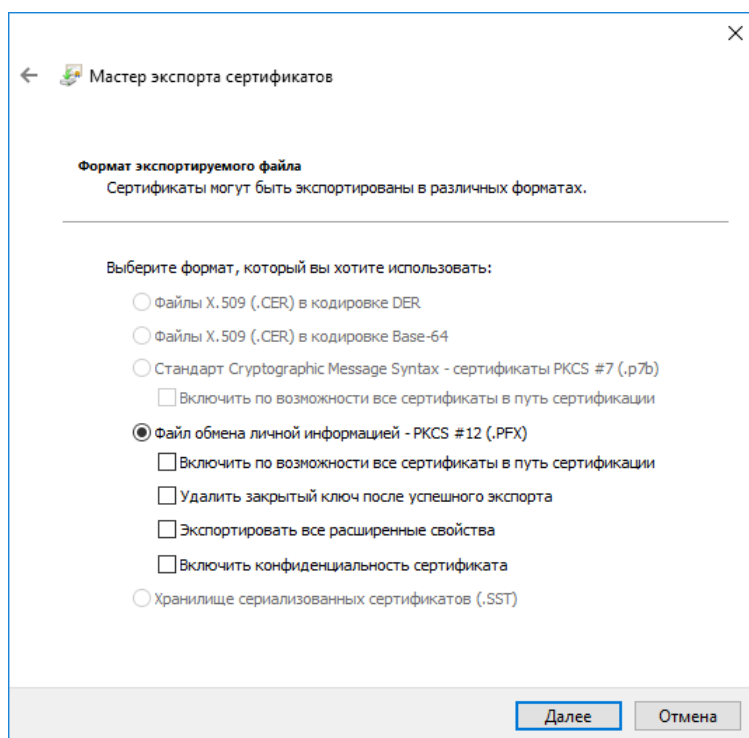


Рисунок 36. Выбор формата экспортируемого файла

- 8 Если вы экспортируете закрытый ключ вместе с сертификатом, на странице **Безопасность** задайте и подтвердите пароль доступа к экспортируемому закрытому ключу, выберите алгоритм шифрования.
- 9 На странице **Имя файла экспорта** укажите папку для создания файла с экспортируемыми ключами и имя этого файла.
- 10 На странице завершения работы мастера экспорта сертификатов нажмите **Готово**.



Внимание! Несмотря на то что файл формата PKCS#12 (с расширением .p12 или .pfx), содержащий закрытый ключ, защищен паролем, по требованиям безопасности он должен передаваться на другой компьютер только доверенным способом.

Импорт сертификата и закрытого ключа из файла



Внимание! Если сертификат и закрытый ключ были экспортированы в файл с помощью программы ViPNet CSP 4.2.10 или более поздней версии, такой файл невозможно будет импортировать в программе ViPNet CSP 4.2.8 или более ранней версии.

На компьютер с установленной программой ViPNet CSP можно импортировать сертификат отдельно или вместе с закрытым ключом из файла.

Если файл содержит только сертификат, для установки сертификата см. раздел Установка сертификата, не добавленного в контейнер ключей (см. [Установка сертификата из файла](#)).

Если файл содержит помимо сертификата закрытый ключ:

- 1 В окне **ViPNet CSP** в разделе **Контейнеры ключей** нажмите **Установить сертификат**.
- 2 В окне **Открыть** укажите путь к файлу, содержащему сертификат вместе с закрытым ключом (см. [Общая информация о ключах и сертификатах](#)).
- 3 В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите **ОК**.
- 4 В окне **ViPNet CSP - инициализация контейнера ключей** нажмите **ОК**.
- 5 В окне **ViPNet CSP - пароль контейнера ключей** задайте пароль доступа к контейнеру ключей и нажмите **ОК**.

Использование ключей подписи пользователя сетевого узла

Контейнер ключей, установленный на сетевом узле ViPNet с программным обеспечением ViPNet Client или ViPNet Coordinator (версии 3.2.2 или выше), можно перенести на другой компьютер для использования в ViPNet CSP. Чтобы использовать в ViPNet CSP ключи подписи пользователя сетевого узла ViPNet:

- 1 В программах ViPNet Client или ViPNet Coordinator откройте окно **Настройки параметров безопасности** и перейдите на вкладку **Ключи**.
- 2 В группе **Электронная подпись** нажмите **Перенести**.

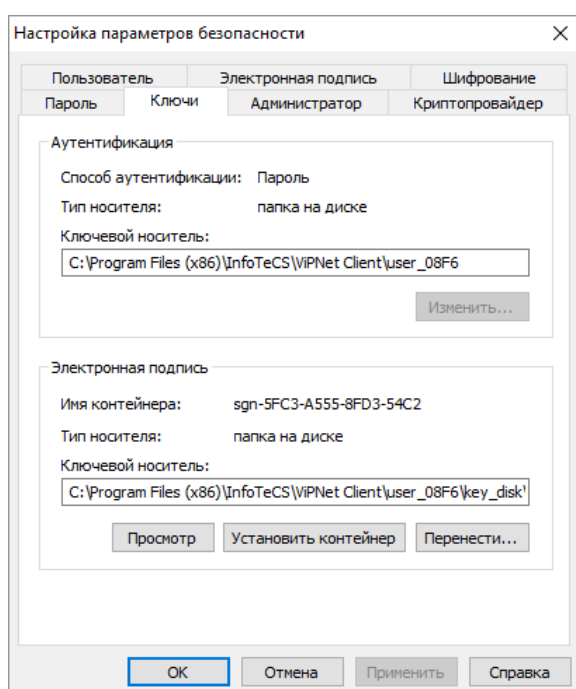


Рисунок 37. Работа с контейнером ключей

- 3 В окне **ViPNet CSP - инициализация контейнера ключей** нажмите **Обзор** и укажите папку или съемный носитель, на который требуется перенести контейнер ключей. Затем нажмите **ОК**, контейнер будет перенесен в указанную папку.
- 4 Скопируйте контейнер ключей на компьютер, на котором установлена ViPNet CSP.



Внимание! При удалении контейнера ключей с сетевого узла ViPNet использование ключей подписи на этом сетевом узле будет невозможно.

- 5 В ViPNet CSP выполните установку контейнера ключей (см. [Установка контейнера ключей из папки](#)).

Удаление контейнера ключей

- 1 В разделе **Контейнеры ключей** выберите контейнер ключей.

Примечание. Папку хранения контейнеров ключей (см. [Общая информация о ключах и сертификатах](#)), отображаемых в списке, вы можете выбрать с помощью раскрывающегося списка в верхней части окна:



- чтобы отобразить в списке контейнеры ключей из папки хранения ключей текущего пользователя, выберите пункт **Ключи пользователя**;
- чтобы отобразить контейнеры ключей из папки хранения ключей компьютера, выберите пункт **Ключи компьютера**;
- чтобы отобразить контейнеры ключей на внешнем устройстве, выберите пункт с именем этого устройства.

Пункт **Ключи компьютера** появляется в списке только при запуске ViPNet CSP с правами администратора и наличии хотя бы одного контейнера ключей в папке хранения ключей компьютера (см. [Общая информация о ключах и сертификатах](#)).

-
- 2 Нажмите .



Внимание! Удаленный контейнер ключей невозможно восстановить. Перед удалением вы можете создать [резервную копию контейнера](#).

-
- 3 Чтобы подтвердить удаление контейнера ключей, в появившемся окне нажмите **ОК**.

7

Работа с внешними устройствами

Доступ к контейнерам ключей на внешнем устройстве	84
Настройка списка опрашиваемых устройств	85
Инициализация устройства	87
Особенности работы с внешними устройствами, на которых установлено более одного апплета	89
Смена ПИН-кода	90
Использование датчика случайных чисел	91

Доступ к контейнерам ключей на внешнем устройстве

ViPNet CSP позволяет работать с контейнерами ключей, которые хранятся на [внешних устройствах](#). Допускается работа только с такими ключами и сертификатами, которые созданы в соответствии со стандартом PKCS#11 и рекомендациями ТК26.

Для просмотра подключенных устройств и хранящихся на них контейнеров ключей выполните следующие действия:

- 1 Перейдите в раздел **Контейнеры ключей**.
- 2 В списке вверху выберите название подключенного устройства.

Если список контейнеров ключей пуст, значит на выбранном устройстве нет контейнеров ключей, созданных в соответствии со стандартом PKCS#11.



Примечание. В раскрывающемся списке помимо [папок хранения контейнеров ключей](#) отображаются только те устройства, которые в данный момент подключены к разъему USB или считывателю смарт-карт.

С контейнером ключей на внешнем устройстве вы можете работать так же, как и с контейнером ключей, хранящемся на вашем компьютере. Исключением являются устройства, которые используют аппаратную криптографию с неизвлекаемым ключом (см. [Список поддерживаемых внешних устройств](#)).

Настройка списка опрашиваемых устройств



Примечание. Не включайте опрос семейств устройств **Infotecs Software Token** и **ViPNet HSM**. Это может вызвать ошибки в работе программы.

При включении опроса устройств семейства **Infotecs Software Token** может появиться [электронная рулетка](#).

По умолчанию ViPNet CSP проводит поиск устройств всех поддерживаемых семейств, кроме **Infotecs Software Token**. Чтобы сократить время поиска нужного ключа, отключите поиск неиспользуемых устройств.

Чтобы указать семейства устройств, которыми будете пользоваться:

- 1 Перейдите в раздел **Подключаемые устройства**.

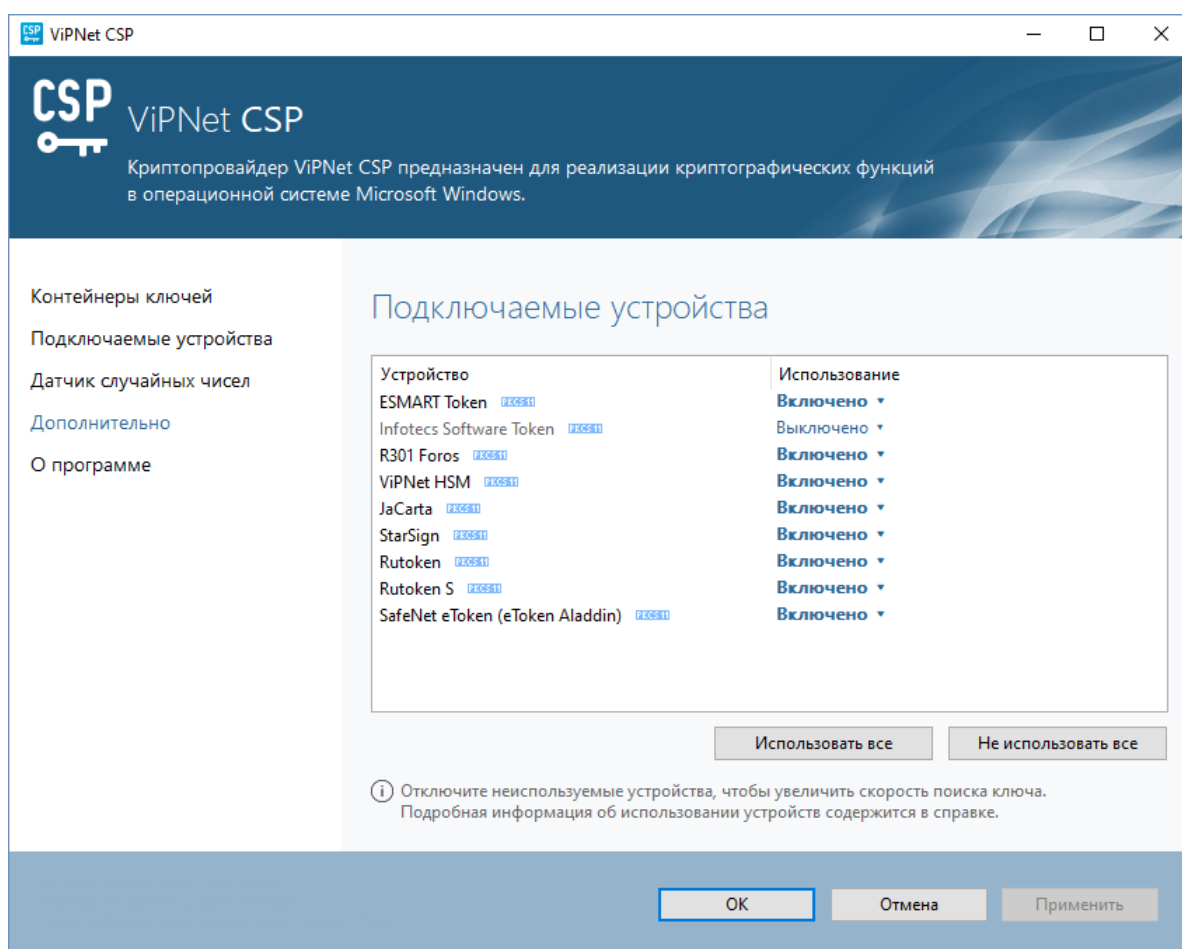


Рисунок 38. Настройка списка опрашиваемых устройств

- 2 Напротив семейств устройств, которые не требуется использовать, нажмите **Включено** и в контекстном меню выберите **Выключить**. После этого работа таких устройств с программой будет невозможна.



Примечание. Чтобы разрешить использование всех семейств устройств, нажмите **Использовать все**.

Инициализация устройства

Инициализацией называется форматирование памяти устройства. В процессе инициализации все данные, хранящиеся на устройстве, удаляются. Пароль и другие настройки устройства сбрасываются.



Внимание! Для большинства поддерживаемых устройств производитель предоставляет специализированное ПО для администрирования, и инициализация таких устройств должна выполняться с помощью этого ПО.

В ViPNet CSP доступна функция инициализации только для устройств **Infotecs Software Token**.

Для инициализации подключенного устройства:

- 1 Убедитесь в том, что устройство, которое необходимо инициализировать, не содержит нужной вам информации.
- 2 В окне **ViPNet CSP** перейдите в раздел **Подключаемые устройства**.
- 3 В списке **Подключаемые устройства** рядом с названием подключенного устройства нажмите .
- 4 В появившемся меню выберите **Инициализировать**.

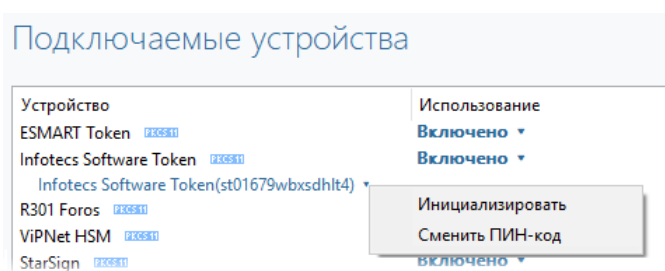
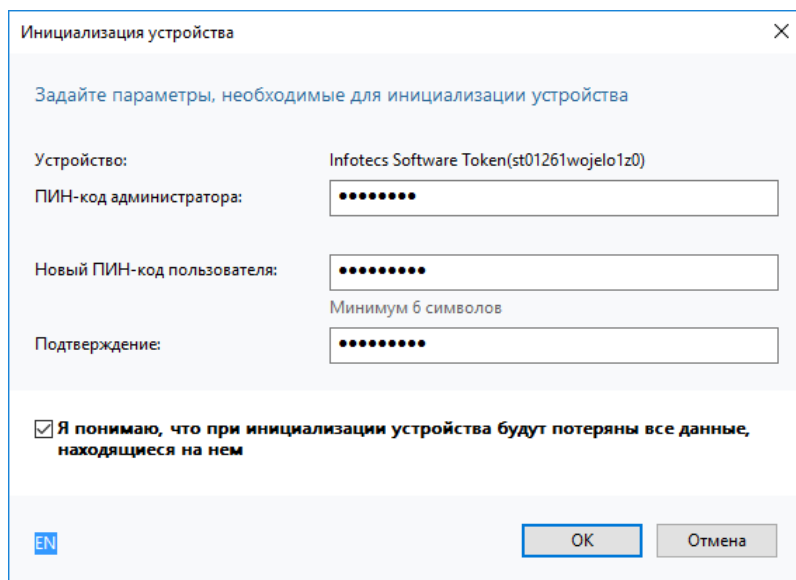


Рисунок 39. Выбор внешнего устройства для инициализации

- 5 В окне **Инициализация устройства**:
 - 5.1 Введите ПИН администратора.
 - 5.2 В двух других полях окна введите новый ПИН пользователя.
 - 5.3 Установите флажок, подтверждающий согласие на инициализацию устройства.
 - 5.4 Нажмите **ОК**.



Инициализация устройства

Задайте параметры, необходимые для инициализации устройства

Устройство: Infotecs Software Token(st01261wojelo1z0)

ПИН-код администратора:

Новый ПИН-код пользователя:
Минимум 6 символов

Подтверждение:

☒ Я понимаю, что при инициализации устройства будут потеряны все данные, находящиеся на нем

EN OK Отмена

Рисунок 40. Инициализация внешнего устройства

После инициализации все хранившиеся на устройстве данные будут удалены. Для доступа к устройству будет использоваться заданный ПИН пользователя.

Особенности работы с внешними устройствами, на которых установлено более одного апплета

ViPNet CSP позволяет работать с комбинированными внешними устройствами, на которых установлено более одного криптографического приложения (далее — апплета).

При подключении таких устройств каждый из установленных апплетов распознается ViPNet CSP как отдельное устройство, то есть так, как если бы вы подключили несколько разных устройств одного семейства.

Чтобы использовать в ViPNet CSP определенный апплет из установленных на вашем устройстве, выберите его из списка внешних устройств.

На рисунке ниже приведен пример отображения устройства JaCarta-2 PKI/ГОСТ.

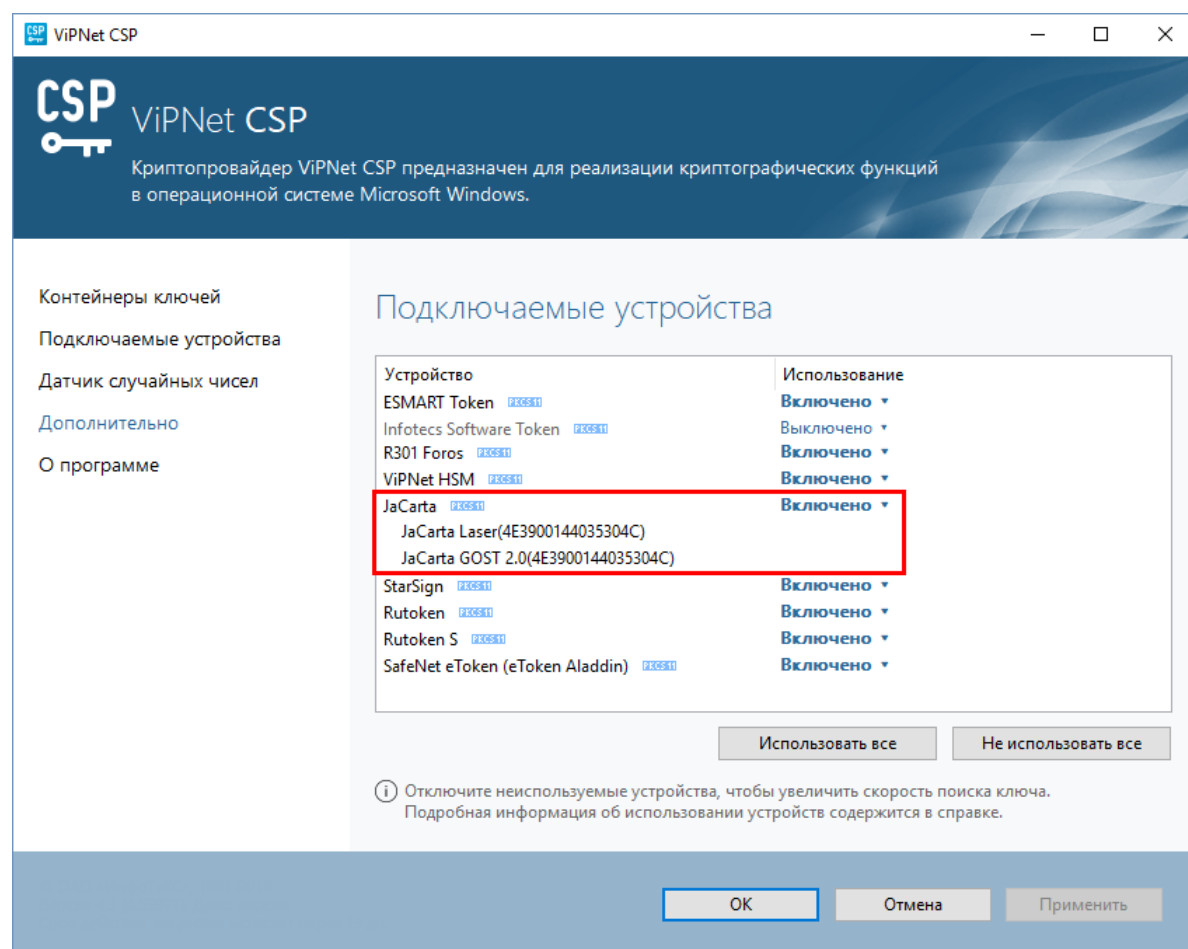


Рисунок 41. Подключение внешнего устройства, на котором установлено два апплета

Смена ПИН-кода

Смена ПИН-кода устройства может потребоваться в связи с истечением срока действия пароля или по другим причинам, утвержденным регламентом организации.



Внимание! Для большинства поддерживаемых устройств производитель предоставляет специализированное ПО для администрирования, и смена ПИН-кода на таких устройствах должна выполняться с помощью этого ПО.

В ViPNet CSP доступна функция смены ПИН-кода только для устройств **Infotecs Software Token**.

Если производитель устройства предоставляет специализированное ПО для администрирования, используйте для смены ПИН-кода это ПО. Для остальных устройств доступна функция смены ПИН-кода в ViPNet CSP.

Чтобы сменить ПИН-код устройства:

- 1 В окне **ViPNet CSP** перейдите в раздел **Подключаемые устройства**.
- 2 В списке **Подключаемые устройства** рядом с названием подключенного устройства нажмите .
- 3 В появившемся меню выберите **Сменить ПИН-код**.
- 4 В окне **Смена ПИН-кода**:
 - 4.1 В списке **Сменить** выберите тип изменяемого ПИН-кода.
 - 4.2 В поле **Текущий ПИН-код** укажите прежний ПИН-код, а в оставшихся двух полях — новый ПИН-код.
 - 4.3 Нажмите **ОК**.

Смена ПИН-кода

Задайте параметры, необходимые для смены ПИН-кода устройства

Устройство: Infotecs Software Token(st01261wojelo1z0)

Сменить: ПИН-код пользователя

Текущий ПИН-код:

Новый ПИН-код:
Минимум 6 символов

Подтверждение:

EN OK Отмена

Рисунок 42. Смена ПИН-кода внешнего устройства

В результате ПИН-код устройства будет изменен.

Использование датчика случайных чисел

Датчик случайных чисел создает случайные последовательности чисел, на основе которых формируются закрытые ключи.

В качестве датчика случайных чисел в ViPNet CSP можно использовать:

- встроенный датчик — биологический (или [электронная рулетка](#));
- аппаратный датчик случайных чисел;
- предварительно созданную последовательность случайных чисел.

Чтобы выбрать используемый датчик случайных чисел:

- 1 В окне **ViPNet CSP** перейдите в раздел **Датчик случайных чисел**.

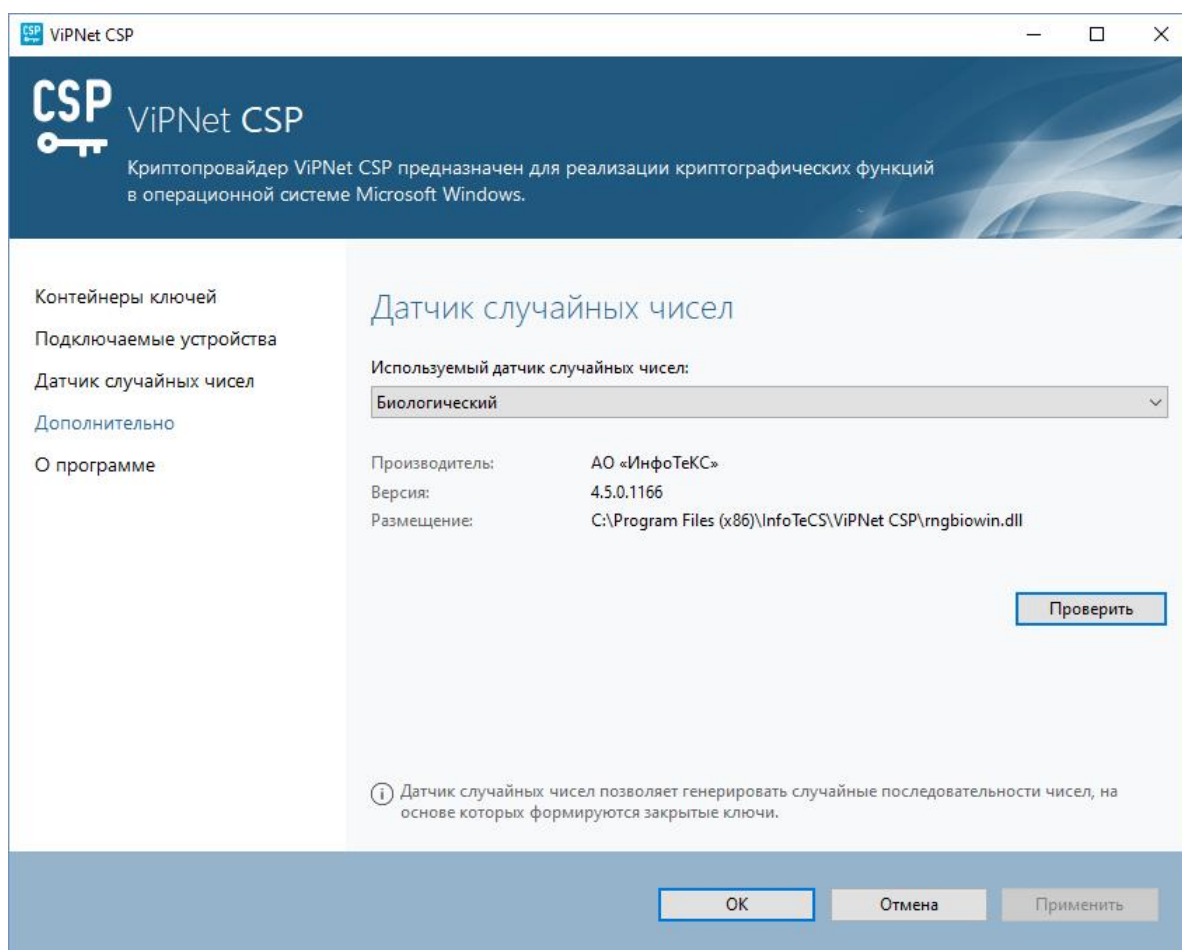


Рисунок 43. Выбор датчика случайных чисел

- 2 В списке **Используемый датчик случайных чисел** выберите один из вариантов:

- **Биологический** — чтобы использовать для создания последовательности случайных чисел «электронную рулетку».
- **Внешнее устройство** — чтобы использовать для создания последовательности случайных чисел подключенное [поддерживаемое внешнее устройство](#).



Примечание. Если в качестве датчика случайных чисел выбрано внешнее устройство, перед созданием запроса на сертификат и проверкой работоспособности датчика случайных чисел подключите к компьютеру это внешнее устройство.

При использовании устройств с аппаратной поддержкой алгоритмов ГОСТ последовательности случайных чисел всегда создаются с помощью этих устройств.

- **ДСДР** — чтобы использовать предварительно созданную последовательность [случайных чисел \(гамму\)](#). После выбора этого варианта выполните следующие действия:
 - Нажмите **Добавить гамму**.
 - В окне **Обзор папок** укажите папку, в которой находятся файлы, содержащие последовательность случайных чисел.



Примечание. Последовательности случайных чисел (гаммы) изготавливаются в Федеральной службе безопасности России (ФСБ) и поставляются на дисках ДСДР в составе ключевых блокнотов.

- **Аппаратный датчик случайных чисел, установленный на компьютере.**



Примечание. Аппаратные датчики случайных чисел, не установленные на компьютере, не отображаются в списке **Используемый датчик случайных чисел**.

При использовании датчика случайных чисел аппаратного модуля доверенной загрузки «Аккорд-АМД3» помимо установки стандартного программного обеспечения скопируйте файл `tmdrv32.dll` из комплекта поставки в папку `C:\Windows\System32` (для 32-разрядной версии Windows) или в папку `C:\Windows\SysWOW64` (для 64-разрядной версии Windows).

3 Для сохранения параметров нажмите **Применить**.

Свойства выбранного устройства отображаются под списком **Используемый датчик случайных чисел**.

Чтобы проверить работоспособность биологического или аппаратного датчика случайных чисел, нажмите **Проверить**. После проверки программа выдаст сообщение о ее результате.



Примечание. При первом запуске проверки датчика случайных чисел может появиться окно с предупреждением о нарушении статистики. Это поведение обусловлено особенностями сбора статистики. В таком случае запустите проверку повторно.

8

Дополнительные настройки ViPNet CSP

Настройка регистрации событий криптопровайдера	94
Включение аудита доступа к объектам	96
Добавление элементов аудита доступа к объектам	97

Настройка регистрации событий криптопровайдера

В ViPNet CSP организовано ведение журнала событий, с помощью которого можно следить за работой криптопровайдера. События записываются в системный журнал Windows.

Чтобы задать режим ведения журнала либо отключить запись событий:

- 1 В главном окне ViPNet CSP перейдите в раздел **Дополнительно**.

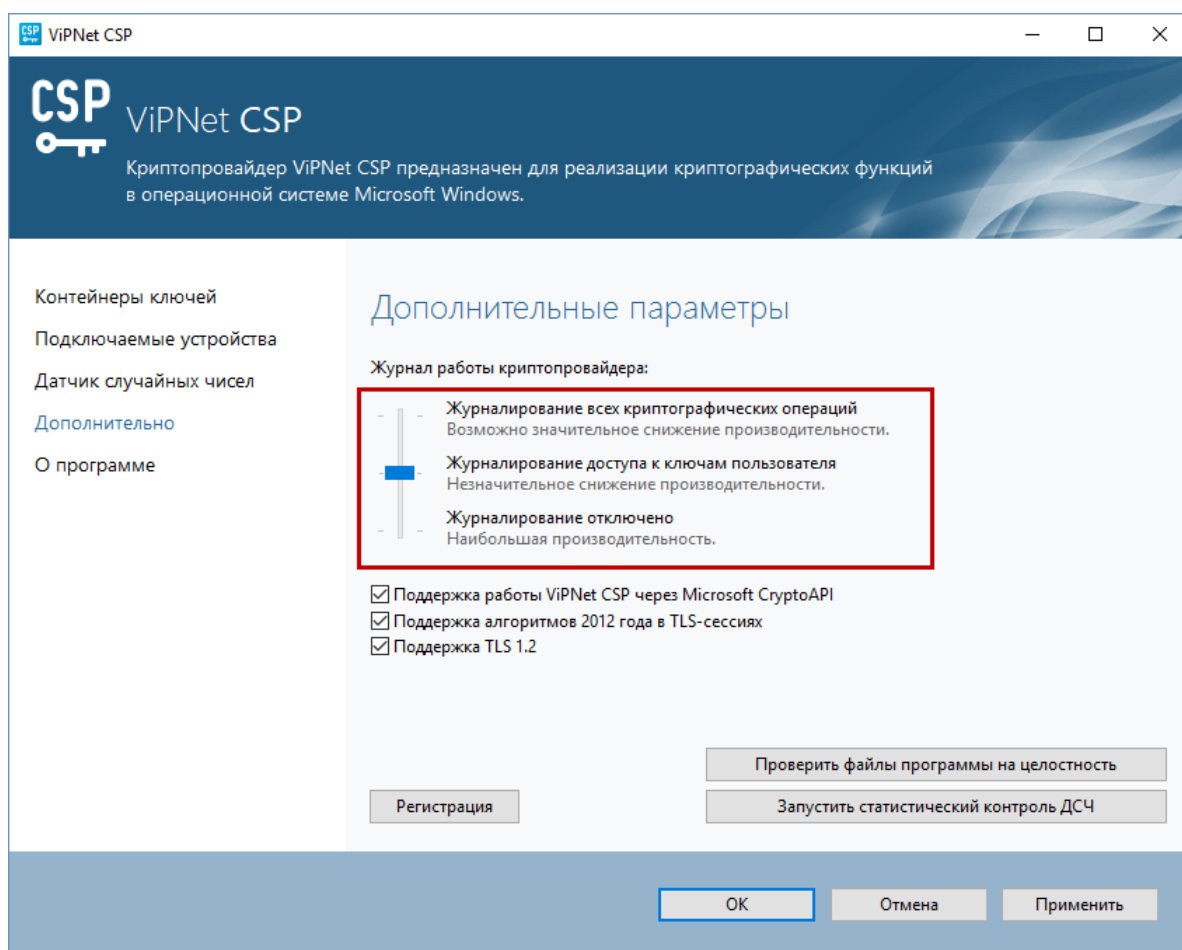


Рисунок 44. Задание режима ведения журнала

- 2 В области **Журнал работы криптопровайдера** переместите ползунок в одно из следующих положений:
 - **Журналирование отключено** — регистрация событий в журнале отключена.
 - **Журналирование доступа к ключам пользователя** — в журнал записываются только события, не связанные с долговременными операциями: обращения к ключам пользователя, подпись или проверка подписи хэш-сумм.

