ViPNet Деловая почта 4

Руководство пользователя

infotecs

ФРКЕ.00116-03 34 03

Версия продукта 4.5.1

ОАО «ИнфоТеКС»

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

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

Веб-сайт: https://infotecs.ru/

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение ... **8**
О документе ... 9
Для кого предназначен документ ... 9
Соглашения документа ... 9
О программе ... 10
Системные требования ... 11
Новые возможности версии 4.5.1 ... 12
Обратная связь ... 13

Глава 1. Быстрый старт ... **14**
Перед началом работы ... 15
Как написать письмо ... 16
Как подписать письмо электронной подписью ... 17
Как прочитать письмо ... 18
Как ответить на письмо ... 19
Как удалить письмо ... 20

Глава 2. Начало работы с программой ViPNet Деловая почта ... **21**
Установка программы ... 22
Запуск и завершение работы с программой ... 23
Смена пользователя ... 24
Способы аутентификации пользователя ... 25
Пароль ... 26
Пароль на устройстве ... 27
Устройство ... 28
Особенности аутентификации с помощью сертификата ... 29
Интерфейс программы ... 32
Организация хранения писем с помощью папок ... 35
Основные папки ... 35
Пользовательские папки ... 36
Адресная книга ... 38
Основная адресная книга ... 39
Пользовательские адресные книги ... 39
Создание пользовательской адресной книги ... 39
Редактирование пользовательской адресной книги ... 40

Добавление и просмотр информации о контакте 41
Обмен информацией о контактах 42
Создание группы рассылки 43
Назначение пользовательской адресной книги книгой по умолчанию 44

Глава 3. Работа с письмами 45
Создание и отправка нового письма 46
Окно создания и просмотра писем 46
Создание письма 47
Запрос извещений о доставке и прочтении в виде отдельного письма 50
Отправка письма в виде вложения 51
Создание и использование шаблонов писем 52
Просмотр письма и его свойств в основном окне программы 53
Просмотр письма и вложений в отдельном окне 56
Ответ на письмо и пересылка письма 58
Поиск писем 60
Экспорт и импорт писем 62
Экспорт писем 62
Импорт писем 63
Перенос писем в другую папку программы 64
Удаление писем 65
Архивация писем 66
Работа с архивами писем 68

Глава 4. Электронная подпись и шифрование 70
Электронная подпись в программе ViPNet Деловая почта 71
Работа с электронной подписью писем 72
Подписание письма 72
Подписание другим сертификатом 73
Использование ключа электронной подписи и ключа проверки электронной подписи, созданных с помощью стороннего криптопровайдера 75
Проверка электронной подписи письма 76
Удаление электронной подписи письма 77
Работа с электронной подписью файлов 79
Подписание файла 79
Открепление и прикрепление подписи файла 80
Проверка электронной подписи файла 80
Удаление электронной подписи файла 81
Шифрование и расшифрование писем 83

Глава 5. Работа с сертификатами и ключами **84**
Просмотр сертификатов 85
Просмотр текущего сертификата пользователя 86
Просмотр личных сертификатов пользователя 86
Просмотр доверенных корневых сертификатов 87
Просмотр изданных сертификатов 87
Просмотр цепочки сертификации 87
Просмотр полей сертификата и печать сертификата 88
Управление сертификатами 89
Установка сертификатов в хранилище операционной системы 90
Установка в хранилище автоматически 90
Установка в хранилище вручную 92
Смена текущего сертификата 95
Обновление ключа электронной подписи и сертификата 96
Настройка оповещения об истечении срока действия ключа электронной подписи и сертификата 97
Процедура обновления ключа электронной подписи и сертификата 98
Ввод сертификата в действие 104
Ввод в действие автоматически 104
Ввод в действие вручную 105
Работа с запросами на сертификаты 105
Просмотр запроса на сертификат 105
Удаление запроса на сертификат 106
Экспорт сертификата 107
Форматы экспорта сертификатов 108
Работа с контейнером ключей 110
Смена пароля к контейнеру 112
Удаление сохраненного на компьютере пароля к контейнеру ключей 113
Проверка контейнера ключей 114
Установка контейнера ключей 114
Перенос контейнера ключей 116
Установка сертификата в контейнер ключей 116

Глава 6. Автопроцессинг **118**
Принцип работы автопроцессинга 119
Настройка правил автопроцессинга 122
Создание правила для исходящих файлов 123
Создание правила для входящих писем 126
Копирование правил автопроцессинга 130

Оптимизация работы автопроцессинга ... 132
Просмотр журнала автопроцессинга ... 133
Настройка параметров журнала автопроцессинга ... 136

Глава 7. Настройка программы ... 138
Настройка общих параметров ... 139
Настройка архивации писем ... 141
Общие параметры архивации ... 141
Параметры автоматической архивации ... 142
Настройка параметров работы с письмами ... 145
Настройка печати ... 147
Настройка внешних программ ... 148
Работа в программе с правами администратора ... 150
Дополнительные настройки и возможности программы ... 150
Дополнительные настройки параметров безопасности ... 151
Изменение способа аутентификации пользователя ... 152

Глава 8. Настройка параметров безопасности ... 154
Смена пароля пользователя ... 155
Выбор собственного пароля ... 156
Выбор пароля на основе парольной фразы ... 156
Выбор цифрового пароля ... 158
Настройка параметров шифрования ... 159
Настройка параметров криптопровайдера ViPNet CSP ... 161
Настройка автоматической установки сертификатов в системное хранилище ... 163

Приложение А. Возможные неполадки и способы их устранения ... 164
Не удается выполнить аутентификацию с помощью сертификата ... 165
Невозможна отправка писем из программы ViPNet Деловая почта ... 166
Письмо упаковано, но не отправлено ... 166
Проверка соединения с координатором ... 166
Просмотр информации в журнале IP-пакетов ... 167
Письмо отправлено, но не доставлено ... 168
Входящее письмо перемещено в папку Проблемные или Поврежденные ... 168
Не удается зашифровать вложение ... 170
Ошибка отправки письма: Ключ не найден ... 170
Невозможно выполнить правило автопроцессинга ... 171

Приложение В. Общие сведения о сертификатах ключей проверки электронной подписи ... 172

Определение и назначение ... 173
Структура ... 176
PKI и асимметричная криптография ... 179
Использование сертификатов для шифрования электронных документов ... 182
Зашифрование ... 182
Расшифрование ... 183
Использование сертификатов для подписания электронных документов ... 185
Подписание ... 185
Проверка подписи ... 186
Использование сертификатов для подписания и шифрования электронных документов ... 187
Подписание и зашифрование ... 187
Расшифрование и проверка ... 188

Приложение C. Внешние устройства ... 190
Общие сведения ... 191
Список поддерживаемых внешних устройств ... 191
Алгоритмы и функции, поддерживаемые внешними устройствами ... 195

Приложение D. История версий ... 198
Что нового 4.5.0 ... 199
Что нового 4.3.4 ... 200
Что нового 4.3.3 ... 201
Что нового 4.3.2 ... 202

Приложение E. Глоссарий ... 204

Приложение F. Указатель ... 209

Введение

О документе 9

О программе 10

Системные требования 11

Новые возможности версии 4.5.1 12

Обратная связь 13

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. глоссарий, стр. 207). 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® for Windows (далее — 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 for Windows. 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.
- Письма программы ViPNet Деловая почта зашифрованы на ключах адресата (см. Адресная книга на стр. 38) 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. 118).

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 1 Гбайт.
- Свободное место на жестком диске — не менее 500 Мбайт (рекомендуется 1 Гбайт).
- Сетевой интерфейс (не более 10 IP-адресов на одном сетевом интерфейсе) или модем.
- Операционная система:
  - Windows Server 2008 R2 (64-разрядная);
  - Windows 7 (32/64-разрядная);
  - Windows 8 (32/64-разрядная);
  - Windows 8.1 (32/64-разрядная);
  - Windows Server 2012 (64-разрядная);
  - Windows Server 2012 R2 (64-разрядная);
  - Windows 10 (32/64-разрядная) следующих версий и сборок:
    - версия 1507, сборка 10240,
    - версия 1511, сборка 10586,
    - версия 1607, сборка 14393,
    - версия 1703, сборка 15063,
    - версия 1709, сборка 16299,
    - версия 1803, сборка 17134,
    - версия 1809, сборка 17763.55;
  - Windows Server 2016 (64-разрядная), сборка 14393.
- Для операционной системы должен быть установлен самый последний накопительный пакет обновлений.

  Для ОС Windows 7 и Windows Server 2008 R2 на компьютере необходим пакет обновления часовых поясов KB2570791, а также KB3033929 или KB3125574 и Microsoft .NET Framework версии 4.5.

Новые возможности версии 4.5.1

В этом разделе представлен краткий обзор изменений в версии 4.5.1 по сравнению с 4.5.0. Информация об изменениях в предыдущих версиях содержится в приложении История версий (на стр. 198).

- **Поддержка Windows 10 версии 1809 (сборка 17763.55)**
- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

Обратная связь

Дополнительная информация

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

- Информация о продуктах ViPNet https://infotecs.ru/product/.
- Информация о решениях ViPNet https://infotecs.ru/resheniya/.
- Часто задаваемые вопросы https://infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet https://infotecs.ru/forum/.

Контактная информация

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

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт https://infotecs.ru/support/request/.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

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

1

Быстрый старт

Перед началом работы 15

Как написать письмо 16

Как подписать письмо электронной подписью 17

Как прочитать письмо 18

Как ответить на письмо 19

Как удалить письмо 20

Перед началом работы

Глава содержит краткие указания по использованию основных возможностей программы ViPNet Деловая почта. Эта информация поможет приступить к работе без подробного изучения 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. 45).

Использование криптографических возможностей программы описано в главе Электронная подпись и шифрование (на стр. 70), автоматическая обработка писем и файлов — в главе Автопроцессинг (на стр. 118).

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, при необходимости измените формат текста письма.

3 Если в письмо требуется вложить файлы, на панели инструментов нажмите кнопку **Вложения**  и в окне **Открыть** выберите нужные файлы.

Примечание. Общий размер письма с вложениями не должен превышать 2 Гбайт, если администратором сети не установлено меньшее ограничение.

---

4 Если необходимо зашифровать письмо, нажмите кнопку **Шифровать**  .

5 Если необходимо подписать письмо электронной подписью, нажмите кнопку **Подписать**  и выберите сертификат для подписи.

6 Нажмите кнопку **Получатели**  и в окне **Выбрать контакты** укажите получателей.

7 Нажмите кнопку **Отправить**  .

Подробнее см. раздел Создание и отправка нового письма (на стр. 46).

Как подписать письмо электронной подписью

Чтобы подписать письмо электронной подписью, выполните следующие действия:

- Если письмо открыто в окне редактирования письма, нажмите кнопку **Подписать**  и выберите сертификат для подписи.
- Если письмо сохранено в папку **Исходящие** или ее подпапку и еще не отправлено:
  - Выберите письмо в списке.
  - Нажмите кнопку **Подписать**  и выберите сертификат для подписи.

Подробнее см. раздел Подписание письма (на стр. 72).

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.

Внимание! Если вы не запускали программу ViPNet Деловая почта более 30 дней, недоставленные входящие письма, отправленные 30 дней назад или раньше, будут помещены в папку **Поврежденные** (см. Входящее письмо перемещено в папку Проблемные или Поврежденные на стр. 168).

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. 56).

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. 16).

Подробнее см. раздел Ответ на письмо и пересылка письма (на стр. 58).

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).

2

Начало работы с программой ViPNet Деловая почта

Установка программы 22

Запуск и завершение работы с программой 23

Способы аутентификации пользователя 25

Интерфейс программы 32

Организация хранения писем с помощью папок 35

Адресная книга 38

Установка программы

Программа ViPNet Деловая почта является одним из компонентов программного обеспечения ViPNet Client. В рамках ПО ViPNet программа ViPNet Деловая почта по умолчанию устанавливается на компьютер вместе с основным компонентом ViPNet Монитор. Подробнее об установке ПО ViPNet Client см. документ «ViPNet Client. 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.

Примечание. Программу ViPNet Деловая почта можно использовать только на сетевых узлах с ролью «Business Mail». 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:

- В окне программы ViPNet Монитор в меню **Приложения** выберите пункт **Деловая почта**. Аутентификация пользователя в этом случае не требуется.
- При получении новых писем появится оповещение транспортного модуля MFTP. Установите флажок **Вызвать программу Деловая почта**, нажмите кнопку **OK** и выполните аутентификацию.

