ViPNet CSP

Руководство пользователя

ViPNet Virtual Private Network

infotecs

ФРКЕ.00061-01 90 01

ОАО "Инфотекс"

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

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

E-mail: hotline@infotecs.ru

WWW: http://www.infotecs.ru

Содержание

Введение **7**
О документе 8
Для кого предназначен документ 8
Соглашения документа 8
О программе 9
Системные требования 9
Информация о внешних устройствах хранения данных 10
Комплект поставки 13
Ограничения бесплатной версии 14
Обратная связь 15
Дополнительная информация 15
Контактная информация 15

Глава 1. Использование криптопровайдера в системах защиты данных **16**
Назначение криптопровайдера 17
Электронная цифровая подпись 18
Аутентичность и конфиденциальность соединений TLS/SSL 19
Контейнер секретного ключа и сертификата 20

Глава 2. Установка и запуск программы **22**
Установка программы 23
Установка с использованием командной строки 24
Запуск программы 25

Глава 3. Регистрация ViPNet CSP **27**
Прежде чем регистрировать ViPNet CSP 28
Зачем нужно регистрировать ViPNet CSP 28
Начало регистрации 28
Покупка программы (получение серийного номера) 31
Получение кода регистрации 32
Получение кода регистрации через Интернет 33
Получение кода регистрации по электронной почте 35

Получение кода регистрации через веб-страницу ... 37
Получение кода регистрации по телефону ... 37
Групповая регистрация ... 38
Регистрация ViPNet CSP ... 41
Сохранение регистрационных данных ... 43
Если конфигурация вашего компьютера изменилась ... 43
Порядок действий системного администратора при групповой регистрации ... 45

Глава 4. Установка контейнеров и сертификатов ... 46
Установка контейнера из папки ... 47
Установка контейнера с внешнего устройства ... 50
Установка сертификата и контейнера секретного ключа ... 52
Ручная установка сертификатов и СОС ... 56

Глава 5. Операции с контейнерами ... 59
Создание резервной копии контейнера ... 60
Отключение контейнера ... 62
Просмотр и настройка свойств контейнера ... 63
Смена пароля к контейнеру ... 63
Удаление сохраненного пароля ... 65
Установка сертификата пользователя ... 65
Проверка соответствия секретного ключа и сертификата ... 66
Удаление секретного ключа ... 67

Глава 6. Работа с внешними устройствами ... 68
Просмотр списка подключенных устройств ... 69
Настройка списка опрашиваемых устройств ... 71
Инициализация устройства ... 72
Смена ПИН-кода ... 74

Глава 7. Дополнительные возможности ... 76
Проверка целостности модулей программы ... 77
Использование датчика случайных чисел ... 78

Глава 8. Цифровая подпись в документах MS Office ... 80
Подписание документа ... 81
Microsoft Office 2003 ... 81
Microsoft Office 2007 ... 82

Просмотр цифровой подписи ... 84
Microsoft Office 2003 ... 84
Microsoft Office 2007 ... 85
Удаление цифровой подписи ... 86
Microsoft Office 2003 ... 86
Microsoft Office 2007 ... 86
Видимая строка подписи в документах Word и Excel ... 87
Вставка видимой строки подписи ... 87
Подписание строки подписи ... 88
Подписание базы данных Microsoft Access 2007 ... 91

Глава 9. Цифровая подпись в Microsoft Outlook ... 93
Добавление подписи ко всем сообщениям ... 94
Добавление подписи к отдельному сообщению ... 97
Добавление цифровой подписи ... 97
Если отсутствует кнопка Сообщение с цифровой подписью ... 98
Просмотр цифровой подписи сообщения ... 100

Глава 10. Цифровая подпись в Microsoft Office InfoPath ... 102
Разрешение подписывать форму InfoPath цифровой подписью ... 103
Microsoft Office InfoPath 2003 ... 103
Microsoft Office InfoPath 2007 ... 103
Подписание формы InfoPath ... 106
Microsoft Office InfoPath 2003 ... 106
Microsoft Office InfoPath 2007 ... 107
Просмотр подписи в форме InfoPath ... 109
Удаление подписи из формы InfoPath ... 110

Глава 11. Цифровая подпись макросов ... 111
Подписание макросов ... 112
Проверка подписи макроса ... 114
Удаление подписи макроса ... 115

Глава 12. Организация защищенного соединения TLS/SSL ... 116
Этапы организации доступа к защищенному веб-серверу ... 117
Настройка серверного узла соединения ... 118
Настройка клиентского узла соединения ... 119

Настройка браузера Internet Explorer для работы по протоколу TLS/SSL 120
Проверка доступности веб-узла по защищенному протоколу HTTPS 121

Глава 13. Проблемы и неисправности 122
Не удается запустить программу 123
Конфликт ViPNet CSP с другими программами 125
Не удается поставить цифровую подпись 126
Не найден секретный ключ, соответствующий сертификату 126
Не удается подписать сообщение электронной почты 126
Не удается подписать макрос или базу данных Microsoft Access 2007 126
Не удается подписать видимую строку подписи в Microsoft Word 2003 или Excel 2003 127
Невозможно редактировать подписанный документ Microsoft Word или Excel 127
Нет соединения с сервером по протоколу HTTPS 128
На IIS сервере и веб-клиенте установлены разные версии ViPNet CSP 128
Не установлены сертификаты пользователя, издателя, СОС в нужное хранилище 128
Обозреватель не настроен на работу по протоколу TLS 130
Требуется перезапуск службы сервера IIS 131
Требуется сохранить пароль к сертификату сервера 132
При соединении с сервером выводится предупреждение системы безопасности 133

Глоссарий 134

Указатель 136

Введение

О документе 8

О программе 9

Ограничения бесплатной версии 14

Обратная связь 15

О документе

В данном документе описывается назначение и применение программы ViPNet CSP, основные возможности программы, принципы работы с программой и описание пользовательского интерфейса.

Для кого предназначен документ

Документ предназначен для пользователей программы ViPNet CSP, использующих в системах документооборота сертификаты для шифрования документов и проверки подлинности ЭЦП, а также для системных администраторов, организующих удаленный доступ к ресурсам по протоколам TLS/SSL.

Соглашения документа

В данном документе содержатся следующие соглашения:

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

О программе

Программа ViPNet CSP представляет собой криптопровайдер (см. "Назначение криптопровайдера" на стр. 17), обеспечивающий вызов криптографических функций через интерфейс Microsoft CryptoAPI 2.0. Это позволяет вызывать криптографические функции из различных приложений Microsoft.

ViPNet CSP обеспечивает:

- Создание ключей электронной цифровой подписи (ЭЦП) по алгоритме и ГОСТ Р 34.10-2001 (см. "Электронная цифровая подпись" на стр. 18).
- Вычисление и проверку ЭЦП по алгоритмам ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001.
- Хэширование данных в соответствии с алгоритмом ГОСТ Р 34.11-94.
- Шифрование и имитозащиту данных в соответствии с алгоритмом ГОСТ 28147-89.
- Хранение сертификатов открытых ключей непосредственно в ключевом контейнере.
- Поддержку различных устройств хранения ключей (eToken, iKey, Smard Card и др.).

Обеспечивается совместимость ViPNet CSP с криптопровайдерами других производителей при условии реализации ими требований, содержащихся в RFC 4357, 4490, 4491.

Системные требования

Для успешной работы ViPNet CSP компьютер должен удовлетворять следующим требованиям:

- процессор не ниже Pentium IV;
- не менее 512 мегабайт оперативной памяти;
- 100 мегабайт свободного места на жестком диске;

- операционная система Microsoft Windows 2000 (32 бит)/XP (32/64 бит)/Server 2003 (32/64 бит)/Vista (32/64 бит)/Server 2008 (32/64 бит)/Windows 7 (32/64 бит)/Server 2008 R2;
- Internet Explorer версии 6.0 и выше.

ViPNet CSP поддерживает работу со следующими электронными ключами:

- Смарт-карта SmartCard RIK.
- Смарт-карта SmartCard Athena.
- Смарт-карта SmartCard ACOS2.
- Смарт-карта Siemens CardOS.
- USB-токен ruTokenECP.
- USB-токен ruToken.
- USB-токен Shipka.
- USB-токен или смарт-карта eTokenAladdin.
- Таблетка iButton Aladdin.
- Таблетка iButton Accord.

Подробную информацию о поддерживаемых электронных ключах см. в разделе Информация о внешних устройствах хранения данных (на стр. 10).

Информация о внешних устройствах хранения данных

В ПО ViPNet для записи и считывания различной информации (паролей, ключей и т.д.) имеется возможность использовать различные внешние устройства хранения данных (аппаратные носители).

Ниже, в таблице перечислены устройства и ключи, с которыми может работать ПО ViPNet.

Примечание. Некоторые программы ViPNet могут работать не со всеми устройствами, указанными в таблице. В этом случае список поддерживаемых устройств указан в документации для конкретной программы ViPNet.

Приведенная таблица содержит следующие данные:

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

Таблица 1.

Тип устройства	Тип ключа	Необходимые условия работы с ключом	Поддержка протокола PKCS#11
eToken Aladdin	**eToken PRO** (персональные электронные ключи, eToken PRO (Java), eToken PRO, смарт-карты eToken PRO (Java), eToken PRO компании Aladdin)	• На компьютере должно быть установлено программное обеспечение PKI Client версии 5.1 и выше. • Поддерживаемые ОС: Windows XP SP2 (32/64bit) и выше, Server 2003 SP2 (32/64bit), Vista SP1 (32/64bit), Server 2008 (32/64bit). • **Замечание:** Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым USB-устройством считывания с карт.	Да
iButton Aladdin	**iButton (Dallas)** (электронные ключи iButton типа DS1992, DS1993, DS1994, DS1995 и DS1996)	• К компьютеру должно быть подключено устройство считывания. • На компьютере должно быть установлено программное обеспечение обмена информации с iButton, 1-Wire Drivers версии 4.02. • Поддерживаемые ОС: Windows XP SP2 (32/64bit) и выше, Server 2003	Нет

		(32/64bit), Vista (32/64bit), Server 2008 (32/64bit), 7 (32/64bit).	
Smartcard Athena	Смарт-карты с памятью типа I2C (ASE M4), синхронные смарт-карты с шиной 2/3 и защищенной памятью, удовлетворяющие стандарту ISO7816-3 (ASE MP42)	• Чтение и запись на смарт-карту осуществляется через считыватель ASEDrive III PRO-S компании Athena. • На компьютере должны быть установлены драйвера версии 2.5.0.0. • Поддерживаемые ОС: Windows 2000, XP (32/64bit), Server 2003 (32bit/64bit), Vista(32bit/64bit).	Нет
SmartCard RIK	**Российская интеллектуальная карта** компании Атлас-Телеком.	• Работа с картой ПО ViPNet может производиться через любой PS\CS-совместимый считыватель.	Нет
Shipka	**ПСКЗИ ШИПКА** компании ОКБ САПР	• На компьютере должно быть установлено программное обеспечение **ACShipka Environment** версии не ниже 3.3.2.6 • Поддерживаемые ОС: Windows, XP (32/64bit), Server 2003 (32/64bit), Vista (32/64bit), Server 2008 (32/64bit). • Для инициализации устройства необходимо пользоваться утилитой производителя «Параметры авторизации». В случае если вы произвели инициализацию в приложении ViPNet, Вам так же необходимо выполнить инициализацию с помощью утилиты «Параметры авторизации».	Да
ruToken	**Rutoken S**, электронный идентификатор компании Актив	• На компьютере должны быть установлены драйверы Rutoken версий не ниже используемых в установочном комплекте версии 2.25.03.0267. • Поддерживаемые ОС: Windows 2000, XP (32/64bit), Server 2003 (32/64bit), Vista (32/64bit), Server 2008 (32/64bit), 7 (32/64bit).	Да

ruTokenECP	**Rutoken ЭЦП**, электронный идентификатор компании Актив	• На компьютере должны быть установлены драйвера версии 2.50. • Поддерживаемые ОС: Windows 2000, XP (32/64bit), Server 2003 (32/64bit), Vista (32/64bit), Server 2008 (32/64bit), 7 (32/64bit).	Да

Комплект поставки

В комплект поставки программы ViPNet CSP входит:

- Установочный файл ViPNet CSP – Setup.exe.
- Руководство пользователя.

Документация поставляется в электронном виде.

Ограничения бесплатной версии

В ViPNet CSP есть возможность работать с бесплатной версией по демо-лицензии.

Особенности демо-лицензии:

- Срок действия: 60 дней.
- Функциональных ограничений нет.

По истечении срока действия демо-лицензии, если программа не зарегистрирована, она переходит в ограниченный режим:

- Запрещаются функции генерации ключей, подписи, обращения к секретным ключам на носителях.
- Доступны функции, обеспечивающие хеширование данных, проверку подписи или имитозащиты.

В ограниченном режиме ViPNet CSP можно использовать только для просмотра и проверки защищенных документов, операции по защите документов производить нельзя.

Обратная связь

Дополнительная информация

Для удобства компания «Инфотекс» собрала все сведения, распространенные вопросы и ответы, приемы и советы в тематические базы знаний. По предложенным ссылкам можно найти ответ практически на любой вопрос, возникающий в процессе эксплуатации продуктов ViPNet.

- Сборник часто задаваемых вопросов (FAQ): http://www.infotecs.ru/faq.htm
- Законодательная база в сфере защиты информации: http://infotecs.ru/law.htm
- Описание технологии ViPNet: http://infotecs.ru/probl.htm

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами компании «Инфотекс»:

- Форум компании «Инфотекс»: http://www.infotecs.ru/forum
- Электронный адрес службы поддержки: hotline@infotecs.ru
- Форма запроса по электронной почте в службу поддержки: http://www.infotecs.ru/mail/0946578ik456.htm
- (495) 737-6196 – «горячая линия» службы поддержки.

1

Использование криптопровайдера в системах защиты данных

Назначение криптопровайдера	17
Электронная цифровая подпись	18
Аутентичность и конфиденциальность соединений TLS/SSL	19
Контейнер секретного ключа и сертификата	20

Назначение криптопровайдера

Для реализации криптографических функций в операционной системе Windows может использоваться криптопровайдер ViPNet CSP.

Примечание. Поскольку криптопровайдер является независимым программным модулем, то для его работы не требуется запуск клиентского ПО ViPNet.

Криптопровайдер ViPNet CSP предназначен для выполнения следующих задач:

- Авторизация и обеспечение юридической значимости документов в процессе защищенного документооборота. Для этого используются средства формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии со стандартами ГОСТ Р 34.11–94, ГОСТ Р 34.10–2001, ГОСТ Р 34.10–94 (используется только для проверки ЭЦП).
- Обеспечение конфиденциальности и контроля целостности информации путем ее шифрования и имитозащиты, в соответствии с ГОСТ 28147–89.
- Обеспечение аутентичности и конфиденциальности соединений TLS/SSL.

Для организации защищенного документооборота и обмена данными криптопровайдер ViPNet использует сертифицированные средства криптографической защиты.

Примечание. В ОС семейства Microsoft, начиная с Windows 2000 встроен криптопровайдер Microsoft Base Cryptographic Provider, который обладает набором основных криптографических функций. Алгоритмы, используемые данными функциями, не являются сертифицированными по ГОСТ.

Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП, или цифровая подпись) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи. Цифровая подпись используется для аутентификации, то есть проверки подлинности цифровой информации (например, документов, сообщений электронной почты, программ) с помощью методов компьютерной криптографии. Цифровая подпись позволяет подтвердить:

- Подлинность: цифровая подпись удостоверяет личность поставившего подпись
- Целостность: цифровая подпись подтверждает, что документ не изменялся после подписания.
- Неотрекаемость: цифровая подпись подтверждает авторство документа.

Таким образом, цифровая 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 цифровой подписи, особенности ее использования в сферах государственного управления и в корпоративной информационной системе прописаны в Законе РФ от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»

Лицо или организация, поставившая цифровую подпись, называется издателем и является законным владельцем цифровой подписи. Чтобы иметь возможность ставить цифровую подпись, издатель получает в компетентном Удостоверяющем центре сертификат цифровой подписи (см. "Контейнер секретного ключа и сертификата" на стр. 20).

Если проверка сертификата по базе данных Удостоверяющего центра показала, что он является законным, действующим, не был просрочен или отозван, то сертификат считается действительным. Документы, подписанные действительным сертификатом цифровой подписи и не изменявшиеся с момента их подписания, также считаются действительными.

Аутентичность и конфиденциальность соединений TLS/SSL

Протокол TLS/SSL используется для организации защищенного доступа к ресурсам удаленного сервера. Необходимость защищенного доступа может возникнуть при реализации общего доступа к базам данных или хранилищам, при создании систем электронных платежей и для другой функциональности.

Взаимодействие двух узлов при защищенном соединении представлено на схеме ниже.

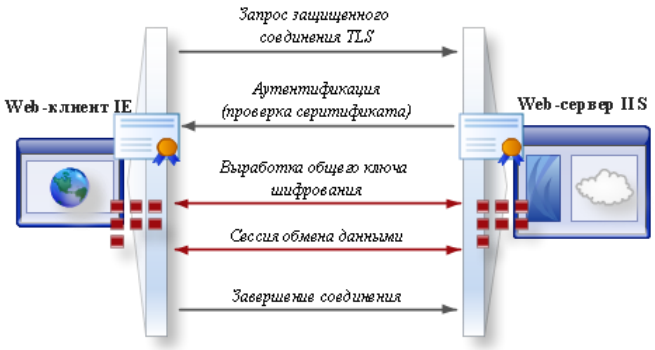

Рисунок 1: Схема взаимодействия узлов при TLS-соединении

Таким образом, использование протокола TLS/SSL, реализуемого средствами криптопровайдера ViPNet, позволяет гарантировать надежное и санкционированное соединение с удаленными серверами и строго ограниченный доступ к защищенным данным.

Контейнер секретного ключа и сертификата

Для осуществления функций шифрования и защиты криптопровайдер ViPNet CSP использует информацию сертификата пользователя (см. "Сертификат (Сертификат пользователя)" на стр. 134) и его секретный ключ. Кроме этого необходимы сертификат издателя (на стр. 134) и СОС (см. "Список отозванных сертификатов" на стр. 135).

Сертификат пользователя можно издать по инициативе администратора Удостоверяющего центра или по запросу пользователя. Запрос на обновление сертификата пользователя выполняется из клиентского ПО ViPNet CryptoService, ViPNet Client или программ других разработчиков.

При организации защищенного документооборота прикладное приложение (программы MS Office, обозреватель Internet Explorer, служба сервера IIS) обращается к криптопровайдеру, передавая ему параметры сертификатов и местоположение секретного ключа. Чтобы обеспечить прикладным приложениям доступ к сертификатам, их необходимо добавить в хранилище операционной системы.

Сертификат пользователя и секретный ключ упакованы в контейнер и устанавливаются с помощью программы ViPNet CSP (см. "Установка контейнеров и сертификатов" на стр. 46).

Сертификат издателя и СОС устанавливаются штатными средствами операционной системы (см. "Ручная установка сертификатов и СОС" на стр. 56).

Приложение ViPNet CSP позволяет добавлять секретные ключи шифрования и сертификаты следующими способами:

- Добавление контейнера, содержащего секретный ключ и сертификат. При этом контейнер может находиться в папке на диске (см. "Установка контейнера из папки" на стр. 47) или на внешнем устройстве (см. "Установка контейнера с внешнего устройства" на стр. 50).
- Установка сертификата и сопоставление ему контейнера секретного ключа из папки на диске или с внешнего устройства (см. "Установка сертификата и контейнера секретного ключа" на стр. 52).

Сертификат может находиться отдельно от секретного ключа, в случаях, когда сертификат создается по запросу пользователя (к внутреннему или внешнему Удостоверяющему центру).

Контейнеры, контейнеры секретного ключа и сертификаты выдаются администратором Удостоверяющего и Ключевого центра сети ViPNet.

В системе может быть установлено неограниченное количество контейнеров и сертификатов.

2

Установка и запуск программы

Установка программы 23

Установка с использованием командной строки 24

Запуск программы 25

Установка программы

Для установки программы ViPNet CSP вы должны обладать правами администратора операционной системы.

1. Запустите файл setup.exe  и следуйте указаниям мастера установки.
2. По окончании установки программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите **Да**.

Установка с использованием командной строки

Приложение ViPNet CSP может быть установлено из командной строки Windows с указанием ряда стандартных параметров Windows Installer.

Таблица 2. Параметры режима установки

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

Таблица 3. Параметры перезагрузки

Параметр	Описание
`/norestart`	Отключение перезагрузки после завершения установки.
`/promptrestart`	Вывод диалогового окна с запросом на перезагрузку.
`/forcerestart`	Перезагрузка компьютера после установки и принудительное закрытие других приложений без сохранения открытых файлов.

