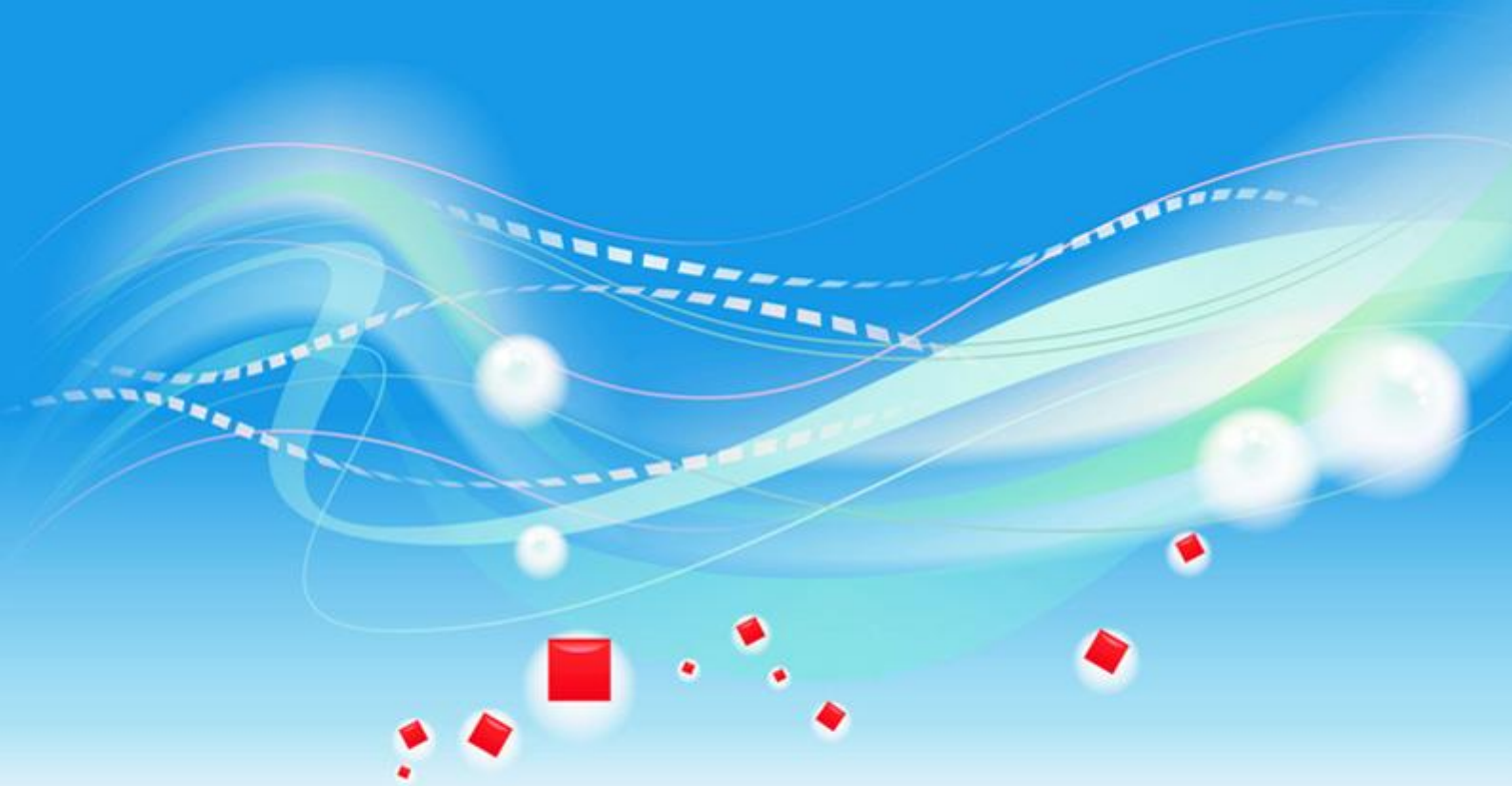


ViPNet Деловая почта 4.2

Руководство пользователя

ViPNet
Virtual Private Network
infotecs

ФРКЕ.00116-03 34 03

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Для кого предназначен документ

Данный документ предназначен для пользователей программы ViPNet Деловая почта и администраторов сети ViPNet. В документе содержится описание работы с программой и указания по ее настройке.

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях

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

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

О программе

Программа ViPNet Деловая почта предназначена для обмена электронными письмами в защищенной сети ViPNet (см. «Сеть ViPNet» на стр. 210). Этой возможностью могут воспользоваться только те пользователи сети ViPNet, у которых есть связь друг с другом.

Программа ViPNet Деловая почта входит в состав программного обеспечения ViPNet Client и может быть установлена на компьютер вместе с другими компонентами данного программного обеспечения или отдельно. Установка ПО ViPNet Client описана в документе «ViPNet Client Монитор. Руководство пользователя».

Программа ViPNet Деловая почта обладает стандартными функциями почтового клиента:

- Отправка и прием писем.
- Отправка и прием вложенных в письма файлов.
- Подписание писем и вложений электронной подписью.
- Шифрование файлов вложений.

Программа ViPNet Деловая почта также имеет ряд особенностей:

- Доступ к программе на сетевом узле ViPNet имеет только пользователь этого сетевого узла.
- Письма программы ViPNet Деловая почта передаются по защищенным каналам в сети ViPNet с помощью транспортного модуля MFTP (см. «Настройка транспортного модуля» на стр. 115).
- Письма программы ViPNet Деловая почта зашифрованы на ключах адресата (см. «Уровни адресации» на стр. 41) и не могут быть прочитаны кем-либо другим.
- Программа ViPNet Деловая почта имеет мощную систему автоматической обработки входящих писем и исходящих файлов (см. «Автопроцессинг» на стр. 87).

Системные требования

Требования к компьютеру для установки программы ViPNet Деловая почта:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 512 Мбайт.
- Свободное место на жестком диске — не менее 150 Мбайт (рекомендуется 250 Мбайт).
- Сетевой адаптер или модем.
- Операционная система — Windows XP (32-разрядная), Server 2003 (32-разрядная), Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Server 2008 R2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Server 2012 (64-разрядная).

  Для операционной системы должен быть установлен самый последний пакет обновлений.
- При использовании Internet Explorer — версия 6.0 или выше.

Обратная связь

Дополнительная информация

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

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

Контактная информация

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

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

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

Быстрый старт

Перед началом работы

Данная глава содержит краткие указания по использованию основных возможностей программы ViPNet Деловая почта. Эта информация поможет приступить к работе без подробного изучение данного руководства.

Чтобы начать работу с электронными письмами, запустите программу (см. «Запуск и завершение работы с программой» на стр. 23). Об основных действиях с письмами можно узнать далее в данной главе. В случае каких-либо затруднений обратитесь к разделу Работа с письмами (на стр. 43).

Использование криптографических возможностей программы описано в главе Электронная подпись и шифрование (на стр. 71), автоматическая обработка писем и файлов — в главе Автопроцессинг (на стр. 87).

Как написать письмо

Чтобы написать письмо, выполните следующие действия:

1. В окне программы ViPNet Деловая почта на панели инструментов нажмите кнопку **Письмо**  .
2. В окне **Исходящее** введите тему и текст письма.
3. Если в письмо требуется вложить файлы, на панели инструментов нажмите кнопку **Вложения**  и в окне **Открыть** выберите нужные файлы.
4. Если необходимо зашифровать письмо, нажмите кнопку **Шифровать**  .
5. Если необходимо подписать письмо электронной подписью, нажмите кнопку **Подписать**  .
6. Нажмите кнопку **Получатели**  и в окне **Адресная книга** выберите получателей.
7. Нажмите кнопку **Отправить**  .

Подробнее см. раздел Создание и отправка нового письма (на стр. 44).

Как подписать письмо электронной подписью

Чтобы подписать письмо электронной подписью, выполните следующие действия:

- Если письмо открыто в окне редактирования письма, нажмите кнопку **Подписать** на панели инструментов.
- Если письмо сохранено в папку **Исходящие** или ее подпапку и еще не отправлено:
  - Выберите письмо в списке.
  - Нажмите кнопку **Подписать** на панели инструментов окна программы ViPNet Деловая почта.

Подробнее см. раздел Подписание письма (на стр. 73).

Как прочитать письмо

При получении новых писем транспортный модуль MFTP выдает соответствующее сообщение. Непрочитанные письма выделяются в списке полужирным шрифтом. Папки программы ViPNet Деловая почта, в которых есть непрочитанные письма, также выделяются полужирным шрифтом, при этом в скобках после имени папки указано количество непрочитанных писем.

Чтобы прочитать письмо:

1. В окне программы ViPNet Деловая почта на левой панели выберите папку, в которой находится письмо.
2. Выберите письмо в списке. Если письмо не зашифровано, его текст отобразится в поле под списком писем.

   Если письмо зашифровано, для его просмотра выполните одно из действий:

   - Нажмите кнопку **Расшифровать**  на панели инструментов.
   - Откройте письмо в отдельном окне двойным щелчком.

Подробнее см. раздел Просмотр письма и вложений в отдельном окне (на стр. 55).

Как ответить на письмо

Чтобы ответить на письмо, выполните следующие действия:

1. Выберите письмо в списке или откройте в отдельном окне двойным щелчком.
2. В окне программы ViPNet Деловая почта или в окне просмотра письма на панели инструментов нажмите кнопку **Ответить**  или **Ответить всем**  .

   Откроется окно создания письма.
3. Напишите и отправьте письмо, как описано в разделе Как написать письмо (на стр. 15).

Подробнее см. раздел Ответ на письмо и пересылка письма (на стр. 57).

Как перенести письмо в Microsoft Outlook

Чтобы перенести письмо в Microsoft Outlook или Outlook Express (Windows Mail), выполните одно из действий:

- Перетащите письмо из окна программы ViPNet Деловая почта в окно нового сообщения Microsoft Outlook или Outlook Express. Письмо будет добавлено в сообщение в виде вложения.
- Перетащите письмо из окна программы ViPNet Деловая почта в какую-либо папку в окне программы Microsoft Outlook или Outlook Express. В выбранной папке появится сообщение, в которое будет вложено письмо программы ViPNet Деловая почта.

Подробнее см. раздел Экспорт и импорт писем (на стр. 62).

Как удалить письмо

Чтобы удалить письмо, выполните следующие действия:

1. В окне программы ViPNet Деловая почта на левой панели выберите папку с письмом, которое нужно удалить.
2. В списке выберите письмо и нажмите кнопку **Удалить** на панели инструментов или нажмите клавишу **Delete**.

   Письмо будут перемещено в папку **Удаленные**, в подпапку с именем, которое совпадает с именем исходной папки письма.

Подробнее см. Удаление писем (на стр. 65).

Начало работы с программой ViPNet Деловая почта

Установка программы

Программа ViPNet Деловая почта является одним из компонентов программного обеспечения ViPNet Client. В рамках ПО ViPNet CUSTOM программа ViPNet Деловая почта по умолчанию устанавливается на компьютер вместе с основным компонентом ViPNet Монитор. Однако в случае необходимости вы можете установить программу ViPNet Деловая почта, но не устанавливать программу ViPNet Монитор. В рамках ПО ViPNet VPN программа ViPNet Деловая почта устанавливается отдельно от программы ViPNet Монитор. Подробнее об установке ПО ViPNet Client см. документ «ViPNet Client Монитор. Руководство пользователя», главу «Установка, обновление и удаление ПО ViPNet Client».

Также для работы с программой ViPNet Деловая почта на компьютере должны быть установлены справочники и ключи ViPNet. Если вы установили справочники и ключи в программе ViPNet Монитор, они будут автоматически использоваться в программе ViPNet Деловая почта. Если программа ViPNet Монитор не установлена на компьютере, перед началом работы с программой ViPNet Деловая почта установите справочники и ключи ViPNet с помощью дистрибутива ключей (файл `*.dst`), который вы можете получить у администратора вашей сети ViPNet. Подробнее см. документ «ViPNet Client Монитор. Руководство пользователя», главу «Установка и обновление справочников и ключей».

Примечание. Программу ViPNet Деловая почта можно использовать только на сетевых узлах с ролью «Деловая почта». Если узлу эта роль не назначена, запустить программу будет невозможно.

Запуск и завершение работы с программой

Чтобы запустить программу ViPNet Деловая почта, выполните следующие действия:

1. Для запуска программы ViPNet Деловая почта используйте один из следующих способов:
   - Если запущена программа ViPNet Монитор, в окне программы в меню **Приложения** выберите пункт **Деловая почта**. Немедленно будет открыто окно программы ViPNet Деловая почта. Аутентификация пользователя в этом случае не требуется.
   - Если через транспортный модуль MFTP будут получены новые письма, появится соответствующее уведомление.

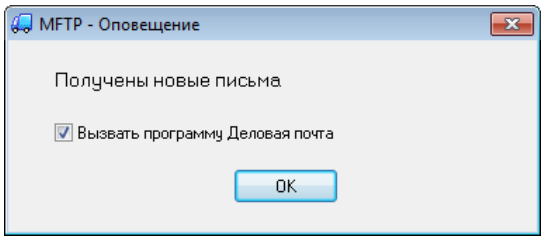


Рисунок 1: Уведомление о получении новых писем

Примечание. Уведомление появляется только в том случае, если сделаны соответствующие настройки транспортного модуля (см. документ «ViPNet MFTP. Руководство пользователя»).

Для запуска программы ViPNet Деловая почта убедитесь, что в окне уведомления установлен флажок **Вызвать программу Деловая почта**, и нажмите кнопку **OK**. Откроется окно входа в программу.

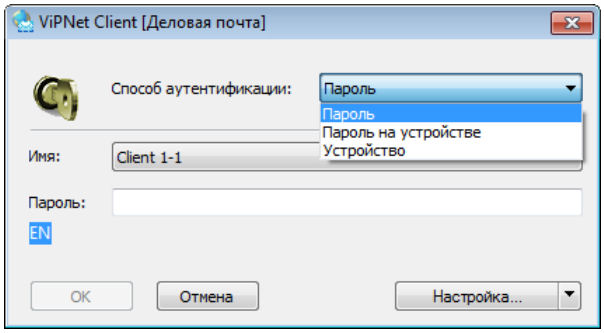


Рисунок 2: Окно входа в программу

- Чтобы запустить программу ViPNet Деловая почта с помощью ярлыка, выполните одно из действий:

  - В меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Client** > **Деловая почта** (во время установки положение программы в меню **Пуск** могло быть изменено).

  - Дважды щелкните ярлык  на рабочем столе (ярлык отображается на рабочем столе, если при установке программы была выбрана соответствующая опция).

  Откроется окно входа в программу.

2 В окне входа в программу выполните следующие действия:

2.1 В зависимости от текущего способа аутентификации (см. «Способы аутентификации пользователя» на стр. 26), для входа в программу введите пароль пользователя либо подключите внешнее устройство хранения данных и введите ПИН-код.

2.2 После ввода необходимых для аутентификации данных нажмите кнопку **OK**. Откроется окно программы ViPNet Деловая почта.

Чтобы свернуть окно программы на панель задач, нажмите кнопку **Свернуть**  в правом верхнем углу окна.

Чтобы завершить работу с программой, выполните одно из действий:

- В окне программы ViPNet Деловая почта в меню **Файл** выберите пункт **Выход**.
- Нажмите кнопку **Закрыть**  в правом верхнем углу окна.

Примечание. Если в окне **Настройка** в разделе **Общие** (см. «Настройка общих параметров» на стр. 107) установлен флажок **По кнопке «Закрыть» сворачивать окно почты в «трей»**, при нажатии кнопки **Закрыть**  окно программы будет свернуто в область уведомлений на панели задач.

Смена пользователя

Если на сетевом узле зарегистрировано несколько пользователей, сменить пользователя можно не выходя из программы ViPNet Деловая почта. Для этого выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Инструменты** выберите пункт **Смена пользователя**. Откроется окно входа в программу (см. рисунок на стр. 24).
2. Введите пароль пользователя, от имени которого требуется войти в программу, и нажмите **OK**.

Примечание. На сетевом узле должны быть установлены справочники и ключи пользователя, от имени которого выполняется вход в программу.

Способы аутентификации пользователя

В программе ViPNet Деловая почта предусмотрено три способа аутентификации:

- Пароль (на стр. 28). Для входа в программу вам следует ввести свой пароль. Каждый раз после ввода пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу.
- Пароль на устройстве (на стр. 29). Для входа в программу вам следует подключить устройство и ввести ПИН-код.

  Как правило, использование этого способа аутентификации предполагает, что ваш пароль хранится на устройстве и вам не известен. Однако если вы знаете пароль, то помимо аутентификации с помощью внешнего устройства для входа в программу можно использовать аутентификацию по паролю. Данная возможность обеспечивает вход в программу в случае неисправности внешнего устройства (для этого вам понадобится узнать свой пароль у администратора сети ViPNet).

Внимание! Способ аутентификации **Пароль на устройстве** не отвечает требованиям безопасности, и возможность его использования оставлена исключительно для совместимости с программным обеспечением ViPNet более ранних версий. В связи с этим, если программа ViPNet Деловая почта была обновлена до версии 4.x и в ней используется данный способ аутентификации, то настоятельно рекомендуется его изменить на **Пароль** или **Устройство**.

- Устройство (на стр. 30). Для входа в программу вам следует подключить устройство и ввести ПИН-код (и в некоторых случаях пароль).

По умолчанию установлен способ аутентификации **Пароль.** В режиме администратора можно изменить способ аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 123).

При использовании способов **Пароль на устройстве** и **Устройство** аутентификация пользователя осуществляется с помощью внешних устройств (см. «Внешние устройства» на стр. 199). Чтобы использовать какое-либо устройство для аутентификации пользователя, на компьютер необходимо установить драйверы этого устройства и затем

записать ключи на это устройство. Записать ключи на внешнее устройство можно при изменении способа аутентификации пользователя или в программе ViPNet Удостоверяющий и ключевой центр при создании дистрибутива ключей (в программе ViPNet Network Manager работа с внешними устройствами невозможна).

Внимание! Если при использовании способов аутентификации **Пароль на устройстве** или **Устройство** внешнее устройство будет отключено, может произойти автоматическая блокировка компьютера — в соответствии с настройками, заданными в режиме администратора. Для продолжения работы необходимо вновь подключить это внешнее устройство.

На схеме ниже представлены факторы аутентификации, используемые при выборе каждого способа аутентификации в зависимости от типа внешнего устройства.

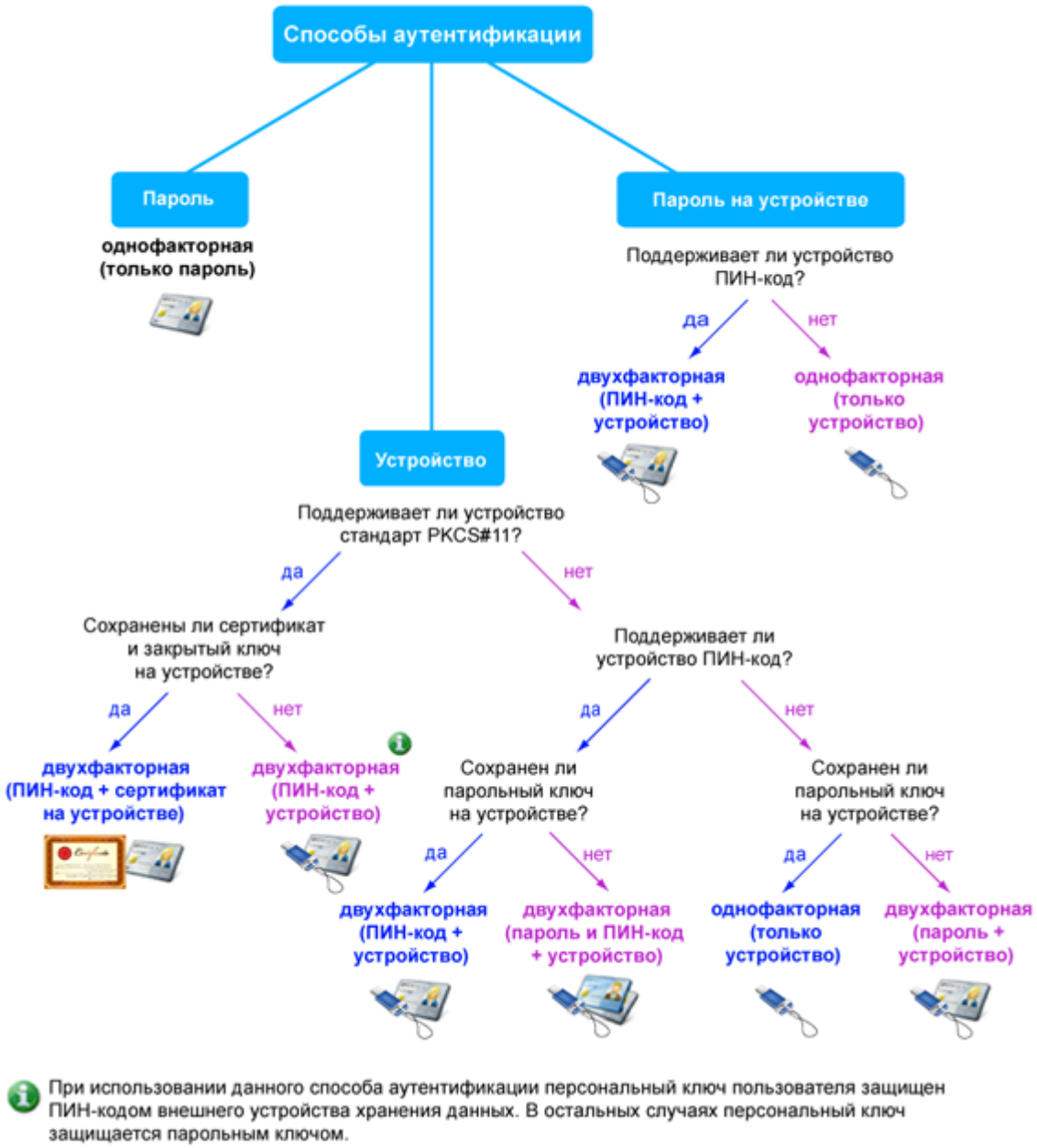


Рисунок 3: Схема соответствия между факторами и способами аутентификации

Пароль

Для входа в программу ViPNet Деловая почта с помощью пароля в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Пароль**.

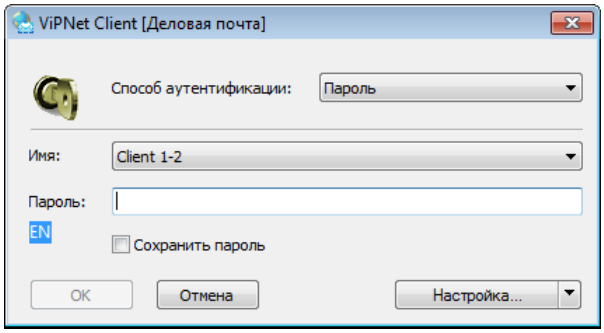


Рисунок 4: Способ аутентификации «Пароль»

2 При необходимости в списке **Имя** выберите ваше имя пользователя ViPNet.

Примечание. В данном списке отображаются имена всех пользователей, ключи которых были установлены на данном сетевом узле. Если на узле не установлены ключи ни одного пользователя, список будет пуст.

3 В поле **Пароль** введите ваш пароль.

Если сохранение пароля в реестре разрешено настройками программы (см. «Дополнительные настройки параметров безопасности» на стр. 122), для сохранения пароля можно установить соответствующий флажок.

4 Нажмите кнопку **OK**.

Пароль на устройстве

Внимание! Во избежание неполадок в работе ПО ViPNet не следует использовать способ аутентификации **Пароль на устройстве**. При использовании данного способа аутентификации рекомендуется его изменить на **Пароль** или **Устройство** (см. «Изменение способа аутентификации пользователя» на стр. 123).

Для входа в программу ViPNet Деловая почта с помощью пароля на устройстве в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Пароль на устройстве**.

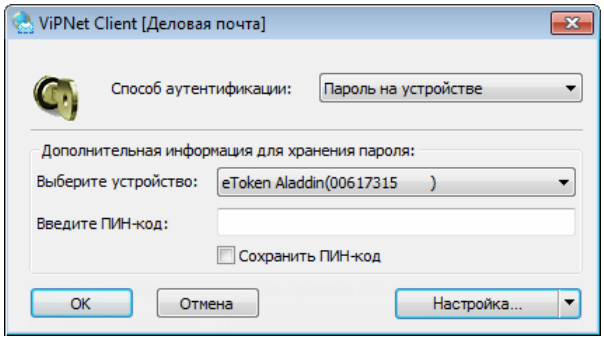


Рисунок 5: Способ аутентификации «Пароль на устройстве»

2 Подключите внешнее устройство, на котором находится ваш пароль.

3 В списке **Выберите устройство** выберите внешнее устройство.

4 Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства (см. рисунок на стр. 28).

Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, установите соответствующий флажок.

5 Нажмите кнопку **OK**.

Устройство

Для входа в программу ViPNet Деловая почта с помощью устройства в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Устройство**.

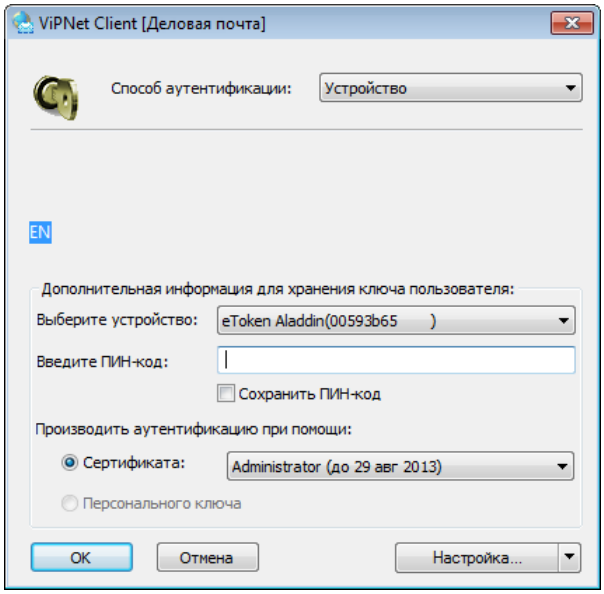


Рисунок 6: Способ аутентификации «Устройство»

2 Подключите внешнее устройство.

3 Если требуется, в списке ниже выберите ваше имя пользователя и в поле **Пароль** введите свой пароль. Необходимость ввода пароля зависит от типа используемого внешнего устройства (см. рисунок на стр. 28).

4 В списке **Устройство** выберите внешнее устройство, на котором находится ваш персональный ключ или сертификат с закрытым ключом подписи.

5 Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства. Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, установите соответствующий флажок.

6 В списке **Производить аутентификацию при помощи** установите переключатель в одно из следующих положений:

- **Сертификата** — чтобы выполнить аутентификацию с помощью вашего сертификата и соответствующего ему закрытого ключа, хранящегося в контейнере ключей на используемом устройстве. В списке сертификатов, обнаруженных на устройстве, выберите нужный сертификат. В случае возникновения затруднений при аутентификации с помощью сертификата см. раздел Не удается выполнить аутентификацию с помощью сертификата (на стр. 191).

Примечание. Для аутентификации с помощью сертификата должны быть выполнены следующие условия:

- Внешнее устройство хранения данных поддерживает стандарт PKCS#11, в том числе операции подписи и шифрования. В текущий момент внешние устройства с поддержкой алгоритма ГОСТ 34.10-2001 использоваться не могут, поскольку они поддерживают только операцию вычисления подписи.
- Сертификат действителен (срок действия сертификата не истек).
- Сертификат не отозван.
- Сертификат имеет назначение «Проверка подлинности клиента». Это назначение отображается в окне **Сертификат**, на вкладке **Состав**, в поле **Расширенное использование ключа**.
- Сертификат издателя установлен в системное хранилище **Доверенные корневые центры сертификации**.

- **Персонального ключа** — чтобы выполнить аутентификацию с помощью персонального ключа (который входит в состав ключей пользователя и хранится на используемом устройстве).

7 Нажмите кнопку **OK**.

Интерфейс программы

Внешний вид окна программы ViPNet Деловая почта представлен на следующем рисунке:

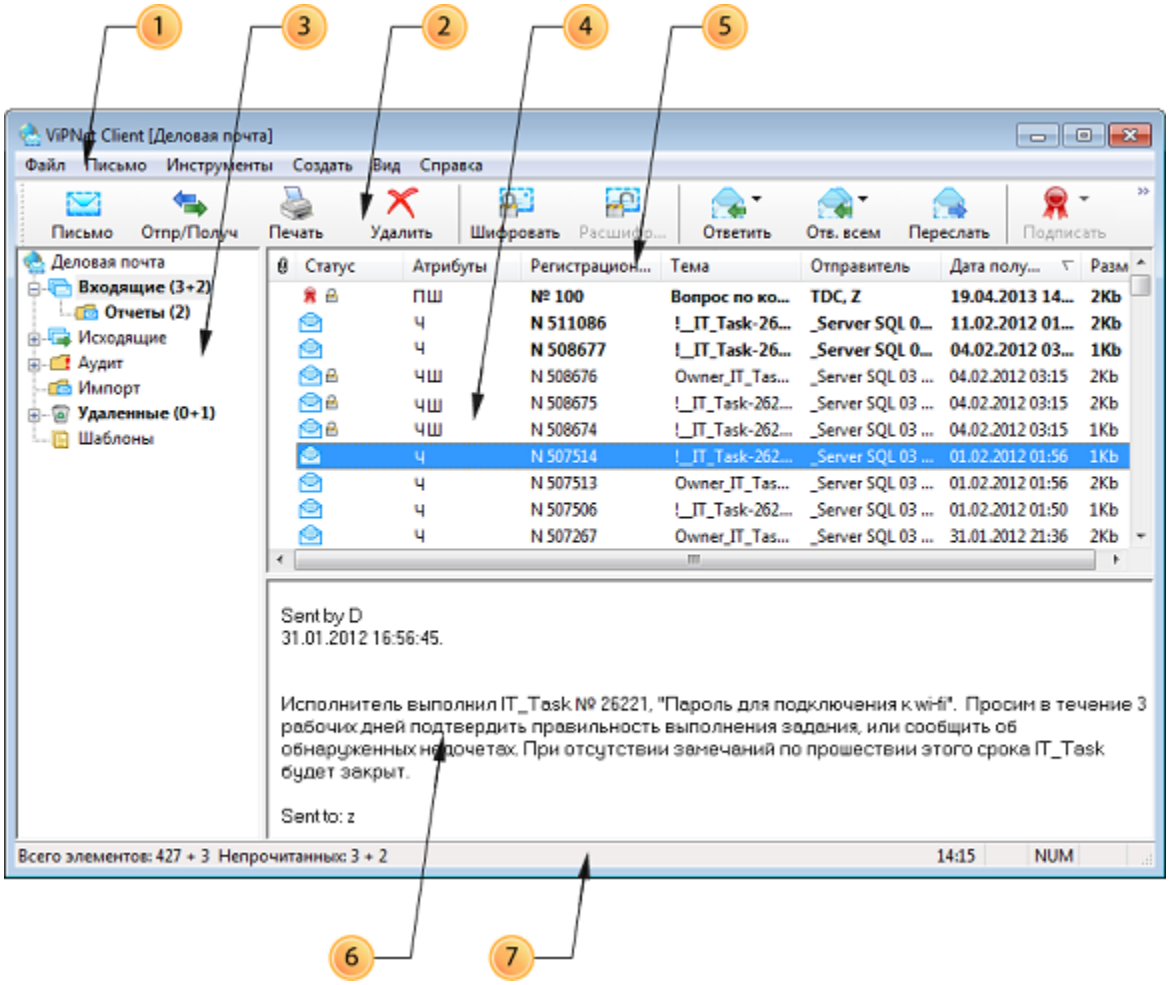


Рисунок 7: Интерфейс программы ViPNet Деловая почта

Цифрами на рисунке обозначены:

1 Главное меню программы.

2 Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Панель инструментов**, затем щелкните **Настройка**.

3 Панель папок. На этой панели отображается иерархическая структура папок программы ViPNet Деловая почта.

Если в папке есть непрочитанные письма, имя папки выделено полужирным шрифтом, а количество непрочитанных писем указано после имени папки в скобках. Если папка содержит вложенные папки, в которых есть непрочитанные письма, в скобках указаны два числа: количество непрочитанных писем в папке и суммарное количество непрочитанных писем во вложенных папках.

4 Панель писем. На этой панели отображается список писем, находящихся в выбранной на панели (**3**) папке.

Чтобы просмотреть список находящихся в папке писем в формате HTML, на панели писем щелкните правой кнопкой мыши заголовок какого-либо столбца и в контекстном меню выберите пункт **Просмотр в HTML-формате.**

5 Столбцы панели писем (**4**).

Чтобы отсортировать список писем по одному из столбцов, щелкните заголовок столбца. С помощью контекстного меню можно удалить или добавить столбцы.

В столбце **Статус** отображаются значки, которые обозначают статус письма. В столбце **Атрибут** отображаются коды статуса письма. Описание значков и кодов статуса представлено в следующей таблице:

Таблица 3. Статусы писем

Значок	Атрибут	Статус
	Ш	Письмо и все вложения зашифрованы
	П	Все элементы письма (текст и вложения) подписаны и все подписи верны
	п	Не все элементы письма подписаны, но все имеющиеся подписи верны
	Н	Все элементы письма подписаны и хотя бы одна подпись неверна
	н	Не все элементы письма подписаны и хотя бы одна подпись неверна
	У	Письмо упаковано для всех выбранных получателей, но еще не отправлено
	у	Письмо упаковано для некоторых получателей (не для всех), но еще не отправлено
	О	Письмо отправлено всем получателям, но еще не доставлено
	о	Письмо отправлено некоторым (не всем) получателям, но еще не доставлено

	Д	Письмо доставлено всем получателям, но еще не прочитано
	д	Письмо доставлено некоторым получателям, но еще не всем
	Ч	В папке **Исходящие**: письмо прочитано всеми получателями. В папке **Входящие**: текст письма и все вложения прочитаны.
	ч	В папке **Исходящие**: письмо прочитано некоторыми получателями, но еще не всеми. В папке **Входящие**: текст письма прочитан, но не все вложения прочитаны.
	!	Письмо не может быть отправлено получателю. Такая ситуация может возникнуть в случае, если клиент, на который отправлено письмо, отключен от координатора или удален из сети.

Примечание. Текст письма считается прочитанным, если письмо было открыто в отдельном окне. После ответа на письмо текст этого письма считается прочитанным.

Вложение считается прочитанным, если оно было просмотрено или сохранено на диск.

При пересылке и при сохранении письма на диск текст письма и все его вложения считаются прочитанными.

6 Панель чтения. На этой панели отображается текст письма, выбранного на панели (**4**).

7 Строка состояния. В строке состояния указано общее количество писем в выбранной папке и ее подпапках, а также количество непрочитанных (в папке **Входящие**) или недоставленных (в папке **Исходящие**) писем.

Количество писем определенного типа отображается в виде суммы двух чисел: количество писем данного типа в выбранной папке и суммарное количество писем данного типа во вложенных папках.

Чтобы отобразить или скрыть строку состояния, в меню **Вид** выберите пункт **Строка состояния**.

Организация хранения писем с помощью папок

Хранение писем в программе ViPNet Деловая почта можно упорядочить с помощью иерархической структуры папок. Папки отображаются на левой панели окна программы (см. «Интерфейс программы» на стр. 33).

Папки в программе ViPNet Деловая почта делятся на две категории:

- Специальные — создаются автоматически программой ViPNet Деловая почта и не могут быть переименованы или удалены.
- Пользовательские — создаются пользователем, могут быть переименованы или удалены.

Действия, которые можно выполнить при работе папками, описаны в следующих подразделах.

Специальные папки

Возможности работы со специальными папками программы ViPNet Деловая почта ограничены. Специальные папки и их особенности перечислены ниже:

- **Входящие** — папка, в которую по умолчанию помещаются входящие письма (см. «Просмотр письма и его свойств в основном окне программы» на стр. 52).
- **Входящие > Извещения** — папка, в которую помещаются извещения о доставке и прочтении в виде отдельных писем (см. «Запрос извещений о доставке и прочтении в виде отдельного письма» на стр. 47).

  Эта папка создается при получении первого извещения, по умолчанию она отсутствует.
- **Исходящие** — папка, в которую помещаются создаваемые письма (см. «Создание письма» на стр. 45).
- **Исходящие > Извещения** — папка, в которую помещаются извещения, отправляемые в виде отдельных писем.

Эта папка создается при отправке первого извещения, по умолчанию она отсутствует.

- **Удаленные** — папка, в которую помещаются удаленные письма (см. «Удаление писем» на стр. 65).

  В папке **Удаленные** нельзя создавать и переименовывать вложенные папки.

- **Аудит** — папка, содержащая информацию о письмах, которые были удалены из папки **Удаленные**.

  В папке **Аудит** нельзя создавать и переименовывать вложенные папки. Удалять папки и письма из папки **Аудит** можно только при работе в режиме администратора (см. «Работа в программе с правами администратора» на стр. 120).

- **Шаблоны** — папка, в которую помещаются шаблоны писем (см. «Создание и использование шаблонов писем» на стр. 50).

- **Импорт** — папка, в которую помещаются импортированные письма (см. «Экспорт и импорт писем» на стр. 62).

Пользовательские папки

Использование папок помогает упорядочить хранилище писем в программе ViPNet Деловая почта.

Чтобы создать папку:

1. На панели папок (см. «Интерфейс программы» на стр. 33) выберите папку, внутри которой требуется создать новую папку (это может быть и корневая папка **Деловая почта**), и выполните одно из действий:

   - Щелкните папку правой кнопкой мыши и в контекстном меню выберите пункт **Создать новую папку**.
   - В меню **Файл** выберите пункт **Папки**, затем щелкните **Новая папка**.

   Откроется окно **Создание новой папки**.

2. В окне **Создание новой папки** введите имя для создаваемой папки и нажмите **OK**. На панели папок появится новая папка с заданным именем.

Примечание. В одной папке нельзя создать две подпапки с одинаковыми именами. В папках **Удаленные** и **Аудит** (см. «Специальные папки» на стр. 36) создание новых папок невозможно.

Чтобы переименовать папку:

1. На панели папок (см. «Интерфейс программы» на стр. 33) выберите пользовательскую папку, которую требуется переименовать, и выполните одно из действий:
   - Щелкните имя папки.
   - Щелкните папку правой кнопкой мыши и в контекстном меню выберите пункт **Переименовать папку**.

   На месте имени папки появится поле ввода.
2. Введите новое имя папки и нажмите клавишу **Enter** или щелкните мышью за пределами поля ввода.

Примечание. В одной папке нельзя создать две подпапки с одинаковыми именами. Невозможно переименовать специальные папки (см. «Специальные папки» на стр. 36).

Чтобы перенести папку, щелкните ее и перетащите в папку назначения. Нельзя переносить папки:

- из папок **Входящие** и **Удаленные > Входящие** в папку **Исходящие**;
- из любых папок, кроме **Удаленные > Входящие**, в папку **Входящие**;
- в папки **Шаблоны**, **Удаленные** и **Аудит**;
- между двумя подпапками папки **Удаленные** или папки **Аудит**.

Чтобы очистить содержимое папки:

1. Щелкните папку правой кнопкой мыши и в контекстном меню выберите пункт **Очистить содержимое папки**.
2. В окне подтверждения нажмите кнопку **Да**.

   Все письма из папки будут удалены (см. «Удаление писем» на стр. 65).

Чтобы удалить папку:

1. Выберите папку, которую требуется удалить, и выполните одно из действий:
   - Нажмите клавишу **Delete**.

- Нажмите кнопку **Удалить**  на панели инструментов.