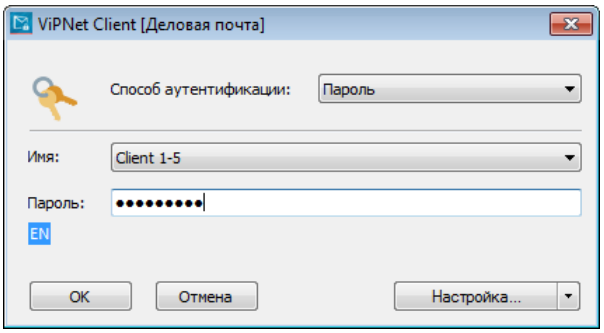


Рисунок 1. Окно входа в программу

Если ранее аутентификация уже была выполнена в программе ViPNet Монитор, то откроется главное окно программы ViPNet Деловая почта.

- В меню **Пуск** начните вводить «Деловая почта» или 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 введите пароль пользователя либо подключите внешнее устройство хранения данных и введите ПИН-код. Затем нажмите кнопку **OK**. Откроется окно программы ViPNet Деловая почта.

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. 139) 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. Чтобы войти под своей учетной записью, выполните следующие действия:

1 В окне программы ViPNet Деловая почта в меню **Инструменты** выберите пункт **Смена пользователя**. Откроется окно входа в программу (см. Рисунок 1 на стр. 23).

2 Введите свой пароль пользователя и нажмите **ОК**.

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. 26). 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. 27). Для входа в программу вам следует подключить устройство и ввести ПИН-код.

  Использование этого способа аутентификации предполагает, что ваш пароль хранится на устройстве и вам не известен. Однако если вы знаете пароль, то для входа в программу можно использовать и 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 используется для совместимости с программным обеспечением ViPNet ранних версий. Если версия программы ViPNet — 3.2 и выше и в ней используется данный способ аутентификации измените его на **Пароль** или **Устройство**.

- Устройство (на стр. 28). Для входа в программу вам следует подключить устройство и ввести ПИН-код (и в некоторых случаях пароль).

По умолчанию установлен способ аутентификации **Пароль**. Изменить способ аутентификации можно при входе в программу. Кроме того, способ аутентификации удаленно может изменить администратор сети ViPNet, отправив на ваш узел политику безопасности из программы ViPNet Policy Manager.

При использовании способов **Пароль на устройстве** и **Устройство** аутентификация пользователя осуществляется с помощью внешних устройств (см. Внешние устройства на стр. 190). Чтобы использовать какое-либо устройство для аутентификации, на компьютер необходимо установить драйверы этого устройства и затем записать на него ключи. Записать ключи на внешнее устройство можно при изменении способа аутентификации пользователя или в программе ViPNet Удостоверяющий и ключевой центр при создании дистрибутива ключей.

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.

Уровень безопасности при входе в программу определяется количеством факторов аутентификации. Чем оно больше, тем выше уровень безопасности. Нульфакторная аутентификация не обеспечивает безопасный вход в программу и не рекомендуется к использованию.

На схеме ниже представлены возможные способы аутентификации и их факторность.

Сохранение в реестре Windows ПИН-кода или пароля при способе **Устройство** превращает аутентификацию в однофакторную, а при способе **Пароль** – в нульфакторную.

Рисунок 2. 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**.

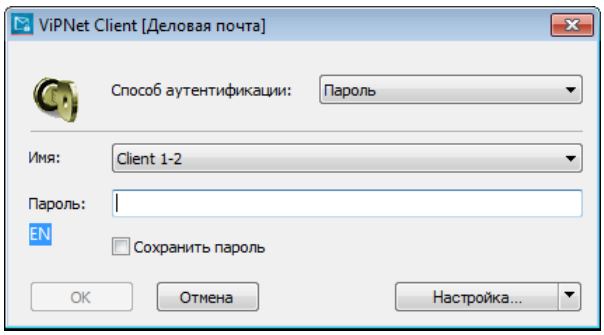


Рисунок 3. Способ аутентификации «Пароль»

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. 151), 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. 152).

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**.

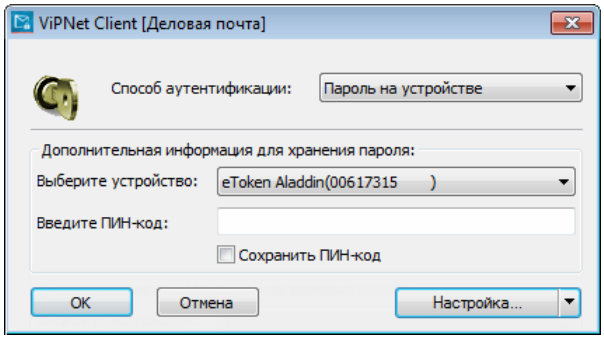


Рисунок 4. Способ аутентификации «Пароль на устройстве»

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 2 на стр. 26).

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**.

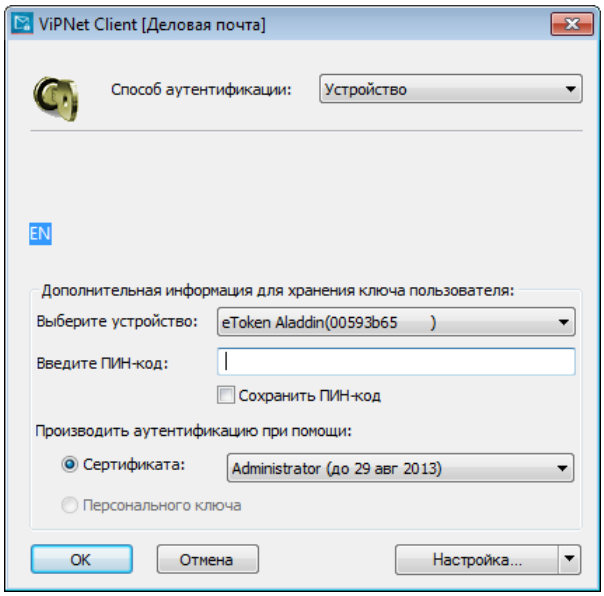


Рисунок 5. Способ аутентификации «Устройство»

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 2 на стр. 26).

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

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** — для аутентификации с помощью сертификата, который хранится на вашем устройстве. В списке сертификатов, обнаруженных на устройстве, выберите нужный сертификат.

  Требования, предъявляемые к сертификатам для аутентификации, представлены в разделе Особенности аутентификации с помощью сертификата (на стр. 29). В случае возникновения затруднений см. раздел Не удается выполнить аутентификацию с помощью сертификата (на стр. 165).

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

7 Нажмите кнопку **ОК**.

Особенности аутентификации с помощью сертификата

Для аутентификации в программе ViPNet Деловая почта с помощью сертификата должны быть выполнены следующие условия:

- Внешнее устройство поддерживает стандарт PKCS#11.
- Аутентификация с помощью сертификата ГОСТ выполняется с помощью устройства, на котором реализована аппаратная поддержка алгоритмов ГОСТ.

Примечание. Информация о том, какие внешние устройства обеспечивают аппаратную поддержку алгоритмов ГОСТ и поддержку стандарта PKCS#11, содержится в разделе Алгоритмы и функции, поддерживаемые внешними устройствами (на стр. 195). В таблице такие устройства вы можете найти по содержимому столбцов **Аппаратная поддержка российских криптографических алгоритмов (на устройстве)** и **Поддержка PKCS#11**.

- Закрытый ключ, соответствующий сертификату ГОСТ, который используется для аутентификации, сформирован с помощью криптопровайдера ViPNet CSP.
- Сертификат имеет назначение «Шифрование ключей» в поле **Использование ключа**.

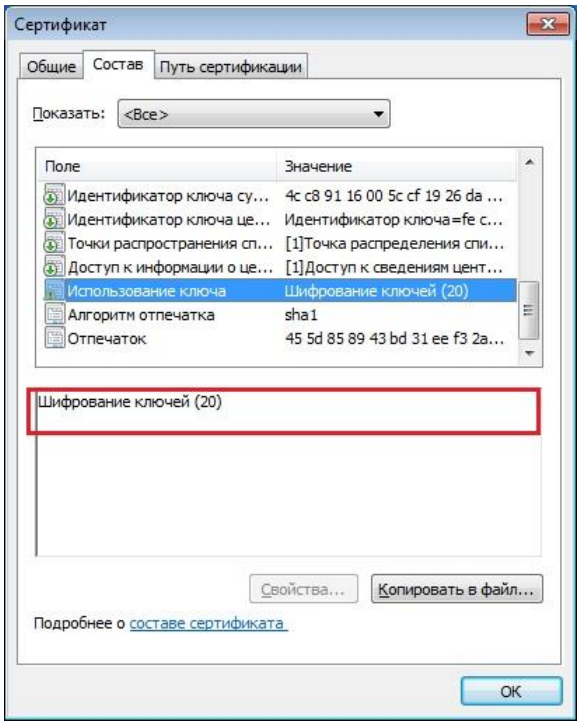


Рисунок 6. Проверка наличия назначения «Шифрование ключей» в сертификате для аутентификации

- В контейнере на устройстве находится закрытый ключ, которому соответствует используемый сертификат.
- Сертификат действителен, то есть срок его действия не истек, он не находится в списке аннулированных сертификатов доверенного удостоверяющего центра, соответствующая ему цепочка сертификации полна, и все входящие в нее сертификаты также действительны.
- В хранилище операционной системы установлены соответствующий список аннулированных сертификатов и все сертификаты из цепочки сертификации, включая корневой сертификат. Для аутентификации в программе до входа в ОС сертификаты и список аннулированных сертификатов установлены в хранилище локального компьютера.

Примечание. При необходимости установки корневого сертификата и списка аннулированных сертификатов в хранилище **Локальный компьютер** ОС Windows 7 или Windows Server 2008 следует запускать программу ViPNet CSP от имени администратора ОС (с помощью команды **Запуск от имени администратора** (**Run as Administrator**) контекстного меню ярлыка). Подробнее см. в документе «ViPNet CSP. Руководство пользователя» раздел «Установка сертификата, не добавленного в контейнер ключей».

В случаях с другими версиями ОС Windows можно также воспользоваться программой ViPNet CSP либо выполнить установку корневого сертификата и списка аннулированных сертификатов стандартными средствами Windows.

Чтобы получить сертификат ГОСТ, подходящий для аутентификации в ПО ViPNet Деловая почта, выполните следующие действия:

1 Создайте запрос на сертификат. При этом сохраните контейнер ключей на внешнее устройство (см. Обновление ключа электронной подписи и сертификата на стр. 96).

2. Предупредите администратора удостоверяющего центра о том, что при издании сертификата в него необходимо добавить назначение «Проверка подлинности клиента». Если обработка запросов на сертификаты производится в автоматическом режиме, администратору следует отключить этот режим и обработать ваш запрос вручную.
3. Установите изданный сертификат в контейнер ключей, сохраненный на устройстве.