Пример команды установки:

```
setup.exe /qn /norestart
```

Запуск программы

Для запуска программы настройки ViPnet CSP выполните действия:

- В меню **Пуск > Все программы > ViPNet > ViPNet CSP** щелкните пункт **Настройка Криптопровайдера ViPNet CSP**.

При запуске незарегистрированной версии программы откроется окно **ViPNet CSP** с предложением зарегистрировать программу. Вы можете перейти к регистрации программы либо начать работу с демо-версией программы (см. "Ограничения бесплатной версии" на стр. 14).

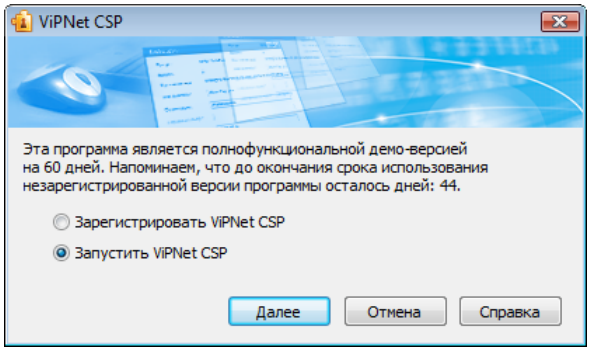

Рисунок 2: Запуск незарегистрированной версии программы

После запуска программы откроется панель **Общие** главного окна ViPNet CSP. Здесь содержится информация о версии программы, владельце лицензии и режиме работы ViPNet CSP.

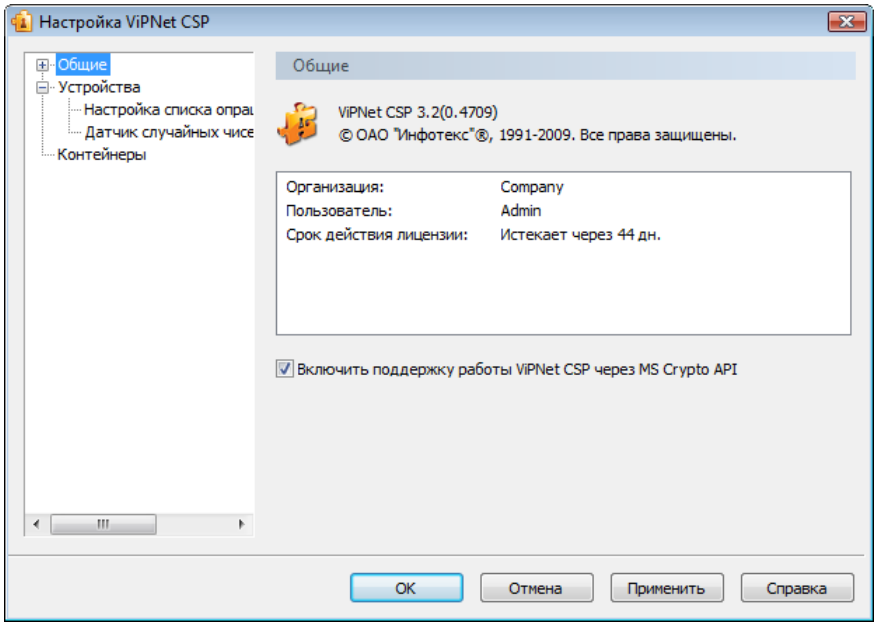

Рисунок 3: Панель Общие главного окна программы

Начните работу с программой с установки контейнера секретного ключа и сертификата (см. "Установка контейнеров и сертификатов" на стр. 46).

3

Регистрация ViPNet CSP

Прежде чем регистрировать ViPNet CSP 28

Покупка программы (получение серийного номера) 31

Получение кода регистрации 32

Регистрация ViPNet CSP 41

Порядок действий системного администратора при групповой регистрации 45

Прежде чем регистрировать ViPNet CSP

Зачем нужно регистрировать ViPNet CSP

После установки ViPNet CSP на компьютер программа работает в демо-режиме (см. раздел «Ограничения бесплатной версии»).

Вы можете принять решение о приобретении ViPNet CSP в любой момент. Зарегистрируйте ViPNet CSP и работайте в полнофункциональной версии программы неограниченное время.

Мы рекомендуем поступить следующим образом:

- установите ViPNet CSP и пользуйтесь бесплатной версией, чтобы оценить возможности и преимущества программы;
- если вы захотите приобрести полную версию программы, зарегистрируйте вашу копию ViPNet CSP.

Начало регистрации

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

Если вы системный администратор и хотите одновременно зарегистрировать несколько копий программы, вы можете использовать возможность групповой регистрации, чтобы собрать запросы на регистрацию от всех пользователей, отправить их в одном сообщении электронной почты и получить все регистрационные коды одновременно. См. разделы Групповая регистрация (на стр. 38) и Порядок действий системного администратора при групповой регистрации (на стр. 45).

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

регистрационных данных" на стр. 43).

Если вы провели незначительное обновление конфигурации компьютера, на котором будете использовать ViPNet CSP, ознакомьтесь с разделом Если конфигурация вашего компьютера изменилась (на стр. 43).

Чтобы зарегистрировать ViPNet CSP, выполните следующие действия:

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

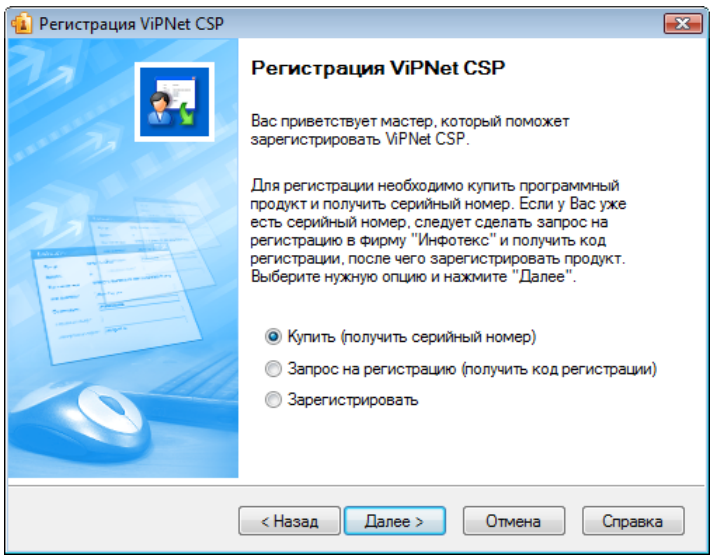

Рисунок 4: Первая страница регистрации

2 Если перед этим:

- вы не приобрели ViPNet CSP, выберите **Купить (получить серийный номер)** (см. "Покупка программы (получение серийного номера)" на стр. 31).

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

- вы уже приобрели ViPNet CSP и имеете серийный номер, выберите **Запрос на регистрацию (получить код регистрации)** (см. "Получение кода регистрации" на стр. 32).

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

- вы уже приобрели ViPNet CSP и получили код регистрации, выберите **Зарегистрировать** (см. "Регистрация ViPNet CSP" на стр. 41).

Покупка программы (получение серийного номера)

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

   В окне вашего браузера откроется страница заказа продуктов ViPNet на сайте компании «Инфотекс». Купите ViPNet CSP через веб-сайт и получите серийный код по электронной почте.

2. Получив серийный номер, вернитесь на страницу **Регистрация ViPNet CSP** (см. "Начало регистрации" на стр. 28) и сделайте запрос на получение кода регистрации (см. "Получение кода регистрации" на стр. 32).

Получение кода регистрации

Чтобы запросить код регистрации для ViPNet CSP:

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 для вас способ. Для этого установите переключатель в одно из положений:
   - **Через Интернет (online)** (см. "Получение кода регистрации через Интернет" на стр. 33).
   - **По электронной почте** (см. "Получение кода регистрации по электронной почте" на стр. 35).
   - **Через веб-страницу** (см. "Получение кода регистрации через веб-страницу" на стр. 37).
   - **По телефону** (см. "Получение кода регистрации по телефону" на стр. 37).
   - **Групповая регистрация (через системного администратора)** (см. "Групповая регистрация" на стр. 38).

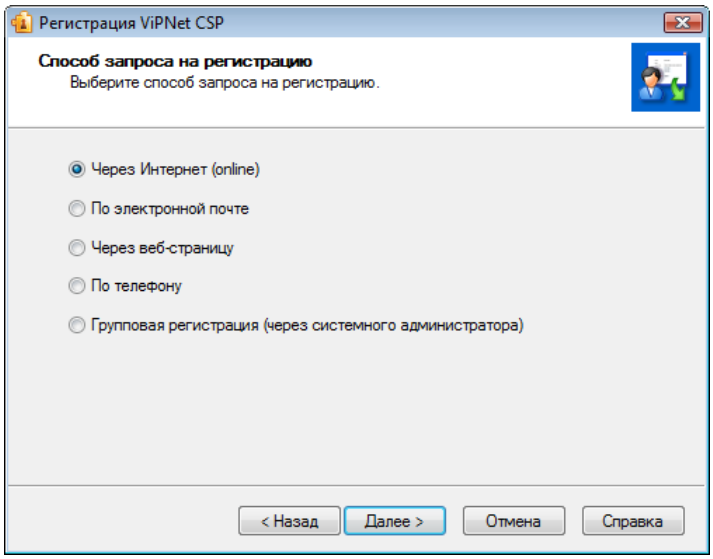

Рисунок 5: Выбор типа запроса на регистрацию

3. Нажмите кнопку **Далее**.

Получение кода регистрации через Интернет

Внимание! Для данного способа регистрации необходим доступ в Интернет.

Если вы выбрали способ регистрации:

Через Интернет (online), **Получение кода регистрации по электронной почте**, или **Групповая регистрация откроется** страница **Регистрационные данные**.

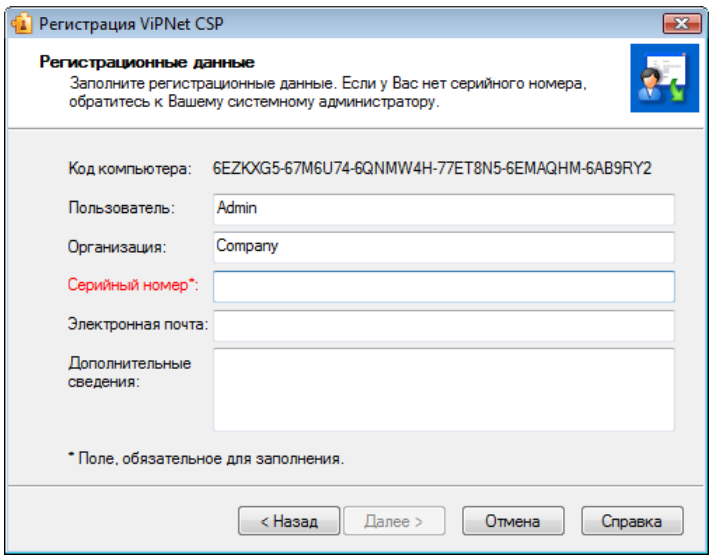

Рисунок 6: Ввод регистрационных данных

На странице **Регистрационные данные** выполните следующие действия:

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

Примечание. Если у вас нет серийного номера, следуйте указаниям раздела Покупка программы (получение серийного номера) (на стр. 31).

Если вы вводили серийный номер в это поле раньше, номер будет введен автоматически.

2 В поле **Пользователь** введите ваше имя. Оно будет использоваться при выпуске лицензии и для обращения к вам. Заполнение этого поля необязательно. По

умолчанию в поле **Пользователь** отображается имя, которое вы ввели во время установки ViPNet CSP.

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

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

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

---

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

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

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

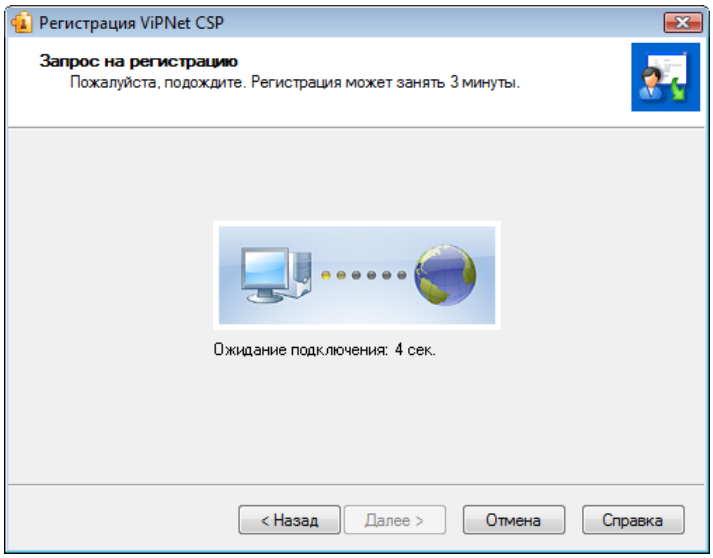

Рисунок 7: Запрос на регистрацию через Интернет

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

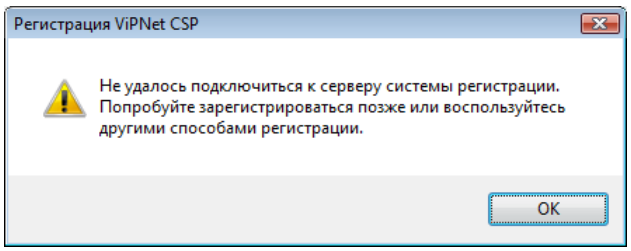

Рисунок 8: Соединение не установлено

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

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

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

Если регистрация прошла успешно, откроется страница **Регистрация ViPNet CSP успешно завершена**. На этой странице дана рекомендация, как безопасно сохранить ваши регистрационные данные (см. "Сохранение регистрационных данных" на стр. 43).

7 Нажмите кнопку **Готово**.

Получение кода регистрации по электронной почте

Внимание! Для данного способа регистрации необходим доступ в Интернет.

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

1 Введите все данные, как описано в разделе Получение кода регистрации через Интернет (на стр. 33).

2 Нажмите кнопку **Далее**. В вашей почтовой программе будет создано новое сообщение электронной почты, содержащее указанные вами регистрационные

данные. Сообщение будет адресовано на электронный почтовый ящик reg@infotecs.biz.

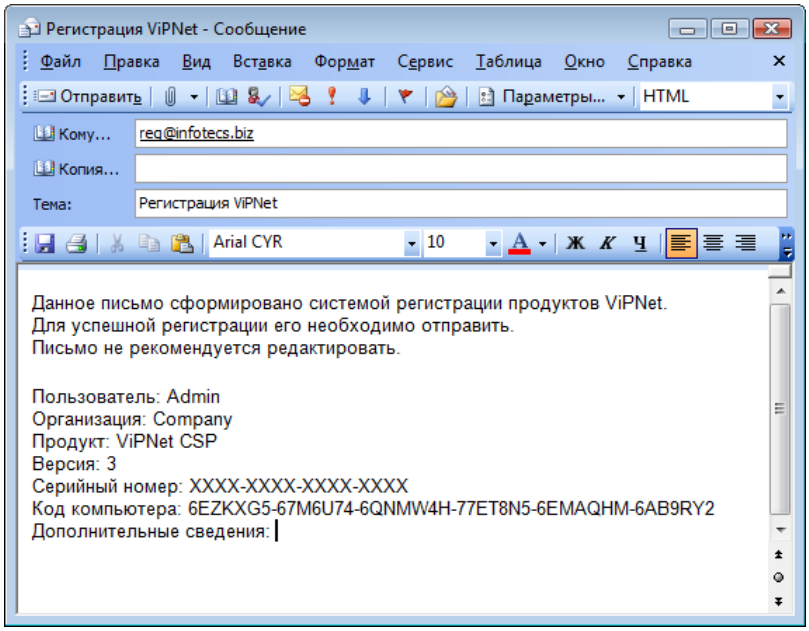

Рисунок 9: Запрос на регистрацию по E-mail

Внимание! Мы не рекомендуем редактировать сообщение с регистрационными данными.

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

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

4 Получив сообщение с кодом регистрации, зарегистрируйте вашу копию ViPNet CSP (см. "Регистрация ViPNet CSP" на стр. 41).

Получение кода регистрации через веб-страницу

Внимание! Для данного способа регистрации необходим доступ в Интернет.

Если вы выбрали способ регистрации **Через веб-страницу**, в вашем Интернет-браузере откроется страница регистрации на сайте компании «Инфотекс».

На странице регистрации введите необходимые данные и нажмите кнопку **Отправить**. После проверки ваших регистрационных данных вы получите код регистрации по электронной почте.

Получив сообщение с кодом регистрации, зарегистрируйте вашу копию ViPNet CSP (см. "Регистрация ViPNet CSP" на стр. 41).

Получение кода регистрации по телефону

Если вы выбрали способ регистрации **По телефону**, откроется страница **Запрос на регистрацию по телефону**.

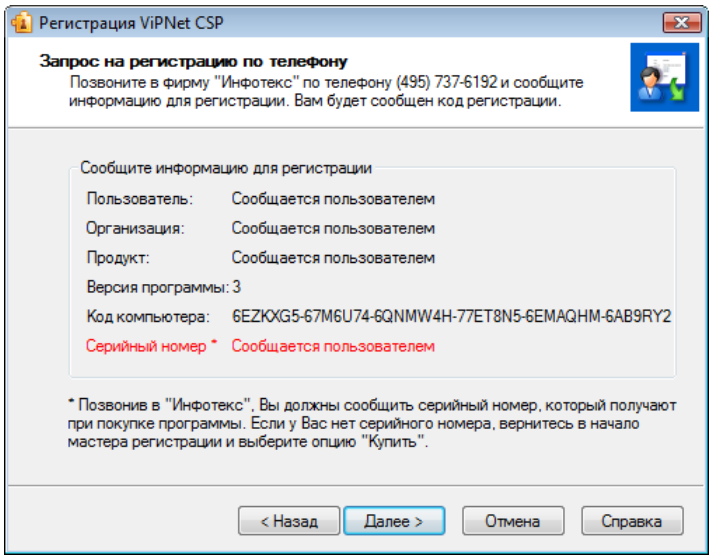

Рисунок 10: Запрос на регистрацию по телефону

На этой странице указаны данные, которые вы должны будете сообщить сотруднику компании «Инфотекс».

1 Позвоните в «Инфотекс» по телефону, указанному в верхней части страницы и сообщите регистрационную информацию, в ответ вам будет сообщен код регистрации.

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

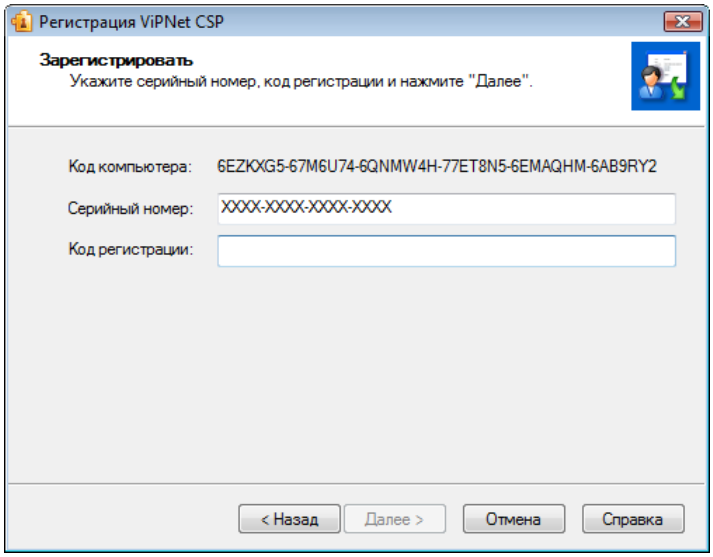

Рисунок 11: Ввод регистрационного кода

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

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

Если вы ввели верные данные, вы попадете на страницу **Регистрация ViPNet CSP успешно завершена**. На этой странице даны рекомендации, как безопасно сохранить ваши регистрационные данные (см. "Сохранение регистрационных данных" на стр. 43).

4 Нажмите **Готово**.

Групповая регистрация

Смысл групповой регистрации состоит в том, что вы перекладываете ответственность за получение кода регистрации на своего системного администратора. Вам не нужно лично запрашивать код регистрации у компании «Инфотекс». Вместо этого вы должны

воспользоваться мастером **Регистрация ViPNet CSP** для формирования файла регистрационных данных и передать файл вашему системному администратору.

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

Чтобы воспользоваться групповой регистрацией:

1. На странице **Способ запроса на регистрацию** выберите **Групповая регистрация (через системного администратора)** и нажмите **Далее**.
2. На странице **Регистрационные данные** введите все данные, как описано в разделе Получение кода регистрации через Интернет (на стр. 33). Нажмите **Далее**.
3. На странице **Сохранение регистрационных** данных нажмите кнопку **Обзор** и укажите папку, в которой будет сохранен файл с вашими регистрационными данными.