2 В окне подтверждения нажмите кнопку **Да.**

Выбранная папка вместе с подпапками и письмами будет перемещена в папку **Удаленные**. При этом в папке **Удаленные** будет автоматически создана структура папок, полностью повторяющая исходную. Например, в папке **Входящие > Папка-1** находится **Папка-2**. При удалении этой папки она вместе со всем содержимым будут перемещена в папку **Удаленные > Входящие > Папка-1**.

Если папка удалена из папки **Удаленные**, она таким же образом переносится в папку **Аудит**. При этом находящиеся в папке письма заменяются записями о времени удаления и о пользователе, осуществившем удаление. Удалить папку из папки **Аудит** может только администратор сетевого узла (см. «Работа в программе с правами администратора» на стр. 120).

Адресная книга

Адресная книга представляет собой список получателей, которым можно отправлять письма. Этот список не может быть изменен пользователем сетевого узла, так как определяется связями, которые были заданы для данного сетевого узла администратором сети ViPNet в программе ViPNet Центр управления сетью или ViPNet Network Manager.

Чтобы открыть адресную книгу, в окне программы ViPNet Деловая почта в меню **Инструменты** выберите пункт **Адресная книга**. Откроется окно **Адресная книга**.

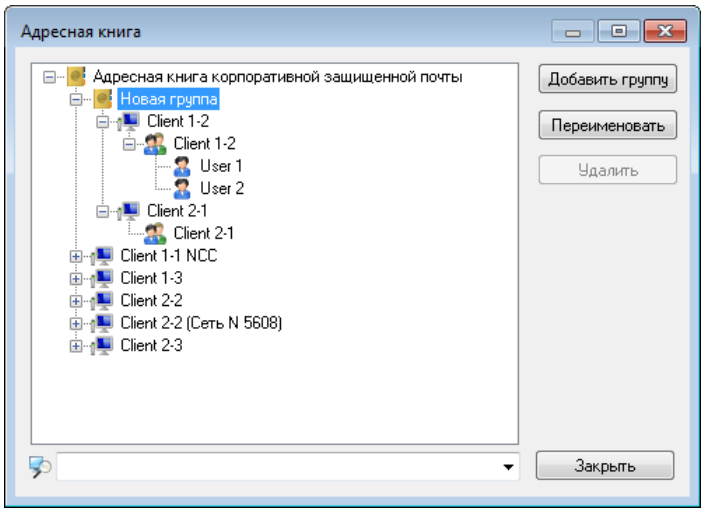


Рисунок 8: Адресная книга программы ViPNet Деловая почта

Адресная книга используется для выбора адресатов при создании писем (см. «Создание и отправка нового письма» на стр. 44). Письмо можно адресовать сетевому узлу, коллективу или пользователю сети ViPNet. Таким образом, в программе ViPNet Деловая почта существует три уровня адресации (см. «Уровни адресации» на стр. 41).

Для удобства клиенты в адресной книге можно распределить по группам (см. «Группы адресатов» на стр. 41).

Уровни адресации

Каждому клиенту, с которым связан данный клиент, в адресной книге программы ViPNet Деловая почта (см. рисунок на стр. 40) соответствует три уровня адресации:

1. Сетевой узел. Данный уровень адресации соответствует всем пользователям узла. То есть зашифрованное письмо, адресованное узлу, могут прочитать все его пользователи.
2. Коллектив. Данный уровень адресации соответствует пользователям, которые зарегистрированы на узле и входят в одну группу пользователей в программе ViPNet Центр управления сетью. Зашифрованное письмо, адресованное коллективу, могут прочитать только члены этого коллектива.
3. Пользователь. Данный уровень соответствует конкретному пользователю узла. Письмо, адресованное пользователю, могут прочесть все члены коллектива, в который входит этот пользователь. Таким образом, этот уровень адресации не может использоваться для разграничения доступа к зашифрованным письмам, а служит только для определения адресата.

Примечание. Если пользователь является единственным членом своего коллектива и его имя совпадает с именем коллектива, то в адресной книге программы ViPNet Деловая почта отображается только коллектив, а пользователь не отображается.

Группы адресатов

По умолчанию в адресной книге программы ViPNet Деловая почта присутствует одна группа, которая называется **Адресная книга корпоративной защищенной почты**. Эту группу нельзя переименовать или удалить.

Чтобы создать новую группу, выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Инструменты** выберите пункт **Адресная книга** либо в окне создания письма (см. «Создание и отправка нового письма» на стр. 44) нажмите кнопку **Получатели**  .
2. В окне **Адресная книга** (см. рисунок на стр. 40) выберите группу клиентов, в которой требуется создать новую группу.
3. Нажмите кнопку **Добавить группу**. В адресной книге появится папка и поле для ввода имени группы.

4 Введите имя для созданной группы и нажмите клавишу **Enter.**

5 Чтобы перенести в новую группу клиент, щелкните этот клиент, его коллектив или пользователя мышью и перетащите в группу.

Чтобы переименовать группу:

1 Выберите группу в окне **Адресная книга.**

2 Нажмите кнопку **Переименовать**. На месте имени группы появится поле ввода.

3 Введите новое имя группы и нажмите клавишу **Enter** или щелкните мышью за пределами поля ввода.

Чтобы удалить группу:

1 Если в группе, которую требуется удалить, есть клиенты, перенесите их в другие группы. Удалить группу, в которой присутствуют клиенты, невозможно.

2 Выберите группу в списке.

3 Нажмите кнопку **Удалить**, группа будет удалена.

3

Работа с письмами

Создание и отправка нового письма

Окно создания и просмотра писем

Внешний вид окна, в котором осуществляется создание новых писем (см. «Создание письма» на стр. 45) и просмотр отправленных и полученных писем (см. «Просмотр письма и вложений в отдельном окне» на стр. 55), представлен на следующем рисунке:

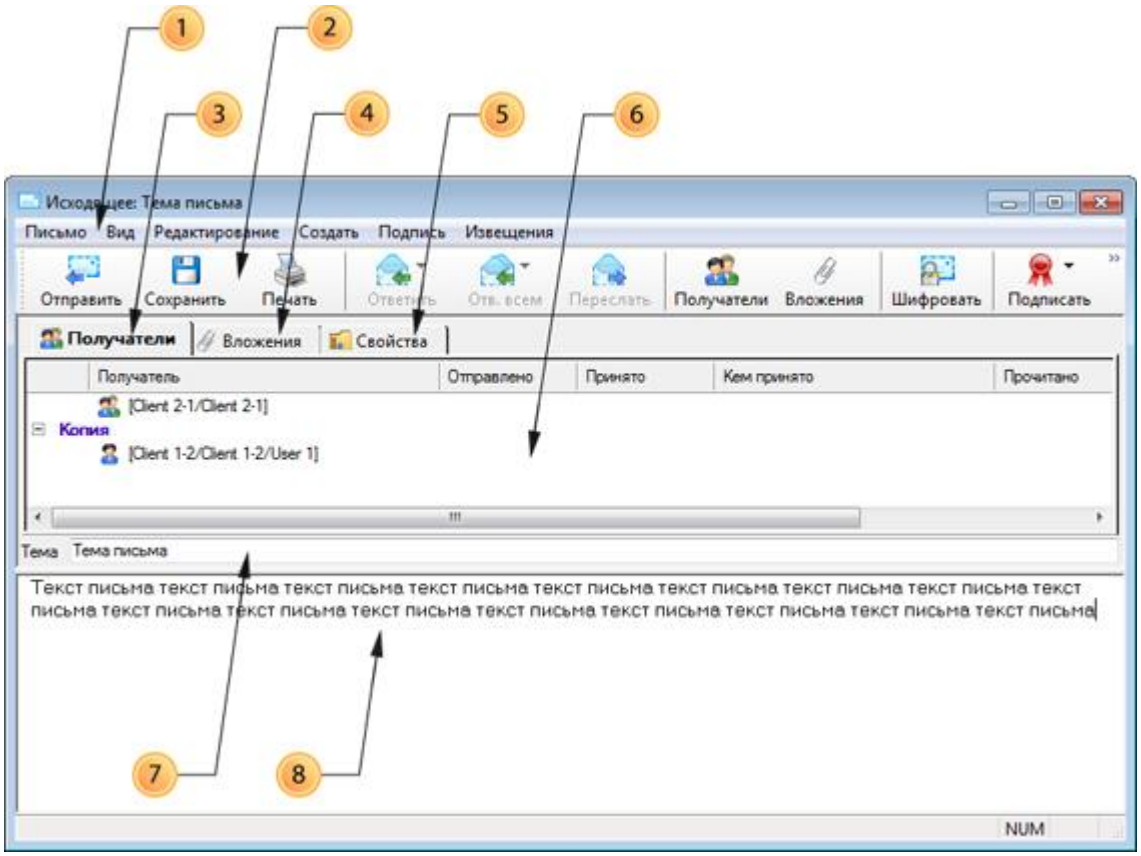


Рисунок 9: Интерфейс окна создания и просмотра писем

Цифрами на рисунке обозначены:

1. Главное меню.
2. Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Панель инструментов**, затем щелкните **Настройка**.

3 Вкладка **Получатели**. На этой вкладке перечислены получатели письма. Если открыто отправленное и полученное письмо, отображается также информация о времени отправки и получения письма, принявшем письмо пользователе и так далее.

4 Вкладка **Вложения**. На этой вкладке отображаются файлы, вложенные в письмо.

5 Вкладка **Свойства**. На этой вкладке содержится информация о регистрационном номере, времени создания и отправителе письма, а также о времени последней проверки электронной подписи (если она есть).

6 Панель, предназначенная для отображения содержимого вкладок **Получатели, Вложения** и **Свойства.**

7 Поле **Тема**. В этом поле отображается тема письма.

8 Панель, на которой отображается текст письма.

Создание письма

Чтобы написать письмо, выполните следующие действия:

1 В окне программы ViPNet Деловая почта на панели инструментов нажмите кнопку **Письмо** . Откроется окно создания письма (см. «Окно создания и просмотра писем» на стр. 44).

2 В поле **Тема** введите тему письма.

3 На нижней панели окна введите текст письма.

4 Если в письмо требуется добавить вложения:

- Выполните одно из действий:
  - Перетащите файлы в окно создания письма.
  - Нажмите кнопку **Вложения** на панели инструментов. В окне **Открыть** выберите один или несколько файлов.

  Для каждого файла будет открыто окно **Введите описание вложения.** По умолчанию описание вложения совпадает с именем файла.

Примечание. Описание вложения должно содержать не более 56 символов.

- Чтобы добавить все файлы без изменения описаний вложений, нажмите кнопку **Добавить все**. Чтобы изменить описания вложений, для каждого файла введите новое описание и нажмите кнопку **Добавить**.

  Выбранные файлы будут добавлены в письмо.

Чтобы удалить вложения из письма:

- В окне создания письма откройте вкладку **Вложения**.
- Выберите вложение, которое нужно удалить, и нажмите клавишу **Delete**.

5 Если необходимо зашифровать письмо, на панели инструментов нажмите кнопку **Шифровать**. Если необходимо подписать письмо электронной подписью (см. «Электронная подпись и шифрование» на стр. 71), нажмите кнопку **Подписать**.

6 Чтобы указать получателей письма:

- На панели инструментов нажмите кнопку **Получатели**. Откроется окно адресной книги (см. «Адресная книга» на стр. 40).

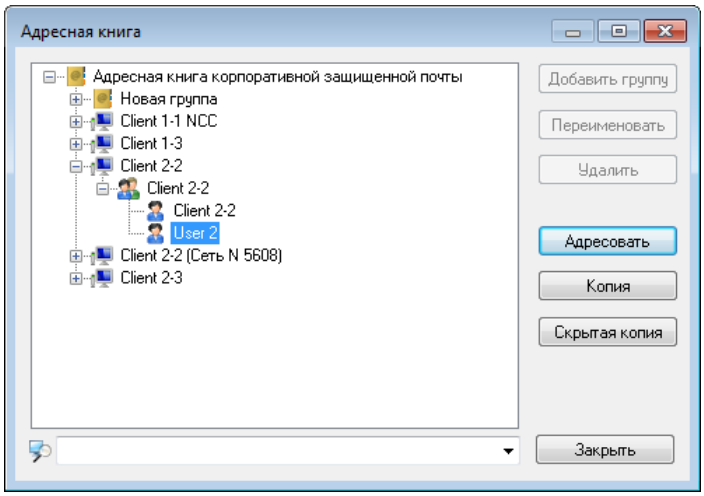


Рисунок 10: Выбор адресатов

- В окне **Адресная книга** выберите клиент, коллектив или пользователя (см. «Уровни адресации» на стр. 41). Чтобы отфильтровать список получателей, в строку поиска внизу окна введите часть имени нужного получателя.

  Выбрав одного или несколько получателей, выполните одно из действий:

  - Чтобы адресовать письмо выбранным получателям, нажмите кнопку **Адресовать**.
  - Чтобы отправить выбранным получателям копию письма, нажмите кнопку **Копия**.

- Чтобы отправить выбранным получателям скрытую копию письма, нажмите кнопку **Скрытая копия**.

- Повторите описанные в предыдущем пункте действия, чтобы добавить необходимое количество получателей. Затем в окне **Адресная книга** нажмите кнопку **Закрыть**.

Чтобы удалить получателя, выберите его на вкладке **Получатели** (см. «Окно создания и просмотра писем» на стр. 44) и нажмите клавишу **Delete**.

7 Для каждого получателя письма можно написать аннотацию — краткое примечание не длиннее 245 символов. Чтобы добавить аннотацию:

- Дважды щелкните имя получателя и в окне **Аннотация** введите текст.
- Нажмите кнопку **OK**. Слева от имени получателя появится значок .

8 Закончив создание нового письма, выполните одно из действий:

- Чтобы сохранить письмо в папке **Исходящие**, нажмите кнопку **Сохранить** на панели инструментов либо закройте окно создания сообщения и в окне сообщения о сохранении изменений нажмите кнопку **Да**.
- Чтобы отправить письмо, на панели инструментов нажмите кнопку **Отправить** .

Примечание. Статус отправленного письма можно посмотреть в папке **Исходящие** в столбце **Атрибуты** (см. «Интерфейс программы» на стр. 33). Также можно запросить извещение о доставке и прочтении письма (см. «Запрос извещений о доставке и прочтении в виде отдельного письма» на стр. 47).

Запрос извещений о доставке и прочтении в виде отдельного письма

При отправке письма из программы ViPNet Деловая почта можно запросить извещение о доставке и прочтении письма. Чтобы запросить извещение:

1 Выполните действия, описанные в разделе Создание письма (на стр. 45).

2 Перед отправкой письма в меню **Извещения** выберите пункт **Запросить извещение** или на панели инструментов нажмите кнопку **Извещение** .

3 Отправьте письмо, нажав кнопку **Отправить** .

После получения письма адресатом отправителю автоматически будет выслано извещение о доставке, после прочтения письма — извещение о прочтении. Извещение представляет собой обычное письмо программы ViPNet Деловая почта. Тема извещения совпадает с темой исходного письма, но к теме извещения о доставке добавляется префикс «AD:», к теме извещения о прочтении — префикс «AR:». Если исходное письмо было зашифровано, извещение также шифруется.

В программе ViPNet Деловая почта на клиенте получателя исходящие извещения помещаются в папку **Исходящие** > **Извещения**, на клиенте отправителя входящие извещения помещаются в папку **Входящие** > **Извещения**. Эти папки создаются при отправке или получении первого извещения и не могут быть удалены или переименованы. Статус извещения, как и статус обычного письма, можно посмотреть в столбце **Атрибуты.**

Текст извещения содержит следующую информацию:

- Дата и время получения или прочтения письма.
- Тема письма.
- Имя отправителя и результат проверки электронной подписи отправителя.
- Регистрационный номер письма.
- Результаты проверки электронных подписей для подписанного текста письма и каждого из подписанных вложений.
- Контрольные суммы электронных подписей для подписанного текста письма и каждого из подписанных вложений.

Отправка письма в виде вложения

Чтобы отправить письмо из программы ViPNet Деловая почта в виде вложения, выполните следующие действия:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) на левой панели выберите папку с письмами, которые требуется отправить в виде вложений.
2. На панели писем выберите одно или несколько писем.
3. Выполните одно из действий:
   - Щелкните письма правой кнопкой мыши и в контекстном меню выберите пункт **Переслать как вложения**.
   - В меню **Письмо** выберите пункт **Переслать как вложения**.

Будет открыто окно создания нового письма. Одновременно для каждого письма, которое было выбрано для отправки в виде вложения, откроется окно **Введите имя вложения**.

4 Чтобы добавить все письма в виде файлов, сохранив их имена, нажмите кнопку **Добавить все**. Чтобы изменить имена файлов, для каждого вложения введите имя и нажмите кнопку **Добавить**.

Выбранные письма будут добавлены в виде вложений.

5 Завершите создание письма и отправьте его, как описано в разделе Создание письма (на стр. 45).

Создание и использование шаблонов писем

При частой отправке однотипных писем удобно использовать шаблоны. В программе ViPNet Деловая почта шаблоны хранятся в папке **Шаблоны**. Создать шаблон можно двумя способами:

- Создать шаблон на основе существующего письма. Для этого выполните следующие действия:
  - Выберите письмо, на основе которого требуется создать шаблон.
  - Перенесите письмо (см. «Перенос писем в другую папку программы» на стр. 64) в папку **Шаблоны** или ее подпапку.

  В папке **Шаблоны** на основе выбранного письма будет создан новый шаблон, само письмо при этом останется в исходной папке.

  Созданный шаблон сохранит все параметры исходного письма, кроме регистрационного номера, электронной подписи и атрибутов отправки, получения и прочтения. В качестве отправителя будет указан пользователь, создавший шаблон.
- Создать новый шаблон. Для этого выполните следующие действия:
  - В окне программы ViPNet Деловая почта в меню **Создать** выберите пункт **Новый шаблон**.
  - Откроется окно **Шаблон**, аналогичное окну создания письма (см. «Окно создания и просмотра писем» на стр. 44).
  - Введите текст и тему письма, укажите получателей и задайте другие параметры, как описано в разделе Создание письма (на стр. 45).
  - Нажмите кнопку **Сохранить**  .

  Шаблон будет сохранен в папке **Шаблоны**. Созданному шаблону не будет присвоен регистрационный номер, в качестве отправителя в шаблоне будет указан пользователь, создавший шаблон.

Чтобы использовать шаблон для создания нового письма, выполните следующие действия:

1. На левой панели окна программы ViPNet Деловая почта выберите папку **Шаблоны** или ее подпапку, в которой находится нужный шаблон.

2 Откройте шаблон двойным щелчком либо выберите его в списке и нажмите клавишу **Enter**.

3 В окне шаблона на панели инструментов нажмите кнопку **Копировать**  . В папке **Исходящие** будет создана письмо, являющееся копией шаблона.

4 При необходимости отредактируйте созданное письмо (см. «Создание письма» на стр. 45) и отправьте его.

Просмотр письма и его свойств в основном окне программы

Чтобы просмотреть письмо:

1 В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) на левой панели выберите папку с письмом, которое требуется прочесть.

> **Примечание.** Если в папке или ее подпапках есть непрочитанные письма, имя папки выделено полужирным шрифтом. Количество непрочитанных писем указано рядом с именем папки в скобках.
>
> Непрочитанные письма, находящиеся в выбранной папке, выделены на панели писем полужирным шрифтом.

2 На панели писем выберите нужное письмо.

Если письмо не зашифровано, его текст отобразится на панели писем. Если письмо не прочитано, после этого оно не считается прочитанным.

Если письмо зашифровано, на панели чтения отобразится текст «Это письмо зашифровано. Для прочтения его необходимо открыть». Чтобы просмотреть зашифрованное письмо, выполните одно из действий:

- Нажмите кнопку **Расшифровать** на панели инструментов. Текст письма отобразится на панели чтения. Если письмо не прочитано, после этого оно не считается прочитанным.
- Откройте письмо в отдельном окне (см. «Просмотр письма и вложений в отдельном окне» на стр. 55).

3 Если в письме есть вложения (в столбце **Вложение** отображается значок скрепки), для просмотра вложений откройте письмо в отдельном окне (см. «Просмотр письма и вложений в отдельном окне» на стр. 55).

Также в основном окне программы доступны следующие действия с письмами:

1 Чтобы пометить непрочитанное письмо как прочитанное, щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Пометить как прочтенные**.

При этом в столбце **Атрибуты** (см. «Интерфейс программы» на стр. 33) появится значок .

2 Чтобы пометить прочитанное письмо как непрочитанное, щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Пометить как непрочтенные.** При этом значок статуса письма не изменятся.

3 Для неотправленного письма можно изменить регистрационный номер (см. «Настройка параметров работы с письмами» на стр. 113). Для этого:

- В папке **Исходящие** выберите неотправленное письмо.
- Щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Изменить регистрационный номер**. Откроется окно **Смена регистрационного номера.**

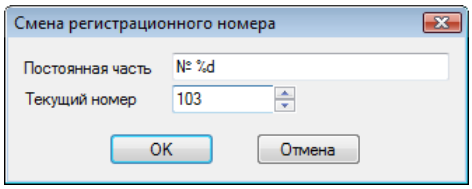


Рисунок 11: Изменение регистрационного номера

- В поле **Постоянная часть** измените постоянную часть номера, если требуется.
- В поле **Текущий номер** введите номер, который требуется присвоить письму. Номер должен быть не меньше последнего присвоенного номера (указан в поле по умолчанию) и может превышать его не более чем на 100.
- Задав регистрационный номер письма, нажмите кнопку **OK**.

Если для письма была изменена постоянная часть регистрационного номера, то постоянная часть в настройках параметров писем не изменится (см. «Настройка параметров работы с письмами» на стр. 113). Если был изменен текущий номер, он также изменится в настройках программы, и в дальнейшем нумерация будет продолжена с заданного номера.

4 Чтобы отправить неотправленное письмо, выберите его в папке **Исходящие**, щелкните правой кнопкой мыши и в контекстном меню выберите пункт **Отправить.**

5 Чтобы просмотреть подробную информацию о письме и его получателях, щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Свойства.** Откроется окно **Свойства письма**.

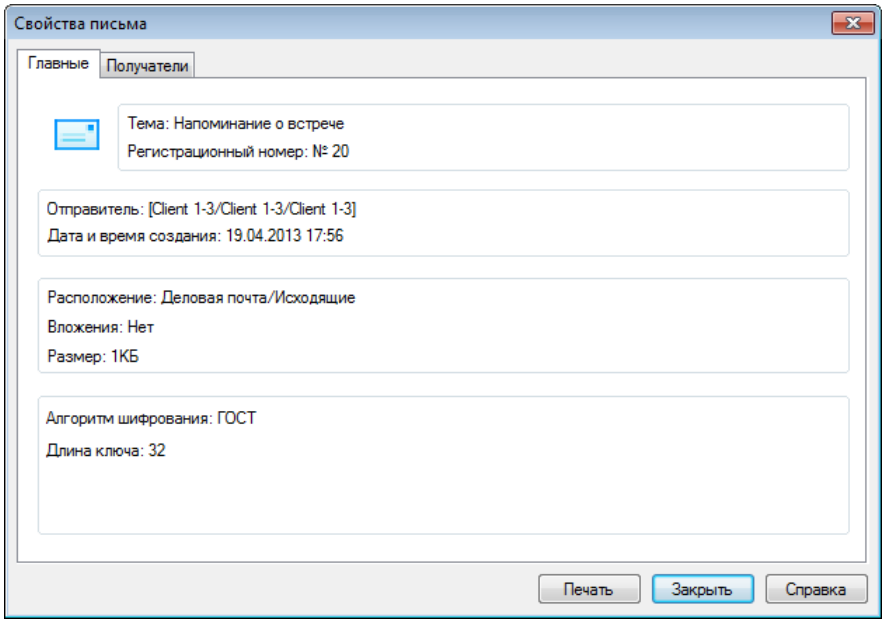


Рисунок 12: Свойства письма

6 Чтобы распечатать письмо, выберите его на панели писем и нажмите кнопку **Печать**  на панели инструментов.

Просмотр письма и вложений в отдельном окне

Чтобы просмотреть письмо в отдельном окне:

1. На панели писем дважды щелкните нужное письмо либо выберите письмо и нажмите клавишу **Enter**. Откроется окно просмотра письма (см. «Окно создания и просмотра писем» на стр. 44). Текст письма отобразится на нижней панели окна. При этом непрочитанное письмо станет прочитанным.

   Если открыто исходящее письмо, которое еще не отправлено и не подписано электронной подписью, его можно редактировать (см. «Создание письма» на стр. 45).

   Примечание. Чтобы редактировать неотправленное письмо, подписанное электронной подписью, удалите электронную подпись (см. «Удаление электронной подписи письма» на стр. 80).

2. Для поиска по тексту письма выполните следующие действия:
   - В меню **Редактирование** выберите пункт **Найти** либо нажмите сочетание клавиш **Ctrl+F**.
   - В окне **Поиск** введите строку для поиска.
   - Если необходимо, задайте параметры и направление поиска.
   - Нажмите кнопку **Найти далее** клавишу **Enter**.
3. Список получателей письма можно посмотреть на вкладке **Получатели** (открывается по умолчанию).
   - Если слева от имени получателя отображается значок , для этого пользователя отправителем добавлена аннотация. Для просмотра аннотации дважды щелкните имя получателя.
   - Чтобы посмотреть подробную информацию о получателе, щелкните его правой кнопкой мыши и в контекстном меню выберите пункт **Свойства.**
4. Чтобы просмотреть вложения письма, откройте вкладку **Вложения**. С вложениями можно выполнить следующие действия:

- Чтобы открыть вложение, дважды щелкните его либо выделите и нажмите клавишу **Enter**. В окне предупреждения о просмотре вложения нажмите **OK**, вложение будет открыто в отдельном окне.
- Если письмо не отправлено и вложение не подписано электронной подписью, вложение можно редактировать. Для этого щелкните вложение правой кнопкой мыши и в контекстном меню выберите пункт **Редактировать**. Вложение будет открыто в программе по умолчанию.

Примечание. Изменения, внесенные в открытое вложение отправленного или полученного письма, невозможно сохранить.

- Чтобы скопировать вложение для вставки в другое письмо программы ViPNet Деловая почта, щелкните вложение правой кнопкой мыши и в контекстном меню выберите пункт **Копировать файл.**

  Чтобы вставить в письмо вложение, скопированное из другого письма, щелкните правой кнопкой мыши на вкладке **Вложения** и в контекстном меню выберите пункт **Вставить файл.**
- Чтобы посмотреть свойства вложения, щелкните его правой кнопкой мыши и в контекстном меню выберите пункт **Свойства.**
- Чтобы сохранить вложение, выполните одно из действий:
  - Щелкните вложение правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить в файл**. В окне **Сохранить как** укажите папку и имя файла для сохранения вложения.
  - Чтобы сохранить все вложения письма, щелкните на вкладке **Вложения** правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить все вложения**. В окне **Обзор папок** укажите папку для сохранения вложений.
  - Щелкните вложение и перетащите в папку, в которой его требуется сохранить.
- Чтобы распечатать вложение, щелкните его правой кнопкой мыши и в контекстном меню выберите пункт **Печать.**

5 Чтобы распечатать текст письма, нажмите кнопку **Печать** на панели инструментов.

Ответ на письмо и пересылка письма

Чтобы ответить на письмо или переслать письмо, выполните следующие действия:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) на левой панели выберите папку, в которой находится нужное письмо.
2. Выберите письмо на панели писем либо откройте его в отдельном окне (см. «Окно создания и просмотра писем» на стр. 44).
3. Чтобы ответить отправителю, выполните одно из действий:
   - На панели писем щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Ответить автору** или **Ответить автору с вложениями** (этот пункт доступен, если письмо содержит вложения).
   - На панели инструментов главного окна программы ViPNet Деловая почта или на панели инструментов окна просмотра писем нажмите кнопку **Ответить**  , затем в меню выберите пункт **Ответить** или **Ответить автору с вложениями** (этот пункт доступен, если письмо содержит вложения).

   Откроется окно создания письма. В теме нового письма будет указана тема исходного письма с префиксом «Re:». В качестве получателя будет указан отправитель исходного письма. В тексте нового письма будут указаны основные свойства и текст исходного письма. В случае ответа с вложениями в новое письмо будут добавлены вложения исходного письма.
4. Чтобы ответить отправителю и всем получателям исходного письма, выполните одно из действий:
   - На панели писем щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Ответить всем** или **Ответить всем с вложениями** (этот пункт доступен, если письмо содержит вложения).
   - На панели инструментов главного окна программы ViPNet Деловая почта или на панели инструментов окна просмотра писем нажмите кнопку **Отв. всем**  , затем в меню выберите пункт **Ответить всем** или **Ответить всем с вложениями** (этот пункт доступен, если письмо содержит вложения).

     Откроется окно создания письма. В теме нового письма будет указана тема исходного письма с префиксом «Re:». В качестве получателей будут указаны отправитель исходного письма и его получатели (за исключением пользователей данного сетевого узла). В тексте нового письма будут указаны основные свойства и текст исходного письма. В случае ответа с вложениями в новое письмо будут добавлены вложения исходного письма.

Примечание. После ответа на письмо текст письма считается прочитанным.

5 Чтобы переслать письмо, выполните одно из действий:

- На панели писем щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Переслать**.
- На панели инструментов главного окна программы ViPNet Деловая почта или на панели инструментов окна просмотра писем нажмите кнопку **Переслать**  .

  Откроется окно создания письма. В теме нового письма будет указана тема исходного письма с префиксом «Fw:». В тексте нового письма будут указаны основные свойства и текст исходного письма. Если в исходном письме содержались вложения, они будут добавлены в новое письмо.

Примечание. После пересылки письма текст письма и все вложения считаются прочитанными.

6 Завершите создание письма и отправьте его, как описано в разделе Создание письма (на стр. 45).

Поиск писем

Для поиска писем в программе ViPNet Деловая почта выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Инструменты** выберите пункт **Поиск документа**. Откроется окно **Поиск документа**.

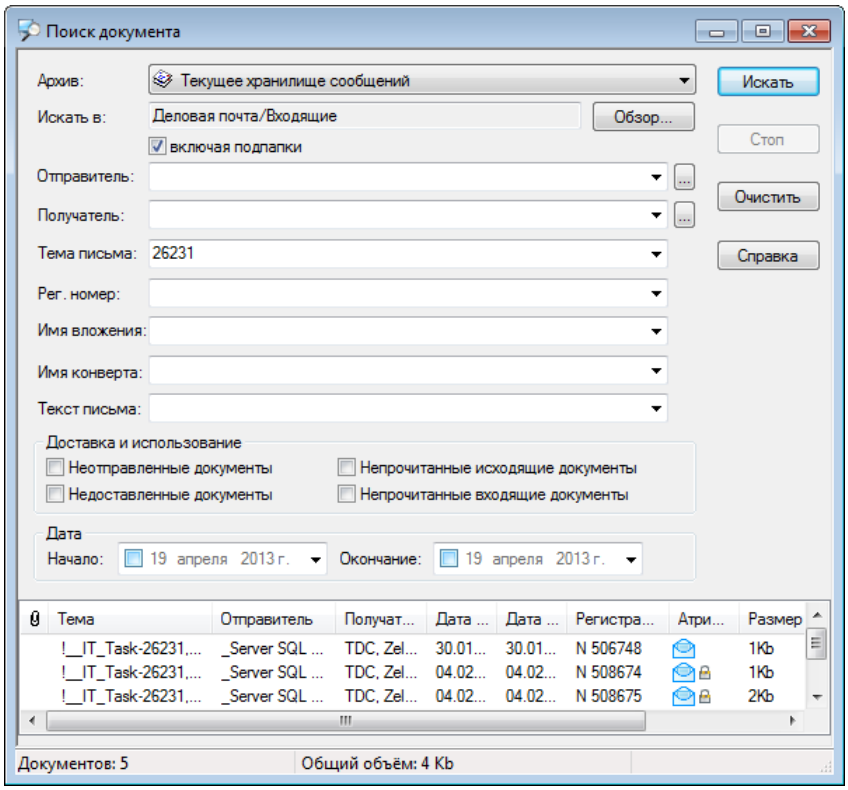


Рисунок 13: Окно поиска писем

2 Из списка **Архив** выберите хранилище сообщений или архив, в котором требуется найти письма.

3 Нажмите кнопку **Обзор** рядом с полем **Искать в** и в окне **Укажите папку** выберите папку, в которой требуется найти письма.

4 Для поиска писем в выбранной папке и ее подпапках установите флажок **включая подпапки**.

5 Чтобы указать отправителя писем, которые требуется найти, нажмите кнопку  рядом с полем **Отправитель** и в адресной книге (см. «Адресная книга» на стр. 40) выберите нужного отправителя.

6 Чтобы указать получателя писем, которые требуется найти, нажмите кнопку  рядом с полем **Получатель** и в адресной книге (см. «Адресная книга» на стр. 40) выберите нужного получателя.

7 Для поиска писем, в теме которых содержится определенная строка, введите эту строку в поле **Тема письма**.

8 Для поиска писем по регистрационному номеру в поле **Рег. номер** введите номер или постоянную часть регистрационного номера.

9 Для поиска писем, содержащих вложения с определенными именами, в поле **Имя вложения** введите часть имени вложения.

10 Для поиска писем по именам транспортных конвертов (см. «Транспортный конверт» на стр. 211) в поле **Имя конверта** введите часть имени конверта.

11 Для поиска писем, в тексте которых содержится определенная строка, введите эту строку в поле **Текст**.

12 Для поиска писем по статусу доставки и прочтения, в группе **Доставка и использование** установите нужные флажки:

- **Неотправленные документы**.
- **Недоставленные документы**.
- **Непрочитанные исходящие документы**.
- **Непрочитанные входящие документы**.

13 Для поиска писем в определенном интервале дат выполните следующие действия:

- Чтобы указать начало интервала, установите флажок в поле **Начало**, затем нажмите кнопку  в правой части поля и выберите дату с помощью календаря.
- Чтобы указать конец интервала, установите флажок в поле **Окончание**, затем нажмите кнопку  в правой части поля и выберите дату с помощью календаря.

14 Если требуется сбросить параметры поиска, нажмите кнопку **Очистить**.

15 Чтобы начать поиск писем с заданными параметрами, нажмите кнопку **Искать**.

Чтобы остановить процесс поиска, нажмите кнопку **Стоп**.

В результате поиска письма, соответствующие заданным параметрам, будут отображены на нижней панели окна **Поиск документа**. В списке найденных писем доступны следующие действия:

- С помощью контекстного меню письма можно выполнить основные действия с письмами: зашифровать, расшифровать, подписать, проверить подпись и так далее.
- Чтобы просмотреть найденное письмо, откройте его двойным щелчком.
- Чтобы перейти в папку, в которой находится найденное письмо, в контекстном меню письма выберите пункт **Перейти в основное окно**.

Экспорт и импорт писем

Экспорт писем

Письма программы ViPNet Деловая почта можно экспортировать в формат BML. При экспорте вместе с письмами сохраняется атрибут электронной подписи и время последней успешной проверки электронной подписи. Если письма зашифрованы, при экспорте они автоматически расшифровываются.

Чтобы сохранить письма программы ViPNet Деловая почта в файле `*.bml`, выполните следующие действия:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) на левой панели выберите папку с письмами, которые требуется экспортировать.
2. На панели писем выберите одно или несколько писем.
3. Щелкните выбранные письма правой кнопкой мыши и в контекстном меню выберите один из пунктов:
   - **Сохранить как.** Выбрав данный пункт, для каждого из писем в окне **Сохранить как** укажите папку и имя файла для сохранения и нажмите кнопку **OK**.
   - **Сохранить в**. Выбрав данный пункт, в окне **Обзор папок** укажите папку, в которой будут сохранены выбранные письма, и нажмите кнопку **OK**. Имя каждого файла будет автоматически сформировано из темы письма и его регистрационного номера.

   Письма будут сохранены в виде файлов `*.bml` в указанных папках.

Чтобы перенести письмо из программы ViPNet Деловая почта в Microsoft Outlook или Outlook Express (Windows Mail), выполните одно из следующих действий:

- Перетащите письмо из окна программы ViPNet Деловая почта в окно создания сообщения Microsoft Outlook или Outlook Express. Письмо будет добавлено в сообщение в виде вложения.
- Перетащите письмо из окна программы ViPNet Деловая почта в какую-либо папку в окне программы Microsoft Outlook или Outlook Express. В выбранной папке появится новое сообщение, в которое будет вложено письмо программы ViPNet Деловая почта.

Примечание. Если в выбранной папке отсутствует доступ на создание сообщений, будет открыто окно создания нового сообщения, в которое будет вложено письмо программы ViPNet Деловая почта.

- Вложите в сообщение Microsoft Outlook или Outlook Express письмо программы ViPNet Деловая почта, экспортированное в файл `*.bml`.

Импорт писем

В программу ViPNet Деловая почта можно импортировать письма из файлов формата `*.bml`, `*.msg` или `*.eml`. Чтобы импортировать письмо, выполните одно из действий:

- В программе ViPNet Деловая почта в меню **Инструменты** выберите пункт **Импорт документа**. В окне **Открыть** укажите один или несколько файлов для импорта и нажмите кнопку **Открыть**.
- Перетащите файлы, которые требуется импортировать, в окно программы ViPNet Деловая почта в папку **Импорт**.

  Импортированные письма появятся в папке **Импорт**.

Чтобы перенести в программу ViPNet Деловая почта сообщения Microsoft Outlook или Outlook Express (Windows Mail):

1. Выполните одно из действий:
   - Перетащите одно или несколько сообщений из окна программы Microsoft Outlook или Outlook Express в одну из папок на панели папок программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33).

     Откроется окно создания нового письма. Одновременно для каждого сообщения откроется окно **Введите имя вложения**.
   - Чтобы добавить все сообщения в виде вложенных файлов, сохранив их имена, нажмите кнопку **Добавить все**. Чтобы изменить имена вложенных файлов, для каждого сообщения введите имя и нажмите кнопку **Добавить**.

   Сообщения будут добавлены в новое письмо в виде вложения.
2. Завершите создание письма (см. «Создание письма» на стр. 45).

Перенос писем в другую папку программы

Перенести письма в другую папку программы ViPNet Деловая почта можно двумя способами:

- На панели писем выберите одно или несколько писем и перетащите их в папку назначения.
- Выполните следующие действия:
  - Выберите одно или несколько писем.
  - Щелкните выбранные письма правой кнопкой мыши и в контекстном меню выберите пункт **Переместить в папку**.
  - В окне **Укажите папку** выберите папку, в которую следует переместить письма, и нажмите **OK**.

При переносе писем действуют следующие ограничения:

- Нельзя переносить письма из папок **Входящие** и **Удаленные > Входящие** в папки **Исходящие** и **Удаленные > Исходящие**.
- Нельзя переносить письма из папки **Исходящие** в папку **Удаленные > Входящие**.
- В папку **Входящие** можно переносить письма только из папки **Удаленные > Входящие** и наоборот.
- Нельзя переносить письма в папку **Аудит** или из нее.
- Нельзя переносить письма между двумя подпапками папки **Удаленные** или папки **Аудит**.

Удаление писем

Чтобы удалить письма из любой папки, кроме папок **Аудит**, **Удаленные** и их подпапок, выполните следующие действия:

1. На панели писем выберите одно или несколько писем.
2. Выполните одно из действий:
   - Нажмите клавишу **Delete**.
   - Нажмите кнопку **Удалить** на панели инструментов.
   - Перетащите письма в папку **Удаленные**.

   Выбранные письма будут перемещены в папку **Удаленные**. При этом в папке **Удаленные** будет автоматически создана структура папок, полностью повторяющая структуру, в которой находилось удаленное письмо. Например, при удалении письма из папки **Входящие > Папка** оно будет перемещено в папку **Удаленные > Входящие > Папка**.