Интерфейс программы

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

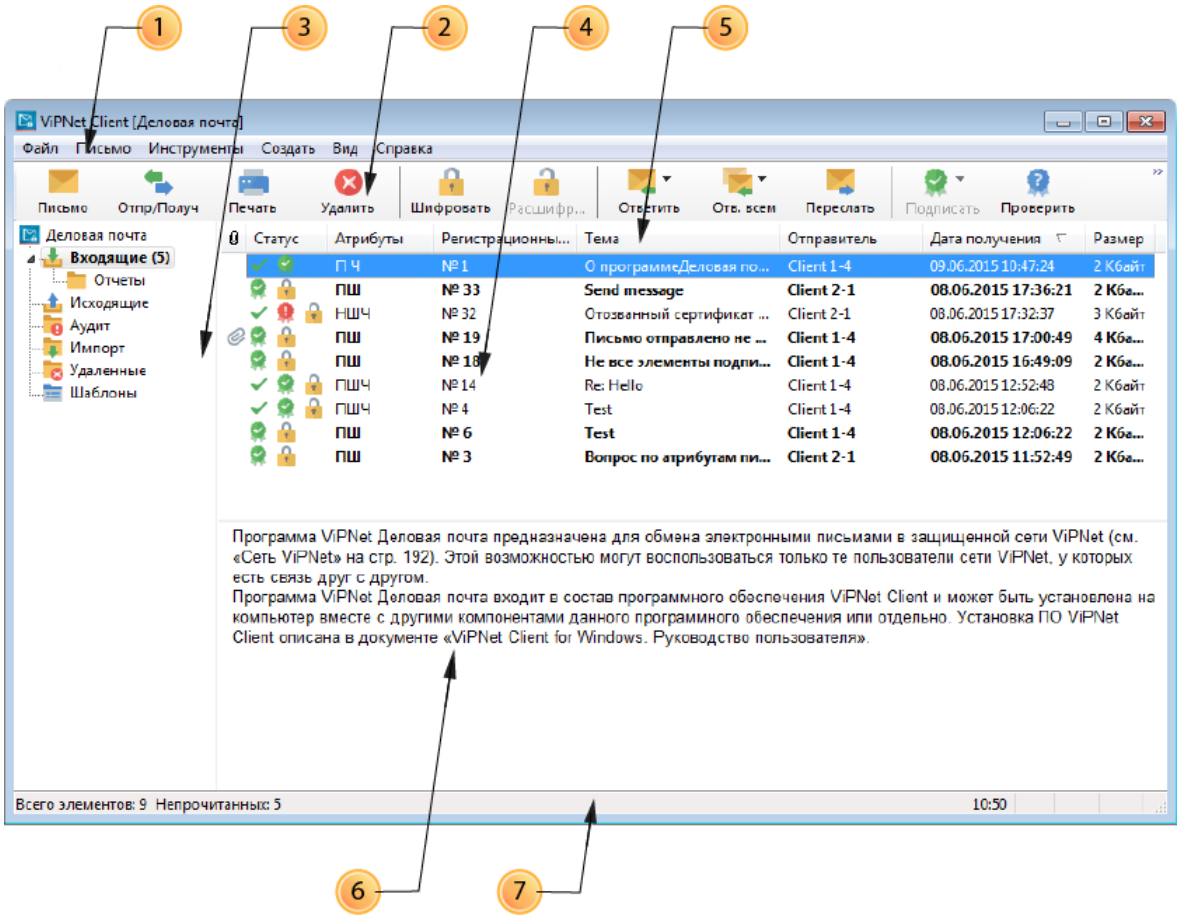


Рисунок 7. Интерфейс программы ViPNet Деловая почта

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. 32).

Папки в программе ViPNet Деловая почта делятся на две категории:

- Основные — 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.

Основные папки

Возможности работы с основными папками программы ViPNet Деловая почта ограничены. Основные 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. 53).
- **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. 50).

  Эта папка создается при получении первого извещения, по умолчанию она отсутствует.
- **Исходящие** — папка, в которую помещаются создаваемые письма (см. Создание письма на стр. 47).
- **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. 150).

- **Аудит** > **Поврежденные** — папка, содержащая входящие письма, при обработке которых произошла критическая ошибка, и письмо не подлежит восстановлению.
- **Аудит** > **Проблемные** — папка, содержащая входящие письма, при получении которых произошла ошибка, которая может быть устранена.

Примечание. Папки **Поврежденные** и **Проблемные** автоматически создаются при появлении первой ошибки, по умолчанию они отсутствуют (см. Входящее письмо перемещено в папку Проблемные или Поврежденные на стр. 168).

Вы можете удалять письма из подпапок **Поврежденные** и **Проблемные** только при работе в режиме администратора.

- **Шаблоны** — папка, в которую помещаются шаблоны писем (см. Создание и использование шаблонов писем на стр. 52).
- **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. 32) 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. Основные папки на стр. 35) создание новых папок невозможно.

Чтобы переименовать папку:

1 На панели папок (см. Интерфейс программы на стр. 32) 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**.
- В меню **Файл** выберите пункт **Папки** и затем **Переименовать**.

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 основные папки (см. Основные папки на стр. 35).

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. 150).

Адресная книга

Контакты, доступные для ведения переписки, хранятся в адресной книге программы ViPNet Деловая почта. Список контактов определяется связями между пользователями сети ViPNet, 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**.

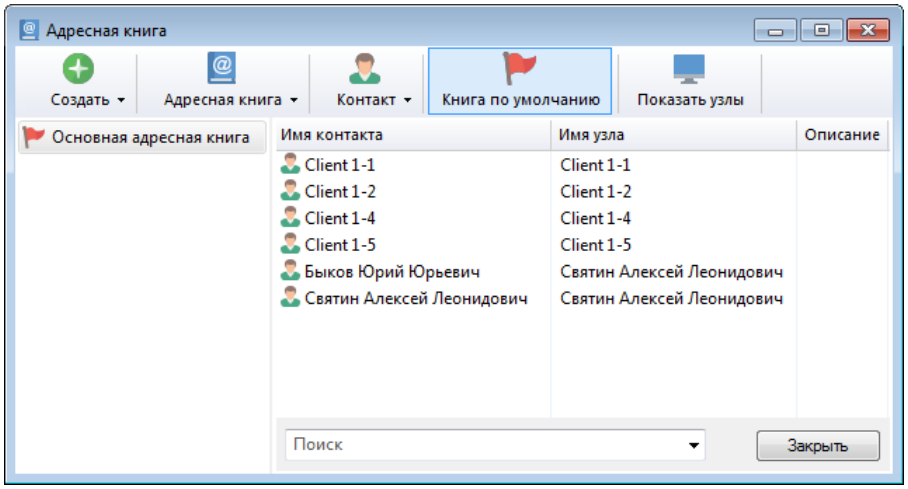


Рисунок 8. Адресная книга программы ViPNet Деловая почта

В программе ViPNet Деловая почта предусмотрены два типа списков контактов: основная адресная книга, доступная пользователю по умолчанию, и пользовательские адресные книги, которые вы можете создать самостоятельно. Количество создаваемых пользовательских адресных книг не ограничено. Список адресных книг отображается на левой панели окна **Адресной книги**.

Каждой записи в адресной книге программы ViPNet Деловая почта может соответствовать один из трех уровней адресации:

- Сетевой узел. Этот уровень адресации соответствует всем пользователям узла. То есть зашифрованное письмо, адресованное узлу, могут прочитать все его пользователи. Для отображения сетевых узлов нажмите кнопку **Показать узлы**  на панели инструментов.
- Пользователь. Этот уровень соответствует конкретному пользователю узла. Письмо, адресованное пользователю, может прочесть только он.
- Группа рассылки. Этот уровень адресации возможен только в пользовательской адресной книге и соответствует всем пользователям и узлам, объединенным в одну группу, которую создает сам пользователь. Письмо, адресованное группе, смогут прочитать все участники группы. Группа рассылки отображается в списке адресных книг под той адресной книгой, в которой она была создана.

Основная адресная книга

По умолчанию в программе ViPNet Деловая почта пользователю доступен только один список контактов — основная адресная книга. Она содержит в себе все доступные пользователю контакты с незаполненными данными.

Вы можете использовать основную адресную книгу при создании писем (см. Создание письма на стр. 47), но основная адресная книга не может быть изменена пользователем сетевого узла. То есть вы не можете добавлять в нее группы рассылки, удалять контакты или редактировать данные контактов. Поэтому для более гибкой настройки списков контактов мы рекомендуем создавать пользовательские адресные книги (см. Создание пользовательской адресной книги на стр. 39), а основную адресную книгу использовать в качестве справочника, в котором содержится полный список ваших контактов.

Пользовательские адресные книги

По сравнению с основной адресной книгой пользовательские адресные книги обладают более широкими возможностями для настройки списков контактов. После создания пользовательской адресной книги вы сможете:

- создавать группы рассылки (см. Создание группы рассылки на стр. 43);
- редактировать данные контактов (см. Добавление и просмотр информации о контакте на стр. 41);
- назначать пользовательскую книгу адресной книгой по умолчанию (см. Назначение пользовательской адресной книги книгой по умолчанию на стр. 44);
- обмениваться данными контактов (см. Обмен информацией о контактах на стр. 42);
- переименовывать адресную книгу и редактировать список контактов (см. Редактирование пользовательской адресной книги на стр. 40).

Основную и пользовательские адресные книги можно использовать для создания других адресных книг.

Создание пользовательской адресной книги

Чтобы создать пользовательскую адресную книгу, вы можете:

- импортировать сохраненную ранее книгу и затем удалить из нее ненужные контакты;
- создать пустую адресную книгу и скопировать нужные контакты из других адресных книг.

Чтобы импортировать существующую адресную книгу:

1 В окне **Адресная книга** (см. Рисунок 8 на стр. 38) выберите адресную книгу.

2 На панели инструментов нажмите кнопку **Адресная книга**  , а затем выберите команду **Экспортировать**.

3 В окне **Сохранить как** введите имя адресной книги, укажите путь сохранения файла и нажмите кнопку **Сохранить**.

Адресная книга будет экспортирована в файл.

4 На панели инструментов нажмите кнопку **Адресная книга**  , а затем выберите команду **Импортировать**.

5 В окне **Открыть** выберите файл экспортированной адресной книги и нажмите кнопку **Открыть**.

Будет создана адресная книга, содержащая все импортированные контакты.

6 Удалите ненужные контакты (см. Редактирование пользовательской адресной книги на стр. 40).

Примечание. При импорте адресной книги всегда происходит автоматическое создание новой пользовательской адресной книги. Вы не можете импортировать данные в существующую адресную книгу.

Чтобы создать новую пользовательскую адресную книгу, выполните следующие действия:

1 В окне **Адресная книга** (см. Рисунок 8 на стр. 38) на панели инструментов нажмите кнопку **Создать**  и затем выберите пункт **Адресную книгу**. В списке адресных книг появится поле для ввода названия новой адресной книги.

2 Введите название адресной книги и нажмите клавишу **Enter**.

Будет создана пустая пользовательская адресная книга.

3 Добавьте нужные контакты (см. Редактирование пользовательской адресной книги на стр. 40).

Если вам больше не требуется пользовательская адресная книга, вы можете удалить ее.

Редактирование пользовательской адресной книги

Вы можете добавлять в пользовательскую адресную книгу только те контакты, связи с которыми были заданы для вашего сетевого узла администратором сети ViPNet. Полный список контактов, доступных для добавления, находится в основной адресной книге (см. Основная адресная книга на стр. 39).

Чтобы добавить контакт, выполните следующие действия:

1 В окне **Адресная книга** (см. Рисунок 8 на стр. 38) выберите адресную книгу с нужным вам контактом.

2 На панели просмотра в списке пользователей и узлов щелкните пользователя или узел и перетащите его в свою адресную книгу.

Совет. Если список пользователей слишком большой, чтобы найти контакт, в строку поиска в нижней части окна введите часть имени нужного контакта.

3 В появившемся окне нажмите кнопку **Да**, чтобы при добавлении контакта также скопировать все его данные.

Контакт будет скопирован в адресную книгу.

Чтобы удалить ненужный контакт из адресной книги, выполните следующие действия:

1 В окне **Адресная книга** выберите пользовательскую адресную книгу.

2 На панели просмотра выберите пользователя или узел, который хотите удалить.

3 На панели инструментов нажмите кнопку **Контакт**  , а затем выберите команду **Удалить**. Контакт будет удален из пользовательской адресной книги.

Чтобы переименовать адресную книгу, выполните следующие действия:

1 В окне **Адресная книга** выберите пользовательскую адресную книгу.

2 На панели инструментов нажмите кнопку **Адресная книга**  , а затем выберите команду **Переименовать**. На месте названия адресной книги появится поле ввода.

3 Введите новое название адресной книги и нажмите клавишу **Enter**.

Добавление и просмотр информации о контакте

По умолчанию в основной адресной книге отсутствует какая-либо информация о контактах. Если у вас есть дополнительные сведения о контакте и вы хотите хранить их в адресной книге, выполните следующие действия:

1 В окне **Адресная книга** (см. Рисунок 8 на стр. 38) выберите пользовательскую адресную книгу.

2 На панели просмотра выберите пользователя или узел.

3 На панели инструментов нажмите кнопку **Контакт**  и выберите пункт **Свойства**.

4 В окне **Свойства адресата** заполните или отредактируйте нужные поля и нажмите кнопку **OK**.

Сведения о контакте будут сохранены в пользовательской адресной книге.