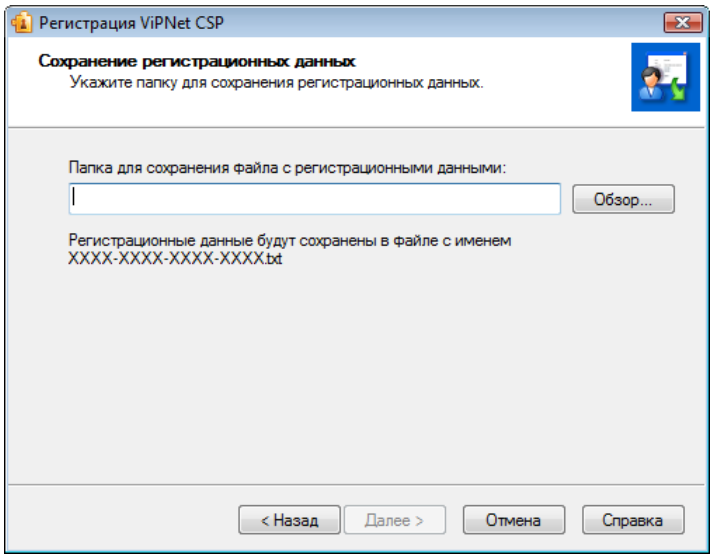

Рисунок 12: Сохранение данных для групповой регистрации

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

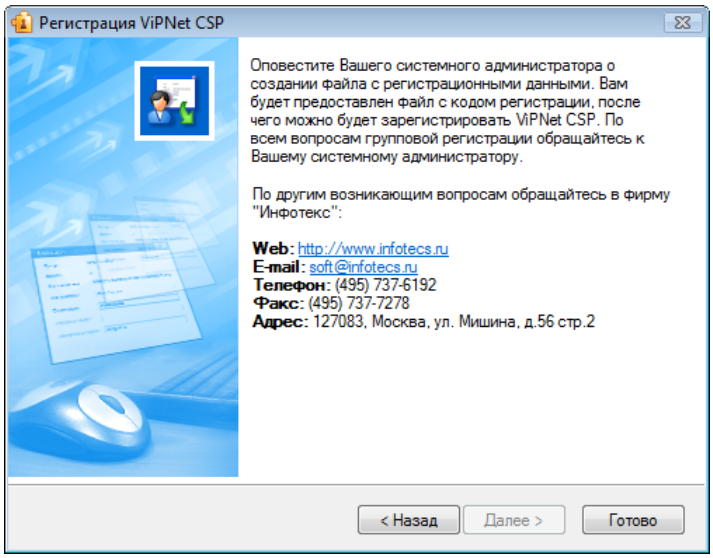

Рисунок 13: Данные для групповой регистрации сохранены

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

6 Передайте файл, содержащий регистрационные данные своему системному администратору.

7 Получив от администратора код регистрации, зарегистрируйте свою копию ViPNet CSP (см. "Регистрация ViPNet CSP" на стр. 41).

Регистрация ViPNet CSP

Получив от компании «Инфотекс» код регистрации, вы можете зарегистрировать вашу копию ViPNet CSP. Для этого:

1 Запустите мастер **Регистрация ViPNet CSP** (см. "Начало регистрации" на стр. 28).

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

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

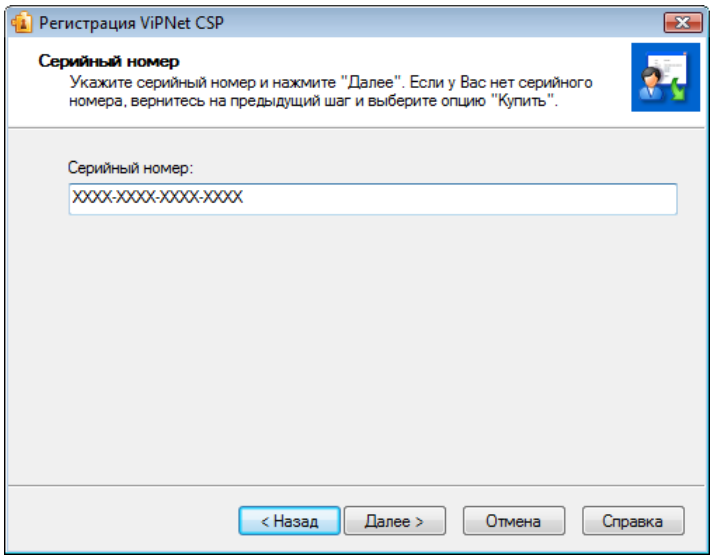

Рисунок 14: Ввод серийного номера

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

4 На странице **Код регистрации**:

- если вы запрашивали код регистрации лично, выберите **Обычная регистрация** и введите код регистрации;

- если запрос на регистрацию делал ваш системный администратор, выберите **Групповая регистрация**, затем нажмите кнопку **Обзор** и укажите путь к файлу, содержащему код регистрации.

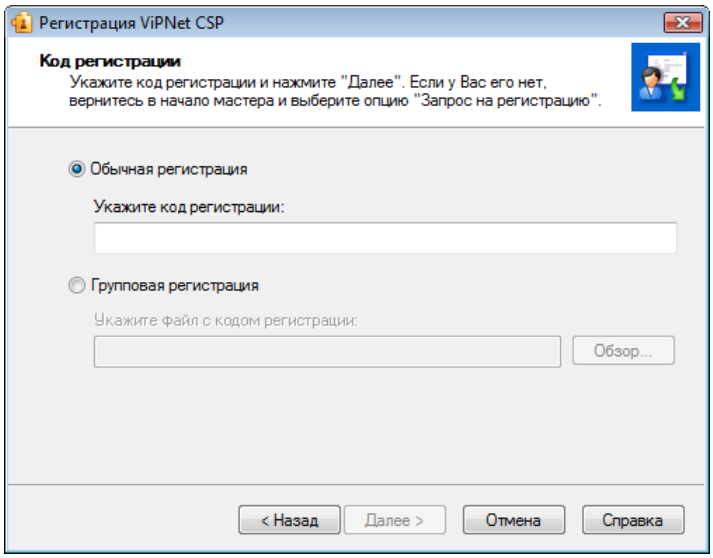

Рисунок 15: Ввод кода регистрации

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

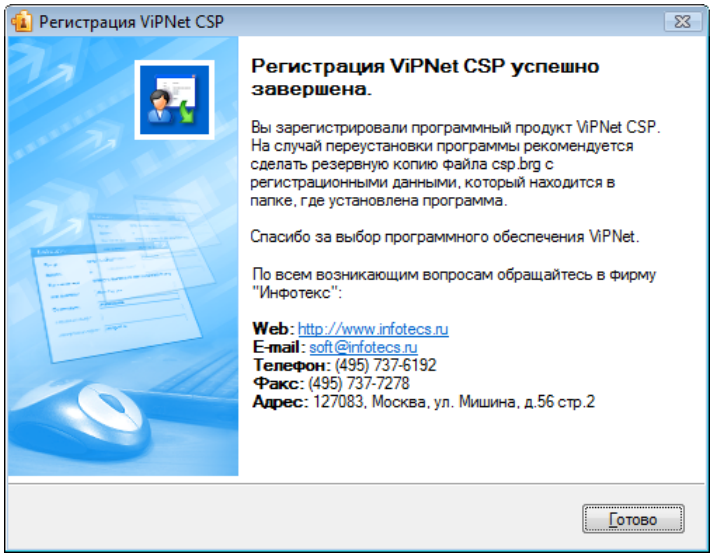

Рисунок 16: Завершение регистрации

6 Нажмите кнопку **Готово**.

7 Сохраните регистрационные данные (см. "Сохранение регистрационных данных" на стр. 43), скопировав в надежное место файл *.brg, находящийся в папке установки программы ViPNet CSP.

Сохранение регистрационных данных

После завершения регистрации программа сохраняет регистрационные данные в файле *.brg, который создается в папке установки программы ViPNet CSP.

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

Мы рекомендуем скопировать файл регистрационных данных в надежне место, так как он может быть полезен при повторной установке ViPNet CSP (например, если вы хотите переустановить программу в другую папку или снова установить программу после форматирования жесткого диска). В таких случаях следует поместить сохраненный файл *.brg в папку установки ViPNet CSP. После перезагрузки компьютера вновь установленная программа будет автоматически зарегистрирована (если регистрационные данные верны и конфигурация компьютера не изменилась).

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

Если конфигурация вашего компьютера изменилась

Если вы обновили конфигурацию компьютера, на котором установлена программа ViPNet CSP, это может сказаться на ее работе. Если изменение конфигурации было значительным (вы заменили большую часть комплектующих), вам придется перерегистрировать вашу копию ViPNet CSP (см. "Получение кода регистрации" на стр. 32).

Если вы сделали небольшие изменения в конфигурации компьютера, вам не придется снова регистрировать ViPNet CSP.

При первом запуске ViPNet CSP после незначительного обновления конфигурации программа выдаст сообщение о том, что в связи с изменением конфигурации компьютера был создан новый файл *.brg. Это значит, что прежний файл

регистрационных данных устарел, и вы не можете использовать его для регистрации программы после переустановки.

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

Порядок действий системного администратора при групповой регистрации

Процедура групповой регистрации позволяет представителю организации (обычно это системный администратор) запросить коды регистрации для нескольких пользователей ViPNet.

Чтобы воспользоваться групповой регистрацией, все пользователи должны иметь серийные номера своих продуктов ViPNet. Если у пользователей нет серийных номеров, их следует купить с помощью мастера **Регистрация ViPNet CSP** (см. "Покупка программы (получение серийного номера)" на стр. 31).

Каждый пользователь на своем компьютере должен создать запрос на групповую регистрацию (см. "Групповая регистрация" на стр. 38). В итоге должен быть создан файл *.txt, содержащий регистрационные данные, который пользователь передает системному администратору.

Если вы являетесь системным администратором:

1. Сохраните файлы с регистрационными данными, полученные от пользователей ViPNet, в одну папку.
2. Склейте все файлы с помощью команды: `copy *.txt registration.all`. Вместо registration.all вы можете использовать любое другое имя файла.
3. Отправьте получившийся файл на адрес электронной почты reg@infotecs.biz. В теме сообщения укажите «ViPNet Group Registration».
4. После обработки запроса компанией «Инфотекс» вы получите сообщение с прикрепленным файлом *.txt. Файл будет содержать коды регистрации для всех пользователей, участвующих в групповой регистрации. После того как вы передадите этот файл пользователям (например, с помощью сетевого диска), они смогут зарегистрировать свои программы ViPNet.

Установка контейнеров и сертификатов

Установка контейнера из папки	47
Установка контейнера с внешнего устройства	50
Установка сертификата и контейнера секретного ключа	52
Ручная установка сертификатов и СОС	56

Установка контейнера из папки

Для работы с защищенными документами и соединениями необходим секретный ключ и соответствующий ему сертификат. Установка ключа и сертификата может выполняться одним контейнером или отдельно установкой сертификата и контейнера секретного ключа (см. "Установка сертификата и контейнера секретного ключа" на стр. 52).

Для установки в систему контейнера из папки на диске:

1 В окне программы **ViPNet CSP** выберите раздел **Контейнеры**.

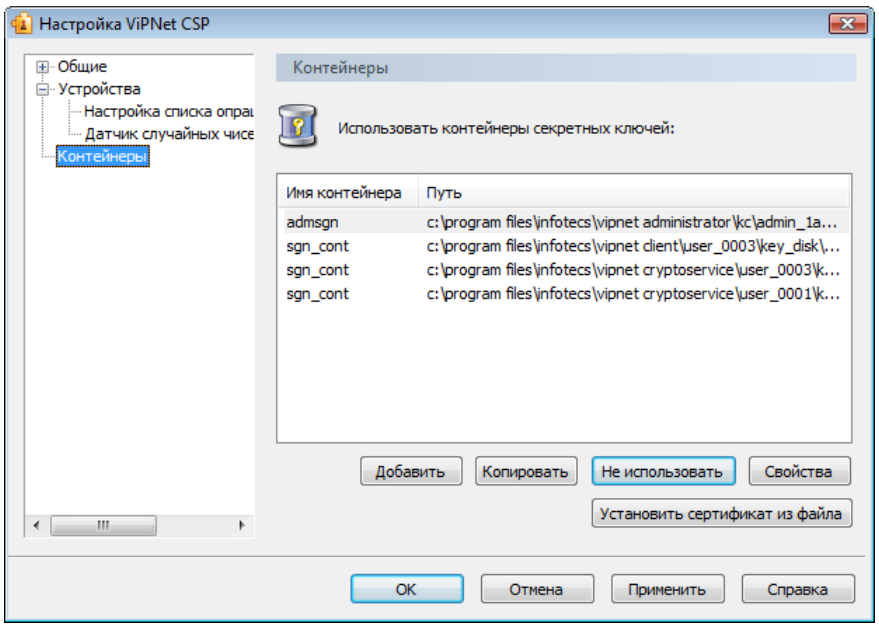

Рисунок 17: Панель управления контейнерами

2 В резделе **Контейнеры** нажмите кнопку **Добавить**.

3 В окне **ViPNet CSP - инициализация контейнера ключа** нажмите кнопку **Обзор**. Укажите путь на диске к папке, содержащей контейнер.

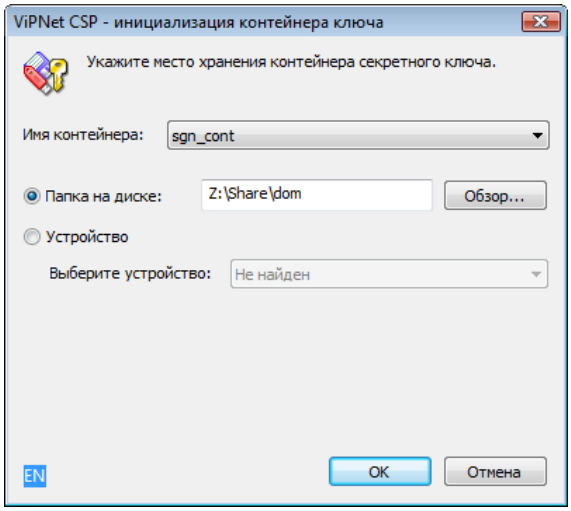

Рисунок 18: Инициализация контейнера ключа из папки

4 Из списка **Имя контейнера** выберите файл контейнера или оставьте значение по умолчанию.

5 Нажмите **ОК**. В окне **Контейнеры** появится сообщение об успешном добавлении контейнера и предложение по установке сертификата в хранилище. Для работы с сертификатами их необходимо установить в хранилище текущего пользователя.

Внимание! Если программа ViPNet CSP установлена на сервере и используется для организации защищенных соединений TLS/SSL, сертификат необходимо устанавливать в хранилище локального компьютера вручную (см. "Установка сертификата пользователя" на стр. 65).

Нажмите кнопку **Да**, сертификаты будут автоматически установлены в хранилище пользователя.

Если сертификаты устанавливать не требуется (или установка будет происходить вручную), нажмите **Нет**.

Для просмотра списка сертификатов в контейнере нажмите кнопку **Сертификаты**.

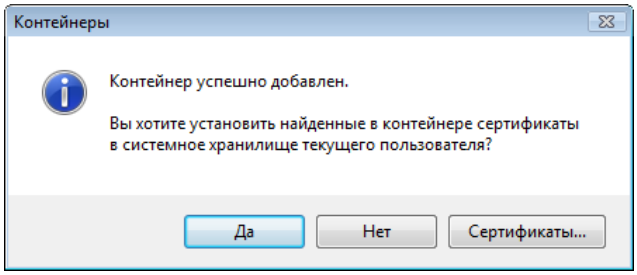

Рисунок 19: Установка сертификатов из контейнера в хранилище

6 После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров (см. Рисунок 17 на стр. 47) появится добавленный контейнер.

Примечание. Установить сертификаты из контейнера можно вручную через окно настройки свойств контейнера (см. "Установка сертификата пользователя" на стр. 65).

После добавления контейнера можно:

- приступать к работе с защищенными документами в MS Office (см. "Цифровая подпись в документах MS Office" на стр. 80);
- подписывать сообщения Microsoft Outlook (см. "Цифровая подпись в Microsoft Outlook" на стр. 93);
- подписывать формы Microsoft Office InfoPath (см. "Цифровая подпись в Microsoft Office InfoPath" на стр. 102);
- подписывать макросы (см. "Цифровая подпись макросов" на стр. 111);
- приступать к работе с защищенными соединениями (см. "Организация защищенного соединения TLS/SSL" на стр. 116).

Установка контейнера с внешнего устройства

Для установки в систему контейнера с внешнего устройства:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. Рисунок 17 на стр. 47).
2. В разделе **Контейнеры** нажмите кнопку **Добавить**.
3. В окне **ViPNet CSP - инициализация контейнера ключа** установите переключатель **Устройство**. Из выпадающего списка выберите нужное устройство.

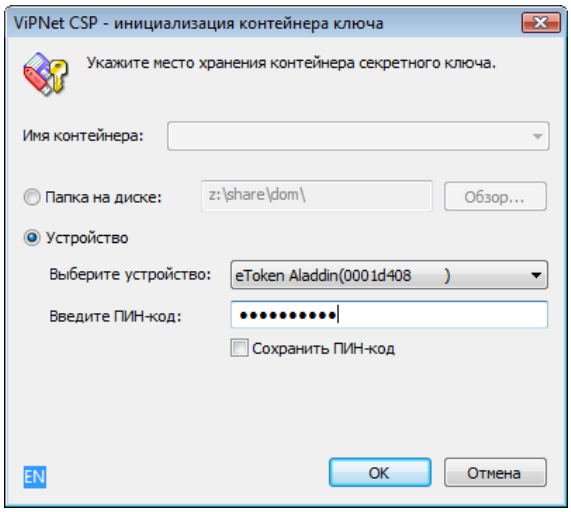

Рисунок 20: Инициализация контейнера ключа с внешнего устройства

4. В поле **Введите ПИН-код** укажите код устройства. Чтобы не вводить ПИН-код каждый раз при обращении к устройству, установите флажок **Сохранить ПИН-код**.

Примечание. Сохранение ПИН-кода к устройству в системе ведет к снижению уровня безопасности.

Подробную информацию о работе с электронными ключами см. в документе «Информация о внешних устройствах хранения данных».

5 Нажмите **ОК**. В окне **Контейнеры** (см. Рисунок 19 на стр. 49) появится сообщение об успешном добавлении контейнера и предложение по установке сертификата в хранилище. Для работы с сертификатами их необходимо установить в хранилище текущего пользователя.

Нажмите кнопку **Да**, сертификаты будут автоматически установлены в хранилище.

Если сертификаты устанавливать не требуется, нажмите **Нет**.

Для просмотра списка сертификатов в контейнере нажмите кнопку **Сертификаты**.

6 После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров (см. Рисунок 17 на стр. 47) появится добавленный контейнер.

Примечание. Установить сертификаты из контейнера можно вручную через окно настройки свойств контейнера (см. "Установка сертификата пользователя" на стр. 65).

После добавления контейнера можно:

- приступать к работе с защищенными документами в MS Office (см. "Цифровая подпись в документах MS Office" на стр. 80);
- подписывать сообщения Microsoft Outlook (см. "Цифровая подпись в Microsoft Outlook" на стр. 93);
- подписывать формы Microsoft Office InfoPath (см. "Цифровая подпись в Microsoft Office InfoPath" на стр. 102);
- подписывать макросы (см. "Цифровая подпись макросов" на стр. 111);
- приступать к работе с защищенными соединениями (см. "Организация защищенного соединения TLS/SSL" на стр. 116).

Установка сертификата и контейнера секретного ключа

Для работы с защищенными документами и соединениями необходим секретный ключ и соответствующий ему сертификат. Установка ключа и сертификата может выполняться путем установки одного контейнера (см. "Установка контейнера из папки" на стр. 47) или путем установки сертификата и контейнера секретного ключа по отдельности.

Если у вас имеется секретный ключ и вам необходимо сформировать на его базе сертификат (или обновить уже имеющийся) – направьте в Удостоверяющий центр запрос на сертификат. Чтобы уточнить правила отправки запроса на сертификат, обратитесь к администратору вашего Удостоверяющего центра.

Внимание! Для выполнения операций по работе с защищенными документами, кроме сертификата пользователя необходимо установить в хранилище корневой сертификат (издателя) и СОС.

Программа ViPNet CSP позволяет установить сертификат и сопоставить его с секретным ключом для шифрования.

Для установки сертификата в хранилище пользователя:

1. В окне программы ViPNet CSP выберите раздел **Контейнеры** (см. Рисунок 17 на стр. 47).
2. В разделе **Контейнеры** нажмите кнопку **Установить сертификат из файла.**
3. В окне **Открыть** укажите путь к файлу сертификата на диске.