Примечание. Если перетащить письма в какую-либо подпапку папки **Удаленные**, письма будут перемещены именно в эту подпапку. При этом дополнительные папки создаваться не будут. Перетаскивание писем в некоторые папки может быть запрещено (см. «Перенос писем в другую папку программы» на стр. 64).

Чтобы удалить письма из папки **Удаленные**:

1. Выберите одно или несколько писем.
2. Нажмите клавишу **Delete** или кнопку **Удалить**.

   В папке **Аудит** будет создана копия структуры папок из папки **Удаленные**, содержащая запись о времени удаления письма и имени пользователя, осуществившего удаление. Удалить эту запись из папки **Аудит** может только администратор сетевого узла (см. «Работа в программе с правами администратора» на стр. 120).

Примечание. При работе в режиме администратора в контекстном меню письма доступен пункт **Полное удаление** (см. «Дополнительные настройки и возможности программы» на стр. 121).

Архивация писем

Под архивацией понимается перемещение определенных категорий писем из рабочего хранилища программы ViPNet Деловая почта в заданную папку на диске. Архивация позволяет уменьшить объем рабочего хранилища и ускорить работу с письмами.

При архивации письма помещаются в архив, который представляет собой папку, имя которой формируется на основе даты и времени создания архива, например `MS_21092010_163539`. По умолчанию архив создается в папке `\ViPNet Client\MSArch`. Папку для хранения архивов можно изменить (см. «Работа с архивами писем» на стр. 68).

Вместе с письмами в архив помещаются вложения, при этом в программе предусмотрены два способа размещения вложений в архиве:

- Перенос вложений из файлов в базу данных для размещения в архиве вместе с письмами.

  При таком способе архив будет содержать один файл. Этот способ позволяет упростить копирование или перенос архива на внешний носитель, например, с целью резервирования.

- Размещение вложений в папках отдельно от писем.

  При таком способе архив будет содержать файл с базой данных писем и набор папок, в которых размещены отдельные файлы вложений.

Письма, помещенные в архив, удаляются из рабочего хранилища программы ViPNet Деловая почта и не отображаются в окне программы, однако их можно просматривать, открыв соответствующий архив (см. «Работа с архивами писем» на стр. 68).

Архивация писем может осуществляться вручную либо автоматически. Автоматическая архивация запускается при выполнении определенных условий. Категории писем, подлежащие архивации, способ размещения вложений в архиве, а также параметры автоматической архивации можно задать в окне **Настройка** в разделе **Архивация** (см. «Настройка архивации писем» на стр. 109).

Для архивации писем выполните следующие действия:

1. В зависимости от режима архивации:
   - Для запуска архивации вручную в окне программы ViPNet Деловая почта в меню **Файл** выберите пункт **Архивировать почту**.

- Автоматическая архивация запускается в соответствии с заданными параметрами (см. «Общие параметры архивации» на стр. 109).

2 Перед началом архивации появится окно для подтверждения архивации. Если в параметрах архивации (см. «Общие параметры архивации» на стр. 109) настроена архивация не всех писем, а только некоторых их категорий, будет выведено предупреждение о том, что архивация может занять продолжительное время.

   Чтобы начать архивацию, в окне подтверждения нажмите кнопку **Да**.

3 Если в момент начала архивации открыты какие-либо письма, программа выдаст сообщение о том, что все письма необходимо закрыть.

   Чтобы отменить архивацию, в окне сообщения нажмите кнопку **Нет**. Чтобы продолжить, нажмите кнопку **Да**, при этом все открытые письма будут автоматически закрыты.

4 Начнется процесс архивации, который можно наблюдать с помощью индикатора выполнения.

   Все подлежащие архивации письма будут перемещены из рабочего хранилища писем в архив.

Работа с архивами писем

Программа ViPNet Деловая почта позволяет просматривать архивы собственных писем или писем других пользователей (если они не зашифрованы), а также перемещать, удалять и переименовывать архивы.

Чтобы просмотреть какой-либо архив писем программы ViPNet Деловая почта, выполните следующие действия:

1 В окне программы ViPNet Деловая почта в меню **Файл** выберите пункт **Выбрать архив**. Откроется окно **Архивы**.

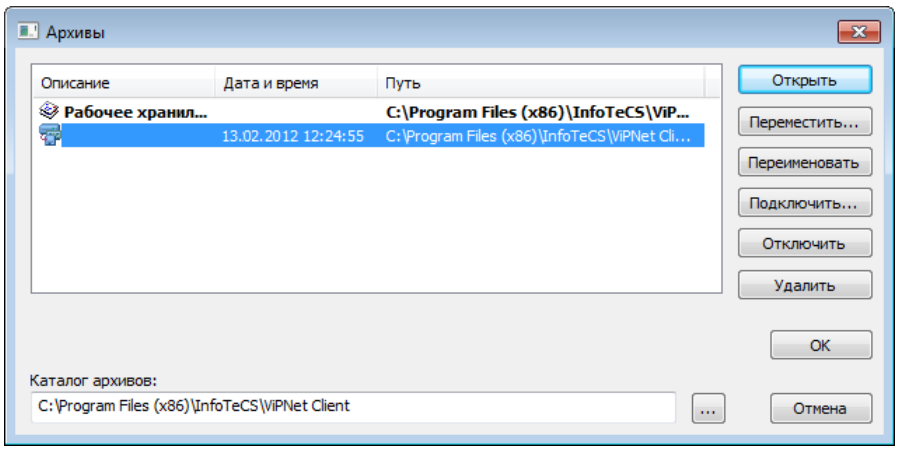


Рисунок 14: Окно управления архивами

2 В списке выберите архив, который требуется просмотреть.

3 Нажмите кнопку **Открыть**.

Письма, содержащиеся в выбранном архиве, будут отображены в окне программы ViPNet Деловая почта. Эти письма будут доступны только для чтения. Однако при необходимости письма могут быть зашифрованы (расшифрованы) с помощью пункта **Зашифровать** (**Расшифровать**) контекстного меню.

Примечание. Зашифровать письмо, которое содержится в архиве, можно только в случае, если архив доступен для записи.

Во время работы с архивом писем рабочее хранилище программы ViPNet Деловая почта будет недоступно, то есть невозможно будет отправлять и принимать письма.

Чтобы вернуться к работе с основным хранилищем писем:

1. В меню **Файл** выберите пункт **Выбрать архив**. Откроется окно **Архивы**.
2. В окне **Архивы** в списке выберите **Рабочее хранилище сообщений**.
3. Нажмите кнопку **Открыть**.

   В окне программы ViPNet Деловая почта откроется рабочее хранилище, в котором возможна полноценная работа с защищенной почтой.

Чтобы просмотреть архив писем, созданный на другом компьютере (например, архив пользователя другого сетевого узла, переданный на съемном носителе), выполните следующие действия:

1. В меню **Файл** выберите пункт **Выбрать архив**. Откроется окно **Архивы**.
2. Нажмите кнопку **Подключить**. Откроется окно **Обзор папок**.
3. В окне **Обзор папок** укажите папку, содержащую архив писем, и нажмите **OK**.

   Указанный архив будет добавлен в список в окне **Архивы**.
4. Выберите архив в списке и нажмите кнопку **Открыть**.

   Письма, содержащиеся в архиве, будут отображены в окне программы ViPNet Деловая почта. Эти письма будут доступны только для чтения. Если в архиве присутствуют письма, зашифрованные на ключах другого коллектива (см. «Коллектив» на стр. 207), они будут недоступны для просмотра.

Также в окне **Архивы** можно выполнить следующие действия:

- Чтобы задать папку для рабочего хранилища сообщений и новых архивов писем:
  - Нажмите кнопку  рядом с полем **Каталог архивов**.
  - В окне **Обзор папок** укажите папку для рабочего хранилища сообщений и архивов писем, затем нажмите кнопку **OK**.

  При следующем запуске программы ViPNet Деловая почта в указанной папке будет создана подпапка `\MSArch`, в которую будут помещаться рабочее хранилище сообщений и создаваемые архивы писем.
- Чтобы переместить архив в другую папку:
  - Выберите архив и нажмите кнопку **Переместить**.

- В окне **Обзор папок** укажите папку, в которую требуется переместить архив, и нажмите кнопку **OK**. Архив будет перемещен в указанную папку.

- Чтобы переименовать архив:
  - Выберите архив и нажмите кнопку **Переименовать**. На месте имени архива в списке появится текстовое поле.
  - Введите новое имя и нажмите клавишу **Enter**.

- Чтобы удалить архив из списка, в окне **Архивы** выберите архив и нажмите кнопку **Отключить**. Архив будет удален из списка, но сохранится на диске.

- Чтобы удалить архив с диска:
  - Выберите архив, который требуется удалить.
  - Нажмите кнопку **Удалить**, в окне подтверждения нажмите **OK**.

4

Электронная подпись и шифрование

Электронная подпись в программе ViPNet Деловая почта

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

Электронная подпись позволяет:

- Подтвердить подлинность документа. Электронная подпись удостоверяет личность поставившего подпись.
- Подтвердить целостность документа. Электронная подпись подтверждает, что документ не изменялся после подписания.
- Обеспечить неотрекаемость. Электронная подпись предотвращает отказ субъектов от авторства документа.

С помощью программы ViPNet Деловая почта можно подписать электронной подписью текст письма и его вложения (см. «Работа с электронной подписью писем» на стр. 73) или отдельные файлы (см. «Работа с электронной подписью файлов» на стр. 81). Также можно проверить и удалить электронную подпись письма или файла.

Для подписания писем и файлов можно использовать следующие типы сертификатов (см. «Сертификат открытого ключа подписи пользователя» на стр. 210):

- Сертификат электронной подписи текущего пользователя клиента.
- Сертификат пользователя другого сетевого узла или сертификат внешнего пользователя сети ViPNet (см. «Подписание выбранным сертификатом» на стр. 75), находящийся во внешнем контейнере ключей (см. «Контейнер ключей» на стр. 207). Контейнер может храниться на диске или на внешнем устройстве (см. «Внешние устройства» на стр. 199).
- Сертификат электронной подписи, изданный сторонним удостоверяющим центром (см. «Использование сертификата, изданного сторонним удостоверяющим центром» на стр. 77).

Работа с электронной подписью писем

Подписание письма

По умолчанию в программе ViPNet Деловая почта настроено автоматическое подписание писем и вложений текущим сертификатом при отправке. Эти настройки можно изменить в разделе **Письмо** (см. «Настройка параметров работы с письмами» на стр. 113).

Чтобы подписать одно или несколько писем электронной подписью, выполните следующие действия:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в папке **Исходящие** или какой-либо ее подпапке выберите одно или несколько неотправленных писем, которые требуется подписать.
2. Выполните одно из действий:
   - Нажмите кнопку **Подписать** на панели инструментов, затем в меню выберите:
     - **Текущим сертификатом**, чтобы подписать письма сертификатом электронной подписи текущего пользователя.
     - **Выбранным сертификатом**, чтобы подписать письма сертификатом из определенного контейнера ключей.
   - Щелкните выбранные письма правой кнопкой мыши и в контекстном меню выберите пункт **Подписать**, затем щелкните **Текущим сертификатом** или **Выбранным сертификатом**.
3. Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе Подписание выбранным сертификатом (на стр. 75).

   Письма будут подписаны электронной подписью, им будет присвоен атрибут подписи. Если письма содержат вложения, вложения также будут подписаны.

Чтобы подписать электронной подписью письмо, открытое в окне создания и просмотра писем (см. «Окно создания и просмотра писем» на стр. 44), выполните следующие действия:

1. Создайте новое письмо (см. «Создание письма» на стр. 45) либо откройте неотправленное письмо в отдельном окне.
2. Выполните одно из действий:
   - Нажмите кнопку **Подписать** на панели инструментов, затем в меню выберите:
     - **Текущим сертификатом**, чтобы подписать письма сертификатом электронной подписи текущего пользователя.
     - **Выбранным сертификатом**, чтобы подписать письмо сертификатом из определенного контейнера ключей.
   - В меню **Подпись** выберите пункт **Подписать все письмо**, затем выберите **Текущим сертификатом** или **Выбранным сертификатом**.
3. Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе Подписание выбранным сертификатом (на стр. 75).

   Письмо и его вложения будут подписаны электронной подписью.

Чтобы подписать электронной подписью только текст письма, выполните следующие действия:

1. Создайте новое письмо (см. «Создание письма» на стр. 45) либо откройте неотправленное письмо в отдельном окне.
2. Выполните одно из действий:
   - В меню **Подпись** выберите пункт **Подписать текст письма**, затем выберите **Текущим сертификатом** или **Выбранным сертификатом**.
   - Щелкните текст письма правой кнопкой мыши, в контекстном меню выберите пункт **Подписать текст письма**, затем выберите **Текущим сертификатом** или **Выбранным сертификатом**.
3. Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе Подписание выбранным сертификатом (на стр. 75).

   Текст письма будет подписан электронной подписью.

Чтобы подписать электронной подписью только вложения письма:

1. Создайте новое письмо (см. «Создание письма» на стр. 45) либо откройте неотправленное письмо в отдельном окне.
2. Добавьте в письмо одно или несколько вложений.
3. На вкладке **Вложения** выберите одно или несколько вложений.
4. Щелкните выбранные вложения правой кнопкой мыши и в контекстном меню выберите пункт **Подписать**, затем щелкните **Текущим сертификатом** или **Выбранным сертификатом**.
5. Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе Подписание выбранным сертификатом (на стр. 75).

   Выбранные вложения будут подписаны электронной подписью.

Подписание выбранным сертификатом

Если при подписании электронной подписью письма или файла выбран пункт **Выбранным сертификатом**, откроется окно **ViPNet CSP - инициализация контейнера ключа**.

Если контейнер хранится на диске, для выбора сертификата выполните следующие действия:

1. В окне **ViPNet CSP - инициализация контейнера ключа** выберите пункт **Папка на диске**.

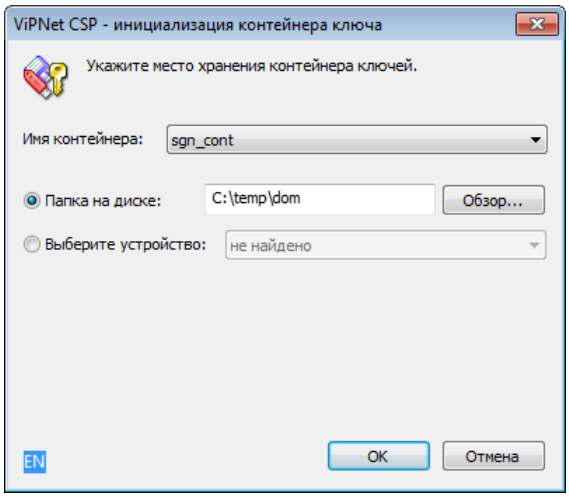


Рисунок 15: Контейнер хранится на диске

2. Нажмите кнопку **Обзор** и укажите путь к папке, в которой хранится контейнер.

3 Если в папке хранится несколько контейнеров, в списке **Имя контейнера** выберите нужный контейнер.

4 Нажмите кнопку **OK**.

5 Если в контейнере хранится несколько сертификатов, откроется окно **Выбор сертификата**. Выберите сертификат и нажмите **OK**.

6 В окне **ViPNet CSP - пароль контейнера ключа** введите пароль доступа к контейнеру и нажмите **OK**.

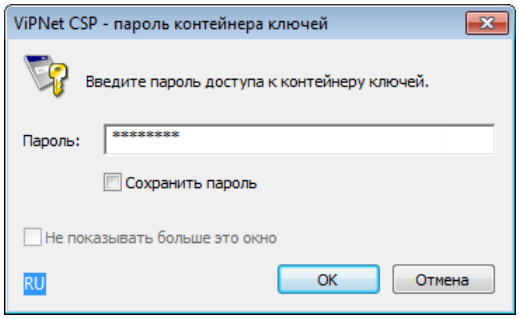


Рисунок 16: Ввод пароля доступа к контейнеру ключей

Письмо (или файл) будет подписано выбранным сертификатом электронной подписи.

Если контейнер ключей хранится на внешнем устройстве (см. «Внешние устройства» на стр. 199), выполните следующие действия:

1 В окне **ViPNet CSP - инициализация контейнера ключа** выберите пункт **Устройство**.

2 Подключите устройство, на котором хранится контейнер. Если подключено несколько устройств, в списке **Выберите устройство** укажите нужное устройство.

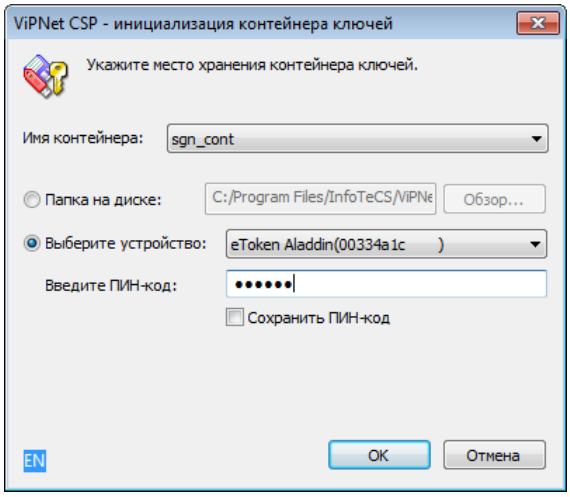


Рисунок 17: Контейнер хранится на внешнем устройстве

3 Если на устройстве хранится несколько контейнеров, в списке **Имя контейнера** выберите нужный контейнер.

4 В поле **Введите ПИН-код** укажите ПИН-код устройства и нажмите **OK**.

Письмо (или файл) будет подписано выбранным сертификатом электронной подписи.

Использование сертификата, изданного сторонним удостоверяющим центром

Письма и файлы в программе ViPNet Деловая почта можно подписывать сертификатами, изданными сторонними удостоверяющими центрами (не являющимися частью своей сети ViPNet).

Чтобы использовать такой сертификат, выполните следующие действия:

1 Если сертификат и соответствующий ему закрытый ключ созданы с помощью криптопровайдера стороннего производителя (не входящего в состав ПО ViPNet):

- В настройках параметров безопасности отключите криптопровайдер ViPNet CSP.
- Установите на компьютер криптопровайдер, необходимый для работы с внешним сертификатом.

2 Импортируйте сертификат и соответствующий закрытый ключ в системное хранилище сертификатов пользователя с помощью оснастки «Сертификаты — текущий пользователь» (certmgr.msc).

Чтобы получить подробную информацию об импорте сертификатов, обратитесь к справке Windows.

3 В окне **Настройка параметров безопасности** убедитесь, что на вкладке **Администратор** установлен флажок **Разрешить использование внешних сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 122).

Примечание. Изменять настройки на вкладке **Администратор** может только администратор сетевого узла (см. «Работа в программе с правами администратора» на стр. 120).

4 На вкладке **Подпись** выберите нужный сертификат в качестве текущего (см. «Смена текущего сертификата» на стр. 162).

5 При подписании писем (см. «Подписание письма» на стр. 73) и файлов (см. «Подписание файла» на стр. 81) в меню выбирайте пункт **Текущим сертификатом.**

Проверка электронной подписи письма

Чтобы проверить электронную подпись письма, выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) на панели писем выберите подписанное письмо (со значком статуса или), для которого требуется проверить электронную подпись.

2 Выполните одно из действий:

- Нажмите кнопку **Проверить** на панели инструментов.
- Щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Проверить подпись.**

Откроется окно **Проверка электронной подписи**.

Чтобы проверить электронную подпись вложения в окне просмотра письма (см. «Окно создания и просмотра писем» на стр. 44):

1 Откройте письмо, содержащее подписанное вложение, в отдельном окне.

2 На вкладке **Вложения** щелкните нужное вложение правой кнопкой мыши и в контекстном меню выберите пункт **Проверить подпись.**

Откроется окно **Проверка электронной подписи**.

В окне **Проверка электронной подписи** содержится информация об электронных подписях каждого элемента письма (текст и вложения). Действительные подписи помечены зеленым значком, недействительные — красным значком.

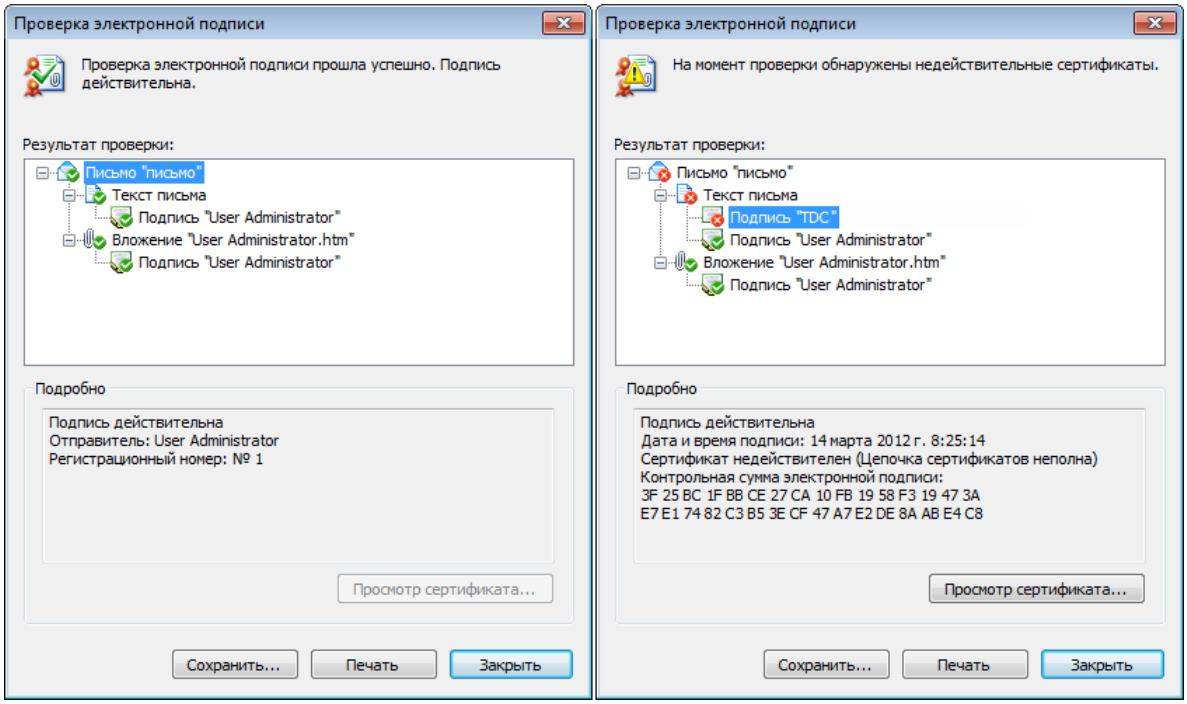


Рисунок 18: Результат проверки электронной подписи

В окне **Проверка электронной подписи** доступны следующие действия:

- Чтобы просмотреть сведения об электронной подписи какого-либо элемента письма (всего письма, текста, какого-либо вложения или электронной подписи), выберите этот элемент на панели **Результат проверки**. Информация о подписи будет отображена на панели **Подробно**.

- Чтобы просмотреть сертификат, которым подписан элемент письма, выберите на панели **Результат проверки** электронную подпись и нажмите кнопку **Просмотр сертификата**.

Удаление электронной подписи письма

Чтобы удалить электронную подпись одного или нескольких писем, выполните следующие действия:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в папке **Исходящие** или какой-либо ее подпапке выберите одно или несколько неотправленных писем с электронной подписью (они имеют значок статуса  или ).
2. Выполните одно из действий:
   - Нажмите кнопку **Удалить**  на панели инструментов.
   - Щелкните выбранные письма правой кнопкой мыши и в контекстном меню выберите пункт **Удалить подпись.**

   Электронные подписи выбранных писем и их вложений будут удалены.

Чтобы удалить электронную подпись письма, открытого в окне создания и просмотра писем (см. «Окно создания и просмотра писем» на стр. 44):

- Чтобы удалить электронную подпись текста письма и всех вложений, нажмите кнопку **Удалить**  на панели инструментов.
- Чтобы удалить электронную подпись вложения, на вкладке **Вложения** щелкните подписанное вложение правой кнопкой мыши и в контекстном меню выберите пункт **Удалить подпись.**
- Чтобы удалить электронную подпись текста письма (при условии, что текст подписан), щелкните правой кнопкой мыши на панели текста и в контекстном меню выберите пункт **Удалить подпись с текста письма.**

Работа с электронной подписью файлов

Подписание файла

Программа ViPNet Деловая почта позволяет подписать электронной подписью файл, не являющийся вложением письма. К подписанному файлу добавляется расширение `.v7s`. Например, файл `Document.txt` после подписания будет заменен файлом `Document.txt.v7s`.

Подписанный файл с расширением `.v7s` невозможно просмотреть или отредактировать. При попытке открыть такой файл будет выполнена проверка электронной подписи (см. «Проверка электронной подписи файла» на стр. 83). Чтобы была возможность просматривать подписанные файлы, нужно отсоединить их электронные подписи (см. «Отсоединение и присоединение подписи файла» на стр. 82). Если файл с присоединенной или отсоединенной электронной подписью каким-либо образом изменить, электронная подпись станет недействительной.

Чтобы подписать электронной подписью один или несколько файлов, не являющихся вложениями писем, выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Файл** выберите пункт **Подпись файлов**, затем выберите:
   - **Подписать файл текущим сертификатом**, чтобы использовать для подписи текущий сертификат электронной подписи.
   - **Подписать файл выбранным сертификатом**, чтобы использовать для подписи сертификат электронной подписи из внешнего контейнера ключей.
2. Если выбрана подпись внешним сертификатом, выполните действия, описанные в разделе Подписание выбранным сертификатом (на стр. 75).
3. Откроется окно **Открыть**. В этом окне укажите один или несколько файлов, которые требуется подписать электронной подписью, и нажмите кнопку **Открыть.**
4. Если для подписи выбран внешний сертификат, хранящийся в контейнере на диске, в окне **ViPNet CSP - пароль доступа к контейнеру ключа** (см. рисунок на стр. 186) введите пароль.

   Файлы будут подписаны выбранным сертификатом.

Примечание. Один и тот же файл можно подписать несколько раз разными сертификатами электронной подписи.

Если подписать файл, уже имеющий отсоединенную электронную подпись (см. «Отсоединение и присоединение подписи файла» на стр. 82), новая подпись будет присоединена к файлу, а отсоединенная подпись не изменится.

Отсоединение и присоединение подписи файла

При подписании файла одной или несколькими электронными подписями создается файл `*.v7s`, содержащий исходный файл и электронные подписи.

Чтобы отсоединить подписи файла, выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Файл** выберите пункт **Подпись файлов**, затем выберите **Отсоединить подпись файла**.
2. В окне **Открыть** укажите один или несколько файлов с расширением `.v7s`, от которых требуется отсоединить электронные подписи, и нажмите кнопку **Открыть**.

   Электронные подписи будут отсоединены от файлов. Файлы примут свой первоначальный вид, а отсоединенные подписи будут сохранены в файлах с расширением `.p7s`.

   Например, если отсоединить электронную подпись от файла `Document.txt.v7s`, в результате получится два файла: `Document.txt` и `Document.txt.p7s`.

Примечание. Если файл имеет одновременно присоединенную и отсоединенную электронные подписи, присоединенная подпись будет сохранена в файл `*.p7s`, заменив существующий файл отсоединенной подписи.

Чтобы присоединить отсоединенную электронную подпись, выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Файл** выберите пункт **Подпись файлов**, затем выберите **Присоединить подпись файла**.
2. В окне **Открыть** укажите один или несколько файлов, которые имеют отсоединенные подписи, и нажмите кнопку **Открыть**. Например, если файл `Document.txt` имеет отсоединенную электронную подпись `Document.txt.p7s`, для присоединения подписи нужно указать файл `Document.txt`.

К выбранным файлам будут присоединены электронные подписи, в результате эти файлы будут заменены файлами `*.v7s`.

Примечание. Если файл имеет одновременно присоединенную и отсоединенную электронные подписи, то присоединение отсоединенной подписи будет возможно только после удаления присоединенной подписи.

Проверка электронной подписи файла

Для проверки электронной подписи файла выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Файл** выберите пункт **Подпись файлов**, затем выберите **Проверить подпись файла**.
2. В окне **Открыть** выберите один или несколько файлов с присоединенной или отсоединенной электронной подписью (например, файл `Document.txt.v7s` или `Document.txt`, но не файл `Document.txt.p7s`).
3. Нажмите кнопку **Открыть**. Откроется окно **Проверка электронной подписи**.

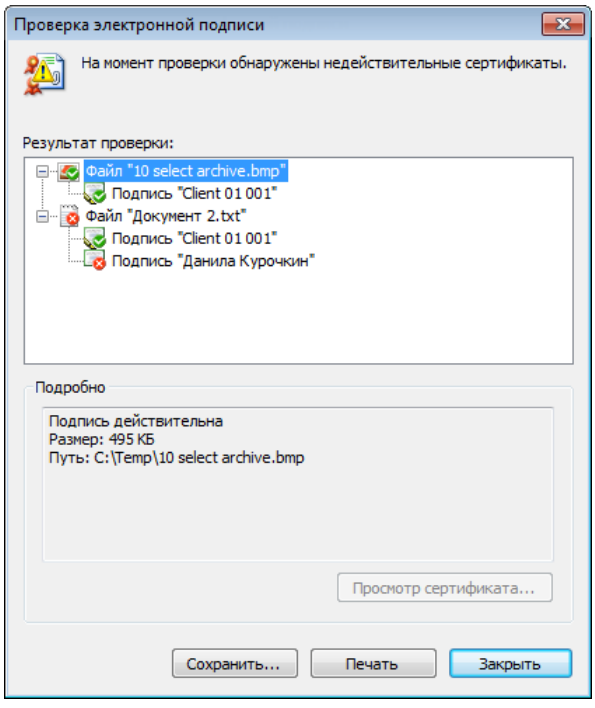


Рисунок 19: Проверка подписей нескольких файлов

В окне **Проверка электронной подписи** перечислены все выбранные файлы и их электронные подписи. Действительные подписи помечены зеленым значком, недействительные — красным значком.

Примечание. Если файл имеет одновременно присоединенную и отсоединенную электронные подписи, отсоединенная подпись не отображается в окне **Проверка электронной подписи**.

В окне **Проверка электронной подписи** доступны следующие действия:

- Чтобы просмотреть сведения о файле или электронной подписи, выберите этот файл или подпись на панели **Результат проверки**. Информация о файле будет отображена на панели **Подробно**.
- Чтобы просмотреть сертификат, которым подписан файл, выберите на панели **Результат проверки** электронную подпись и нажмите кнопку **Просмотр сертификата**.

Удаление электронной подписи файла

Чтобы удалить электронную подпись файла, выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Файл** выберите пункт **Подпись файлов**, затем выберите **Удалить подпись файла**.
2. В окне **Открыть** выберите один или несколько файлов с присоединенной или отсоединенной электронной подписью (например, файл `Document.txt.v7s` или `Document.txt`, но не файл `Document.txt.p7s`).
3. Нажмите кнопку **Открыть**. Электронные подписи выбранных файлов будут удалены.

Примечание. Если файл имеет одновременно присоединенную и отсоединенную электронные подписи, будет удалена только присоединенная подпись.

Шифрование и расшифрование писем

По умолчанию в программе ViPNet Деловая почта настроено автоматическое шифрование писем и вложений при отправке. Эти настройки можно изменить (см. «Настройка параметров работы с письмами» на стр. 113).

Чтобы зашифровать или расшифровать одно или несколько писем, выполните следующие действия:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) на панели писем выберите одно или несколько писем, которые требуется зашифровать или расшифровать.
2. Чтобы зашифровать выбранные письма, выполните одно из действий:
   - Нажмите кнопку **Шифровать** на панели инструментов.
   - Щелкните выбранные письма правой кнопкой мыши и в контекстном меню выберите пункт **Зашифровать.**

   Выбранные письма будут зашифрованы вместе с вложениями.
3. Чтобы расшифровать выбранные письма, выполните одно из действий:
   - Нажмите кнопку **Расшифровать** на панели инструментов.
   - Щелкните выбранные письма правой кнопкой мыши и в контекстном меню выберите пункт **Расшифровать.**

   Выбранные письма будут расшифрованы вместе с вложениями.

Чтобы зашифровать или расшифровать письмо, открытое в окне создания и просмотра писем (см. «Окно создания и просмотра писем» на стр. 44), выполните следующие действия:

1. Создайте новое письмо (см. «Создание письма» на стр. 45) либо откройте неотправленное письмо в отдельном окне.
2. Чтобы зашифровать или расшифровать письмо, нажмите кнопку **Шифровать** на панели инструментов.

   Если письмо зашифровано, кнопка **Шифровать** выглядит следующим образом:
   

   .

Если письмо не зашифровано, кнопка **Шифровать** выглядит так: 

.

5

Автопроцессинг

Принцип работы автопроцессинга

Автопроцессингом называется автоматическая обработка писем и файлов по определенным правилам.

Правила автопроцессинга делятся на две категории:

- Правила обработки исходящих файлов: файлы с определенной маской имени, находящиеся в определенной папке, автоматически отправляются заданным пользователям сети ViPNet.
- Правила обработки входящих писем: входящие письма, соответствующие заданным параметрам, переносятся в заданную папку программы ViPNet Деловая почта или текст письма и вложения копируются в заданную папку на диске. Также возможна отправка квитанции о прочтении письма.

Правила автопроцессинга можно создать в окне **Настройка** в разделе **Автопроцессинг** (см. «Настройка правил автопроцессинга» на стр. 91).

Схема работы автопроцессинга представлена на следующем рисунке:

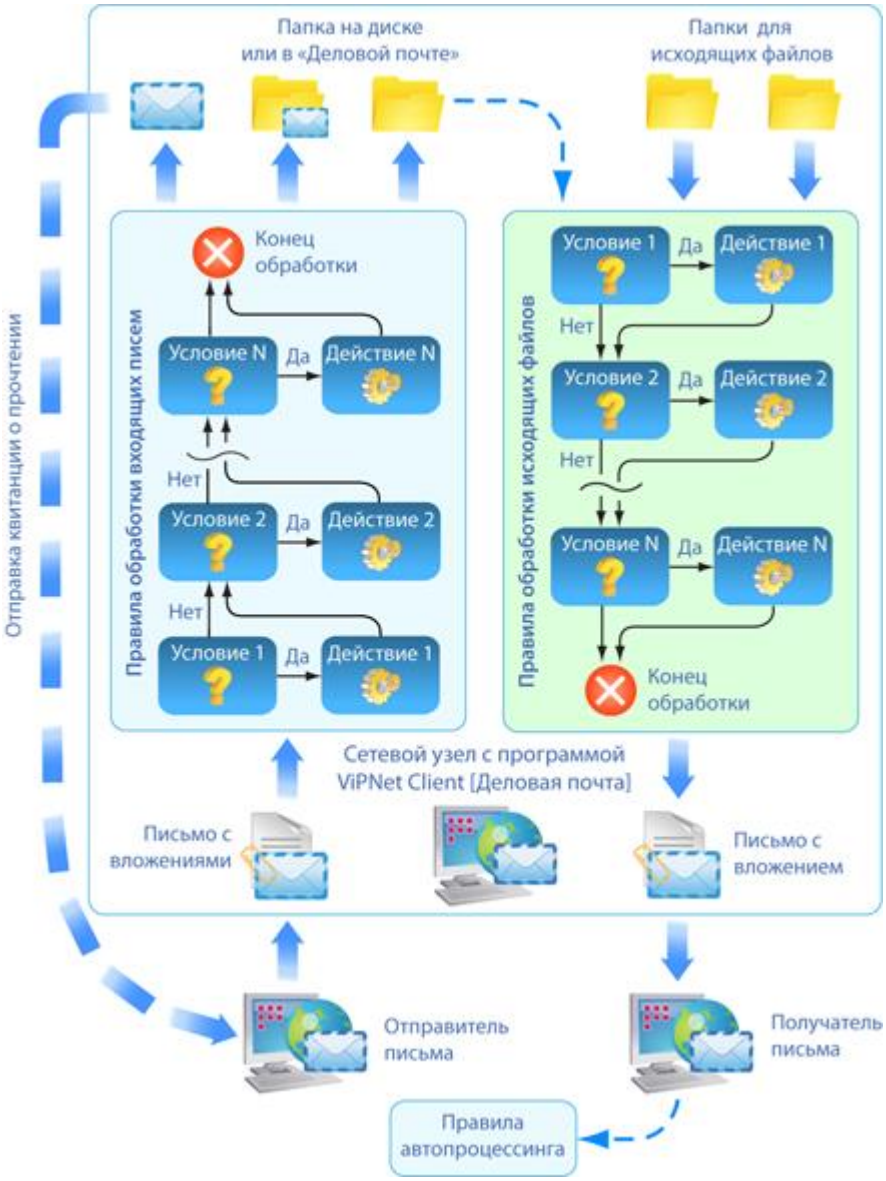


Рисунок 20: Схема работы автопроцессинга

Обработка писем и файлов осуществляется следующим образом:

1. Программа ViPNet Деловая почта принимает новое входящее письмо или в заданную папку для исходящих файлов помещается файл. Папки проверяются на наличие файлов каждые 5 секунд.

2. Начинается обработка письма или файла соответствующими правилами автопроцессинга. Обработка выполняется в порядке расположения правил в списке в разделе **Автопроцессинг**.

3 Каждое правило автопроцессинга состоит из условия и действия. Если письмо или файл удовлетворяет условиям правила:

- Над ним выполняется заданное действие.
- Если в действии правила не задано прекращение дальнейшей обработки, письмо или файл обрабатывается следующим правилом.

4 Обработка письма или файла прекращается после проверки всех правил или если выполняется действие, прекращающее дальнейшую обработку.

Примечание. При попытке обработки файлов, имеющих атрибуты «Только чтение» или «Скрытый», а также системных файлов возникает ошибка автопроцессинга. Программа не отправляет письмо, а предлагает отключить в текущем сеансе работы программы правило, при обработке которого возникла ошибка. Если в окне сообщения нажать кнопку **Да**, данное правило отключается. Если нажать **Нет**, программа больше не будет пытаться отправить данный файл в текущем сеансе работы. При повторной загрузке программы ViPNet Деловая почта правило будет включено, и программа снова попытается отправить файл, вызвавший ошибку.

Настройка правил автопроцессинга

Для настройки правил автопроцессинга выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Инструменты** выберите пункт **Настройка**.

2. В окне **Настройка** на панели навигации выберите раздел **Автопроцессинг**.

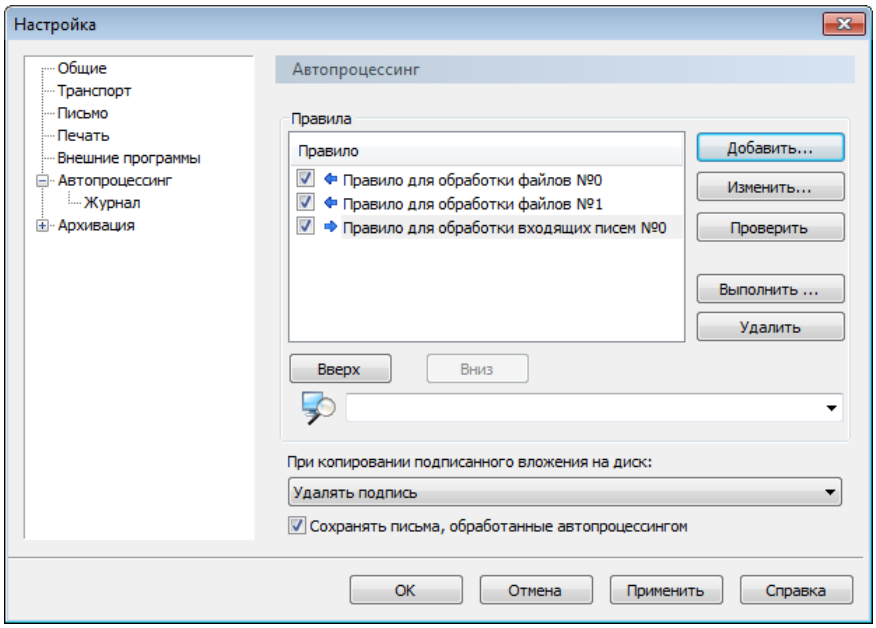


Рисунок 21: Настройка правил автопроцессинга

3. Чтобы настроить правило для обработки файлов, следуйте указаниям раздела Создание правила для исходящих файлов (на стр. 92).