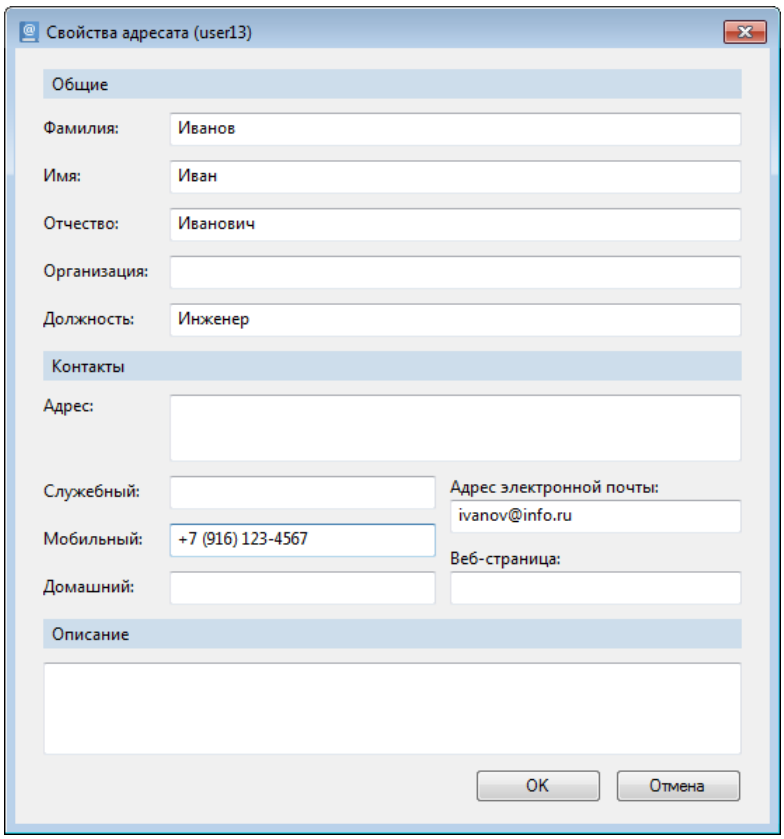


Рисунок 9: Добавление информации о контакте

Примечание. Если у вас есть несколько адресных книг, содержащих один и тот же контакт, данные контакта будут сохранены только в той адресной книге, которая была выбрана на шаге 1. Чтобы обновить информацию о контакте в другой адресной книге, добавьте в нее контакт с обновленными данными (см. Редактирование пользовательской адресной книги на стр. 40).

Если ваша пользовательская адресная книга содержит много контактов, чтобы быстро оценить, для каких контактов дополнительные сведения не были еще указаны, вы можете выбрать, какие сведения о них отображать на панели просмотра списка контактов в окне **Адресная книга**. Для этого на панели просмотра списка контактов щелкните правой кнопкой мыши заголовок любого столбца и с помощью контекстного меню добавьте или удалите столбцы.

Обмен информацией о контактах

Обмен информацией о контактах — еще один способ выполнить обновление данных контактов в пользовательской адресной книге. Если у вас нет дополнительных сведений о контакте, вы можете запросить у других пользователей из вашего списка контактов файл адресной книги, содержащий нужные контакты с дополнительной информацией. Либо вы сами по запросу других пользователей можете отправить файл адресной книги с данными, которые имеются у вас.

Чтобы отправить запрашиваемые данные, выполните следующие действия:

1 Создайте пользовательскую адресную книгу (см. Создание пользовательской адресной книги на стр. 39) с контактами, информацию о которых требуется передать другому пользователю.

2 В окне **Адресная книга** выберите созданную адресную книгу.

3 На панели инструментов нажмите кнопку **Адресная книга**  , а затем выберите команду **Отправить**.

4 В окне **Введите описание вложения** укажите имя адресной книги и нажмите кнопку **Добавить**. Откроется новое письмо с вложенной адресной книгой.

5 Нажмите кнопку **Отправить**  .

Примечание. Вы можете передать адресную книгу не только по Деловой почте, но и другим удобным способом. Для этого в меню **Адресная книга** выберите команду **Экспортировать** и передайте файл с адресной книгой другим пользователям. Для добавления полученной адресной книги в меню **Адресная книга** выберите команду **Импортировать**.

Если вы запрашивали данные контактов у другого пользователя и получили письмо с файлом адресной книги, чтобы обновить данные в своей адресной книге, выполните следующие действия:

1 Откройте письмо (см. Как прочитать письмо на стр. 18) и на вкладке **Вложения** дважды щелкните файл адресной книги.

Будет создана новая адресная книга.

Внимание! В созданную адресную книгу войдут только те контакты, связи с которыми были заданы для вашего сетевого узла администратором сети ViPNet.

Если в переданном вам файле адресной книги хранятся контакты, с которыми у вас нет установленных связей, они не будут добавлены в созданную адресную книгу.

Если в переданном вам файле адресной книги нет ни одного контакта, связанного с вами, появится сообщение о невозможности создания адресной книги.

2 Добавьте полученные контакты с данными в свою адресную книгу (см. Редактирование пользовательской адресной книги на стр. 40).

Создание группы рассылки

Если вы регулярно отправляете письма одной и той же группе получателей, объедините их в группу рассылки. В дальнейшем при создании письма (см. Создание письма на стр. 47) в адресной книге достаточно будет выбрать только созданную группу, и письмо будет доставлено каждому пользователю сети ViPNet, входящему в эту группу рассылки.

Количество контактов, которые можно включить в группу рассылки, не ограничено.

Чтобы создать группу рассылки, выполните следующие действия:

1 В окне **Адресная книга** (см. Рисунок 8 на стр. 38) выберите пользовательскую адресную книгу.

2 На панели инструментов нажмите кнопку **Создать**  и затем выберите пункт **Группу рассылки**. В списке адресных книг под названием адресной книги появится поле для ввода имени группы.

3 Введите имя созданной группы и нажмите клавишу **Enter**.

4 Чтобы скопировать контакт в новую группу, выберите в списке адресных книг адресную книгу, затем на панели просмотра щелкните нужного пользователя или узел и перетащите его в группу.

Примечание. Если в группу рассылки, созданную в одной пользовательской адресной книге, добавляется контакт из другой адресной книги, появится сообщение о копировании контакта из одной адресной книги в другую. Если вы хотите скопировать контакт вместе с его данными, нажмите кнопку **Да**. Если вы хотите скопировать только сам контакт без дополнительных сведений о нем, нажмите кнопку **Нет**.

Чтобы переименовать группу, выполните следующие действия:

1 В окне **Адресная книга** щелкните правой кнопкой мыши группу рассылки и в контекстном меню выберите команду **Переименовать**. На месте имени группы появится поле ввода.

2 Введите новое имя группы и нажмите клавишу **Enter**.

Чтобы удалить ненужную группу, выполните следующие действия:

1 В окне **Адресная книга** щелкните правой кнопкой мыши группу рассылки и в контекстном меню выберите команду **Удалить**.

2 В окне сообщения нажмите кнопку **Да**, группа будет удалена.

Назначение пользовательской адресной книги книгой по умолчанию

При создании письма (см. Создание письма на стр. 47) в окне выбора получателей отображается список контактов из адресной книги, назначенной книгой по умолчанию. Автоматически в программе ViPNet Деловая почта книгой по умолчанию назначается основная адресная книга. Поэтому для выбора другой адресной книги необходимо развернуть список в правом верхнем углу окна выбора получателей (см. Рисунок 11 на стр. 49).

Вы можете назначить книгой по умолчанию свою часто используемую адресную книгу, чтобы при создании письма не выбирать ее каждый раз из списка. Выполните следующие действия:

1 В окне **Адресная книга** (см. Рисунок 8 на стр. 38) выберите пользовательскую адресную книгу.

2 На панели инструментов нажмите кнопку **Книга по умолчанию**  .

Выбранная адресная книга будет отмечена соответствующим значком.

3

Работа с письмами

Создание и отправка нового письма 46

Создание и использование шаблонов писем 52

Просмотр письма и его свойств в основном окне программы 53

Просмотр письма и вложений в отдельном окне 56

Ответ на письмо и пересылка письма 58

Поиск писем 60

Экспорт и импорт писем 62

Перенос писем в другую папку программы 64

Удаление писем 65

Архивация писем 66

Работа с архивами писем 68

Создание и отправка нового письма

Окно создания и просмотра писем

Внешний вид окна, в котором осуществляется создание новых писем (см. Создание письма на стр. 47) и просмотр отправленных и полученных писем (см. Просмотр письма и вложений в отдельном окне на стр. 56), представлен на следующем рисунке:

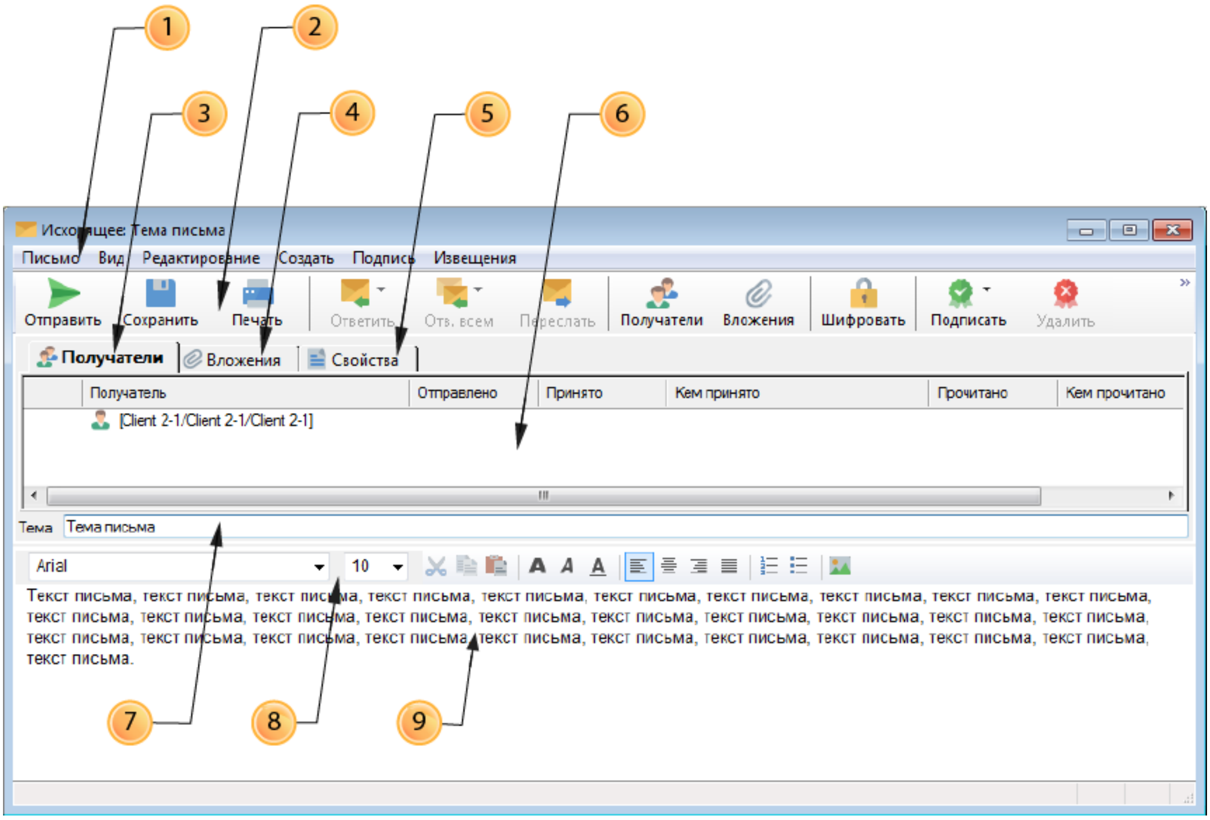


Рисунок 10. Интерфейс окна создания и просмотра писем

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 форматирования текста письма. С помощью этой панели при создании письма вы можете изменять тип, размер, начертание шрифта, вставлять в текст изображение, маркированный или нумерованный список и так далее. Назначение основных кнопок панели форматирования описано в таблице ниже.