- **Журналирование всех криптографических операций** — в журнал все криптографические операции, в том числе связанные с долговременными операциями: хэшированием, шифрованием, расшифрованием, контролем целостности файлов. При выборе этого режима возможно значительное снижение производительности криптопровайдера из-за большого количества регистрируемых событий.

Регистрируемые события криптопровайдера вы можете [просматривать в системном журнале Windows](#).

Просмотр событий криптопровайдера в системном журнале

Если в ViPNet CSP включена регистрация событий криптопровайдера (см. [Настройка регистрации событий криптопровайдера](#)), вы можете следить за этими событиями с помощью системного журнала Windows:

- 1 Нажмите **Win+R**.
- 2 В поле **Открыть** введите `eventvwr` и нажмите **OK**.
- 3 В окне **Просмотр событий** на левой панели выберите **Журналы приложений и служб > ViPNet > BCRYPT > Audit** или **Журналы приложений и служб > ViPNet > CSP > Audit**.

В результате на правой панели отобразится список зарегистрированных событий.

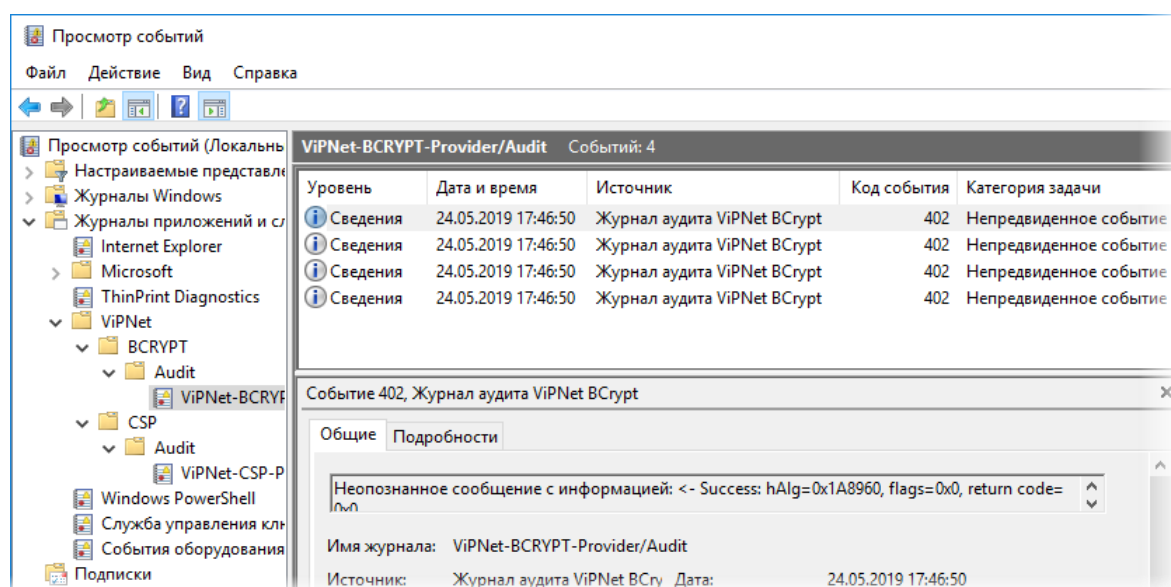


Рисунок 45. Просмотр событий ViPNet CSP

Включение аудита доступа к объектам

Для включения системного механизма аудита доступа к объектам для всех попыток доступа:

- 1 Нажмите **Win+R**.
- 2 В поле **Открыть** введите `mmc` и нажмите **ОК**.
- 3 В окне консоли на левой панели выберите **Политика «Локальный компьютер» > Конфигурация компьютера > Конфигурация Windows > Параметры безопасности > Локальные политики > Политика аудита**.
- 4 Двойным щелчком откройте свойства аудита доступа к объектам.

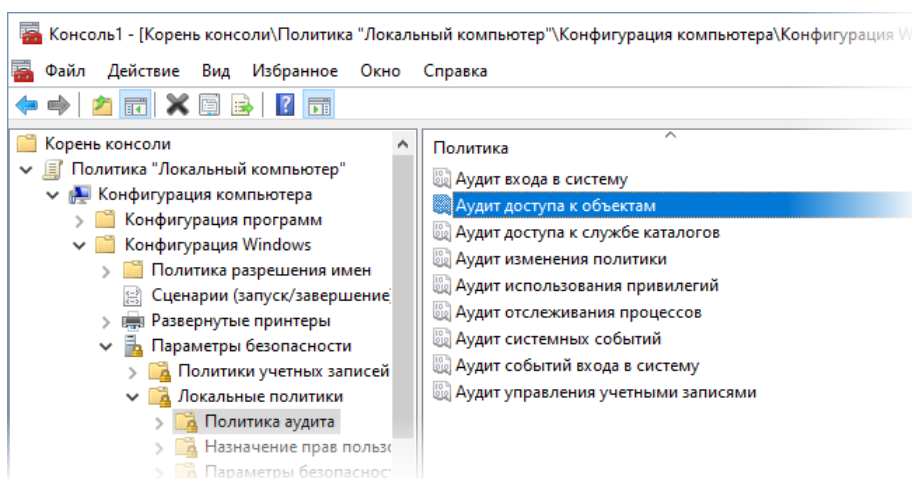


Рисунок 46. Включение системного механизма аудита доступа к объектам

- 5 В окне свойств установите флажки **Успех** и **Отказ**.
- 6 Нажмите **ОК**.

Добавление элементов аудита доступа к объектам

- 1 Нажмите **Win+R**.
- 2 В поле **Открыть** введите `eventvwr` и нажмите **OK**.
- 3 В окне консоли на левой панели выберите **Просмотр событий > Журналы приложений и служб > ViPNet > CSP > Audit > ViPNet-CSP-Provider > Audit**.

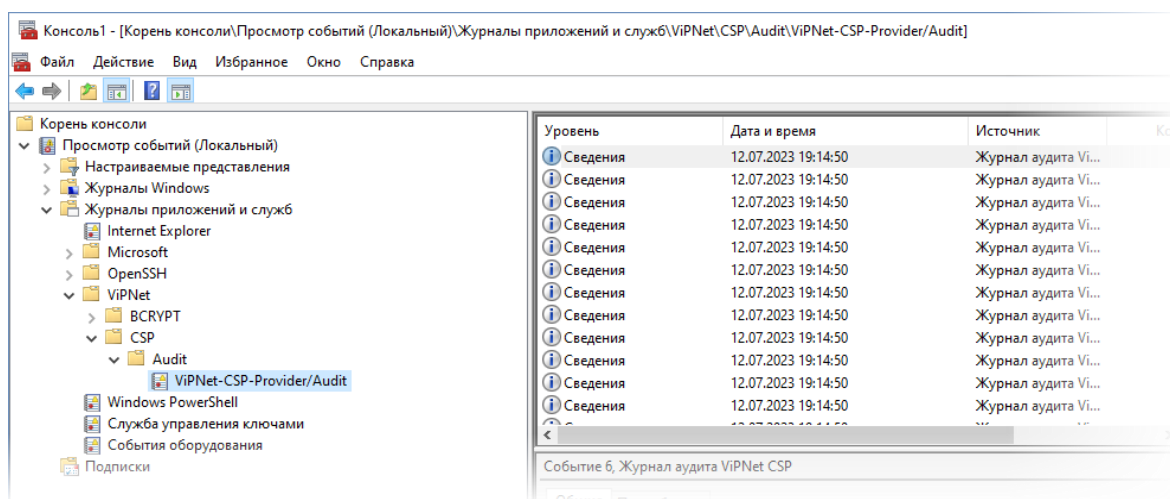


Рисунок 47. Журнал аудита ViPNet CSP

- 4 Нажатием правой клавиши мыши по файлу журнала вызовите контекстное меню и выберите **Свойства**.
- 5 Из поля **Путь журнала** скопируйте путь к файлу журнала и с его помощью найдите файл журнала в **Проводнике**.

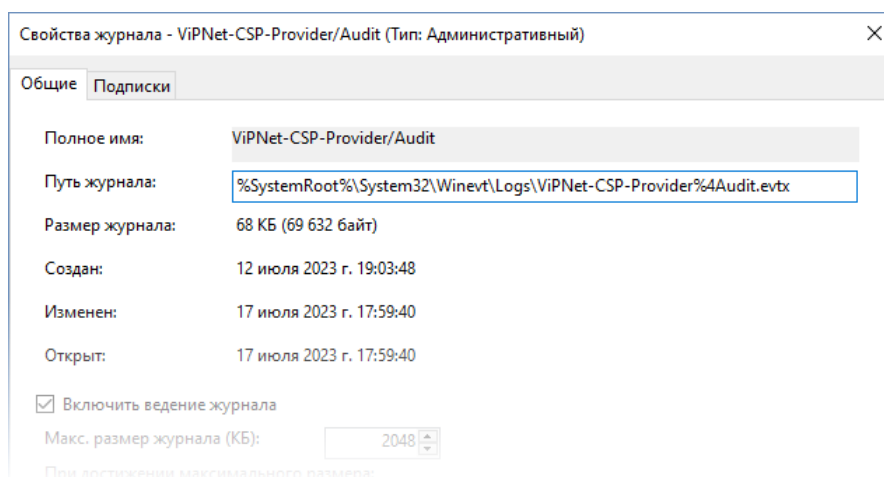


Рисунок 48. Путь к файлу журнала

- 6 Откройте свойства файла журнала (по умолчанию `ViPNet-CSP-Provider%4Audit.evtx`) и выберите **Безопасность** > **Дополнительно**.
- 7 В дополнительных параметрах безопасности откройте вкладку **Аудит** и нажмите **Добавить**.

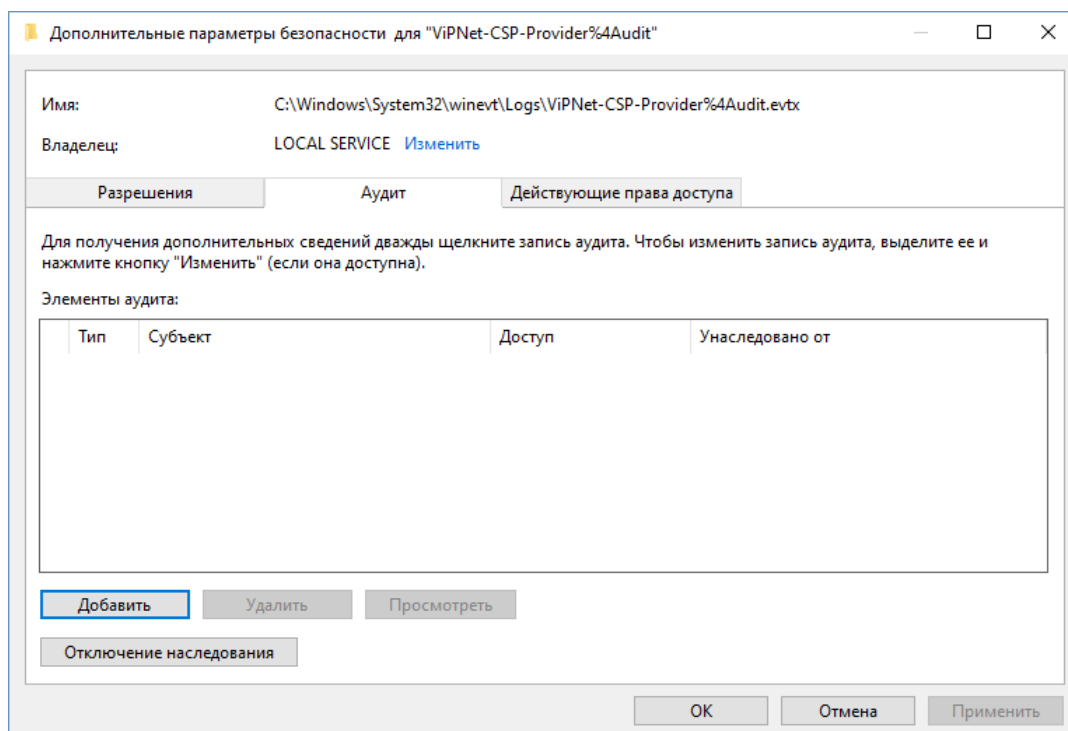


Рисунок 49. Дополнительные параметры безопасности журнала ViPNet CSP

- 8 Нажмите **Выберите субъект**.
- 9 В поле **Введите имена выбираемых объектов** укажите **Все** и нажмите **ОК**.
- 10 В списке **Тип** выберите **Все**.
- 11 В списке **Общие разрешения** выберите **Изменение**, **Чтение и выполнение**, **Чтение**, **Запись**.

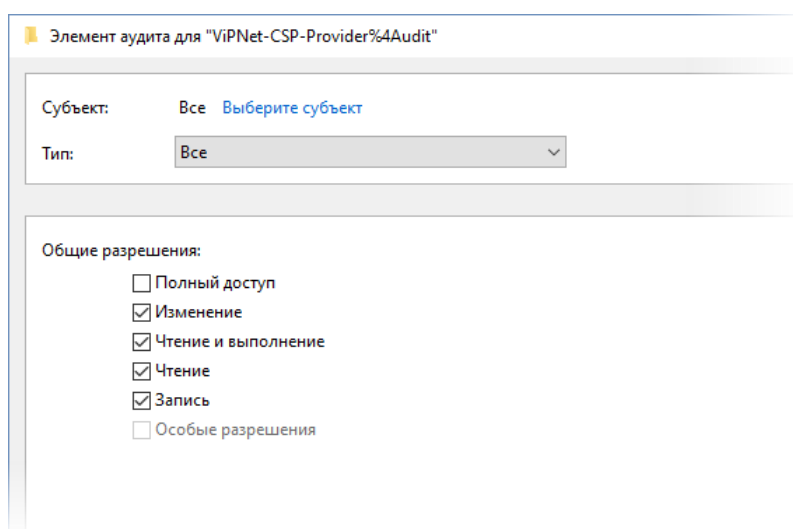


Рисунок 50. Добавление элемента аудита доступа к объектам

- 12 Нажмите **ОК**.

9

Использование функций криптопровайдера при разработке программ

Настройка проекта для использования функций ViPNet CSP	100
Криптографические библиотеки, входящие в состав ViPNet CSP	101

Настройка проекта для использования функций ViPNet CSP



Внимание! Для сборки проектов, использующих библиотеки ViPNet CSP, вам понадобится среда разработки Microsoft Visual Studio 2015 или более поздней версии.

ViPNet CSP версии 4.4 и более поздних версий не включает компонент ViPNet SoftToken. Для работы с ViPNet SoftToken необходимо установить ПО ViPNet OSSSL.

Вместе с ViPNet CSP распространяется комплект средств разработки (SDK), который представляет собой архив с заголовочными файлами ViPNet CSP и примерами программ.

Для использования функций ViPNet CSP в своем проекте:

- 1 Извлеките файлы из архива SDK в папку на вашем жестком диске.



Примечание. Далее путь к папке, в которую вы разархивировали файлы, будет обозначаться `C:\CSP_SDK`.

- 2 В настройках проекта укажите папки:

- o `C:\CSP_SDK\headers\cspsdk` — для поиска заголовочных файлов криптоинтерфейса ViPNet CSP;
- o `C:\CSP_SDK\headers\pkcs11` — для поиска заголовочных файлов криптоинтерфейса PKCS#11 (работа с внешними устройствами);
- o рабочая папка Microsoft Windows SDK — для системных заголовочных файлов.

- 3 В исходный код проекта включите заголовочный файл `wincrypt.h`:

```
#include <wincrypt.h>
```

- 4 Чтобы использовать параметры, специфичные для ViPNet CSP, включите заголовочный файл `importitccsp.h`:

```
#include <importitccsp.h>
```

В результате вы сможете использовать в своем проекте функции, описанные в документе «Криптографический интерфейс ViPNet CSP 4.4. Руководство разработчика».

Криптографические библиотеки, входящие в состав ViPNet CSP

После установки ViPNet CSP криптографические библиотеки будут размещены в папке:

- C:\Program Files\InfoTeCS\ViPNet CSP — для 32-разрядных версий Windows;
- C:\Program Files (x86)\InfoTeCS\ViPNet CSP — для 64-разрядных версий Windows.

Описание используемых криптографических библиотек приведено в документе «Криптографический интерфейс ViPNet CSP 4.4. Руководство разработчика».

10

Интеграция ViPNet CSP с центром сертификации на базе Microsoft CA

Порядок действий	103
Развертывание центра сертификации Microsoft CA	104

Порядок действий

Вы можете использовать удостоверяющий центр Microsoft (центр сертификации Microsoft CA) для выполнения криптографических функций в соответствии с алгоритмами ГОСТ. Для этого необходимо при развертывании центра сертификации задать в качестве поставщика криптографических функций ViPNet CSP.

Вы можете развернуть центр сертификации Microsoft CA на любом сервере, работающем под управлением одной из [поддерживаемых операционных систем Windows Server](#). В приведенном ниже примере предполагается, что для развертывания выделен сервер с операционной системой Microsoft Windows Server 2012, который подключен к локальной сети.

Для интеграции ViPNet CSP с центром сертификации Microsoft CA выполните следующие действия:

- 1 Установите и зарегистрируйте ViPNet CSP (см. [Установка и запуск программы](#)).
- 2 Разверните центр сертификации, добавив на сервер центра соответствующую роль (см. [Развертывание центра сертификации Microsoft CA](#)).

Развертывание центра сертификации Microsoft CA

Чтобы развернуть на сервере с ОС Windows Server 2012 центр сертификации, взаимодействующий с криптопровайдером ViPNet CSP, на сервер требуется установить специальную роль «Службы сертификации Active Directory». В процессе установки роли будет сформирована пара ключей и издан сертификат центра сертификации.

Для развертывания и настройки центра сертификации Microsoft CA:

- 1 На панели управления Windows в категории **Администрирование** запустите консоль **Диспетчер серверов**.
- 2 В меню **Управление консолью Диспетчер серверов** выберите **Добавить роли и компоненты**.
- 3 Следуйте указаниям мастера, при этом на странице **Выбор ролей сервера** выберите **Службы сертификатов Active Directory**, и в окне **Мастер добавления ролей и компонентов** нажмите **Добавить компоненты**.
- 4 На странице **Выбор служб ролей** выберите **Служба регистрации в центре сертификации через Интернет**.
- 5 В меню **Уведомления консоли Диспетчер серверов** в пункте **Конфигурация после развертывания** нажмите **Настроить службы сертификатов Active Directory**.

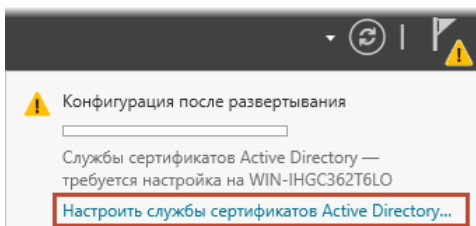


Рисунок 51. Настройка службы сертификатов Active Directory

- 6 В окне **Конфигурация службы сертификатов Active Directory**:
 - 6.1 На странице **Службы ролей** выберите **Центр сертификации**.
 - 6.2 На странице **Вариант установки** выберите один из следующих вариантов: **Автономный ЦС** или **ЦС предприятия**.
 - 6.3 На странице **Тип ЦС** задайте нужный тип центра сертификации и нажмите **Далее**.
 - 6.4 На странице **Закрытый ключ** выберите **Создать новый закрытый ключ** и нажмите **Далее**.
 - 6.5 На странице **Шифрование для ЦС** выполните следующие действия:
 - В качестве поставщика служб шифрования в соответствующем списке выберите поставщик **Infotecs Cryptographic Service Provider**.
 - Выберите **Разрешить взаимодействие с администратором, если ЦС обращается к закрытому ключу**.

Нажмите **Далее**.

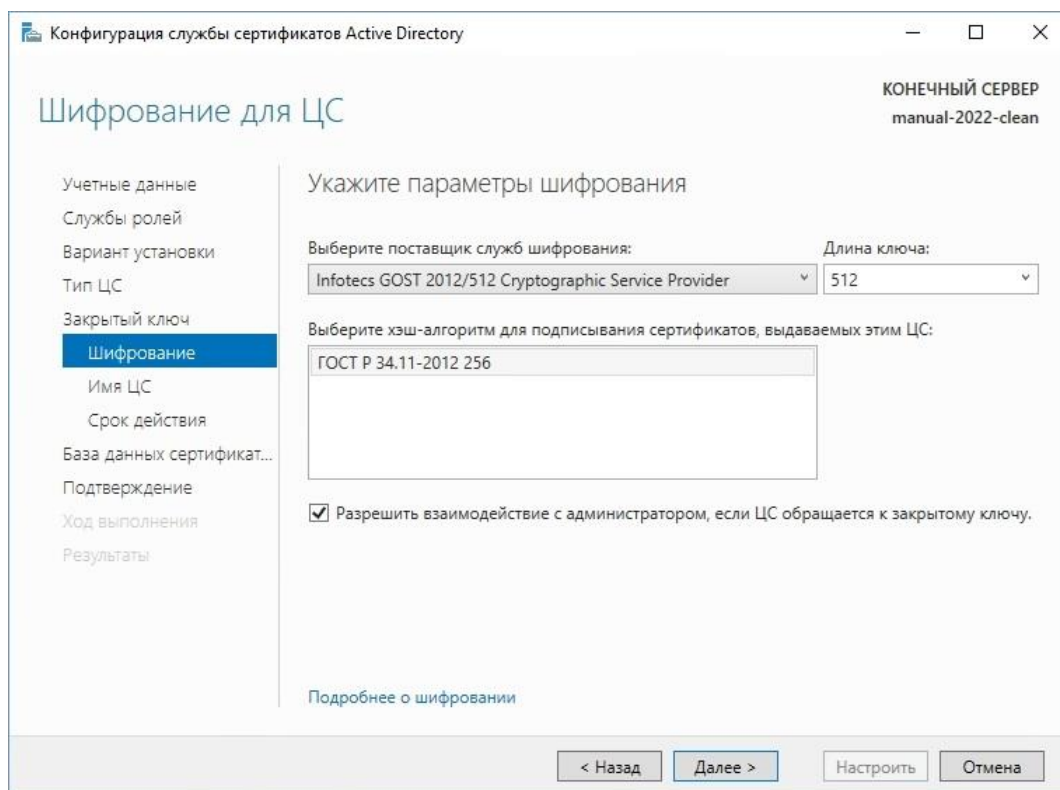


Рисунок 52. Выбор криптопровайдера при настройке удостоверяющего центра

- 7 На странице **Подтверждение** нажмите **Настроить**. При этом криптопровайдер ViPNet CSP начнет создание контейнера ключей с корневым сертификатом центра сертификации.
- 8 На странице **Результаты** нажмите **Заккрыть**.

11

Электронная подпись в документах Microsoft Office

Электронная подпись	107
Подписание документов Microsoft Word, Excel и PowerPoint	108
Просмотр электронной подписи в Microsoft Word, Excel и PowerPoint	111
Удаление электронной подписи в Microsoft Word, Excel и PowerPoint	114
Видимая строка подписи в документах Microsoft Word и Excel	115

Электронная подпись

Электронная подпись — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием ключа электронной подписи.

Электронная подпись позволяет:

- удостоверить личность лица, подписавшего документ (подлинность);
- подтвердить, что документ не был изменен после подписания (целостность);
- подтвердить авторство документа (неотрекаемость).

Таким образом, электронная подпись может использоваться физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью. Условия использования электронной подписи, особенности ее использования в сферах государственного управления и в корпоративной информационной системе регламентируются [Законом РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»](#).

Подписание документов Microsoft Word, Excel и PowerPoint

В данном разделе содержится информация о том, как добавить электронную подпись в документы Microsoft Word, Excel и PowerPoint в случаях использования различных версий Microsoft Office.

Microsoft Office 2010

Чтобы добавить электронную подпись в документ Microsoft Word, Excel и PowerPoint:

- 1 Сохраните документ.
- 2 Откройте вкладку **Файл** и выберите раздел **Сведения**.
- 3 В группе **Разрешения** нажмите **Защитить документ**, **Защитить книгу** или **Защитить презентацию**, затем выберите **Добавить цифровую подпись**.



Примечание. Если документ не был предварительно сохранен, появится сообщение с предложением сохранить его перед добавлением подписи. В окне сообщения нажмите **Да**.

- 4 В окне **Подписание** заполните поле **Цель подписания документа**. Ниже в этом же окне приведены краткие сведения о сертификате, которым предполагается подписать документ. При необходимости нажмите **Изменить** и выберите другой сертификат.

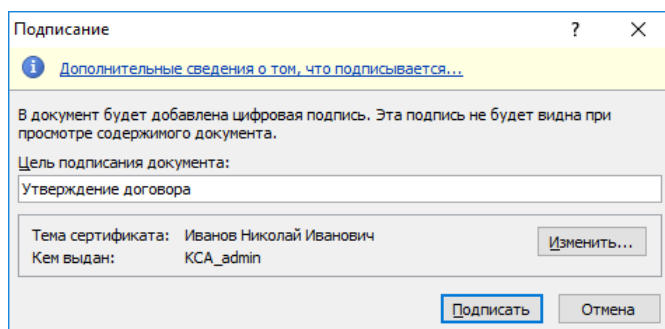


Рисунок 53. Добавление электронной подписи

- 5 Выбрав сертификат, нажмите **Подписать**.
- 6 В окне **ViPNet CSP – пароль контейнера ключей** введите пароль и нажмите **ОК**.

В разделе **Сведения** будет отображена информация о том, что документ помечен как окончательный.

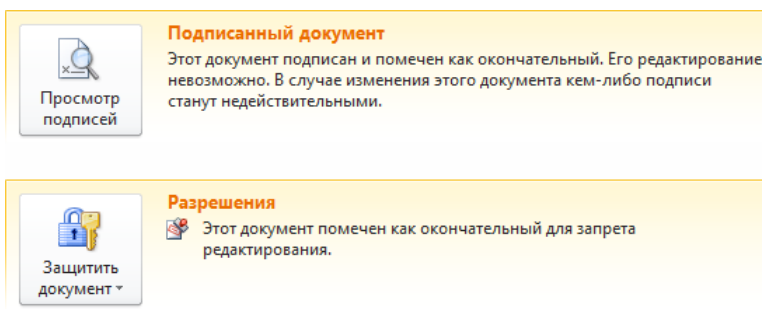


Рисунок 54. Информация о том, что документ помечен как окончательный

В строке состояния документа появится значок , обозначающий, что документ содержит электронную подпись.



Совет. Возможность внесения правок в подписанный документ заблокирована. Если необходимо внести правки, сначала удалите электронную подпись (см. [Удаление электронной подписи в Microsoft Word, Excel и PowerPoint](#)).

Microsoft Office 2013

Чтобы добавить электронную подпись в документ Microsoft Word, Excel и PowerPoint:

- 1 Сохраните документ.
- 2 Откройте вкладку **Файл** и выберите раздел **Сведения**.
- 3 Нажмите **Защита документа**, **Защита книги** или **Защита презентации** в одноименной группе и выберите команду **Добавить цифровую подпись**.



Примечание. Если документ не был предварительно сохранен, появится сообщение с предложением сохранить его перед добавлением подписи. В окне сообщения нажмите **Да**.

- 4 В окне **Подписание** вы можете:
 - в списке **Тип подтверждения** выбрать одну из заданных причин подписания документа;
 - в поле **Цель подписания документа** указать цель подписания документа.

Ниже в этом же окне приведены краткие сведения о сертификате, которым предполагается подписать документ. При необходимости добавьте дополнительные сведения или нажмите **Изменить**, чтобы выбрать другой сертификат.

Рисунок 55. Добавление электронной подписи

5 Выбрав сертификат, нажмите **Подписать**.

6 В окне **ViPNet CSP – пароль контейнера ключей** введите пароль и нажмите **ОК**.

В разделе **Сведения** будет отображена информация о том, что документ помечен как окончательный.

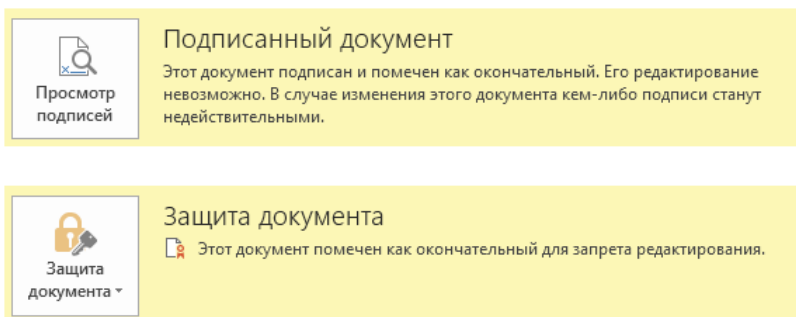


Рисунок 56. Информация о том, что документ помечен как окончательный

В строке состояния документа появится значок , обозначающий, что документ содержит электронную подпись.



Совет. Возможность внесения правок в подписанный документ заблокирована. Если необходимо внести правки, сначала удалите электронную подпись (см. [Удаление электронной подписи в Microsoft Word, Excel и PowerPoint](#)).

Просмотр электронной подписи в Microsoft Word, Excel и PowerPoint

Microsoft Office 2010

Для просмотра электронной подписи в документе Microsoft Word, Excel или PowerPoint:

- 1 Откройте вкладку **Файл** и в разделе **Сведения** нажмите **Просмотр подписей**.

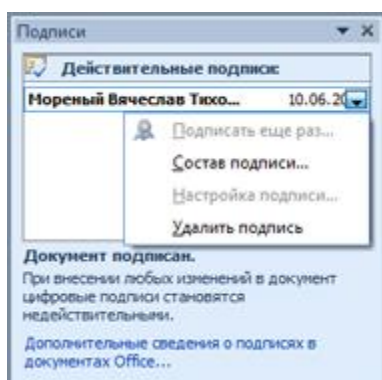


Рисунок 57. Панель «Подписи»



Примечание. Вы также можете вызвать панель **Подписи**, щелкнув в строке состояния значок электронной подписи .

- 2 На панели **Подписи** щелкните правой кнопкой мыши строку подписи (либо нажмите кнопку вызова меню справа). В меню выберите **Состав подписи**.
- 3 В окне **Состав подписи** содержатся краткие сведения о подписи и сертификате. В нем вы можете:
 - нажать **Просмотр**, чтобы открыть сертификат;
 - нажать **Дополнительные сведения, которые будут включены в подпись**, чтобы просмотреть дополнительные сведения о подписи.

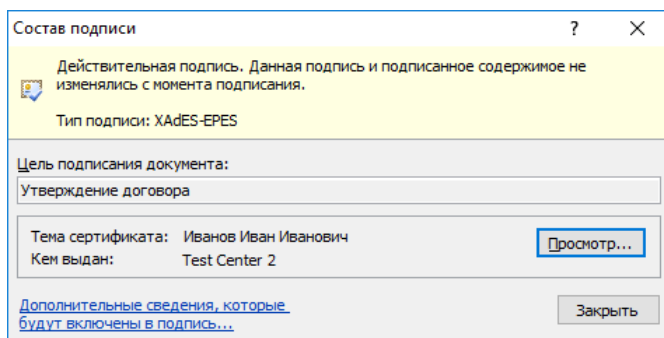


Рисунок 58. Состав подписи



Примечание. Если при проверке сертификата возникли ошибки, сообщение об этом будет выведено под заголовком окна.