   Чтобы настроить правило для обработки писем, следуйте указаниям раздела Создание правила для входящих писем (на стр. 95).

4. Для поиска правила в списке введите часть имени правила в строку поиска, расположенную под списком.

5. Чтобы выключить или включить правило автопроцессинга, снимите или установите флажок слева от имени правила в списке.

6. Чтобы изменить положение правила в списке, выберите правило и переместите его с помощью кнопок **Вверх** и **Вниз**, расположенных под списком.

Примечание. Обработка писем и файлов правилами автопроцессинга выполняется в порядке расположения правил в списке.

7 Чтобы изменить параметры правила, выберите его в списке и нажмите кнопку **Изменить**. Настройка правил описана в разделах Создание правила для исходящих файлов (на стр. 92) и Создание правила для входящих писем (на стр. 95).

8 Чтобы проверить правильность параметров правила, выберите правило в списке и нажмите кнопку **Проверить.** Программа выдаст сообщение с результатом проверки.

9 Чтобы вручную запустить обработку входящих писем определенным правилом, выберите правило в списке и нажмите кнопку **Выполнить.**

Письма, находящиеся в папке **Входящие**, будут обработаны выбранным правилом. Например, ручной запуск обработки можно использовать, чтобы перенести письма с определенными признаками из папки **Входящие** в другие папки программы ViPNet Деловая почта.

10 Чтобы удалить правило, выберите его в списке и нажмите кнопку **Удалить.**

11 Чтобы указать, как следует поступать с электронной подписью файлов, копируемых на диск, выберите нужный вариант из списка **При копировании подписанного вложения на диск**.

12 Чтобы сохранять письма, обработанные автопроцессингом в папках программы ViPNet Деловая почта или удалять их, установите или снимите соответствующий флажок.

Если данный флажок снят, обработанные письма автоматически удаляются, информация об этих письмах сохраняется в папке **Аудит**.

Создание правила для исходящих файлов

Чтобы создать правило для обработки исходящих файлов, выполните следующие действия:

1 В окне программы ViPNet Деловая почта в меню **Инструменты** выберите пункт **Настройка**.

2 В окне **Настройка** на панели навигации выберите раздел **Автопроцессинг** (см. рисунок на стр. 91).

3 На вкладке **Автопроцессинг** нажмите кнопку **Добавить**, откроется окно **Создание нового правила автопроцессинга**.

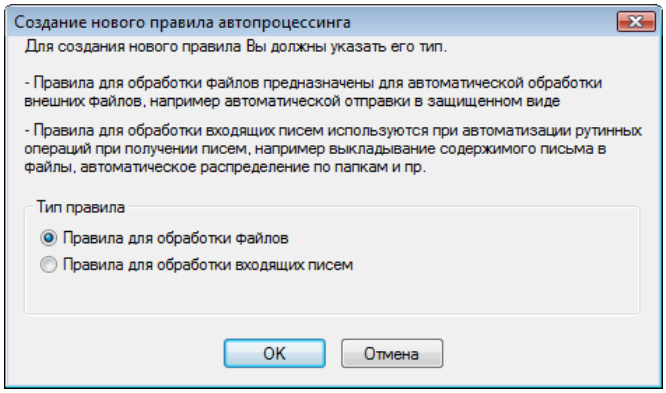


Рисунок 22: Выбор типа правила

4 Выберите тип правила **Правило для обработки файлов** и нажмите кнопку **OK**. Откроется окно **Редактирование правила обработки файлов**.

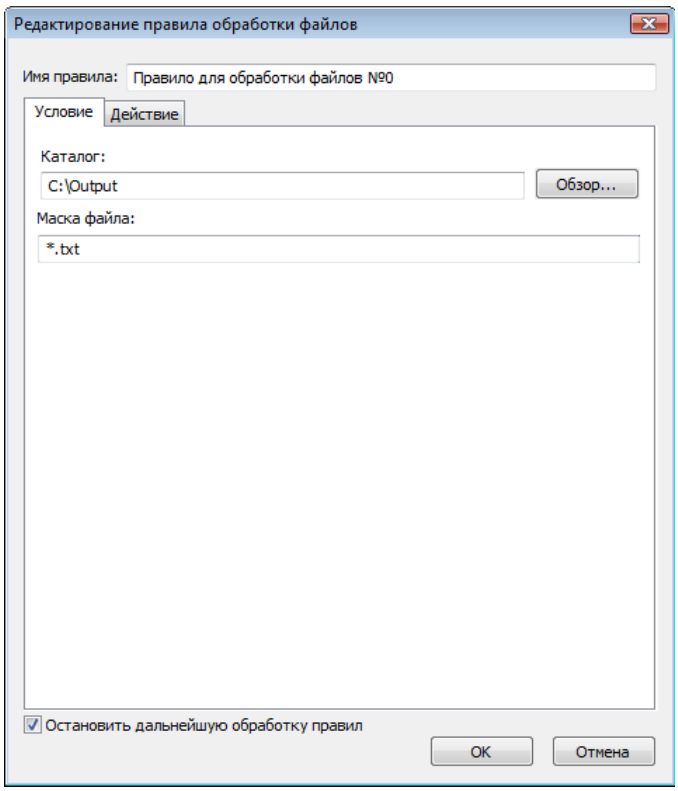


Рисунок 23: Условие для правила обработки исходящих файлов

5 В поле **Имя правила** укажите имя для создаваемого правила.

6 На вкладке **Условие** нажмите кнопку **Обзор** и в окне **Обзор папок** укажите папку, в которую будут помещаться файлы для отправки.

7 В поле **Маска файла** введите маску имени файла, который должен быть обработан создаваемым правилом. Можно задать только одну маску.

При задании маски регистр не учитывается, можно использовать следующие специальные символы:

- * — соответствует любой последовательности символов.
- ? — соответствует любому единичному символу.

8 Откройте вкладку **Действие**.

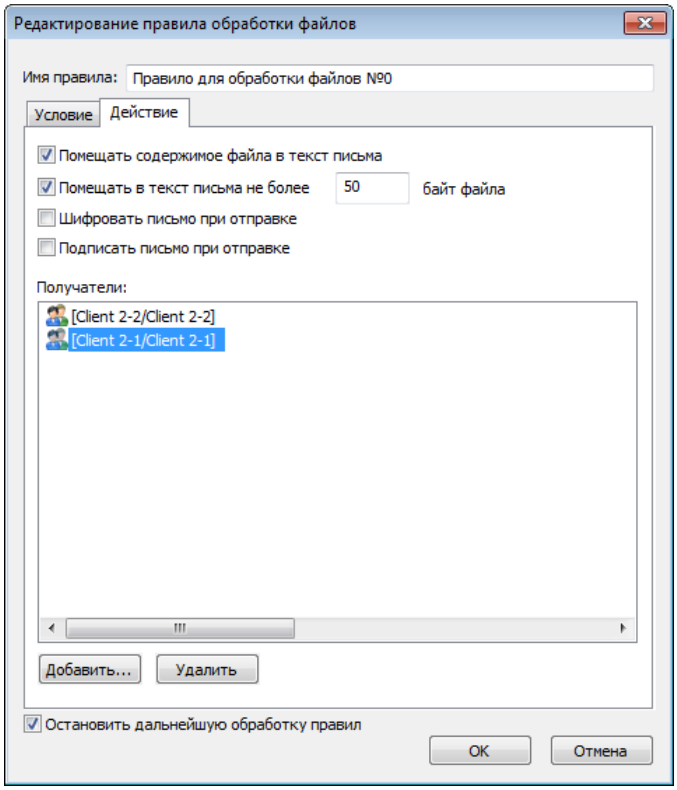


Рисунок 24: Действие правила обработки файлов

9 Если требуется помещать содержимое файла в текст письма, установите соответствующий флажок. При этом станет доступен флажок **Помещать в текст письма не более**.

Внимание! Данный флажок рекомендуется устанавливать только для обработки текстовых файлов, то есть файлов формата TXT. Если использовать эту функцию для файлов другого формата, в текст письма будет помещен нечитаемый набор символов.

Флажок **Помещать в текст письма не более** действует следующим образом:

- Если этот флажок не установлен (по умолчанию), файл будет полностью помещен в текст письма.
- Чтобы помещать в текст письма только фрагмент файла, установите флажок **Помещать в текст письма не более** и в текстовое поле введите количество байт для вставки в письмо.

  Если размер файла превышает указанное количество байт, фрагмент файла будет помещен в текст письма, а сам файл будет добавлен в письмо в качестве вложения.

10 Чтобы шифровать вложенный файл, установите флажок **Шифровать письмо при отправке**.

11 Чтобы подписывать вложенный файл электронной подписью, установите флажок **Подписать письмо при отправке**.

12 Чтобы добавить получателей, которым будет отправлен файл:

- Нажмите кнопку **Добавить**.
- В окне **Адресная книга** выберите получателя и нажмите кнопку **Выбрать.**
- Чтобы добавить других получателей, повторите предыдущий шаг.
- Нажмите кнопку **Закрыть.**

Чтобы удалить получателей, выберите одного или несколько получателей в списке и нажмите кнопку **Удалить.**

13 Если требуется, чтобы после обработки файла данным правилом этот файл мог быть обработан последующими правилами, снимите флажок **Остановить дальнейшую обработку правил** (по умолчанию установлен).

14 Чтобы сохранить правило, нажмите кнопку **OK.**

Создание правила для входящих писем

Чтобы создать правило для обработки входящих писем, выполните следующие действия:

1 В окне программы ViPNet Деловая почта в меню **Инструменты** выберите пункт **Настройка**.

2 В окне **Настройка** на панели навигации выберите раздел **Автопроцессинг** (см. рисунок на стр. 91).

3 На вкладке **Автопроцессинг** нажмите кнопку **Добавить**, откроется окно **Создание нового правила автопроцессинга.**

4 Выберите тип правила **Правило для обработки входящих писем** и нажмите кнопку **OK**. Откроется окно **Редактирование правила обработки входящих писем**.

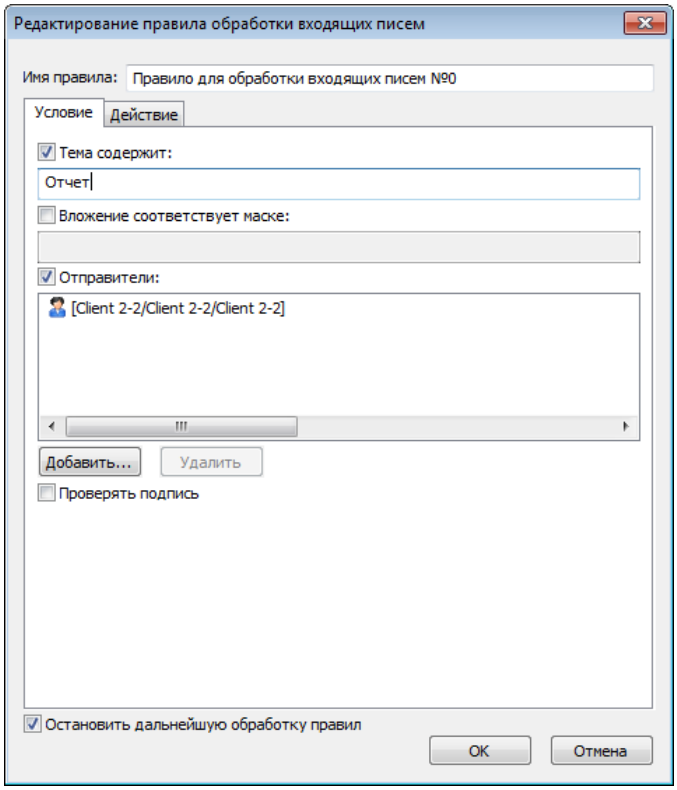


Рисунок 25: Условие правила обработки входящих писем

5 В поле **Имя правила** укажите имя для создаваемого правила.

6 На вкладке **Условие** задайте условия, при выполнении которых письмо будет обработано данным правилом:

- Если необходимо обрабатывать письма, в теме которых содержится определенная последовательность символов, установите флажок **Тема содержит** и в поле под этим флажком введите требуемые символы.
- Если необходимо обрабатывать письма с вложениями, имена которых соответствуют определенной маске, установите флажок **Вложение соответствует маске** и в поле под этим флажком введите маску имени вложения. Можно задать только одну маску.

  При задании маски регистр не учитывается, можно использовать следующие специальные символы:

  - * — соответствует любой последовательности символов.
  - ? — соответствует любому единичному символу.

Для выполнения условия требуется, чтобы имена одного или нескольких вложений письма соответствовали заданной маске. При выполнении данного условия будут обработаны только те вложения, имена которых соответствуют маске.

- Если необходимо обрабатывать письма от определенных отправителей:
  - Установите флажок **Отправители**.
  - Нажмите кнопку **Добавить**. Откроется **Адресная книга** (на стр. 40).
  - В адресной книге выберите одного или несколько отправителей и нажмите кнопку **Выбрать**.
  - Выбрав нужных отправителей, нажмите кнопку **Закрыть**.
  - Если требуется удалить каких-либо отправителей, выберите их в списке и нажмите кнопку **Удалить**.

  Для выполнения условия требуется, чтобы отправитель письма совпадал с одним из пользователей, указанным в данном списке.
- Если необходимо обрабатывать письма, подписанные электронной подписью, установите флажок **Проверять подпись**.

  Для выполнения условия требуется, чтобы вложения письма были подписаны и подпись была действительна.

Внимание! Если для правила задано несколько условий, письмо будет обработано данным правилом только при одновременном выполнении всех условий.

7 Откройте вкладку **Действие**.

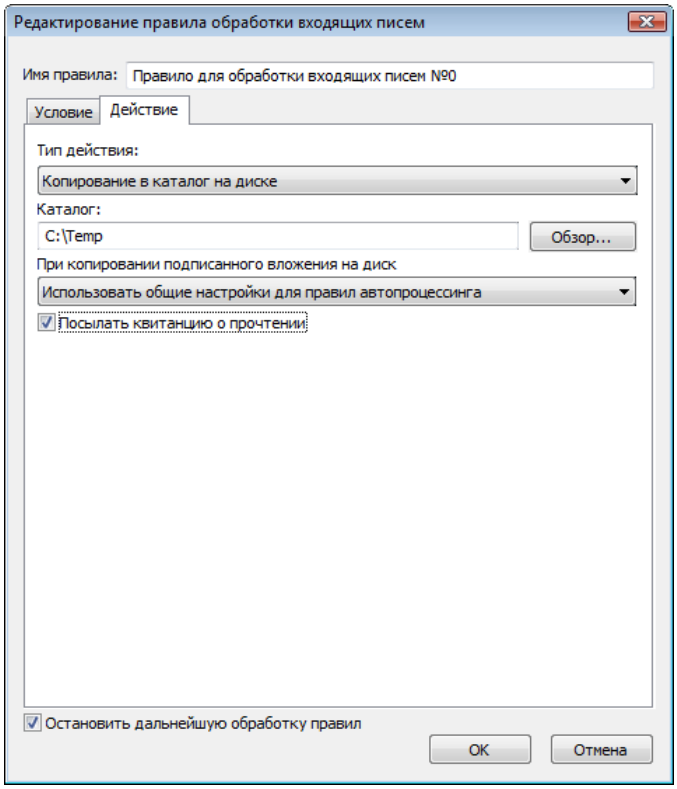


Рисунок 26: Действие правила обработки входящих писем

8 Из списка **Тип действия** выберите один из вариантов:

- **Копирование в каталог на диске.**
- **Копирование в каталог с заменой существующих файлов**. При совпадении имен файл, уже находящийся в папке назначения, заменяется файлом вложения из обработанного письма.
- **Копирование в каталог с заменой более старых файлов**. При совпадении имен файл, уже находящийся в папке назначения, заменяется файлом вложения, только если файл вложения был изменен позже.
- **Копирование в каталог с переименованием копируемого файла**. При совпадении имен к имени сохраняемого файла добавляется постфикс `_copy<номер копии>`.
- **Перемещение письма в папку Деловой почты.**

При копировании письма на диске в указанной папке сохраняются файлы вложений и текст письма в виде файла `blank.txt`. Если письмо не содержит текста, файл `blank.txt` не создается.

9 Если выбрано копирование письма в каталог на диске, выполните следующие действия:

- Нажмите кнопку **Обзор** и в окне **Обзор папок** укажите папку, в которую будут скопированы текст письма и его вложения.
- Из списка **При копировании подписанного вложения на диск** выберите один из вариантов:
  - **Использовать общие настройки для правил автопроцессинга**. При выборе этого варианта будет выполнено действие, заданное в разделе **Автопроцессинг** (см. «Настройка правил автопроцессинга» на стр. 91).
  - **Удалять подпись**.
  - **Сохранять в виде файла с присоединенной подписью**.
  - **Отсоединять подпись в отдельный файл**.

  Подробнее о присоединенной и отсоединенной электронной подписи файла см. Отсоединение и присоединение подписи файла (на стр. 82).
- Если после обработки письма данным правилом требуется отправлять уведомление о прочтении письма, установите флажок **Посылать квитанцию о прочтении**.

10 Если выбрано перемещение письма в папку программы ViPNet Деловая почта, нажмите кнопку **Обзор** и в окне **Укажите папку** выберите папку для сохранения писем. Это должна быть какая-либо подпапка папки **Входящие**.

11 Если требуется, чтобы после обработки письма данным правилом это письмо могло быть обработано последующими правилами, снимите флажок **Остановить дальнейшую обработку правил** (по умолчанию установлен).

12 Чтобы сохранить правило, нажмите кнопку **OK**.

Оптимизация работы автопроцессинга

В некоторых случаях правилами автопроцессинга обрабатывается очень большое количество писем. Обработка большого объема данных с настройками автопроцессинга по умолчанию может существенно замедлить работу программы ViPNet Деловая почта, приостановить прием текущей корреспонденции, вызвать непредвиденные ошибки.

Чтобы ускорить работу автопроцессинга с большим количеством писем, рекомендуется выполнить следующие настройки:

1. Войдите в программу ViPNet Деловая почта с правами администратора (см. «Работа в программе с правами администратора» на стр. 120).
2. В окне программы в меню **Инструменты** выберите пункт **Настройка**.
3. В окне **Настройка** на панели навигации выберите раздел **Администратор**.
4. В разделе **Администратор** снимите флажок **Сохранять историю в папке «Аудит»**.
5. На панели навигации выберите раздел **Автопроцессинг**.
6. В разделе **Автопроцессинг** (см. «Настройка правил автопроцессинга» на стр. 91) снимите флажок **Сохранять письма, обработанные автопроцессингом**.

Данные настройки позволят существенно повысить скорость обработки писем правилами автопроцессинга.

Просмотр журнала автопроцессинга

Информация о событиях, возникающих при работе автопроцессинга, фиксируется в журнале автопроцессинга. Настройка параметров журнала описана ниже (см. «Настройка параметров журнала автопроцессинга» на стр. 104).

Для просмотра журнала автопроцессинга выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Файл** выберите пункт **Журнал автопроцессинга**. Откроется окно **Просмотр журналов**.

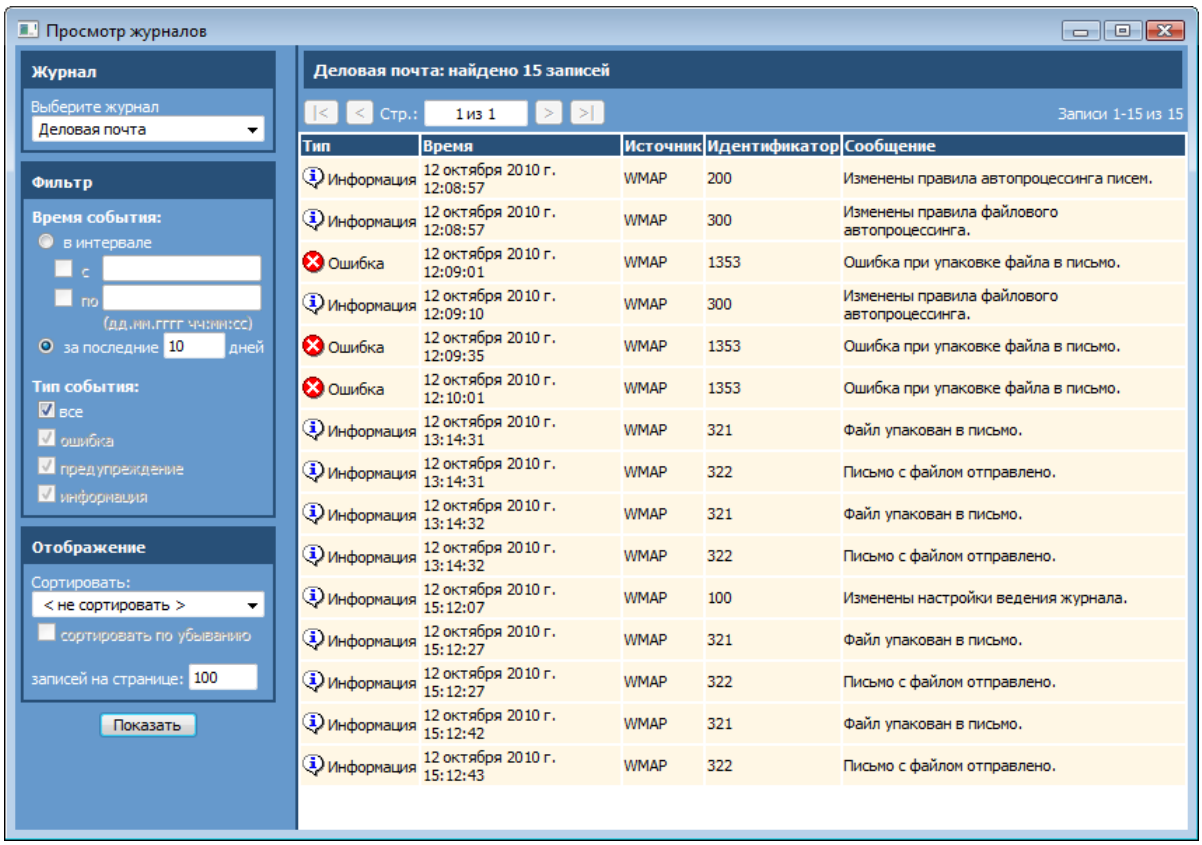


Рисунок 27: Просмотр журнала автопроцессинга

2 В левой части окна **Просмотр журналов** на панели **Фильтр** задайте параметры поиска событий в журнале:

- Задайте время события одним из двух способов:

- Для поиска событий, произошедших в определенном интервале времени, выберите пункт **в интервале**. Чтобы указать начало и конец интервала, установите соответствующие флажки (**с** и **по**) и в поле справа введите дату и время в формате `дд.мм.гггг чч:мм:сс`.
- Для поиска событий, произошедших за последние несколько дней, выберите пункт **за последние** и в поле справа введите количество дней.

По умолчанию задан поиск событий за последние 10 дней.

- Задайте тип события, установив или сняв флажки **все**, **ошибка**, **предупреждение**, **информация**. По умолчанию задан поиск всех событий.

3 На панели **Отображение**:

- Из списка **Сортировать** выберите порядок сортировки. По умолчанию выбран пункт **< не сортировать >**.
- Если требуется изменить порядок сортировки событий, установите флажок **сортировать по убыванию** (этот флажок недоступен, если в списке **Сортировать** выбран пункт **< не сортировать >**).
- В поле **Записей на странице** укажите число событий, отображаемых на одной странице (по умолчанию 100).

4 Задав параметры поиска, нажмите кнопку **Показать**. На правой панели окна **Просмотр журналов** отобразится список найденных событий (см. рисунок на стр. 101).

5 Если результаты поиска отображаются на нескольких страницах, для переключения между страницами используйте кнопки, расположенные над списком событий.

6 Чтобы просмотреть подробную информацию о каком-либо событии, щелкните строку этого события. Откроется окно **Информация о событии**.

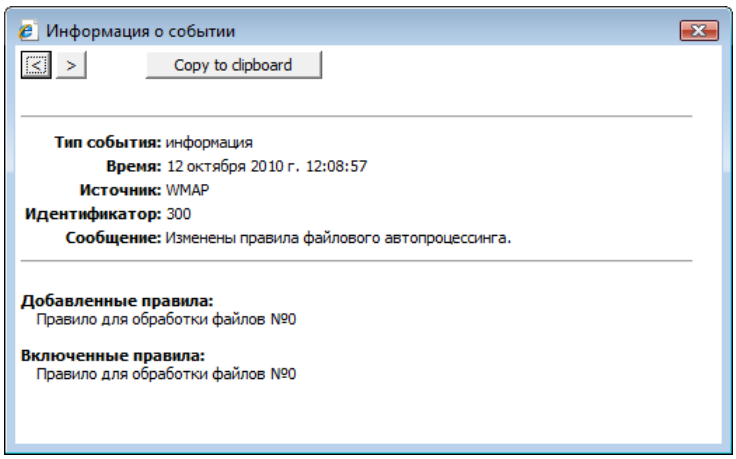


Рисунок 28: Подробная информация о событии

Чтобы перейти к предыдущему событию в списке, нажмите кнопку < в верхней части окна **Информация о событии**. Чтобы перейти к следующему событию, нажмите кнопку >.

События, регистрируемые в журнале автопроцессинга, перечислены ниже.

Таблица 4. События автопроцессинга

Тип события	Идентификатор события	Описание события
Информация	100	Изменены настройки ведения журнала
	200	Изменены правила автопроцессинга писем
	210	Сработало правило автопроцессинга писем
	211	Письмо перемещено
	212	Текст письма сохранен в файл
	213	Вложение сохранено в файл
	300	Изменены правила файлового автопроцессинга
	312	Файловый автопроцессинг перезапущен
	321	Файл упакован в письмо
	322	Письмо с файлом отправлено
Предупреждение	311	Файловый автопроцессинг приостановлен
Ошибка	1251	Ошибка при обработке письма
	1252	Ошибка при поиске правила
	1253	Ошибка при применении правила
	1254	Ошибка при перемещении письма
	1255	Ошибка при сохранении текста письма
	1256	Ошибка при сохранении вложения
	1351	Ошибка при поиске файлов
	1352	Ошибка при обработке файла
	1353	Ошибка при упаковке файла в письмо
	1354	Ошибка при отправке письма с файлом

Настройка параметров журнала автопроцессинга

Для настройки параметров журнала автопроцессинга выполните следующие действия:

1. В окне программы ViPNet Деловая почта в меню **Инструменты** выберите пункт **Настройка**.
2. В окне **Настройка** на панели навигации выберите раздел **Автопроцессинг** > **Журнал**.

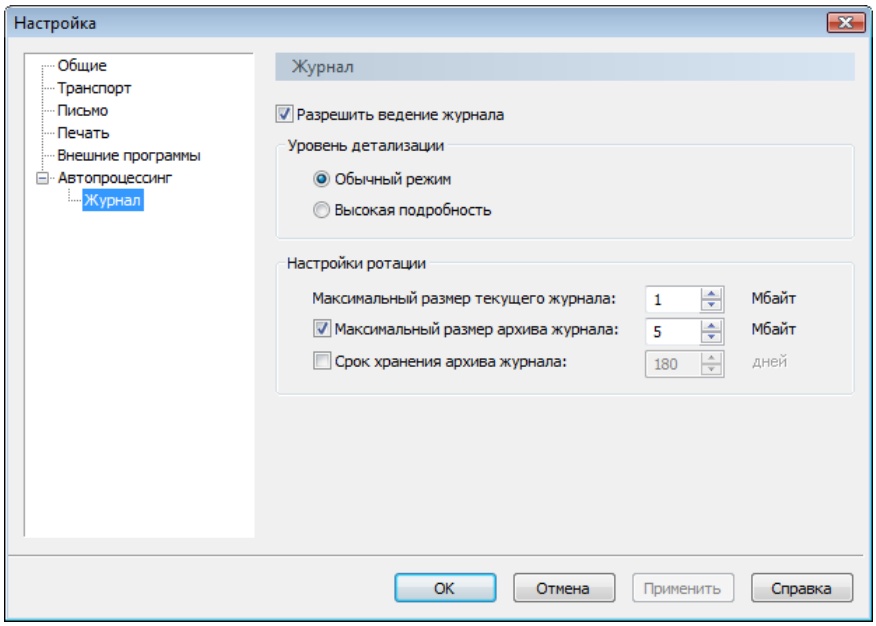


Рисунок 29: Настройка журнала автопроцессинга

3. Если требуется отключить ведение журнала автопроцессинга, снимите флажок **Разрешить ведение журнала** (по умолчанию установлен).

   Если данный флажок снят, настройка остальных параметров журнала автопроцессинга недоступна.

4. В группе **Уровень детализации** выберите один из пунктов:
   - **Обычный режим** (выбран по умолчанию) — фиксируется наиболее важная информация.
   - **Высокая подробность** — фиксируется вся информация.

5 В группе **Настройки ротации** задайте следующие параметры:

- В поле **Максимальный размер текущего журнала** введите размер журнала в мегабайтах (по умолчанию 1).

  Если размер текущего файла журнала превышает заданное значение, файлу присваивается статус архивного и создается новый текущий файл журнала.

- Чтобы задать ограничение по размеру архива журнала, установите флажок **Максимальный размер архива журнала** и в поле справа введите размер архива в мегабайтах (по умолчанию 5).

  Если суммарный размер архивных файлов журнала превысил заданное значение, последовательно удаляются самые старые архивные файлы до тех пор, пока суммарный размер архивов не станет меньше или равен заданному значению.

- Чтобы задать ограничение по времени хранения архива, установите флажок **Срок хранения архива журнала** и в поле справа введите максимальное время хранения архива в днях (по умолчанию 180).

  Если время хранения архивного файла журнала (разница между текущим временем и временем перевода файла в архив) превышает заданное значение, такой файл удаляется.

Примечание. Если установлен флажок **Срок хранения архива журнала**, не рекомендуется изменять системное время, так как это может иметь негативные последствия.

6 Чтобы сохранить настройки, нажмите кнопку **Применить.**

6

Настройка программы

Настройка общих параметров

Для настройки общих параметров программы ViPNet Деловая почта выполните следующие действия:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Инструменты** выберите пункт **Настройка**.

2. В окне **Настройка** на панели навигации выберите раздел **Общие**.

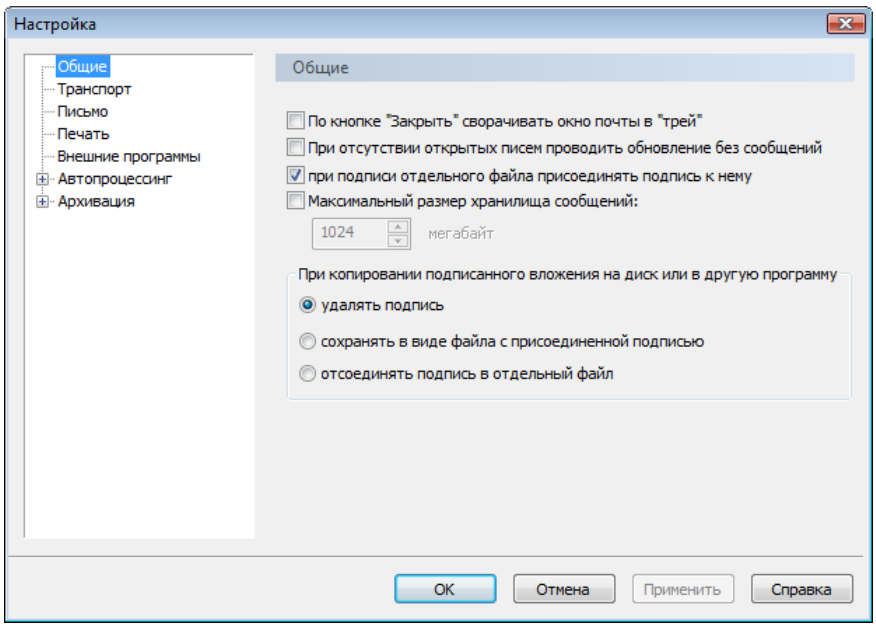


Рисунок 30: Общие настройки программы ViPNet Деловая почта

3. Чтобы при нажатии на кнопку **Закрыть**  программа сворачивалась в область уведомлений, установите флажок **По кнопке «Закрыть» сворачивать окно почты в «трей»** (по умолчанию снят).

4. Чтобы при отсутствии открытых писем проводить обновление справочников и ключей, а также программного обеспечения без уведомлений, установите флажок **При отсутствии открытых писем проводить обновление без сообщений** (по умолчанию снят).

5. Если требуется отсоединять электронную подпись при подписании отдельного файла (см. «Подписание файла» на стр. 81), снимите флажок **При подписи отдельного файла присоединять подпись к нему** (по умолчанию установлен).

6 Чтобы ограничить размер хранилища писем, установите флажок **Максимальный размер хранилища сообщений** и в поле под флажком укажите размер в мегабайтах.

Если размер хранилища ограничен, при достижении максимального размера программа перестанет забирать почтовые конверты из папки транспортного модуля (то есть вы перестанете получать новые письма).

7 В группе **При копировании подписанного вложения на диск или в другую программу** выберите одно из действий:

- **удалять подпись** (по умолчанию);
- **сохранять в виде файла с присоединенной подписью**;
- **отсоединять подпись в отдельный файл**.

Подробнее о присоединенной и отсоединенной электронной подписи файла см. Отсоединение и присоединение подписи файла (на стр. 82).

8 Выполнив необходимые настройки, нажмите кнопку **Применить**.

Настройка архивации писем

Общие параметры архивации

При настройке архивации писем, выполняемой вручную или автоматически (см. «Архивация писем» на стр. 66), вы можете указать, какие письма следует помещать в архив и каким способом следует размещать в архиве вложения.

Чтобы задать параметры архивации писем, выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Инструменты** выберите пункт **Настройка**.

2 В окне **Настройка** на панели навигации выберите раздел **Архивация**.

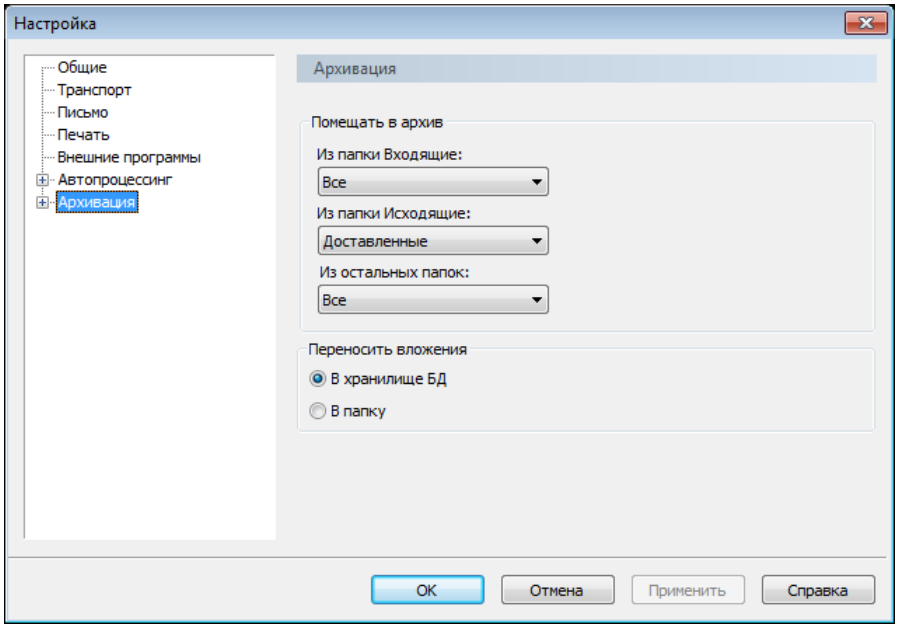


Рисунок 31: Настройка параметров архивации

3 В группе **Помещать в архив** выберите категории писем, которые следует архивировать:

- В списке **Из папки Входящие** выберите, какие входящие письма требуется помещать в архив: **Прочитанные** или **Все** (по умолчанию **Все**).

- В списке **Из папки Исходящие** выберите, какие исходящие письма требуется помещать в архив: **Отправленные, Доставленные, Прочитанные** или **Все** (по умолчанию **Доставленные**).
- В списке **Из остальных папок** выберите, какие входящие письма из папок **Удаленные** и **Аудит** требуется помещать в архив: **Не архивировать** или **Все** (по умолчанию **Все**).

Если для всех папок выбрано значение **Все** (полная архивация), при архивации текущее хранилище сообщений преобразуется в архив, а для дальнейшей работы создается новое хранилище сообщений. При неполной архивации создается новый архив, в который копируются письма для архивации. Таким образом, полная архивация выполняется значительно быстрее, чем неполная.

Внимание! Если с помощью программы ViPNet Деловая почта ежедневно обрабатывается большое количество писем, рекомендуется настроить полную архивацию писем во всех папках.

4 В группе **Переносить вложения** с помощью переключателя укажите способ размещения вложений:

- **В хранилище БД** — добавление вложений в базу данных и их размещение в архиве вместе с письмами (по умолчанию). При таком способе архив будет содержать один файл с базой данных, который при необходимости легко скопировать или перенести на внешний носитель.
- **В папку** — размещение вложений в папках отдельно от писем. В этом случае архив будет содержать файл с базой данных писем и набор папок с размещенными в них вложениями.

Внимание! Способ размещения вложений учитывается только при неполной архивации.

5 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Параметры автоматической архивации

Для настройки параметров автоматической архивации выполните следующие действия:

1 В окне **Настройка** на панели навигации выберите подраздел **Архивация** > **Автоматическая архивация**.

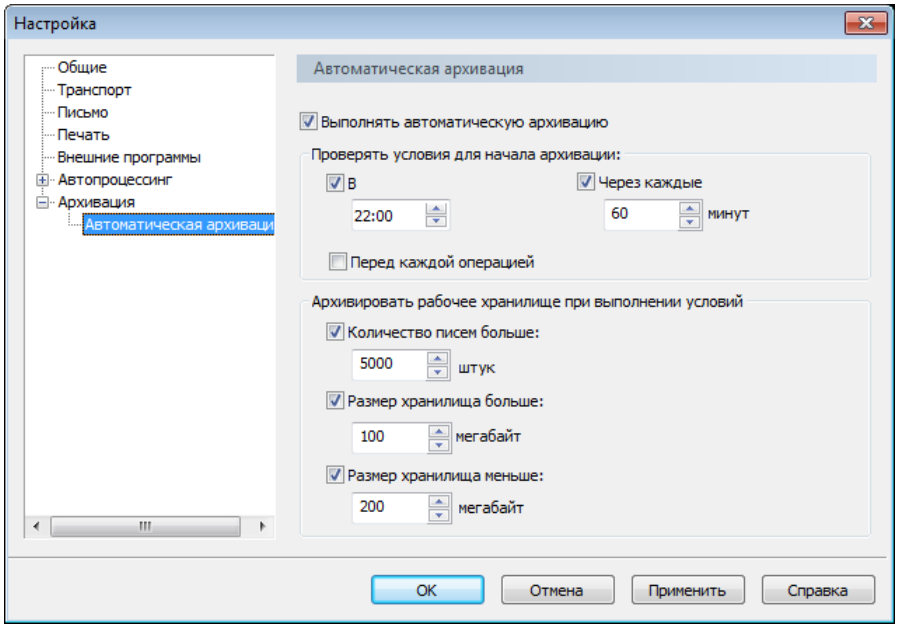


Рисунок 32: Параметры автоматической архивации

2 Чтобы включить автоматическую архивацию писем, установите флажок **Выполнять автоматическую архивацию** (по умолчанию снят).