Таблица 4. Кнопки панели форматирования

Кнопка	Действие	Сочетание клавиш
	Вырезать	**Ctrl+X**
	Копировать	**Ctrl+C**
	Вставить	**Ctrl+V**
	Выделить полужирным начертанием	**Ctrl+B**
	Выделить курсивным начертанием	**Ctrl+I**
	Подчеркнуть	**Ctrl+U**
	Выровнять по левому краю (по умолчанию)	**Ctrl+L**
	Выровнять по центру	**Ctrl+E**
	Выровнять по правому краю	**Ctrl+R**
	Выровнять по ширине окна	**Ctrl+J**
	Создать нумерованный список	—
	Создать маркированный список	—
	Вставить изображение	—

Примечание. По умолчанию панель форматирования не отображается, и письмо создается без форматирования. Если вы хотите форматировать текст письма, включите возможность форматирования в настройках общих параметров программы (см. Настройка общих параметров на стр. 139).

9 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. 46).

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

3 На нижней панели окна введите текст письма.

4 При необходимости настройте формат текста письма с помощью панели форматирования. Если панель форматирования не отображается в окне создания письма, включите возможность форматирования в настройках общих параметров программы (см. Настройка общих параметров на стр. 139).

Примечание. Если вы отправите письмо с применением форматирования получателю, использующему программу ViPNet Деловая почта ранней версии, в которой не поддерживается форматирование текста, он получит текст вашего письма в файле вложения в формате RTF (расширенный текстовый документ) и сможет прочесть его с помощью текстового редактора, например, Microsoft Office Word или Microsoft WordPad.

---

5 Если в письмо требуется добавить вложения:

- Выполните одно из действий:
  - Перетащите файлы или другие письма 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.

Примечание. Общий размер письма с вложениями не должен превышать 2 Гбайт, если администратором сети не установлено меньшее ограничение.

Чтобы удалить вложения из письма:

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

6 Если необходимо зашифровать письмо, на панели инструментов нажмите кнопку **Шифровать** . Если необходимо подписать письмо электронной подписью (см. Электронная подпись и шифрование на стр. 70), нажмите кнопку **Подписать** и выберите сертификат для подписи.

7 Чтобы указать получателей письма:

- На панели инструментов нажмите кнопку **Получатели** .

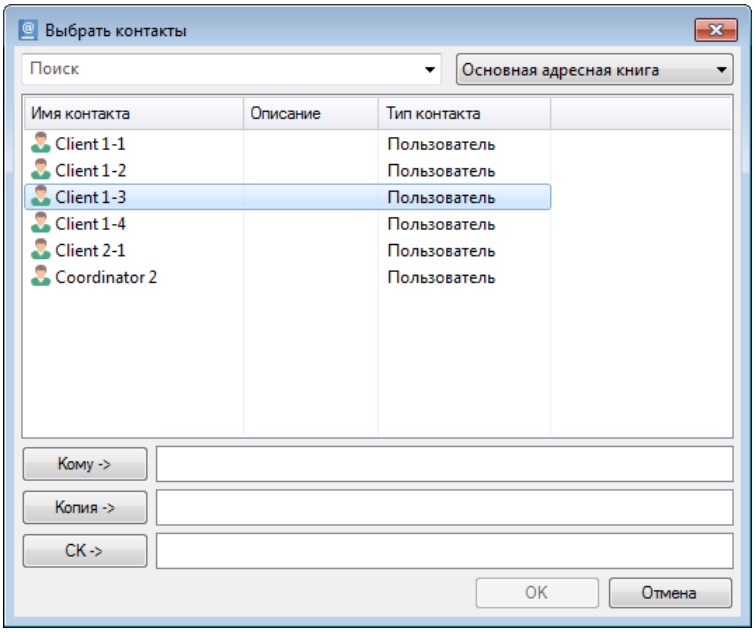


Рисунок 11. Выбор получателей

- В окне **Выбрать контакты** в списке в правом верхнем углу выберите нужную адресную книгу.

Совет. Назначьте книгой по умолчанию часто используемую адресную книгу, чтобы не выбирать ее в списке при каждом создании письма (см. Назначение пользовательской адресной книги книгой по умолчанию на стр. 44).

- Выберите узел, пользователя или группу рассылки (см. Адресная книга на стр. 38). Чтобы отфильтровать список получателей, в строку поиска в верхней части окна введите часть имени нужного получателя.
- Добавьте необходимое количество получателей в поля **Кому**, **Копия** и **СК** и нажмите кнопку **OK**.
- Чтобы удалить получателя, выберите его на вкладке **Получатели** (см. Окно создания и просмотра писем на стр. 46) и нажмите клавишу **Delete**.

8 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 .

9 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. 32). Также можно запросить извещение о доставке и прочтении письма (см. Запрос извещений о доставке и прочтении в виде отдельного письма на стр. 50).

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. 47).

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 в виде вложения, выполните действия:

1 В окне программы ViPNet Деловая почта (см. Интерфейс программы на стр. 32) на левой панели выберите папку с письмами, которые требуется отправить в виде вложений.

2 На панели писем выберите письмо и выполните одно из действий:

   - Щелкните письмо 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 и окно **Введите описание вложения**.

3 Введите имя файла для вложения и нажмите кнопку **Добавить**.

4 Завершите создание письма и отправьте его, как описано в разделе Создание письма (на стр. 47).

Для добавления нескольких писем в виде вложений, выполните действия:

1 Создайте письмо (см. Создание письма на стр. 47).

2 На панели писем выделите одно или несколько писем и перетащите их в окно создания письма.

   Для каждого вложенного письма откроется окно **Введите описание вложения**.

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

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. 46).
  - Введите текст и тему письма, укажите получателей и задайте другие параметры, как описано в разделе Создание письма (на стр. 47).
  - 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. 47) 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. 32) 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 просмотра 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. 56).

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. 56).

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 **Статус** (см. Интерфейс программы на стр. 32) 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. 145). 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**.

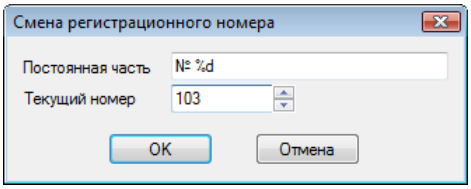


Рисунок 12. Изменение регистрационного номера

- 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).
- 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. 145). 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**.

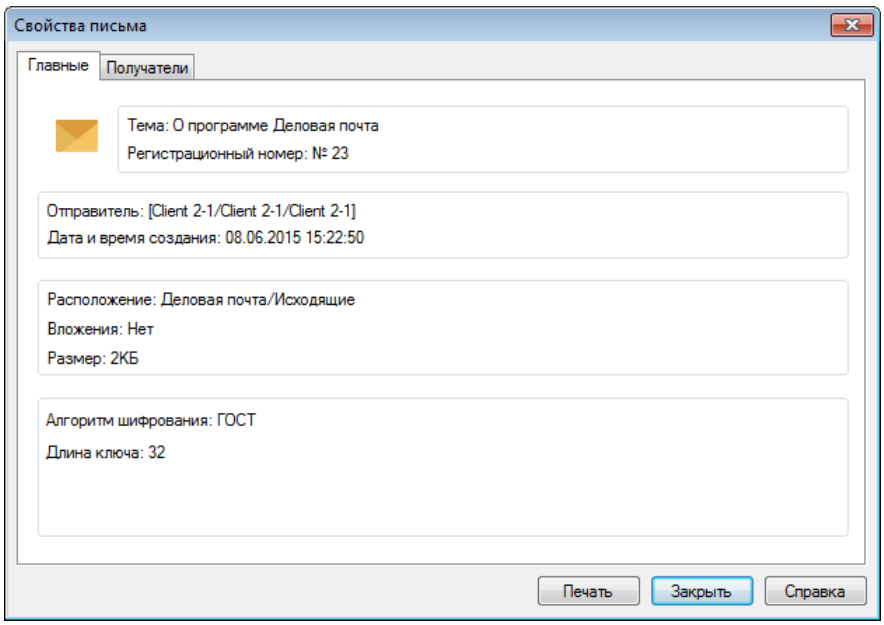


Рисунок 13. Свойства письма

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

Внимание! Текст письма, созданного с применением форматирования и содержащего изображения, распечатывается с сохранением форматирования, но без изображений. О настройке параметров печати см. в разделе Настройка печати (на стр. 147).

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. 46). 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. 47).

Примечание. Чтобы редактировать неотправленное письмо, подписанное электронной подписью, удалите электронную подпись (см. Удаление электронной подписи письма на стр. 77).

---

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** или 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.

Внимание! Текст письма, созданного с применением форматирования и содержащего изображения, распечатывается с сохранением форматирования, но без изображений. О настройке параметров печати см. в разделе Настройка печати (на стр. 147).

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. 32) 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. 46).
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. 47).

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. 32) в меню **Инструменты** выберите пункт **Поиск документа**. Откроется окно **Поиск документа**.

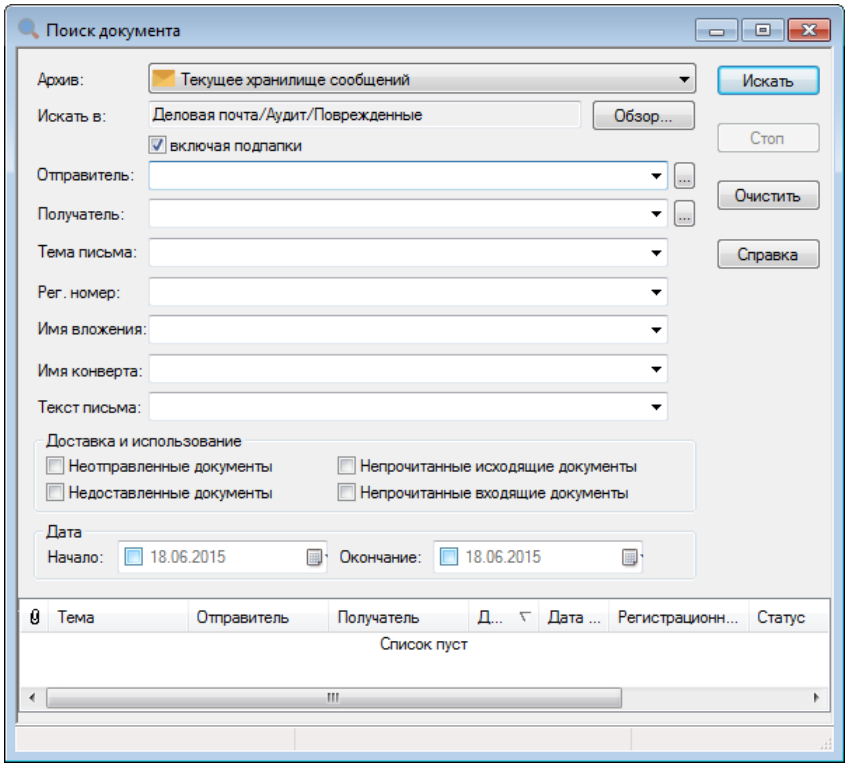


Рисунок 14. Поиск писем

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 окне **Выбрать контакты** выберите нужного отправителя.

6 Чтобы указать получателя писем, которые требуется найти, нажмите кнопку  рядом с полем **Получатель** и в окне **Выбрать контакты** 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. глоссарий, стр. 207) 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**.

Примечание. В зависимости от выбранного хранилища сообщений могут быть доступны не все из перечисленных действий с письмами.

Экспорт и импорт писем

Экспорт писем

Если вам необходимо поделиться информацией или продолжить обсуждение с контактом, не имеющим доступа к защищенной сети ViPNet, вы можете экспортировать письма в формат BML — внутренний формат программы ViPNet Деловая почта. 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. 32) 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 **ОК**.
   - **Сохранить в**. Выбрав данный пункт, в окне **Обзор папок** укажите папку, в которой будут сохранены выбранные письма, и нажмите кнопку **ОК**. 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

Вы можете импортировать письма, сохраненные в формате BML — внутреннем формате программы ViPNet Деловая почта. 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. 32).

     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. 47).

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 **ОК**.

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. 150).

Примечание. При работе в режиме администратора в контекстном меню письма доступен пункт **Полное удаление** (см. Дополнительные настройки и возможности программы на стр. 150).

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.

Внимание! В базе данных ViPNet Деловая почта может храниться не более 500.000 писем, работа с большим количеством писем не гарантируется. Для корректной работы программы включите автоматическую архивацию (см. Параметры автоматической архивации на стр. 142) и задайте параметр **Количество писем больше:** 500.000 **штук**.

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. 141).

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. 141).