4 На странице приветствия **Мастера установки сертификатов** нажмите кнопку **Далее**.

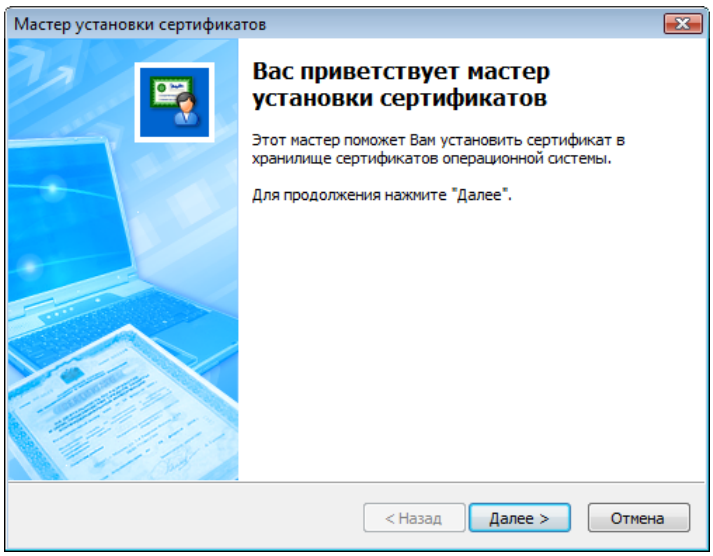

Рисунок 21: Мастер установки сертификата в хранилище

5 На странице **Выбор хранилища сертификатов** укажите, в какое хранилище будет установлен ваш сертификат и нажмите **Далее**.

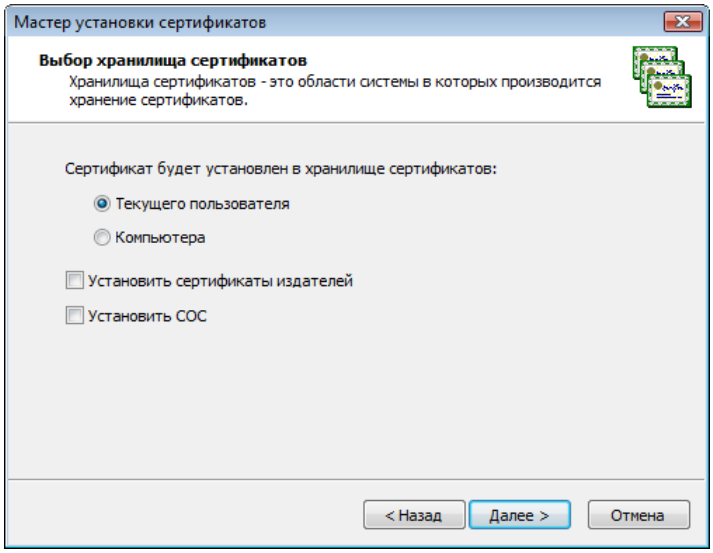

Рисунок 22: Выбор хранилища сертификатов

Примечание. Сертификат следует устанавливать в хранилище пользователя для целей шифрования, расшифрования и подписывания файлов, а также для

доступа к защищенным ресурсам через браузер.

Сертификат устанавливается в хранилище компьютера при использовании ViPNet CSP на web-сервере для организации доступа к защищенным ресурсам.

6 На странице **Готовность к установке сертификата** установите флажок **Указать контейнер с секретным ключом**, если требуется сопоставить сертификату секретный ключ. Нажмите **Далее**.

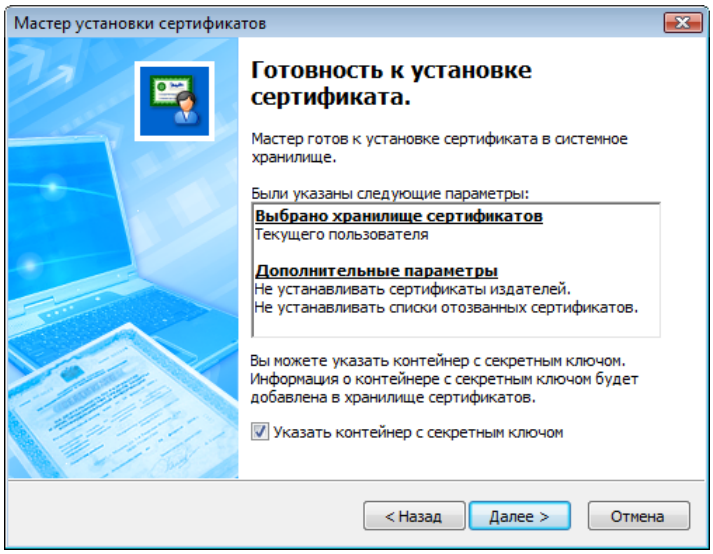

Рисунок 23: Страница Готовность к установке сертификата

7 В случае выбора **Указать контейнер с секретным ключом** откроется окно **ViPNet CSP - инициализация контейнера ключа**. Здесь вы можете указать контейнер из папки на диске (см. "Установка контейнера из папки" на стр. 47) или контейнер на внешнем устройстве (см. "Установка контейнера с внешнего устройства" на стр. 50).

8 На странице **Завершение работы мастера установки сертификата** нажмите **Готово**. Сертификат успешно установлен в хранилище, контейнер секретного ключа, сопоставленного с сертификатом появится в списке контейнеров (см. Рисунок 17 на стр. 47).

Вы можете установить еще один сертификат и секретный ключ либо:

- приступать к работе с защищенными документами в MS Office (см. "Цифровая подпись в документах MS Office" на стр. 80);
- подписывать сообщения Microsoft Outlook (см. "Цифровая подпись в Microsoft Outlook" на стр. 93);

- подписывать формы Microsoft Office InfoPath (см. "Цифровая подпись в Microsoft Office InfoPath" на стр. 102);
- подписывать макросы (см. "Цифровая подпись макросов" на стр. 111);
- приступать к работе с защищенными соединениями (см. "Организация защищенного соединения TLS/SSL" на стр. 116).

Ручная установка сертификатов и СОС

Для выполнения операций с защищенными файлами и соединениями в системное хранилище должны быть установлены сертификат пользователя, издателя и СОС. Установка сертификата пользователя осуществляется средствами программы ViPNet CSP в контейнере или отдельно.

Установка сертификата издателя и СОС выполняется средствами операционной системы. Такой способ установки сертификата также необходим, если ПО ViPNet CSP установлено на web-сервере и используется для организации защищенных TLS/SSL соединений.

Для установки сертификатов и СОС:

1. Откройте папку с файлом сертификата или СОС и щелкните правой кнопкой мыши по значку сертификата. В контекстном меню выберите пункт **Установить сертификат** или **Установить список отзыва (CRL).**
2. В окне приветствия мастера импорта сертификатов нажмите **Далее.**

3 На странице **Хранилище сертификатов** выберите, где следует разместить сертификат, и нажмите **Далее**.

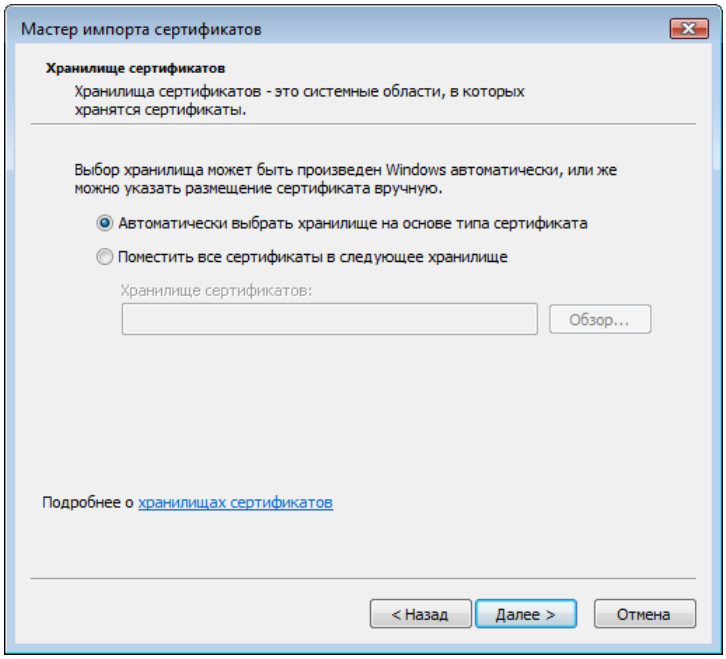

Рисунок 24: Выбор хранилища для сертификата издателя или СОС

4 На странице **Завершение работы 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**. Для того, чтобы установить сертификат, нажмите **Да**.

Устанавливайте только те сертификаты, в подлинности которых вы уверены.

---

5 В окне **Мастер импорта сертификатов** появится сообщение об успешном импорте сертификата. Нажмите **ОК**, установка завершена.

Если вы уже выполнили установку сертификата пользователя, можно:

- приступать к работе с защищенными документами в MS Office (см. "Цифровая подпись в документах MS Office" на стр. 80);
- подписывать сообщения Microsoft Outlook (см. "Цифровая подпись в Microsoft Outlook" на стр. 93);

- подписывать формы Microsoft Office InfoPath (см. "Цифровая подпись в Microsoft Office InfoPath" на стр. 102);
- подписывать макросы (см. "Цифровая подпись макросов" на стр. 111);
- приступать к работе с защищенными соединениями (см. "Организация защищенного соединения TLS/SSL" на стр. 116).

5

Операции с контейнерами

Создание резервной копии контейнера 60

Отключение контейнера 62

Просмотр и настройка свойств контейнера 63

Создание резервной копии контейнера

Вы можете перенести контейнер секретного ключа и сертификата в папку на диске или на внешнее устройство. Эта функция полезна для создания резервной копии контейнера и повышения уровня защиты данных.

Для переноса контейнера:

1. В окне программы **ViPNet CSP** откройте раздел **Контейнеры** (см. Рисунок 17 на стр. 47).
2. В разделе **Контейнеры** выберите контейнер для переноса и нажмите кнопку **Копировать**.
3. В окне **ViPNet CSP - пароль контейнера ключа** введите пароль (или ПИН-код, если контейнер находится на внешнем устройстве) для доступа к контейнеру.

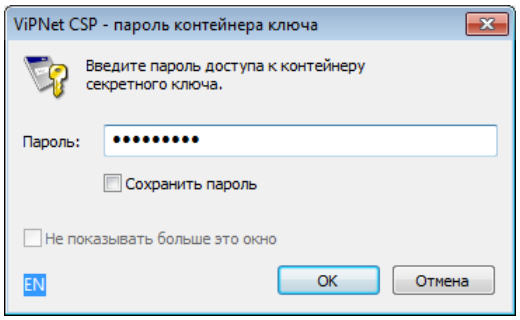

Рисунок 25: Ввод пароля доступа к контейнеру секретного ключа

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

4. В окне **ViPNet CSP - инициализация контейнера ключа** укажите новое имя для контейнера и место расположения. Вы можете скопировать контейнер в папку на диске (см. "Установка контейнера из папки" на стр. 47) или на внешнее устройство (см. "Установка контейнера с внешнего устройства" на стр. 50).

5 Копия контейнера появится в списке контейнеров и в указанной папке (либо на устройстве).

Отключение контейнера

Чтобы не использовать какой-либо секретный ключ и сертификат для работы с защищенными файлами и соединениями, необходимо отключить соответствующий контейнер.

Для отключения контейнера:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. Рисунок 17 на стр. 47).
2. В разделе **Контейнеры** выберите контейнер для отключения и нажмите кнопку **Не использовать.**

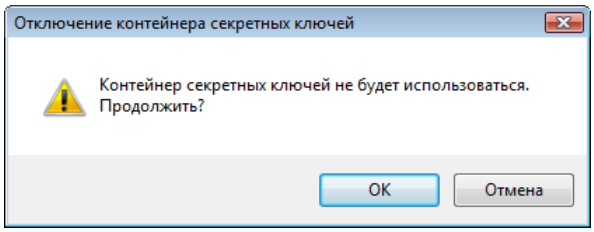

Рисунок 26: Отключение контейнера секретных ключей

3. В окне предупреждения **Контейнер секретных ключей** нажмите **OK.**
4. Контейнер будет удален из списка контейнеров.

Внимание! При отключении контейнера файл контейнера и сертификат из хранилища не удаляются.

При обращении к сертификату отключенного контейнера (например, при попытке подписать документ Microsoft Word) появится окно **ViPNet - инициализация контейнера ключа** (см. Рисунок 18 на стр. 48). Если вы укажете в нем путь к контейнеру на диске или устройстве, контейнер станет активным и появится в списке добавленных контейнеров на панели **Контейнеры (см.** Рисунок 17 **на стр. 47).**

Для полного удаления контейнера из системы необходимо отключить его, удалить файл контейнера из папки или с внешнего устройства и удалить сертификат из хранилища.

Просмотр и настройка свойств контейнера

В окне свойств контейнера можно:

- Просмотреть информацию о секретном ключе и сертификате, которые находятся в контейнере.
- Сменить пароль доступа к контейнеру.
- Удалить сохраненный пароль доступа к контейнеру.
- Произвести ручную установку сертификата пользователя.
- Проверить или удалить секретный ключ, хранящийся в контейнере.

Смена пароля к контейнеру

Для смены пароля к контейнеру в папке на диске:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 47).
2. В разедел **Контейнеры** выберите контейнер, к которому требуется сменить пароль, и нажмите кнопку **Свойства** либо дважды щелкните по нужному контейнеру.

3 В окне **Свойства контейнера** нажмите кнопку **Сменить пароль**.

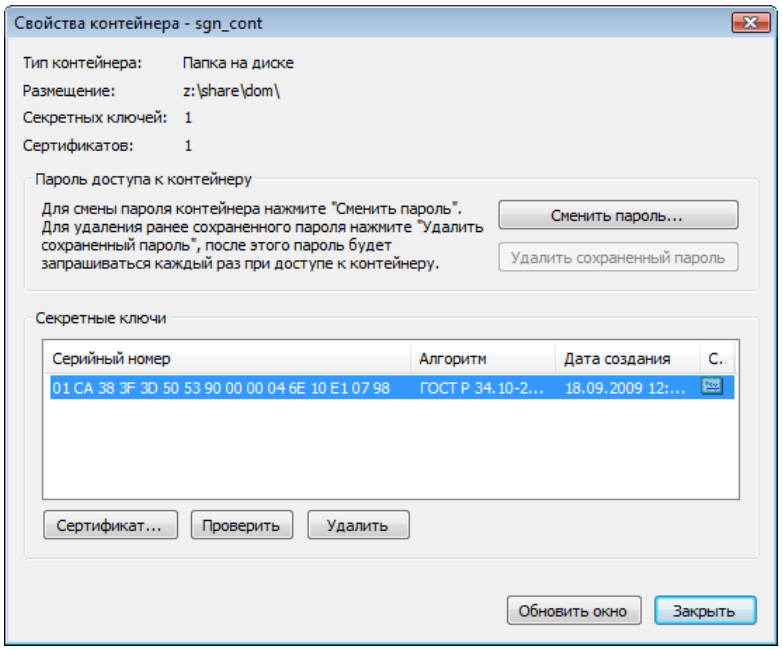

Рисунок 27: Окно Свойства контейнера

4 В окне **Пароль** введите текущий пароль доступа к контейнеру и нажмите кнопку **ОК**.

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

---

5 В окне **ViPNet CSP - пароль контейнера ключа** укажите новый пароль в полях **Введите пароль** и **Подтверждение**. Нажмите **ОК**.

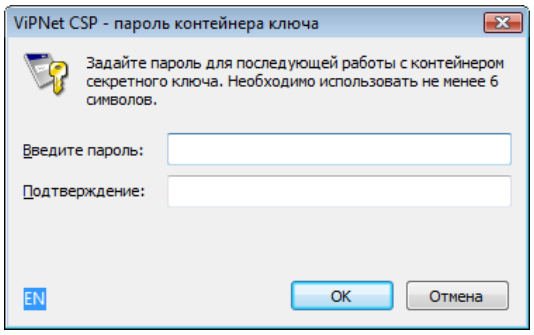

Рисунок 28: Смена пароля доступа к контейнеру

Пароль доступа к контейнеру изменен.

Удаление сохраненного пароля

Для удаления ранее сохраненного в системе пароля к контейнеру:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 47).
2. В разделе **Контейнеры** выберите контейнер, сохраненный пароль к которому требуется удалить и нажмите кнопку **Свойства** либо дважды щелкните по нужному контейнеру.
3. В окне **Свойства контейнера** (см. Рисунок 27 на стр. 64) нажмите кнопку **Удалить сохраненный пароль**. Пароль будет удален.

Установка сертификата пользователя

Установка сертификата пользователя вручную может понадобиться в случае, если ПО ViPNet CSP используется на сервере для организации доступа к защищенным ресурсам по протоколам TLS/SSL. Сертификат сервера необходимо устанавливать в хранилище локального компьютера.

Для установки сертификата:

1. В окне программы **ViPNet CSP** выберите раздел **Контейнеры** (см. рисунок на стр. 47).
2. В разделе **Контейнеры** выберите контейнер, сертификат которого требуется установить, и нажмите кнопку **Свойства** либо дважды щелкните по нужному контейнеру.
3. В окне **Свойства контейнера** (см. Рисунок 27 на стр. 64) выберите нужный секретный ключ и нажмите кнопку **Сертификат**.

4 В окне **Сертификат** на вкладке **Общие** нажмите кнопку **Установить сертификат...**. Запустится мастер установки сертификатов (см. Рисунок 21 на стр. 53).

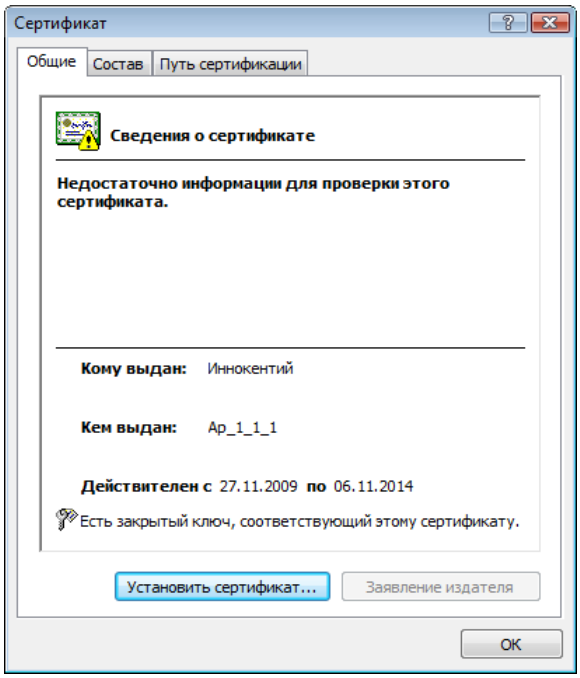

Рисунок 29: Окно свойств сертификата

5 На странице приветствия **Мастера установки сертификатов** нажмите **Далее**.

6 На странице **Выбор хранилища сертификатов** укажите нужное хранилище.

7 На странице **Готовность к установке сертификата** снимите флажок **Указать контейнер с секретным ключом** и нажмите **Далее**.

8 На странице **Завершение работы мастера установки сертификатов** нажмите **Готово**. Сертификат установлен в хранилище.

Кроме сертификата пользователя, для работы с защищенными файлами и соединениями необходимо установить сертификат издателя и СОС (см. "Ручная установка сертификатов и СОС" на стр. 56).

Проверка соответствия секретного ключа и сертификата

Чтобы проверить соответствие секретного ключа и сертификата, хранящихся в контейнере:

1 В окне **Свойства контейнера** (см. Рисунок 27 на стр. 64) в списке **Секретные ключи** выберите строку секретного ключа.

2 Нажмите кнопку **Проверить.**

3 В окне **ViPNet CSP - пароль контейнера ключа** (см. Рисунок 25 на стр. 60) введите пароль доступа к контейнеру и нажмите **OK.**

После этого программа сформирует фрагмент данных, подпишет его с помощью секретного ключа, а затем проверит цифровую подпись с помощью сертификата открытого ключа. Таким образом, будет проверена пригодность секретного ключа и его совместимость с сертификатом, хранящимся в контейнере.

Примечание. Проверка возможна только в том случае, если в контейнере есть сертификат, соответствующий секретному ключу.

При проверке секретного ключа проверка действительности сертификата (срок его действия, присутствие в списках отозванных сертификатов и пр.) **не выполняется.**

При успешном выполнении проверки секретного ключа программа выдаст соответствующее сообщение.

Удаление секретного ключа

Чтобы удалить секретный ключ из контейнера:

1 В окне **Свойства контейнера** (см. Рисунок 27 на стр. 64) в списке **Секретные ключи** выберите строку секретного ключа.