3 Если автоматическая архивация включена, в группе **Проверять условия для начала архивации** установите один или несколько флажков:

- Если требуется проверять условия архивации в определенное время, установите флажок **В** и в поле под флажком укажите время проверки (по умолчанию флажок установлен, задано время 22:00).
- Если требуется проверять условия архивации через определенный интервал времени, установите флажок **Через каждые** и в поле под флажком укажите время в минутах (по умолчанию флажок установлен, задано время 60 минут).
- Если требуется проверять условия архивации перед отправкой и получением писем, установите флажок **Перед каждой операцией** (по умолчанию снят).

Примечание. Если в группе **Проверять условия для начала архивации** установлены несколько флажков, проверка условия архивации будет выполняться во всех указанных случаях.

---

4 Если автоматическая архивация включена, в группе **Начинать архивацию при выполнении условия** установите один или несколько флажков:

- Чтобы выполнять автоматическую архивацию при накоплении определенного количества писем, установите флажок **Количество писем больше** и в поле под флажком укажите количество писем (по умолчанию 5000).
- Чтобы выполнять автоматическую архивацию при достижении определенного размера хранилища, установите флажок **Размер хранилища больше** и в поле под флажком укажите размер в мегабайтах (по умолчанию 100).

Примечание. Если флажки **Количество писем больше** и **Размер хранилища больше** установлены одновременно, архивация будет выполняться при выполнении любого из заданных условий.

- Чтобы ограничить размер архива, установите флажок **Размер хранилища меньше** и в поле под флажком укажите размер в мегабайтах (по умолчанию 200).

  Если суммарный размер писем, подлежащих архивации, превышает заданный максимальный размер архива, то будет создано несколько архивов писем. Размер каждого из них будет меньше заданного значения.

5 Чтобы сохранить настройки, нажмите кнопку **Применить.**

Настройка параметров работы с письмами

Для настройки параметров работы с письмами выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Инструменты** выберите пункт **Настройка**.

2 В окне **Настройка** на панели навигации выберите раздел **Письмо**.

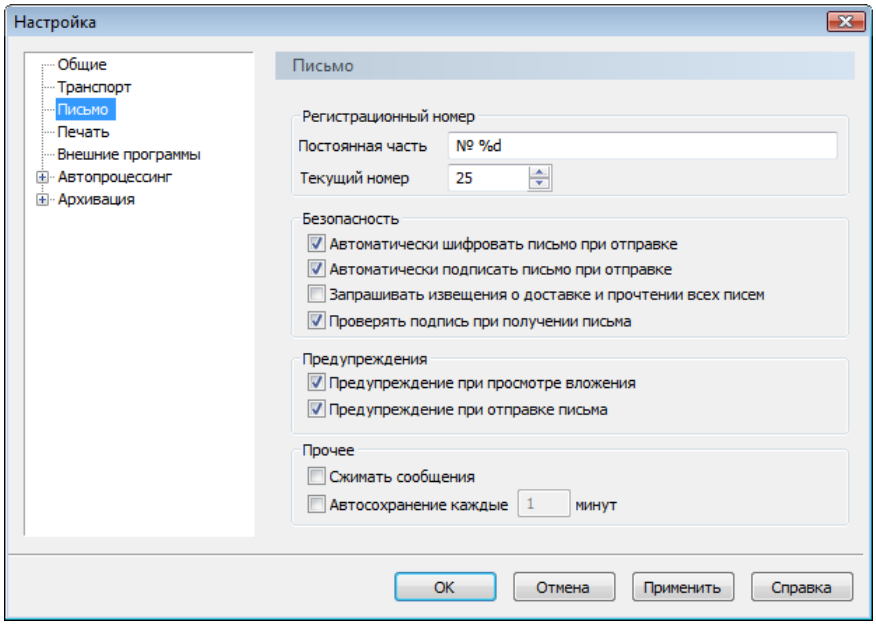


Рисунок 33: Параметры работы с письмами

3 В случае необходимости настройте формат регистрационного номера.

Регистрационный номер присваивается каждому письму при создании. Входящие письма имеют регистрационные номера, которые присвоены отправителями. Регистрационные номера отображаются в списке на панели писем (см. «Интерфейс программы» на стр. 33).

Чтобы изменить формат регистрационного номера, в группе **Регистрационный номер** выполните следующие действия:

- В поле **Постоянная часть** укажите постоянную часть регистрационного номера. Постоянная часть не должна быть длиннее 12 символов и должна обязательно содержать символы «%d», вместо которых подставляется текущий номер.

- Если требуется изменить текущий номер, в поле **Текущий номер** укажите любое число, которое больше указанного в данный момент номера, но меньше 999999999.

4 Чтобы изменить параметры шифрования и электронной подписи, в группе **Безопасность** выполните следующие действия:

- Установите или снимите флажок **Автоматически шифровать письмо при отправке**.
- Установите или снимите флажок **Автоматически подписать письмо при отправке**. Если этот флажок установлен, текст письма и все вложения будут автоматически подписаны текущим сертификатом (см. «Электронная подпись в программе ViPNet Деловая почта» на стр. 72).
- Установите или снимите флажок **Запрашивать извещения о доставке и прочтении всех писем** (см. «Запрос извещений о доставке и прочтении в виде отдельного письма» на стр. 47).
- Установите или снимите флажок **Проверять подпись при получении письма**.

5 Чтобы изменить параметры уведомления при просмотре вложений и отправке писем, в группе **Предупреждения** выполните следующие действия:

- Установите или снимите флажок **Предупреждение при просмотре вложения**.

  Если этот флажок установлен, перед просмотром вложения программа выдаст предупреждение.
- Установите или снимите флажок **Предупреждение при отправке письма**.

  Если этот флажок установлен, при отправке письма программа запросит подтверждение.

6 В группе **Прочие** доступны следующие настройки:

- Чтобы уменьшить размер передаваемых конвертов, установите флажок **Сжимать сообщения** (по умолчанию снят). Перед отправкой письма будут обрабатываться алгоритмом сжатия.
- Чтобы включить автоматическое сохранение редактируемых писем, установите флажок **Автосохранение каждые** (по умолчанию снят) и в поле справа укажите интервал автоматического сохранения в минутах.

Настройка транспортного модуля

Для настройки параметров транспортного модуля MFTP выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Инструменты** выберите пункт **Настройка**.

2 В окне **Настройка** на панели навигации выберите раздел **Транспорт**.

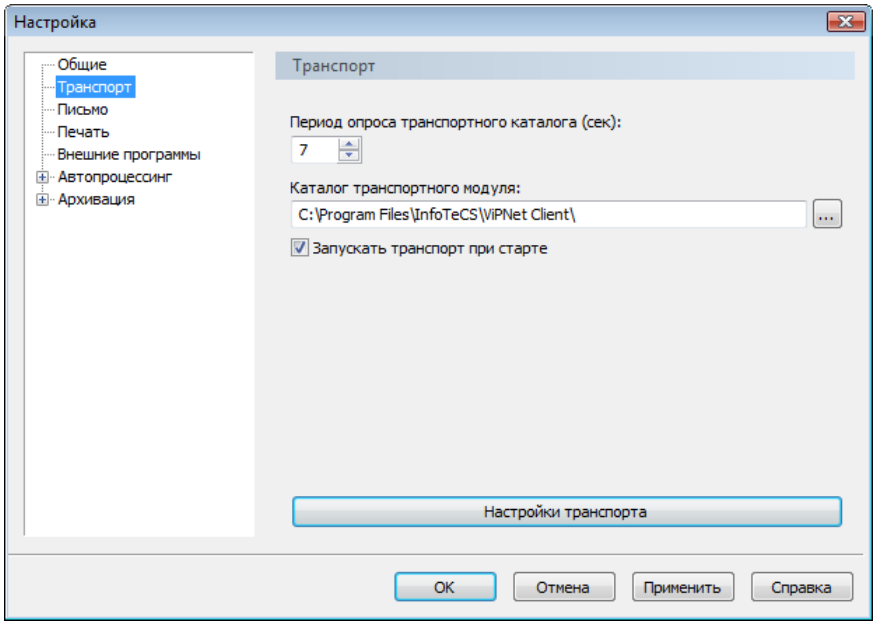


Рисунок 34: Настройки транспортного модуля

3 В разделе **Транспорт** при необходимости можно изменить следующие параметры:

- В поле **Период опроса транспортного каталога (сек)** укажите нужный период в секундах.
- Чтобы изменить транспортный каталог, нажмите кнопку ... и в окне **Обзор папок** укажите папку, в которой находится транспортный модуль MFTP.

Внимание! Не следует изменять папку транспортного модуля без необходимости.

- Если не требуется запускать транспортный модуль при запуске программы ViPNet Деловая почта, снимите флажок **Запускать транспорт при старте** (по умолчанию установлен).

4 Чтобы вызвать окно настройки, доступное из основного окна транспортного модуля, нажмите кнопку **Настройки транспорта**.

Подробная информация о транспортном модуле и его настройке содержится в документе «ViPNet MFTP. Руководство администратора».

5 Выполнив необходимые настройки, нажмите кнопку **OK**.

Настройка печати

Чтобы настроить параметры печати писем, выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Инструменты** выберите пункт **Настройка**.

2 В окне **Настройка** на панели навигации выберите раздел **Печать**.

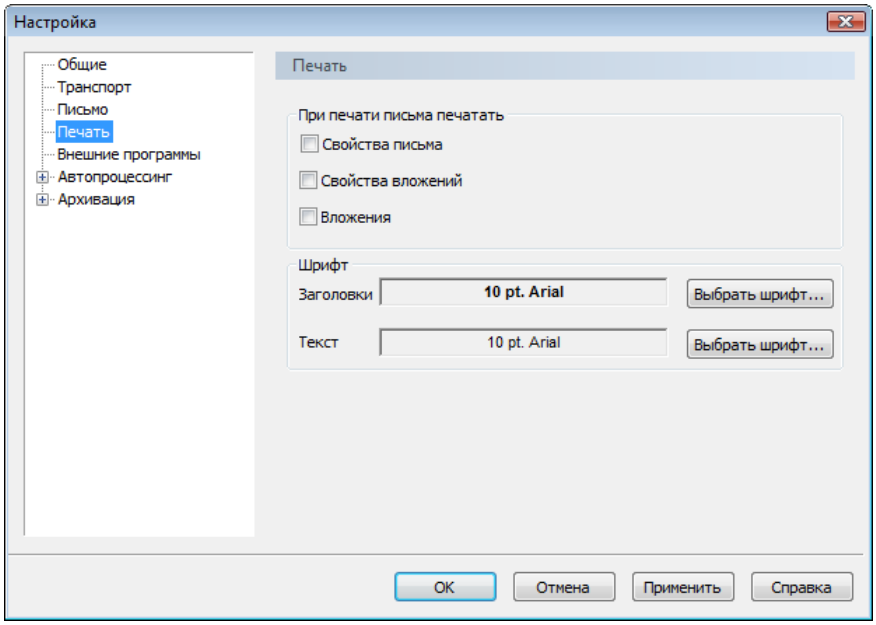


Рисунок 35: Настройки печати

3 В группе **При печати письма печатать** укажите, какую дополнительную информацию требуется добавлять к тексту письма, установив соответствующие флажки (по умолчанию все флажки сняты):

- **Свойства письма**.
- **Свойства вложений**.
- **Вложения**.

4 Чтобы изменить шрифт заголовка или текста при печати, нажмите кнопку **Выбрать шрифт** напротив поля **Заголовки** или **Текст** и в окне **Шрифт** задайте параметры шрифта.

5 Выполнив необходимые настройки, нажмите кнопку **Применить**.

Настройка внешних программ

В программе ViPNet Деловая почта существует возможность вызова внешних программ. Для этого в окне программы ViPNet Деловая почта в меню **Инструменты** выберите **Запуск внешних программ**.

Чтобы изменить список доступных для вызова программ, выполните следующие действия:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Инструменты** выберите пункт **Настройка**.

2. В окне **Настройка** на панели навигации выберите раздел **Внешние программы**.

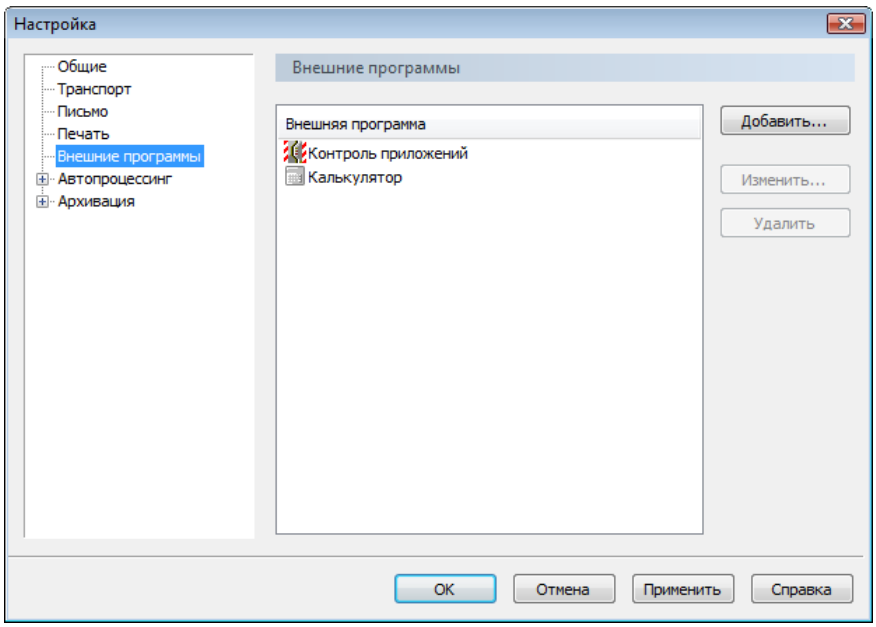


Рисунок 36: Настройка внешних программ

3. Чтобы добавить программу в список программ, доступных для вызова из программы ViPNet Деловая почта:
   - Нажмите кнопку **Добавить**.
   - В окне **Внешняя программа** укажите путь к исполняемому файлу программы, затем нажмите кнопку **Далее**.
   - В окне **Имя внешней программы** укажите имя, которое будет отображаться в интерфейсе программы ViPNet Деловая почта, затем нажмите **Готово**.

4 Чтобы изменить путь к программе или имя программы, выберите программу из списка и нажмите кнопку **Изменить**.

5 Чтобы удалить программу из списка, выберите программу и нажмите кнопку **Удалить**.

6 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Работа в программе с правами администратора

В программе ViPNet Деловая почта предусмотрена возможность работы с правами администратора. В режиме администратора становятся доступны следующие функции и настройки:

- Дополнительные настройки и возможности программы (на стр. 121).
- Дополнительные настройки параметров безопасности (на стр. 122).
- Изменение способа аутентификации пользователя (на стр. 123).

При работе в режиме администратора все ограничения, накладываемые уровнем полномочий пользователя (см. «Полномочия пользователя» на стр. 208), снимаются.

Чтобы войти в программу в качестве администратора:

1. В окне программы ViPNet Деловая почта (см. «Интерфейс программы» на стр. 33) в меню **Инструменты** выберите пункт **Настройка параметров безопасности**.
2. В окне **Настройка параметров безопасности** откройте вкладку **Администратор** и нажмите кнопку **Вход администратора**.
3. В окне **Пароль** введите пароль администратора сетевого узла ViPNet.

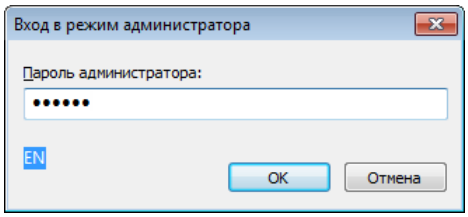


Рисунок 37: Ввод пароля администратора сетевого узла

4. Нажмите кнопку **OK**. Если введен верный пароль, станут доступны дополнительные настройки.

Дополнительные настройки и возможности программы

При работе в режиме администратора можно удалять из папки **Аудит** информацию об удаленных письмах. В любых папках программы ViPNet Деловая почта в контекстном меню письма доступен пункт **Полное удаление**. При полном удалении письмо удаляется из хранилища без соответствующей записи в папке **Аудит**.

Если полномочия пользователя (на стр. 208) в программе ViPNet Деловая почта ограничены, то в режиме администратора все ограничения снимаются.

Кроме того, в режиме администратора в окне **Настройка** доступен раздел **Администратор**, в котором можно отключить сохранение истории удаленных писем в папке **Аудит**. Для этого выполните следующие действия:

1. Войдите в программу ViPNet Деловая почта в качестве администратора (см. «Работа в программе с правами администратора» на стр. 120).
2. В окне программы в меню **Инструменты** выберите пункт **Настройка**.
3. В окне **Настройка** на панели навигации выберите раздел **Администратор**.

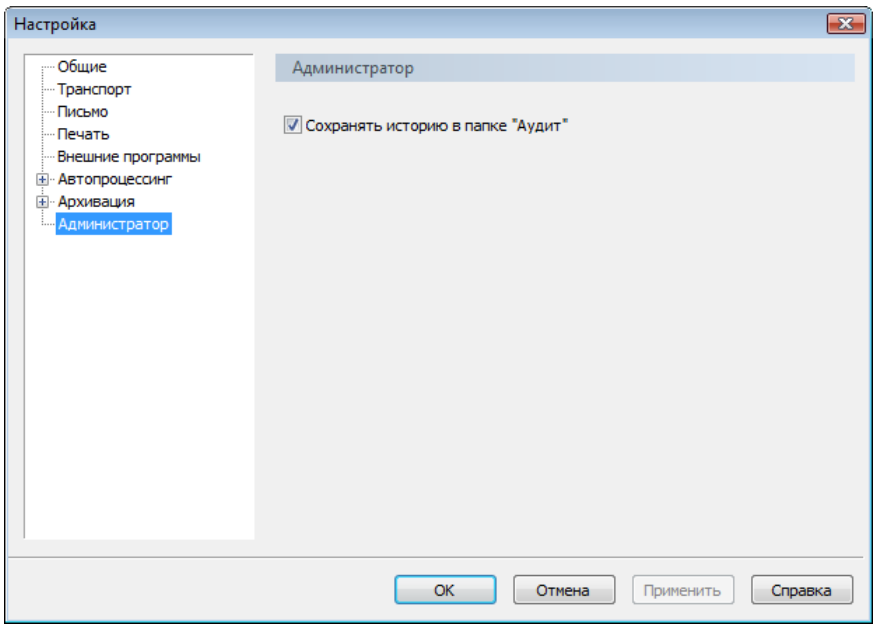


Рисунок 38: Дополнительные настройки в разделе «Администратор»

4. Чтобы отключить сохранение информации об удаленных письмах в папке **Аудит**, снимите флажок **Сохранять историю в папке «Аудит»** (по умолчанию установлен).
5. Чтобы сохранить настройки, нажмите кнопку **Применить**.

Дополнительные настройки параметров безопасности

Помимо дополнительных параметров настройки в разделе **Администратор**, во время работы в режиме администратора сетевого узла доступны следующие параметры на вкладке **Администратор** в окне **Настройка параметров безопасности**:

- **Разрешить сохранение пароля в реестре** — позволяет пользователю сетевого узла установить флажок **Сохранить пароль** при входе в программу ViPNet Деловая почта. Если этот флажок установлен, пароль пользователя хранится в реестре Windows и автоматически подставляется в поле ввода пароля при запуске программы ViPNet Монитор.

Примечание. Если для управления сетью ViPNet используется программа ViPNet Network Manager, изменить состояние флажка **Разрешить сохранение пароля в реестре** невозможно. Чтобы изменить этот параметр, обратитесь к администратору сети ViPNet.

Для сетей ViPNet CUSTOM такая функциональность не предусмотрена.

- **Автоматически входить в ViPNet** — позволяет выполнять вход в ПО ViPNet Деловая почта без необходимости подтверждения пароля пользователя ViPNet в окне входа в программу. Если флажок установлен, при запуске программы на текущем сетевом узле окно входа в программу не появляется и вход в ПО ViPNet Деловая почта выполняется автоматически. Это происходит в следующих случаях:
  - при использовании способа аутентификации **Пароль** — если пароль сохранен в реестре, то есть установлен флажок **Разрешить сохранение пароля в реестре**, а в окне входа в программу указан верный пароль и установлен флажок **Сохранить пароль**;
  - при использовании способов аутентификации **Пароль на устройстве** и **Устройство** — если внешнее устройство подключено к компьютеру и в окне входа в программу указан верный ПИН-код и установлен флажок **Сохранить ПИН-код**.
- **Разрешить использование внешних сертификатов** — позволяет использовать сертификаты не только из личного хранилища (хранилища программы), но также из хранилища операционной системы. Это может понадобиться в том случае, если в ПО ViPNet предполагается использовать криптопровайдер другого производителя (например, КриптоПро), а также сертификаты, изданные внешними Удостоверяющими центрами (вне сети ViPNet).
- **Доверять только сертификатам администраторов УЦ ViPNet** — если этот флажок снят, при проверке сертификата поиск корневого сертификата выполняется

не только во внутреннем хранилище ПО ViPNet, но и в системных хранилищах **Доверенные корневые центры сертификации** и **Промежуточные центры сертификации**.

- **Игнорировать отсутствие списков отозванных сертификатов** — этот флажок следует установить, если в системе используются сертификаты, изданные внешними Удостоверяющими центрами, так как в таких сертификатах информация о списках отозванных сертификатов может отсутствовать.

Изменение способа аутентификации пользователя

Способ аутентификации определяет, какие данные должен предоставить пользователь для входа в программу ViPNet Деловая почта. Чтобы изменить способ аутентификации пользователя, выполните следующие действия:

1. Выполните вход в программу в режиме администратора.
2. В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите кнопку **Изменить**.
3. В окне **Способ аутентификации** выберите один из способов аутентификации. Описание возможных способов аутентификации пользователя приведено в разделе Способы аутентификации пользователя (на стр. 26).

Примечание. Способ **Пароль на устройстве** выбрать нельзя, поскольку он перестал отвечать требованиям безопасности.

При выборе способа аутентификации по сертификату подключите внешнее устройство и укажите нужный сертификат в списке сертификатов, обнаруженных на устройстве. При возникновении затруднений в выборе сертификата см. раздел Не удается выполнить аутентификацию с помощью сертификата (на стр. 191).

При выборе способа аутентификации по персональному ключу подключите внешнее устройство для сохранения на нем персонального ключа пользователя. При сохранении персонального ключа (ключа защиты) на устройство стоит учитывать следующую особенность. Если пользователь производит процедуры подписи и шифрования внутри сторонних приложений (например, в Microsoft Office), то в этом случае настоятельно рекомендуется его контейнер ключей (на стр. 207) сохранять также на этом устройстве. Иначе подписание и шифрование в сторонних приложениях будет невозможно из-за проблемы с доступом к ключу защиты. Контейнер ключей можно также перенести из текущей папки в другую папку на

диске, но в этом случае каждый раз при подписании и шифровании в стороннем приложении вам потребуется вводить пароль.

Внимание! Если при использовании способа аутентификации **Устройство** внешнее устройство будет отключено, компьютер может быть автоматически заблокирован — в соответствии с настройками, заданными в режиме администратора. Для продолжения работы необходимо вновь подключить это внешнее устройство. При необходимости параметры автоматической блокировки компьютера и IP-трафика могут быть изменены.

4 Нажмите кнопку **OK**.

На вкладке **Ключи** в группе **Аутентификация** значения полей **Способ аутентификации** и **Тип носителя** изменятся в соответствии с выбранным режимом.

В сетях ViPNet CUSTOM способ аутентификации также может изменить администратор сети в программе ViPNet Удостоверяющий и ключевой центр. Если администратор назначает пользователю способ аутентификации по сертификату, то пользователь в данном случае должен предоставить администратору внешнее устройство с сертификатом и закрытым ключом для регистрации. При этом должны быть соблюдены условия, описанные в примечании в разделе Устройство (на стр. 30). После назначения пользователю нового способа аутентификации администратор вышлет обновление ключей узла. Приняв данное обновление ключей, пользователь сможет выполнить аутентификацию на узле только выбранным способом.

Настройка параметров безопасности

Смена пароля пользователя

Пароль пользователя рекомендуется менять раз в 3 месяца. В целом же частота смены пароля пользователя определяется регламентом безопасности организации.

Смена текущего пароля пользователя требуется в следующих случаях:

- По истечении срока действия текущего пароля (в случае, если этот срок действия ограничен).
- При поступлении на сетевой узел обновления ключей из программы ViPNet Удостоверяющий и ключевой центр, содержащего новый пароль пользователя. В этом случае появится окно с сообщением «Рекомендуется сменить пароль пользователя», однако пароль не будет изменен автоматически, поэтому процедуру смены пароля необходимо выполнить вручную.
- Если контейнер ключей защищен с использованием не пароля, а персонального ключа пользователя, пароль к контейнеру ключей будет совпадать с паролем пользователя. Поэтому при необходимости смены пароля к контейнеру ключей (см. «Смена пароля к контейнеру» на стр. 183), следует сменить пароль пользователя.

Кроме того, рекомендуется менять пароль пользователя при первом входе в программу после установки справочников и ключей. Это повысит надежность пароля, поскольку он не будет известен администратору.

Для того чтобы сменить пароль пользователя:

1 В окне **Настройка параметров безопасности** откройте вкладку **Пароль.**

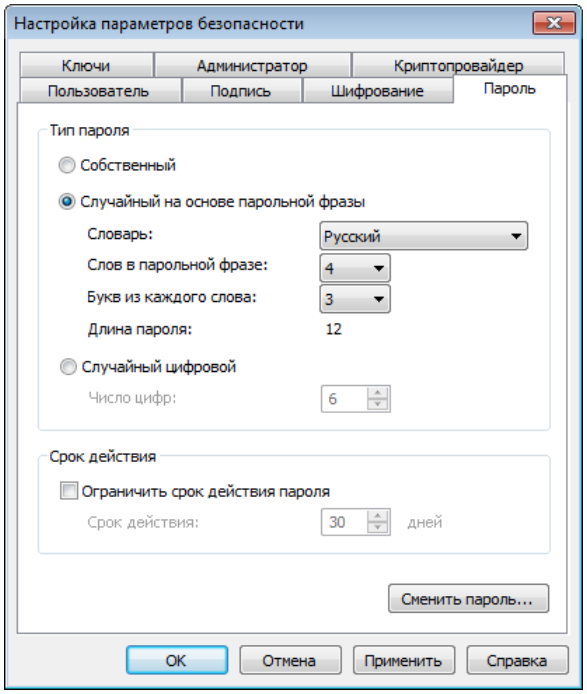


Рисунок 39: Смена текущего пароля пользователя

2 В группе **Тип пароля** выберите тот тип, которому должен соответствовать новый пароль:

- **Собственный** — пароль, определяемый пользователем (см. «Выбор собственного пароля» на стр. 128);
- **Случайный на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы, по заданным параметрам (см. «Выбор пароля на основе парольной фразы» на стр. 128);
- **Случайный цифровой** — пароль, формируемый автоматически из заданного числа цифр (см. «Выбор цифрового пароля» на стр. 129).

3 Нажмите кнопку **Сменить пароль.** Дальнейшие действия по смене пароля зависят от выбранного типа пароля и описаны в соответствующем разделе.

4 При необходимости ограничения срока действия нового пароля установите флажок **Ограничить срок действия пароля**, после чего укажите желаемое число дней.

5 Нажмите кнопку **ОК.**

Выбор собственного пароля

Для того чтобы сменить текущий пароль пользователя на собственный:

1. На вкладке **Пароль** (см. рисунок на стр. 127) выберите **Собственный**.
2. Нажмите кнопку **Сменить пароль**.
3. Выполните действия, предлагаемые в окне **Электронная рулетка**.

> **Примечание.** Если в рамках текущего сеанса электронная рулетка уже была запущена, данное окно не появится.

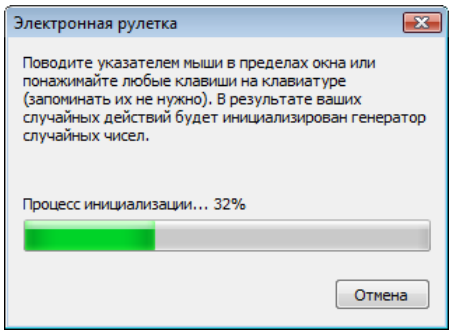


Рисунок 40: Электронная рулетка

4. В окне **Смена пароля** введите новый пароль (длиной не менее шести символов) поочередно в каждом из полей, учитывая регистр и раскладку клавиатуры.

   Нажмите кнопку **ОК**.

Теперь при запуске программы ViPNet Деловая почта от имени того же пользователя следует вводить указанный пароль.

Выбор пароля на основе парольной фразы

Для того чтобы сменить текущий пароль на случайный, составленный на основе парольной фразы:

1. На вкладке **Пароль** (см. рисунок на стр. 127) выберите **Случайный на основе парольной фразы**, после чего задайте параметры нового пароля:
   - В списке **Словарь** выберите язык парольной фразы.

- В списке **Слов в парольной фразе** выберите число слов (3, 4, 6 или 8), из которых будет состоять парольная фраза. Чем больше число слов, тем длиннее и, соответственно, надежнее будет пароль.
- В списке **Букв из каждого слова** выберите число начальных букв каждого слова (3 или 4), которые войдут в пароль.

В строке **Длина пароля** отобразится количество букв в пароле, который будет сформирован с учетом указанных параметров.

2 Нажмите кнопку **Сменить пароль**.

3 Запомните пароль (или парольную фразу), отображенный в окне **Смена пароля**.

При необходимости измените парольную фразу и пароль на другие, также соответствующие указанным параметрам, с помощью кнопки **Другой пароль**.

Нажмите кнопку **ОК**.

Теперь при запуске программы ViPNet Деловая почта от имени того же пользователя следует, используя английскую раскладку клавиатуры, вводить указанное число букв каждого слова русской парольной фразы, без пробелов. Например, для парольной фразы «тенор победил горемыку» с параметрами пароля по умолчанию (3 буквы из каждого слова) при запуске программы следует, используя английскую раскладку клавиатуры, вводить буквы «тенпобгор».

Выбор цифрового пароля

Для того чтобы сменить текущий пароль пользователя на цифровой:

1 На вкладке **Пароль** (см. рисунок на стр. 127) выберите **Случайный цифровой**, после чего в поле **Число цифр** укажите длину пароля.

2 Нажмите кнопку **Сменить пароль**.

3 Запомните цифровой пароль, предложенный в окне **Смена пароля**.

При необходимости измените этот пароль на другой, также содержащий указанное число цифр, с помощью кнопки **Другой ПИН-код**.

Нажмите кнопку **ОК**.

Теперь при запуске программы ViPNet Деловая почта от имени того же пользователя следует вводить предложенный цифровой пароль.

Настройка параметров шифрования

Вы можете настроить параметры шифрования исходящей информации. Для этого выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Шифрование**.

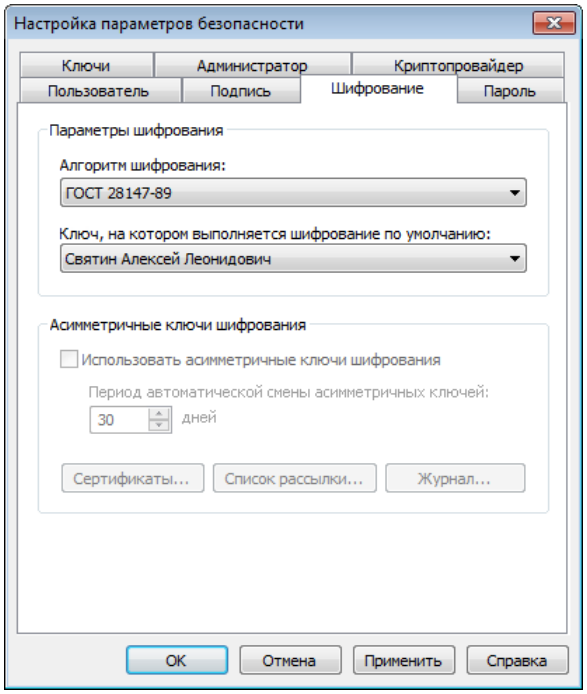


Рисунок 41: Настройка параметров шифрования

2 В списке **Алгоритм шифрования** выберите алгоритм, по которому будет осуществляться шифрование исходящей информации:

- ГОСТ 28147-89 (длина ключа 256 бит) — российский стандарт симметричного шифрования.
- AES (256 бит) — принятый в США стандарт симметричного шифрования на основе алгоритма Rijndael.

По умолчанию выбран алгоритм ГОСТ 28147-89. В соответствии с выбранным алгоритмом будет осуществляться как шифрование исходящего трафика, так и шифрование информации, передаваемой с помощью встроенных приложений ViPNet (например, программой ViPNet Деловая почта).

Внимание! В сертифицированной версии программы алгоритм AES не поддерживается, возможность его выбора отсутствует.

3 В следующем списке укажите ключи, на которых должно выполняться шифрование информации, передаваемой с помощью встроенных приложений ViPNet. Для шифрования могут быть выбраны как ключи, доступ к которым имеете только вы, так и ключи, доступные другим пользователям вашего узла (если такие есть). Просмотреть список пользователей, имеющих доступ к каким-либо ключам шифрования, вы можете на вкладке **Пользователь.**

Выбор ключей шифрования позволяет разграничить доступ пользователей, работающих на одном сетевом узле, к зашифрованной информации (например, письмам программы ViPNet Деловая почта). То есть если исходящее сообщение было зашифровано на ключах, доступных только вам, то другие пользователи, зарегистрированные на вашем узле, его прочитать не смогут.

4 Нажмите кнопку **OK**.

Настройка параметров криптопровайдера ViPNet CSP

В состав программного обеспечения ViPNet Деловая почта включена программа ViPNet CSP. ViPNet CSP представляет собой криптопровайдер, который обеспечивает вызов криптографических функций, реализованных в соответствии с российскими стандартами, через интерфейс Microsoft CryptoAPI 2.0. Это позволяет использовать российские криптографические алгоритмы в различных приложениях Microsoft и других программах, использующих данный интерфейс. Кроме этого, программа ViPNet CSP обеспечивает работу с контейнерами ключей (см. «Контейнер ключей» на стр. 207) и поддержку различных внешних устройств хранения ключей (см. «Внешние устройства» на стр. 199).

Чтобы настроить программу ViPNet CSP или задать параметры автоматической установки сертификатов в системное хранилище, выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Криптопровайдер**.

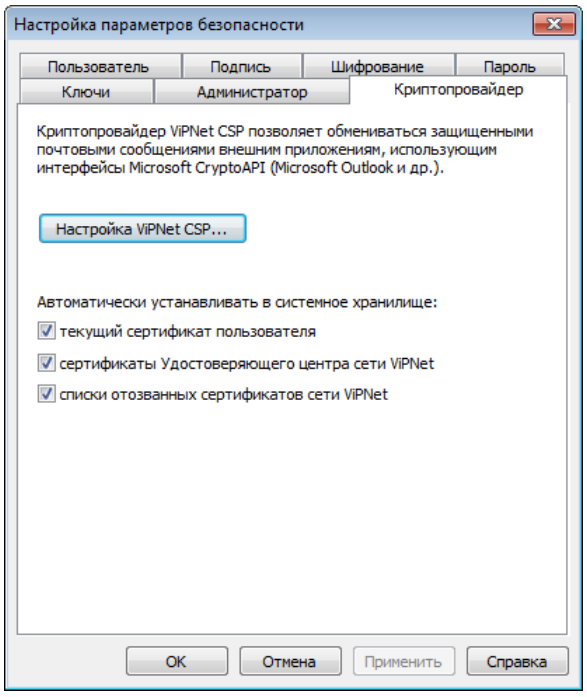


Рисунок 42: Настройка параметров криптопровайдера

2 Чтобы настроить программу ViPNet CSP, нажмите кнопку **Настройка ViPNet CSP**. Откроется окно **ViPNet CSP**, в котором вы можете:

- Задать необходимые параметры криптопровайдера.
- Выполнить операции с контейнерами ключей.
- Настроить параметры использования внешних устройств хранения данных — задать типы устройств, которые могут использоваться, выполнить инициализацию или изменить ПИН-код устройства.

Подробнее о настройке и работе с программой ViPNet CSP см. документ «ViPNet CSP. Руководство пользователя».

3 При необходимости укажите, какие сертификаты и списки отозванных сертификатов следует устанавливать в системное хранилище автоматически (см. «Установка в хранилище автоматически» на стр. 157), установив нужные флажки:

- **текущий сертификат пользователя** — для установки в системное хранилище Windows сертификата, который был назначен текущим;
- **сертификаты Удостоверяющего центра сети ViPNet —** для установки в системное хранилище Windows сертификатов издателей (корневых сертификатов), получаемых из программы ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager в составе обновления ключей;
- **списки отозванных сертификатов сети ViPNet** — для установки в системное хранилище списков отозванных сертификатов, получаемых из программы ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager в составе обновления ключей.

4 Выполнив необходимые настройки, нажмите кнопку **OK**.

8

Работа с сертификатами и ключами

Общие сведения о сертификатах открытых ключей

Определение и назначение

Сертификат открытого ключа является одним из объектов криптографии с открытым ключом, в которой для прямого и обратного преобразований используются разные ключи:

- Закрытый ключ — для формирования электронной подписи (см. «Электронная подпись» на стр. 211) и расшифрования сообщения. Закрытый ключ хранится в тайне и не подлежит распространению.
- Открытый ключ — для проверки электронной подписи и зашифрования сообщения. Открытый ключ известен всем участникам информационного обмена и может передаваться по незащищенным каналам связи.

Таким образом, криптография с открытым ключом позволяет выполнять следующие операции:

- Подписание сообщения — формирование электронной подписи, прикрепление ее к сообщению и проверка электронной подписи на стороне получателя;
- Шифрование — зашифрование документа с возможностью расшифрования на стороне получателя.

Открытый и закрытый ключи являются комплементарными по отношению друг к другу — только владелец закрытого ключа может подписать данные, а также расшифровать данные, которые были зашифрованы открытым ключом, соответствующим закрытому ключу владельца. Простой аналогией может служить почтовый ящик: любой может кинуть письмо в почтовый ящик («зашифровать»), но только владелец секретного (закрытого) ключа может извлечь письма из ящика («расшифровать»).

Поскольку открытый ключ распространяется публично, существует опасность того, что злоумышленник, подменив открытый ключ одного из пользователей, может выступать от его имени. Для обеспечения доверия к открытым ключам создаются удостоверяющие

центры (согласно Федеральному закону РФ № 63 «Об электронной подписи» от 6 апреля 2011 года), которые играют роль доверенной третьей стороны и заверяют открытые ключи каждого из пользователей своими электронными подписями — иначе говоря, сертифицируют эти открытые ключи.

Сертификат открытого ключа (далее — сертификат) представляет собой цифровой документ, заверенный электронной подписью удостоверяющего центра и призванный подтверждать принадлежность открытого ключа определенному пользователю.

Примечание. Несмотря на то, что защита сообщений выполняется фактически с помощью открытого ключа, в профессиональной речи используются выражения «подписать сертификатом (с помощью сертификата)», «зашифровать на сертификате (с помощью сертификата)».