2 Перед началом архивации появится окно для подтверждения архивации. Если в параметрах архивации (см. Общие параметры архивации на стр. 141) 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**.

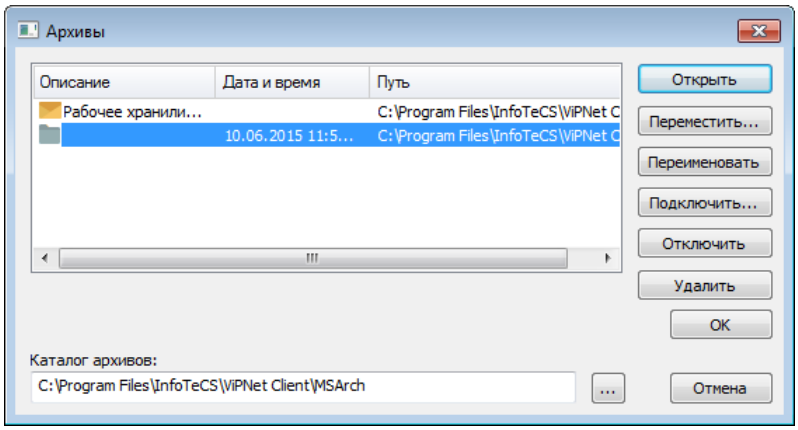


Рисунок 15. Управление архивами

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**.

   Незашифрованные 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 пользователя, 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 71

Работа с электронной подписью писем 72

Работа с электронной подписью файлов 79

Шифрование и расшифрование писем 83

Электронная подпись в программе ViPNet Деловая почта

Примечание. Описанные в данном разделе возможности доступны, если вы располагаете действительным сертификатом электронной подписи. Для получения сертификата обратитесь к администратору вашего удостоверяющего центра.

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. 72) или отдельные файлы (см. Работа с электронной подписью файлов на стр. 79). Также можно проверить и удалить электронную подпись письма или файла.

Для подписания писем и файлов можно использовать следующие типы сертификатов (см. глоссарий, стр. 207):

- Сертификат электронной подписи текущего пользователя клиента.
- Сертификат пользователя другого сетевого узла или сертификат внешнего пользователя сети ViPNet (см. Подписание другим сертификатом на стр. 73), находящийся во внешнем контейнере ключей (см. глоссарий, стр. 206). Контейнер может храниться на диске или на внешнем устройстве (см. Внешние устройства на стр. 190).
- Сертификат электронной подписи, изданный сторонним удостоверяющим центром (см. Использование ключа электронной подписи и ключа проверки электронной подписи, созданных с помощью стороннего криптопровайдера на стр. 75).

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. 145).

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

1. В окне программы ViPNet Деловая почта (см. Интерфейс программы на стр. 32) 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.
     - **Другим 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 **Другим сертификатом**.
3. Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе Подписание другим сертификатом (на стр. 73).

   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. 46), выполните следующие действия:

1. Создайте новое письмо (см. Создание письма на стр. 47) 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.
     - **Другим сертификатом**, чтобы подписать письмо сертификатом из определенного контейнера ключей.

- В меню **Подпись** выберите пункт **Подписать все письмо**, затем выберите **Текущим сертификатом** или **Другим сертификатом**.

3 Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе Подписание другим сертификатом (на стр. 73).

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. 47) 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 **Другим сертификатом**.
- Щелкните текст письма правой кнопкой мыши, в контекстном меню выберите пункт **Подписать текст письма**, затем выберите **Текущим сертификатом** или **Другим сертификатом**.

3 Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе Подписание другим сертификатом (на стр. 73).

Текст письма будет подписан электронной подписью.

Чтобы подписать электронной подписью только вложения письма:

1 Создайте новое письмо (см. Создание письма на стр. 47) 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 **Другим сертификатом**.

5 Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе Подписание другим сертификатом (на стр. 73).

Выбранные вложения будут подписаны электронной подписью.

Подписание другим сертификатом

Если вы хотите подписать письмо или файл сертификатом из определенного контейнера ключей или подпись текущим сертификатом недоступна, при подписании письма (см. Подписание письма на стр. 72) выберите пункт **Другим сертификатом**.

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

1 В окне **Выбор сертификата** в списке выберите нужный сертификат из контейнера, хранящегося на диске, и нажмите кнопку **OK**.

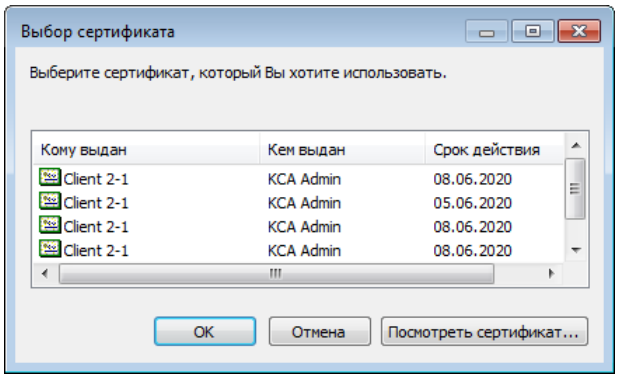


Рисунок 16. Выбор другого сертификата

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

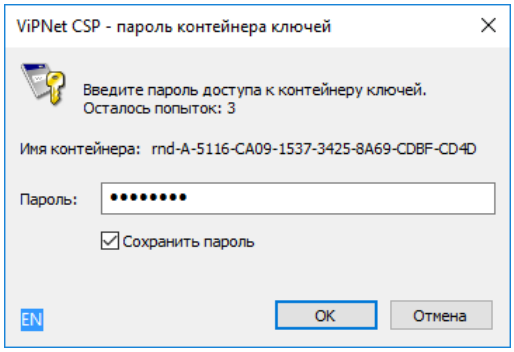


Рисунок 17. Ввод пароля доступа к контейнеру ключей

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

Если контейнер ключей, соответствующий выбранному сертификату, хранится на внешнем устройстве (см. Внешние устройства на стр. 190), выполните следующие действия:

1 В окне **Выбор сертификата** в списке выберите нужный сертификат из контейнера, хранящегося на внешнем устройстве, и нажмите кнопку **OK**.

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

3 Подключите устройство, на котором хранится контейнер. Если подключено несколько устройств, в списке **Выберите устройство** укажите нужное устройство. Имя нужного контейнера автоматически появится в списке **Имя контейнера**.

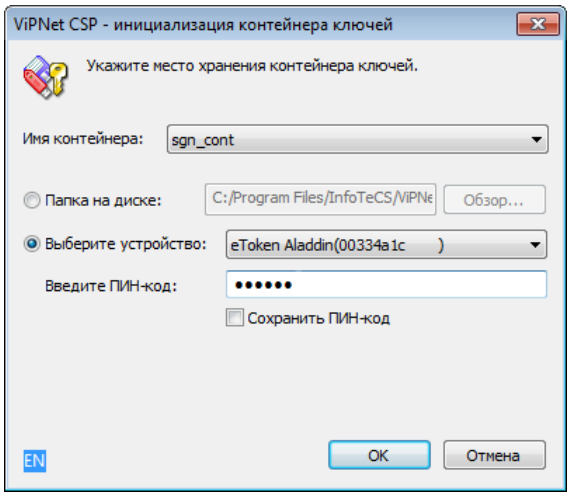


Рисунок 18. Выбор контейнера ключей на внешнем устройстве

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

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

Использование ключа электронной подписи и ключа проверки электронной подписи, созданных с помощью стороннего криптопровайдера

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 В программе ViPNet CSP выберите пункт **Дополнительно** и убедитесь, что снят флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**. Подробнее см. документ «ViPNet CSP. Руководство пользователя».

2 Установите на компьютер криптопровайдер, необходимый для работы с внешним сертификатом.

3 Установите сертификат в системное хранилище **Личное** с помощью оснастки «Сертификаты — текущий пользователь» (certmgr.msc).

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

4 Убедитесь в наличии закрытого ключа, соответствующего установленному сертификату.

Примечание. Процедуры получения и установки сертификата и соответствующего ему закрытого ключа определяются используемым криптопровайдером.

5 В окне **Настройка параметров безопасности** убедитесь, что на вкладке **Администратор** установлен флажок **Разрешить использование сертификатов из хранилища ОС** (см. Дополнительные настройки параметров безопасности на стр. 151).

Примечание. Изменять настройки на вкладке **Администратор** может только администратор сетевого узла (см. Работа в программе с правами администратора на стр. 150).

6 На вкладке **Подпись** выберите нужный сертификат в качестве текущего (см. Смена текущего сертификата на стр. 95).

7 При подписании писем (см. Подписание письма на стр. 72) и файлов (см. Подписание файла на стр. 79) 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. 32) 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. 46):

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.

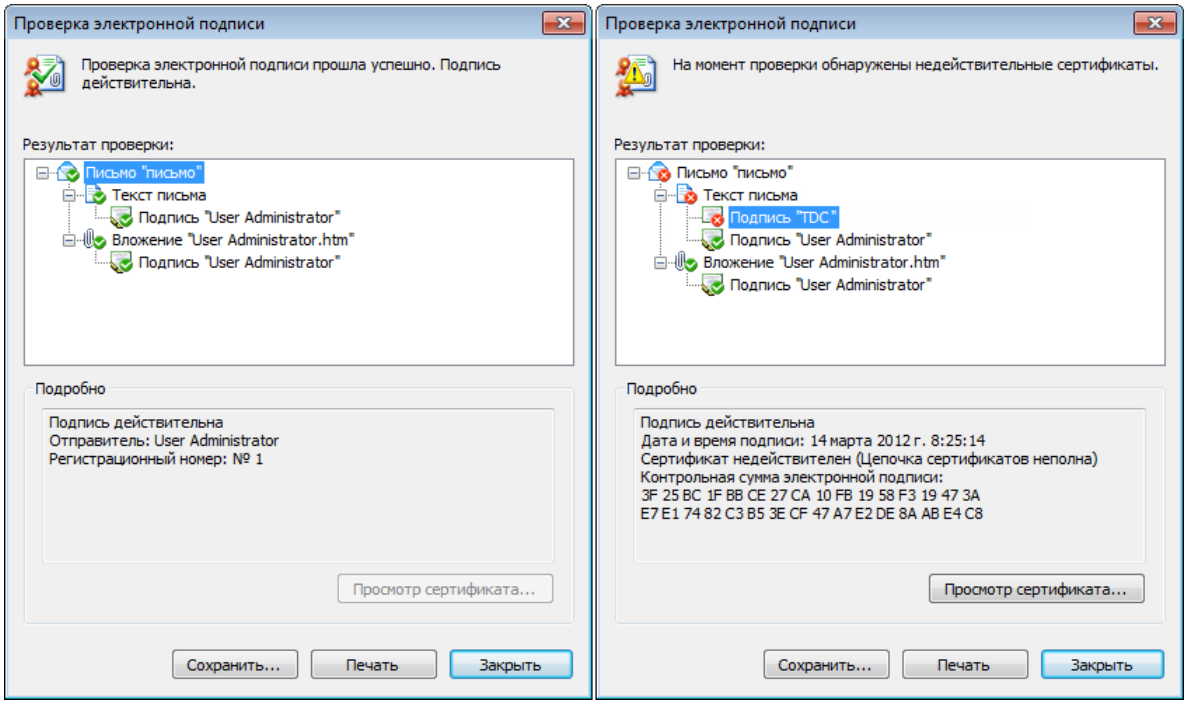


Рисунок 19. Результат проверки электронной подписи

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. 32) 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. 46):

- 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. 80). Чтобы была возможность просматривать подписанные файлы, нужно открепить их электронные подписи (см. Открепление и прикрепление подписи файла на стр. 80). Если файл с прикрепленной или откреплённой 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 другим сертификатом**, чтобы использовать для подписи сертификат электронной подписи из внешнего контейнера ключей.
2. Если выбрана подпись внешним сертификатом, выполните действия, описанные в разделе Подписание другим сертификатом (на стр. 73).
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 17 на стр. 74) введите пароль (окно не появится, если ранее вы сохранили 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 откреплённую электронную подпись (см. Открепление и прикрепление подписи файла на стр. 80), новая подпись будет прикреплена к файлу, а откреплённая подпись не изменится.

Открепление и прикрепление подписи файла

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

Чтобы открепить 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 открепить электронные подписи, и нажмите кнопку **Открыть**.