2 Нажмите кнопку **Удалить**. Программа выдаст предупреждение о том, что удаленные секретные ключи невозможно восстановить.

3 В окне предупреждения нажмите **Да.**

Выбранный секретный ключ и соответствующий ему сертификат будут удалены из контейнера.

6

Работа с внешними устройствами

Просмотр списка подключенных устройств 69

Настройка списка опрашиваемых устройств 71

Инициализация устройства 72

Смена ПИН-кода 74

Просмотр списка подключенных устройств

ViPNet CSP позволяет работать с контейнерами сертификатов, которые хранятся на внешних устройствах.

Для просмотра подключенных устройств и хранящихся на них контейнеров ключей:

1 В окне программы **ViPNet CSP** откройте раздел **Устройства**.

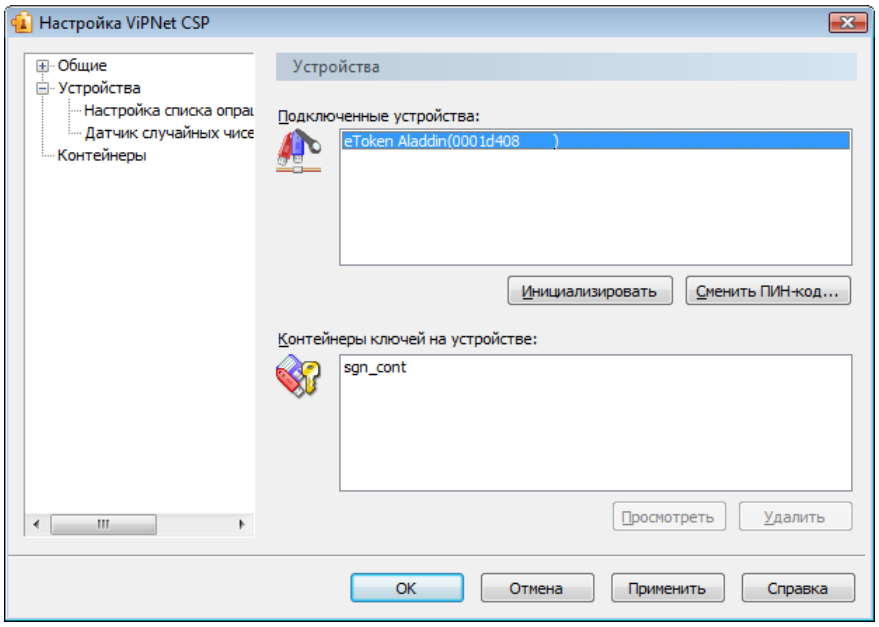

Рисунок 30: Вкладка Устройства

2 В списке **Подключенные устройства** выберите нужное устройство.

Примечание. В списке **Подключенные устройства** отображаются только те устройства, которые в данный момент подключены или вставлены в соответствующий считыватель.

3 В списке **Контейнеры ключей на устройстве** выберите контейнер.

- Чтобы просмотреть свойства выбранного контейнера, нажмите кнопку **Просмотреть** (см. "Просмотр и настройка свойств контейнера" на стр. 63).
- Чтобы удалить контейнер с устройства, нажмите кнопку **Удалить.**

Примечание. Если список **Контейнеры ключей на устройстве** пуст, это значит, что на выбранном устройстве нет контейнеров.

Настройка списка опрашиваемых устройств

На вкладке **Настройка списка опрашиваемых устройств** можно указать типы устройств, которые будут опрашиваться при поиске электронного ключа.

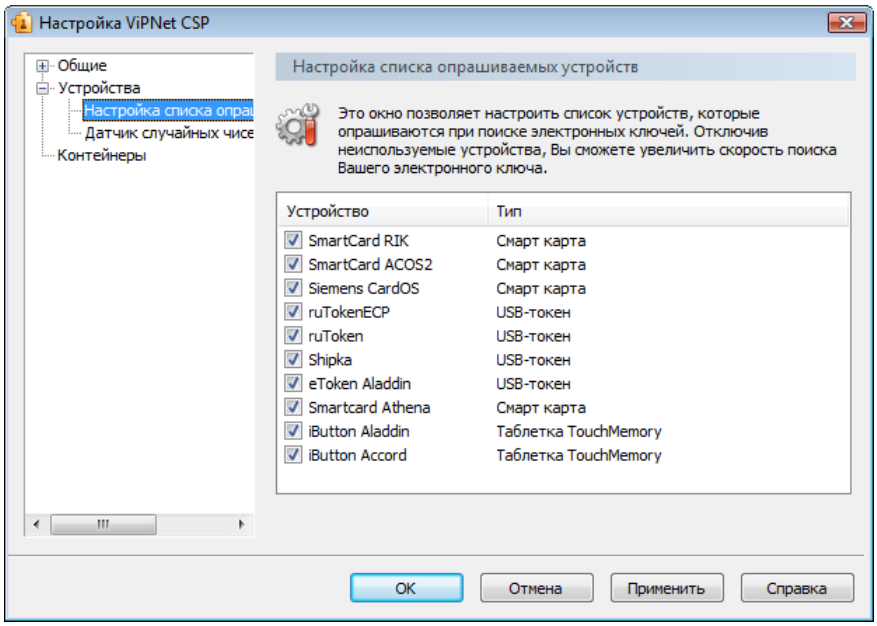

Рисунок 31: Настройка списка опрашиваемых устройств

По умолчанию ViPNet CSP проводит поиск всех поддерживаемых типов устройств. Чтобы сократить время поиска нужного электронного ключа, отключите неиспользуемые устройства:

1. В окне программы **ViPNet CSP** откройте раздел **Настройка списка опрашиваемых устройств**.
2. Снимите флажки напротив типов устройств, которые не используются.
3. Чтобы сохранить настройки, нажмите кнопку **Применить**.

Инициализация устройства

Внимание! В случае, если вы используете устройство ОКБ САПР Шипка (Shipka) и произвели инициализацию в приложении ViPNet, для корректной работы устройства вам так же необходимо выполнить инициализацию с помощью утилиты ОКБ САПР "Параметры авторизации". Подробнее см. в документе "Информация о внешних устройствах хранения данных".

Утилита "Параметры авторизации" поставляется ОКБ САПР и не входит в комплект поставки продуктов ViPNet.

Чтобы инициализировать подключенное устройство:

1. В окне программы **ViPNet CSP** откройте раздел **Устройства** (см. Рисунок 30 на стр. 69).
2. Выберите устройство из списка **Подключенные устройства**.

Примечание. В списке **Подключенные устройства** отображаются только те устройства, которые в данный момент подключены или вставлены в соответствующий считыватель.

3. Нажмите кнопку **Инициализировать**. Появится предупреждение о том, что при инициализации все данные на устройстве будут потеряны.
4. В окне предупреждения нажмите **Да**. Откроется окно **Инициализация.**

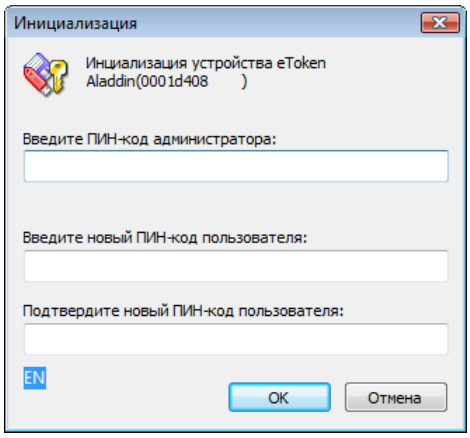

Рисунок 32: Окно Инициализация

5 В окне **Инициализация**:

- В поле **Введите ПИН-код администратора** введите ПИН-код администратора устройства.
- В поле **Введите новый ПИН-код пользователя** задайте ПИН-код доступа к устройству и подтвердите его в поле **Подтвердите новый ПИН-код пользователя**.

6 Нажмите кнопку **OK**.

Устройство будет инициализировано. При этом все хранившиеся на нем данные будут потеряны. Для доступа к устройству будет использоваться заданный ПИН-код пользователя.

Смена ПИН-кода

Чтобы сменить ПИН-код устройства:

1 В окне программы **ViPNet CSP** откройте раздел **Устройства** (см. Рисунок 30 на стр. 69).

2 Выберите устройство из списка **Подключенные устройства**.

> **Примечание.** В списке **Подключенные устройства** отображаются только те устройства, которые в данный момент подключены или вставлены в соответствующий считыватель.

3 Нажмите кнопку **Сменить ПИН-код**. Откроется окно **Смена ПИН-кода**.

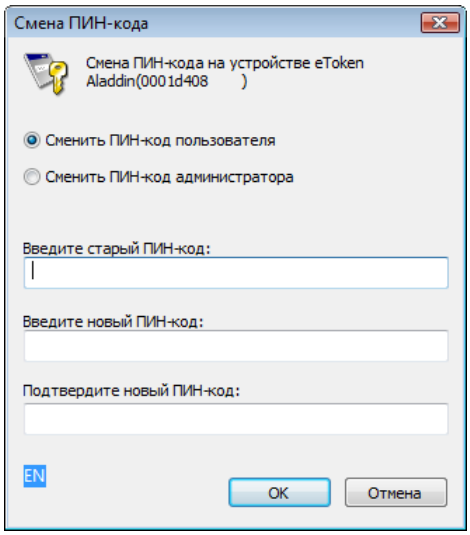

Рисунок 33: Окно Смена ПИН-кода

4 Если требуется сменить ПИН-код пользователя, с помощью переключателя выберите **Сменить ПИН-код пользователя** (выбрано по умолчанию).

Если требуется сменить ПИН-код администратора устройства, выберите **Сменить ПИН-код администратора**.

5 В поле **Введите старый ПИН-код** введите действующий ПИН-код.

6 В поле **Введите новый ПИН-код** задайте новый ПИН-код и подтвердите его в поле **Подтвердите Новый ПИН-код**.

7 Нажмите кнопку **OK**.

ПИН-код устройства будет изменен.

7

Дополнительные возможности

Проверка целостности модулей программы 77

Использование датчика случайных чисел 78

Проверка целостности модулей программы

Для визуального контроля наличия необходимых библиотек:

1. В левой панели окна программы ViPNet CSP выберите элемент **Состав**.
2. В таблице **Исполняемые модули** проверьте состав библиотек.

Для проверки целостности библиотек:

1. В окне программы ViPNet CSP выберите раздел **Состав**.
2. В разделе **Состав** нажмите кнопку **Тестировать**.

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

   По окончании проверки отобразится окно с сообщением о результатах проверки.

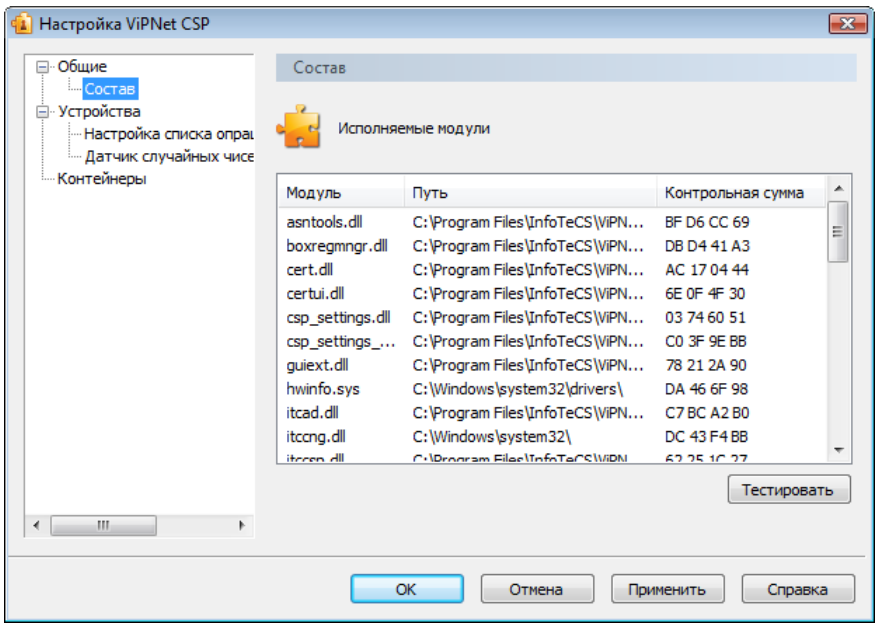

Рисунок 34: Панель Состав

Использование датчика случайных чисел

Датчик случайных чисел позволяет генерировать случайные последовательности чисел, на основе которых формируются секретные ключи.

Примечание. В состав криптопровайдера ViPNet CSP входит только **Биологический** датчик случайных чисел («Электронная рулетка»). Если в системе установлены датчики случайных чисел других производителей, их можно выбрать для использования в ViPNet CSP. В противном случае в списке присутствует только **Биологический** датчик.

Чтобы выбрать используемый датчик случайных чисел:

1 На левой панели окна **Настройка ViPNet CSP** разверните элемент **Устройства**, затем выберите **Датчик случайных чисел**.

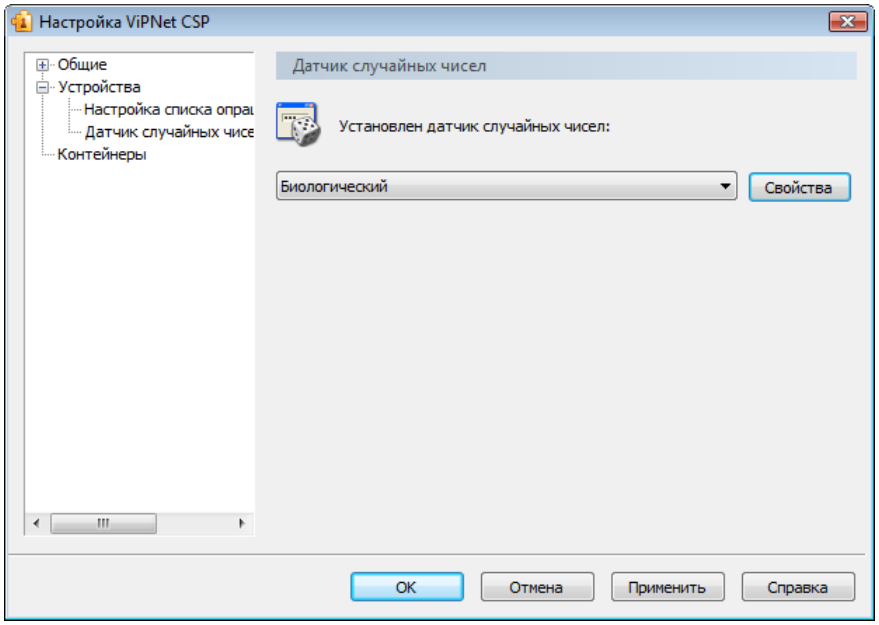

Рисунок 35: Вкладка Датчик случайных чисел

2 Из списка **Установлен датчик случайных чисел** выберите датчик, который будет использоваться для получения случайных чисел (например, при генерации секретных ключей).

3 Для сохранения параметров нажмите кнопку **Применить**.

4 Для просмотра информации о выбранном датчике случайных чисел нажмите кнопку **Свойства**.

Чтобы проверить работоспособность датчика случайных чисел, в окне **Свойства** нажмите кнопку **Тестировать**. После проведения теста программа выдаст сообщение о его результате.

8

Цифровая подпись в документах MS Office

Подписание документа	81
Просмотр цифровой подписи	84
Удаление цифровой подписи	86
Видимая строка подписи в документах Word и Excel	87
Подписание базы данных Microsoft Access 2007	91

Подписание документа

Средства пакета Microsoft Office позволяют заверить цифровой подписью созданные с его помощью документы.

В данном разделе содержится информация о том, как добавить цифровую подпись в документы Microsoft Word, Excel и PowerPoint в случаях использования Microsoft Office 2003 и Microsoft Office 2007.

Microsoft Office 2003

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

1. Сохраните документ.
2. В меню **Сервис** выберите пункт **Параметры**.
3. Выберите вкладку **Безопасность**, на вкладке нажмите кнопку **Цифровые подписи**.
4. В окне **Цифровая подпись** нажмите кнопку **Добавить**.

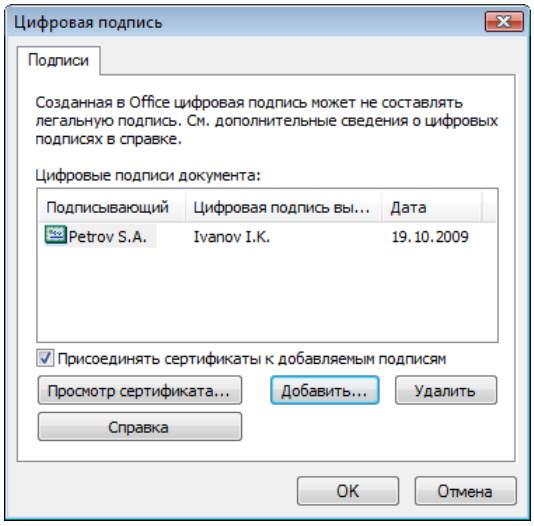

Рисунок 36: Окно Цифровая подпись

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

5 Откроется окно **Выбор сертификата** со списком доступных сертификатов цифровой подписи. Чтобы просмотреть сведения о сертификате, выделите его и нажмите кнопку **Просмотр сертификата**.

6 В окне **Выбор сертификата** выделите нужный сертификат и нажмите **ОК**. Откроется окно **ViPNet CSP – пароль контейнера ключа** (см. Рисунок 25 на стр. 60).

7 Введите пароль и нажмите **ОК**. Выбранный сертификат появится в списке **Цифровые подписи документа** в окне **Цифровая подпись**.

8 Дважды нажмите **ОК**, чтобы закрыть диалоговые окна. В строке состояния в окне документа появится значок  , означающий, что документ содержит цифровую подпись.

Если после подписания документа в него были внесены какие-либо правки, при попытке сохранить документ появится предупреждение о том, что при сохранении все цифровые подписи будут удалены. При необходимости вы можете снова подписать документ после сохранения изменений.

Microsoft Office 2007

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

1 Нажмите кнопку **Microsoft Office**  , выберите пункт **Подготовка**, а затем нажмите **Добавить цифровую подпись**. Откроется окно **Подписание**.

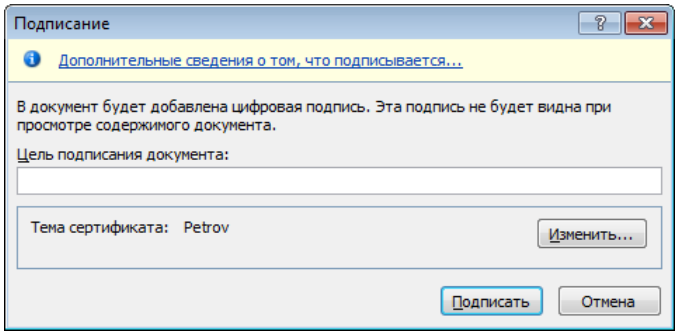

Рисунок 37: Окно Подписание

2 В окне **Подписание** вы можете заполнить поле **Цель подписания документа**. Ниже в этом же окне приведены краткие сведения о сертификате, которым предполагается подписать документ. При необходимости нажмите кнопку **Изменить** и выберите другой сертификат.

3 Выбрав сертификат, нажмите кнопку **Подписать**. Откроется окно **ViPNet CSP – пароль контейнера ключа** (см. Рисунок 25 на стр. 60).

4 Введите пароль и нажмите **ОК**. Появится сообщение об успешном добавлении цифровой подписи и сохранении документа. В строке состояния окна документа появится значок  , означающий, что документ содержит цифровую подпись.

После добавления цифровой подписи редактирование документа невозможно. Чтобы внести в документ какие-либо изменения, удалите цифровую подпись.

Просмотр цифровой подписи

Чтобы просмотреть сертификат цифровой подписи в документе Microsoft Word, Excel или PowerPoint, выполните следующие действия.

Microsoft Office 2003

1. В меню **Сервис** выберите пункт **Параметры**.
2. Выберите вкладку **Безопасность**, на вкладке нажмите кнопку **Цифровые подписи**.
3. В окне **Цифровая подпись** выберите сертификат подписи и нажмите кнопку **Просмотр сертификата** (см. Рисунок 36 на стр. 81).

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

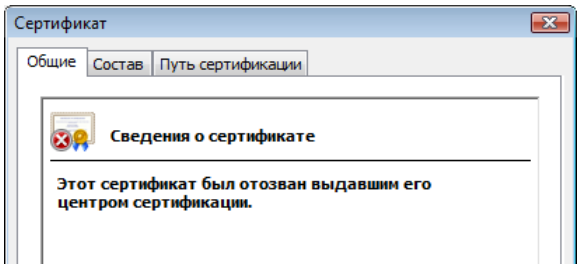

Рисунок 38: Отозванный сертификат

Microsoft Office 2007

1 Нажмите кнопку **Microsoft Office**  , выберите пункт **Подготовка**, а затем нажмите **Просмотр подписей**. Откроется панель **Подписи**.