Сертификат включает открытый ключ и список дополнительных атрибутов, принадлежащих пользователю (владельцу сертификата). К таким атрибутам относятся: имена владельца и издателя сертификата, номер сертификата, время действия сертификата, предназначение открытого ключа (электронная подпись, шифрование) и так далее. Структура и протоколы использования сертификатов определяются международными стандартами (см. «Структура» на стр. 138).

Различаются следующие виды сертификатов:

- Сертификат пользователя — для зашифрования исходящих сообщений и для проверки электронной подписи на стороне получателя.
- Сертификат издателя — сертификат, с помощью которого был издан текущий сертификат пользователя. Помимо основных возможностей, которые предоставляет сертификат пользователя, сертификат издателя позволяет также проверить все сертификаты, подписанные с помощью закрытого ключа, соответствующего этому сертификату.
- Корневой сертификат — самоподписанный сертификат издателя, являющийся главным из вышестоящих сертификатов. Корневой сертификат не может быть проверен с помощью другого сертификата, поэтому пользователь должен безусловно доверять источнику, из которого получен данный сертификат.
- Кросс-сертификат — это сертификат администратора удостоверяющего центра, изданный администратором другого удостоверяющего центра. Таким образом, для кросс-сертификата значения полей «Издатель» и «Субъект» различны и определяют разные удостоверяющие центры. С помощью кросс-сертификатов устанавливаются доверительные отношения между различными удостоверяющими центрами. В зависимости от модели доверительных отношений, установленной между удостоверяющими центрами (см. «Роль PKI для криптографии с открытым

ключом» на стр. 141), может использоваться либо как сертификат издателя (в иерархической модели), либо для проверки сертификатов пользователей другой сети (в распределенной модели).

Рисунок 43: Типы сертификатов

Используя корневой сертификат, каждый пользователь может проверить достоверность сертификата, выпущенного удостоверяющим центром, и воспользоваться его содержимым. Если проверка сертификата по цепочке сертификатов, начиная с корневого, показала, что он является законным, действующим, не был просрочен или отозван, то сертификат считается действительным. Документы, подписанные действительным сертификатом и не изменявшиеся с момента их подписания, также считаются действительными.

Таким образом, криптография с открытым ключом и инфраструктура обмена сертификатами открытых ключей (см. «Роль PKI для криптографии с открытым ключом» на стр. 141) позволяют выполнять шифрование сообщений, а также предоставляют возможность подписывать сообщения с помощью электронной подписи.

Посредством шифрования конфиденциальная информация может быть передана по незащищенным каналам связи. В свою очередь, электронная подпись позволяет обеспечить:

- Подлинность (аутентификация) — возможность однозначно идентифицировать отправителя. Если сравнивать с бумажным документооборотом, то это аналогично собственноручной подписи отправителя.
- Целостность — защиту информации от несанкционированной модификации как при хранении, так и при передаче.
- Неотрекаемость — невозможность для отправителя отказаться от совершенного действия. Если сравнивать с бумажным документооборотом, то это аналогично предъявлению отправителем паспорта перед выполнением действия.

Структура

Чтобы сертификат можно было использовать, он должен обладать доступной универсальной структурой, позволяющей извлечь из него нужную информацию и легко ее понять. Например, благодаря тому, что паспорта имеют простую однотипную структуру, можно легко понять информацию, изложенную в паспорте любого государства, даже если вы никогда не видели раньше таких паспортов. Так же дело обстоит и с сертификатами: стандартизация форматов сертификатов позволяет читать и понимать их независимо от того, кем они были изданы.

Один из форматов сертификата открытого ключа определен в рекомендациях Международного Союза по телекоммуникациям (International Telecommuncations Union, ITU) X.509 | ISO/IEC 9594–8 и документе RFC 3280 Certificate & CRL Profile Организации инженерной поддержки Интернета (Internet Engineering Task Force, IETF). В настоящее время наиболее распространенной версией X.509 является версия 3, позволяющая задать для сертификата расширения, с помощью которых можно разместить в сертификате дополнительную информацию (о политиках безопасности, использовании ключа, совместимости и так далее).

Сертификат содержит элементы данных, сопровождаемые электронной подписью издателя сертификата. В сертификате имеются обязательные и дополнительные поля.

К обязательным полям относятся:

- номер версии стандарта X.509,
- серийный номер сертификата,
- идентификатор алгоритма подписи издателя,

- идентификатор алгоритма подписи владельца,
- имя издателя,
- период действия,
- открытый ключ владельца,
- имя владельца сертификата.

Примечание. Под владельцем понимается сторона, контролирующая закрытый ключ, соответствующий данному открытому ключу. Владельцем сертификата может быть конечный пользователь или удостоверяющий центр.

К необязательным полям относятся:

- уникальный идентификатор издателя,
- уникальный идентификатор владельца,
- расширения сертификата.

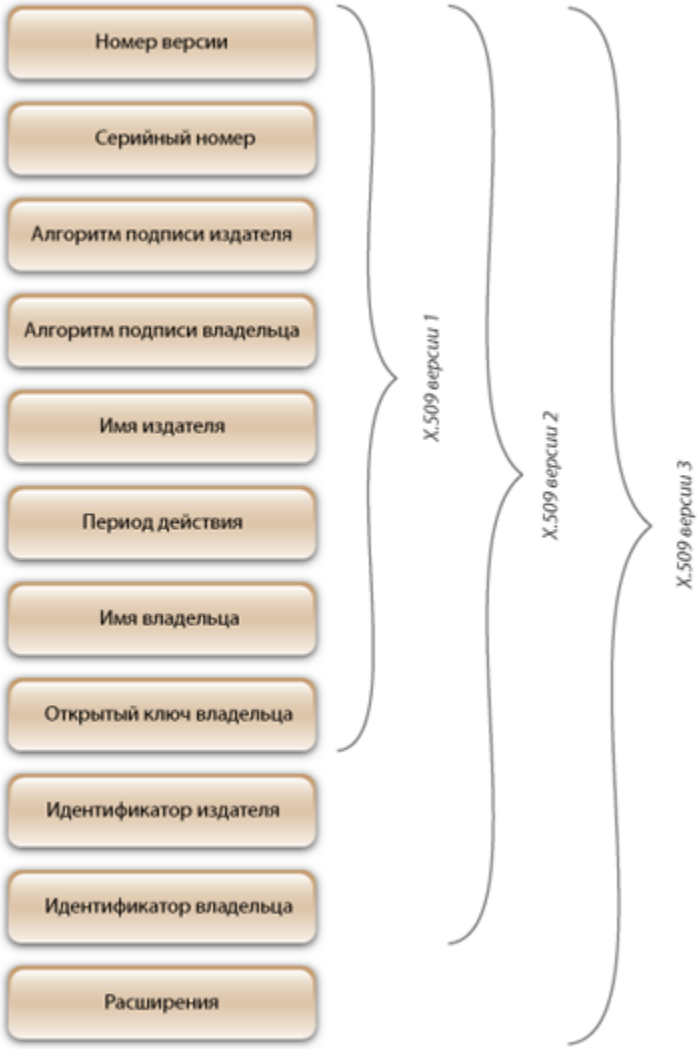
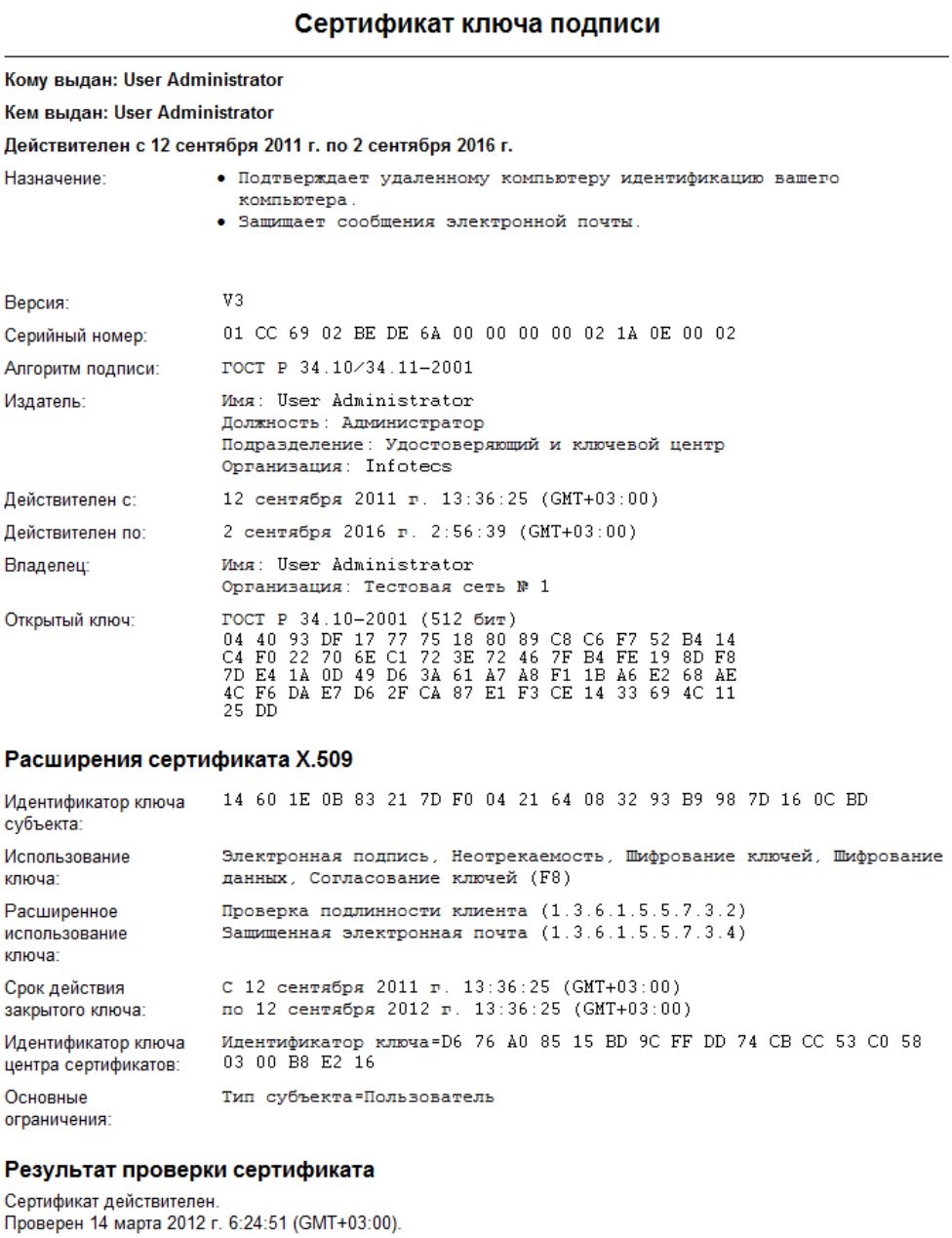


Рисунок 44: Структура сертификата, соответствующего стандарту X.509 версий 1, 2 и 3



Сертификат ключа подписи

Кому выдан: User Administrator

Кем выдан: User Administrator

Действителен с 12 сентября 2011 г. по 2 сентября 2016 г.

Назначение:
- Подтверждает удаленному компьютеру идентификацию вашего компьютера.
- Защищает сообщения электронной почты.

Версия:	V3
Серийный номер:	01 CC 69 02 BE DE 6A 00 00 00 00 02 1A 0E 00 02
Алгоритм подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Имя: User Administrator Должность: Администратор Подразделение: Удостоверяющий и ключевой центр Организация: Infotecs
Действителен с:	12 сентября 2011 г. 13:36:25 (GMT+03:00)
Действителен по:	2 сентября 2016 г. 2:56:39 (GMT+03:00)
Владелец:	Имя: User Administrator Организация: Тестовая сеть № 1
Открытый ключ:	ГОСТ Р 34.10-2001 (512 бит) 04 40 93 DF 17 77 75 18 80 89 C8 C6 F7 52 B4 14 C4 F0 22 70 6E C1 72 3E 72 46 7F B4 FE 19 8D F8 7D E4 1A 0D 49 D6 3A 61 A7 A8 F1 1B A6 E2 68 AE 4C F6 DA E7 D6 2F CA 87 E1 F3 CE 14 33 69 4C 11 25 DD

Расширения сертификата X.509

Идентификатор ключа субъекта:	14 60 1E 0B 83 21 7D F0 04 21 64 08 32 93 B9 98 7D 16 0C BD
Использование ключа:	Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8)
Расширенное использование ключа:	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Срок действия закрытого ключа:	С 12 сентября 2011 г. 13:36:25 (GMT+03:00) по 12 сентября 2012 г. 13:36:25 (GMT+03:00)
Идентификатор ключа центра сертификатов:	Идентификатор ключа=D6 76 A0 85 15 BD 9C FF DD 74 CB CC 53 C0 58 03 00 B8 E2 16
Основные ограничения:	Тип субъекта=Пользователь

Результат проверки сертификата

Сертификат действителен.
Проверен 14 марта 2012 г. 6:24:51 (GMT+03:00).

Рисунок 45: Пример сертификата ViPNet, соответствующего стандарту X.509 версии 3

Роль PKI для криптографии с открытым ключом

Для сертификатов требуется инфраструктура, которая позволяла бы управлять ими в той среде, в которой эти сертификаты предполагается использовать. Одной из реализаций такой инфраструктуры является технология PKI (Public Key Infrastructure — инфраструктура открытых ключей). PKI обслуживает жизненный цикл сертификата:

издание сертификатов, хранение, резервное копирование, печать, взаимную сертификацию, ведение списков отозванных сертификатов (СОС), автоматическое обновление сертификатов после истечения срока их действия.

Основой технологии PKI являются отношения доверия, а главным управляющим компонентом — удостоверяющий центр. Удостоверяющий центр предназначен для регистрации пользователей, выпуска сертификатов, их хранения, выпуска СОС и поддержания его в актуальном состоянии. В сетях ViPNet удостоверяющий центр издает сертификаты как по запросам от пользователей, сформированным в специальной программе (например, ViPNet CSP или ViPNet Client), так и без запросов (в процессе создания пользователей ViPNet).

Для сетей с большим количеством пользователей создается несколько удостоверяющих центров. Доверительные отношения между этими удостоверяющими центрами могут выстраиваться по распределенной или иерархической модели.

- В иерархической модели доверительных отношений удостоверяющие центры объединяются в древовидную структуру, в основании которой находится головной удостоверяющий центр. Головной удостоверяющий центр выдает кросс-сертификаты подчиненным ему центрам, тем самым обеспечивая доверие к открытым ключам этих центров. Каждый удостоверяющий центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие к сертификату открытого ключа каждого удостоверяющего центра основано на заверении его ключом вышестоящего центра. Сертификат головного удостоверяющего центра (корневой сертификат (на стр. 208)) является самоподписанным. В остальных удостоверяющих центрах администраторы не имеют собственных корневых сертификатов и для установления доверительных отношений формируют запросы на кросс-сертификат к своим вышестоящим удостоверяющим центрам.

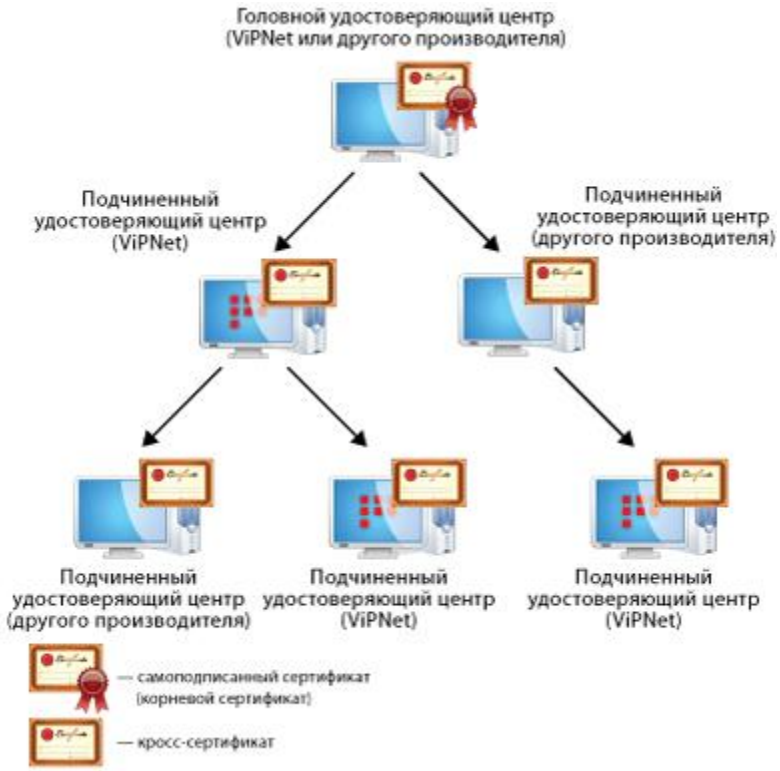


Рисунок 46: Иерархическая модель доверительных отношений

- В распределенной модели доверительных отношений все удостоверяющие центры равнозначны: в каждом удостоверяющем центре администратор имеет свой корневой (самоподписанный) сертификат. Доверительные отношения между удостоверяющими центрами в этой модели устанавливаются обычно путем двусторонней кросс-сертификации, когда два удостоверяющих центра издают кросс-сертификаты друг для друга. Взаимная кросс-сертификация проводится попарно между всеми удостоверяющими центрами. В результате в каждом удостоверяющем центре в дополнение к корневому сертификату имеются кросс-сертификаты, изданные для администраторов в других удостоверяющих центрах.

  Для подписания сертификатов пользователей каждый удостоверяющий центр продолжает пользоваться своим корневым сертификатом, а кросс-сертификат, изданный для другого удостоверяющего центра, использует для проверки сертификатов пользователей другой сети. Это возможно в силу того, кросс-сертификат для доверенного удостоверяющего центра издается на базе его корневого сертификата и содержит сведения о его открытом ключе. Поэтому в сети, отправившей запрос, нет необходимости переиздавать сертификаты пользователей.

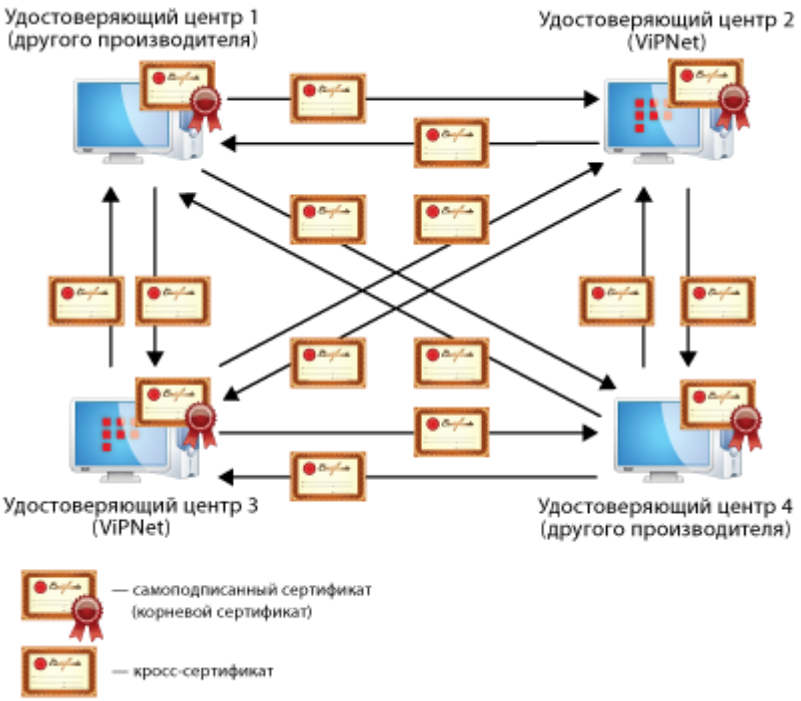


Рисунок 47: Распределенная модель доверительных отношений

Зная иерархию и подчиненность удостоверяющих центров друг другу, можно всегда точно установить, является ли тот или иной пользователь владельцем данного открытого ключа.

Использование сертификатов для шифрования электронных документов

Отправитель может зашифровать документ с помощью открытого ключа получателя, при этом расшифровать документ сможет только сам получатель. В данном случае для зашифрования применяется сертификат получателя сообщения.

Зашифрование

1. Пользователь создает электронный документ.
2. Открытый ключ получателя извлекается из сертификата.
3. Формируется симметричный сеансовый ключ (на стр. 209), для однократного использования в рамках данного сеанса.

4 Подписанный документ зашифровывается с использованием сеансового ключа (в соответствии с алгоритмом ГОСТ 28147–89).

5 Сеансовый ключ зашифровывается на ключе, который вырабатывается по протоколу Диффи — Хеллмана (см. «Протокол Диффи — Хеллмана» на стр. 209) с использованием открытого ключа получателя.

6 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

7 Документ отправляется.

Рисунок 48: Процесс зашифрования электронных документов

Расшифрование

1 Пользователь получает электронный документ.

2 Зашифрованное содержимое документа и зашифрованный сеансовый ключ извлекаются из документа.

3 Закрытый ключ получателя документа извлекается из контейнера ключей.

4 Сеансовый ключ расшифровывается с использованием закрытого ключа получателя.

5 Документ расшифровывается с использованием расшифрованного сеансового ключа.

6 Расшифрованный документ доступен получателю.

Рисунок 49: Процесс расшифрования электронных документов

Использование сертификатов для подписания электронных документов

Когда отправитель подписывает документ, он использует закрытый ключ, соответствующий открытому ключу, который хранится в сертификате. Когда получатель проверяет электронную подпись (см. «Электронная подпись» на стр. 211) сообщения, он извлекает открытый ключ из сертификата отправителя.

Подписание

1. Пользователь создает электронный документ.
2. Вычисляется значение хэш-функции документа.

   Хэш-функция документа используется при формировании электронной подписи на стороне отправителя, а также при дальнейшей проверке электронной подписи на стороне получателя.
3. Закрытый ключ отправителя извлекается из контейнера ключей.
4. С использованием закрытого ключа отправителя на основе значения хэш-функции формируется электронная подпись.
5. Электронная подпись прикрепляется к документу.
6. Зашифрованный документ отправляется.

Рисунок 50: Процесс подписания электронного документа

Проверка подписи

1. Пользователь получает электронный документ.
2. Электронная подпись (зашифрованное значение хэш-функции) извлекается из документа.
3. Вычисляется значение хэш-функции документа.
4. Открытый ключ отправителя извлекается из сертификата отправителя.
5. Электронная подпись расшифровывается с использованием открытого ключа отправителя.
6. Значение хэш-функции электронной подписи сравнивается с полученным значением хэш-функции документа.
7. Если значения хэш-функций совпадают, электронная подпись документа считается действительной.

   Если значения хэш-функций не совпадают (то есть полученный документ был изменен с момента подписания), электронная подпись документа считается недействительной. Подпись считается недействительной также в том случае, если сертификат отправителя просрочен, отозван, искажен или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

Рисунок 51: Процесс проверки подписи

Использование сертификатов для подписания и шифрования электронных документов

Подписание и зашифрование

1. Пользователь создает электронный документ.
2. Вычисляется значение хэш-функции документа.
3. Закрытый ключ отправителя извлекается из контейнера ключей.
4. Открытый ключ получателя извлекается из сертификата получателя.
5. С использованием закрытого ключа отправителя на основе значения хэш-функции формируется электронная подпись.
6. Электронная подпись прикрепляется к документу.
7. Формируется симметричный сеансовый ключ (на стр. 209), для однократного использования в рамках данного сеанса.
8. Подписанный документ зашифровывается с использованием сеансового ключа (в соответствии с алгоритмом ГОСТ 28147–89).

9 Сеансовый ключ зашифровывается на ключе, который вырабатывается по протоколу Диффи — Хеллмана (см. «Протокол Диффи — Хеллмана» на стр. 209) с использованием открытого ключа получателя.

10 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

11 Документ отправляется.

Рисунок 52: Процесс подписания и зашифрования электронных документов

Расшифрование и проверка

1 Пользователь получает электронный документ.

2 Зашифрованное содержимое документа и зашифрованный сеансовый ключ извлекаются из сообщения.

3 Закрытый ключ получателя документа извлекается из контейнера ключей.

4 Сеансовый ключ расшифровывается с помощью закрытого ключа получателя.

5 Документ расшифровывается с использованием расшифрованного сеансового ключа.

6 Электронная подпись (зашифрованное значение хэш-функции) извлекается из документа.

7 Вычисляется значение хэш-функции документа.

8 Открытый ключ отправителя извлекается из сертификата отправителя.

9 Электронная подпись расшифровывается с использованием открытого ключа отправителя.

10 Значение хэш-функции электронной подписи сравнивается с полученным значением хэш-функции документа.

11 Если значения хэш-функций совпадают, электронная подпись документа считается действительной.

Если значения хэш-функций не совпадают (то есть полученный документ был изменен с момента подписания), электронная подпись документа считается недействительной. Подпись считается недействительной также в том случае, если сертификат отправителя просрочен, отозван, искажен или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

12 Расшифрованный документ доступен получателю.

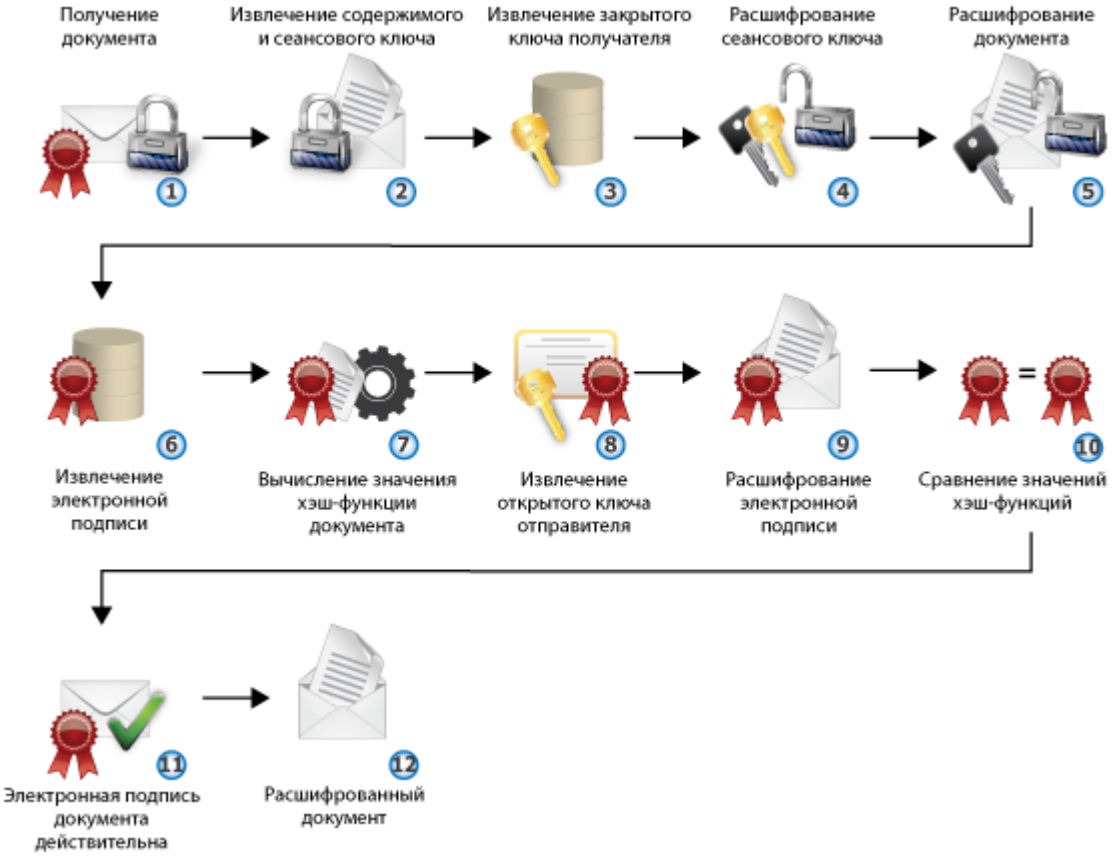


Рисунок 53: Процесс расшифрования и проверки электронного документа

Просмотр сертификатов

Просмотр сертификата может потребоваться при необходимости получения более подробной информации о сертификате — о назначении сертификата, о его издателе, составе полей, причине недействительности сертификата и так далее.

В программе ViPNet Деловая почта можно просматривать следующие типы сертификатов:

- текущий сертификат пользователя (см. «Просмотр текущего сертификата пользователя» на стр. 152),
- личные сертификаты пользователя (см. «Просмотр личных сертификатов пользователя» на стр. 152),
- доверенные корневые сертификаты (см. «Просмотр доверенных корневых сертификатов» на стр. 153),
- изданные сертификаты (см. «Просмотр изданных сертификатов» на стр. 153).

Основная информация о выбранном сертификате отображается в окне **Сертификат** на вкладке **Общие**:

- назначение сертификата или (для недействительных сертификатов) причина недействительности сертификата;
- имя владельца открытого ключа, которому выдан сертификат;
- имя издателя сертификата;
- срок действия сертификата;
- срок действия закрытого ключа, соответствующего данному сертификату (только для сертификатов пользователей);
- информация о политиках применения сертификата, отображаемая при нажатии кнопки **Заявление издателя**.

Примечание. В сертификате пользователя сети ViPNet CUSTOM кнопка **Заявление издателя** доступна только в том случае, если политики применения были присвоены сертификату при его издании в программе ViPNet

Удостоверяющий и ключевой центр.

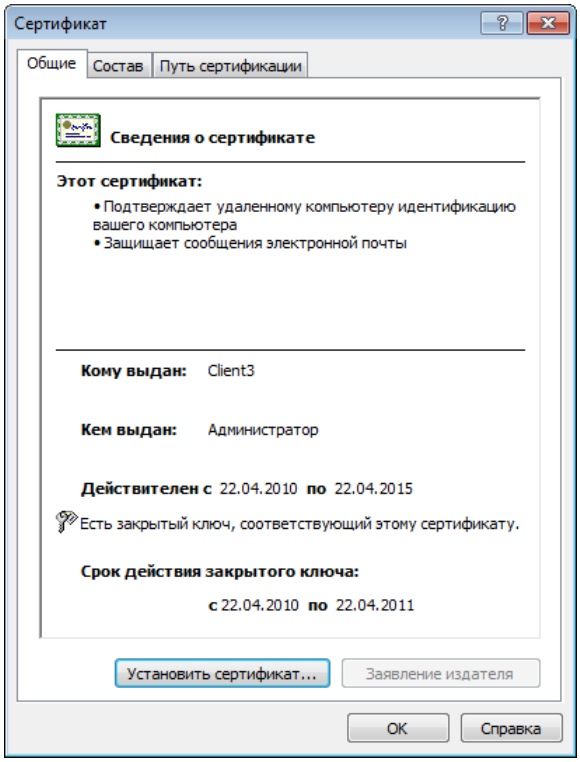


Рисунок 54: Просмотр основной информации о сертификате

Просмотр текущего сертификата пользователя

Для просмотра текущего сертификата пользователя в окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Подробнее**.

Откроется окно **Сертификат** с информацией о сертификате, который используется в качестве текущего.

Просмотр личных сертификатов пользователя

Для просмотра личных сертификатов пользователя:

1. В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Сертификаты**.

Откроется окно **Менеджер сертификатов** с информацией обо всех личных сертификатах пользователя, а также о сертификатах, установленных в хранилище операционной системы. Все данные сертификаты введены в действие.

Примечание. Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование внешних сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 122).

2 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или дважды щелкните этот сертификат.

Откроется окно **Сертификат** с информацией о выбранном личном сертификате.

Просмотр доверенных корневых сертификатов

Для просмотра доверенных корневых сертификатов:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Сертификаты**.

2 В окне **Менеджер сертификатов** откройте вкладку **Доверенные корневые сертификаты**.

3 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или дважды щелкните этот сертификат.

Откроется окно **Сертификат** с информацией о выбранном корневом сертификате.

Просмотр изданных сертификатов

Для просмотра изданных сертификатов:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Изданные сертификаты**.

Откроется окно **Менеджер сертификатов** с информацией о сертификатах, которые изданы в программе ViPNet Удостоверяющий и ключевой центр по запросам пользователей или по инициативе администратора УКЦ, но еще не введены в действие.

2 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или дважды щелкните этот сертификат.

Откроется окно **Сертификат** с информацией о выбранном изданном сертификате.

Просмотр цепочки сертификации

Для просмотра цепочки сертификации (см. «Цепочка сертификации» на стр. 211) определенного сертификата:

1 Вызовите окно **Сертификат** для того сертификата, цепочку сертификации которого необходимо просмотреть.

2 Откройте вкладку **Путь сертификации**.

На данной вкладке отображаются сертификаты, образующие иерархию издателей того сертификата, для которого вызвано окно **Сертификат**, а также информация об их статусе.

3 При необходимости просмотра более подробной информации о сертификате одного из издателей выберите нужный сертификат, после чего нажмите кнопку **Просмотр сертификата** или выполните двойной щелчок мыши для этого сертификата.

Откроется окно **Сертификат** с информацией о выбранном сертификате.

Просмотр полей сертификата и печать сертификата

Для просмотра полей определенного сертификата:

1 Вызовите окно **Сертификат** для того сертификата, состав полей которого необходимо просмотреть.

2 Откройте вкладку **Состав**.

По умолчанию на данной вкладке отображается перечень всех полей сертификата.

3 Для ограничения количества просматриваемых полей выберите нужную группу полей в выпадающем списке **Показать:**

- **Только поля V1** — все поля, кроме расширений;
- **Только расширения** — дополнительные поля сертификата, соответствующего стандарту X.509 версии 3;

Примечание. Расширение **Срок действия закрытого ключа** отображается в том случае, если срок действия сертификата превышает 1 год. Если срок действия сертификата превышает 1 год, то срок действия закрытого ключа составляет ровно 1 год.

- **Только критические расширения** — только те расширения, которые признаны издателем критическими;
- **Только свойства** — параметры, которые не являются полями сертификата, но присваиваются сертификату при хранении его в системном хранилище используемой рабочей станции.

4 Выберите в таблице нужное поле, после чего в нижней части окна ознакомьтесь с содержимым этого поля.

Для отправки сертификата на принтер, используемый по умолчанию на текущей рабочей станции, нажмите кнопку **Печать**.

Управление сертификатами

Возможности программы ViPNet Деловая почта по управлению сертификатами с помощью окна **Настройка параметров безопасности** представлены в таблице.

Функциональная возможность	Ссылка
Установка сертификатов в хранилище. Возможна настройка параметров автоматической установки сертификатов в хранилище, а также установка сертификатов в хранилище вручную	Установка в хранилище автоматически (на стр. 157) Установка в хранилище вручную (на стр. 159)
Смена текущего сертификата. Можно выбрать другой сертификат (из числа действительных личных сертификатов пользователя) в качестве текущего.	Смена текущего сертификата (на стр. 162)
Обновление закрытого ключа и сертификата. Можно настроить параметры автоматического оповещения об истечении срока действия текущего сертификата и соответствующего ему закрытого ключа, а также, при необходимости, сформировать запрос на обновление этого сертификата и закрытого ключа.	Настройка оповещения об истечении срока действия закрытого ключа и сертификата (на стр. 165) Процедура обновления закрытого ключа и сертификата (на стр. 165)
Ввод сертификата в действие. Если требуется использовать сертификат, переданный на данный сетевой узел, необходимо ввести этот сертификат в действие. Можно настроить параметры автоматического ввода сертификатов в действие или выполнить ввод в действие вручную.	Ввод сертификата в действие (на стр. 172) Ввод в действие автоматически (на стр. 173) Ввод в действие вручную (на стр. 173)
Просмотр и удаление запросов на сертификаты. Можно просмотреть состояние запросов на сертификаты, сформированных текущим пользователем, а также удалить ненужные запросы.	Работа с запросами на сертификаты (на стр. 174) Просмотр запроса на сертификат (на стр. 174) Удаление запроса на сертификат (на стр. 175)
Экспорт сертификата. В зависимости от целей использования сертификата за пределами ПО ViPNet, сертификат может быть экспортирован в файлы различных форматов.	Экспорт сертификата (на стр. 176)

Установка сертификатов в хранилище

Установка сертификатов в хранилище позволяет использовать сертификаты во внешних приложениях (таких как Windows Live Mail, Microsoft Outlook, Microsoft Word и других). Можно установить сертификат в хранилище операционной системы или хранилище программы ViPNet Деловая почта (в папку `D_STATION`, находящуюся в папке установки).

Установку можно выполнить автоматически или вручную.

Внимание! При установке сертификата в хранилище ОС Windows Vista или Windows Server 2008 следует запускать программу ViPNet Деловая почта от имени администратора ОС (с помощью команды **Запуск от имени администратора** (**Run as Administrator**) контекстного меню ярлыка).

Установка в хранилище автоматически

Установка сертификатов запускается автоматически при соблюдении следующих двух условий:

- сертификаты (текущий сертификат пользователя, корневой сертификат и списки отозванных сертификатов) отсутствуют в хранилище;
- в окне **Настройка параметров безопасности** на вкладке **Криптопровайдер** установлены флажки группы **Автоматически устанавливать в системное хранилище.**

Примечание. В автоматическом режиме выполняется установка сертификатов в хранилище текущего пользователя.

Следует иметь в виду, что автоматическая установка корневого сертификата может занимать продолжительное время в зависимости от используемой программы ViPNet:

- В программе ViPNet Монитор опрос параметров выполняется через пять минут после запуска и далее с 2-часовым интервалом. При открытом окне **Настройка параметров безопасности** интервал опроса сокращается до 10–15-ти минут.
- В программах ViPNet Деловая почта и ViPNet CryptoService опрос параметров выполняется с интервалом 30–60 минут.

Для автоматической установки текущего сертификата пользователя и списков отозванных сертификатов (при соблюдении приведенных выше условий) не требуется никаких дополнительных действий со стороны пользователя.

Для автоматической установки корневого сертификата:

1 При появлении окна **Установка корневого сертификата**:

Примечание. Окно **Установка корневого сертификата** появляется тогда, когда корневой сертификат отсутствует в хранилище сертификатов Windows. Это может произойти в следующих случаях:

- При первичном запуске ПО ViPNet после развертывания сетевого узла.
- Если получено обновление текущего сертификата пользователя, содержащее новый корневой сертификат.

- чтобы выполнить автоматическую установку сертификата, нажмите кнопку **OK**;
- если автоматическая установка корневого сертификата и других сертификатов не требуется, установите флажок **Отключить автоматическую установку сертификатов**, после чего нажмите кнопку **OK**.

Примечание. В окне **Настройка параметров безопасности** на вкладке **Криптопровайдер** флажки группы **Автоматически устанавливать в системное хранилище** будут также сняты.

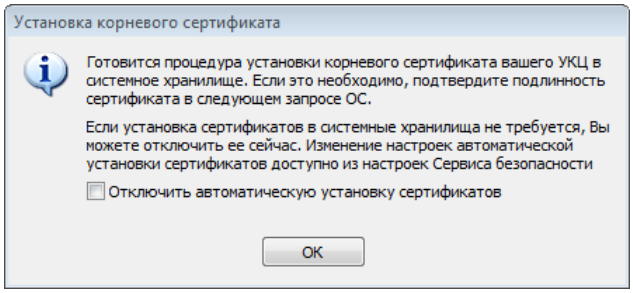


Рисунок 55: Установка корневого сертификата

2 Если автоматическая установка сертификатов не была прервана, в окне запроса на добавление сертификата в хранилище проверьте подлинность сертификата, после чего нажмите кнопку **Да**.