Microsoft Office 2013

Для просмотра электронной подписи в документе Microsoft Word, Excel или PowerPoint:

- 1 Сохраните документ.
- 2 Откройте вкладку **Файл** и в разделе **Сведения** нажмите **Просмотр подписей**.

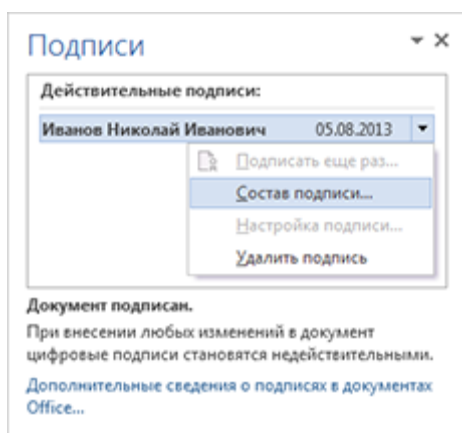


Рисунок 59. Панель «Подписи»



Примечание. Вы также можете вызвать панель **Подписи**, щелкнув в строке состояния значок электронной подписи .

- 3 На панели **Подписи** щелкните правой кнопкой мыши строку подписи (или нажмите кнопку вызова меню справа). В меню выберите **Состав подписи**.
- 4 В окне **Состав подписи** содержатся краткие сведения о подписи и сертификате. В нем вы можете:
 - нажать **Просмотр**, чтобы открыть сертификат;

- нажать **Дополнительные сведения, которые будут включены в подпись**, чтобы просмотреть дополнительные сведения о подписи;
- нажать **Просмотр сведений о подписавшем**, чтобы получить информацию о владельце сертификата.

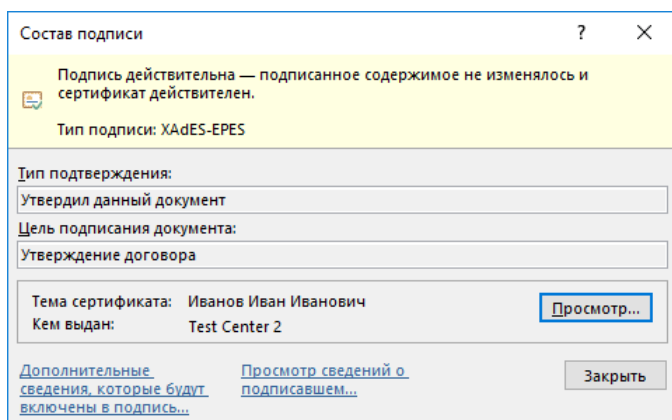


Рисунок 60. Состав подписи



Примечание. Если при проверке сертификата возникли ошибки, сообщение об этом будет выведено под заголовком окна.

Удаление электронной подписи в Microsoft Word, Excel и PowerPoint

Microsoft Office 2010

Чтобы удалить электронную подпись из документа Microsoft Word, Excel или PowerPoint:

- 1 Откройте вкладку **Файл** и в разделе **Сведения** нажмите **Просмотр подписей**.



Примечание. Вы можете также вызвать панель **Подписи**, щелкнув в строке состояния документа значок электронной подписи .

- 2 На панели **Подписи** щелкните правой кнопкой мыши строку подписи (либо нажмите кнопку вызова меню справа), в меню выберите **Удалить подпись**.
- 3 В окне подтверждения нажмите **Да**.

Microsoft Office 2013

Чтобы удалить электронную подпись из документа Microsoft Word, Excel или PowerPoint:

- 1 Откройте вкладку **Файл** и в разделе **Сведения** нажмите **Просмотр подписей**.



Примечание. Вы можете также вызвать панель **Подписи**, щелкнув в строке состояния документа значок электронной подписи .

- 2 На панели **Подписи** щелкните правой кнопкой мыши строку подписи (либо нажмите кнопку вызова меню справа), в меню выберите **Удалить подпись**.
- 3 В окне подтверждения нажмите **Да**.

Видимая строка подписи в документах Microsoft Word и Excel

Приложения Microsoft Word и Microsoft Excel позволяют вставить в документ одну или несколько видимых строк подписи. Такая строка выглядит как место для подписи в бумажном документе и одновременно с видимым представлением подписи в документе добавляет электронную подпись для удостоверения личности подписавшего.

Вставка видимой строки подписи

Чтобы добавить в документ видимую строку для подписи:

- 1 Поместите курсор в то место документа, куда требуется вставить строку подписи.
- 2 На вкладке **Вставка** в группе **Текст** нажмите **Строка подписи**.
- 3 В окне **Настройка подписи** заполните поля **Предложенный подписывающий**, **Должность предложенного подписывающего**, **Адрес электронной почты предложенного подписывающего**. Вы можете ввести краткие инструкции для подписывающего, а также разрешить подписывающему добавлять примечания в окне подписи и включить отображение даты подписи (установив соответствующие флажки).

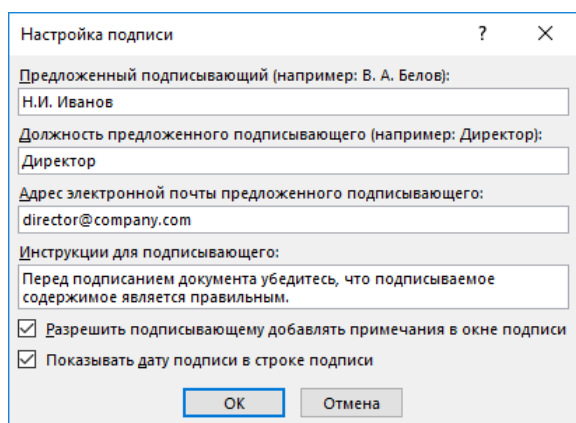


Рисунок 61. Окно «Настройка подписи»

- 4 Выполнив настройку подписи, нажмите **ОК**. В документ будет вставлена пустая строка для подписи, которая также будет отображаться на панели **Подписи**.



Рисунок 62. Видимая строка подписи и ее представление на панели «Подписи» в Microsoft Word 2013



Примечание. После подписания документа вы сможете просмотреть свойства подписи в окне **Настройки подписи**, но внесение изменений будет невозможно.

Добавление электронной подписи в строку подписи

В приложениях Microsoft Word и Excel вы можете подписать документ, используя видимую строку подписи.

Чтобы добавить электронную подпись в строку подписи:

- 1 Щелкните правой кнопкой мыши строку подписи и в контекстном меню выберите **Подписать**.
- 2 В окне **Подписание** введите свое имя либо нажмите **Выбрать рисунок**, чтобы вставить графическое изображение подписи. Ниже дано краткое описание сертификата, которым предполагается подписать документ. Чтобы подписать документ другим сертификатом, нажмите **Изменить** и выберите сертификат.

В программе Microsoft Word или Excel версии 2013 в данном окне вы можете также:

- выбрать одну из заданных причин подписания документа в списке **Тип подтверждения**;
- указать цель подписания документа в поле **Цель подписания документа**;
- добавить дополнительные сведения о подписавшем, нажав **Сведения**.

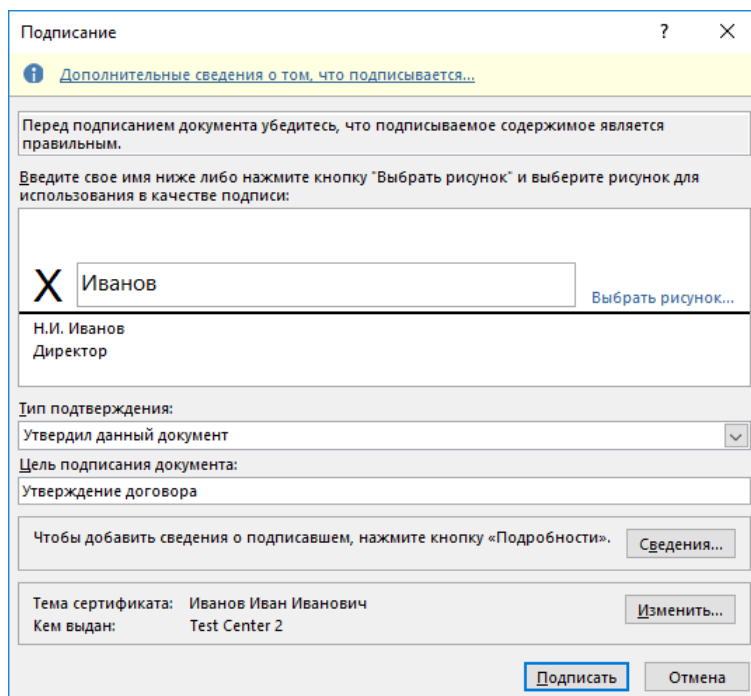


Рисунок 63. Подписание строки подписи в приложениях Microsoft Office 2013

- 3 После ввода имени и выбора сертификата нажмите **Подписать**.
- 4 В окне ViPNet CSP – пароль контейнера ключей введите пароль и нажмите **ОК**. В строке подписи появится имя подписавшего или графическое изображение его подписи.

Если по каким-либо причинам не удалось проверить надежность сертификата подписи, над строкой подписи будет стоять пометка **Недействительная подпись**.

 **Недействительная подпись** 18.10.2016

 **А. Иванов**
 А. В. Иванов
 Директор

Рисунок 64. Недействительная подпись



Примечание. Строку с недействительной подписью можно подписать еще раз. Для этого щелкните правой кнопкой мыши строку подписи (или название подписи на панели **Подписи**) и выберите **Подписать еще раз**.

Просмотреть состав подписи или **удалить подпись** из видимой строки подписи можно так же, как в случае невидимой подписи.

12

Электронная подпись и шифрование в Microsoft Outlook

Шифрование и подписание документов	119
Порядок организации обмена защищенными сообщениями	121
Обмен сертификатами с получателем сообщения	122
Настройка дополнительных параметров электронной подписи и шифрования	124
Добавление электронной подписи к отдельному сообщению	126
Добавление электронной подписи ко всем сообщениям	128
Просмотр электронной подписи сообщения	130
Шифрование сообщений электронной почты	131
Шифрование документов и файлов	133
Просмотр зашифрованных сообщений	134

Шифрование и подписание документов

Для шифрования и проверки электронной подписи криптопровайдер ViPNet CSP использует открытый ключ, находящийся в [сертификате](#) того пользователя, которому адресован зашифрованный документ или от которого поступил документ с электронной подписью.

Для расшифрования и формирования электронной подписи криптопровайдер применяет закрытый ключ пользователя, который расшифровывает или подписывает документ. Ключ указывает сам пользователь.

На рисунке ниже представлена схема защищенного обмена документами на примере передачи конфиденциального сообщения электронной почты.

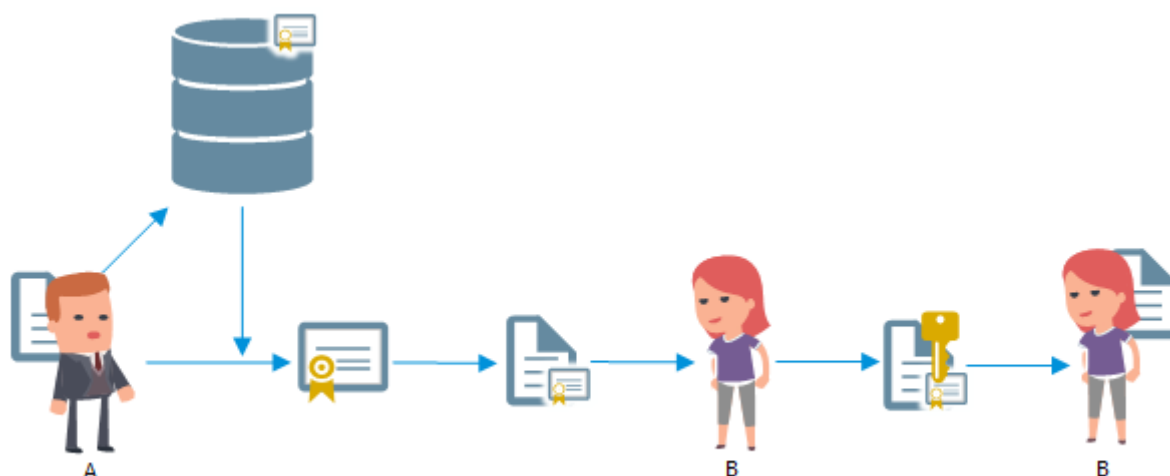


Рисунок 65. Обмен защищенными документами

Пользователю **A** необходимо передать пользователю **B** конфиденциальное сообщение электронной почты. Для этого пользователи выполняют следующие действия:

- 1 Пользователь **A** запрашивает из сетевого хранилища сертификат открытого ключа пользователя **B** и сопоставляет его с контактом **B** в своей почтовой программе.
- 2 Пользователь **A** зашифровывает документ с использованием открытого ключа из сертификата пользователя **B**.
- 3 Пользователь **A** отправляет пользователю **B** зашифрованное сообщение.
- 4 Пользователь **B** расшифровывает документ с помощью своего закрытого ключа.

Таким образом, пользователь **B** получает конфиденциальное сообщение от пользователя **A**.

Если сообщение перехватит злоумышленник, ему не удастся прочитать письмо, поскольку у него нет закрытого ключа пользователя **B**.

Если пользователь **В** не сможет расшифровать сообщение, пришедшее от пользователя **А**, то сообщение было изменено сторонними лицами или повреждено в процессе пересылки. В этом случае пользователь **В** может запросить у пользователя **А** повторную отправку сообщения.

Процесс формирования и проверки электронной подписи представлен ниже.

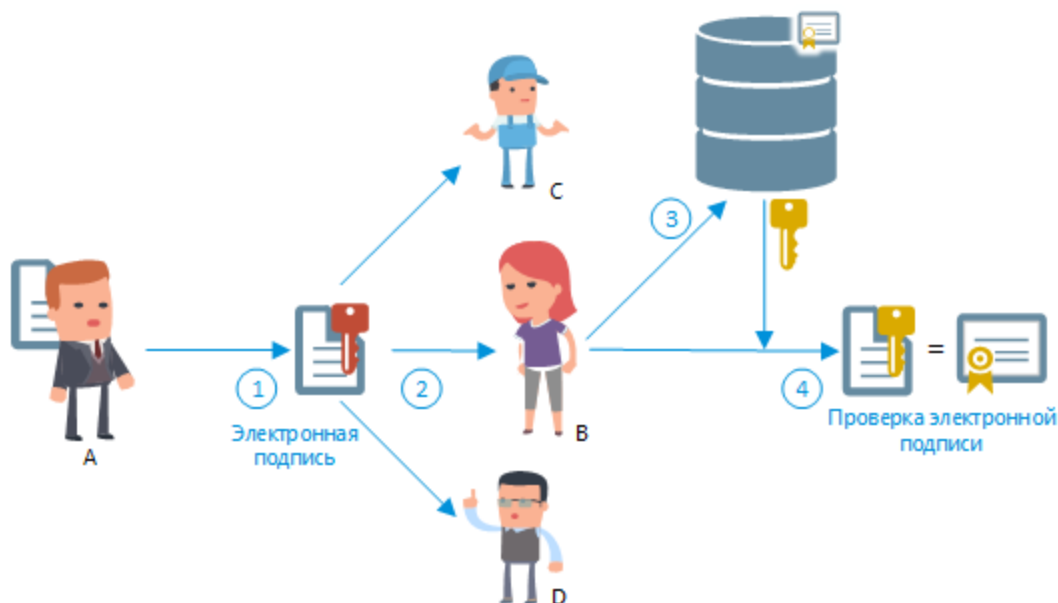


Рисунок 66. Процесс формирования и проверки электронной подписи

Пользователю **А** необходимо заверить документ (например, сообщение электронной почты) электронной подписью, чтобы остальные пользователи не смогли внести в него изменения и каждый мог удостовериться, что автор данного документа — пользователь **А**. Для этого:

- 1 Пользователь **А** подписывает документ своим закрытым ключом.
- 2 Пользователь **А** отправляет документ всем заинтересованным лицам (пользователи **В**, **С** и **Д**) или выкладывает для общего доступа.
- 3 Пользователь **В** запрашивает сертификат открытого ключа пользователя **А** в сетевом хранилище, где хранятся сертификаты, изданные удостоверяющим центром.
- 4 Пользователь **В** проверяет электронную подпись документа с помощью открытого ключа пользователя **А**, который находится в сертификате пользователя **А**.

Если проверка прошла успешно, то автор документа — пользователь **А** и документ не подвергался изменениям с момента подписания.

Если проверка показала несоответствие электронной подписи и открытого ключа в сертификате отправителя, то документ либо не принадлежит пользователю **А**, либо редактировался сторонними лицами, либо был поврежден в процессе пересылки. В этом случае пользователь **В** может запросить у пользователя **А** документ повторно.

Порядок организации обмена защищенными сообщениями

Чтобы организовать обмен защищенными сообщениями с помощью ViPNet CSP и почтовой программы Microsoft Office Outlook (2010 или 2013):

- 1 Установите контейнер ключей и сертификат в ViPNet CSP, а также сертификат издателя и список аннулированных сертификатов.
- 2 Обменяйтесь сертификатами с получателем (отправителем) сообщения.
- 3 При необходимости настройте почтовую программу для работы с цифровой подписью и зашифрованными сообщениями.
- 4 В зависимости от того, являетесь ли вы отправителем или получателем зашифрованного сообщения:
 - Подпишите сообщение электронной подписью,.
 - Создайте и отправьте зашифрованное сообщение (см. [Шифрование сообщений электронной почты](#)).
 - Расшифруйте полученное сообщение (см. [Просмотр зашифрованных сообщений](#)).



Внимание! Чтобы получить возможность подписания сообщений электронной почты, создайте запрос и получите сертификат электронной подписи (см. [Получение закрытого ключа и сертификата](#)).

Кроме обмена зашифрованными сообщениями электронной почты, с помощью программы Microsoft Outlook можно шифровать документы и файлы (см. [Шифрование документов и файлов](#)).

Обмен сертификатами с получателем сообщения

Чтобы зашифровать сообщение электронной почты для определенного получателя, вам необходим сертификат этого получателя. Обмен сертификатами может быть произведен одним из следующих способов:

- Путем отправки сообщения с электронной подписью (см. [Добавление электронной подписи к отдельному сообщению](#)). Добавляя имя отправителя в контакты, получатель тем самым добавляет сертификат отправителя.
- Путем отправки файла сертификата (с расширением `.cer`) получателю в сообщении электронной почты, на внешнем носителе или размещения его в общедоступном сетевом хранилище. Это дает возможность получателю импортировать CER-файл в контакт.
- Путем создания контакта с CER-файлом и его отправка.



Внимание! Сертификат получателя и ваш сертификат должны содержать адреса электронной почты своих владельцев.

Чтобы импортировать сертификат в карточку контактов, в программе Microsoft Outlook:

- 1 Откройте представление **Контакты** (в Microsoft Outlook 2013 — представление **Люди**).
- 2 Двойным щелчком откройте нужный контакт.
- 3 Откройте окно управления сертификатами пользователя одним из способов:
 - В программе Microsoft Outlook 2010 выберите **Контакт** > **Показать** и нажмите **Сертификаты** .
 - В программе Microsoft Outlook 2013 выберите **Контакт** > **Показ** и нажмите **Сертификаты** .
- 4 Нажмите **Импорт**.
- 5 В окне **Поиск сертификата** укажите путь к файлу сертификата и нажмите **Открыть**.
Выбранный сертификат будет добавлен к данному контакту.



Внимание! Если после импорта сертификата появилось сообщение о том, что [адрес электронной почты из сертификата не найден в списке](#), то зашифровать письмо с помощью данного сертификата не удастся.

- 6 Чтобы убедиться, что добавленный сертификат является доверенным, выберите его и нажмите **Свойства**.

Если в окне **Свойства сертификата** на вкладке **Общие** отображается значок  или , то сертификат не является доверенным.

- 7 Если сертификат не является доверенным, в окне **Свойства сертификата** откройте вкладку **Доверие** и в разделе **Изменение правил доверия** выберите **Явно доверять этому сертификату**. Нажмите **ОК**.

Чтобы отправить карточку контакта с сертификатом:

- 1 В программе Microsoft Outlook создайте новый контакт и заполните карточку своими данными.
- 2 Импортируйте в контакт ваш сертификат.
- 3 В контекстном меню контакта выберите **Переслать контакт > Как контакт Outlook**.
- 4 В окне письма укажите адрес получателя, добавьте сопроводительный текст и нажмите **Отправить**.

После того как вы обменялись сертификатами с получателем, можно приступать к отправке зашифрованных сообщений.

Настройка дополнительных параметров электронной подписи и шифрования

Для выбора сертификатов подписи и шифрования, формата криптографии и настройки других параметров:

- 1 В MS Outlook выберите **Файлы > Параметры > Центр управления безопасностью > Параметры центра управления безопасностью > Защита электронных писем > Параметры**.
- 2 Убедитесь, что в списке **Формат криптографии** выбрано значение **S/MIME**.
- 3 Нажмите **Выбрать** напротив поля **Сертификат подписи** и укажите нужный сертификат.

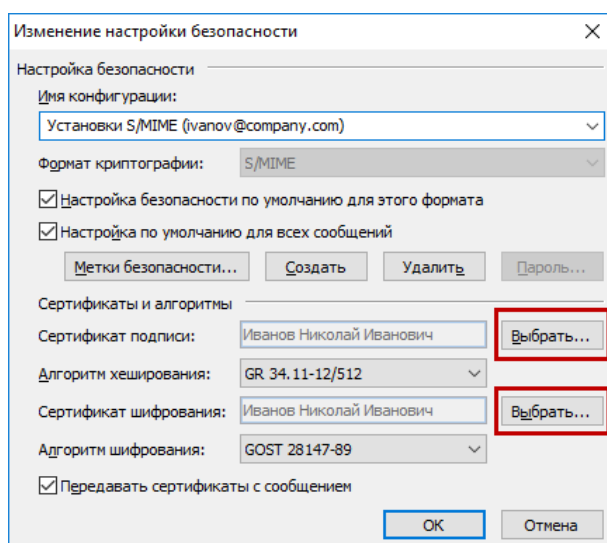


Рисунок 67. Выбор сертификатов для подписи и шифрования

- 4 Нажмите **Выбрать** напротив поля **Сертификат шифрования** и укажите нужный сертификат.



Внимание! Если выбранный для создания электронной подписи сертификат не содержит адреса электронной почты или адрес не совпадает с адресом отправки сообщения электронной почты, Microsoft Outlook не позволит выбрать данный сертификат в качестве сертификата электронной подписи.

Если выбранный сертификат не содержит электронного адреса отправки сообщения, возможны следующие сценарии:

- В хранилище операционной системы имеется другой сертификат с адресом электронной почты, который совпадает с адресом отправки сообщения электронной почты. При подписании сообщения электронной почты электронная подпись будет создана с помощью этого сертификата, а не указанного ранее.

- В хранилище операционной системы нет других сертификатов с адресом электронной почты, который бы совпадал с адресом отправки сообщения. При попытке подписания сообщения электронная подпись добавлена не будет.

Чтобы получить возможность подписания сообщений электронной почты сертификатом, создайте запрос на новый сертификат, укажите в нем корректный адрес электронной почты и передайте запрос администратору вашего удостоверяющего центра.

- 5 Если требуется, настройте остальные параметры и нажмите **ОК**.

Добавление электронной подписи к отдельному сообщению



Внимание! Чтобы получить возможность подписания сообщений электронной почты, создайте запрос и получите сертификат электронной подписи (см. [Получение закрытого ключа и сертификата](#)).

Чтобы подписать отдельное сообщение электронной подписью:

- 1 Создайте новое сообщение.
- 2 Выберите **Параметры > Разрешение:**
 - в Microsoft Outlook 2010 нажмите **Подписать**
 - в Microsoft Outlook 2013 нажмите **Подписать**



Примечание. Кнопка **Сообщение с цифровой подписью** или **Подписать** может отсутствовать на панели инструментов, если предварительно в окне **Изменение настроек безопасности** не был выбран сертификат электронной подписи, используемый по умолчанию (см. [Добавление электронной подписи ко всем сообщениям](#)).

- 3 Если на панели инструментов нет кнопки **Сообщение с цифровой подписью** (или **Подписать** , **Подписать**):
 - 3.1 В Microsoft Outlook выберите **Параметры > Дополнительные параметры** и нажмите **Свойства** . В окне **Свойства** нажмите **Параметры безопасности**.

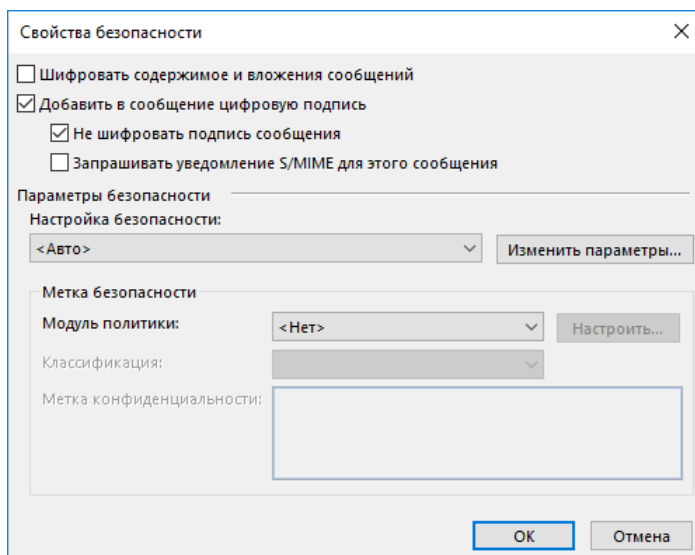


Рисунок 68. Окно «Свойства безопасности»

- 3.2 Выберите **Добавить в сообщение цифровую подпись**.
- 3.3 По умолчанию в списке **Настройка безопасности** установлено значение **<Авто>**. Это значит, что сертификат электронной подписи будет выбран автоматически. Чтобы выбрать сертификат самостоятельно, нажмите **Изменить параметры** (см. [Настройка дополнительных параметров электронной подписи и шифрования](#)).
- 3.4 Чтобы сохранить настройки, нажмите **ОК**.
- 4 Введите текст сообщения, укажите тему и адресата. Если требуется, добавьте вложения.
- 5 Нажмите **Отправить**. Откроется окно **ViPNet CSP – пароль контейнера ключей**.
- 6 Введите пароль и нажмите **ОК**.



Примечание. В некоторых случаях может потребоваться ввести пароль несколько раз.

Добавление электронной подписи ко всем сообщениям



Внимание! Чтобы получить возможность подписания сообщений электронной почты, создайте запрос и получите сертификат электронной подписи (см. [Получение закрытого ключа и сертификата](#)).

Microsoft Outlook позволяет добавлять в сообщения электронной почты электронную подпись, чтобы гарантировать подлинность и целостность сообщения, а также обеспечить неотрекаемость. Чтобы обеспечить конфиденциальность сообщения, его нужно зашифровать (см. [Шифрование сообщений электронной почты](#)).



Примечание. Более подробные сведения о защите электронной почты средствами криптографии можно получить на веб-узле [Office Online](#).

Чтобы добавить электронную подпись ко всем сообщениям:

- 1 Откройте окно управления безопасностью электронной почты:
 - Откройте вкладку **Файл** > **Параметры** > **Центр управления безопасностью** и нажмите **Параметры центра управления безопасностью**.
 - В окне **Центр управления безопасностью** перейдите в раздел **Защита электронной почты**.
- 2 В разделе **Шифрованная электронная почта** выберите **Добавлять цифровую подпись к исходящим сообщениям**.

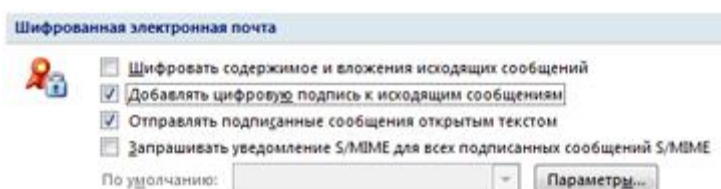


Рисунок 69. Группа «Шифрованная электронная почта» в окне управления безопасностью

- 3 Убедитесь, что установлен флажок **Отправлять подписанные сообщения открытым текстом** (иначе получатели, не использующие протокол S/MIME, не смогут прочесть сообщение).
- 4 Нажмите **Параметры**.
- 5 Заполните поле **Имя конфигурации**.
- 6 Нажмите **Выбрать** напротив поля **Сертификат подписи**.
- 7 В окне **Выбор сертификата** выберите сертификат из списка. Чтобы просмотреть выбранный сертификат, нажмите **Просмотреть свойства сертификата**.

Выбрав сертификат подписи, нажмите **ОК**. Тот же сертификат автоматически будет задан для шифрования сообщений.



Внимание! Если выбранный для создания электронной подписи сертификат не содержит адреса электронной почты или адрес не совпадает с адресом отправки сообщения электронной почты, Microsoft Outlook не позволит выбрать данный сертификат в качестве сертификата электронной подписи.

Если выбранный сертификат не содержит электронного адреса отправки сообщения, возможны следующие сценарии:

- В хранилище операционной системы имеется другой сертификат с адресом электронной почты, который совпадает с адресом отправки сообщения электронной почты. При подписании сообщения электронной почты электронная подпись будет создана с помощью этого сертификата, а не указанного ранее.
- В хранилище операционной системы нет других сертификатов с адресом электронной почты, который бы совпадал с адресом отправки сообщения. При попытке подписания сообщения электронная подпись добавлена не будет.

Чтобы получить возможность подписания сообщений электронной почты сертификатом, создайте запрос на новый сертификат, укажите в нем корректный адрес электронной почты и передайте запрос администратору вашего удостоверяющего центра.

- 8 Чтобы сохранить настройки, дважды нажмите **ОК**.

Просмотр электронной подписи сообщения

Для проверки электронной подписи сообщения в Microsoft Outlook:

- 1 Откройте сообщение с электронной подписью.
- 2 В строке **Подписано** проверьте адрес электронной почты лица, подписавшего сообщение.

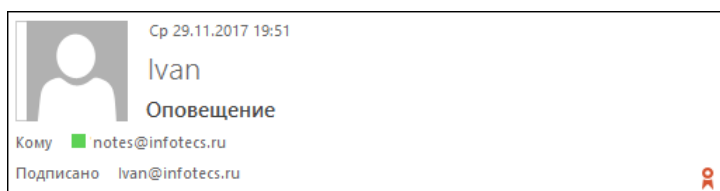


Рисунок 70. Проверка электронной подписи в сообщении



Внимание! Если адрес электронной почты в строке **Подписано** не совпадает с адресом отправителя, то истинным отправителем сообщения следует считать подписавшее его лицо.

Если при проверке электронной подписи возникли какие-либо проблемы, строка **Подписано** подчеркнута красной линией.

- 3 Чтобы получить более подробную информацию об электронной подписи, нажмите **Цифровая подпись** .
- Если электронная подпись, содержащаяся в сообщении, действительна, откроется окно **Цифровая подпись: правильная**.
- Если электронная подпись, содержащаяся в сообщении, недействительна, откроется окно **Цифровая подпись: неправильная**.

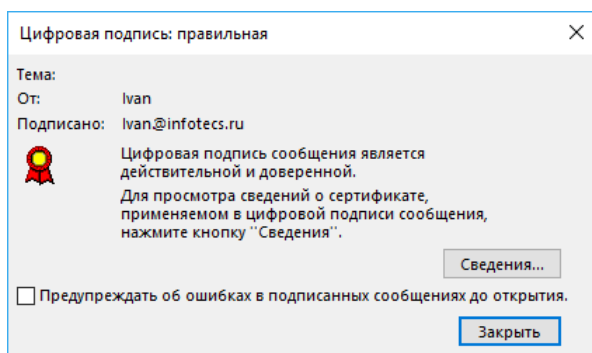


Рисунок 71. Сведения о действительности электронной подписи

- 4 Чтобы получить информацию о сертификате подписи, нажмите **Сведения**.

Шифрование сообщений электронной почты

Шифрование отдельного сообщения в Microsoft Outlook

- 1 Создайте новое сообщение и укажите нужного получателя.
- 2 Установите функцию шифрования одним из способов:
 - Откройте **Параметры > Разрешение** нажмите **Шифровать**.
 - Откройте **Параметры > Дополнительные параметры** нажмите **Свойства** . В окне **Свойства** нажмите **Параметры безопасности**. В окне **Свойства безопасности** выберите **Шифровать содержимое и вложения сообщений**.