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

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

Примечание. Если файл имеет одновременно прикрепленную и открепленную электронные подписи, прикрепленная подпись будет сохранена в файл `*.p7s`, заменив существующий файл открепленной подписи.

Чтобы прикрепить открепленную 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 открепленные подписи, и нажмите кнопку **Открыть**. Например, если файл `Document.txt` имеет открепленную электронную подпись `Document.txt.p7s`, для прикрепления подписи нужно указать файл `Document.txt`.

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

Примечание. Если файл имеет одновременно прикрепленную и открепленную электронные подписи, то прикрепление открепленной подписи будет возможно только после удаления прикрепленной 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 прикрепленной или открепленной 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**.

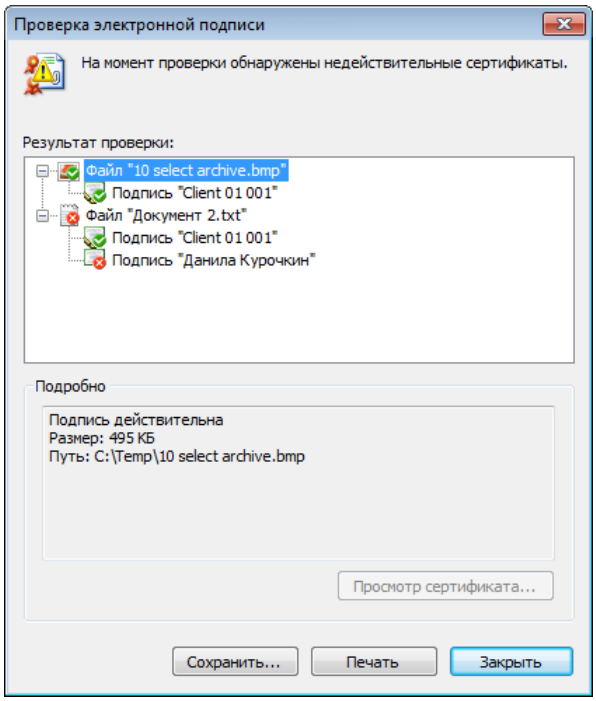


Рисунок 20. Проверка подписей нескольких файлов

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 прикрепленную и открепленную электронные подписи, открепленная 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 прикрепленной или откреплённой 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 прикрепленную и откреплённую электронные подписи, будет удалена только прикрепленная 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. 145).

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

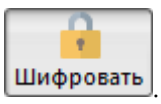
1. В окне программы ViPNet Деловая почта (см. Интерфейс программы на стр. 32) на панели писем выберите одно или несколько писем, которые требуется зашифровать или расшифровать.
2. Чтобы зашифровать выбранные письма, выполните одно из действий:
   - Нажмите кнопку **Шифровать** на панели инструментов.
   - 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. 46), выполните следующие действия:

1. Создайте новое письмо (см. Создание письма на стр. 47) 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

Работа с сертификатами и ключами

Просмотр сертификатов 85

Управление сертификатами 89

Работа с контейнером ключей 110

Просмотр сертификатов

Примечание. Описанные в данном разделе возможности доступны, если вы располагаете действительным сертификатом электронной подписи. Для получения сертификата обратитесь к администратору вашего удостоверяющего центра.

Просмотр сертификата может понадобиться для получения информации о его назначении, издателе, составе полей, причине недействительности сертификата и так далее. Подробная информация о сертификатах содержится в разделе Общие сведения о сертификатах ключей проверки электронной подписи (на стр. 172).

В программе ViPNet Деловая почта можно просматривать следующие типы сертификатов:

- текущий сертификат пользователя (см. Просмотр текущего сертификата пользователя на стр. 86);
- личные сертификаты пользователя (см. Просмотр личных сертификатов пользователя на стр. 86);
- доверенные корневые сертификаты (см. Просмотр доверенных корневых сертификатов на стр. 87);
- изданные сертификаты (см. Просмотр изданных сертификатов на стр. 87).

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

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

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

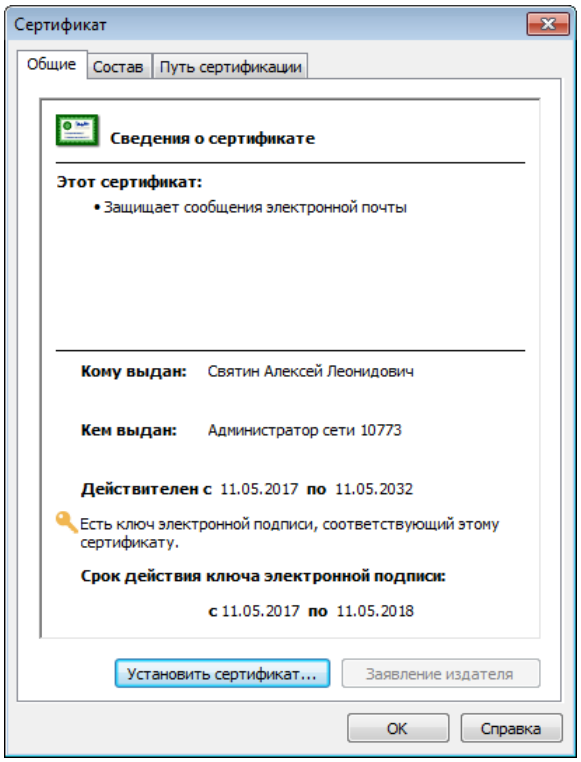


Рисунок 21. Просмотр основной информации о сертификате

Просмотр текущего сертификата пользователя

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

Просмотр личных сертификатов пользователя

Для просмотра личных сертификатов пользователя:

1 В окне **Настройка параметров безопасности** откройте вкладку **Электронная 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 сертификатов из хранилища ОС** (см. Дополнительные настройки параметров безопасности на стр. 151).

---

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 **Электронная 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 сертификатов, которые изданы в программе ViPNet Удостоверяющий и ключевой центр (см. глоссарий, стр. 204) по запросам пользователей или по инициативе администратора УКЦ, но еще не введены в действие, выполните следующие действия:

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

   Откроется окно **Менеджер сертификатов** с информацией об изданных сертификатах.

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. глоссарий, стр. 208) 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 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 ключа электронной подписи 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. 90) Установка в хранилище вручную (на стр. 92)
Смена текущего сертификата. Можно выбрать другой сертификат (из числа действительных личных сертификатов пользователя) в качестве текущего.	Смена текущего сертификата (на стр. 95)
Обновление ключа электронной подписи и сертификата. Можно настроить параметры автоматического оповещения об истечении срока действия текущего сертификата и соответствующего ему ключа электронной подписи, а также, при необходимости, сформировать запрос на обновление этого сертификата и ключа электронной подписи.	Настройка оповещения об истечении срока действия ключа электронной подписи и сертификата (на стр. 97) Процедура обновления ключа электронной подписи и сертификата (на стр. 98)
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 в действие автоматически (на стр. 104) Ввод в действие вручную (на стр. 105)
Просмотр и удаление запросов на сертификаты. Можно просмотреть состояние запросов на сертификаты, сформированных текущим пользователем, а также удалить ненужные запросы.	Просмотр запроса на сертификат (на стр. 105) Удаление запроса на сертификат (на стр. 106)
Экспорт сертификата. В зависимости от целей использования сертификата за пределами ПО ViPNet, сертификат может быть экспортирован в файлы различных форматов.	Экспорт сертификата (на стр. 107)

Установка сертификатов в хранилище операционной системы

Установка сертификатов в хранилище операционной системы позволяет использовать сертификаты во внешних приложениях (таких как Windows Live Mail, Microsoft Outlook, Microsoft Word и других).

Внимание! Для работы с защищенными документами, помимо сертификата пользователя, необходимо также установить в хранилище корневой сертификат (издателя) и список аннулированных сертификатов (см. глоссарий, стр. 207).

Установку можно выполнить автоматически или вручную.

Внимание! При необходимости установки сертификатов 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 условий:

- сертификаты (текущий сертификат пользователя, корневой сертификат и списки аннулированных сертификатов) еще не были установлены 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 и списков аннулированных сертификатов в хранилище текущего пользователя.

Если необходимо обеспечить автоматическое обновление списков аннулированных сертификатов в хранилище локального компьютера, выполните следующие действия:

- Предварительно вручную установите в это хранилище соответствующие корневой сертификат и список аннулированных сертификатов (см. Установка в хранилище вручную на стр. 92).
- Убедитесь, что установлен компонент программы ViPNet CSP «Поддержка работы ViPNet CSP через MS Crypto API». Подробнее см. документ «ViPNet CSP. Руководство пользователя» раздел «Добавление, удаление и восстановление компонентов программы».
- Для запуска программы ViPNet Монитор используйте учетную запись, обладающую правами администратора.

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

Для установки корневого сертификата необходимо подтверждение этого действия пользователем в окне **Установка корневого сертификата**. Данное окно 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 совместно с обновлением текущего сертификата пользователя получен новый корневой сертификат.

Для подтверждения автоматической установки корневого сертификата выполните следующие действия:

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

   - 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.

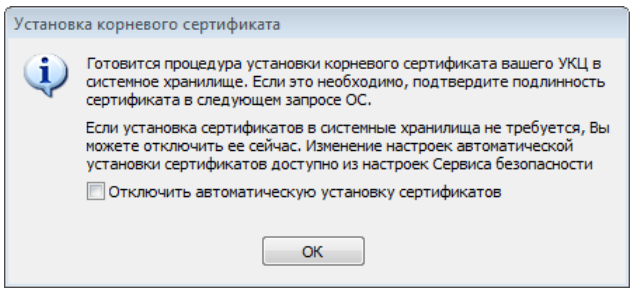


Рисунок 22. Установка корневого сертификата

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

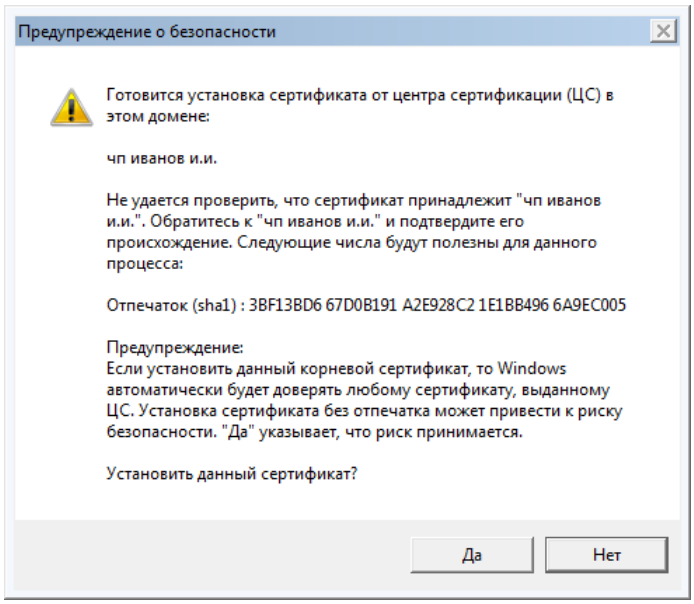


Рисунок 23. Подтверждение подлинности корневого сертификата

Следует иметь в виду, что пауза перед автоматической установкой корневого сертификата может занимать продолжительное время в зависимости от используемой программы ViPNet:

- В программе ViPNet Монитор опрос параметров выполняется через 5 минут после запуска и далее с 2-часовым интервалом. При открытом окне **Настройка параметров безопасности** интервал опроса сокращается до 10–15 минут.
- В программе ViPNet Деловая почта опрос параметров выполняется через 5 минут после запуска программы, а затем с интервалом 60 минут.

Корневой сертификат установлен в хранилище сертификатов текущего пользователя.

Установка в хранилище вручную

Если изданный сертификат пользователя не был установлен в хранилище автоматически (см. Установка в хранилище автоматически на стр. 90), вы можете установить его в хранилище и сопоставить с ключом электронной подписи вручную. Также совместно с сертификатом пользователя вы можете установить в хранилище операционной системы сертификат издателя и список аннулированных сертификатов (CRL) (см. глоссарий, стр. 207).

Для установки сертификата пользователя, а также сертификата издателя и CRL в хранилище операционной системы выполните следующие действия:

1. Вызовите окно **Сертификат** для того сертификата, который необходимо установить в хранилище (см. Просмотр сертификатов на стр. 85).
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 на сетевой узел кроме сертификата пользователя также поступили сертификаты издателей и CRL, для их установки установите соответствующие флажки.