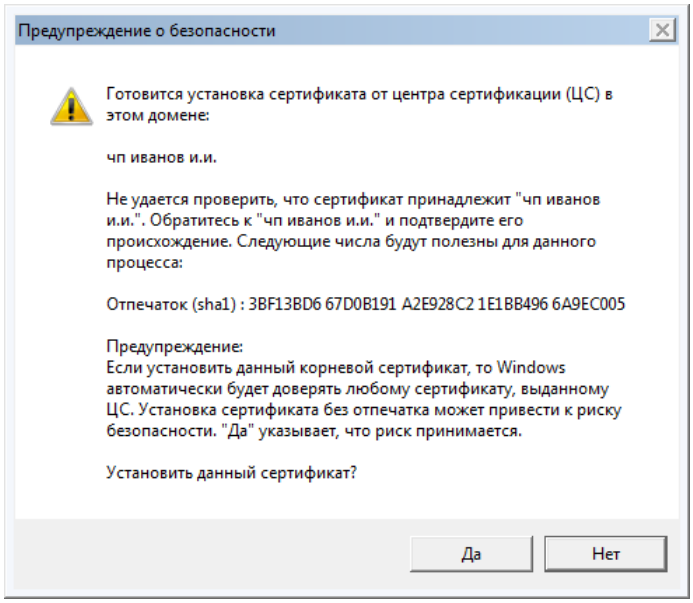


Рисунок 56: Подтверждение подлинности корневого сертификата

Корневой сертификат установлен в хранилище сертификатов текущего пользователя.

Установка в хранилище вручную

Для работы с защищенными документами необходим закрытый ключ и соответствующий ему сертификат. Установка ключа и сертификата может выполняться путем установки одного контейнера или путем установки сертификата и контейнера ключей по отдельности.

Если у вас имеется закрытый ключ и вам необходимо сформировать на его базе сертификат (или обновить уже имеющийся) — направьте в Удостоверяющий центр запрос на сертификат.

Внимание! Для работы с защищенными документами, помимо сертификата пользователя, необходимо также установить в хранилище корневой сертификат (издателя) и СОС.

Сертификат можно установить отдельно и сопоставить его с персональным закрытым ключом.

Для установки сертификата в хранилище пользователя:

1. Вызовите окно **Сертификаты** для того сертификата, который необходимо установить в хранилище (см. «Просмотр сертификатов» на стр. 151).
2. Нажмите кнопку **Установить сертификат**.
3. На странице приветствия мастера установки сертификатов нажмите кнопку **Далее**.
4. На странице **Выбор хранилища сертификатов** выполните следующие действия:
   - Укажите, в какое хранилище будет установлен ваш сертификат.
   - Если в файле с расширением `*p7b` или `*p7s` помимо сертификата также содержатся сертификаты издателей и СОС для их установки установите соответствующие флажки.

   Нажмите кнопку **Далее**.

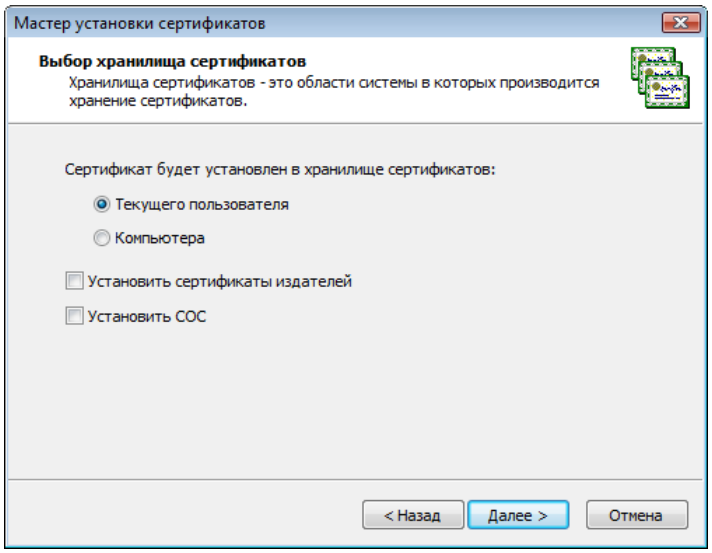


Рисунок 57: Выбор хранилища сертификатов

Примечание. Сертификат следует устанавливать в хранилище текущего пользователя для целей шифрования, расшифрования и подписания файлов, а также для доступа к защищенным ресурсам через веб-браузер. В хранилище компьютера следует устанавливать сертификаты, которые будут использоваться службами данного компьютера.

Сертификат следует устанавливать в хранилище компьютера при использовании ViPNet Деловая почта на веб-сервере для организации доступа к защищенным ресурсам.

Если возможность установки сертификата в хранилище компьютера недоступна, войдите в систему с правами администратора.

---

5 На странице **Готовность к установке сертификата**:

- Проверьте правильность выбранных параметров. При необходимости вернитесь на предыдущую страницу мастера с помощью кнопки **Назад** и выберите другие параметры.

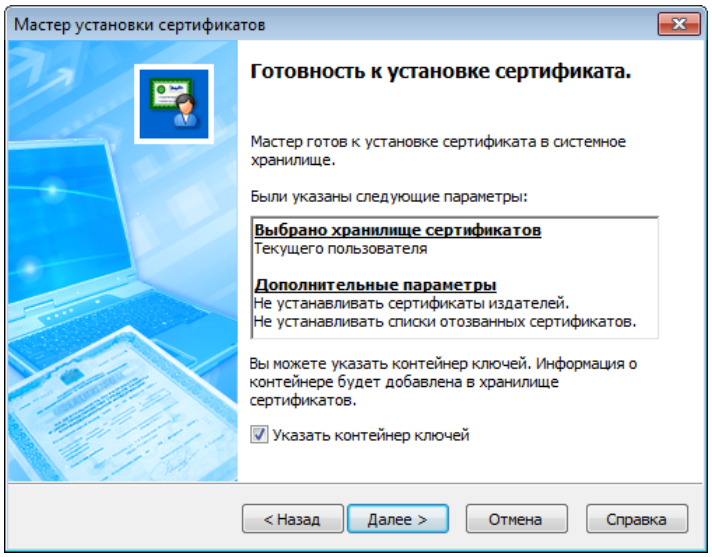


Рисунок 58: Сертификат готов к установке

- Если сертификат хранится в файле отдельно от закрытого ключа, установите флажок **Указать контейнер ключей**.

Примечание. Флажок **Указать контейнер ключей** можно не устанавливать. В этом случае необходимо указать расположение контейнера позже, после завершения работы мастера установки сертификата.

- Нажмите кнопку **Далее**.

6 Если флажок **Указать контейнер ключей** установлен и контейнер не найден либо недоступен, в появившемся окне **ViPNet CSP – инициализация контейнера ключей** укажите расположение контейнера ключей:

- папку на диске;
- устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 199).

После этого нажмите кнопку **OK**.

7 В окне подтверждения нажмите кнопку **Да**, чтобы добавить сертификат в контейнер ключей, или кнопку **Нет**, чтобы оставить сертификат в виде отдельного файла.

Совет. Сохранение сертификата в одном контейнере с закрытым ключом удобно, если контейнер планируется переносить и устанавливать на другом компьютере.

8 Если флажок **Указать контейнер ключей** установлен и контейнер доступен, в появившемся окне **ViPNet CSP – пароль контейнера ключей** в поле **Пароль** введите пароль доступа к контейнеру, после чего нажмите кнопку **OK**.

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

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

Сертификат установлен в выбранное хранилище сертификатов. В случае если в процессе установки сертификата ему не был сопоставлен закрытый ключ, необходимо установить контейнер ключей, соответствующий этому сертификату (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 187).

Смена текущего сертификата

Если у вас есть несколько действительных личных сертификатов, вы можете использовать любой из них в качестве текущего.

Внимание! Если при обновлении сертификата новый сертификат, изданный по запросу пользователя, передан на сетевой узел в составе ключей пользователя, то для использования такого сертификата необходимо выбрать его в качестве текущего.

Для выбора действительного личного сертификата в качестве текущего:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Выбрать**.

Если у вас есть хотя бы один действительный личный сертификат, появится окно **Выбор сертификата** с информацией обо всех личных сертификатах, а также о сертификатах, установленных в хранилище операционной системы.

Примечание. Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование внешних сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 122).

Если не найден ни один действительный личный сертификат, появится окно с сообщением «Нет действительных сертификатов с действительным закрытым ключом».

2 В окне **Выбор сертификата** выберите нужный сертификат, при необходимости воспользовавшись кнопкой **Свойства** для просмотра подробной информации о сертификате, после чего нажмите кнопку **ОК**.

Примечание. В качестве текущего можно использовать только тот действительный личный сертификат, который введен в действие. Изданный, но не введенный в действие личный сертификат необходимо сначала ввести в действие (см. «Ввод сертификата в действие» на стр. 172), а затем назначить текущим.

При успешном выполнении описанных действий выбранный сертификат назначается текущим. При этом на вкладке **Ключи** (см. рисунок на стр. 182) в группе **Подпись** меняется информация о контейнере ключей, в котором хранится выбранный сертификат.

Обновление закрытого ключа и сертификата

Сертификат открытого ключа и закрытый ключ имеют ограниченный срок действия, поэтому их требуется регулярно обновлять. При обновлении сертификата также обновляется закрытый ключ.

Обновление сертификата и закрытого ключа, который соответствует данному сертификату, требуется в следующих случаях:

- Истек срок действия сертификата открытого ключа. Срок действия сертификата может составлять до 5 лет.
- Истек срок действия закрытого ключа. Срок действия закрытого ключа составляет 1 год (если срок действия сертификата превышает 1 год) или равен сроку действия сертификата (если срок действия сертификата меньше 1 года).
- Требуется получить сертификат, в котором будут изменены данные о его владельце (должность, подразделение и другие) или добавлены дополнительные атрибуты, расширения. Например, для использования сертификата в системах документооборота в него могут быть добавлены нужные политики применения.

Таким образом, требуется обновлять сертификат открытого ключа и закрытый ключ не реже, чем 1 раз в год.

Обновить сертификат и закрытый ключ вы можете не только в программе ViPNet Деловая почта (из окна **Настройка параметров безопасности**), но и с помощью ее компонента — программы ViPNet CSP (см. документ «ViPNet CSP. Руководство пользователя»).

Примечание. Если истек срок действия закрытого ключа, но при этом сертификат открытого ключа остается действительным, можно создать запрос на обновление сертификата. Запрос будет подписан закрытым ключом, но подпись будет недействительной. Она будет использоваться не для подтверждения авторства, а только для проверки целостности запроса. В этом случае потребуется ваше подтверждение корректности запроса согласно регламенту, принятому в удостоверяющем центре.

Если истек срока действия и закрытого ключа и сертификата, запрос на обновление создать невозможно. Новый сертификат в этом случае может быть издан только по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр.

В случае отсутствия закрытого ключа создать запрос на сертификат также невозможно.

Настройка оповещения об истечении срока действия закрытого ключа и сертификата

По умолчанию программа ViPNet Деловая почта начинает выдавать предупреждения за 15 дней до истечения срока действия сертификата или закрытого ключа.

Чтобы изменить настройки оповещения, выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись.**

В поле **Информация о текущем сертификате** указан срок действия сертификата.

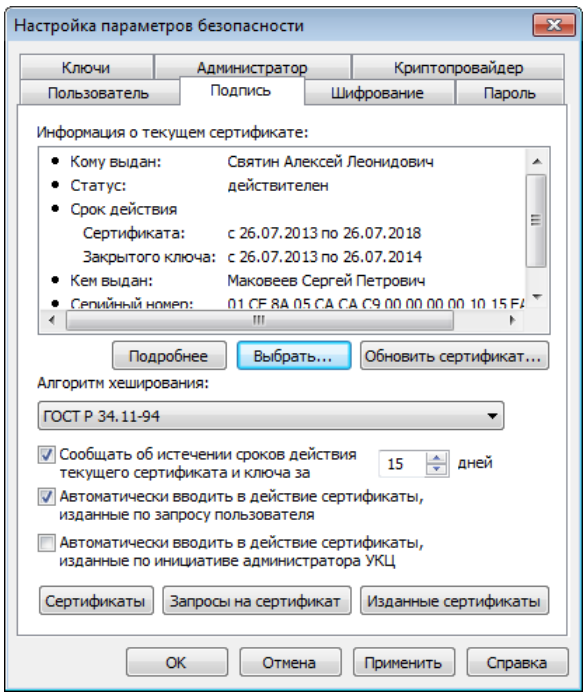


Рисунок 59: Просмотр информации о текущем сертификате и настройка параметров оповещения об истечении сроков действия закрытого ключа и сертификата

2 Установите или снимите флажок **Сообщать об истечении сроков действия текущего сертификата и ключа за** и в поле справа введите число дней не более 30.

Процедура обновления закрытого ключа и сертификата

За несколько дней до истечения срока действия сертификата или закрытого ключа требуется выполнить следующие действия:

- Если включено оповещение об истечении срока действия сертификата и закрытого ключа:

- Когда до истечения срока остается заданное количество дней, программа ViPNet Деловая почта выдаст соответствующее сообщение.

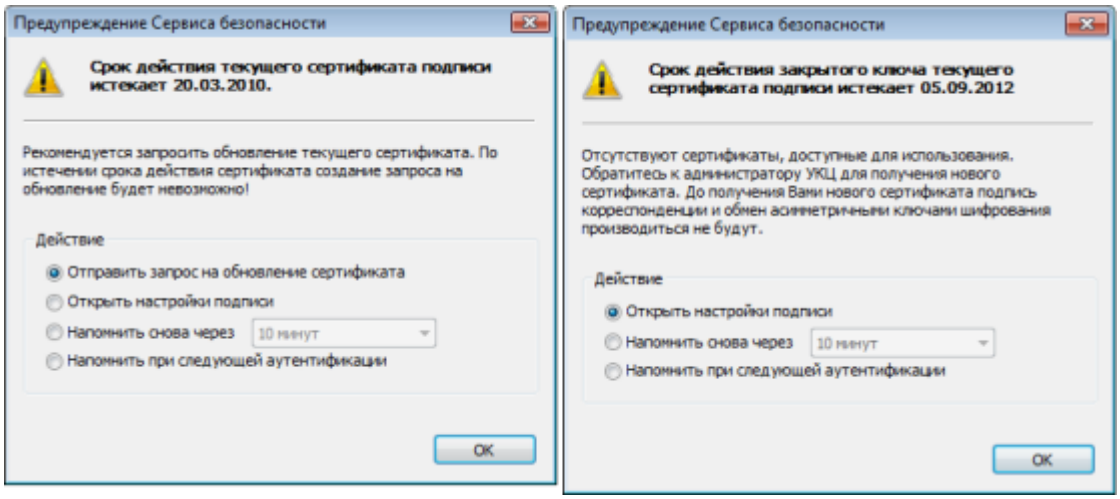


Рисунок 60: Предупреждения о скором истечении срока действия сертификата и закрытого ключа

- Если истекает срок действия сертификата, в окне сообщения выберите **Отправить запрос на обновление сертификата**, после чего нажмите кнопку **ОК**. Будет запущен **Мастер обновления сертификата**.

Примечание. Можно также открыть окно настройки параметров подписи или отложить отправку запроса на обновление сертификата.

- Если истекает срок действия закрытого ключа, в окне сообщения выберите **Открыть настройки подписи**, после чего нажмите кнопку **ОК**. В появившемся окне **Настройка параметров безопасности** на вкладке **Подпись** нажмите кнопку **Обновить сертификат**.

- Если оповещение об истечении срока действия сертификата и закрытого ключа отключено:
  - В окне **Настройка параметров безопасности** откройте вкладку **Подпись**.
  - На вкладке **Подпись** (см. рисунок на стр. 165) нажмите кнопку **Обновить сертификат**. Будет запущен **Мастер обновления сертификата**.

Чтобы сформировать и отправить запрос на обновление сертификата и закрытого ключа с помощью мастера:

1 На первой странице мастера обновления сертификата нажмите кнопку **Далее**.

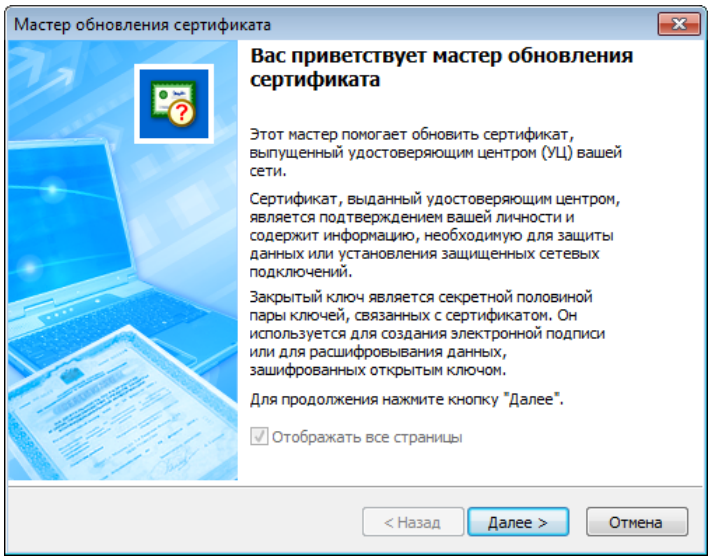


Рисунок 61: Стартовая страница мастера обновления сертификата

2 На странице **Открытый ключ** выполните следующие действия:

2.1 Укажите назначение ключа и сертификата:

- если предполагается их использовать только для подписи — значение **Подпись**;
- если предполагается их использовать как для подписи, так и для шифрования — значение **Подпись и шифрование**.

2.2 Задайте алгоритм формирования ключа и параметры алгоритма в соответствии с приведенной ниже таблицей:

Таблица 5. Характеристики алгоритмов

Алгоритм и его описание	**Параметры алгоритма**	**Длина открытого ключа**
ГОСТ Р 34.10-2001 См. RFC 4357 http://www.ietf.org/rfc/rfc4357.txt	**Для подписи:** ГОСТ Р 34.10 - 2001. Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 35.1»	512

Алгоритм и его описание	Параметры алгоритма	Длина открытого ключа
Стандарт электронной подписи, основанный на арифметике эллиптических кривых OID «1.2.643.2.2.19»	ГОСТ Р 34.10 - 2001 «Оскар» OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи 3 OID «1.2.643.2.2. 35.3» **Для подписи и шифрования:** ГОСТ Р 34.10 - 2001. EDH Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 36.0» ГОСТ Р 34.10 - 2001. EDH Параметры обмена 2 OID «1.2.643.2.2. 36.1»	
ГОСТ Р 34.10-2012/512 Новый стандарт электронной подписи от 2012 года с длиной закрытого ключа 256 бит OID «1.2.643.7.1.1.1.1»	ГОСТ Р 34.10 - 2001. Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 «Оскар» OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи 3 OID «1.2.643.2.2. 35.3»	512
ГОСТ Р 34.10-2012/1024 Новый стандарт электронной подписи от 2012 года с длиной закрытого ключа 512 бит OID «1.2.643.7.1.1.1.2»	ГОСТ Р 34.10 - 2012/1024. Набор параметров А	1024

Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки подписи, шифрования и расшифрования.

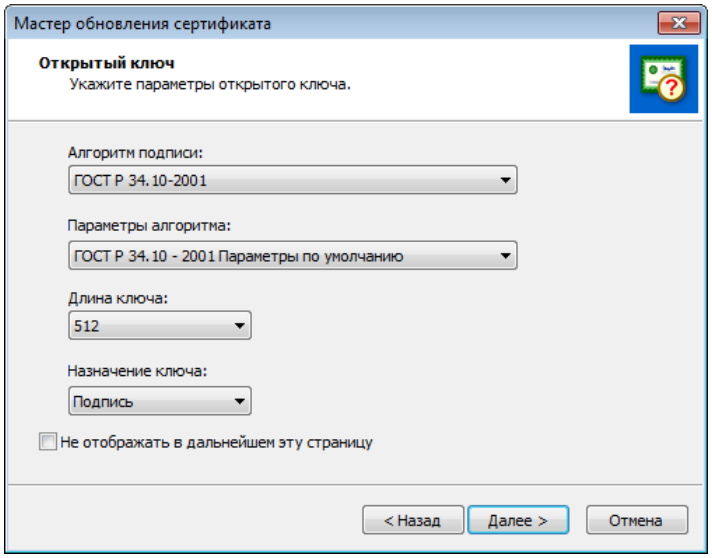


Рисунок 62: Выбор алгоритма и его параметров

2.3 Нажмите кнопку **Далее**.

3 На странице **Контейнер с закрытым ключом** укажите место хранения контейнера ключей:

- папку на диске,
- устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 199).

После этого нажмите кнопку **Далее**.

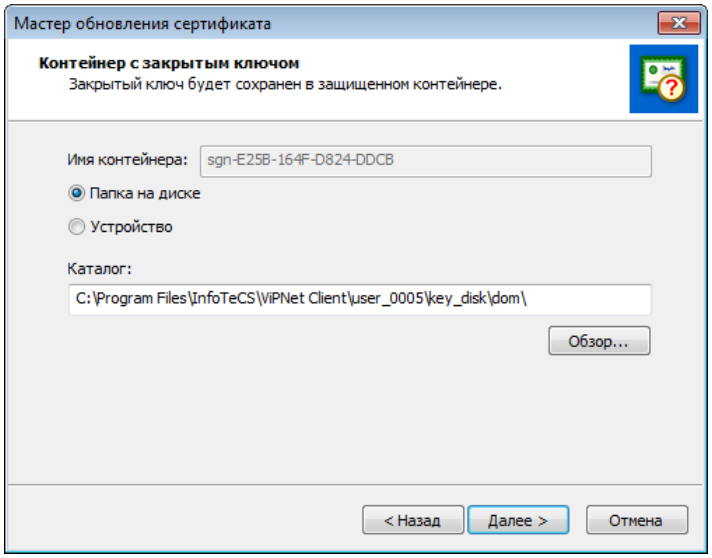


Рисунок 63: Указание места хранения контейнера ключей

4 На странице **Срок действия сертификата** задайте желаемый срок действия обновляемого сертификата удобным для вас способом, после чего нажмите кнопку **Далее**.

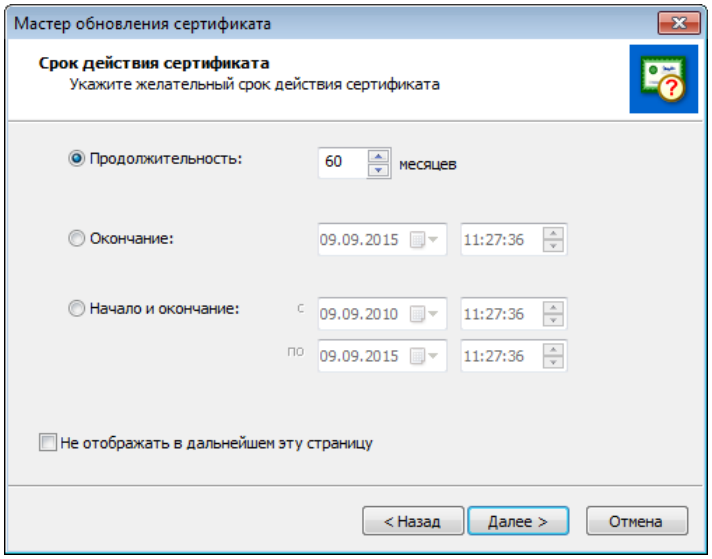


Рисунок 64: Указание желаемого срока действия сертификата

5 На странице **Готовность к созданию запроса на сертификат**:

- Убедитесь в правильности параметров, заданных на предыдущих страницах мастера. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

- При необходимости печати информации о запросе на принтере, используемом по умолчанию на данном сетевом узле, убедитесь в том, что установлен флажок **Печатать информацию о запросе**. В противном случае снимите флажок.

После этого нажмите кнопку **Далее.**

6 При появлении электронной рулетки следуйте указаниям окна.

Примечание. В случае если в рамках текущей сессии электронная рулетка уже была запущена, данное окно не появится.

7 На странице **Завершение работы мастера обновления сертификата** нажмите кнопку **Готово.**

В результате запрос на обновление сертификата будет передан в программу ViPNet Удостоверяющий и ключевой центр.

Примечание. Время ожидания ответа от программы ViPNet Удостоверяющий и ключевой центр может значительно варьироваться в зависимости от параметров настройки этой программы. Если программа ViPNet Удостоверяющий и ключевой центр настроена на автоматическую обработку запросов на сертификаты, время ожидания ответа не превышает 5 минут. Если обработка запросов в программе ViPNet Удостоверяющий и ключевой центр осуществляется вручную, время ожидания ответа не ограничено. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Если запрос на обновление сертификата в программе ViPNet Удостоверяющий и ключевой центр будет удовлетворен, на сетевой узел поступит обновленный сертификат. Изданный сертификат будет введен в действие и назначен текущим сразу после получения в том случае, если:

- В окне **Настройка параметров безопасности** на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**.
- Доступен контейнер, в котором хранится закрытый ключ, соответствующий сертификату.

Внимание! Если контейнер с закрытым ключом хранится в папке на диске, то он доступен всегда. Если контейнер хранится на внешнем устройстве, то он будет

доступен только в том случае, если устройство подключено и сохранен ПИН-код к нему.

В окне **Менеджер сертификатов** для запроса, по которому был издан сертификат, будет отображаться статус **сертификат введен в действие** (см. «Просмотр запроса на сертификат» на стр. 174).

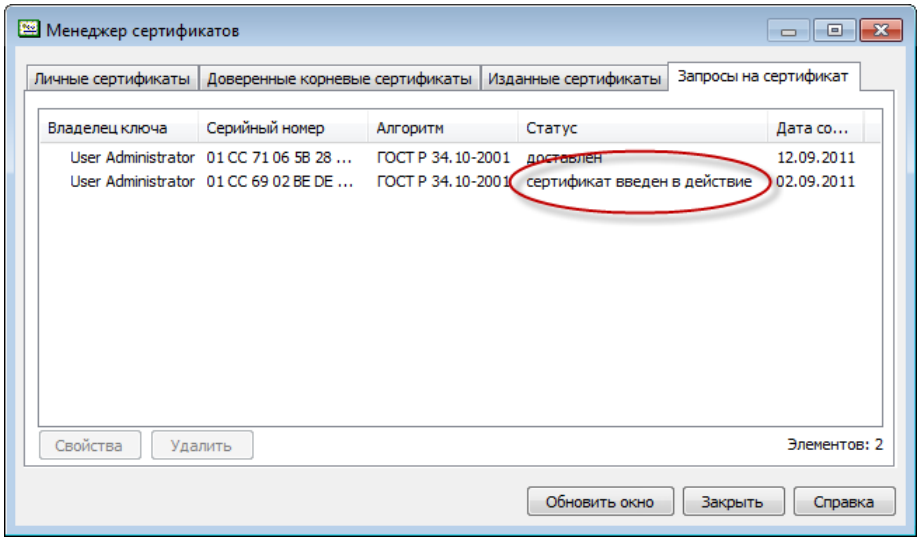


Рисунок 65: Статус запроса в случае ввода сертификата в действие

Если сертификат был получен, но не введен в действие автоматически, для запроса, по которому он был издан, будет отображаться статус **удовлетворен**. Выполните в данном случае ввод сертификата в действие вручную (см. «Ввод в действие вручную» на стр. 173).

Если запрос на обновление сертификата в программе ViPNet Удостоверяющий и ключевой центр будет отклонен, сертификат не будет издан. Запрос на сертификат будет иметь статус **отклонен**. Обратитесь к администратору программы ViPNet Удостоверяющий и ключевой центр для уточнения причин отклонения запроса.

Ввод сертификата в действие

Для того чтобы использовать сертификат, полученный из программы ViPNet Удостоверяющий и ключевой центр, необходимо ввести этот сертификат в действие, то есть установить этот сертификат в контейнер путем сопоставления его с соответствующим закрытым ключом.

Ввод в действие автоматически

Для того чтобы ввод в действие сертификатов, полученных из программы ViPNet Удостоверяющий и ключевой центр, выполнялся автоматически, убедитесь в том, что в окне **Настройка параметров безопасности** на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**, а также флажок **Автоматически вводить в действие сертификаты, изданные по инициативе администратора УКЦ**.

При наличии данных флажков сертификаты будут вводиться в действие автоматически в течение часа с момента их получения. Сертификаты, изданные по вашим запросам, смогут вводиться в действие автоматически только в том случае, если доступны контейнеры с соответствующими закрытыми ключами. В противном случае они могут быть введены в действие только вручную (см. «Ввод в действие вручную» на стр. 173).

Внимание! Если контейнер с закрытым ключом хранится в папке на диске, то он доступен всегда. Если контейнер хранится на внешнем устройстве, то он будет доступен только в том случае, если устройство подключено и сохранен ПИН-код к нему.

При вводе в действие сертификата, изданного по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр, появится окно **Предупреждение сервиса безопасности** с соответствующим сообщением.

Ввод в действие вручную

Ввод сертификатов, полученных из программы ViPNet Удостоверяющий и ключевой центр, в действие вручную требуется выполнять в следующих случаях:

- Если не установлены флажки, позволяющие выполнять автоматический ввод сертификатов в действие.
- При автоматическом вводе сертификата в действие был недоступен контейнер с соответствующим закрытым ключом.

Чтобы вручную ввести в действие полученный сертификат, выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Изданные сертификаты**.

2 В окне **Менеджер сертификатов** на вкладке **Изданные сертификаты** выберите полученный сертификат, который необходимо ввести в действие, после чего нажмите кнопку **Ввести в действие**.

В результате введенный в действие сертификат отобразится в окне **Менеджер сертификатов** на вкладке **Личные сертификаты**. Если необходимо использовать этот сертификат для подписания электронных документов, назначьте его текущим (см. «Смена текущего сертификата» на стр. 162).

Работа с запросами на сертификаты

Работа с запросами на сертификаты (см. «Запрос на сертификат» на стр. 207) выполняется в окне **Менеджер сертификатов** на вкладке **Запросы на сертификат**.

Для вызова окна **Менеджер сертификатов**:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**.

2 Нажмите кнопку **Запросы на сертификаты**.

Просмотр запроса на сертификат

Для просмотра подробной информации о запросе на сертификат:

1 В окне **Менеджер сертификатов** на вкладке **Запросы на сертификат** выберите нужный запрос, после чего нажмите кнопку **Свойства** или дважды щелкните по этому запросу.

2 В окне **Запрос на сертификат** просмотрите нужную информацию на соответствующих вкладках.

При необходимости запрос можно распечатать (на принтере, используемом по умолчанию на данном компьютере) с помощью кнопки **Печать**, а также сохранить в файл формата `*.txt` — с помощью кнопки **Копировать в файл**.

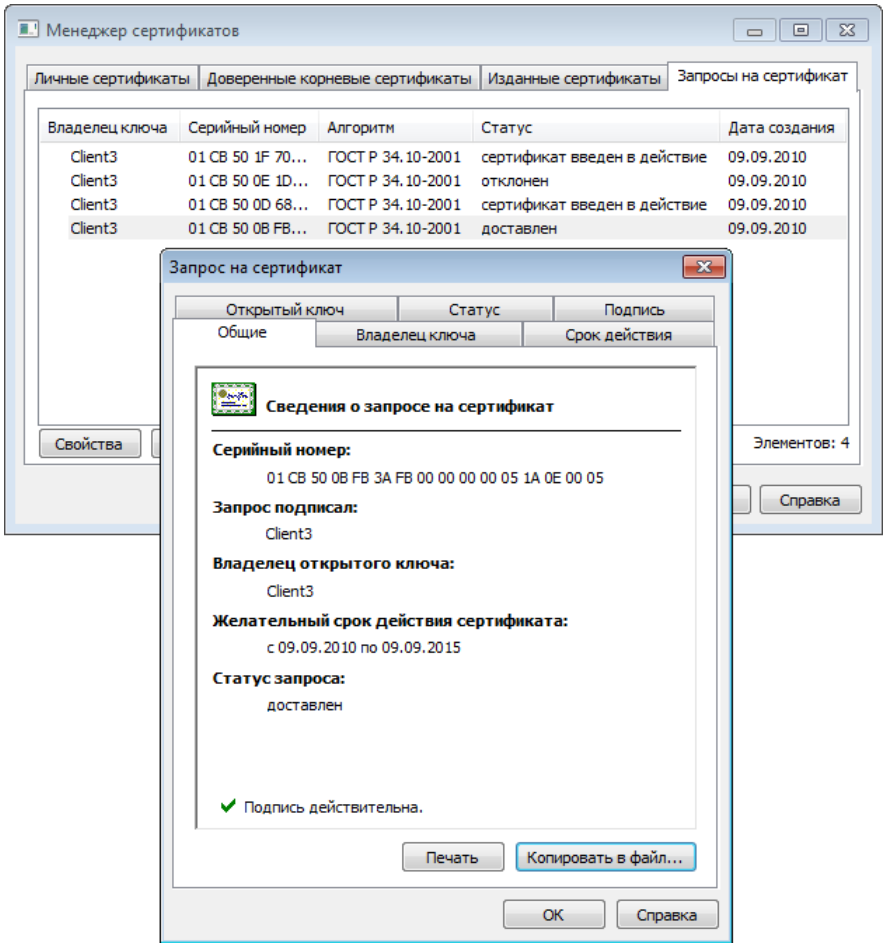


Рисунок 66: Просмотр подробной информации о запросе на сертификат

Удаление запроса на сертификат

Для удаления запроса на сертификат:

1. В окне **Менеджер сертификатов** на вкладке **Запросы на сертификат** выберите нужный запрос (или несколько, удерживая клавишу **Ctrl**), после чего нажмите кнопку **Удалить**.
2. В окне подтверждения нажмите кнопку **Да**.

Информация о запросе будет удалена. Удаленный запрос не будет отображаться на вкладке **Запросы на сертификаты**.

Экспорт сертификата

В программе ViPNet можно выполнить экспорт сертификата пользователя в различные форматы. Выбор формата экспорта зависит от целей, для которых проводится данный экспорт.

Экспорт сертификата может понадобиться для выполнения следующих задач:

- архивирование сертификата;
- копирование сертификата для использования на другом компьютере;
- отправка сертификата другому пользователю для организации обмена зашифрованными сообщениями;
- просмотр сертификата в удобной форме.

Для экспорта сертификата в файл определенного формата:

1. Вызовите окно **Сертификат** для того сертификата, который необходимо экспортировать (см. «Просмотр сертификатов» на стр. 151).
2. Откройте вкладку **Состав**, после чего нажмите кнопку **Копировать в файл**.
3. На начальной странице мастера экспорта сертификатов нажмите кнопку **Далее**.

Совет. Если при последующих запусках мастера желательно пропускать первую страницу, установите на ней флажок **Не отображать в дальнейшем эту страницу**.

4. На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов (см. «Форматы экспорта сертификатов» на стр. 177), после чего нажмите кнопку **Далее**.

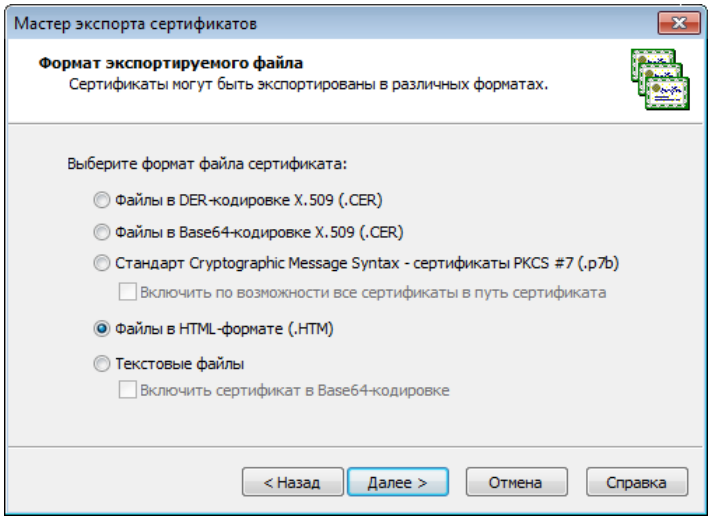


Рисунок 67: Выбор формата файла

5 На странице **Имя файла** укажите полный путь к создаваемому файлу, после чего нажмите кнопку **Далее**.

6 На странице **Завершение работы мастера экспорта сертификатов** убедитесь в правильности параметров экспорта, заданных на предыдущих страницах мастера, после чего нажмите кнопку **Готово**.

7 В окне с сообщением об успешном экспорте нажмите кнопку **ОК**.

Форматы экспорта сертификатов

При выборе формата экспорта сертификата следует руководствоваться перечисленными положениями.

- При экспорте сертификатов для импорта на компьютер с ОС Windows наиболее предпочтительный формат экспорта — PKCS #7, в первую очередь потому, что этот формат обеспечивает сохранение цепочки центров сертификации (пути сертификации) любого сертификата. Некоторые приложения требуют при импорте сертификата из файла представления в виде DER или Base64. Поэтому формат экспорта необходимо выбирать в соответствии с требованиями приложения или системы, в которую этот сертификат предполагается импортировать.

- Для просмотра сертификата и вывода его на печать используются текстовый и HTML-форматы.

Ниже приведена подробная информация о каждом из форматов экспорта сертификатов, поддерживаемых ПО ViPNet.

- **Стандарт Cryptographic Message Syntax (PKCS #7)**

  Формат PKCS #7 позволяет передавать сертификат и все сертификаты в цепочке сертификации с одного компьютера на другой или с компьютера на внешнее устройство. Файлы PKCS #7 обычно имеют расширение `.p7b` и совместимы со стандартом ITU-T X.509. Формат PKCS#7 разрешает такие атрибуты, как удостоверяющие подписи, связанные с обычными подписями. Для таких атрибутов, как метка времени, можно выполнить проверку подлинности вместе с содержимым сообщения. Дополнительные сведения о формате PKCS #7 см. на странице PKCS #7 веб-узла RSA Labs http://www.rsa.com/rsalabs/node.asp?id=2129.

- **Файлы в DER-кодировке X.509**

  DER (Distinguished Encoding Rules) для ASN.1, как определено в рекомендации ITU-T Recommendation X.509, — более ограниченный стандарт кодирования, чем альтернативный BER (Basic Encoding Rules) для ASN.1, определенный в рекомендации ITU-T Recommendation X.209, на котором основан DER. И BER, и DER обеспечивают независимый от платформы метод кодирования объектов, таких как сертификаты и сообщения, для передачи между устройствами и приложениями.

  При кодировании сертификата большинство приложений используют стандарт DER, так как сертификат (сведения о запросе на сертификат) должен быть закодирован с помощью DER и подписан. Файлы сертификатов DER имеют расширение `.cer`.

  Дополнительные сведения см. в документе «ITU-T Recommendation X.509, Information Technology — Open Systems Interconnection — The Directory: Authentication Framework» на веб-узле International Telecommunication Union (ITU) http://www.itu.int/ru/Pages/default.aspx.

- **Файлы в Base64-кодировке X.509**

  Этот метод кодирования создан для работы с протоколом S/MIME, который популярен при передаче бинарных файлов через Интернет. Base64 кодирует файлы в текстовый формат ASCII, при этом в процессе прохождения через шлюз файлы практически не повреждаются. Протокол S/MIME обеспечивает работу некоторых криптографических служб безопасности для приложений электронной почты, включая механизм неотрекаемости (с помощью электронных подписей), секретность и безопасность данных (с помощью кодирования, процесса проверки подлинности и целостности сообщений). Файлы сертификатов Base64 имеют расширение `.cer`.

  MIME (Multipurpose Internet Mail Extensions, спецификация RFC 1341 и последующие) определяет механизмы кодирования произвольных двоичных данных для передачи по электронной почте.

Дополнительные сведения см. в документе «RFC 2633 S/MIME Version 3 Message Specification, 1999» на веб-узле Internet Engineering Task Force (IETF) http://www.ietf.org/rfc/rfc2633.txt?number=2633.