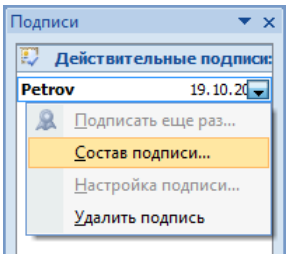

Рисунок 39: Панель Подписи

Примечание. Панель **Подписи** можно вызвать, нажав значок цифровой подписи  в строке состояния.

---

2 На панели **Подписи** наведите указатель мыши на строку подписи и щелкните правой кнопкой мыши (либо нажмите кнопку вызова меню справа), в меню выберите пункт **Состав подписи**.

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.

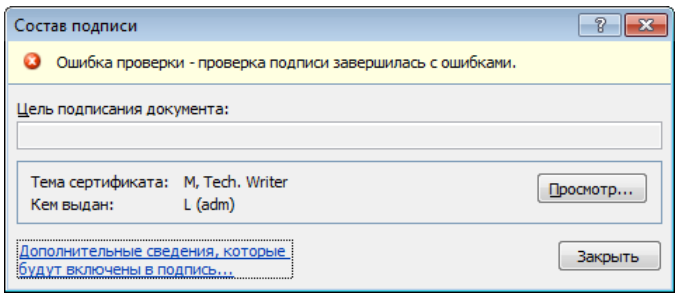

Рисунок 40: Состав подписи

4 Чтобы открыть сертификат, нажмите кнопку **Просмотр**. Чтобы просмотреть дополнительные сведения о подписи, нажмите ссылку **Дополнительные сведения, которые будут включены в подпись...**

Удаление цифровой подписи

Чтобы удалить из документа цифровую подпись, выполните следующие действия.

Microsoft Office 2003

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

1. В меню **Сервис** выберите пункт **Параметры**.
2. Выберите вкладку **Безопасность**, на вкладке нажмите кнопку **Цифровые подписи**.
3. В окне **Цифровая подпись** (см. Рисунок 36 на стр. 81) выберите подпись для удаления. Вы можете просмотреть сертификат подписи, нажав кнопку **Просмотр сертификата**.
4. Выбрав цифровую подпись, нажмите **Удалить**. Подпись будет удалена из документа.

Microsoft Office 2007

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

1. Откройте панель **Подписи**. Для этого выполните одно из двух действий:
   - Нажмите кнопку **Microsoft Office**  , выделите пункт **Подготовка**, а затем нажмите **Просмотр подписей**.
   - Нажмите значок цифровой подписи  в строке состояния окна документа.
2. На панели **Подписи** (см. Рисунок 39 на стр. 85) наведите указатель мыши на строку подписи и щелкните правой кнопкой мыши (либо нажмите кнопку вызова меню справа), в меню выберите пункт **Удалить подпись.**
3. В окне подтверждения нажмите **Да**. Цифровая подпись будет удалена из документа.

Видимая строка подписи в документах Word и Excel

Приложения Microsoft Word 2007 и Microsoft Excel 2007 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 цифровую подпись для удостоверения личности подписавшего.

Вставка видимой строки подписи

Чтобы добавить в документ видимую строку для подписи:

1. Поместите курсор в то место в документе, куда требуется вставить строку подписи.
2. На вкладке **Вставка** в группе **Текст** нажмите кнопку **Строка подписи**. Откроется окно **Настройка подписи**.

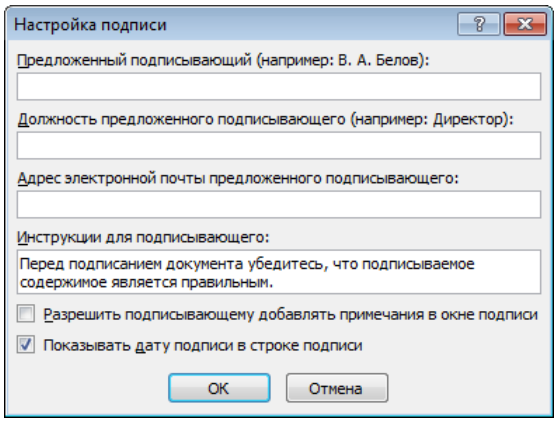

Рисунок 41: Окно Настройка подписи

3. 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).

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

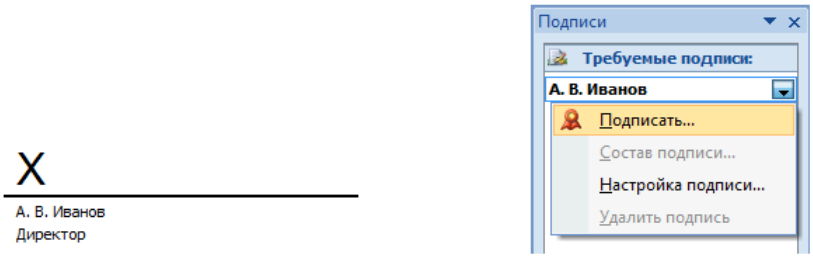

Рисунок 42: Видимая строка подписи и ее представление в панели Подписи

До того как в строку подписи будет добавлена цифровая подпись, вы можете изменить ее настройки. Для этого:

1 Нажмите кнопку **Microsoft Office** , выделите пункт **Подготовка**, а затем нажмите **Просмотр подписей**. Откроется панель **Подписи** (см. Рисунок 39 на стр. 85).

2 На панели **Подписи** щелкните правой кнопкой мыши на названии строки подписи (или щелкните правой кнопкой мыши на самой строке подписи в документе), в меню выберите пункт **Настройка подписи**.

3 В окне **Настройка подписи** (см. Рисунок 41 на стр. 87) внесите необходимые изменения и нажмите **ОК**.

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

Подписание строки подписи

В приложениях Microsoft Word 2007 и Microsoft Excel 2007 вы можете подписать видимую строку подписи, содержащуюся в документе.

Примечание. Если открыть документ с видимой строкой подписи в приложении более ранней версии, чем Microsoft Office 2007, строка подписи будет заменена обычным рисунком и ее невозможно будет подписать.

Чтобы добавить цифровую подпись в строку подписи:

1. Нажмите кнопку **Microsoft Office**  , выберите пункт **Подготовка**, а затем нажмите **Просмотр подписей**. Откроется панель **Подписи** (см. Рисунок 39 на стр. 85).
2. На панели **Подписи** щелкните правой кнопкой мыши на названии строки подписи (или щелкните правой кнопкой мыши на самой строке подписи в документе), в меню выберите пункт **Подписать.**
3. В окне **Подписание** введите свое имя либо нажмите ссылку **Выбрать рисунок**, чтобы вставить графическое изображение подписи. Ниже дано краткое описание сертификата, которым предполагается подписать документ. Чтобы подписать документ другим сертификатом, нажмите кнопку **Изменить** и выберите сертификат.

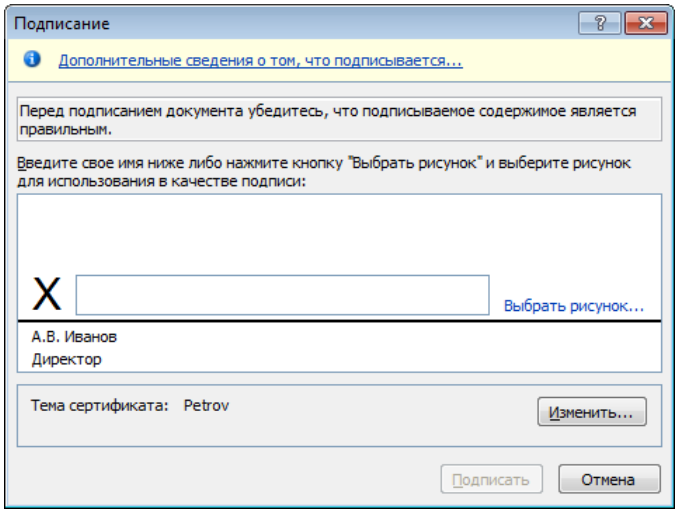

Рисунок 43: Подписание строки подписи

4. После ввода имени и выбора сертификата нажмите кнопку **Подписать**. Откроется диалоговое окно **ViPNet CSP – пароль контейнера ключа** (см. Рисунок 25 на стр. 60).
5. Введите пароль и нажмите **ОК**. В строке подписи появится имя подписавшего или графическое изображение его подписи.

Если сертификат подписи по каким-либо причинам ненадежен, над строкой подписи будет стоять пометка **Недействительная подпись**.

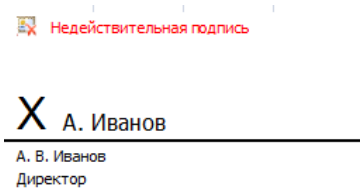

Рисунок 44: Недействительная подпись

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

Просмотреть состав подписи (см. "Просмотр цифровой подписи" на стр. 84) или удалить подпись (см. "Удаление цифровой подписи" на стр. 86) из видимой строки подписи можно так же, как в случае невидимой подписи:

1. Нажмите кнопку **Microsoft Office**, выделите пункт **Подготовка**, а затем нажмите **Просмотр подписей** (или нажмите значок цифровой подписи в строке состояния окна документа). Откроется панель **Подписи** (см. Рисунок 39 на стр. 85).
2. На панели **Подписи** щелкните правой кнопкой мыши на названии строки подписи (или щелкните правой кнопкой мыши на самой строке подписи в документе). В зависимости от того, что вы хотите сделать, выберите в меню пункт **Состав подписи** или **Удалить подпись**.

Подписание базы данных Microsoft Access 2007

В приложении Microsoft Access 2007 предусмотрена возможность подписания базы данных при публикации. После создания файла базы данных в формате Microsoft Access 2007 его можно упаковать, добавить электронную цифровую подпись, а затем распространить подписанный пакет среди других пользователей. Пользователи, получившие пакет, могут извлечь из него базу данных и далее работать с ней.

Примечание. Базы данных более ранних версий, чем Microsoft Access 2007, невозможно заверить цифровой подписью, но можно подписать отдельные компоненты базы данных. Подробнее см. в главе Подписание макросов (см. "Цифровая подпись макросов" на стр. 111).

Чтобы упаковать и подписать базу данных Microsoft Access 2007:

1. Нажмите кнопку **Microsoft Office**  , выберите пункт **Опубликовать**, а затем нажмите **Упаковать и подписать**. Откроется окно **Выбор сертификата.**
2. Выберите сертификат цифровой подписи и нажмите кнопку **ОК**. Откроется окно **Создать подписанный пакет Microsoft Office Access.**

Внимание! Для подписания базы данных цифровой подписью нужно выбрать сертификат, который имеет атрибут «Подписывание кода» в расширенном использовании ключа. Если сертификата с таким атрибутом нет, вы не сможете создать подписанный пакет. За нужным сертификатом обратитесь к администратору Удостоверяющего и Ключевого центра (см. Руководство администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр]).

3. Выберите папку для сохранения подписанного пакета.
4. В поле **Имя файла** введите имя для пакета и нажмите кнопку **Создать.**

   Подписанный пакет базы данных будет сохранен в указанной папке.

9

Цифровая подпись в Microsoft Outlook

Добавление подписи ко всем сообщениям 94

Добавление подписи к отдельному сообщению 97

Просмотр цифровой подписи сообщения 100

Добавление подписи ко всем сообщениям

Microsoft Outlook позволяет добавлять в сообщения электронной почты цифровую подпись, чтобы гарантировать подлинность и целостность сообщения, а также неотрекаемость. Для обеспечения конфиденциальности сообщения можно также шифровать.

Примечание. Более подробные сведения о защите электронной почты средствами криптографии можно получить на веб-узле Office Online http://office.microsoft.com/ru-ru/outlook/HP010461711049.aspx.

Ниже описано, как настроить добавление цифровой подписи к исходящим сообщениям в Microsoft Outlook 2003 и Microsoft Outlook 2007.

Внимание! Чтобы подписывать сообщения электронной почты, нужно иметь сертификат цифровой подписи, в котором указан адрес электронной почты субъекта и присутствует атрибут «Защищенная электронная почта» в расширенном использовании ключа. Если такого сертификата нет, добавление цифровой подписи к сообщению будет невозможно. За нужным сертификатом обратитесь к администратору Удостоверяющего и Ключевого центра (см. Руководство администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр]).

Чтобы цифровая подпись добавлялась ко всем сообщениям:

1. Откройте окно управления безопасностью электронной почты. Для этого выполните следующие действия.

   Если вы используете Microsoft Outlook 2003:

   - В меню **Сервис** выберите пункт **Параметры**.

- В окне **Параметры** откройте вкладку **Безопасность**.

Если вы используете Microsoft Outlook 2007:

- В меню **Сервис** выберите пункт **Центр управления безопасностью**.
- В окне **Центр управления безопасностью** откройте вкладку **Защита электронной почты**.

2 В группе **Шифрованная электронная почта** установите флажок **Добавлять цифровую подпись к исходящим сообщениям**.

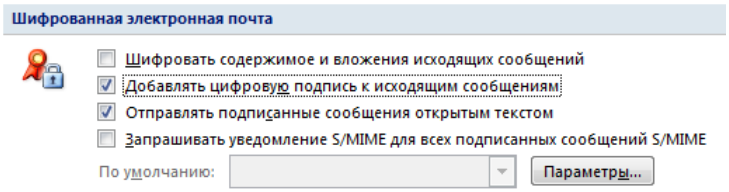

Рисунок 45: Группа Шифрованная электронная почта в окне управления безопасностью

3 Убедитесь, что установлен флажок **Отправлять подписанные сообщения открытым текстом** (иначе получатели, не использующие протокол S/MIME, не смогут прочесть сообщение).

4 Если вы хотите, чтобы исходящие сообщения были зашифрованы, установите флажок **Шифровать содержимое и вложения исходящих сообщений**.

5 Нажмите кнопку **Параметры**. Откроется окно **Изменение настройки безопасности**.

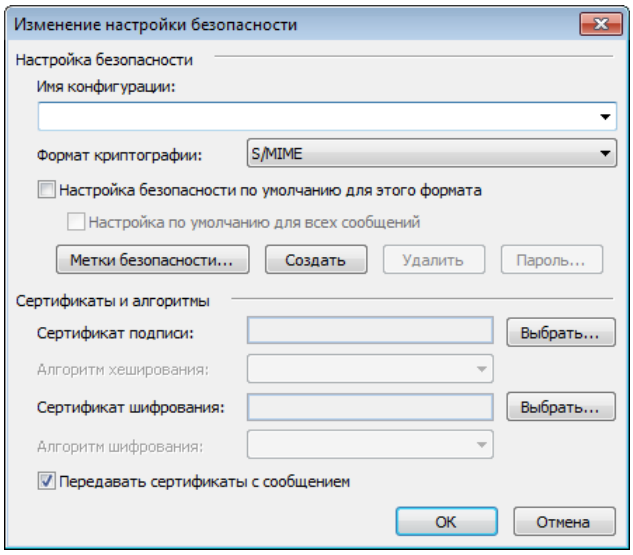

Рисунок 46: Окно Изменение настройки безопасности

6 Заполните поле **Имя конфигурации**.

7 Нажмите кнопку **Выбрать** напротив поля **Сертификат подписи**.

8 В окне **Выбор сертификата** выберите сертификат из списка. Чтобы просмотреть выбранный сертификат, нажмите кнопку **Просмотр сертификата**.

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

9 При необходимости выберите алгоритмы хеширования и шифрования из раскрывающихся списков. Вы также можете задать другой сертификат шифрования, нажав кнопку **Выбрать** напротив соответствующего поля.

10 Дважды нажмите **ОК**, чтобы сохранить настройки.

Добавление подписи к отдельному сообщению

Чтобы добавить цифровую подпись к отдельному сообщению, выполните следующие действия.

Внимание! Чтобы подписывать сообщения электронной почты, нужно иметь сертификат цифровой подписи, в котором указан адрес электронной почты субъекта и присутствует атрибут «Защищенная электронная почта» в расширенном использовании ключа. Если такого сертификата нет, добавление цифровой подписи к сообщению будет невозможно. За нужным сертификатом обратитесь к администратору Удостоверяющего и Ключевого центра (см. Руководство администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр]).

Добавление цифровой подписи

1. Создайте новое сообщение.
2. Чтобы добавить к нему цифровую подпись, нажмите кнопку **Сообщение с цифровой подписью** на панели инструментов.

Примечание. В Microsoft Outlook 2007 кнопка **Сообщение с цифровой подписью** находится в группе **Параметры** на вкладке **Сообщение**.

Кнопка **Сообщение с цифровой подписью** может отсутствовать на панели инструментов, если предварительно в окне **Изменение настроек безопасности** не был выбран сертификат цифровой подписи, используемый по умолчанию (см. "Добавление подписи ко всем сообщениям" на стр. 94).

3 Если на панели инструментов нет кнопки **Сообщение с цифровой подписью**  , обратитесь к разделу Если отсутствует кнопка Сообщение с цифровой подписью (на стр. 98).

4 Введите текст сообщения, укажите тему и адресата и нажмите кнопку **Отправить**. Откроется окно **ViPNet CSP – пароль контейнера ключа** (см. Рисунок 25 на стр. 60).

5 Введите пароль и нажмите кнопку **ОК**.

Если отсутствует кнопка Сообщение с цифровой подписью

1 Нажмите кнопку **Параметры** (в Microsoft Outlook 2003) или кнопку вызова диалогового окна группы **Параметры** на вкладке **Сообщение** (в Microsoft Outlook 2007). Откроется окно **Параметры сообщения**.

2 Нажмите кнопку **Параметры безопасности**. Откроется окно **Свойства безопасности**.

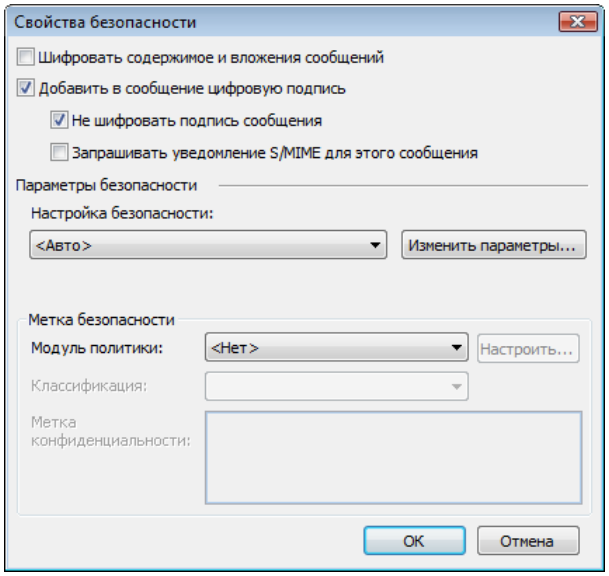

Рисунок 47: Окно Свойства безопасности

3 Установите флажок **Добавить в сообщение цифровую подпись**.

Примечание. По умолчанию в раскрывающемся списке **Настройка безопасности** установлено значение **<Авто>**. Это значит, что сертификат цифровой подписи будет выбран автоматически. Чтобы выбрать сертификат самостоятельно, нажмите кнопку **Изменить параметры**.

4 Чтобы сохранить настройки, нажмите **ОК**.

Просмотр цифровой подписи сообщения

Для проверки цифровой подписи сообщения выполните следующие действия:

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

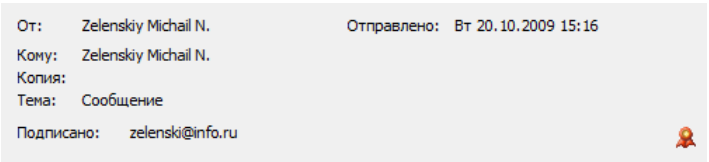

Рисунок 48: Проверка цифровой подписи в сообщении

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

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

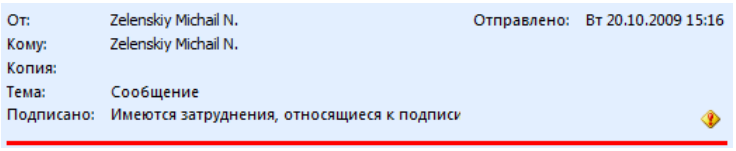

Рисунок 49: Сообщение с недействительной цифровой подписью

3 Чтобы получить более подробную информацию о цифровой подписи, нажмите кнопку **Цифровая подпись**  . Откроется окно **Цифровая подпись: правильная**. Если цифровая подпись, содержащаяся в сообщении, недействительна, откроется окно **Цифровая подпись: неправильная**.