Чтобы изменить дополнительные параметры настройки (см. [Настройка дополнительных параметров электронной подписи и шифрования](#)), такие как выбор персонального сертификата из нескольких установленных, нажмите **Изменить параметры**.

- 3 Отправьте сообщение.

Шифрование всех отправляемых сообщений в Microsoft Outlook

- 1 В главном окне Microsoft Outlook выберите **Файл > Параметры > Центр управления безопасностью > Параметры центра управления безопасностью > Защита электронных писем**.
- 2 В разделе **Шифрованная электронная почта** выберите **Шифровать содержимое и вложения исходящих сообщений**.

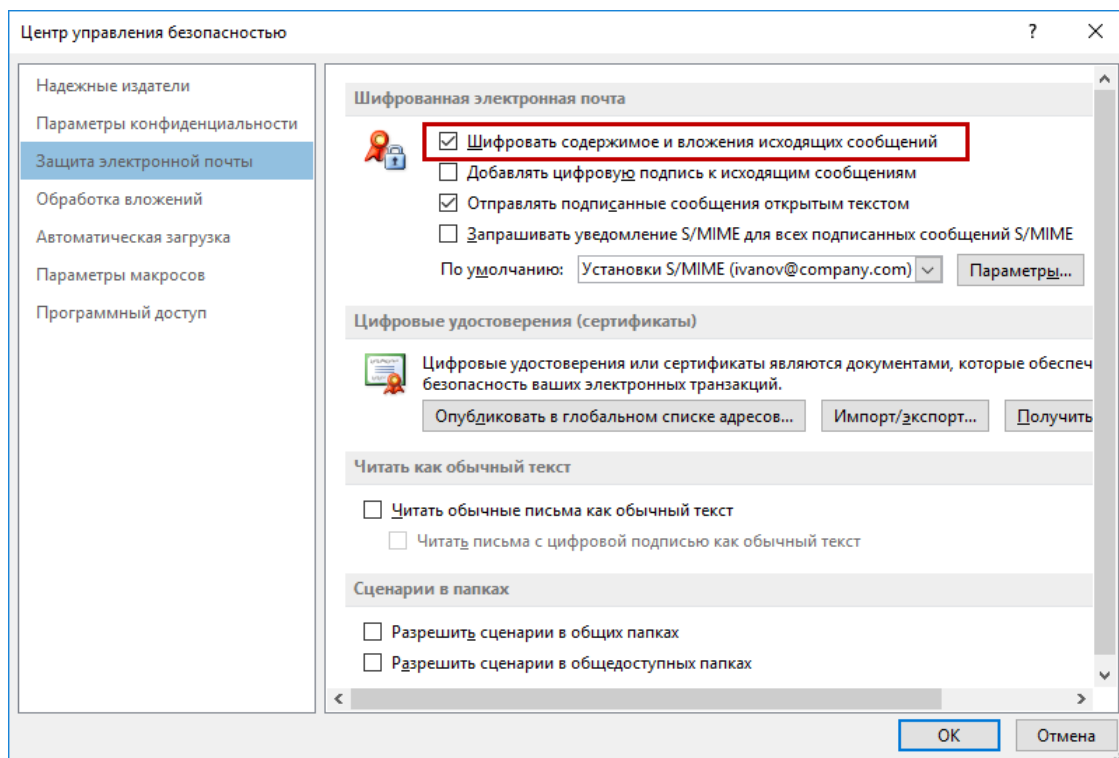


Рисунок 72. Установка параметра для шифрования всех сообщений

- 3 Чтобы [изменить дополнительные параметры настройки](#), такие как выбор персонального сертификата из нескольких установленных, нажмите **Параметры**. Чтобы сохранить изменения, нажмите **ОК**.
- 4 Два раза нажмите **ОК**.

После этого все отправляемые сообщения будут зашифрованы, если для их получателей в карточке контактов добавлены сертификаты (см. [Обмен сертификатами с получателем сообщения](#)).

Шифрование документов и файлов

Чтобы зашифровать документы или файлы:

- 1 Создайте зашифрованное сообщение (см. [Шифрование сообщений электронной почты](#)).
- 2 Вложите необходимые документы или файлы.
- 3 Отправьте сообщение на адрес получателя или на свой адрес. В первом случае зашифрованные документы сможет просмотреть только указанный вами получатель, во втором — только вы.

Просмотр зашифрованных сообщений



Внимание! Для просмотра зашифрованного сообщения необходима ViPNet CSP.

В Microsoft Outlook полученное зашифрованное сообщение в списке сообщений отмечено значком .

Чтобы просмотреть зашифрованное сообщение:

- 1 Дважды щелкните нужное сообщение в списке.
- 2 В окне **ViPNet CSP - пароль контейнера ключей** введите пароль, которым защищен ваш закрытый ключ.

13

Электронная подпись макросов, форм и баз данных

Электронная подпись в Microsoft Office InfoPath	136
Электронная подпись макросов	140

Электронная подпись в Microsoft Office InfoPath

Разрешение подписывать форму InfoPath электронной подписью

При создании шаблона формы Microsoft Office InfoPath вы можете разрешить добавление к форме электронной подписи. Заполнив форму, пользователи смогут подписать всю форму или отдельные ее части.

Чтобы разрешить пользователям подписывать форму Microsoft Office InfoPath 2010 и 2013:

- 1 В приложении Microsoft InfoPath Designer создайте или откройте шаблон формы.
- 2 На вкладке **Файл** в разделе **Сведения** нажмите **Параметры формы**.
- 3 В окне **Параметры формы** откройте раздел **Цифровые подписи**.

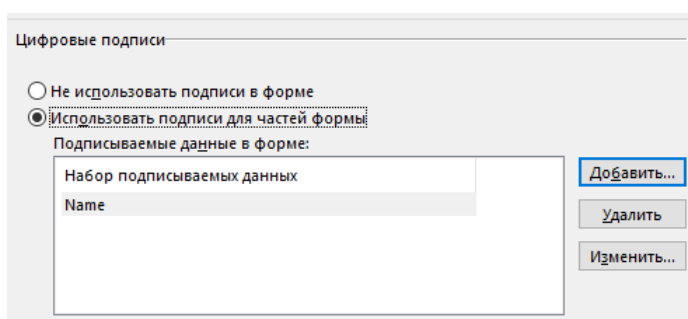


Рисунок 73. Вкладка «Цифровые подписи»

- 4 Чтобы указать подписываемые данные, нажмите **Добавить**.
 - 5 В окне **Набор подписываемых данных**:
 - 5.1 Введите имя для подписываемых данных в соответствующее поле.
 - 5.2 Нажмите **Выбрать XPath** рядом с полем **Подписываемые поля и группы**. В окне **Выбор поля или группы** выберите подписываемое поле и нажмите **ОК**.
- Вы также можете указать тип взаимосвязи между несколькими подписями, установив переключатель в желаемое положение (по умолчанию **Допускать использование только одной подписи**) и добавить сообщение для подтверждения подписи.
- 6 Выполнив необходимые настройки, нажмите **ОК**.

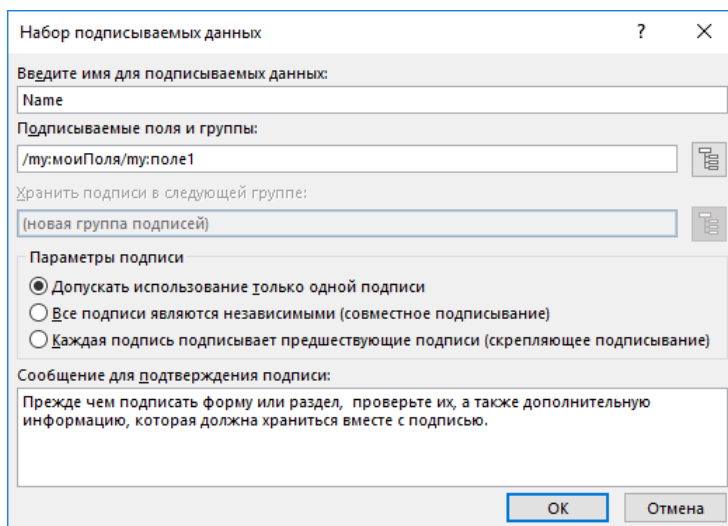


Рисунок 74. Окно «Набор подписываемых данных»

- 7 Чтобы сохранить настройки, нажмите **ОК**.

Подписание формы InfoPath

Если при создании формы была предусмотрена возможность ее подписания, пользователь сможет добавить к форме свою электронную подпись. Чтобы подписать форму:

- 1 Откройте форму или шаблон формы в программе InfoPath Filler 2010 или InfoPath Filler 2013.
- 2 Откройте вкладку **Файл** и в разделе **Сведения** нажмите **Подписать форму**.
- 3 В окне **Цифровые подписи** нажмите **Добавить**.
- 4 В окне **Выбор данных для подписания**:
 - 4.1 Если электронная подпись применяется для всей формы, выберите единственный пункт списка — **Вся форма**.
 - 4.2 Если подпись применяется для отдельных данных, выберите из списка подписываемые данные.
- 5 Нажмите **ОК**.
- 6 В окне **Подписание**:
 - 6.1 Введите свое имя в поле рядом с крестиком или нажмите **Выбрать рисунок**, чтобы вставить графическое изображение подписи.
 - 6.2 При необходимости заполните поле **Цель подписания документа**. В InfoPath Filler 2013 в этом окне вы также можете выбрать причину подписания из нескольких заданных вариантов в списке **Тип подтверждения**.

В нижней части окна **Подписание** приведены краткие сведения о сертификате, которым предполагается подписать данные. Если вы хотите подписаться другим сертификатом, нажмите **Изменить** и выберите сертификат.

7 Нажмите **Подписать**.

8 В окне **ViPNet CSP – пароль контейнера ключей** введите пароль и нажмите **ОК**.

После подписания внесение изменений в форму (или в поля) будет невозможно.

Просмотр подписи в форме InfoPath

Чтобы просмотреть подпись в форме Microsoft InfoPath:

1 Откройте вкладку **Файл** и в разделе **Сведения** нажмите **Просмотр подписей**.

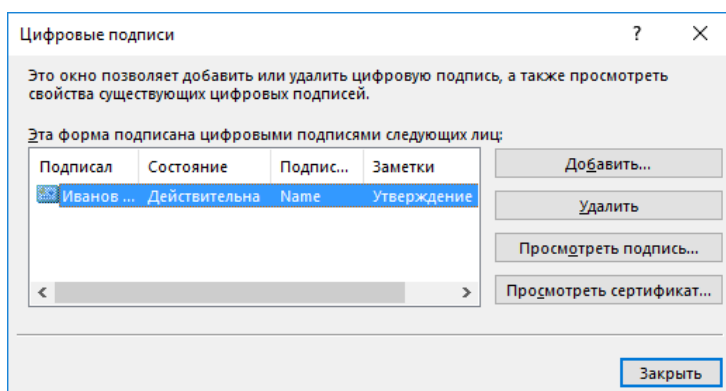


Рисунок 75. Просмотр подписи в форме

2 В окне **Цифровые подписи**:

2.1 Если вы используете Microsoft InfoPath Filler 2010, выберите электронную подпись из списка и нажмите **Просмотреть подписанную форму**.

2.2 Если вы используете Microsoft InfoPath Filler 2013, выберите электронную подпись из списка и нажмите **Просмотреть подпись**.

3 В окне **Состав подписи** содержатся краткие сведения о подписи и сертификате. Если при проверке сертификата возникли ошибки, сообщение об этом будет выведено под заголовком окна.

4 Чтобы открыть сертификат, нажмите **Просмотр**.

Удаление подписи из формы InfoPath

Чтобы удалить подпись из формы Microsoft InfoPath:

1 Откройте вкладку **Файл** и в разделе **Сведения** нажмите **Просмотр подписи**.

2 В окне **Цифровые подписи** выберите электронную подпись из списка.

Чтобы просмотреть подпись перед удалением, нажмите **Просмотреть подпись**.

3 Выбрав электронную подпись, нажмите **Удалить**.

4 В окне подтверждения нажмите **Да**.

Электронная подпись макросов

Подписание макросов

Создав макрос в приложениях Microsoft Office, вы можете заверить его электронной подписью. Электронная подпись подтверждает происхождение макроса и его безопасность. Создать и подписать макрос позволяют приложения Microsoft Word, Excel, Outlook, PowerPoint, Publisher и Visio.



Внимание! Чтобы подписать макрос, сертификат должен иметь расширение «Подписывание кода» в поле «Расширенное использование ключа» («Улучшенный ключ»). Для получения нужного сертификата обратитесь к администратору программы ViPNet Удостоверяющий и ключевой центр (см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора»).

Чтобы подписать макрос:

- 1 В приложении Microsoft Office Outlook, Publisher, Visio, Word, Excel или PowerPoint на вкладке **Разработчик** в разделе **Код** нажмите **Visual Basic**.



Примечание. Вкладка **Разработчик** по умолчанию не отображается. Чтобы она появилась, в меню **Файл** выберите пункт **Параметры** и в открывшемся окне в разделе **Настроить ленту** добавьте вкладку **Разработчик**.

В любом из перечисленных приложений для вызова редактора Microsoft Visual Basic можно также воспользоваться сочетанием клавиш **Alt+F11**.

- 2 В окне редактора Microsoft Visual Basic в меню **Tools (Сервис)** выберите **Digital Signature (Цифровая подпись)**.

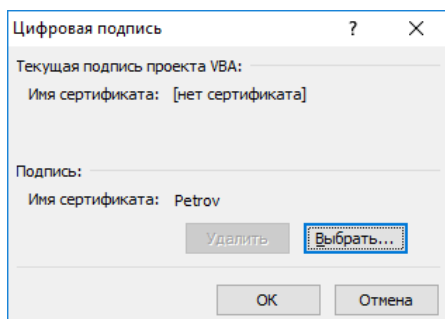


Рисунок 76. Добавление электронной подписи

- 3 В окне **Цифровая подпись** нажмите **Выбрать**, выберите сертификат электронной подписи и нажмите **ОК**.

Проверка подписи макроса

1 В окне редактора Microsoft Visual Basic в меню **Сервис** выберите **Цифровая подпись**.

2 В окне **Цифровая подпись** указан текущий сертификат подписи. Чтобы просмотреть сертификат, нажмите **Подробности**.

Если сертификат ненадежен, то на вкладке **Общее** в окне **Сертификат** будет выведено сообщение о возникшей проблеме. Ненадежный сертификат помечается красным крестом.

Удаление подписи макроса

Чтобы удалить электронную подпись из проекта макроса:

1 В окне редактора Microsoft Visual Basic в меню **Сервис** выберите **Цифровая подпись**.

2 Чтобы удалить электронную подпись, нажмите **Удалить**.

Подписание базы данных Microsoft Access

В приложении Microsoft Access предусмотрена возможность подписания базы данных при публикации. После создания файла базы данных в формате Microsoft Access его можно упаковать, добавить электронную подпись, а затем распространить подписанный пакет среди других пользователей. Пользователи, получившие пакет, могут извлечь из него базу данных и далее работать с ней.

Чтобы упаковать и подписать базу данных Microsoft Access:

1 В Microsoft Access 2010 или 2013 откройте вкладку **Файл** и выберите раздел **Сохранить как** (в Access 2010 — **Сохранить и опубликовать**). В разделе **Сохранить базу данных как** нажмите **Упаковать и подписать**, а затем — **Сохранить как**.

2 Выберите сертификат электронной подписи и нажмите **ОК**.



Внимание! Для подписания базы данных электронной подписью необходимо выбрать сертификат, который имеет расширение «Подписывание кода» в поле «Расширенное использование ключа» («Улучшенный ключ»). Если в сертификате в поле «Расширенное использование ключа» не добавлено данное расширение, вы не сможете создать подписанный пакет. За необходимым сертификатом обратитесь к администратору удостоверяющего центра (см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора»).

3 В окне **Создать подписанный пакет Microsoft Office Access** выберите папку для сохранения подписанного пакета и введите имя пакета в поле **Имя файла**.

4 Нажмите **Создать**.

14

Организация защищенного TLS-соединения

TLS-соединение	143
Организация доступа к защищенному веб-серверу	144
Настройка веб-браузера Internet Explorer для работы по протоколу TLS	146
Проверка доступности веб-узла по защищенному протоколу HTTPS	147

TLS-соединение

Протокол TLS используется для организации удаленного защищенного соединения, например доступа к ресурсам удаленного сервера. Протокол позволяет провести одностороннюю или взаимную аутентификацию взаимодействующих сторон, а также обеспечить конфиденциальную передачу информации. Необходимость защищенного доступа может возникнуть при реализации общего доступа к базам данных или хранилищам, при создании систем электронных платежей и в других случаях.

Взаимодействие двух узлов при защищенном соединении представлено на схеме ниже.

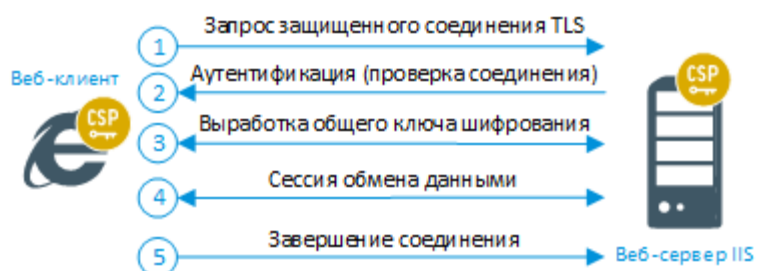


Рисунок 77. Схема взаимодействия узлов при TLS-соединении

Использование протокола TLS, реализуемого средствами криптопровайдера ViPNet CSP, позволяет гарантировать надежное и санкционированное соединение с удаленными серверами и строго ограниченный доступ к защищенным данным.

Организация доступа к защищенному веб-серверу

Чтобы с помощью криптопровайдера ViPNet CSP организовать доступ к защищенному веб-серверу:

Таблица 3. Порядок организации доступа к защищенному веб-серверу

Действие	Ссылка
☐ Настройте сервер IIS.	Настройка серверной части
☐ При необходимости настройте браузер Internet Explorer для работы по протоколу TLS.	Настройка клиентской части

Настройка серверной части

- 1 Настройте сервер IIS, см. «Практическое руководство. Создание удаленных веб-узлов IIS» в [библиотеке MSDN](#).
- 2 Установите ViPNet CSP (см. [Установка и запуск программы](#)).
- 3 Создайте запрос на сертификат для веб-сервера IIS (см. [Получение закрытого ключа и сертификата](#)) (используйте шаблон сертификата **Веб-сервер**) и отправьте его в УЦ.
- 4 Получите у администратора УЦ сертификат для сервера IIS, изданный по запросу, а также сертификат издателя и список аннулированных сертификатов (CRL).



Внимание! Сертификат пользователя для сервера должен иметь расширение «Шифрование данных» в поле «Использование ключа» и расширение «Проверка подлинности сервера» в поле «Расширенное использование ключа» («Улучшенный ключ»).

- 5 Установите полученный сертификат для сервера в контейнер ключей (см. [Добавление сертификата в контейнер ключей](#)).
- 6 Сохраните пароль доступа к контейнеру ключей (см. [Просмотр и настройка свойств контейнера ключей](#)).
- 7 Установите в хранилище сертификатов локального компьютера сертификат сервера (см. [Установка сертификата в системное хранилище Windows](#)), а также сертификат издателя и список CRL (см. [Установка сертификата издателя и списка аннулированных сертификатов](#)).
- 8 Настройте права доступа к контейнеру ключей (см. [Настройка прав доступа к контейнеру ключей](#)). Мы рекомендуем задать следующие права:
 - Для группы SYSTEM — **Полный доступ, Чтение**.

- Для группы Administrators — **Полный доступ, Чтение**.
 - Для встроенной учетной записи, под которой работает приложение (LOCAL SYSTEM, LOCAL SERVICE, NETWORK SERVICE или IIS AppPool\Имя пула), — **Полный доступ, Чтение**.
- 9 Проверьте доступность веб-узла по защищенному протоколу HTTPS (см. [Проверка доступности веб-узла по защищенному протоколу HTTPS](#)).

Настройка клиентской части

- 1 Установите ViPNet CSP (см. [Установка и запуск программы](#)).
- 2 Создайте запрос на сертификат пользователя (см. [Получение закрытого ключа и сертификата](#)) и отправьте его в УЦ.
- 3 Получите у администратора УЦ сертификат для веб-клиента, изданный по запросу, а также сертификат издателя и список CRL.



Внимание! Сертификат пользователя для веб-клиента должен иметь расширение «Проверка подлинности клиента» в поле «Расширенное использование ключа» («Улучшенный ключ»).

- 4 Установите полученный сертификат для клиента в контейнер ключей.
- 5 Установите в хранилище сертификатов текущего пользователя сертификат для веб-клиента, а также сертификат издателя и список CRL.
- 6 Выполните [настройку веб-браузера Internet Explorer](#) для работы по защищенному протоколу.
- 7 Проверьте доступность веб-узла по защищенному протоколу HTTPS.

Настройка веб-браузера Internet Explorer для работы по протоколу TLS



Примечание. В веб-браузере Google Chrome 26 и более поздних версий организовать защищенное соединение TLS с помощью криптопровайдера ViPNet CSP невозможно.

Настройки веб-браузера Internet Explorer по умолчанию позволяют работать по протоколу TLS. Если настройки браузера отличны от первоначальных или соединение с сервером не происходит, выполните следующие действия:

- 1 В меню **Сервис** веб-браузера Internet Explorer выберите пункт **Свойства обозревателя** (**Свойства браузера**).
- 2 В окне **Свойства обозревателя** (**Свойства браузера**) выполните следующие действия:
 - Откройте вкладку **Безопасность** и убедитесь, что флажок **Включить защищенный режим** снят.
 - Откройте вкладку **Дополнительно** и убедитесь, что установлены флажки **TLS 1.0** и **Использовать TLS 1.2**.
- 3 Проверьте доступность веб-узла по защищенному протоколу HTTPS.

Проверка доступности веб-узла по защищенному протоколу HTTPS

Для доступа к веб-узлу по протоколу HTTPS:

- 1 В адресной строке браузера Internet Explorer введите `https://имя_сервера`.
- 2 При успешном соединении и аутентификации пользователя откроется страница веб-сервера.

Если соединение с веб-сервером установить не удалось, обратитесь к разделу [Нет соединения с сервером по протоколу TLS](#).

15

Взаимодействие с ViPNet HSM

Общие сведения о ViPNet HSM	149
Настройка взаимодействия с ViPNet HSM	150

Общие сведения о ViPNet HSM

ViPNet HSM представляет собой программно-аппаратный комплекс (далее — ПАК), предназначенный для выполнения криптографических операций по запросам клиентов, а также для защищенного хранения ключей и конфиденциальных данных клиентов. Подробно см. в документе «Программно-аппаратный комплекс ViPNet HSM. Руководство администратора».

С помощью ViPNet CSP можно подключиться к ПАК ViPNet HSM и использовать его для защищенного хранения ключей и выполнения криптографических операций. Для этого между ViPNet CSP и ПАК ViPNet HSM необходимо настроить соединение.

Настройка взаимодействия с ViPNet HSM

Для направления [ViPNet HSM](#) запросов на выполнение криптографических операций и получения результатов их выполнения, а также для работы с ключами, хранящимися на ViPNet HSM:

- 1 В окне **ViPNet CSP** в разделе **Подключаемые устройства** убедитесь, что опрос устройств **ViPNet HSM** включен (см. [Настройка списка опрашиваемых устройств](#)).
- 2 Установите ПО ViPNet HSM SDK согласно документу «Программно-аппаратный комплекс ViPNet HSM. Руководство разработчика прикладного сервиса».
- 3 Настройте ПО ViPNet HSM SDK согласно документу «Программно-аппаратный комплекс ViPNet HSM. Руководство разработчика прикладного сервиса».

Теперь вы можете работать с ключами, хранящимися в ПАК ViPNet HSM, как если бы они находились на внешнем устройстве, подключенном к вашему компьютеру (см. [Операции с контейнерами ключей](#)).

Региональные настройки

Для корректного отображения русской локализации интерфейса программ ViPNet в русифицированных ОС Microsoft Windows английской локализации необходимо установить поддержку кириллицы для программ, не поддерживающих Юникод. Эти настройки рекомендуется производить до установки самой программы.

Данные настройки также понадобятся сделать, если установлен русскоязычный MUI (Multilanguage User Interface). Это значит, что ядро операционной системы английское, а русский язык для интерфейса и файлов справки был установлен позже. В этом случае региональные настройки по умолчанию английские и требуют изменения.



Внимание! Для изменения региональных настроек вы должны обладать правами администратора операционной системы.

Региональные настройки в Windows

Чтобы установить поддержку кириллицы:

- 1 Откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Изменение форматов даты, времени и чисел (Change date, time, or number formats)**.
- 2 В окне **Регион (Region)** перейдите на вкладку **Дополнительно (Administrative)**.

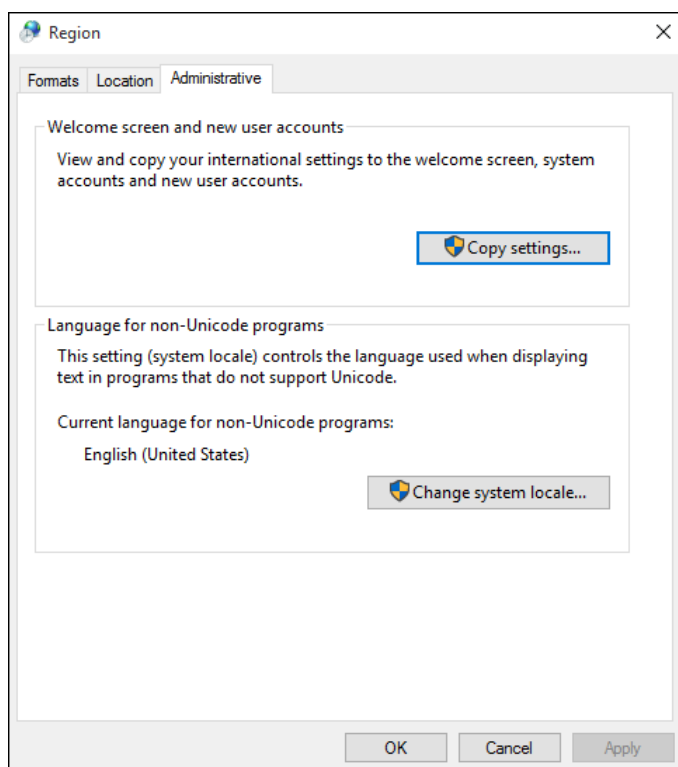


Рисунок 78. Дополнительные языковые параметры

- 3 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Изменить язык системы (Change system locale)**.
- 4 В появившемся окне в списке выберите **Русский (Россия) (Russian (Russia))**.

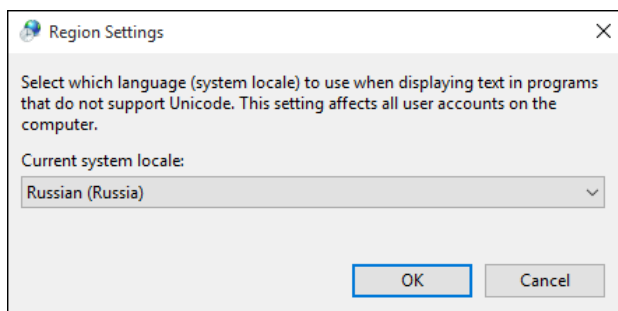


Рисунок 79. Выбор языка системы

- 5 Нажмите кнопку **ОК**. Перезагрузите компьютер.
- 6 Дождитесь завершения перезагрузки компьютера, откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Изменение форматов даты, времени и чисел (Change date, time, or number formats)**.
- 7 В окне **Регион (Region)** перейдите на вкладку **Дополнительно (Administrative)**.
- 8 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Копировать параметры (Copy settings)**.
- 9 В открывшемся окне в списке **Копировать текущие параметры в (Copy your current settings to)** установите флажок **Экран приветствия и системные учетные записи (Welcome screen and system accounts)** и нажмите кнопку **ОК**.

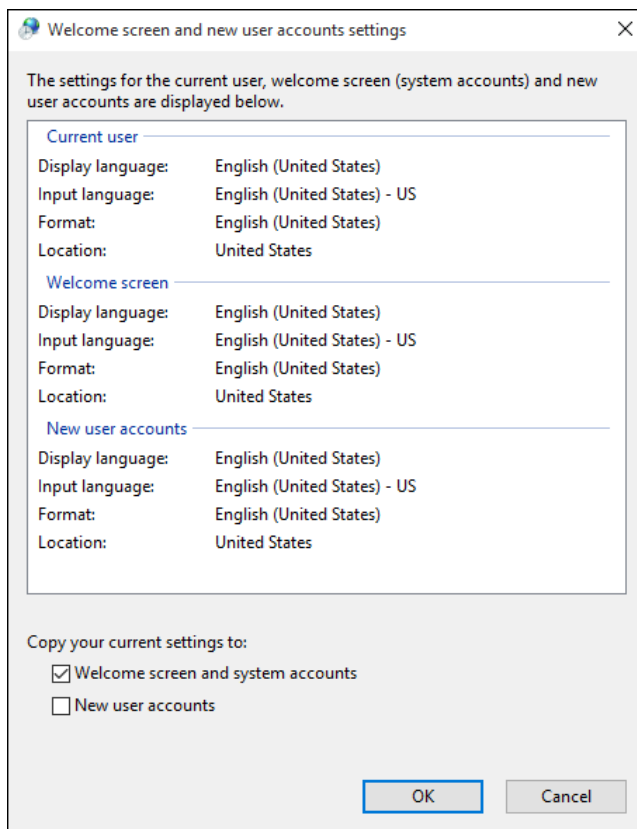


Рисунок 80. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах мы рекомендуем выполнить следующие действия:

- 1 В окне **Регион (Region)** на вкладке **Форматы (Formats)** в списке **Формат (Format)** выберите **Русский (Россия) (Russian (Russia))**.

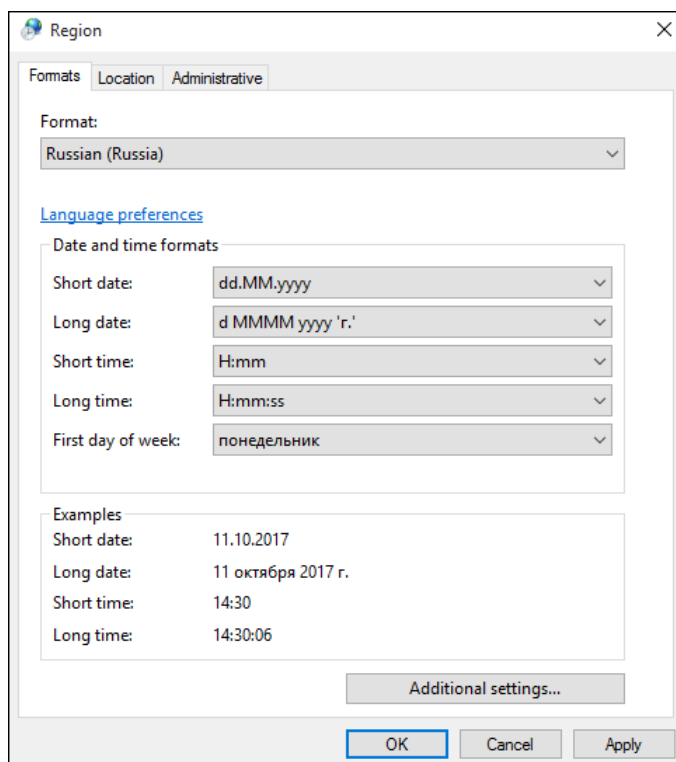


Рисунок 81. Настройка форматов

- 2 В окне **Регион (Region)** на вкладке **Местоположение (Location)** в списке **Основное расположение (Home location)** выберите **Россия (Russia)**.



Примечание. В Windows 10 версии 1809 и выше нет вкладки **Location**, поэтому указанный параметр настраивать не нужно.