- **Файлы в HTML-формате**

  Файлы для просмотра и печати в любом веб-браузере, а также в офисных и других программах, поддерживающих язык разметки гипертекста HTML.

- **Текстовые файлы**

  Файлы кодировки ANSI для просмотра в любом текстовом редакторе и вывода на печать.

Работа с контейнером ключей

Контейнер ключей содержит закрытый ключ подписи (см. «Закрытый ключ» на стр. 206) и сертификат (см. «Сертификат открытого ключа подписи пользователя» на стр. 210), соответствующий закрытому ключу.

В программе ViPNet Деловая почта доступны следующие операции с контейнером ключей:

- Установка (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 187).

  Устанавливать новый или выполнять смену контейнера ключей с текущим сертификатом может потребоваться в следующих случаях:

  - Если сертификат не был сопоставлен закрытому ключу, который хранится в контейнере, — например, вследствие того, что сертификат хранится отдельно от закрытого ключа. Контейнер ключей может быть установлен как совместно с сертификатом (см. «Установка сертификатов в хранилище» на стр. 157), так и отдельно (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 187) (например, в случае если закрытый ключ хранится в контейнере, а сертификат сформирован по запросу пользователя в программе ViPNet Удостоверяющий и ключевой центр).
  - Если контейнер был сформирован другим приложением или перенесен с другого компьютера.

- Смена и удаление сохраненного пароля к контейнеру (см. «Смена пароля к контейнеру» на стр. 183).

  Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль. Удалять сохраненный пароль к контейнеру ключей может потребоваться в том случае, если изменились условия эксплуатации пароля или регламент вашей организации, вследствие чего хранение пароля на компьютере стало недопустимым.

- Удаление закрытого ключа, который хранится в контейнере (см. «Удаление закрытого ключа» на стр. 186).

  Удаление закрытого ключа из контейнера ключей требуется в следующих случаях:

  - в том случае, если в этом закрытом ключе нет больше необходимости — например, вследствие истечения срока его действия;

- при компрометации или отзыве сертификата, соответствующего закрытому ключу.

- Изменение расположения контейнера (см. «Перенос контейнера ключей» на стр. 188).

  Перенос текущего контейнера ключей требуется в следующих случаях:

  - если расположение контейнера было изменено, например, вследствие того, что хранение контейнера по прежнему пути было признано небезопасным;
  - при переходе на способ аутентификации **Устройство** в случае, если используются процедуры подписи и шифрования внутри сторонних приложений и при этом контейнер ключей изначально не хранился на внешнем устройстве, используемом для аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 123).

Внимание! В рамках ПО ViPNet CUSTOM выполнять различные операции с контейнером ключей может только пользователь, который обладает правом подписи. Такое право предоставляется пользователям сети ViPNet в программе ViPNet Центр управления сетью.

Для работы с контейнером ключей (см. «Контейнер ключей» на стр. 207):

1 Откройте вкладку **Ключи**.

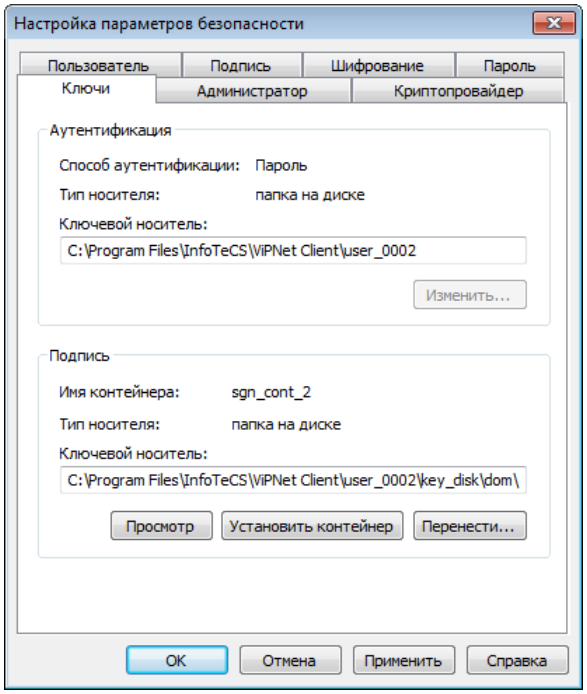


Рисунок 68: Работа с контейнером ключей

2 В группе **Подпись** нажмите одну из следующих кнопок:

- **Просмотр** — для просмотра подробной информации об используемом контейнере ключей, а также для изменения свойств контейнера:
  - смены пароля (см. «Смена пароля к контейнеру» на стр. 183);
  - удаления пароля (см. «Удаление сохраненного на компьютере пароля к контейнеру ключей» на стр. 185);
  - проверки соответствия закрытого ключа сертификату (см. «Проверка контейнера ключей» на стр. 185);
  - удаления закрытого ключа (см. «Удаление закрытого ключа» на стр. 186).
- **Установить контейнер** — для установки нового и смены контейнера ключей с текущим сертификатом (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 187).
- **Перенести** — для изменения расположения контейнера ключей (см. «Перенос контейнера ключей» на стр. 188).

Примечание. В группе **Подпись** отображается информация о закрытом ключе, соответствующем текущему сертификату. При установке нового контейнера ключей (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 187) информация о текущем сертификате,

отображаемая на вкладке **Подпись**, меняется автоматически.

Смена пароля к контейнеру

Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль.

Для смены пароля к контейнеру ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. рисунок на стр. 182) нажмите кнопку **Просмотр**.
2. В окне **Свойства контейнера ключей** нажмите кнопку **Сменить пароль**.

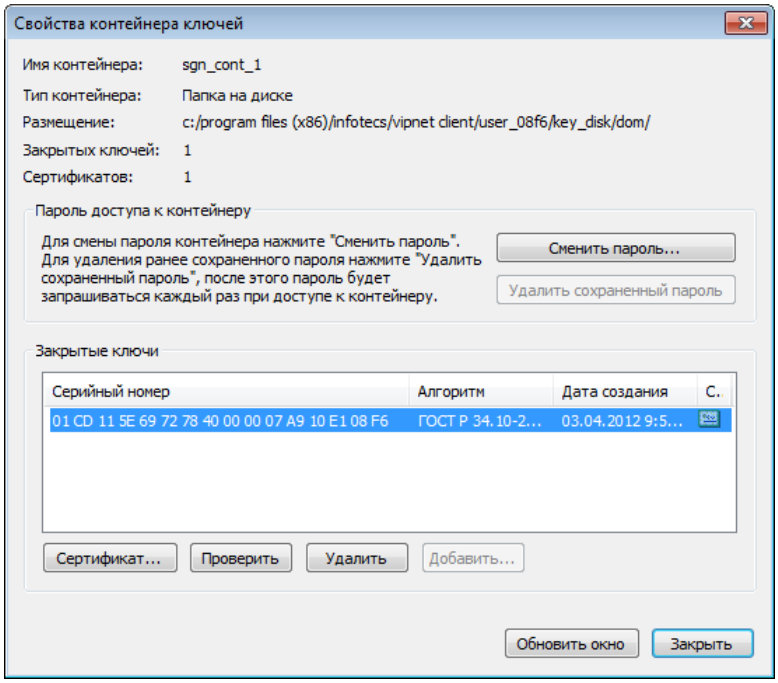


Рисунок 69: Информация о контейнере ключей

3. При появлении сообщения «Для данного контейнера смена пароля возможна только в настройке безопасности приложений ViPNet» нажмите кнопку **OK**, после чего завершите работу с окном **Свойства контейнера ключей** и измените пароль пользователя (см. «Смена пароля пользователя» на стр. 126).

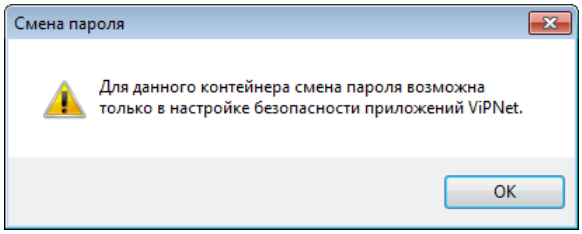


Рисунок 70: Сообщение о невозможности смены пароля для доступа к контейнеру

Примечание. Появление данного окна связано с тем, что контейнер ключей защищен с использованием не пароля, а персонального ключа пользователя. В этом случае пароль к контейнеру совпадает с паролем пользователя, поэтому изменение пароля к контейнеру возможно только вместе с изменением пароля пользователя.

4 Если контейнер ключей пользователя создан в программе ViPNet Registration Point либо был перенесен (см. «Перенос контейнера ключей» на стр. 188) из папки ключей пользователя (по умолчанию `C:\Program Files (x86)\InfoTeCS\ViPNet Деловая почта\user_<идентификатор пользователя>\key_disk\dom`) в другую папку, после нажатия на кнопку **Сменить пароль** появится окно **Пароль**. В окне **Пароль** введите текущий пароль доступа к контейнеру ключей и нажмите кнопку **OK**.

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

5 В окне **ViPNet CSP - пароль контейнера ключей** укажите и подтвердите новый пароль. Нажмите кнопку **OK**.

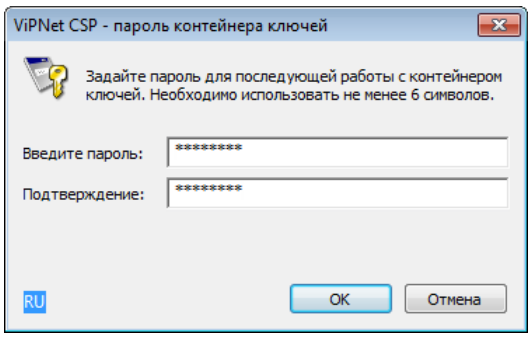


Рисунок 71: Смена пароля доступа к контейнеру ключей

Пароль доступа к контейнеру ключей изменен.

Удаление сохраненного на компьютере пароля к контейнеру ключей

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

Для удаления сохраненного пароля к контейнеру ключей и отображения окна ввода пароля при доступе к контейнеру:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. рисунок на стр. 182) нажмите кнопку **Просмотр.**
2. В окне **Свойства контейнера ключей** (см. рисунок на стр. 183) нажмите кнопку **Удалить сохраненный пароль.**

Сохраненный пароль удален. Теперь пароль необходимо вводить всякий раз при доступе к контейнеру ключей.

Проверка контейнера ключей

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

Чтобы проверить контейнер ключей:

1. В окне **Свойства контейнера ключей** (см. рисунок на стр. 183) в списке **Закрытые ключи** выберите нужный закрытый ключ.
2. Нажмите кнопку **Проверить.**
3. В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите кнопку **OK.**

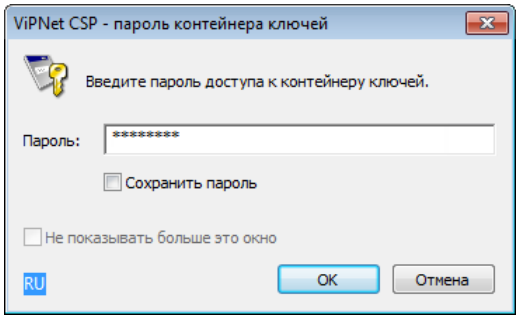


Рисунок 72: Ввод пароля доступа к контейнеру ключей

4 Будет сформирован фрагмент данных, который будет подписан с помощью закрытого ключа, после чего будет выполнена проверка электронной подписи с помощью сертификата открытого ключа. Таким образом, будет проверена пригодность закрытого ключа и его соответствие сертификату, хранящемуся в контейнере.

Примечание. Проверка возможна только в том случае, если в контейнере ключей есть сертификат, соответствующий закрытому ключу. Сертификат может отсутствовать в контейнере ключей, если он размещен отдельно. Сертификат размещается отдельно от контейнера ключей, если запрос на обновление сертификата сформирован в ПО ViPNet CSP. Если запрос сформирован в другой программе, сертификат автоматически помещается в контейнер ключей.

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

Удаление закрытого ключа

Удаление закрытого ключа (и сертификата, при его наличии) из контейнера ключей требуется в следующих случаях:

- если в этом закрытом ключе нет больше необходимости — например, вследствие истечения срока его действия;
- при компрометации или отзыве сертификата, соответствующего закрытому ключу.

Чтобы удалить закрытый ключ и сертификат из контейнера ключей:

1 В окне **Свойства контейнера ключей** (см. рисунок на стр. 183) в списке **Закрытые ключи** выберите строку закрытого ключа.

2 Нажмите кнопку **Удалить**. Появится предупреждение о том, что удаленный закрытый ключ невозможно восстановить.

3 В окне предупреждения нажмите кнопку **Да.**

Выбранный закрытый ключ и соответствующий ему сертификат будут удалены из контейнера ключей. После этого необходимо удалить контейнер.

Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом

Устанавливать новый контейнер ключей или выполнять смену контейнера ключей с текущим сертификатом может потребоваться в следующих случаях:

- если при установке сертификата в системное хранилище или хранилище программы ViPNet Деловая почта (см. «Установка сертификатов в хранилище» на стр. 157) ему не был сопоставлен соответствующий закрытый ключ — например, вследствие того, что сертификат хранится отдельно от закрытого ключа, то есть не в контейнере ключей;
- если контейнер ключей был сформирован в другом приложении или перенесен с другого компьютера.

Примечание. Установить или сменить можно только контейнер с ключами, сформированными в ПО ViPNet версии не ниже 3.2.x.

Для установки нового или смены текущего контейнера ключей:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. рисунок на стр. 182) нажмите кнопку **Установить контейнер.**

2 В окне **ViPNet CSP – инициализация контейнера ключа** укажите место хранения контейнера ключей:

   - папку на диске;
   - устройство с указанием его параметров и ПИН-кода.

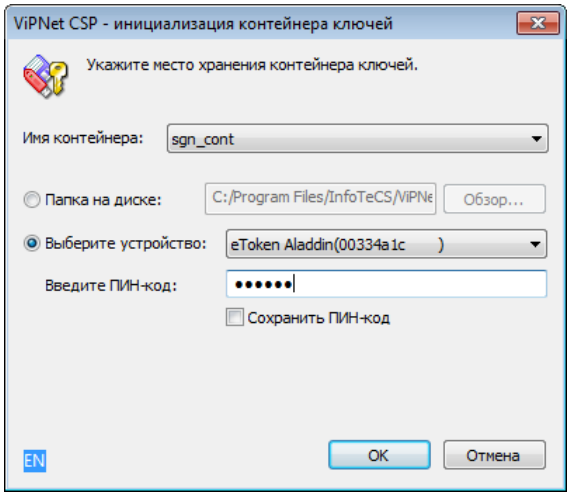


Рисунок 73: Инициализация контейнера ключей с внешнего устройства

Нажмите кнопку **ОК**.

3 Если в контейнере отсутствует закрытый ключ, в окне с сообщением нажмите кнопку **ОК**, затем выберите другой контейнер.

4 В окне **Выбор сертификата** укажите, какой из сертификатов, находящихся в контейнере, требуется назначить текущим. Затем нажмите кнопку **ОК**.

В результате закрытый ключ и сертификат, которые хранятся в выбранном контейнере, будут назначены текущими. Информация о сертификате, который хранится в установленном контейнере, отобразится на вкладке **Подпись**.

Перенос контейнера ключей

Перенос текущего контейнера ключей может потребоваться для изменения расположения контейнера, например, если хранение контейнера по прежнему пути было признано небезопасным.

Примечание. Перенести можно только контейнер с ключами, сформированными в ПО ViPNet версии не ниже 3.2.x.

Не поддерживается перенос контейнера ключей на устройства eToken ГОСТ, ruToken, Shipka, Kaztoken (см. «Внешние устройства» на стр. 199).

Для того чтобы поменять расположение контейнера ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. рисунок на стр. 182) нажмите кнопку **Перенести.**
2. В окне **ViPNet CSP – инициализация контейнера ключа** укажите новое место хранения контейнера ключей:
   - папку на диске;
   - устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 199).

Контейнер ключей будет перенесен по указанному пути.

Возможные неполадки и способы их устранения

Не удается выполнить аутентификацию с помощью сертификата

Если вам не удается войти в программу ViPNet Деловая почта, используя для аутентификации сертификат и соответствующий ему закрытый ключ, которые хранятся на внешнем устройстве, это может быть вызвано одной из следующих причин:

- Внешнее устройство хранения данных не поддерживает стандарт PKCS#11. Проверить, поддерживает ли ваше устройство этот стандарт, можно по разделу Внешние устройства (на стр. 199).
- Срок действия выбранного сертификата истек. При выборе недействительного сертификата появится соответствующее сообщение. В этом случае следует передать сертификат администратору вашего удостоверяющего центра для обновления.
- Выбранный сертификат присутствует в списке отозванных сертификатов, который установлен в хранилище данного узла. При выборе отозванного сертификата появится соответствующее сообщение. В этом случае следует обратиться к администратору вашего удостоверяющего центра.
- Выбранный сертификат не имеет расширения «Проверка подлинности клиента». Это расширение должно отображаться в окне **Сертификат**, на вкладке **Состав**, в поле **Расширенное использование ключа**. В этом случае следует обратиться к администратору вашего удостоверяющего центра для переиздания сертификата.
- Сертификат издателя не установлен в системное хранилище **Доверенные корневые центры сертификации**. В этом случае следует получить сертификат издателя у администратора вашего удостоверяющего центра и установить его в указанное системное хранилище. Для этого дважды щелкните по сертификату и следуйте указаниям мастера установки сертификатов.

Невозможна отправка писем из программы ViPNet Деловая почта

О том, что письмо программы ViPNet Деловая почта не доставлено адресату, свидетельствует наличие у этого письма следующих атрибутов:

- — упаковано — письмо подготовлено к отправке, но не передано на координатор (координатор, на котором данный клиент зарегистрирован в программе ViPNet Центр управления сетью).
- — отправлено — письмо передано на координатор, но не передано на сетевой узел получателя.

Письмо упаковано, но не отправлено

В случае если отправленное письмо имеет атрибут , на клиенте в программе ViPNet Монитор выполните следующие действия:

- Проверьте соединение с координатором клиента.

> **Примечание.** Чтобы узнать имя координатора, в программе ViPNet MFTP в окне **Настройки** откройте вкладку **Каналы**. Координатор будет указан в первой строке списка.

- Просмотрите информацию в журнале IP-пакетов.

Проверка соединения с координатором

Для того чтобы проверить соединение с координатором, в программе ViPNet Монитор выполните следующие действия:

1. В разделе **Защищенная сеть** выберите координатор, за которым находится данный клиент.
2. Нажмите кнопку **Проверить** панели инструментов или клавишу F5.

3 Дождитесь, пока в окне **Проверка соединения** в столбце **Статус** отобразится сообщение о доступности координатора. Проверка соединения может длиться до одной минуты.

Совет. Выполните проверку несколько раз с интервалом в 1–2 минуты. В случае если в момент проверки связи с координатором на нем выполняется установка обновления справочников и ключей, этот координатор будет недоступен в течение некоторого времени.

Если связь с координатором не восстановлена (в окне **Проверка соединения** для координатора отображается статус **Недоступен**), просмотрите информацию в журнале IP-пакетов.

Просмотр информации в журнале IP-пакетов

Для просмотра информации в журнале IP-пакетов в программе ViPNet Монитор выполните одно из следующих действий:

- На панели навигации выберите раздел **Журнал IP-пакетов**, затем на панели просмотра нажмите кнопку **Поиск**.
- В разделе **Защищенная сеть** щелкните правой кнопкой мыши координатор, за которым находится данный клиент, и в контекстном меню выберите пункт **Журнал регистрации IP-пакетов**. Затем в открывшемся разделе **Журнал IP-пакетов** нажмите кнопку **Поиск**.

Ознакомьтесь с информацией о входящих и исходящих IP-пакетах:

- В журнале IP-пакетов не зарегистрированы исходящие IP-пакеты ( , ) в адрес координатора.

  Это может свидетельствовать о том, что на используемом компьютере не задан IP-адрес шлюза. Для решения данной проблемы в сетевых настройках ОС Windows укажите IP-адрес шлюза (**Основной шлюз** или **Шлюз по умолчанию**).

- В журнале IP-пакетов зарегистрированы исходящие IP-пакеты на адрес координатора (с кодом 40), но не зарегистрированы ответные входящие IP-пакеты ( , ).

  В этом случае на клиенте в командной строке выполните команду `ping <ip>`, где `<ip>` — IP-адрес видимости координатора.

Примечание. В окне свойств координатора на вкладке **IP-адреса** IP-адреса видимости координатора (реальные или виртуальные, в зависимости от настроек) выделены полужирным шрифтом.

Если после выполнения команды `ping` в **Журнале IP-пакетов** не зарегистрированы входящие ответные IP-пакеты от координатора, а в окне консоли отображаются сообщения **Превышен интервал ожидания для запроса** (**Request time out**):

- Проверьте маршруты передачи данных от клиента до координатора (например, из командной строки с помощью команды `route print`).
- Проверьте, что на клиенте в сетевых настройках ОС Windows отображается корректный IP-адрес.
- Выполните команду `ping` на координаторе для проверки связи с данным клиентом.

Если после выполнения команды `ping` получены ответы от координатора, но при этом письма по-прежнему не отправляются, выполните следующие действия:

- Убедитесь в том, что на координаторе запущена программа ViPNet Монитор, а также транспортный модуль MFTP.
- Проверьте, зарегистрированы ли в журнале IP-пакетов пакеты транспортного модуля MFTP (в колонке **Порт источника** или **Порт назначения** для этих пакетов отображается значение 5000, 5001 или 5002). В противном случае убедитесь в том, что на используемом компьютере запущен транспортный модуль MFTP.
- Убедитесь, что в настройках транспортного модуля на клиенте включен канал связи с координатором. Для этого в программе ViPNet MFTP в окне **Настройки** откройте вкладку **Каналы**. Убедитесь, что в строке координатора (первая строка) указан тип канала **MFTP**.

- В журнале IP-пакетов на клиенте и на координаторе зарегистрированы блокированные IP-пакеты с событием 1.

  Это может быть связано с тем, что на клиент не поступило обновление ключей после смены мастер-ключей сети ViPNet или после процедуры компрометации (этого клиента или координатора). Для решения данной проблемы следует получить у администратора вашей сети ViPNet новый дистрибутив ключей, после чего провести процедуру обновления ключей вручную.

Письмо отправлено, но не доставлено

В случае если письмо имеет атрибут  :

1. Убедитесь в том, что сетевой узел получателя включен и на нем запущены программы ViPNet Монитор и ViPNet MFTP.
2. Обратитесь к администратору вашей сети ViPNet для проведения аналогичной проверки на всех компьютерах, составляющих маршрут передачи данных от вашего клиента до узла получателя.

Не удается зашифровать вложение

При попытке отправить письмо с вложением возникает сообщение об ошибке: «Ключи для связи с сетью <номер сети> устарели. Для них не допускается шифрование файлов размером более 4 Мбайт. Обратитесь к администратору сети ViPNet».

Причина возникновения данной ошибки в том, что для связи с сетью, номер которой указан в сообщении, используется ключ старого формата. С помощью таких ключей невозможно зашифровать вложение размером больше 4 Мбайт. Для решения проблемы сообщите администратору вашей сети ViPNet о необходимости обновить межсетевой мастер-ключ для указанной сети.

Восстановление базы писем

Общая информация

Восстановление базы писем требуется в результате ее повреждения. Аварийная ситуация может возникнуть в следующих случаях:

- Перезагрузка компьютера (например, при сбое электропитания или в результате некорректной работы операционной системы) во время активной работы с программой ViPNet Деловая почта (при создании писем, изменении настроек программы и так далее).
- Принудительное завершение работы программы.
- Утеря или повреждение хотя бы одного из управляющих файлов программы.
- Отсутствие доступа к данным в результате неисправности жесткого диска используемого компьютера.

Как правило, восстановление базы писем выполняется автоматически и не требует участия пользователя. Для автоматического восстановления необходимо, чтобы в папке `\MS` присутствовали и не были повреждены следующие управляющие файлы: `attach3.db`, `rcpt3.db`, `folders3.db`, `docs3.db`. Однако в случае отсутствия или повреждения хотя бы одного из указанных файлов восстановление базы писем необходимо выполнять вручную (см. «Методика восстановления базы писем» на стр. 197).

Примечание. Расположение папки `\MS` зависит от набора программ, установленных на используемом компьютере:

- Установлена программа ViPNet Деловая почта (в составе программы ViPNet Client или отдельно) — по умолчанию `C:\Program Files\InfoTeCS\ViPNet Client`.
- Установлены программы ViPNet Administrator и ViPNet Client — по умолчанию `C:\Program Files\InfoTeCS\ViPNet Administrator\SS`.

О необходимости восстановления базы писем вручную свидетельствует появление во время работы программы ViPNet Деловая почта сообщения об ошибке открытия

почтовой базы или сообщения о том, что не найден один или несколько управляющих файлов.

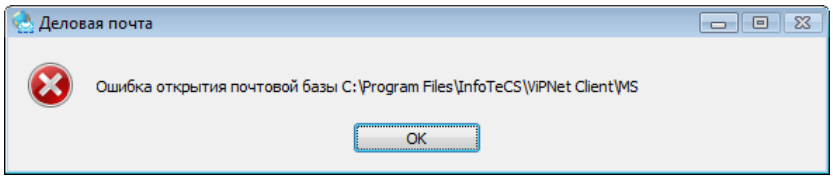


Рисунок 74: Сообщение о невозможности открытия почтовой базы

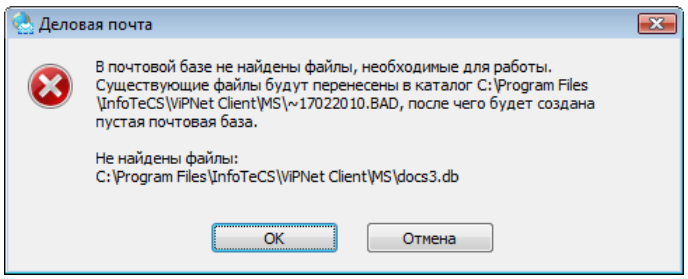


Рисунок 75: Сообщение об отсутствии управляющего файла

Внимание! Чтобы облегчить процесс восстановления базы писем, рекомендуется регулярно архивировать письма программы ViPNet Деловая почта. Архивация может выполняться автоматически (см. «Параметры автоматической архивации» на стр. 110) или с помощью меню **Файл > Архивировать почту**. Архив помещается в папку `\MSArch`, которая расположена по тому же пути, что и папка `\MS`.

Методика восстановления базы писем

Восстановление базы писем вручную можно выполнить одним из следующих способов:

- С помощью папки с расширением `REP`, расположенной в папке `\MS`.

  Папки с расширением `REP` создаются автоматически в случае некорректного завершения работы программы и содержат управляющие файлы, актуальные на момент создания папки. Дата создания содержится в названии папки в формате **~ддммгггг**.

- С помощью папки `\MSArch`, расположенной по тому же пути, что и папка `\MS`.

  Папка `\MSArch` создается при архивации писем (автоматически или с помощью меню **Файл > Архивировать почту**) и содержит управляющие файлы программы, актуальные на момент создания архива, а также базу писем.

Для восстановления базы писем вручную выполните следующие действия:

1. В случае появления окна с сообщением об отсутствии в папке `\MS` необходимого файла и предложением создать новую пустую папку нажмите кнопку **Отмена** (см. рисунок на стр. 197).
2. Завершите работу программы ViPNet Деловая почта.
3. Перейдите в одну из папок с расширением `REP` или в папку `\MSArch` (в зависимости от того, какая папка имеет более позднюю дату создания) и выполните одно из действий:
   - При выборе папки с расширением `REP`:
     - Перенесите все содержимое (файлы и папки) папки `\MS` в любое место на диске.
     - Скопируйте всё содержимое из папки с расширением `REP` в папку `\MS`.
   - При выборе папки `\MSArch`:
     - Перенесите всё содержимое папки `\MS` в любое место на диске.
     - Скопируйте всё содержимое из папки `\MSArch` в папку `\MS`.
4. Запустите программу ViPNet Деловая почта.
5. В случае появления сообщения о невозможности открыть почтовую базу повторите действия **2–4**, используя другую папку с расширением `REP` или другую папку `\MSArch`.
6. Если вышеописанные действия не дали результата, поврежденная информация не подлежит восстановлению. Переустановите программу ViPNet Деловая почта и начните работу с новой базой писем.

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей (см. «Контейнер ключей» на стр. 207), которые вы можете использовать для аутентификации, формирования электронной подписи (см. «Электронная подпись» на стр. 211) или для других целей.

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

Программное обеспечение ViPNet Деловая почта поддерживает два способа аутентификации с помощью внешнего устройства (см. «Способы аутентификации пользователя» на стр. 26):

- По персональному ключу пользователя ViPNet, который хранится на устройстве. Этот способ аутентификации имеет следующие ограничения:
  - Одно внешнее устройство невозможно использовать для аутентификации нескольких пользователей ViPNet.
  - Одно внешнее устройство невозможно использовать для аутентификации одного пользователя на нескольких узлах ViPNet.

- Если используется этот способ аутентификации, тогда ключи электронной подписи пользователя, изданные в удостоверяющем центре на базе ПО ViPNet, должны храниться на одном устройстве с персональным ключом.

- По сертификату, который хранится на устройстве вместе с соответствующим закрытым ключом.

Примечание. В настоящий момент для аутентификации по сертификату невозможно использовать устройства с поддержкой алгоритма ГОСТ 34.10-2001.

Сертификат для аутентификации можно запросить в домене Windows, сохранив контейнер ключей на внешнем устройстве, которое поддерживает стандарт PKCS#11.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP (см. «Настройка параметров криптопровайдера ViPNet CSP» на стр. 132). Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

В следующей таблице перечислены внешние устройства, которые могут быть использованы в программном обеспечении ViPNet. Для каждого внешнего устройства в таблице приведено описание, условия и особенности работы с устройством, информация о поддержке стандарта PKCS#11.

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

Таблица 6. Поддерживаемые внешние устройства

Название устройства в программе ViPNet CSP	Полное название и тип устройства	Необходимые условия работы с устройством	Поддержка стандарта PKCS#11
UEC	**Универсальная электронная карта**	На компьютере необходимо указать расположение сертификатов и контейнера ключей, полученных в пункте выдачи карт.	Да
ESMART CryptoToken 64K	Смарт-карты **ESMART CryptoToken 64K**	На компьютере должно быть установлено программное обеспечение ESMART PKI Client.	Да
Infotecs Software Token	**Infotecs Software Token** — программная реализация стандарта PKCS#11	Входит в поставку программы ViPNet CSP.	Да
A-Key S1000	Смарт-карта **AkToken** производства компании Ak Kamal Security	На компьютере должны быть установлены драйверы, предоставленные компанией Ak Kamal Security. Перенос ключей подписи на данный тип устройств невозможен.	Да
Magistra	Смарт-карты **Магистра** производства компании «СмартПарк»	Устройство не поддерживает ГОСТ 34.10-2012; создание ключей по этому алгоритму невозможно, перенос ключей, созданных по этому алгоритму, на данный тип устройств невозможен.	Да
ViPNet HSM	Виртуальный токен **ViPNet HSM** производства компании «ИнфоТеКС»	Необходимо установить клиентское приложение ViPNet HSM и проинициализировать виртуальный токен.	Да
KAZTOKEN	**KAZTOKEN**, электронный идентификатор производства компании «Цифровой поток»	На компьютере должны быть установлены драйверы ktDrivers.x64.v.2.73.00.04.08 (для 64-разрядной ОС) или ktDrivers.x86.v.2.73.00.04.08. Перенос ключей подписи на данный тип устройств невозможен.	Да

JaCarta	Персональные электронные ключи **JaCarta Laser** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено программное обеспечение JC-Client компании «Аладдин Р.Д.».	Да
JCDS	Смарт-карты **Gemalto Optelio Contactless D72**, **KONA 131 72K** с апплетом от компании «Аладдин Р.Д.»	На карту должен быть загружен апплет, позволяющий модулю jcpkcs11ds.dll компании «Аладдин Р.Д.» работать с картой.	Да
Mifare Standard4K	Смарт-карты **MIFARE Classic 4K** для считывателей ACR128	Для работы с устройством используется интерфейс подключения USB 2.0 (совместимый с USB 1.1). Карта MIFARE Classic 4K поддерживается только через считыватель ACR128.	Нет
SmartCard RIK	**Российская интеллектуальная карта (РИК)** производства компании «Атлас-Телеком»	Работа с картой ПО ViPNet может производиться через любой PC/SC-совместимый считыватель.	Нет
Rosan Mifare	Смарт-карты **MIFARE** для считывателей компании «Розан»	Необходимо наличие COM-порта и считывателя от компании «Розан».	Нет
Siemens CardOS	Смарт-карты **CardOS/M4.01a**, **CardOS V4.3B**, **CardOS V4.2B**, **CardOS V4.2B DI**, **CardOS V4.2C**, **CardOS V4.4** производства компании Atos (Siemens)	На компьютере должно быть установлено ПО Siemens CardOS API V5.0 или более поздних версий.	Да

eToken GOST	Персональные электронные ключи **eToken ГОСТ** и **JaCarta ГОСТ** производства компании «Аладдин Р.Д.»	Создание ключей подписи возможно только по ГОСТ 34.10-2001, ГОСТ 34.10-2012 не поддерживается; перенос ключей подписи на данный тип устройств невозможен.	Да
Rutoken ECP/Rutoken Lite	**Рутокен ЭЦП**, **Рутокен Lite** — электронные идентификаторы производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken версии 2.89.00.0491. В программе ViPNet CSP настоятельно рекомендуется отключить поддержку устройств Рутокен. Создание ключей подписи возможно только по ГОСТ 34.10-2001, ГОСТ 34.10-2012 не поддерживается; перенос ключей подписи на данный тип устройств невозможен.	Да
Rutoken/ Rutoken S	**Рутокен**, **Рутокен S** — электронные идентификаторы производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken версии 2.89.00.0491. Постоянная корректная работа ПО ViPNet при использовании устройств Рутокен с драйверами указанной версии не гарантирована. Для гарантированной корректной работы ПО ViPNet рекомендуется использовать устройства другого типа.	Да
Shipka	ПСКЗИ **ШИПКА** (любой версии) производства компании «ОКБ САПР»	На компьютере должно быть установлено программное обеспечение ACShipka Environment версии не ниже 3.3.2.7. Проведите инициализацию устройства с помощью утилиты производителя «Параметры авторизации».	Да
eToken Aladdin	Персональные электронные ключи **eToken PRO (Java)**, **eToken PRO**, смарт-карты **eToken PRO (Java)**, **eToken PRO** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено программное обеспечение PKI Client версии 5.1 и выше. Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым USB-устройством считывания с карт.	Да
Smartcard	Смарт-карты с	Чтение и запись на смарт-карту	Нет

Athena	памятью типа I2C (ASE M4), синхронные смарт-карты с шиной 2/3 и защищенной памятью, удовлетворяющие стандарту ISO7816-3 (ASE MP42)	осуществляется через считыватель ASEDrive III PRO-S компании Athena. На компьютере должны быть установлены драйверы версии 2.5.0.0.	
iButton Accord	Электронные ключи **iButton** типа **DS1993**, **DS1994**, **DS1995** и **DS1996** для использования с платой Аккорд-5MX производства компании «ОКБ САПР»	Необходимо использование платы Аккорд-5MX На компьютере должен быть установлен драйвер версии не ниже 3.18.0.0.	Нет
iButton Aladdin	Электронные ключи **Dallas, iButton** типа **DS1993**, **DS1994**, **DS1995** и **DS1996**	К компьютеру должно быть подключено устройство считывания. На компьютере должно быть установлено программное обеспечение для обмена информации с iButton — 1-Wire Drivers версии 3.20 либо версии 4.0.3. На ОС Windows XP и Server 2003 совместно с ПО ViPNet может использоваться только ПО 1-Wire Drivers версии 3.20.	Нет

Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

Глоссарий

P

PKI (инфраструктура открытых ключей)

От англ. Public Key Infrastructure — инфраструктура открытых ключей. Комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам в распределенных системах через создание сертификатов открытых ключей и поддержание их жизненного цикла.

См. также: Открытый ключ (на стр. 208).

V

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками отозванных сертификатов.

См. также: Список отозванных сертификатов (СОС) (на стр. 210).

ViPNet Центр управления сетью (ЦУС)

В сети ViPNet CUSTOM ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

В сети ViPNet VPN Центр управления сетью — это рабочее место администратора сети ViPNet. В ЦУСе создается структура сети ViPNet, формируются и отправляются на сетевые узлы обновления наборов ключей и программного обеспечения ViPNet.

См. также: Клиент (ViPNet-клиент) (на стр. 207), Полномочия пользователя (на стр. 208), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 205).

Д

Дистрибутив ключей

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

См. также: Сетевой узел ViPNet (на стр. 210), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 205).

З

Закрытый ключ

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

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

См. также: Открытый ключ (на стр. 208), Электронная подпись (на стр. 211).

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, открытый ключ и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

См. также: Закрытый ключ (на стр. 206), Открытый ключ (на стр. 208), Сертификат открытого ключа подписи пользователя (на стр. 210), Электронная подпись (на стр. 211).

К

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

См. также: Сетевой узел ViPNet (на стр. 210).

Коллектив

Совокупность пользователей одного сетевого узла ViPNet, имеющих одни и те же ключи для шифрования конфиденциальной информации.

См. также: Сетевой узел ViPNet (на стр. 210).

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Контейнер ключей

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

См. также: Закрытый ключ (на стр. 206), Сертификат открытого ключа подписи пользователя (на стр. 210).

Корневой сертификат

Самоподписанный сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

См. также: Сертификат издателя (на стр. 209), Сертификат открытого ключа подписи пользователя (на стр. 210).

О

Общий коллектив

Коллектив, который автоматически регистрируется на сетевом узле и включает всех пользователей данного сетевого узла.

См. также: Коллектив (на стр. 207).

Открытый ключ

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

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

См. также: Закрытый ключ (на стр. 206), Электронная подпись (на стр. 211).

П

Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

См. также: Роль (на стр. 209), Сетевой узел ViPNet (на стр. 210).

Протокол Диффи — Хеллмана

Протокол открытого распределения ключей, позволяющий двум пользователям вырабатывать общий секретный ключ путем динамического взаимодействия на основе обмена открытыми сообщениями без какой-либо общей секретной информации, распределяемой заранее.

Р

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла `infotecs.reg` и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

См. также: Полномочия пользователя (на стр. 208), Сеть ViPNet (на стр. 210).

С

Сеансовый ключ

Случайный или производный ключ, предназначенный для шифрования одного сообщения.

Сертификат издателя

Сертификат уполномоченного лица удостоверяющего центра, которым заверяются издаваемые сертификаты.

См. также: Сертификат открытого ключа подписи пользователя (на стр. 210).

Сертификат открытого ключа подписи пользователя

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

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

См. также: Открытый ключ (на стр. 208), Электронная подпись (на стр. 211), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 205).

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью или ViPNet Network Manager.

См. также: ViPNet Центр управления сетью (ЦУС) (на стр. 205).

Сеть ViPNet

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

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

См. также: Сетевой узел ViPNet (на стр. 210).

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны или приостановлены администратором удостоверяющего центра и недействительны на момент, указанный в данном списке отозванных сертификатов.

Т

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на сетевые узлы ViPNet транспортным модулем ViPNet MFTP.

См. также: Транспортный модуль (MFTP) (на стр. 211).

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Ц

Цепочка сертификации

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

См. также: Корневой сертификат (на стр. 208), Сертификат открытого ключа подписи пользователя (на стр. 210).

Э

Электронная подпись

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

См. также: Закрытый ключ (на стр. 206), Сертификат открытого ключа подписи пользователя (на стр. 210).

Указатель