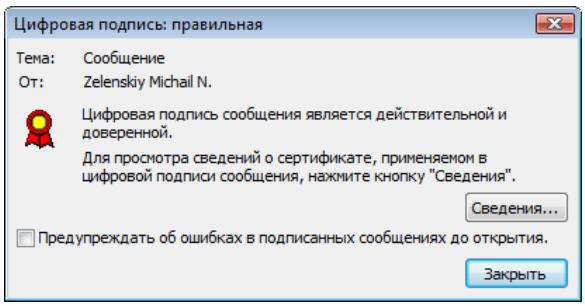

Рисунок 50: Сведения о действительной цифровой подписи

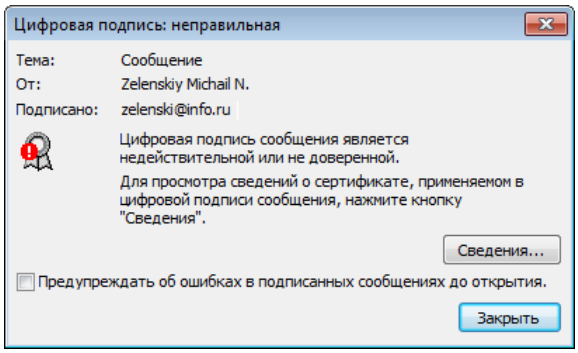

Рисунок 51: Сведения о недействительной цифровой подписи

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

10

Цифровая подпись в Microsoft Office InfoPath

Разрешение подписывать форму InfoPath цифровой подписью	103
Подписание формы InfoPath	106
Просмотр подписи в форме InfoPath	109
Удаление подписи из формы InfoPath	110

Разрешение подписывать форму InfoPath цифровой подписью

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

Microsoft Office InfoPath 2003

Чтобы разрешить пользователям подписывать форму Microsoft Office InfoPath 2003, выполните следующие действия:

1. Создайте или откройте шаблон формы в режиме конструктора.
2. В меню **Сервис** выберите пункт **Параметры формы**.
3. В окне **Параметры формы** на вкладке **Безопасность** установите флажок **Разрешить пользователям подписывать эту форму цифровой подписью**.
4. При необходимости установите флажок **При отправке этой формы без цифровой подписи запрашивать подпись**.
5. Чтобы сохранить настройки, нажмите **ОК**.

Microsoft Office InfoPath 2007

Чтобы разрешить пользователям подписывать форму Microsoft Office InfoPath 2007, выполните следующие действия:

1. Создайте или откройте шаблон формы в режиме конструктора.
2. В меню **Сервис** выберите пункт **Параметры формы**.

3 В окне **Параметры формы** откройте вкладку **Цифровые подписи**.

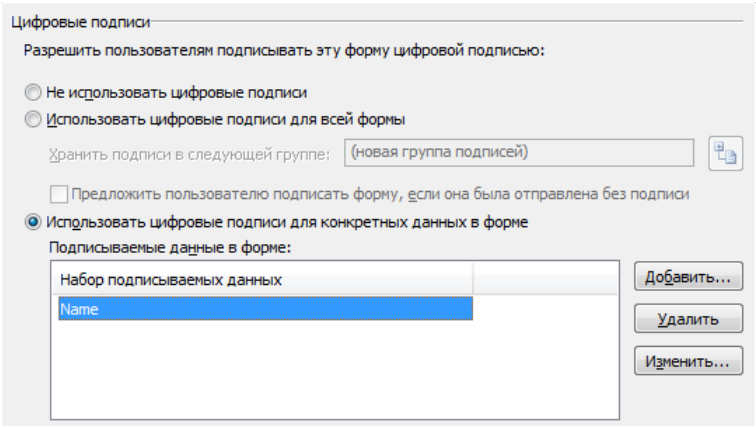

Рисунок 52: Вкладка Цифровые подписи

4 Если вы хотите, чтобы пользователь мог подписать всю форму, выберите **Использовать цифровые подписи для всей формы**.

Если вы используете цифровые подписи для всей формы, вы можете установить флажок **Предложить пользователю подписать форму, если она была отправлена без подписи**.

5 Если вы хотите, чтобы пользователь мог подписывать отдельные элементы формы, выберите **Использовать цифровые подписи для конкретных данных в форме**.

- Чтобы указать подписываемые данные, нажмите кнопку **Добавить**. Откроется окно **Набор подписываемых данных**.

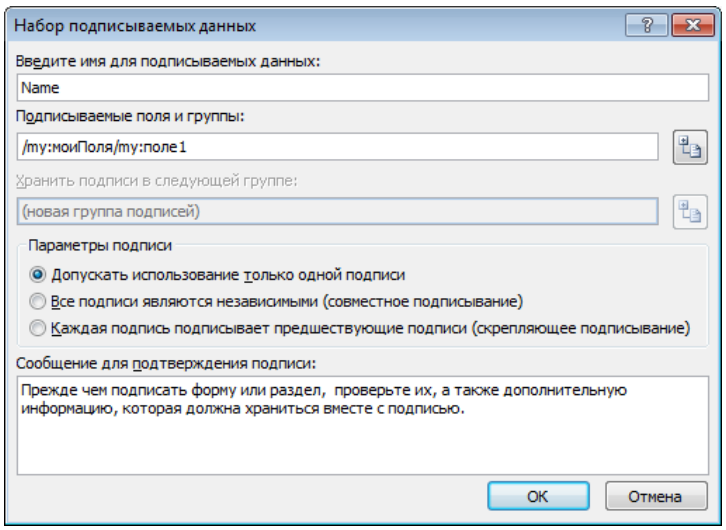

Рисунок 53: Окно Набор подписываемых данных

- Введите имя для подписываемых данных в соответствующее поле.
- Нажмите кнопку **Выбрать XPath** рядом с полем **Подписываемые поля и группы**.
- В окне **Выбор поля или группы** выберите подписываемое поле и нажмите **OK**.
- 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.
- Выполнив необходимые настройки, нажмите **OK**. Выбранное поле появится в списке **Набор подписываемых данных** (см. Рисунок 52 на стр. 104).
- Если требуется разрешить подписывать несколько полей формы, повторите описанные в шаге 5 действия необходимое число раз.

6 Чтобы сохранить настройки, нажмите **OK**.

Подписание формы InfoPath

Если при создании формы была предусмотрена возможность ее подписания, пользователь сможет добавить к форме свою цифровую подпись. Ниже описано, как это сделать.

Microsoft Office InfoPath 2003

1. Откройте форму или шаблон формы.
2. В меню **Сервис** выберите пункт **Цифровые подписи** (или нажмите кнопку **Цифровые подписи** на панели инструментов). Откроется окно **Цифровые подписи.**

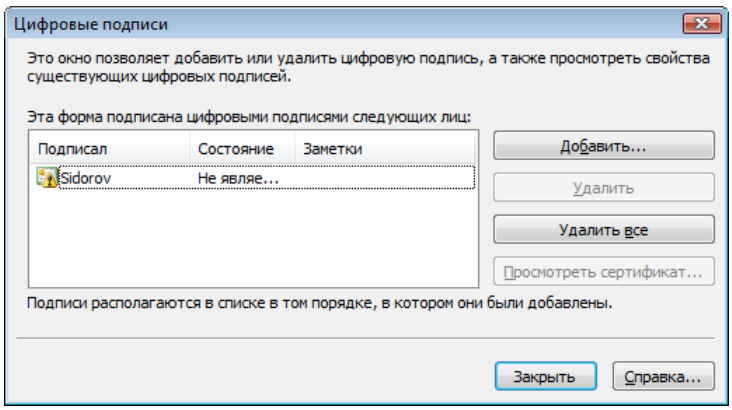

Рисунок 54: Окно Цифровые подписи

3. Нажмите кнопку **Добавить**, в открывшемся окне **Добавление подписи** нажмите кнопку **Выбор сертификата**.
4. Из списка выберите сертификат. Вы можете открыть его, нажав кнопку **Просмотр сертификата**. Выбрав сертификат, нажмите **ОК**.
5. В окне **Добавление подписи** при необходимости введите заметки, которые будут добавлены в подпись. Нажмите **ОК**.
6. В открывшемся окне **ViPNet CSP – пароль контейнера ключа** (см. Рисунок 25 на стр. 60) введите пароль и нажмите **ОК**.

После подписания внесение изменений в форму невозможно.

Microsoft Office InfoPath 2007

1. Откройте форму или шаблон формы.
2. В меню **Сервис** выберите пункт **Цифровые подписи** (или нажмите кнопку **Цифровые подписи** на панели инструментов). Откроется окно **Цифровые подписи**.

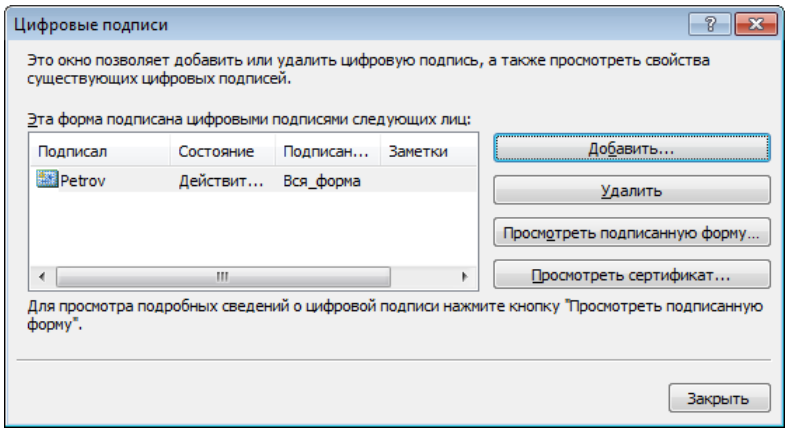

Рисунок 55: Окно Цифровые подписи

3. Нажмите кнопку **Добавить**. Откроется окно **Выбор данных для подписания.**
4. Если цифровая подпись применяется для всей формы, выберите единственный пункт списка – **Вся_форма**. Если подпись применяется для отдельных данных, выберите из списка подписываемые данные.
5. Нажмите **ОК**, откроется диалоговое окно **Подписание** (см. Рисунок 43 на стр. 89).
6. Если вы подписываете отдельные данные, введите свое имя в поле рядом с крестиком или щелкните ссылку **Выбрать рисунок**, чтобы вставить графическое изображение подписи.
7. При необходимости заполните поле **Цель подписания документа.**
8. В нижней части окна **Подписание** приведены краткие сведения о сертификате, с помощью которого предполагается подписать данные. Если вы хотите подписаться другим сертификатом, нажмите кнопку **Изменить** и выберите сертификат.
9. Нажмите кнопку **Подписать**, откроется окно **ViPNet CSP – пароль контейнера ключа** (см. Рисунок 25 на стр. 60).
10. Введите пароль и нажмите **ОК**.

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

Просмотр подписи в форме InfoPath

Чтобы просмотреть подпись в форме Microsoft Office InfoPath, выполните следующие действия:

1. В меню **Сервис** выберите пункт **Цифровые подписи** (или нажмите кнопку **Цифровые подписи**  на панели инструментов). Откроется диалоговое окно **Цифровые подписи.**
2. Если вы используете Microsoft Office InfoPath 2003, выберите сертификат подписи из списка и нажмите кнопку **Просмотреть сертификат.**

   Если сертификат ненадежен, то на вкладке **Общее** в окне **Сертификат** (см. Рисунок 38 на стр. 84) будет выведено сообщение о возникшей проблеме. Ненадежный сертификат помечен красным крестом.
3. Если вы используете Microsoft Office InfoPath 2007, выберите цифровую подпись из списка и нажмите кнопку **Просмотреть подписанную форму**. Откроется окно **Состав подписи** (см. Рисунок 40 на стр. 85).
   - 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.
   - Чтобы открыть сертификат, нажмите кнопку **Просмотр**. Чтобы просмотреть дополнительные сведения о подписи, нажмите ссылку **Дополнительные сведения, которые будут включены в подпись...**

Удаление подписи из формы InfoPath

Чтобы удалить подпись из формы Microsoft Office InfoPath, выполните следующие действия:

1. В меню **Сервис** выберите пункт **Цифровые подписи** (или нажмите кнопку **Цифровые подписи**  на панели инструментов). Откроется окно **Цифровые подписи.**
2. Выберите цифровую подпись из списка. Чтобы просмотреть подпись перед удалением:
   - В Microsoft Office InfoPath 2003 нажмите кнопку **Просмотреть сертификат.** Откроется окно **Сертификат.**
   - В Microsoft Office InfoPath 2007 нажмите кнопку **Просмотреть подписанную форму**. Откроется окно **Состав подписи**. Чтобы открыть сертификат, нажмите кнопку **Просмотр.**
3. Выбрав цифровую подпись, нажмите кнопку **Удалить.**

Примечание. В Microsoft Office InfoPath 2003 вы можете удалить сразу все цифровые подписи, нажав кнопку **Удалить все.**

4. В окне подтверждения нажмите **Да**. Цифровая подпись будет удалена из формы.

11

Цифровая подпись макросов

Подписание макросов 112

Проверка подписи макроса 114

Удаление подписи макроса 115

Подписание макросов

Создав макрос в приложениях Microsoft Office, вы можете заверить его цифровой подписью. Цифровая подпись позволяет подтвердить происхождение макроса и его безопасность. Создать и подписать макрос позволяют приложения Microsoft Word, Excel, Outlook, PowerPoint, Access, Publisher и Visio.

Внимание! Чтобы подписать макрос, нужно иметь сертификат с атрибутом «Подписывание кода» в расширенном использовании ключа. Если такого сертификата нет, вы не сможете добавить цифровую подпись к макросу. Для получения нужного сертификата обратитесь к администратору Удостоверяющего и Ключевого Центра (см. Руководство администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр]).

Чтобы подписать макрос, выполните следующие действия.

1. Откройте редактор Microsoft Visual Basic.
   - Если вы используете любое из перечисленных приложений версии Microsoft Office 2003 или Microsoft Outlook 2007, Publisher 2007, Visio 2007: в меню **Сервис** выберите пункт **Макрос**, затем щелкните команду **Редактор Visual Basic**.
   - Если вы используете Microsoft Word 2007, Excel 2007 или PowerPoint 2007: на вкладке **Разработчик** в группе **Код** нажмите кнопку **Visual Basic**.
   - Если вы используете Microsoft Access 2007: на вкладке **Работа с базами данных** в группе **Макрос** нажмите кнопку **Visual Basic**.

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

2 В окне редактора Microsoft Visual Basic в меню **Сервис** выберите пункт **Цифровая подпись**. Откроется окно **Цифровая подпись**.

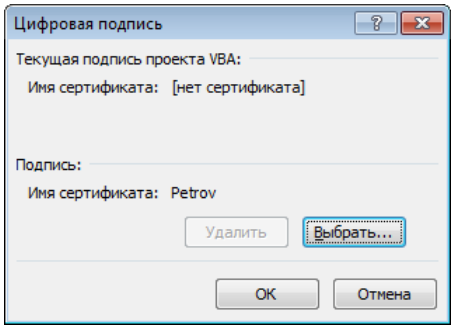

Рисунок 56: Добавление цифровой подписи

3 Нажмите кнопку **Выбрать**, из открывшегося списка выберите сертификат цифровой подписи и нажмите **ОК**. Цифровая подпись будет добавлена к макросу.

Проверка подписи макроса

Чтобы проверить цифровую подпись в проекте макроса, выполните следующие действия:

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

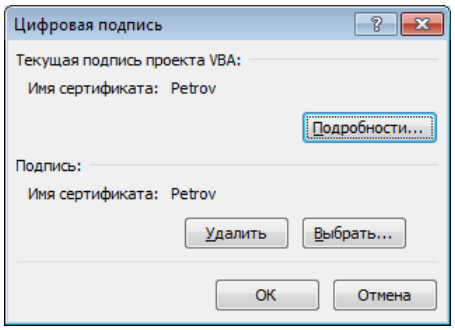

Рисунок 57: Окно Цифровая подпись

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

Если сертификат ненадежен, то на вкладке **Общее** в окне **Сертификат** (см. Рисунок 38 на стр. 84) будет выведено сообщение о возникшей проблеме. Ненадежный сертификат помечен красным крестом.

Удаление подписи макроса

Чтобы удалить цифровую подпись из проекта макроса, выполните следующие действия:

1. В окне редактора Microsoft Visual Basic в меню **Сервис** выберите пункт **Цифровая подпись**. Откроется окно **Цифровая подпись** (см. Рисунок 57 на стр. 114).
2. Чтобы удалить цифровую подпись, нажмите кнопку **Удалить**, цифровая подпись будет удалена из проекта.

12

Организация защищенного соединения TLS/SSL

Этапы организации доступа к защищенному веб-серверу 117

Настройка серверного узла соединения 118

Настройка клиентского узла соединения 119

Настройка браузера Internet Explorer для работы по протоколу TLS/SSL 120

Проверка доступности веб-узла по защищенному протоколу HTTPS 121

Этапы организации доступа к защищенному веб-серверу

Чтобы с помощью криптопровайдера ViPNet CSP организовать доступ к защищенному веб-серверу, нужно выполнить настройку серверного узла соединения и узла веб-клиента.

1. Для настройки серверного узла соединения (см. "Настройка серверного узла соединения" на стр. 118):
   - Настроить сервер IIS (см. «Практическое руководство. Создание удаленных веб-узлов IIS» в библиотеке MSDN http://msdn.microsoft.com/ru-ru/library/default.aspx).
   - Установить криптопровайдер ViPNet CSP.
   - Установить в хранилище сертификатов локального компьютера сертификат пользователя (сервера), сертификат издателя и СОС.
2. Для настройки клиентского узла соединения (см. "Настройка клиентского узла соединения" на стр. 119):
   - Установить криптопровайдер ViPNet CSP.
   - Установить в хранилище сертификатов пользователя сертификат пользователя (клиента), сертификат издателя и СОС
   - При необходимости настроить браузер Internet Explorer для работы по протоколу TLS/SSL.

Настройка серверного узла соединения

Для настройки серверной части выполните следующие действия:

1. Запросите у администратора сети контейнер секретного ключа и сертификата для сервера IIS, корневой сертификат и СОС.

   

   Внимание! Сертификат пользователя для сервера должен иметь атрибут «Проверка подлинности сервера» в расширенном использовании ключа.

2. Установите ПО ViPNet CSP (см. "Установка программы" на стр. 23).
3. Выполните установку полученного контейнера секретного ключа (см. "Установка контейнеров и сертификатов" на стр. 46).
4. Установите в хранилище сертификатов локального компьютера находящийся в контейнере сертификат сервера (см. "Установка сертификата пользователя" на стр. 65), а также корневой сертификат и СОС (см. "Ручная установка сертификатов и СОС" на стр. 56).
5. Проверьте доступность веб-узла по защищенному протоколу HTTPS.

Настройка клиентского узла соединения

Для настройки клиентской части выполните следующие действия:

1. Запросите у администратора сети контейнер секретного ключа и сертификата для веб-клиента, корневой сертификат и СОС.

   

   Внимание! Сертификат пользователя для веб-клиента должен иметь атрибут «Проверка подлинности клиента» в расширенном использовании ключа.

2. Установите ПО ViPNet CSP (см. "Установка программы" на стр. 23).
3. Выполните установку полученного контейнера секретного ключа и сертификат веб-клиента (см. "Установка контейнеров и сертификатов" на стр. 46).
4. Установите в хранилище сертификатов текущего пользователя корневой сертификат и СОС (см. "Ручная установка сертификатов и СОС" на стр. 56).
5. Если необходимо, выполните настройку обозревателя Internet Explorer для работы по защищенному протоколу (см. "Настройка браузера Internet Explorer для работы по протоколу TLS/SSL" на стр. 120).
6. Проверьте доступность веб-узла по защищенному протоколу HTTPS.

Настройка браузера Internet Explorer для работы по протоколу TLS/SSL

Как правило, настройки браузера по умолчанию позволяют работать с TLS/SSL соединениями. Если настройки браузера отличны от первоначальных или соединение с сервером не происходит, выполните следующие действия:

1. В меню **Сервис** обозревателя Internet Explorer выберите пункт **Свойства обозревателя**.
2. В **Свойства обозревателя** откройте вкладку **Дополнительно**.
3. Установите флажки **SSL 2.0**, **SSL 3.0**, **TLS 1.0**.
4. Проверьте доступность веб-узла по защищенному протоколу HTTPS.

Проверка доступности веб-узла по защищенному протоколу HTTPS

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

Если соединения с веб-сервером установить не удалось – обратитесь к разделу Проблемы и неисправности (на стр. 122).

13

Проблемы и неисправности

Не удается запустить программу 123

Конфликт ViPNet CSP с другими программами 125

Не удается поставить цифровую подпись 126

Нет соединения с сервером по протоколу HTTPS 128

При соединении с сервером выводится предупреждение системы безопасности 133

Не удается запустить программу

Если при попытке запустить ViPNet CSP появляется сообщение о нарушении целостности программы или об отсутствии компонентов, дальнейшая работа программы будет невозможна.