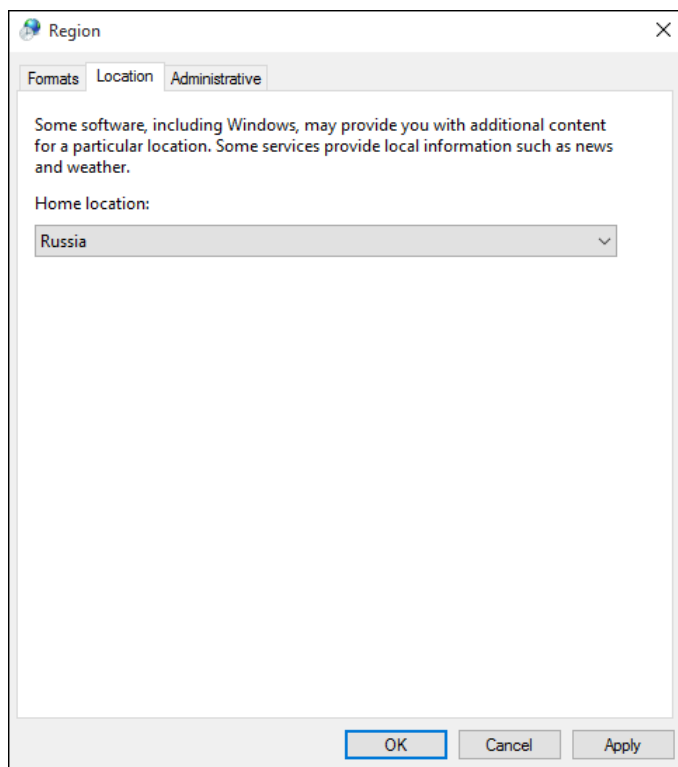


Рисунок 82. Выбор текущего расположения

А

Возможные неполадки

Требование обновления Windows при установке ViPNet CSP

В процессе установки ViPNet CSP может быть выдано сообщение о необходимости обновления Windows.

Запустите Центр обновления Windows и установите все последние обновления. Это обеспечит правильную работу ViPNet CSP и защиту вашего компьютера.

Не удастся запустить ViPNet CSP из-за нарушения целостности файлов программы

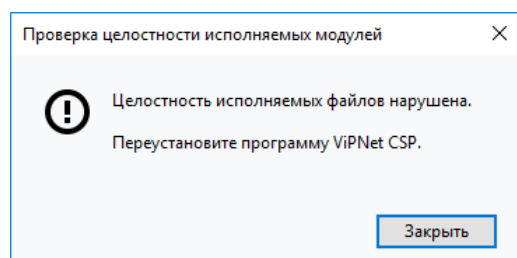


Рисунок 83. Сообщение о нарушении целостности файлов программы

Чтобы вернуть работоспособность ViPNet CSP, запустите установочный файл и восстановите установленные компоненты программы.

После перезагрузки ViPNet CSP будет полностью работоспособна. Если программа была зарегистрирована, повторная регистрация не требуется.

Не удастся получить код регистрации через Интернет

Если при попытке получить код регистрации через Интернет соединение с сервером регистрации АО «ИнфоТеКС» установить не удастся в течение 3 минут, появится окно с предупреждением.

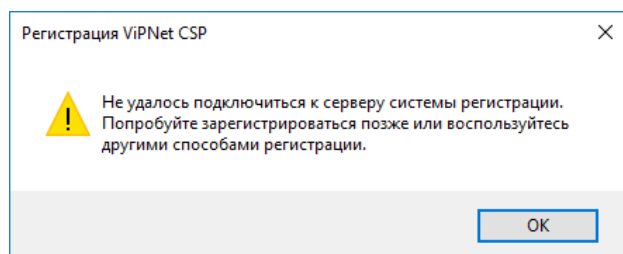


Рисунок 84. Не удалось соединиться с сервером регистрации АО «ИнфоТеКС»

В этом случае проверьте настройки вашего сетевого экрана. Доступ к [серверу регистрации АО «ИнфоТеКС»](#) по протоколу TCP, порт 80 не должен быть заблокирован.

Проблемы при использовании аппаратного модуля доверенной загрузки «Аккорд-АМД3»

Если на компьютере установлен аппаратный модуль доверенной загрузки «Аккорд-АМД3», но его не удастся использовать в ViPNet CSP в качестве датчика случайных чисел, выполните следующие действия:

- 1 Убедитесь, что на компьютере установлены драйверы «Аккорд-АМД3».
- 2 Из папки установки драйверов (по умолчанию C:\Accord) скопируйте файл `tmdrv32.dll` в следующую папку:
 - При использовании 32-разрядной версии Windows — C:\Windows\System32.
 - При использовании 64-разрядной версии Windows — C:\Windows\SysWOW64.
- 3 В ViPNet CSP выберите «Аккорд-АМД3» в качестве датчика случайных чисел (см. [Использование датчика случайных чисел](#)).

Проблемы при использовании устройства типа SafeNet eToken (eToken Aladdin)

Если вы используете устройство типа SafeNet eToken (eToken Aladdin), и при формировании запроса на сертификат ваш компьютер зависает, убедитесь, что установлено программное обеспечение eToken PKI Client 5.1 SP1 или SafeNet Authentication Client.

Сертификат автоматически некорректно устанавливается в хранилище при подключении внешнего устройства

При подключении к компьютеру некоторых внешних устройств, например устройств семейства ESMART Token, сертификаты, хранящиеся на них, устанавливаются в системное хранилище автоматически. После такой установки работа ViPNet CSP с этими сертификатами будет невозможна. Чтобы отключить автоматическую установку сертификатов при подключении устройства, предварительно выполните следующие действия:

- 1 Откройте консоль MMC:
 - 1.1 Выберите **Пуск > Выполнить** или нажмите **Win+R**.
 - 1.2 В поле **Открыть** введите `mmc` и нажмите **ОК**.
- 2 В меню **Файл** окна консоли выберите **Добавить или удалить оснастку**.
- 3 В окне **Добавление и удаление оснасток** в списке **Доступные оснастки** выберите оснастку **Редактор объектов групповой политики** и нажмите **Добавить**.
- 4 В окне **Выбор объекта групповой политики** выберите объект **Локальный компьютер**. В результате будет добавлена оснастка **Политика "Локальный компьютер"**.
- 5 На левой панели окна консоли выберите раздел **Корень консоли > Политика "Локальный компьютер" > Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Смарт-карта**.
- 6 На правой панели окна консоли дважды щелкните параметр **Включить распространение корневого сертификата со смарт-карты**.
- 7 В окне **Включить распространение корневого сертификата со смарт-карты** установите переключатель в положение **Отключено**.

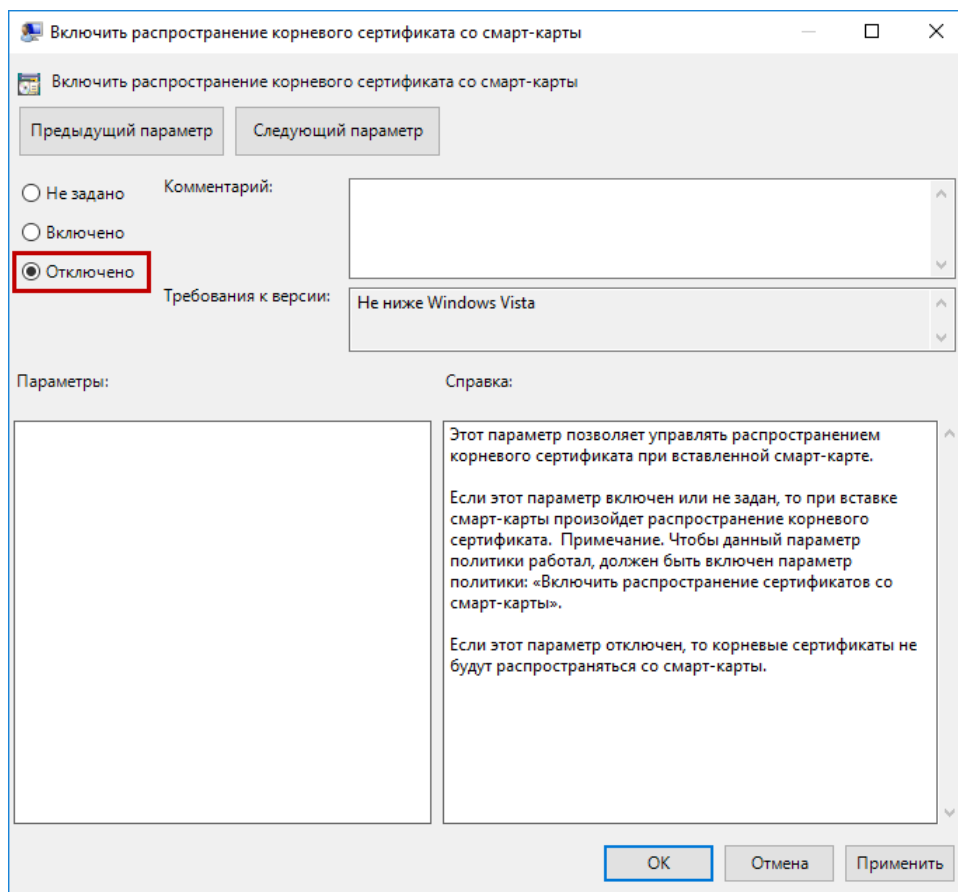


Рисунок 85. Отключение автоматической установки сертификатов в системное хранилище при подключении внешнего устройства к компьютеру

Теперь вы можете подключить внешнее устройство к компьютеру и установить нужные контейнеры ключей и сертификаты (см. [Установка контейнеров ключей и сертификатов](#)).

Не удастся зашифровать документ

Адрес электронной почты из сертификата не найден в списке адресов контакта

При импорте сертификата в карточку контакта Microsoft Outlook может появиться предупреждение о том, что сертификат не содержит адрес электронной почты, который бы соответствовал адресу данного контакта.

В этом случае зашифровать сообщение на этом сертификате получателя не удастся.

Возможны следующие причины появления проблемы:

- Сертификат не принадлежит данному контакту, в этом случае выполните следующие действия:
 - Откройте окно **Сертификат**, дважды щелкнув файл сертификата.

- На вкладке **Общие** удостоверьтесь, что сертификат принадлежит данному получателю. Если это не так, укажите для импорта нужный сертификат.

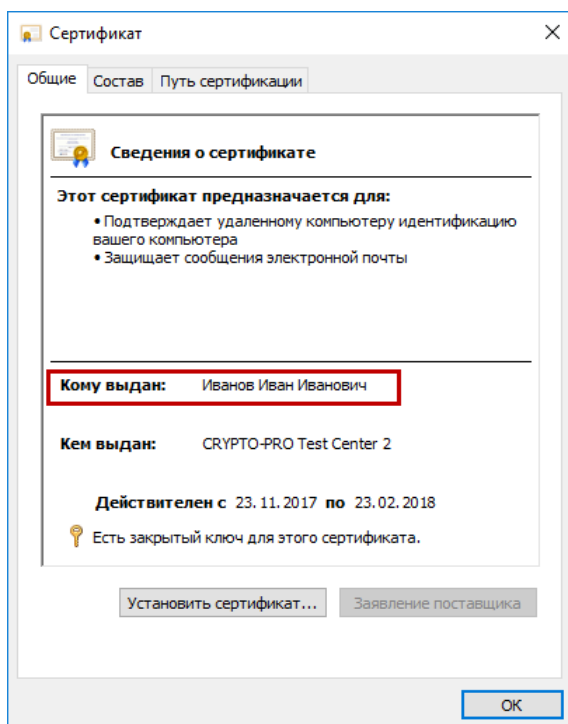


Рисунок 86. Проверка владельца сертификата

- В сертификате не прописан адрес электронной почты данного контакта, в этом случае выполните следующие действия:
 - Откройте окно **Сертификат**, дважды щелкнув файл сертификата на диске.
 - На вкладке **Состав** выберите поле **Субъект** и удостоверьтесь, в качестве значения параметра **E** задан нужный адрес электронной почты.

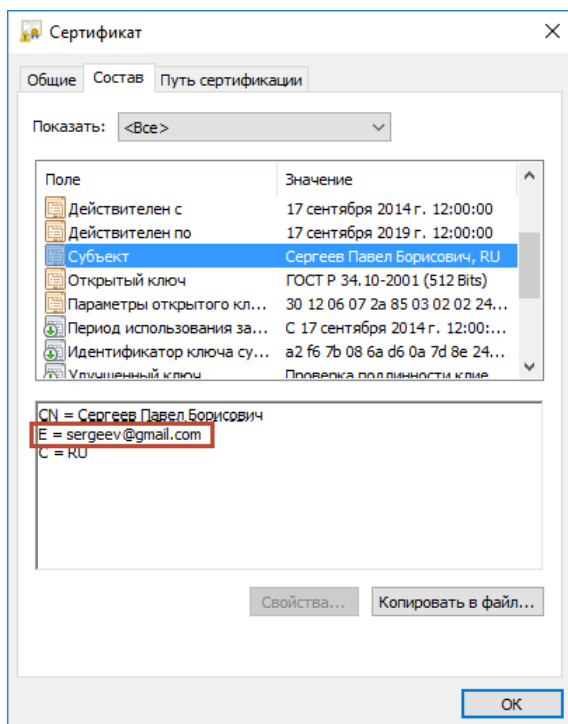


Рисунок 87. Проверка адреса электронной почты в сертификате

Если это не так, выполните следующие действия:

- Если вы импортировали сертификат контакта, запросите новый сертификат у получателя.
- Если вы добавляли в систему свой сертификат, запросите новый сертификат у администратора вашего удостоверяющего центра.

Недопустимый сертификат

При отправке зашифрованного сообщения может появиться предупреждение:

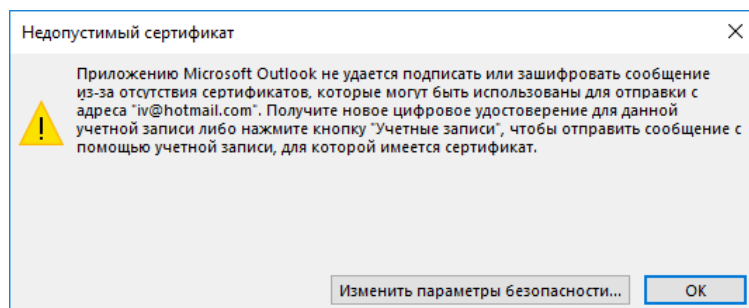


Рисунок 88. Недопустимый сертификат в Microsoft Outlook

Это может быть связано со следующими причинами:

- Сертификат получателя не содержит адреса электронной почты данного получателя (см. [Адрес электронной почты из сертификата не найден в списке адресов контакта](#)).

- Ваш сертификат не содержит адреса вашей электронной почты (см. [Адрес электронной почты из сертификата не найден в списке адресов контакта](#)).
- Сертификат получателя или ваш сертификат недействителен. Запросите новый сертификат у получателя или у администратора вашего удостоверяющего центра.
- Не указан персональный сертификат подписи и шифрования (см. [Настройка дополнительных параметров электронной подписи и шифрования](#)).
- В системное хранилище не был установлен сертификат издателя (см. [Установка сертификата издателя и списка аннулированных сертификатов](#)).

Не удается поставить электронную подпись

Не найден закрытый ключ, соответствующий сертификату

Если при выборе сертификата для подписания открывается окно **ViPNet CSP - инициализация контейнера ключей**, это значит, что не найден закрытый ключ, соответствующий выбранному сертификату. Это может произойти в том случае, если контейнер ключей был удален в ViPNet CSP (см. [Удаление контейнера ключей](#)).

Чтобы подписать документ выбранным сертификатом, в окне **ViPNet CSP - инициализация контейнера ключей** укажите путь к контейнеру, который содержит закрытый ключ, соответствующий сертификату. Если вы не знаете местоположение контейнера ключей, использование выбранного сертификата невозможно.

Если в окне **ViPNet CSP - инициализация контейнера ключей** вы укажете путь к контейнеру ключей, этот контейнер будет добавлен в список в разделе **Контейнеры ключей** окна **ViPNet CSP**.

Не удается подписать сообщение электронной почты

Если при попытке подписать сообщение электронной почты выводится сообщение о том, что отсутствуют сертификаты, которые могут быть использованы для отправки с данного адреса электронной почты, вам следует обратиться за таким сертификатом в удостоверяющий центр. В сертификате должен быть указан ваш адрес электронной почты и присутствовать расширение **Защищенная электронная почта** в поле **Расширенное использование ключа (Улучшенный ключ)**.

Не удалось подписать сообщение электронной почты нужным сертификатом

Если при попытке подписать сообщение электронной почты подписание происходит, но используется сертификат, отличный от выбранного, это означает, что указанный сертификат электронной подписи не содержит адреса электронной почты владельца сертификата или этот адрес не совпадает с адресом отправки сообщения электронной почты. При этом в момент

подписания сообщения из системного хранилища выбирается другой сертификат, содержащий адрес электронной почты, с которого отправляется сообщение.

Для устранения ошибки выполните следующие действия:

- 1 Создайте запрос на новый сертификат и укажите в нем корректный адрес электронной почты.
- 2 Отправьте запрос на сертификат администратору вашего удостоверяющего центра и дождитесь выполнения запроса.
- 3 Укажите в качестве сертификата для электронной подписи полученный сертификат.

Невозможно редактировать подписанный документ Microsoft Word или Excel

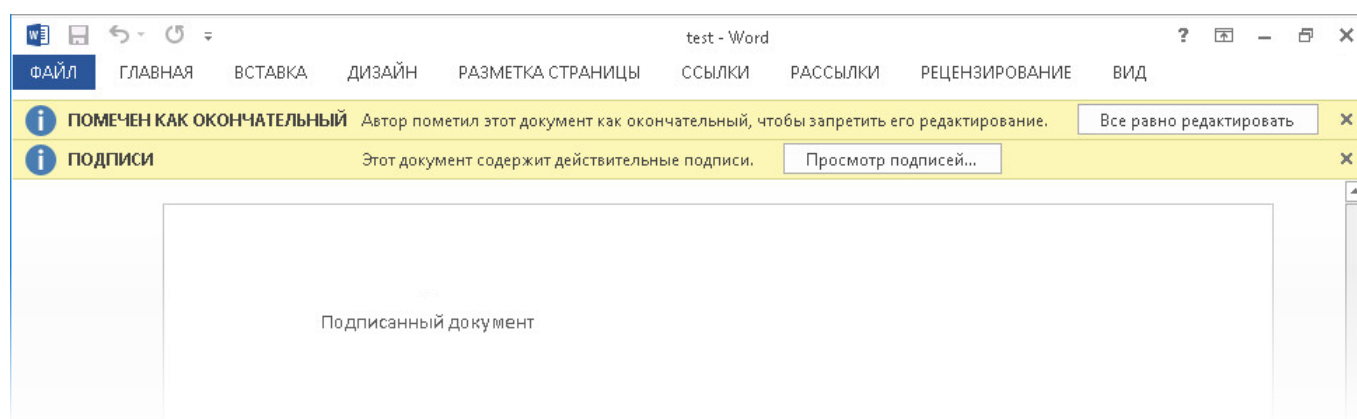


Рисунок 89. Предупреждения при открытии подписанного документа

Чтобы внести изменения в подписанный документ Microsoft Word или Excel, удалите электронную подпись (см. [Удаление электронной подписи в Microsoft Word, Excel и PowerPoint](#)) и внесите необходимые изменения. После этого вы можете снова подписать документ.



Внимание! Не следует удалять электронную подпись из документа, подписанного другим лицом, или если документ имеет юридическую значимость.

Нет соединения с сервером по протоколу TLS

На IIS-сервере и веб-клиенте установлены разные версии ViPNet CSP

Установите на веб-клиенте ту же версию ViPNet CSP, что установлена на сервере.

Если это невозможно и на сервере установлена более ранняя версия ViPNet CSP, чем 4.2, на веб-клиенте с последней версией ViPNet CSP выполните следующие действия:

- 1 В окне **ViPNet CSP** перейдите в раздел **Дополнительно**.

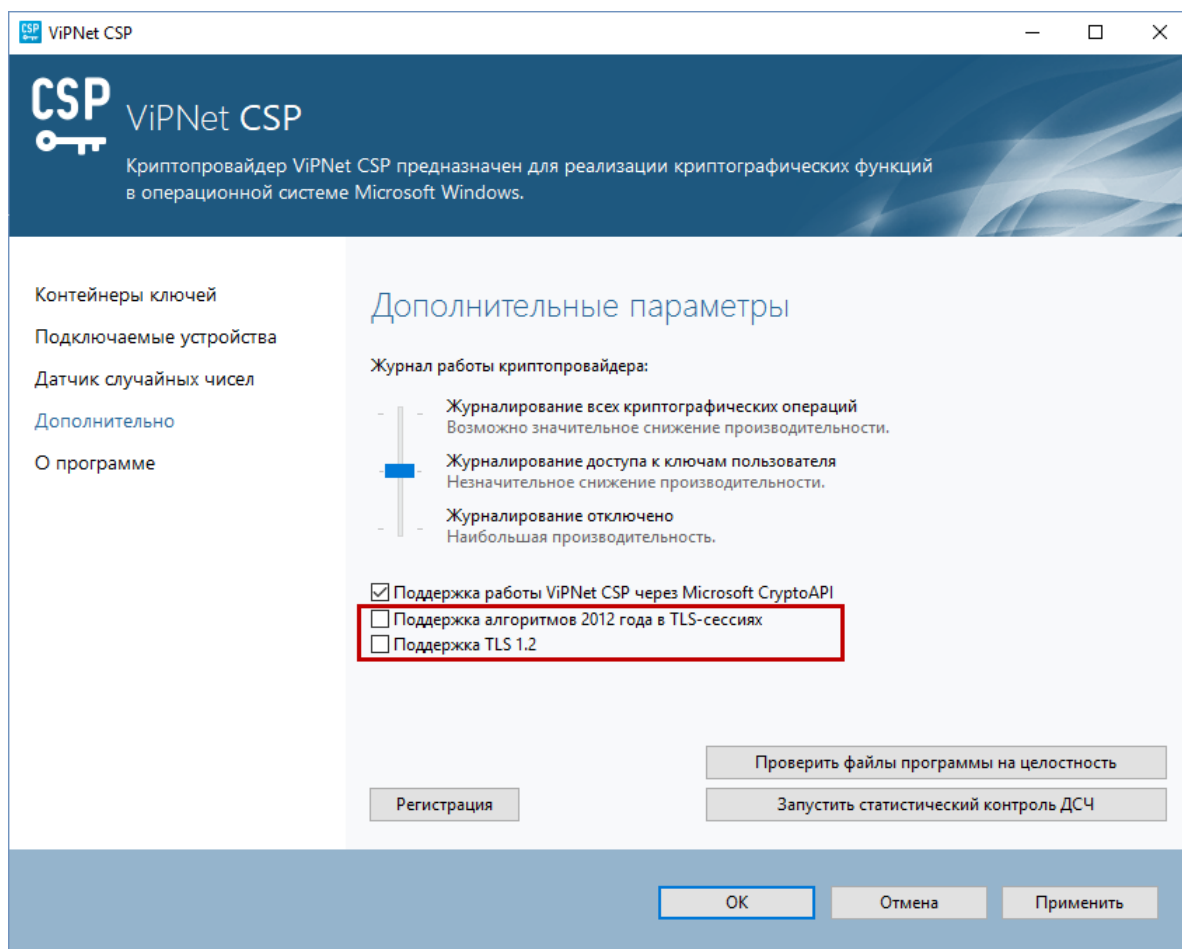


Рисунок 90. Отключение поддержки протокола TLS 1.2

- 2 Снимите флажки **Поддержка алгоритмов 2012 года в TLS-сессиях** и **Поддержка TLS 1.2**.
- 3 В окне **Свойства обозревателя (Свойства браузера)** вашего браузера Internet Explorer снимите флажок **Использовать TLS 1.2** и установите флажки **TLS 1.0**, **Использовать TLS 1.1** (см. [Настройка веб-браузера Internet Explorer для работы по протоколу TLS](#)).
- 4 Закройте программы перезагрузите компьютер.

Попробуйте снова организовать TLS-соединение.

Не установлены сертификаты пользователя, издателя, CRL в нужное хранилище

Проверьте корректность установки сертификатов в хранилище с помощью стандартной консоли MMC (Microsoft Management Console).

Чтобы просмотреть сертификаты, установленные в хранилище, выполните следующие действия:

- 1 Откройте консоль MMC:
 - 1.1 Выберите **Пуск > Выполнить** или нажмите **Win+R**.

1.2 В поле **Открыть** введите mmc и нажмите **ОК**.

2 В меню **Файл** окна консоли выберите **Добавить или удалить оснастку**.

3 В окне **Добавление и удаление оснастки** в списке **Доступные оснастки** выберите оснастку **Сертификаты** и нажмите **Добавить**.

4 В окне **Оснастка диспетчера сертификатов** выберите нужный тип оснастки:

- **моей учетной записи пользователя** — для просмотра сертификатов веб-клиента;
- **учетной записи компьютера** — для просмотра сертификатов сервера.



Примечание. Чтобы не добавлять оснастку **Сертификаты** в консоль каждый раз, когда она вам понадобится, вы можете сохранить консоль. Для этого в меню **Консоль** выберите пункт **Сохранить**.

Сертификаты пользователя, издателя и список CRL должны быть установлены в нужное хранилище, и при их открытии не должно возникать ошибок.

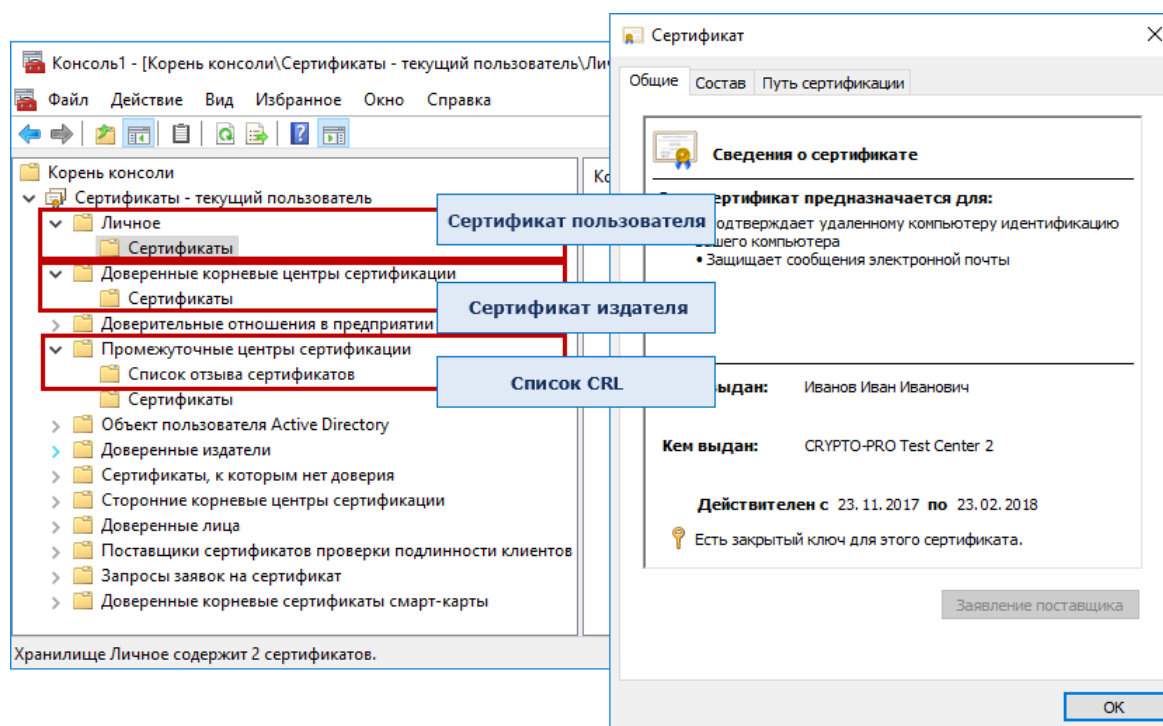


Рисунок 91. Сертификат веб-клиента в хранилище сертификатов текущего пользователя

Для сервера IIS в оснастке MMC сертификатов локального компьютера должны присутствовать следующие сертификаты:

- Раздел **Личные** > **Сертификаты** — сертификат пользователя (сервера).
- Раздел **Доверенные корневые центры сертификации** > **Сертификаты** — сертификат издателя.
- Раздел **Промежуточные центры сертификации** > **Список отзыва сертификатов** — список CRL.

Для веб-клиента в оснастке MMC сертификатов текущего пользователя должны присутствовать следующие сертификаты:

- Раздел **Личные > Сертификаты** — сертификат пользователя (веб-клиента).
- Раздел **Доверенные корневые центры сертификации > Сертификаты** — сертификат издателя.
- Раздел **Промежуточные центры сертификации > Список отзыва сертификатов** — список CRL.

Если сертификат не установлен или установлен некорректно, выполните установку сертификата в хранилище (см. [Установка сертификата издателя и списка аннулированных сертификатов](#)).

Веб-браузер не настроен на работу по протоколу TLS

Если после соответствующей настройки веб-браузера (см. [Настройка веб-браузера Internet Explorer для работы по протоколу TLS](#)) соединения с сервером не происходит, выполните следующие действия:

- Проверьте наличие нужного сертификата.
- Убедитесь, что в свойствах обозревателя разрешено использование протокола TLS (см. [Настройка веб-браузера Internet Explorer для работы по протоколу TLS](#)).

Для проверки наличия сертификата выполните следующие действия:

- 1 В меню **Сервис** веб-браузера Internet Explorer выберите **Свойства обозревателя (Свойства браузера)**.
- 2 В окне **Свойства обозревателя (Свойства браузера)** откройте вкладку **Содержание** и нажмите **Сертификаты**.
- 3 В окне **Сертификаты** откройте вкладку **Личное** и проверьте, что в списке сертификатов присутствует нужный.
- 4 Выберите нужный сертификат и нажмите **Просмотр**.
- 5 В окне **Сертификат** убедитесь, что сертификат содержит расширение **Проверка подлинности клиента**. Если такой атрибут отсутствует, обратитесь в удостоверяющий центр за сертификатом, в котором будет указан данный параметр.

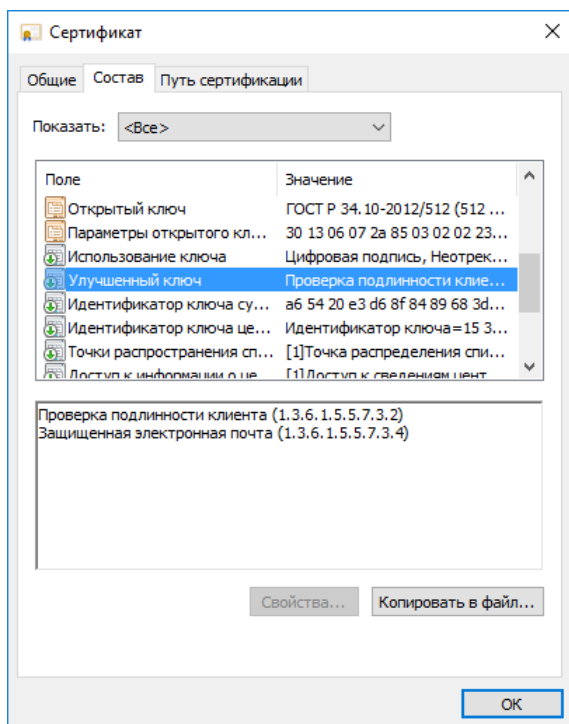


Рисунок 92. Состав сертификата веб-клиента

Требуется перезапуск службы сервера IIS

В некоторых случаях для доступа к серверу по вновь настроенному протоколу TLS необходимо перезапустить службу сервера. Для этого выполните следующие действия:

- 1 Откройте окно **Диспетчер задач Windows**.
- 2 Остановите службу `inetinfo.exe`.
- 3 После того как служба автоматически запустится, проверьте подключение к серверу.

Требуется сохранить пароль к сертификату сервера

Для доступа к серверу необходимо сохранить пароль к контейнеру ключей. Для этого выполните следующие действия:

В окне ViPNet CSP в разделе **Контейнеры ключей** выберите контейнер ключей, пароль к которому требуется сохранить, и нажмите **Свойства**.

- 1 В окне **Свойства контейнера ключей** нажмите **Проверить**.
- 2 В окне **ViPNet CSP - пароль контейнера ключей** укажите пароль к контейнеру ключей и выберите **Сохранить пароль**.

В результате пароль к контейнеру ключей будет сохранен на компьютере.