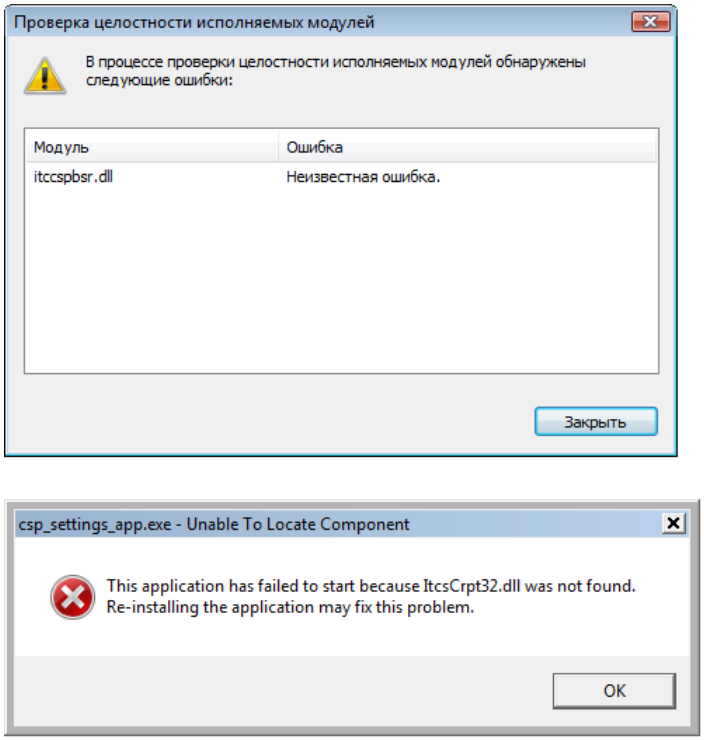

Рисунок 58: Сообщения об ошибках при запуске ViPNet CSP

Чтобы восстановить работоспособность ViPNet CSP, снова установите программу «поверх» уже установленной копии ViPNet CSP (не удаляя ее):

1 Запустите установочный файл Setup.exe  .

2 В окне **Установка ViPNet CSP** с помощью переключателя выберите **Обновить**, затем нажмите кнопку **Продолжить**. Начнется обновление компонентов программы.

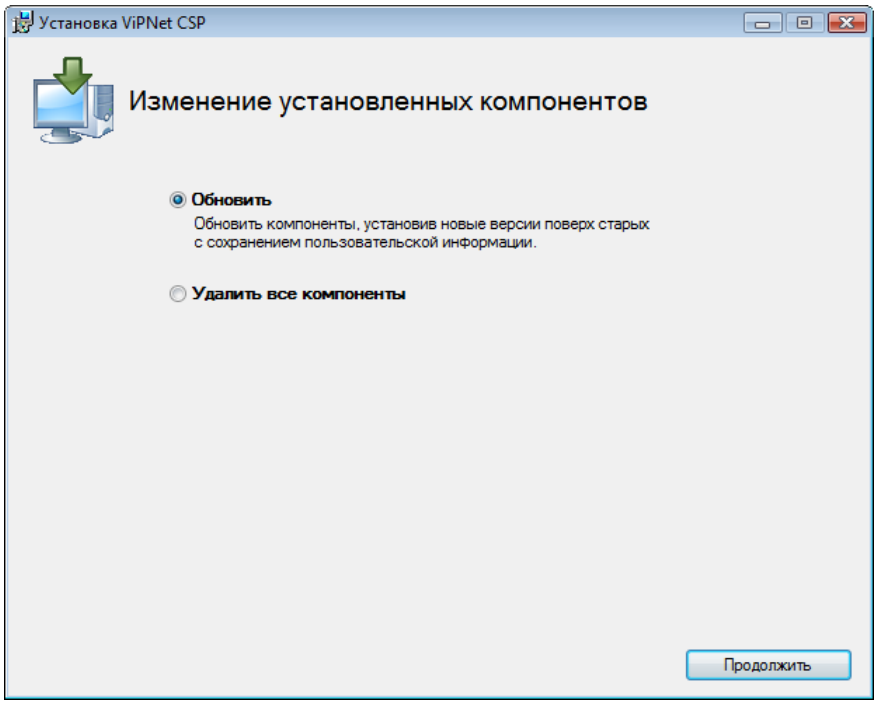

Рисунок 59: Окно Переустановить/Удалить

3 По завершении обновления программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите **Да.**

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

Конфликт ViPNet CSP с другими программами

Если ViPNet CSP конфликтует с другими программами (например, с криптопровайдерами других разработчиков), можно отключить поддержку работы ViPNet CSP через интерфейс MS Crypto API.

Внимание! После отключения поддержки интерфейса MS Crypto API невозможно будет использовать криптографические функции ViPNet CSP в Microsoft Office и других приложениях, использующих этот интерфейс. Однако сохранится возможность использовать ViPNet CSP в различных приложениях ViPNet.

Чтобы отключить поддержку интерфейса MS Crypto API, на вкладке **Общие** (см. Рисунок 3 на стр. 26) снимите флажок **Включить поддержку работы ViPNet CSP через MS Crypto API**. Изменения полностью вступят в силу после перезагрузки компьютера.

Не удается поставить цифровую подпись

Не найден секретный ключ, соответствующий сертификату

Если при выборе сертификата для подписания открывается окно **ViPNet CSP - инициализация контейнера ключа**, это значит, что не найден секретный ключ, соответствующий выбранному сертификату. Это может произойти в том случае, если контейнер секретного ключа был отключен в программе ViPNet CSP (см. "Отключение контейнера" на стр. 62).

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

Если в окне **ViPNet CSP - инициализация контейнера** вы укажете путь к контейнеру секретного ключа, этот контейнер будет добавлен в список на вкладке **Контейнеры**.

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 и Ключевой Центр. В сертификате должен быть указан ваш адрес электронной почты и присутствовать атрибут «Защищенная электронная почта» в расширенном использовании ключа.

Не удается подписать макрос или базу данных Microsoft Access 2007

Если при попытке подписать макрос или создать подписанный пакет Microsoft Access 2007 в окне выбора сертификата цифровой подписи нет доступных сертификатов, это

значит, что вы не можете подписывать код. Обратитесь в Удостоверяющий и Ключевой Центр за сертификатом, который имеет атрибут «Подписывание кода» в расширенном использовании ключа.

Не удается подписать видимую строку подписи в Microsoft Word 2003 или Excel 2003

Приложения Microsoft Word и Excel более ранних версий, чем Microsoft Office 2007, не позволяют подписывать видимые строки подписи. Чтобы подписать строку подписи, откройте документ с помощью приложения Microsoft Office 2007.

Невозможно редактировать подписанный документ Microsoft Word или Excel

Чтобы внести изменения в подписанный документ Microsoft Word или Excel, удалите цифровую подпись (см. "Удаление цифровой подписи" на стр. 86) и внесите необходимые изменения. После этого вы можете снова подписать документ.

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

Нет соединения с сервером по протоколу HTTPS

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

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

Не установлены сертификаты пользователя, издателя, СОС в нужное хранилище

Проверьте корректность установки сертификатов в хранилище с помощью стандартной консоли MMC.

Чтобы просмотреть сертификаты, установленные в хранилище:

1. Откройте консоль MMC:
   - В меню **Пуск** выберите пункт **Выполнить**.
   - В поле **Открыть** введите "mmc" и нажмите **OK**.
2. В меню **Консоль** окна консоли выберите пункт **Добавить или удалить оснастку…**
3. В окне **Добавить или удалить оснастку** нажмите кнопку **Добавить…**
4. В окне **Добавить изолированную оснастку** выберите **Сертификаты** и нажмите кнопку **Добавить**.
5. 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 СОС должны быть установлены в нужное хранилище и при их открытии не должно возникать ошибок.

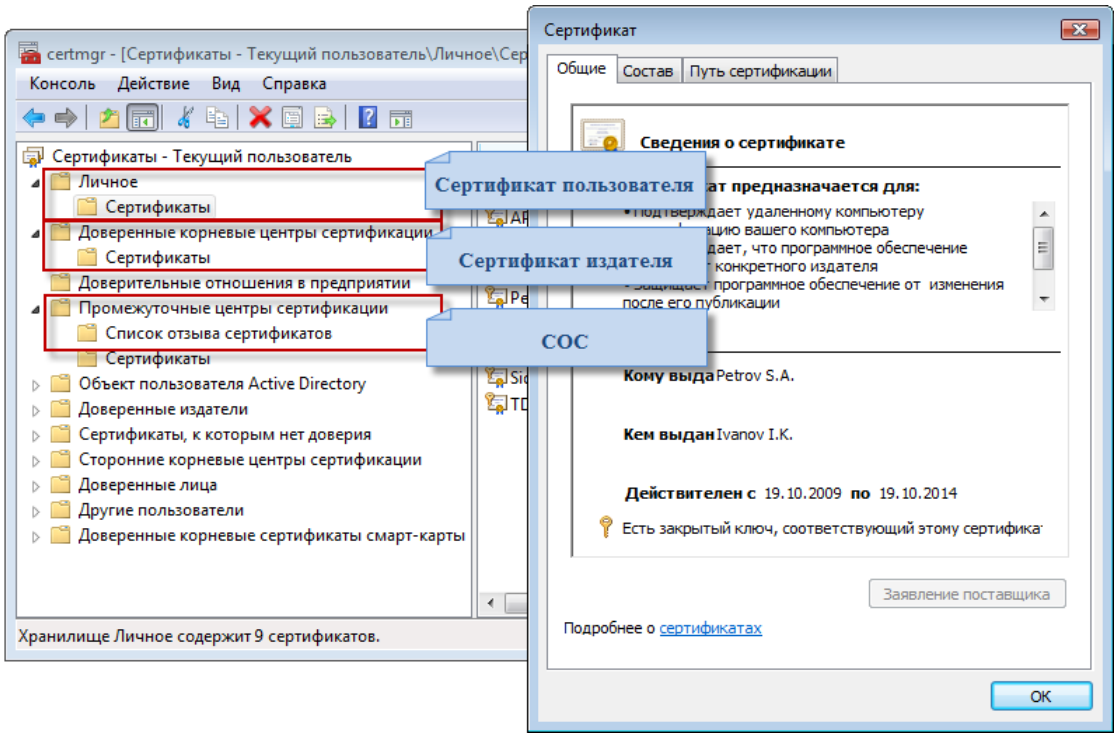

Рисунок 60: Сертификат веб-клиента в хранилище сертификатов текущего пользователя

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

- Раздел **Личные > Сертификаты** – сертификат пользователя (сервера).
- Раздел **Доверенные корневые центры сертификации > Сертификаты – сертификат издателя** (корневой сертификат).
- Раздел **Промежуточные центры сертификации > Список отзыва сертификатов** – СОС.

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

- Раздел **Личные > Сертификаты** – сертификат пользователя (веб-клиента).
- Раздел **Доверенные корневые центры сертификации > Сертификаты** – сертификат издателя (корневой сертификат).
- Раздел **Промежуточные центры сертификации > Список отзыва сертификатов** – СОС.

Если сертификат не установлен или установлен некорректно, выполните установку сертификата в хранилище (см. "Ручная установка сертификатов и СОС" на стр. 56).

Обозреватель не настроен на работу по протоколу TLS

По умолчанию настройки обозревателя Internet Explorer позволяют работать по защищенному протоколу TLS. Если соединения с сервером не происходит, проверьте наличие в обозревателе нужного сертификата и активность протоколов TLS/SSL.

Для проверки наличия сертификата:

1. В меню **Сервис** обозревателя Internet Explorer выберите пункт **Свойства обозревателя**.
2. В окне **Свойства обозревателя** откройте вкладку **Содержание** и нажмите кнопку **Сертификаты**.
3. В окне **Сертификаты** откройте вкладку **Личное** и проверьте, что в списке сертификатов присутствует нужный.
4. Выберите нужный сертификат и нажмите кнопку **Просмотр**.

5 В окне **Сертификат** убедитесь, что сертификат содержит атрибут **Проверка подлинности клиента** (см. Рисунок 61 на стр. 131). Если такой атрибут отсутствует, обратитесь в Удостоверяющий и ключевой центр за сертификатом, в котором будет указан данный параметр (см. Руководство администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр]).

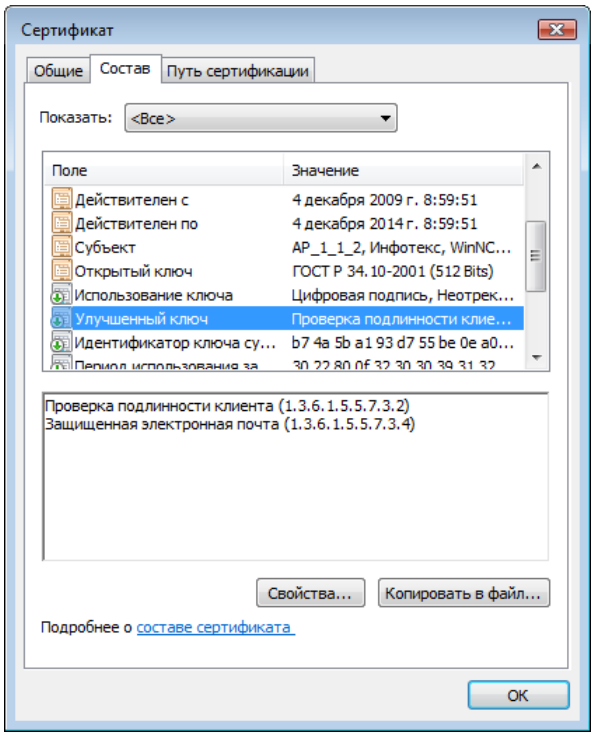

Рисунок 61: Состав сертификата веб-клиента

Для проверки активности протоколов TLS/SSL:

1 В меню **Сервис** обозревателя Internet Explorer выберите пункт **Свойства обозревателя**.

2 В диалоговом окне **Свойства обозревателя** откройте вкладку **Дополнительно**.

3 Убедитесь, что установлены флажки **SSL 2.0**, **SSL 3.0**, **TLS 1.0**.

4 Проверьте подключение к веб-серверу.

Требуется перезапуск службы сервера IIS

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

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

В некоторых случаях для доступа к серверу требуется сохранить пароль к контейнеру секретного ключа. Для этого:

1. В оснастке консоли MMC откройте нужный сертификат.
2. На вкладке **Состав** окна **Сертификат** нажмите кнопку **Копировать в файл…**
3. На странице приветствия **Мастера экспорта сертификатов** нажмите **Далее**.
4. В окне ввода пароля к контейнеру ключа введите пароль пользователя сетевого узла-сервера, установите флажки **Сохранить пароль** и **Не показывать больше это окно**.
5. Нажмите **OK**. Теперь работу мастера можно завершить – пароль сохранен.

При соединении с сервером выводится предупреждение системы безопасности

Если при попытке соединения с сервером обозреватель выводит **Предупреждение системы безопасности**: «Указанное в сертификате название неправильно или не совпадает с названием узла», проверьте, что название домена сервера и имя пользователя, на которое выдан сертификат сервера, совпадают.

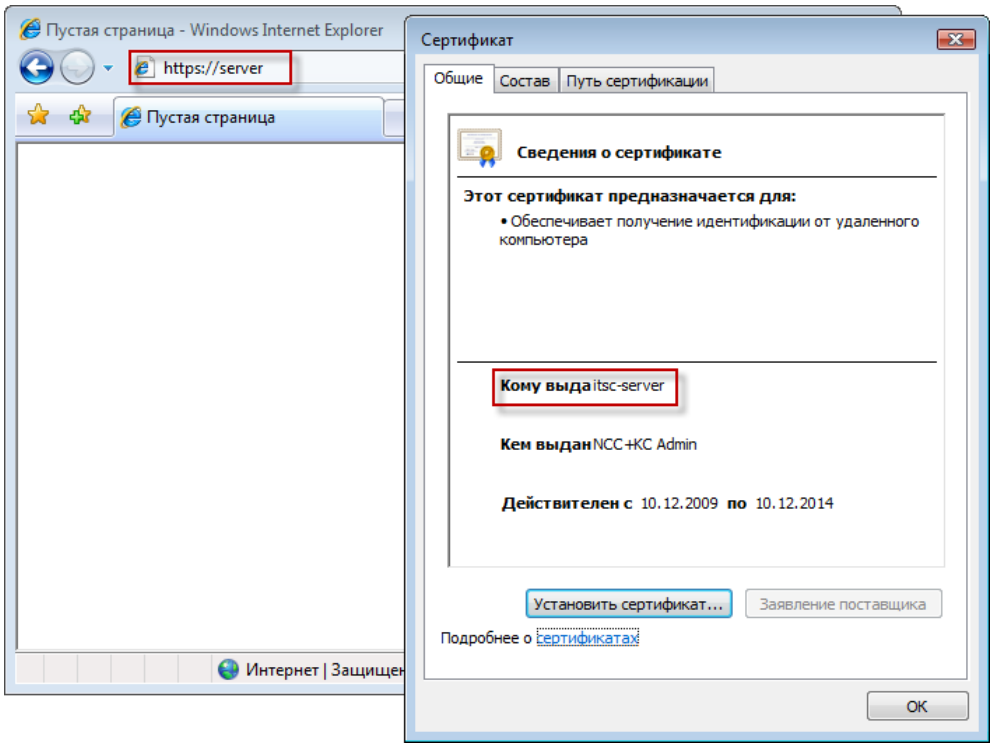

Рисунок 62: Предупреждение системы безопасности о несовпадении имен

Глоссарий

К

Контейнер

Файл, содержащий секретный ключ пользователя и сертификат. Доступ к файлу контейнера защищен паролем.

Контейнер секретного ключа

Файл, содержащий секретный ключ пользователя, которым происходит шифрование и расшифровка документов. Файл контейнера защищен паролем.

С

Сертификат (Сертификат пользователя)

Содержит открытый ключ цифровой подписи пользователя и дополнительные параметры сферы действия сертификата. Данный сертификат создается при создании ключевого дистрибутива пользователя в программе ViPNet Administrator УКЦ (см. Руководство администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр]) или любым Удостоверяющим центром.

Сертификат издателя

Сертификат издателя (корневой сертификат) – сертификат, содержащий цифровую подпись администратора УКЦ, которой заверяются сертификаты пользователей. При

соединении двух защищенных узлов аутентификация пройдет успешно, если на обоих узлах установлены одинаковые корневые сертификаты.

Список отозванных сертификатов

Списки отозванных сертификатов (СОС) – списки сертификатов, недействительных на данный момент.

Указатель

Г
Групповая регистрация • 28, 32, 45

Д
Добавление подписи ко всем сообщениям • 97

Е
Если конфигурация вашего компьютера изменилась • 28
Если отсутствует кнопка Сообщение с цифровой подписью • 98

И
Информация о внешних устройствах хранения данных • 10

К
Контейнер секретного ключа и сертификата • 18

Н
Назначение криптопровайдера • 9
Настройка браузера Internet Explorer для работы по протоколу TLS/SSL • 119
Настройка клиентского узла соединения • 117
Настройка серверного узла соединения • 117
Начало регистрации • 31, 41

О
Ограничения бесплатной версии • 25
Организация защищенного соединения TLS/SSL • 49, 51, 55, 58
Отключение контейнера • 126

П
Покупка программы (получение серийного номера) • 29, 33, 45
Получение кода регистрации • 29, 31, 43
Получение кода регистрации по телефону • 32
Получение кода регистрации по электронной почте • 32
Получение кода регистрации через веб-страницу • 32
Получение кода регистрации через Интернет • 32, 35, 39
Порядок действий системного администратора при групповой регистрации • 28
Проблемы и неисправности • 121
Просмотр и настройка свойств контейнера • 70
Просмотр цифровой подписи • 90

Р
Регистрация ViPNet CSP • 30, 36, 37, 40
Ручная установка сертификатов и СОС • 20, 66, 118, 119, 130

С
Сертификат (Сертификат пользователя) • 20
Сертификат издателя • 20
Сохранение регистрационных данных • 28, 35, 38, 43
Список отозванных сертификатов • 20

У
Удаление цифровой подписи • 90, 127
Установка контейнера из папки • 20, 52, 54, 60
Установка контейнера с внешнего устройства • 20, 54, 60
Установка контейнеров и сертификатов • 20, 26, 118, 119
Установка программы • 118, 119
Установка сертификата и контейнера секретного ключа • 20, 47
Установка сертификата пользователя • 48, 49, 51, 118

Ц
Цифровая подпись в Microsoft Office InfoPath • 49, 51, 55, 58
Цифровая подпись в Microsoft Outlook • 49, 51, 54, 57
Цифровая подпись в документах MS Office • 49, 51, 54, 57
Цифровая подпись макросов • 49, 51, 55, 58, 91

Э
Электронная цифровая подпись • 9