На компьютере установлен антивирус Kaspersky Internet Security

Если на вашем компьютере помимо ViPNet CSP установлен антивирус Kaspersky Internet Security 2017, TLS-соединение может блокироваться антивирусом. Чтобы блокировка соединения не происходила, выполните следующие действия:

- 1 В области уведомлений Windows щелкните правой кнопкой мыши значок  **Kaspersky Internet Security**.
- 2 В контекстном меню выберите пункт **Настройка**.
- 3 В окне **Настройка** перейдите в раздел **Дополнительно** и на правой панели нажмите **Сеть**.

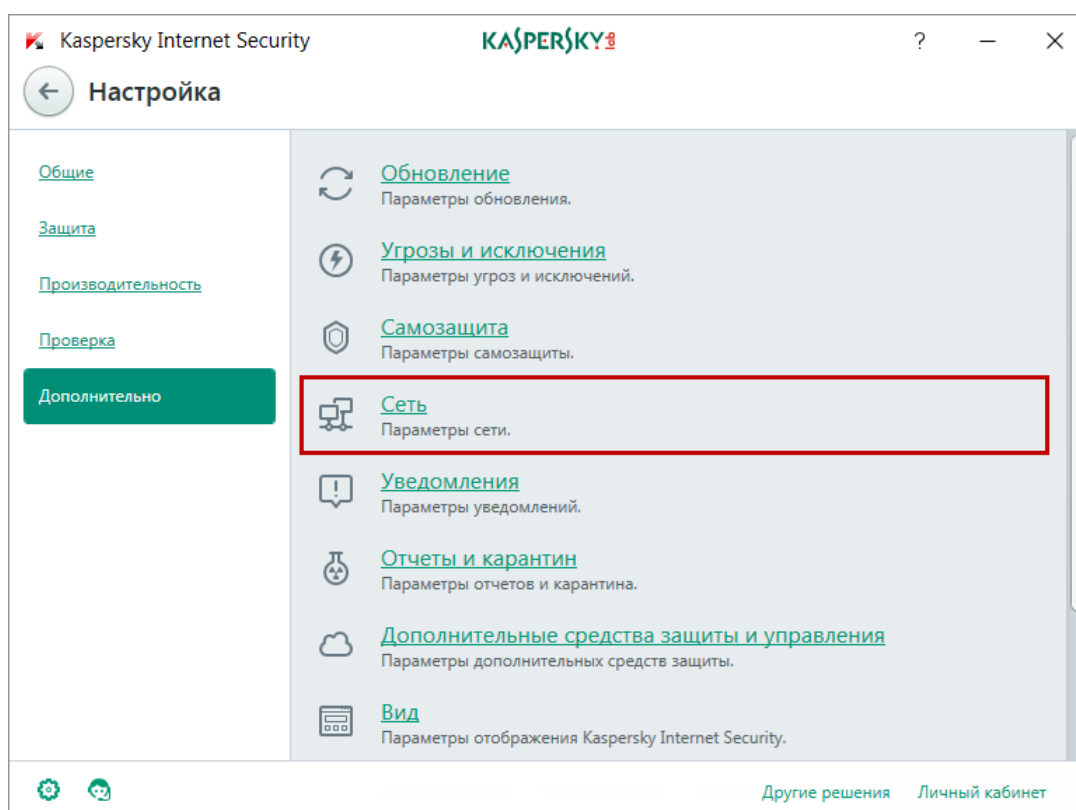


Рисунок 93. Начало настройки антивируса Kaspersky Internet Security для обеспечения совместной работы с ViPNet CSP

- 4 В окне **Параметры сети** снимите флажок **Внедрять в трафик скрипт взаимодействия с веб-страницами** и выберите **Не проверять защищенные соединения**.

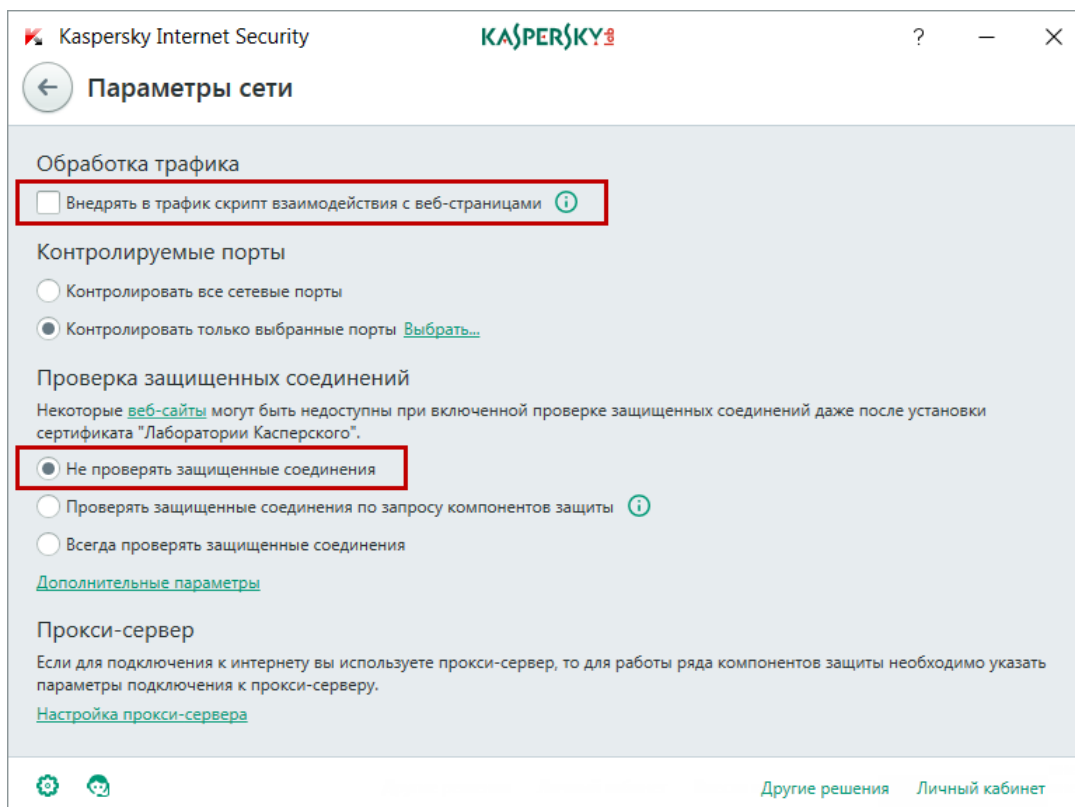


Рисунок 94. Настройка антивируса Kaspersky Internet Security для обеспечения совместной работы с ViPNet CSP

Попробуйте снова организовать TLS-соединение.

После обновления Windows пропало соединение по протоколу TLS

После установки некоторых пакетов обновлений операционной системы Windows работа ViPNet CSP по протоколу TLS может быть прекращена.

В этом случае запустите установочный файл программы и выполните восстановление ее компонентов.

После обновления ViPNet CSP пропало TLS-соединение, организованное с помощью стороннего ПО

Проблема может возникнуть при следующих начальных условиях:

- на вашем компьютере с помощью стороннего программного обеспечения (например, КриптоПро CSP) организовано защищенное соединение по протоколу TLS;
- на вашем компьютере установлена программа ViPNet CSP 4.2.2 или более ранней версии.

Если при этом после обновления ViPNet CSP до текущей версии TLS-соединение перестало функционировать, вам необходимо восстановить программное обеспечение, с помощью которого было установлено это защищенное соединение. Например, в случае программы КриптоПро CSP, запустите установочный файл этой программы и выполните процедуру восстановления.

Не удается подключиться к центру сертификации Microsoft CA по протоколу HTTP

Для удаленного доступа к серверу, на котором развернут центр сертификации Microsoft CA с интегрированным ViPNet CSP (см. [Интеграция ViPNet CSP с центром сертификации на базе Microsoft CA](#)), по протоколу HTTPS пользователю не требуется выполнять каких-либо дополнительных настроек.

Для удаленного доступа к серверу, на котором развернут центр сертификации Microsoft CA с интегрированным ViPNet CSP, по протоколу HTTP:

- 1 Запустите веб-браузер Internet Explorer.
- 2 В окне **Свойства браузера** на вкладке **Безопасность**:
 - Нажмите **Сайты** и добавьте веб-сайт с центром сертификации в зону **Надежные сайты**.
 - Нажмите **Другой** и в окне **Параметры безопасности - зона надежных сайтов** для параметра **Использование элементов управления ActiveX, не помеченных как безопасные для использования** установите переключатель в положение **Включить**.

При соединении с сервером выводится предупреждение системы безопасности

При попытке соединения с сервером в веб-браузере могут появляться предупреждения системы безопасности.

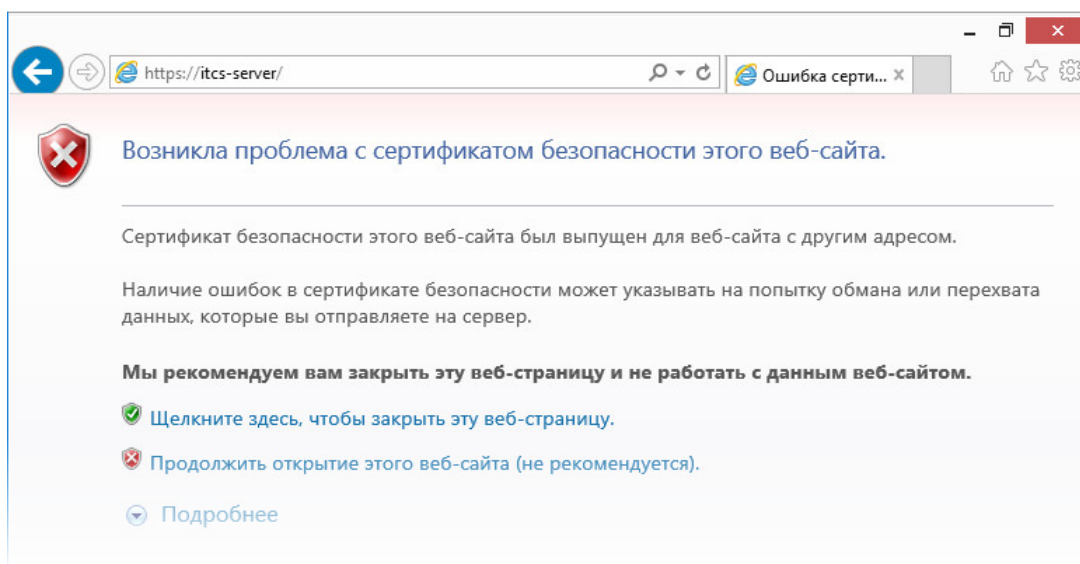
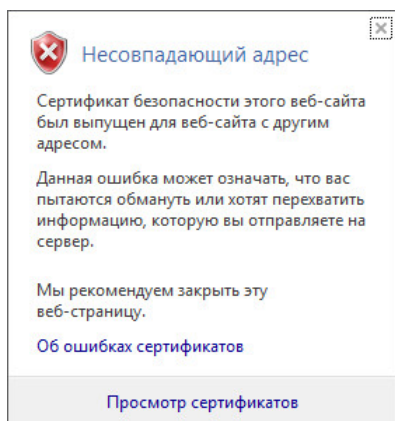


Рисунок 95. Предупреждения о несоответствии доменного имени сервера и имени владельца сертификата сервера

В этом случае проверьте, что доменное имя сервера и имя пользователя, на которое выдан сертификат сервера, совпадают.

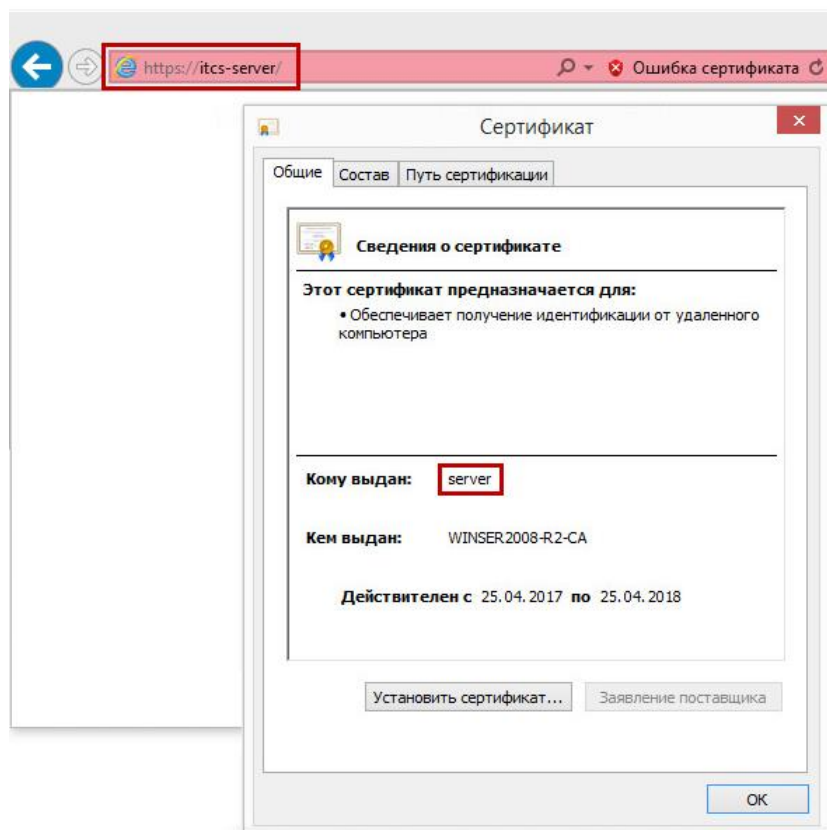


Рисунок 96. Проверка соответствия доменного имени сервера и имени владельца сертификата сервера

Аварийная остановка ViPNet CSP при одновременном использовании нескольких внешних устройств

Подобная неполадка может возникнуть из-за конфликта драйверов для внешних устройств eToken или JaCarta с драйверами для других поддерживаемых внешних устройств.

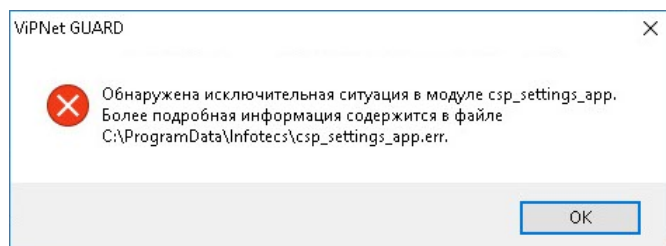


Рисунок 97. Ошибка при одновременном использовании нескольких внешних устройств

Аварийная остановка программы может произойти при одновременном выполнении следующих условий:

- На вашем компьютере установлены драйверы для внешнего устройства eToken или JaCarta, а также драйверы для хотя бы одного другого поддерживаемого внешнего устройства.
- В ViPNet CSP в списке опрашиваемых устройств включено использование нескольких внешних устройств, в том числе eToken или JaCarta.

Чтобы устранить неполадку, в главном окне ViPNet CSP в разделе **Подключаемые устройства** отключите использование всех типов устройств, кроме требуемого (см. [Настройка списка опрашиваемых устройств](#)).

Не удастся подключиться к компьютеру с ViPNet CSP по протоколу RDP

Указанная проблема может быть вызвана конфликтом с обновлением Windows [KB2919355](#).

Для решения проблемы восстановите установленные компоненты ViPNet CSP.

Проверка целостности файлов программы

При необходимости вы можете проверить целостность файлов программы. Для этого выполните следующие действия:

- 1 В окне **ViPNet CSP** перейдите в раздел **Дополнительно**.
- 2 Нажмите **Проверить файлы программы на целостность**.

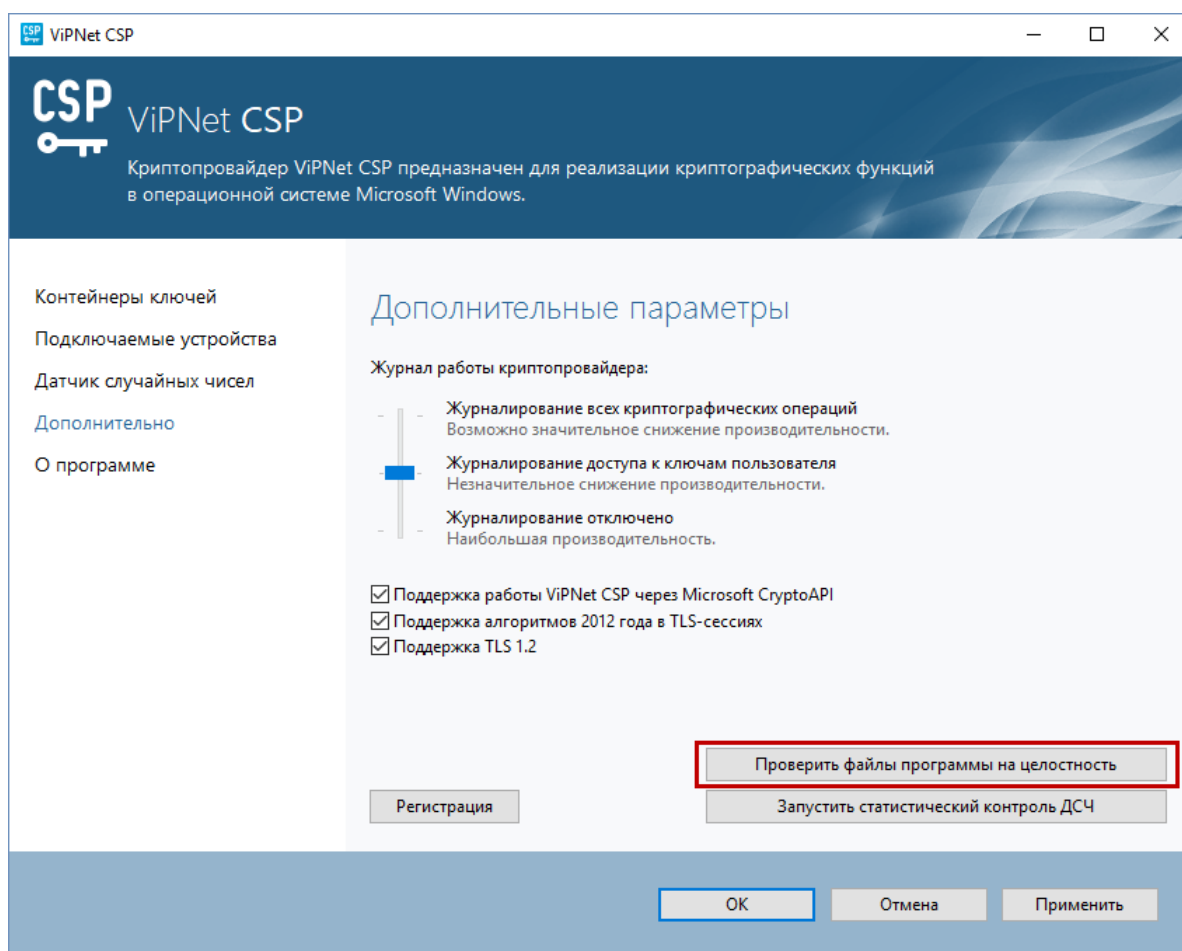


Рисунок 98. Проверка целостности файлов программы

При этом произойдет пересчет контрольных сумм и проверка их соответствия суммам, указанным в каждом из файлов программы.

По окончании проверки отобразится окно с сообщением о результатах проверки. В случае несоответствия контрольным суммам восстановите компоненты программы.

Статистический контроль датчиков случайных чисел программы

Для проведения статистического контроля датчиков случайных чисел программы:

- 1 В окне **ViPNet CSP** перейдите в раздел **Дополнительно**.
- 2 Нажмите **Запустить статистический контроль ДСЧ**.

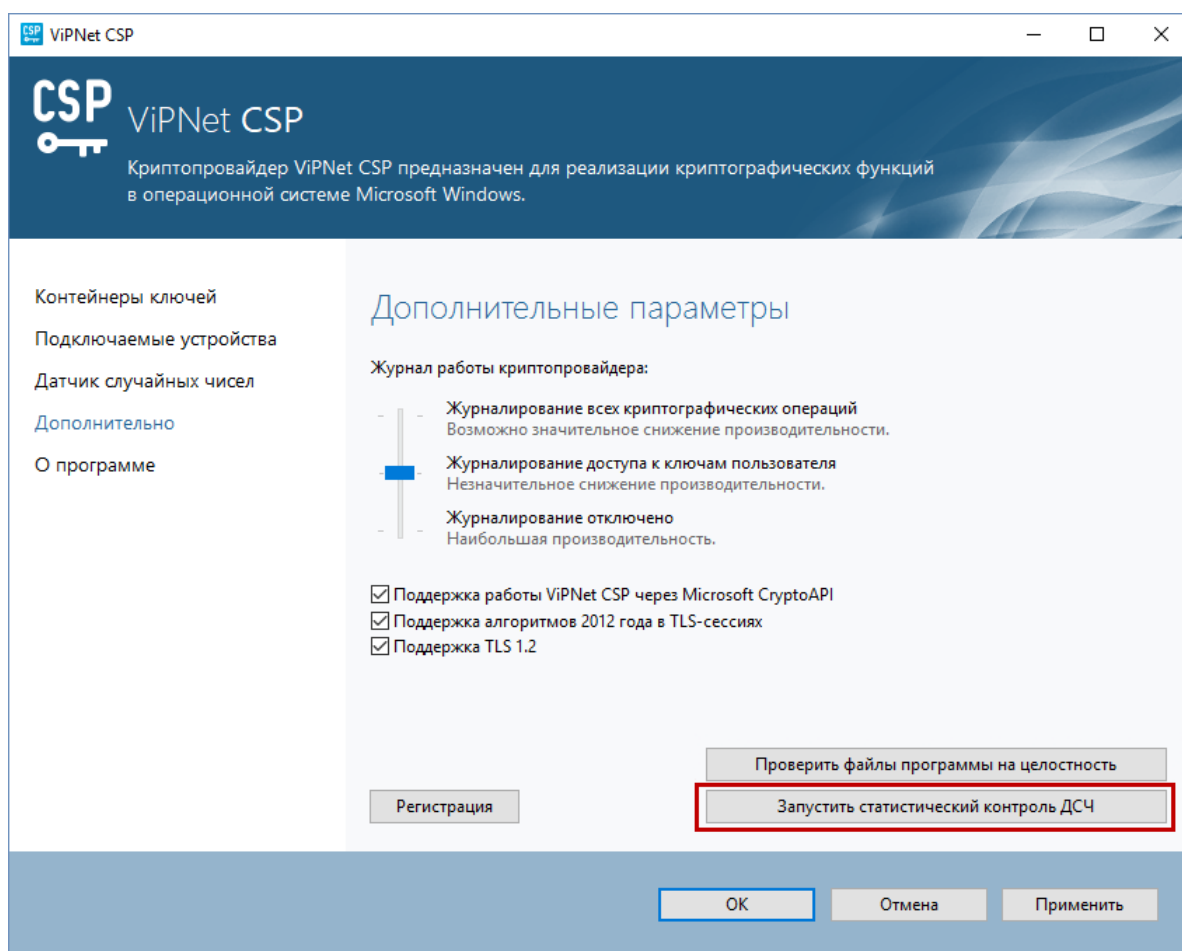


Рисунок 99. Проверка целостности файлов программы

Восстановление системных файлов и параметров ОС Windows после неудачной установки ViPNet CSP

Если после установки ViPNet CSP ваш компьютер перестал загружаться либо если операционная система начала циклически перезагружаться, верните операционную систему в состояние, предшествующее установке ViPNet CSP с помощью точки восстановления, созданной во время установки программы. Например, если вы используете ОС Windows 10, выполните следующие действия:

- 1 Подключите к компьютеру накопитель с дистрибутивом операционной системы, установленной на вашем компьютере.
- 2 В программе настройки BIOS выберите в качестве загрузочного носителя подключенный носитель и перезагрузите компьютер.
- 3 В окне **Установка Windows** при необходимости измените предлагаемые параметры ввода и нажмите **Далее**.

- 4 Нажмите **Восстановление системы**.

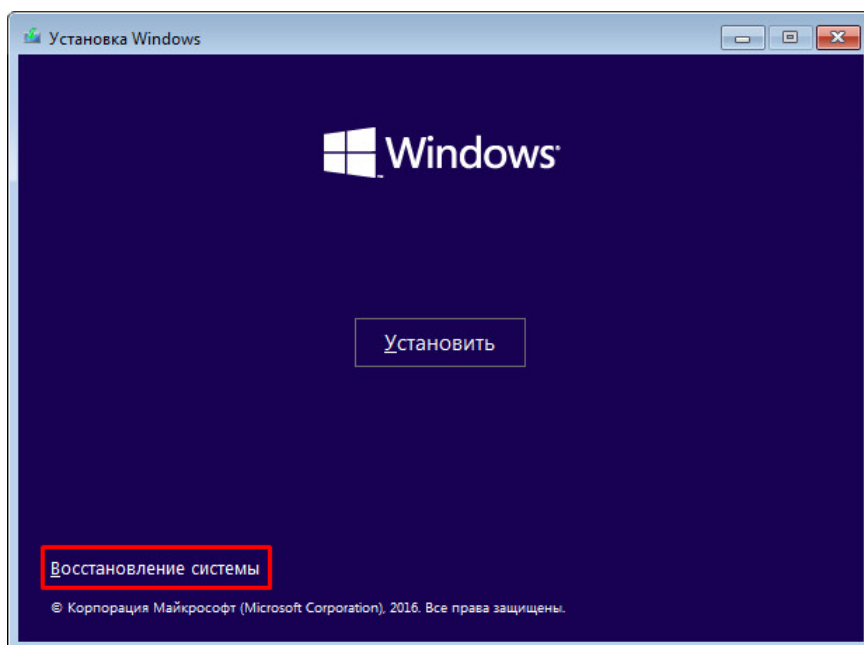


Рисунок 100. Запуск Windows для восстановления системы

- 5 На странице **Выбор действия** нажмите **Поиск и устранение неисправностей**.
6 На странице **Дополнительные параметры** нажмите **Восстановление системы**.

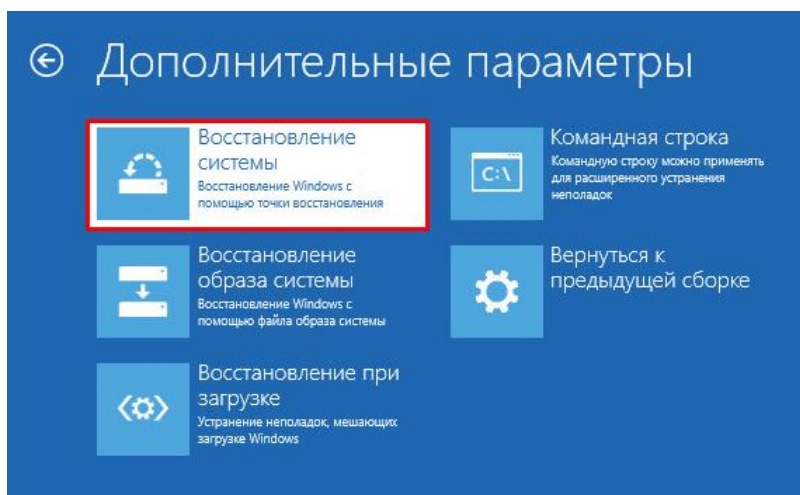


Рисунок 101. Выбор способа восстановления системы

- 7 На страницах мастера **Восстановление системы** выберите необходимую точку восстановления и подтвердите восстановление системы.

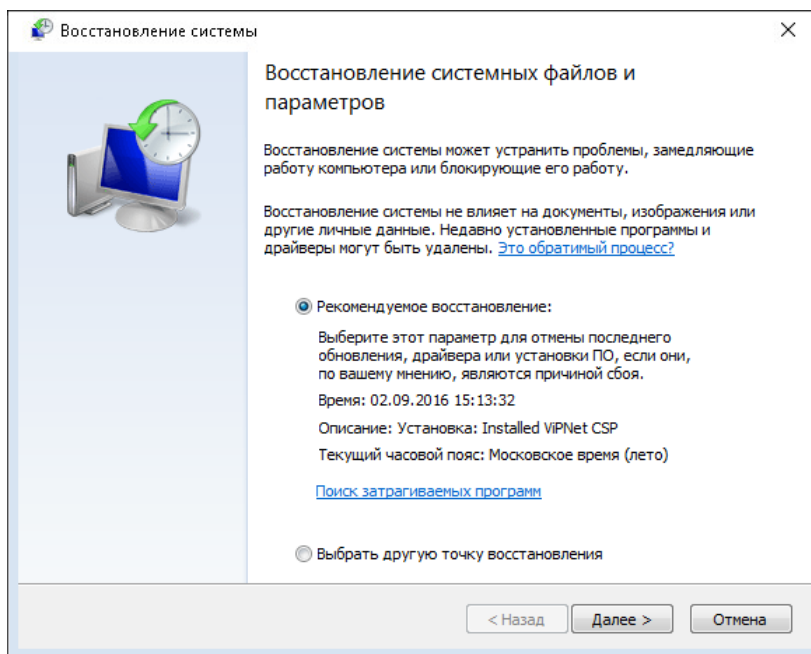


Рисунок 102. Выбор точки восстановления

По окончании восстановления компьютер перезагрузится.

Повторная регистрация для устранения неполадок

Для устранения некоторых неполадок может потребоваться повторная регистрация ViPNet CSP. В этом случае сотрудник технической поддержки АО «ИнфоТекС» предоставит вам новый серийный номер. Чтобы заново зарегистрировать программу:

- 1 В окне **ViPNet CSP** перейдите в раздел **Дополнительно**.
- 2 Нажмите **Регистрация**. Откроется окно мастера **Регистрация ViPNet CSP**.

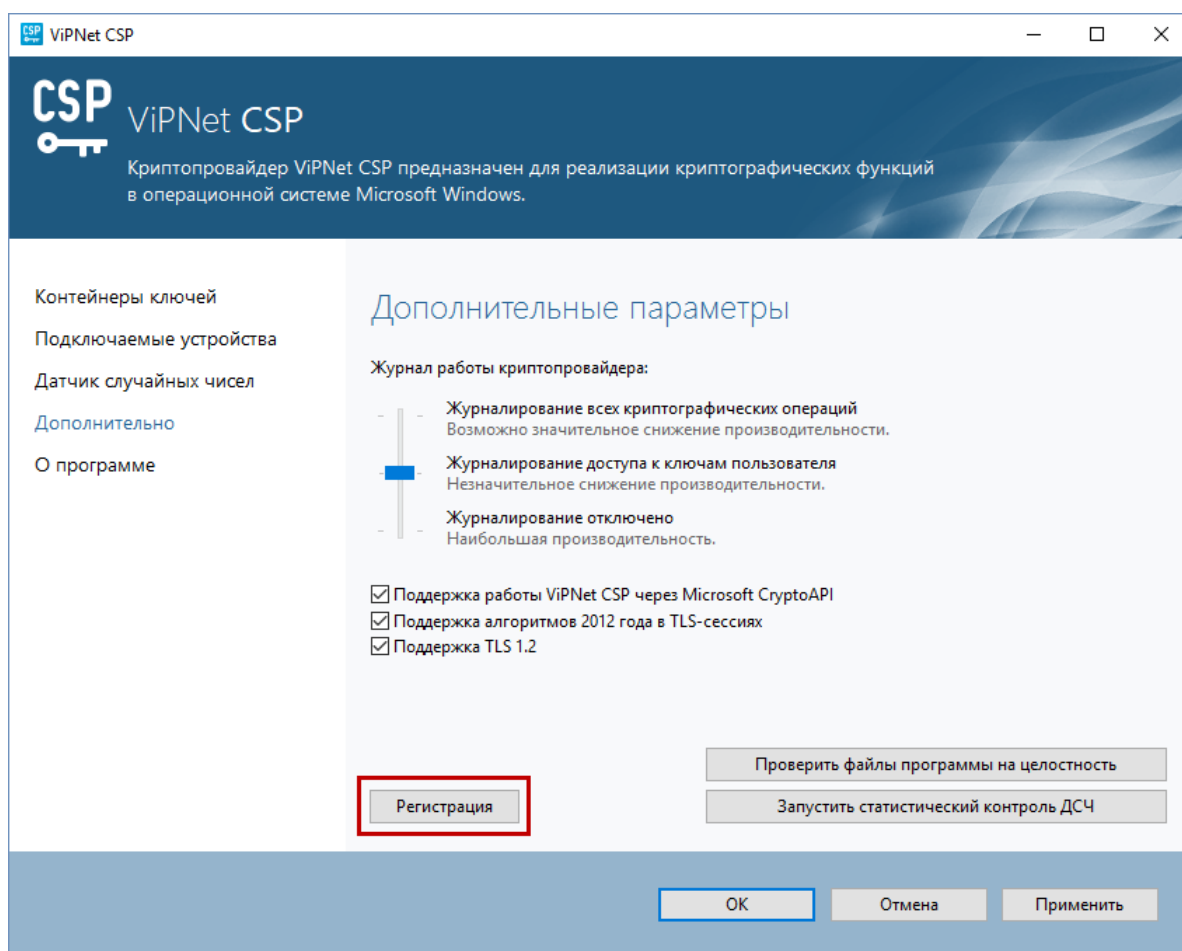


Рисунок 103. Запуск мастера регистрации

- 3 Повторно зарегистрируйте программу с помощью нового серийного номера, следуя инструкциям из раздела [Регистрация ViPNet CSP](#).

После обновления ViPNet CSP исчезли ранее сохраненные пароли контейнеров ключей

При обновлении ViPNet CSP с версии 4.2.11 на версию 4.4 или более позднюю не сохраняются сохраненные пароли контейнеров ключей, находящихся в папках хранения ключей пользователей (см. [Общая информация о ключах и сертификатах](#)).

При этом сохраняются пароли для контейнеров ключей, расположенных в папке хранения ключей компьютера. Также сохраняются ПИН-коды системных контейнеров, хранящихся на устройствах (как аппаратных, так и программных токенах), которые будут корректно использоваться при обращении системных служб и сервисов.

Однако при этом в **Панели управления ViPNet CSP** сохраненные пароли или ПИН-коды отображаться не будут. Пользователю также понадобится ввести пароль для зашифрования или

подписания файла с помощью сертификата из контейнера, расположенного в папке хранения ключей компьютера.

Для восстановления паролей необходимо заново сохранить их (см. [Операции с контейнерами ключей](#)).

Предоставление дополнительной информации о неисправности

Для устранения неисправности сотрудник технической поддержки АО «ИнфоТеКС» может попросить вас предоставить дополнительную информацию для анализа.

Если неисправность возникает на этапе установки или обновления программы, выполните следующие действия:

1 Откройте папку:

`C:\ProgramData\InfoTeCS\InstallerData\ViPNet CSP\Logs`

2 Добавьте находящиеся в папке файлы журнала в архив и отправьте вместе с описанием неисправности в [службу технической поддержки](#).

Если неисправность возникает во время работы программы:

1 Откройте консоль MMC:

- Нажмите сочетание клавиш **Win+R**.
- В меню **Пуск** выберите **Выполнить**.
- В поле **Открыть** введите команду `regedit` и нажмите клавишу **Enter**.

2 В программе «Редактор реестра» перейдите в раздел `Logs`, который находится по следующему пути:

- в 32-разрядных операционных системах Windows:
`HKEY_LOCAL_MACHINE\SOFTWARE\Itcs\Logs;`
- в 64-разрядных операционных системах Windows:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Itcs\Logs.`

3 Измените значения ключей `level` на `0xff` (255) в указанных сотрудником поддержки подразделах.

4 Перезагрузите компьютер.



Примечание. В некоторых случаях запуск компьютера может занять более продолжительное время, чем обычно.

5 Нажмите сочетание клавиш **Win+R**.

В меню **Пуск** также можно выбрать пункт **Выполнить**.

- 6 В поле **Открыть** введите команду `msinfo32` и нажмите клавишу **Enter**.
- 7 В программе «Сведения о системе» в меню **Файл** выберите пункт **Сохранить**.
- 8 Сохраните файл NFO с произвольным именем.
- 9 Скачайте программу [DebugView](#).
- 10 Запустите файл `DbgView.exe` от имени администратора.
- 11 В меню **Capture** установите флажки напротив всех пунктов, кроме **Log Boot**.
- 12 Повторите действия, при которых у вас возникала неисправность.
- 13 В программе DebugView выделите все записи и скопируйте в текстовый файл.
- 14 Добавьте получившийся текстовый файл и файл NFO, сохраненный на шаге 9, в архив и отправьте вместе с описанием неисправности в [службу технической поддержки](#).



Примечание. Если для воспроизведения ошибки необходимо стороннее ПО, укажите это в письме.

Присвойте измененным ключам `level` (см. пункт 4) значение `0x10` (16).

- 15 Перезагрузите компьютер.

В

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения [контейнеров ключей](#), которые вы можете использовать для аутентификации, формирования [электронной подписи](#) или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объема памяти устройства.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP. Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

Таблица 4. Поддерживаемые внешние устройства

Название семейства устройств в ViPNet CSP	Типы и полные названия устройств	Условия и особенности использования семейства устройств
ESMART Token	Смарт-карты и токены типов: • ESMART Token 64K, • ESMART Token ГОСТ, • ESMART Token 192K.	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.13.2). Устройства типа ESMART Token необходимо отформатировать с помощью ПО ESMART PKI Client для Windows с профилем ViPNet2. Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом
Infotecs Software Token	ViPNet SoftToken — программная реализация стандарта PKCS#11.	На компьютере должен быть установлен компонент ViPNet SoftToken (входит в состав ПО ViPNet OpenSSL). С помощью программы <code>token_manager.exe</code> должен быть создан программный токен. Подробнее см. в документе «ViPNet SoftToken. Руководство разработчика» > «Использование утилиты <code>token_manager</code> для работы с программными токенами»
SafeNet eToken (eToken Aladdin)	Персональные электронные ключи и смарт-карты производства компаний Gemalto (SafeNet) и «Аладдин Р.Д.»: • Gemalto SafeNet eToken 5100/5105, 5200/5205, 7300, • eToken PRO, • eToken NG-OTP, NG-FLASH, • eToken 5300, • SafeNet eToken 5110, • Gemalto SafeNet eToken 4100.	На компьютере с Windows 10 должен быть установлен SafeNet Authentication Client (рекомендуемая версия — 10.6.146). На компьютере с другой ОС — PKI Client версии 5.1 SP1 или SafeNet Authentication Client (рекомендуемая версия — 10.6.146). Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт. Примечание. Установка «Единый Клиент JaCarta» и SafeNet Authentication Client на один компьютер не рекомендуется производителем. Это может вызвать ошибки при выполнении криптографических операций с использованием устройств из семейства SafeNet eToken (eToken Aladdin)

Название семейства устройств в ViPNet CSP	Типы и полные названия устройств	Условия и особенности использования семейства устройств
ViPNet HSM	Программно-аппаратный комплекс ViPNet HSM 3.3 производства АО «ИнфоТеКС».	На компьютере должно быть установлено ViPNet HSM SDK. В ViPNet CSP необходимо задать параметры подключения к серверу ViPNet HSM (см. Настройка взаимодействия с ViPNet HSM)
JaCarta	Персональные электронные ключи и смарт-карты производства компании «Аладдин Р.Д.»: • JaCarta-2 SE, • JaCarta-2 SF, • JaCarta SF/ГОСТ, • JaCarta-2 SE/PKI/ГОСТ, • JaCarta-2 PKI/BIO/ГОСТ, • JaCarta PKI/BIO, • JaCarta PKI, • JaCarta LT, • JaCarta PKI/ГОСТ, • JaCarta PRO, • JaCarta-2 PKI/ГОСТ, • JaCarta-2 ГОСТ, • JaCarta-2 PRO/ГОСТ.	Рекомендуемая версия прошивки для устройств JaCarta-2 — 2.5.5. На компьютере должно быть установлено ПО «Единый Клиент JaCarta 3.0» компании «Аладдин Р.Д.» Рекомендуемая минимальная версия — 3.0.0 (сборка 3300). Перенос ключей подписи с апплетов «Криптотокен» и «Криптотокен 2 ЭП» (модели JaCarta со словом «ГОСТ» в названии) и на эти апплеты невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. Работа с апплетом PRO через ПО «Единый Клиент JaCarta» версии 2.12 не поддерживается. Необходимо установить последнее обновление ПО «Единый Клиент JaCarta» с сайта производителя либо обратиться в службу поддержки компании «Аладдин Р.Д.»
Rutoken	Электронные идентификаторы производства компании «Актив»: • Рутокен ЭЦП 2.0 Flash, • Рутокен ЭЦП 2.0 Touch, • Рутокен ЭЦП 2.0, • Рутокен ЭЦП 2.0 3000, • Рутокен Lite, • Рутокен ЭЦП PKI (2.0), • Рутокен ЭЦП 2.0 2100, • Рутокен ЭЦП 3.0 (NFC) 3100, • Рутокен ЭЦП 3.0 3220.	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.16.0.0). Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП 2.0 невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом

Название семейства устройств в ViPNet CSP	Типы и полные названия устройств	Условия и особенности использования семейства устройств
Rutoken S	Электронные идентификаторы Рутокен S производства компании «Актив».	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.16.0.0)
Foros	Смарт-карты и токены R301 Foros для ViPNet CSP производства компании «СмартПарк».	На компьютере должен быть установлен драйвер ForosMaster (рекомендуемая версия — 1.0.0.19). Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом



Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств см. на официальном сайте производителя этого устройства.

Алгоритмы и функции, поддерживаемые внешними устройствами

Таблица 5. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств в ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Работа с ДСЧ в ViPNet CSP	Поддержка PKCS#11
ESMART Token	ESMART Token — отсутствует; ESMART Token ГОСТ — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	ESMART Token — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 ESMART Token ГОСТ — отсутствует	Да	Да
Infotecs Software Token	Изолированная программная реализация: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012		Нет	Да
SafeNet eToken (eToken Aladdin)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да
JaCarta (устройства JaCarta PKI, JaCarta SE, JaCarta LT, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом Laser, JaCarta PRO)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

Название семейства устройств в ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Работа с ДСЧ в ViPNet CSP	Поддержка PKCS#11
JaCarta (устройства JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом ГОСТ, JaCarta-2 ГОСТ)	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	Да	Да
Rutoken	Рутокен ЭЦП 2.0 — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012; Рутокен Lite — отсутствует	Рутокен ЭЦП 2.0 — отсутствует; Рутокен Lite — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	ЭЦП 2.0 — да; Lite — нет	Да
Rutoken S	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

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

Выработка ключей шифрования (функция `C_DeriveKey` интерфейса PKCS#11) поддерживается не всеми перечисленными устройствами. Для получения более подробной информации см. документацию к устройству.



История версий

В приложении описаны основные изменения в предыдущих версиях ViPNet CSP.

Версия 4.4.8

- **Расширение списка поддерживаемых внешних устройств**
Добавлена совместимость с устройствами Rutoken 3.0 3220.
- **Отображение срока действия ключей**
Теперь срок действия ключа отображается в интерфейсе ViPNet CSP.
- **Изменения в интерфейсе**
На контрольную панель ViPNet CSP добавлен новый логотип.
- **Расширение списка поддерживаемых ОС**
Реализована поддержка новых версий и сборок Windows Server.
- **Исправление ошибок**
В версии 4.4.8 исправлены ошибки, выявленные в процессе эксплуатации версии 4.4.6.

Версия 4.4.6

- **Поддержка новых версий Windows**
Реализована поддержка новых версий и сборок Windows 10 и Windows 11.
- **Изменения в интерфейсе**
Для продукта создана новая иконка.

- **Обновление процедуры проведения автоматической регистрации**
- **Расширение списка поддерживаемых внешних устройств**

В новой версии ViPNet CSP реализована совместимость с устройствами Рутокен ЭЦП 2.0 3000, 3.0 3100.

- **Исключение устройств aKey из списка поддерживаемых внешних устройств**
- **Поддержка новых драйверов для внешних устройств**
- **Поддержка работы с контейнерами ключей из стороннего ПО**

Обеспечена работа ViPNet CSP с контейнерами, созданными в ПО производителей поддерживаемых внешних устройств.

- **Исправление ошибок**

В версии 4.4.6 исправлены ошибки, выявленные в процессе эксплуатации версии 4.4.4.

Версия 4.4.4

- **Поддержка новых версий Windows**

Реализована поддержка операционной системы Windows 11 (включая обновление KB5009566) и Windows 10 (обновления KB5009543).

- **Улучшение совместимости с ПО КриптоПро**

Устранены проблемы, возникавшие при совместной работе ViPNet CSP и ПО КриптоПро.

- **Исправление ошибок**

В версии 4.4.4 исправлены ошибки, выявленные в процессе эксплуатации версии 4.4.2.

Версия 4.4.2

- **Поддержка новых версий Windows**

Реализована поддержка операционных систем:

- Windows 10 версия 20H2, сборка 19042;
- Windows Server 2019 версия 1809, сборка 17763.

Из списка поддерживаемых ОС исключены:

- Windows 10 версия 1703, сборка 15063;
- Windows 10 версия 1511, сборка 10586.

- **Доработки для соответствия приказу ФСБ №795**

ViPNet CSP доработан для выполнения требований приказа ФСБ РФ от 27 декабря 2011 г. № 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки

электронной подписи" и позволяет формировать ЭП, соответствующую требованиям документа.

- **Установка сертификатов ГУЦ**

При установке ViPNet CSP в хранилище сертификатов автоматически устанавливаются корневые сертификаты Головного удостоверяющего центра.

- **Поддержка TLS включена по умолчанию**

Поддержка TLS активируется сразу после установки ViPNet CSP. Производить ручную настройку не требуется.

- **Контроль обновления операционной системы до неподдерживаемой версии**

Если операционная система будет обновлена до версии, не поддерживаемой текущей версией ViPNet CSP, пользователь получит уведомление о необходимости обновить ViPNet CSP.

- **Исключение поддержки ГОСТ Р 34.10-2001**

В соответствии с документом ФСБ России №149/7/1/3-58 от 31.01.2014 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования» ViPNet CSP больше не поддерживает формирование электронной подписи согласно ГОСТ Р 34.10-2001.

- **Исключение поддержки устаревших устройств**

В новой версии программы больше не поддерживаются устаревшие устройства:

- JaCarta GOST;
- eToken GOST;
- Rutoken ECP.

Данные устройства поддерживают только ГОСТ 34.10-2001, применение которого для формирования ЭП не допускается.

- **Изменение юридического адреса и названия компании**

В ПО и документацию внесены изменения в связи с изменением юридического адреса и названия компании. Новое наименование: АО «ИнфоТеКС». Юридический адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29.

- **Исправление ошибок**

В версии 4.4.2 исправлены ошибки, выявленные в процессе эксплуатации версии 4.4.0.

Версия 4.4.0

- **Поддержка новых версий Windows**

Реализована поддержка ОС:

- Windows 10 версия 1909, сборка 18363.

- Windows Server 2019, сборка 17763.
- **Поддержка устройств JaCarta-2**
В новой версии программы ViPNet CSP поддерживаются устройства JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ. Новые устройства сгруппированы в семейство JaCarta.
- **Поддержка устройств R301 Форос PKCS**
В новой версии программы ViPNet CSP поддерживаются устройства R301 Форос PKCS.
- **Изменение состава семейств устройств**
В новой версии программы ViPNet CSP изменился состав следующих семейств устройств:
 - К семейству JaCarta отнесены устройства, ранее входившие в семейства eToken GOST / JaCarta GOST и JCDS.
 - К семейству Rutoken отнесены устройства, ранее входившие в семейство Rutoken ECP / Rutoken Lite.
 - К семейству Rutoken S отнесены устройства, ранее входившие в семейство Rutoken / Rutoken S.
- **Перенос компонента ViPNet SoftToken в состав ПО ViPNet OSSL**
Из состава ViPNet CSP удален компонент ViPNet SoftToken. Для работы с программными токенами компонент ViPNet SoftToken может быть установлен в составе ПО ViPNet OSSL.
- **Изменение работы с ViPNet HSM**
В предыдущих версиях ViPNet CSP настройка производилась в самой программе. Для работы новой версии программы ViPNet CSP с ключами, хранящимися на ПАК [ViPNet HSM](#), необходимо произвести установку и настройку ViPNet HSM SDK (см. [Взаимодействие с ViPNet HSM](#)).
- **Исправление ошибок**
В версии 4.4.0 исправлены ошибки, выявленные в процессе эксплуатации версии 4.2.11.

Версия 4.2.11

- **Улучшение взаимодействия с другими программными продуктами**
В программу ViPNet CSP внесены изменения, затрагивающие взаимодействие с ViPNet Client. Для более подробной информации см. документацию к ViPNet Client версии 4.5.3 и выше. Либо обращайтесь в службу технической поддержки АО «ИнфоТеКС».
- **Исправление ошибок**
В версии 4.2.11 исправлены ошибки, выявленные в процессе эксплуатации версии 4.2.10.

Версия 4.2.10

- **Обновление команд для работы с программными токенами Infotecs Software Token**

В новой версии ViPNet CSP обновлена версия Infotecs Software Token — программной реализации интерфейса PKCS#11. Новые команды для работы с программными токенами см. в документе «ViPNet SoftToken 4.4. Руководство разработчика», раздел «Использование утилиты token_manager для работы с программными токенами».



Внимание! Чтобы продолжить работу с программными токенами, необходимо перед обновлением ПО экспортировать объекты, хранящиеся на программных токенах (ключи, сертификат), в файлы, а после обновления создать новые программные токены и импортировать в них эти объекты. Подробнее см. в документе «ViPNet SoftToken 4.4. Руководство разработчика», раздел «Перенос токенов при обновлении ViPNet SoftToken с версии 4.3 на версию 4.4».

- **Прекращение поддержки универсальных электронных карт (УЭК)**

Так как выпуск и выдача карт УЭК прекращены с 1 января 2017 года, поддержка этих карт в ViPNet CSP также прекращена.

- **Изменения в списке поддерживаемых веб-браузеров**

В связи с тем, что компания Microsoft прекратила поддержку веб-браузера Internet Explorer 10, взаимодействие ViPNet CSP с этим веб-браузером также более не поддерживается.

- **Исправление ошибок**

В версии 4.2.10 исправлены ошибки, выявленные в процессе эксплуатации версии 4.2.9.

Версия 4.2.9

- **Взаимодействие с сервером ViPNet HSM с помощью протокола TLS**

В новой версии программы ViPNet CSP появилась возможность организации защищенного подключения к серверу ViPNet HSM. Для защиты соединения используется протокол TLS, при этом параметры подключения указываются в специальной области окна **Параметры ViPNet HSM** (см. [Настройка взаимодействия с ViPNet HSM](#)).

Параметры ViPNet HSM

Параметры для связи с сервером

IP-адрес: 192 . 168 . 1 . 132

Порт: 9090

☒ Использовать защищенное TLS-соединение с сервером

Идентификатор программного токена: 0

ПИН-код программного токена:

Серийный номер закрытого ключа для аутентификации: 01D07C3B830200000000C150C1

Серийный номер сертификата для аутентификации: 01D07C3DC686B2B00000000115E

Путь к корневому сертификату сервера: C:\oss\ca-2.cer

OK Отмена

Рисунок 104. Настройка параметров TLS-соединения с сервером ViPNet HSM

- **Изменения в списке поддерживаемых операционных систем**

Реализована поддержка ОС Windows Server 2016 (64-разрядная), сборка 14393.

В связи с тем, что компания Microsoft прекратила поддержку операционной системы Windows 8 (32/64-разрядная), работа ViPNet CSP на компьютерах с этой операционной системой также более не поддерживается АО «ИнфоТеКС».

- **Исправление ошибок**

В версии 4.2.9 исправлены ошибки, выявленные в процессе эксплуатации версии 4.2.8.

Версия 4.2.8

- **Изменения в списке поддерживаемых операционных систем**

В криптопровайдере ViPNet CSP частично реализована поддержка операционной системы Windows 10 (32-разрядная и 64-разрядная). Поддерживаются все заявленные криптографические операции, кроме организации защищенных подключений по протоколу TLS в веб-браузере Microsoft Edge.

В связи с тем, что компания Microsoft прекратила общую поддержку операционных систем Windows 2003 (32-разрядная) и Windows Vista (32/64-разрядная), работа ViPNet CSP на компьютерах с этими операционными системами также более не поддерживается АО «ИнфоТеКС». Кроме того, работа ViPNet CSP более не поддерживается на компьютерах с операционной системой Windows Server 2008 (32/64-разрядная).

- **Контроль версии операционной системы Windows при установке ViPNet CSP**

Во избежание появления ошибок ViPNet CSP из-за возможных конфликтов с версиями операционных систем, работа с которыми не была протестирована, установка ViPNet CSP 4.2.8 возможна только на компьютеры под управлением определенных версий (сборок) операционных систем Windows. При попытке установки ViPNet CSP на компьютер под управлением неподдерживаемой версии операционной системы появляется окно с предупреждением и процесс установки прекращается.

- **Создание точки восстановления Windows при установке ViPNet CSP**

Чтобы обеспечить возможность восстановления состояния операционной системы Windows, предшествовавшего установке ViPNet CSP, при установке новой версии ViPNet CSP автоматически создается точка восстановления Windows. Если в настройках Windows отключена функция создания точек восстановления, программа установки ViPNet CSP автоматически включит эту функцию. При этом, в зависимости от настроек восстановления системы, Windows может отменить создание точки восстановления (например, если такая точка в этот день уже создавалась). Использование точек восстановления не поддерживается в серверных версиях Windows (см. [Восстановление системных файлов и параметров ОС Windows после неудачной установки ViPNet CSP](#)).

- **Совместимость ViPNet CSP с системой Microsoft Device Guard**

Драйверы ViPNet CSP были подписаны электронной подписью доверенного издателя WHQL (Windows Hardware Quality Lab). Теперь при проверке программного обеспечения система Microsoft Device Guard, входящая в некоторые версии операционной системы Windows, считает программу ViPNet CSP доверенным приложением и при включенном компоненте Secure Boot не препятствует запуску драйверов ViPNet CSP.

- **Добавление комплекта средств разработки (SDK)**

Вместе с новой версией ViPNet CSP распространяется архив SDK, включающий в себя набор заголовочных файлов и примеры программ.

- **Работа с ключами, находящимися на удаленном сервере ViPNet HSM**

В новой версии программы ViPNet CSP появилась возможность использовать закрытые и открытые ключи, находящиеся на удаленном сервере [ViPNet HSM](#), как если бы эти ключи находились на токене, подключенном к вашему компьютеру. Для этого в списке подключаемых устройств необходимо выбрать пункт **ViPNet HSM** и в специальном окне задать параметры подключения к серверу ViPNet HSM. Подробнее см. в разделе [Взаимодействие с сервером ViPNet HSM](#) (см. [Взаимодействие с ViPNet HSM](#)).

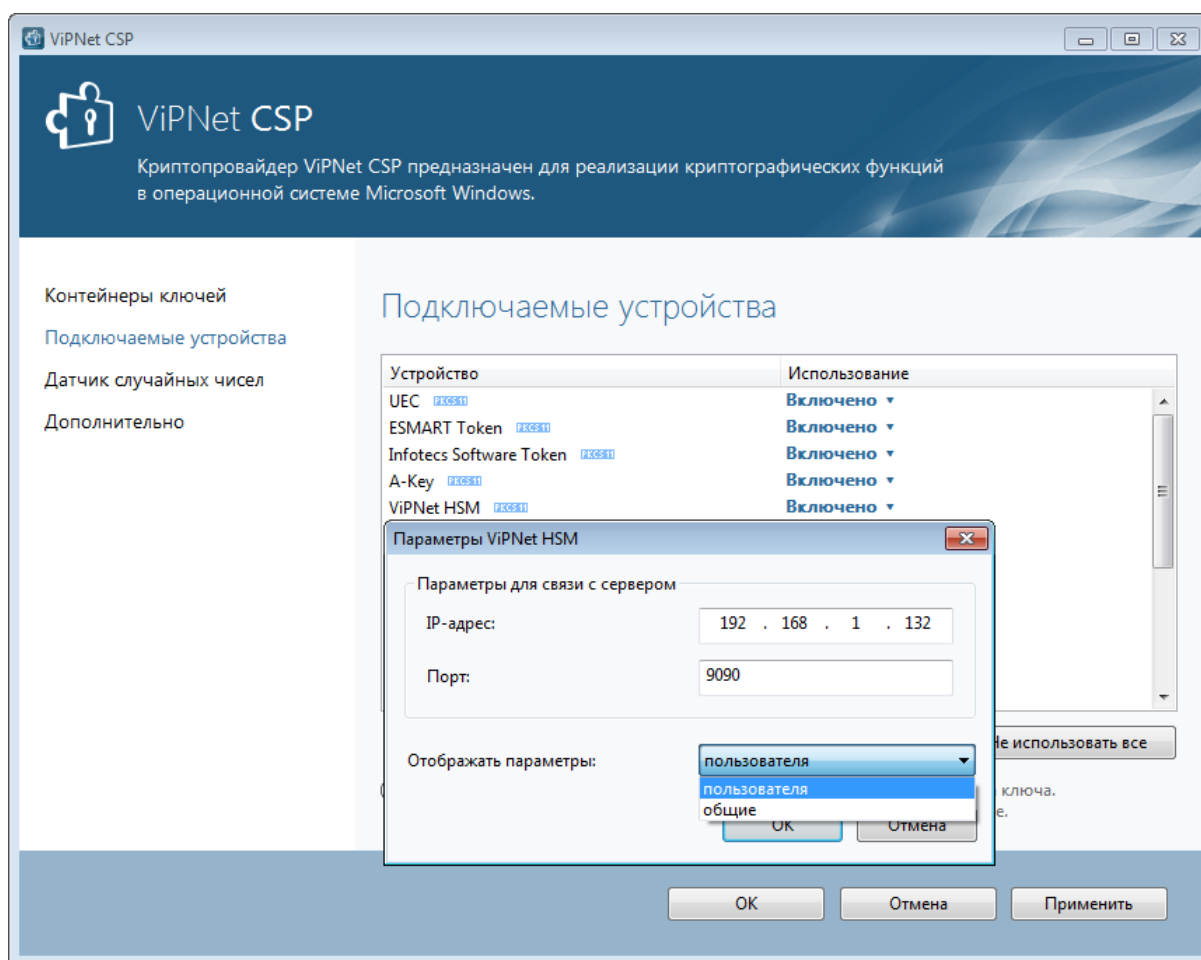


Рисунок 105. Задание параметров подключения к серверу ViPNet HSM

Функции, необходимые для взаимодействия с сервером ViPNet HSM, объединены в отдельный компонент программы ViPNet CSP. При необходимости в процессе установки или после установки ViPNet CSP вы можете отключить этот компонент.

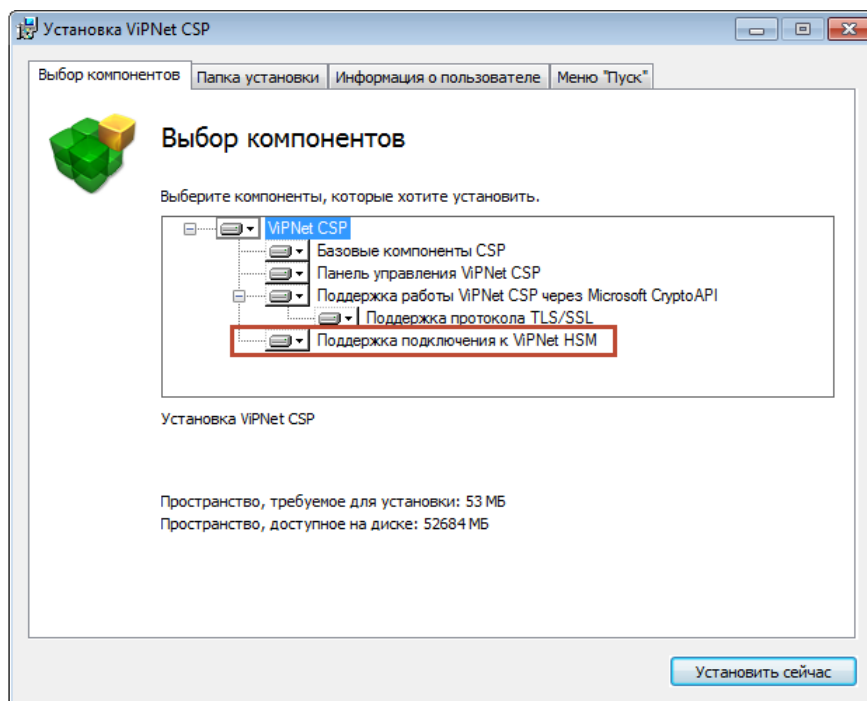


Рисунок 106. Компонент программы ViPNet CSP, предназначенный для взаимодействия с сервером ViPNet HSM

- Изменение списка компонентов ViPNet CSP, устанавливаемых по умолчанию на компьютер под управлением Windows 10

При установке новой версии ViPNet CSP на компьютер под управлением Windows 10 компонент **Поддержка протокола TLS/SSL** по умолчанию теперь отключен.

- Поддержка новых внешних устройств хранения данных

Реализована поддержка новых устройств хранения данных:

- Персональные электронные ключи Gemalto SafeNet eToken 5100, 5105, 5200, 5205, 5110, 7300, а также смарт-карта Gemalto SafeNet eToken 4100 производства компании Gemalto (SafeNet).

Так как для работы с указанными устройствами на компьютер необходимо установить то же программное обеспечение, что и для работы с устройствами семейства **eToken Aladdin**, это семейство устройств было переименовано в **SafeNet eToken (eToken Aladdin)**.

- Электронный идентификатор Рутокен ЭЦП 2.0 производства компании «Актив».

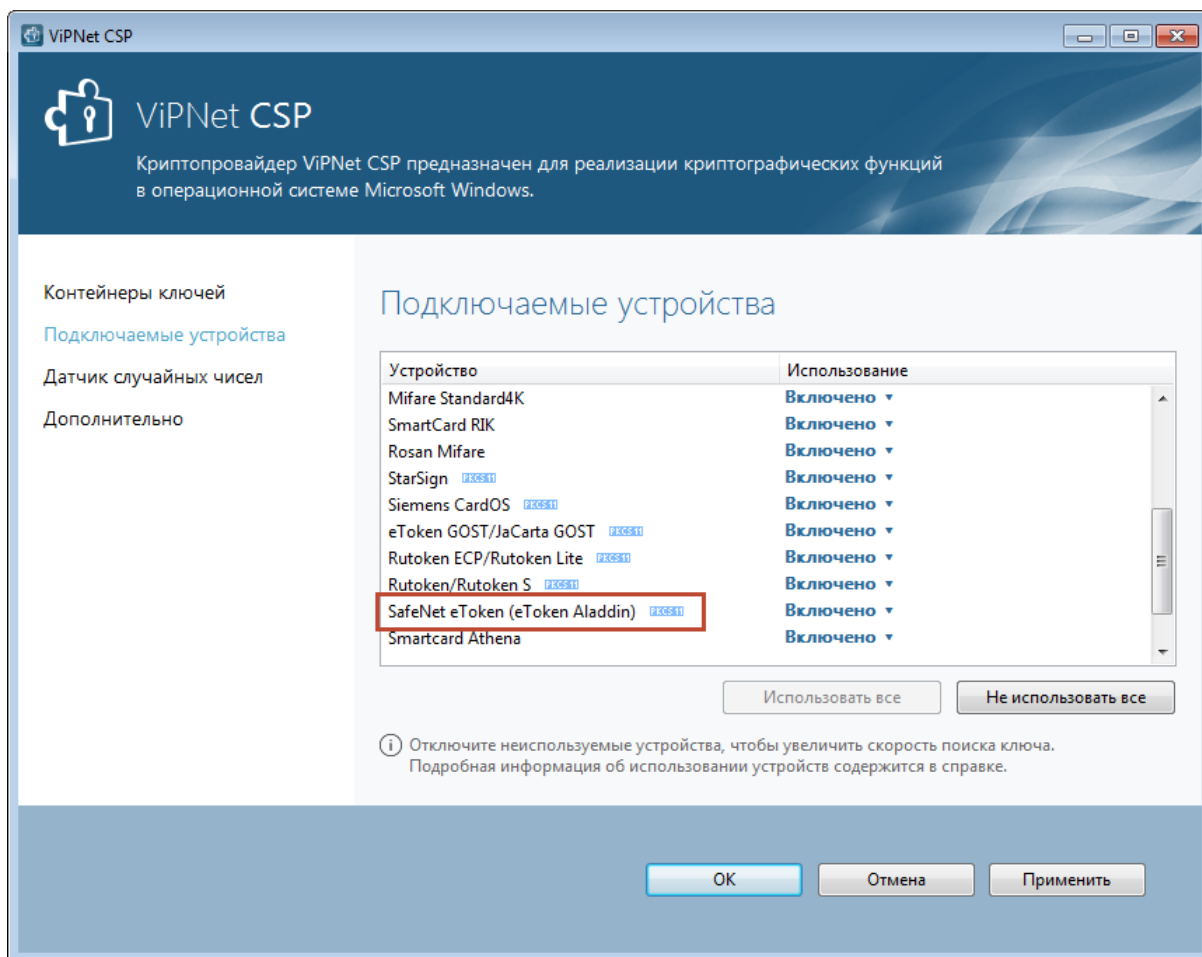


Рисунок 107. Поддержка устройств SafeNet eToken

- **Изменение в списке поддерживаемых пакетов программ Microsoft Office**

В связи с тем, что компания Microsoft в 2017 году прекращает поддержку пакета программ Microsoft Office 2007, работа ViPNet CSP в этих программах также более не поддерживается АО «ИнфоТекС».

- **Изменение в списке поддерживаемых почтовых программ Microsoft**

В связи с тем, что компания Microsoft прекратила поддержку программы Почта Windows Live, взаимодействие ViPNet CSP с этой программой также более не поддерживается АО «ИнфоТекС».

- **Исправление ошибок**

В версии 4.2.8 исправлены ошибки, выявленные в процессе эксплуатации версии 4.2.2.

Версия 4.2.2

- **Соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КСЗ теперь обеспечивается утилитой ViPNet SysLocker, входящей в комплект поставки**

Из программы ViPNet CSP удалены функции настройки замкнутой программной среды. Аналогичные функции администратор Windows теперь может выполнить в программе ViPNet SysLocker, которую при необходимости следует установить дополнительно.

- **Изменения в интерфейсе программы**

В интерфейсе программы произошли следующие изменения:

- Для экспорта сертификатов и закрытых ключей в файл теперь используется системный мастер Windows (см. [Экспорт сертификата и закрытого ключа в файл](#)).
- Для отображения свойств сертификата теперь используется системное окно Windows. В этом окне, наряду с информацией, доступной в прошлых версиях ViPNet CSP, для аннулированных сертификатов вы можете просмотреть дату и время их аннулирования в поле **Расширенные сведения об ошибке**.

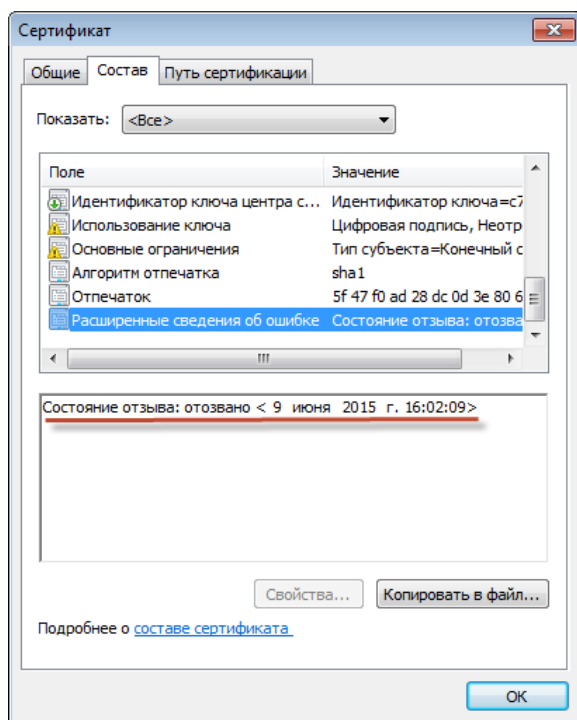


Рисунок 108. Информация о дате и времени отзыва сертификата

- **Изменение комплекта документации**

В комплект добавлен документ «ViPNet SysLocker. Руководство администратора».

- **Изменения в списке поддерживаемых операционных систем**

В связи с тем, что компания Microsoft прекратила поддержку операционной системы Windows XP (32-разрядная), работа ViPNet CSP на компьютерах с этой операционной системой также более не поддерживается АО «ИнфоТекС».

- **Изменения в списке поддерживаемых пакетов программ Microsoft Office**

В связи с тем, что компания Microsoft прекратила поддержку пакета программ Microsoft Office 2003, работа ViPNet CSP в этих программах также более не поддерживается АО «ИнфоТекС».

- **Изменения в списке поддерживаемых веб-браузеров**

Ввиду не востребоваемости прекращена поддержка веб-браузеров Internet Explorer 6 и 7.

- **Изменения в списке внешних устройств хранения данных**

Реализована поддержка устройств линейки «ESMART Token ГОСТ».

Ввиду не востребоваемости прекращена поддержка следующих типов внешних устройств: Shipka, iButton Accord, iButton Aladdin, KAZTOKEN.

Версия 4.2.0

- **Новый формат контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012**

Для обеспечения соответствия рекомендациям [Технического комитета по стандартизации \(ТК 26\) «Криптографическая защита информации»](#) изменен формат контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012.

- **Изменения в списке поддерживаемых внешних устройств**

Ввиду не востребоваемости прекращена поддержка следующих типов внешних устройств: Mifare Standard4K, SmartCard RIK, Rosan Mifare, Smartcard Athena.

Версия 4.1.0

- **Обновленный пользовательский интерфейс**

Полностью переработан дизайн пользовательского интерфейса программы.

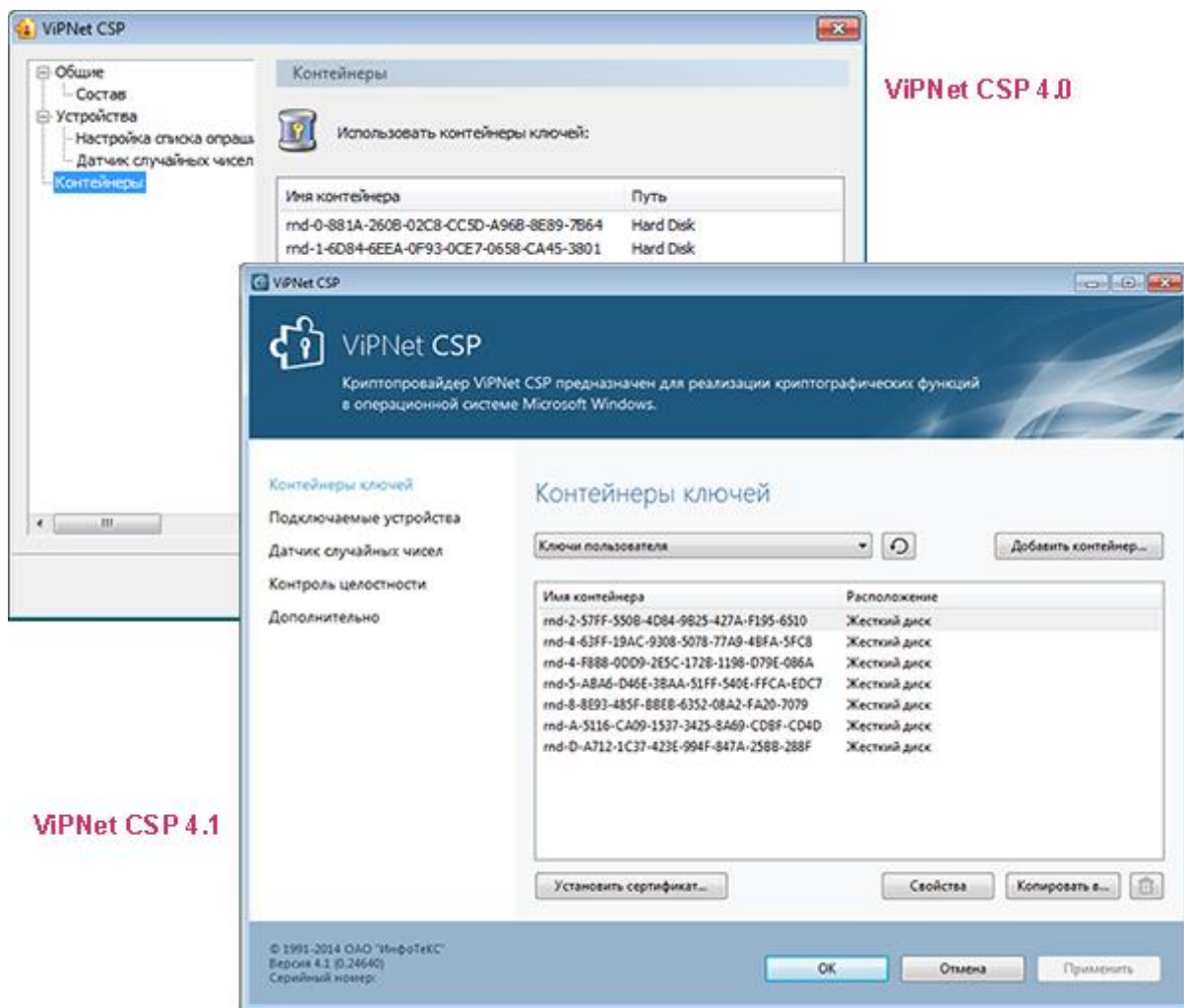


Рисунок 109. Пользовательский интерфейс программы ViPNet CSP 4.1

- Соответствие рекомендациям Технического комитета по стандартизации (ТК 26) «Криптографическая защита информации»

Криптографические алгоритмы ViPNet CSP приведены в соответствии с рекомендациями ТК 26 «Криптографическая защита информации».

- Расширенная поддержка алгоритма ГОСТ 34.10-2012
 - Добавлена возможность организации защищенного соединения TLS/SSL с использованием ключей, созданных по алгоритму ГОСТ 34.10-2012.
 - Добавлена возможность экспорта контейнеров ключей, созданных по алгоритму ГОСТ 34.10-2012, в файлы формата PKCS#12 (*.pfx), а также импорта таких контейнеров ключей из файлов PKCS#12.
 - Добавлена возможность работы с внешними устройствами, поддерживающими хранение ключей, созданных по алгоритму ГОСТ 34.10-2012.
- Организация защищенного соединения TLS/SSL с использованием универсальной электронной карты (УЭК)

Добавлена возможность использования контейнера ключей, записанного на вашу универсальную электронную карту, для организации защищенного соединения TLS/SSL с помощью ViPNet CSP.

- **Новый порядок работы с внешними устройствами**

В главном окне программы убран раздел **Устройства**. Теперь контейнеры ключей, сохраненные на внешнем устройстве, отображаются в разделе **Контейнеры ключей** при выборе названия устройства в раскрывающемся списке.

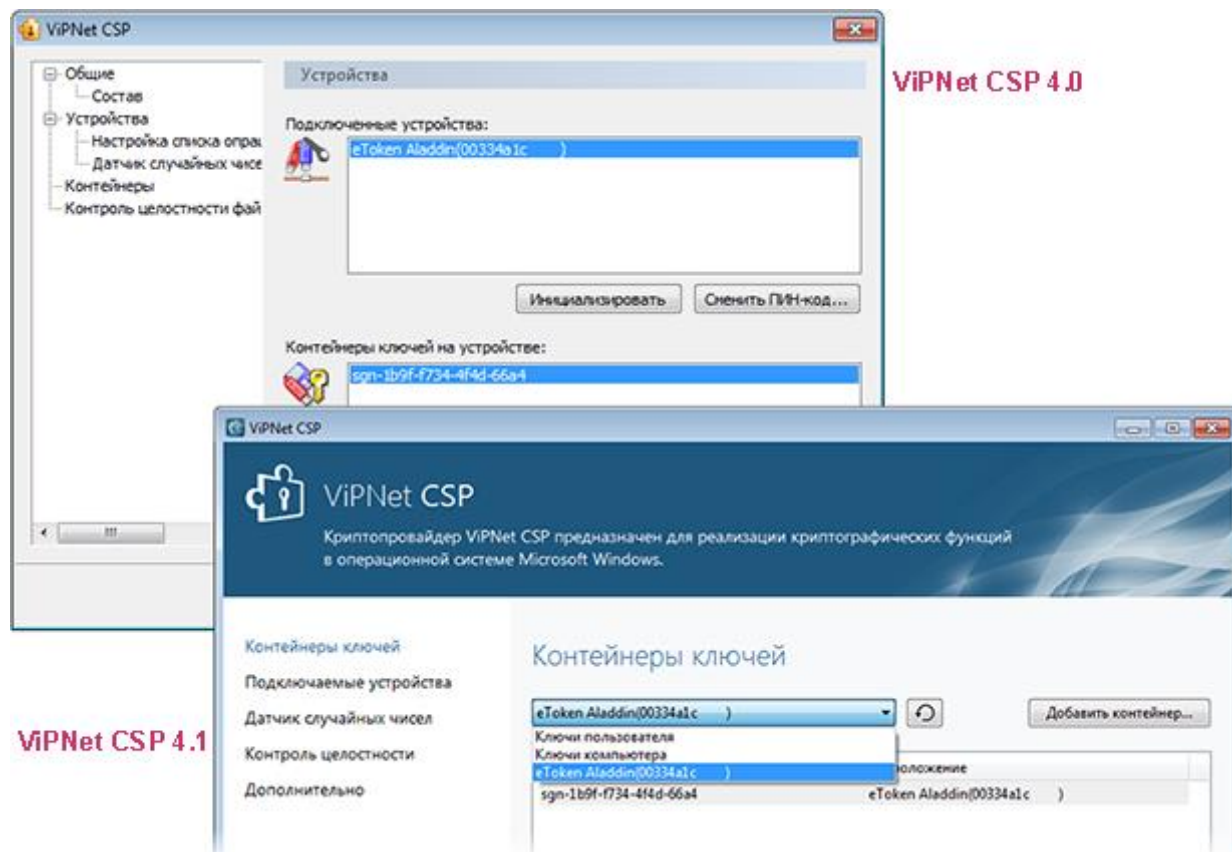


Рисунок 110. Изменение порядка работы с внешними устройствами

- **Новый интерфейс для настройки регистрации событий криптопровайдера**

Функция настройки регистрации событий криптопровайдера перенесена в раздел **Другое**. Теперь режимы ведения журнала задаются с помощью ползунка, для каждого режима добавлена подсказка.

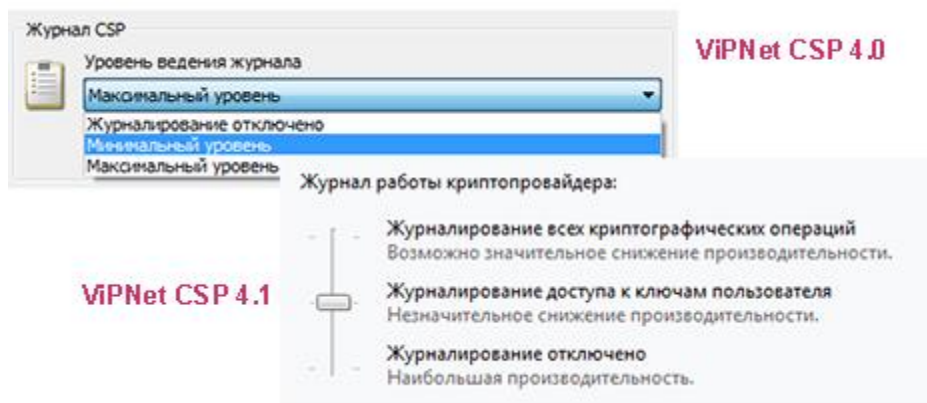


Рисунок 111. Настройка регистрации событий криптопровайдера

- Автоматический поиск контейнера ключей, которому соответствует сертификат

В мастере установки сертификатов добавлена возможность автоматического поиска контейнера ключей, соответствующего устанавливаемому сертификату. Поиск осуществляется по контейнерам ключей, установленным в ViPNet CSP. Новая возможность позволяет значительно ускорить работу, если в ViPNet CSP установлено большое количество контейнеров ключей.

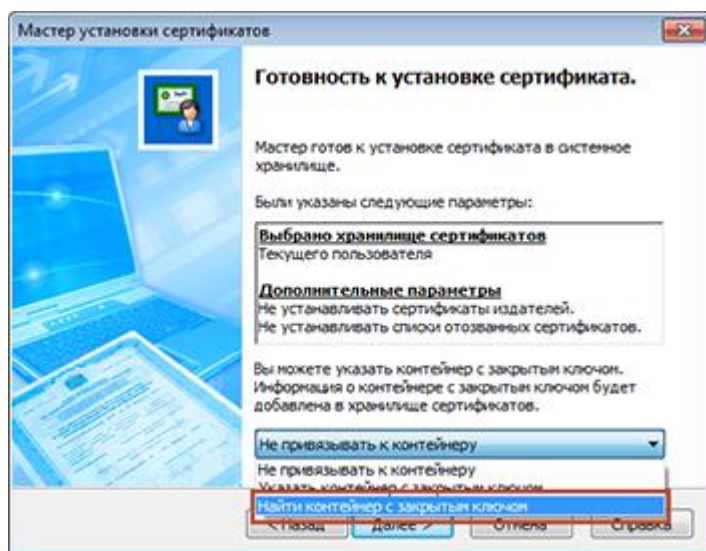


Рисунок 112. Задание автоматического поиска контейнера ключей

- Комплект документации

В комплект документации добавлено руководство «ViPNet CSP. Быстрый старт».

Версия 4.0.0

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.0.

- Соответствие новым стандартам хэширования и работы с электронной подписью

Хэширование данных и работа с электронной подписью осуществляется в соответствии со стандартами ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012.

- **Поддержка новых операционных систем**

В криптопровайдере реализована поддержка операционных систем Windows 8 (32-разрядная и 64-разрядная) и Windows Server 2012 (64-разрядная).

- **Поддержка интерфейса Cryptography API: Next Generation (CNG)**

В программе реализована поддержка интерфейса CNG, пришедшего на смену CryptoAPI. Подробнее об интерфейсе CNG см. «Криптографический интерфейс ViPNet CNG. Руководство разработчика».

- **Поддержка стандарта PKCS #11 для 64-разрядной архитектуры**

Реализована поддержка стандарта PKCS #11, определяющего интерфейс доступа к криптографическим устройствам.

- **Обновление программы создания запроса на сертификат**

- Добавлена возможность формирования запроса на сертификат для ключей, созданных с помощью различных криптопровайдеров: как от АО «ИнфоТекС», так и от корпорации Microsoft.
- В список **Шаблон сертификата** добавлен пункт **WEB server**, позволяющий создать запрос на сертификат для установки на веб-сервере IIS.
- Появилась возможность с помощью флажков **Экспортируемый** и **Системный** задавать следующие параметры издаваемого сертификата:
 - Будет ли возможно вместе с издаваемым сертификатом экспортировать соответствующий ему закрытый ключ.
 - Следует ли устанавливать издаваемый сертификат в системное хранилище локального компьютера.

Версия 3.2.x
Параметры сертификата

Криптопровайдер: Infotecs Cryptographic Service Provider

Назначение: Подпись и шифрование

Шаблон сертификата: Стандартный

Версия 4.0
Параметры сертификата

Криптопровайдер: Microsoft Base Cryptographic Provider v1.0

Алгоритм хеширования: SHA-1

Назначение: Подпись и шифрование

Шаблон сертификата: Стандартный

Параметры ключа: ☒ Экспортируемый ☐ Системный

Рисунок 113. Новый интерфейс программы создания запроса на сертификат

- Отдельное отображение контейнеров ключей, установленных в папку хранения контейнеров ключей пользователя и локального компьютера

В разделе **Контейнеры** добавлен переключатель, позволяющий фильтровать контейнеры ключей по месту их хранения.

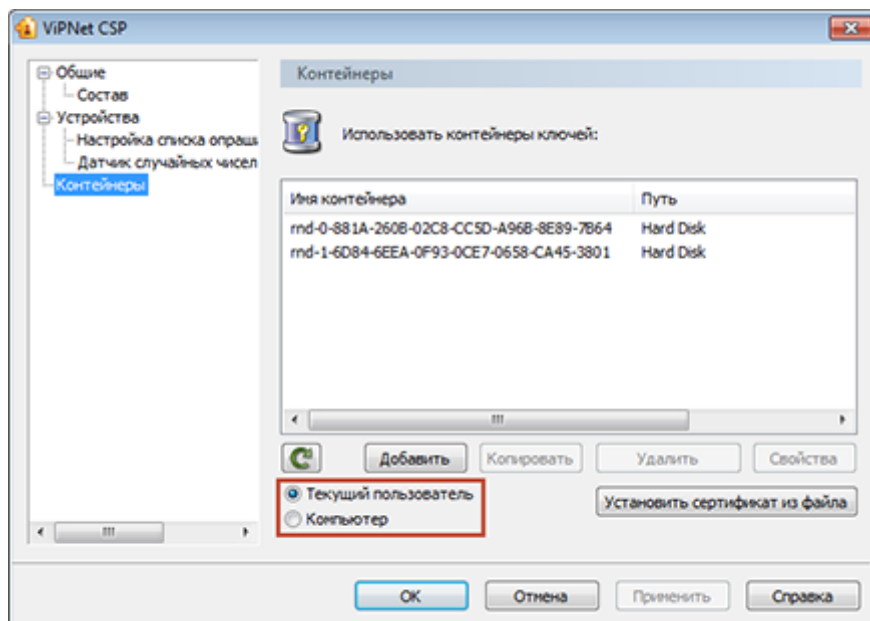


Рисунок 114. Переключатель для фильтрации контейнеров ключей

- Настройка прав доступа к контейнеру ключей

Добавлена возможность задания прав доступа к контейнеру ключей для встроенных учетных записей операционной системы Windows.

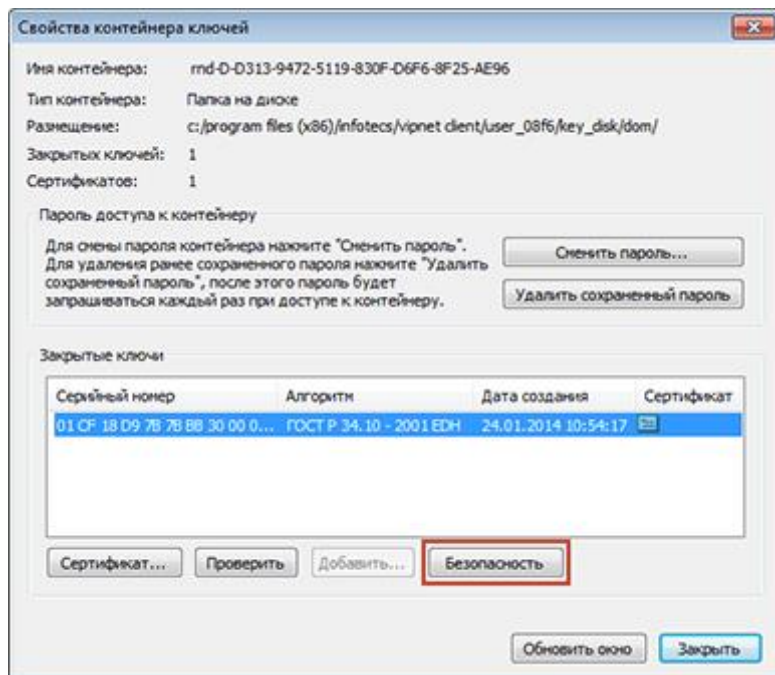


Рисунок 115. Настройка прав доступа к контейнеру ключей

- **Поддержка новых внешних устройств хранения данных**

Реализована поддержка новых устройств хранения данных, таких как универсальные электронные карты (УЭК), смарт-карты Magistra и других.

- **Интеграция с пакетом программ Microsoft Office 2013**

Реализована поддержка шифрования и работы с электронной подписью в программах пакета Microsoft Office 2013.

- **Поддержка новых веб-браузеров**

Добавлена возможность использования ViPNet CSP для работы по протоколу TLS/SSL в веб-браузерах Google Chrome и Яндекс.Браузер.

- **Регистрация событий криптопровайдера в журнале операционной системы Windows**

Добавлена возможность ведения журнала событий криптопровайдера. Вы можете задать один из двух режимов ведения журнала (см. [Настройка регистрации событий криптопровайдера](#)).

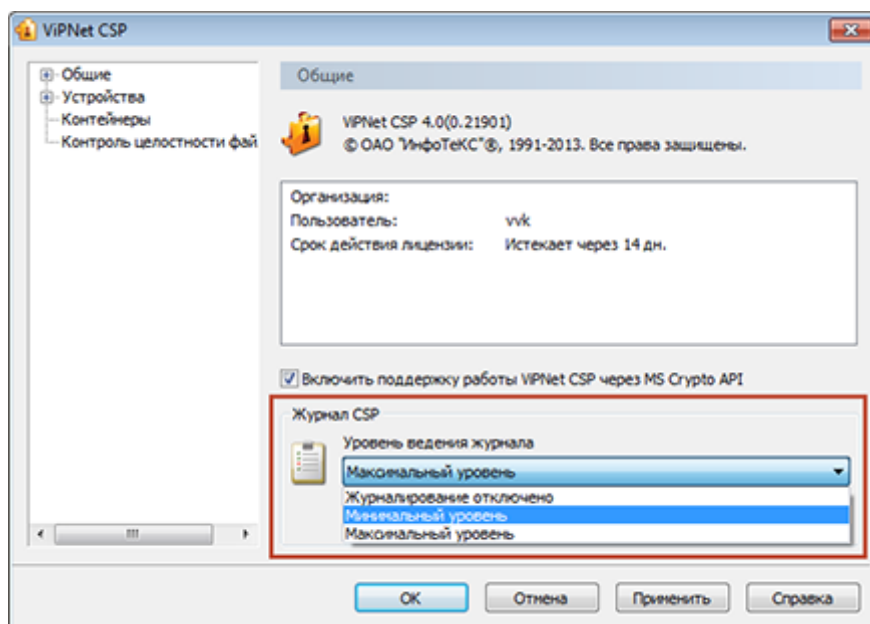


Рисунок 116. Выбор уровня ведения журнала событий криптопровайдера

- **Соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КСЗ**

Добавлен механизм контроля целостности файлов, позволяющий создать замкнутую программную среду. Параметры, необходимые для этого, можно настроить в специальном разделе **Контроль целостности**.

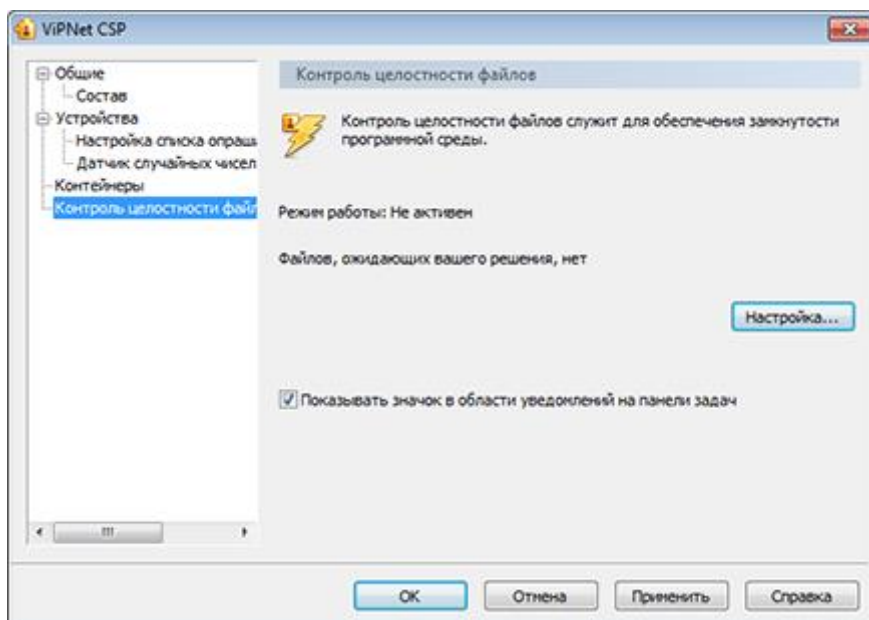


Рисунок 117. Настройка контроля целостности файлов



Примечание. Механизм контроля целостности файлов по умолчанию недоступен. Для его добавления выберите соответствующий компонент при установке программы.

- **Расширенный комплект документации**

Комплект документации дополнен руководствами разработчика по криптографическим интерфейсам ViPNet CSP, ViPNet CNG и ViPNet PKCS11.



Термины и сокращения

PKI (Public Key Infrastructure)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих доверие к открытым ключам (в том числе ключам проверки электронной подписи) путём издания сертификатов ключей проверки электронной подписи и поддержания их жизненного цикла.

S/MIME (Secure Multipurpose Internet Mail Extensions)

Спецификация безопасных сообщений электронной почты, использующая стандарт X.509 и различные механизмы шифрования (ГОСТ 28147-89, 3DES и другие).

Асимметричное шифрование

Шифрование с использованием двух математически связанных ключей: открытого (несекретного) ключа для зашифрования и закрытого (секретного) ключа для расшифрования.

Доверенное лицо удостоверяющего центра (администратор УЦ)

Лицо, уполномоченное действовать от имени удостоверяющего центра (в том числе издавать, аннулировать сертификаты ключей проверки электронной подписи).

Запрос на сертификат

Документ с информацией, которая требуется для издания сертификата ключа проверки электронной подписи в удостоверяющем центре (владелец, срок действия, назначение сертификата и прочее).

Квалифицированный сертификат

Сертификат ключа проверки электронной подписи, изданный аккредитованным удостоверяющим центром или уполномоченным федеральным органом исполнительной власти.

Ключ проверки электронной подписи (ключ проверки ЭП)

Несекретный (открытый) ключ из пары асимметричных ключей, который представляет собой уникальную последовательность символов, однозначно связанную с секретным ключом (ключом электронной подписи или закрытым ключом) и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи (ключ ЭП)

Секретный (закрытый) ключ из пары асимметричных ключей, который представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Ключевой блокнот ДСДР

Ключевой блокнот ДСДР содержит последовательности случайных чисел, которые используются при шифровании конфиденциальной информации. ДСДР предназначен для средств криптографической защиты данных, не содержащих сведений, составляющих государственную тайну.

Контейнер ключей

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

Корневой сертификат

Самоподписанный сертификат головного удостоверяющего центра. Используется для подписи сертификатов, издаваемых головным удостоверяющим центром, с целью обеспечения доверия к ним.

ПАК ViPNet HSM

Программно-аппаратный комплекс, предоставляющий интерфейс PKCS#11 для защищенного хранения ключей и выполнения криптографических операций в защищенном окружении. Является средством криптографической защиты информации класса KB и средством электронной подписи класса KB2.

Программный токен

Программный аналог внешнего устройства хранения ключей и сертификатов, для взаимодействия с которым используется расширенный интерфейс PKCS#11 (подробнее см. «ViPNet SoftToken. Руководство разработчика»).

Разностный список аннулированных сертификатов (delta CRL)

Список аннулированных сертификатов, который содержит только сертификаты, аннулированные после выпуска полного (базового) списка аннулированных сертификатов.

Сертификат издателя

Сертификат ключа проверки электронной подписи, принадлежащий удостоверяющему центру и служащий для подписи сертификатов, издаваемых удостоверяющим центром.

Сертификат ключа проверки электронной подписи

Документ, изданный удостоверяющим центром 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.

Токен

Устройство аутентификации, предназначенное для обеспечения информационной безопасности пользователя.

Точка распространения списков аннулированных сертификатов (CDP)

Хранилище, в которое удостоверяющий центр публикует актуальные списки аннулированных сертификатов. URL таких точек указываются в соответствующем расширении сертификатов, издаваемых удостоверяющим центром.

Удостоверяющий центр (УЦ)

Организация, уполномоченная издавать сертификаты ключа проверки электронной подписи для физических и юридических лиц, а также управлять жизненным циклом этих сертификатов.

Цепочка сертификатов

Иерархия сертификатов, в которой каждый сертификат подписан вышестоящим сертификатом вплоть до корневого (самоподписанного) сертификата. Наличие для сертификата полной цепочки действительных сертификатов подтверждает доверие к этому сертификату.

Электронная подпись (ЭП)

Созданная криптографической операцией дополнительная информация, с помощью которой можно подтвердить авторство и неизменность основной информации.

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, позволяющий инициализировать датчик случайных чисел по действиям пользователя. Полученная последовательность используется при формировании криптографических ключей.