Нажмите кнопку **Далее**.

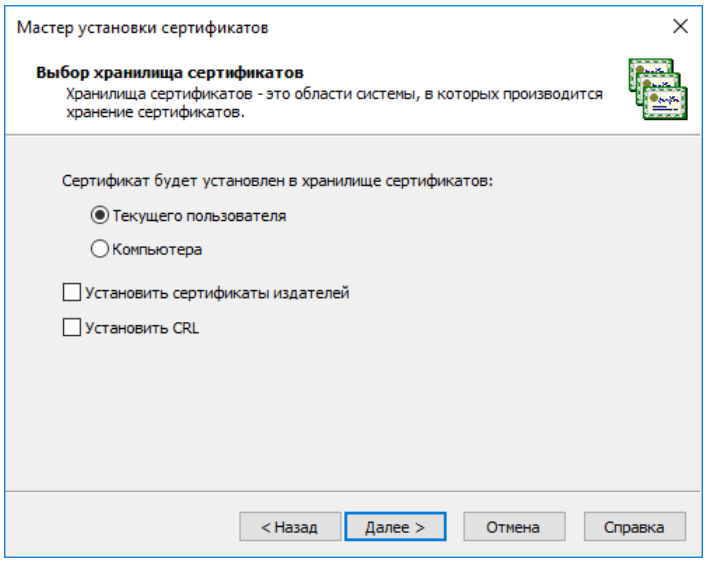


Рисунок 24. Выбор хранилища сертификатов

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, и сертификаты для аутентификации в программе ViPNet.

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, запустите программу ViPNet от имени 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.

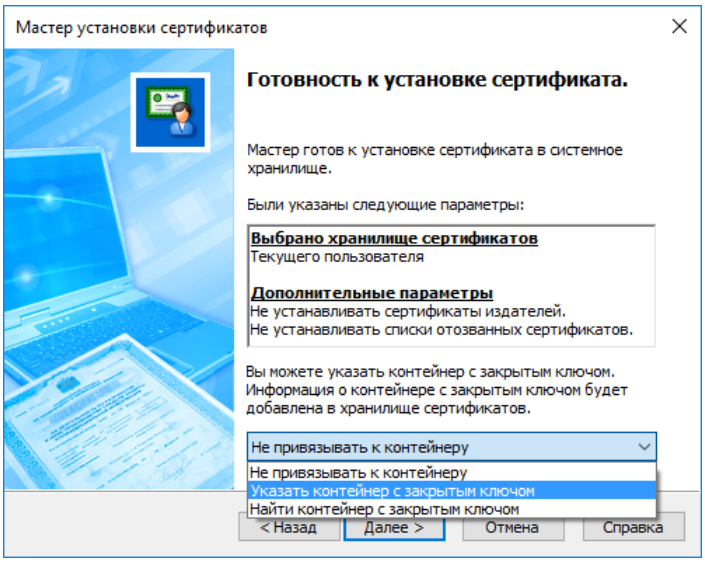


Рисунок 25. Сертификат готов к установке

- Для сопоставления сертификата пользователя с ключом электронной подписи установите флажок **Указать контейнер с ключом электронной подписи**.
- Нажмите кнопку **Далее**.

6 Если флажок **Указать контейнер с ключом электронной подписи** 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 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. 190).

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.

8 Если появилось окно **ViPNet CSP – пароль контейнера ключей**, то в поле **Пароль** введите пароль доступа к контейнеру, после чего нажмите кнопку **OK**.

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

Примечание. Окно **ViPNet CSP – пароль контейнера ключей** отображается в следующих случаях:

- контейнер, в котором находится сертификат, сформирован с помощью программы ViPNet CSP или ViPNet Registration Point;
- если ранее при сохранении пароля не был установлен флажок **Сохранить пароль**.

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

Сертификат установлен в выбранное хранилище сертификатов. Если в процессе установки сертификата ему не был сопоставлен ключ электронной подписи, вы можете вручную установить сертификат в контейнер ключей (см. Установка сертификата в контейнер ключей на стр. 116).

Смена текущего сертификата

Если у вас есть несколько действительных личных сертификатов, вы можете использовать любой из них в качестве текущего. Текущий сертификат используется программой ViPNet Деловая почта по умолчанию при подписании письма или зашифровании файла.

Внимание! Если при обновлении сертификата новый сертификат, изданный по запросу пользователя, передан на сетевой узел в составе ключей, для его использования необходимо назначить этот сертификат текущим. Чтобы делать это автоматически, в окне **Настройка параметров безопасности** на вкладке **Электронная подпись** установите флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**. При этом новый сертификат станет текущим только в том случае, если старый сертификат недействителен.

Для выбора действительного личного сертификата в качестве текущего:

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

Если у вас есть хотя бы один действительный личный сертификат, появится окно **Назначение сертификата текущим** 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 сертификатов из хранилища ОС** (см. Дополнительные настройки параметров безопасности на стр. 151).

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

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

Примечание. В качестве текущего допускается использовать 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. 104), а затем назначить текущим.

При успешном выполнении описанных действий выбранный сертификат назначается текущим. При этом на вкладке **Ключи** (см. Рисунок 35 на стр. 111) в группе **Электронная подпись** меняется информация о контейнере ключей, с которым сопоставлен выбранный сертификат.

Обновление ключа электронной подписи и сертификата

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

Обновление требуется в следующих случаях:

- Истек срок действия сертификата. Срок действия сертификата может составлять до 5 лет.
- Истек срок действия ключа электронной подписи. Срок действия ключа электронной подписи 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 ключа проверки электронной подписи и ключ электронной подписи не реже, чем 1 раз в год.

Обновить сертификат и ключ электронной подписи 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»).

Таблица 5. Последовательность действий при обновлении ключа электронной подписи и сертификата

Действие	Ссылка

	Действие	Ссылка
☐	Проверьте настройки обновления сертификатов. При необходимости настройте автоматическую установку сертификатов в хранилище и их автоматический ввод в действие	Установка в хранилище автоматически (на стр. 90) Ввод в действие автоматически (на стр. 104)
☐	Создайте запрос на сертификат	Процедура обновления ключа электронной подписи и сертификата (на стр. 98)
☐	Дождитесь, пока сертификат будет издан в УКЦ и передан на ваш узел	
☐	Установите сертификат в контейнер ключей и в системное хранилище, если не было настроено автоматическое выполнение этих действий	Установка в хранилище вручную (на стр. 92)
☐	При необходимости сделайте полученный сертификат текущим	Смена текущего сертификата (на стр. 95)
☐	Введите сертификат в действие, если не было настроено автоматическое выполнение этого действия	Ввод в действие вручную (на стр. 105)

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

Примечание. Если истек срок действия ключа электронной подписи, но при этом сертификат ключа проверки электронной подписи остается действительным, можно создать запрос на обновление сертификата. Запрос будет подписан ключом электронной подписи, но электронная 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 срок действия и ключа электронной подписи 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 ключа электронной подписи создать запрос на сертификат также невозможно.

Настройка оповещения об истечении срока действия ключа электронной подписи и сертификата

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

Чтобы изменить настройки оповещения, выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**.

В поле **Информация о текущем сертификате** указан срок действия сертификата и ключа электронной подписи.

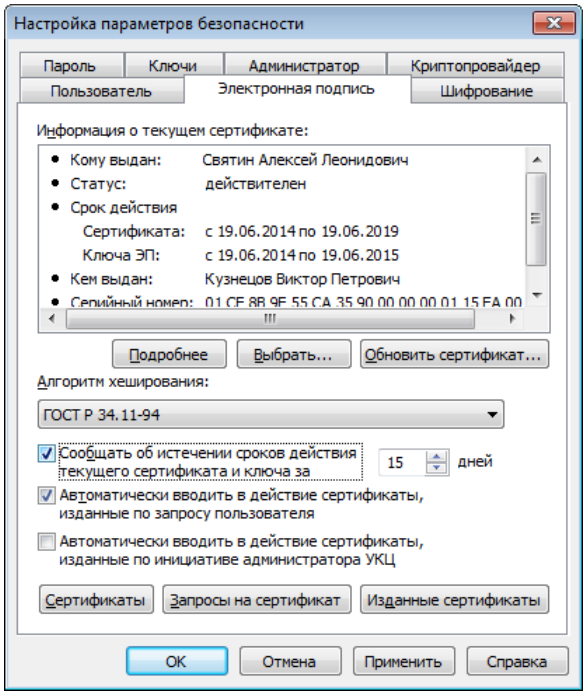


Рисунок 26. Просмотр информации о текущем сертификате и настройка параметров оповещения об истечении сроков действия ключа электронной подписи и сертификата

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 ключа электронной подписи и сертификата

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

- Если включено оповещение об истечении срока действия сертификата и ключа электронной подписи:
  - Когда до истечения срока остается заданное количество дней, программа ViPNet Деловая почта выдаст соответствующее сообщение.

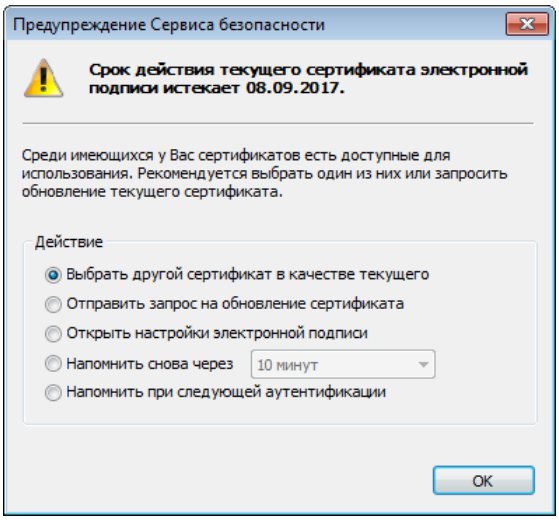


Рисунок 27. Предупреждения о скором истечении срока действия сертификата и ключа электронной подписи

- 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 электронной подписи, отложить отправку запроса на обновление сертификата или выбрать другой сертификат при его наличии.

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

- Если оповещение об истечении срока действия сертификата и ключа электронной подписи отключено:
  - В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**.
  - На вкладке **Электронная подпись** (см. Рисунок 26 на стр. 98) нажмите кнопку **Обновить сертификат**. Будет запущен **Мастер обновления сертификата**.

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

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

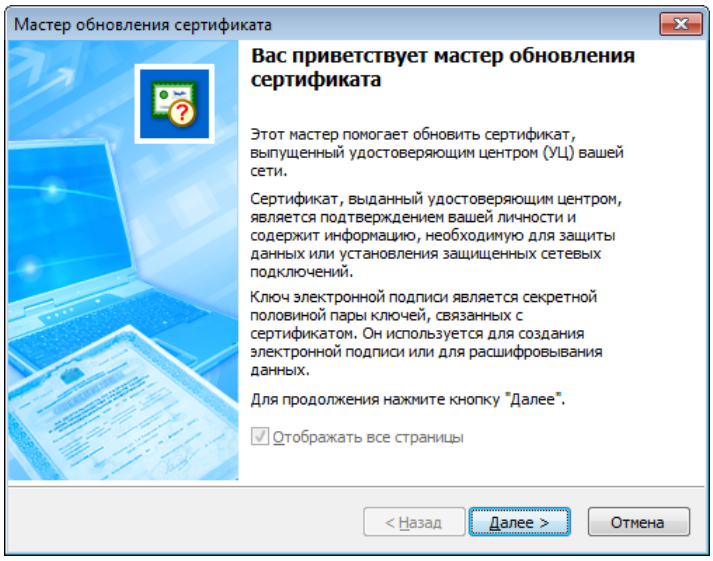


Рисунок 28. Стартовая страница мастера обновления сертификата

2 На странице **Ключ электронной подписи** выполните следующие действия:

2.1 Укажите назначение ключа и сертификата:

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

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

Таблица 6. Характеристики алгоритмов

Алгоритм и его описание	Параметры алгоритма	Длина ключа проверки электронной подписи
ГОСТ Р 34.10-2001 См. RFC 4357 (http://www.ietf.org/rfc/rfc4357.txt) Стандарт электронной подписи, основанный на арифметике эллиптических кривых OID «1.2.643.2.2.19»	**Для подписи:** ГОСТ Р 34.10 - 2001 Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 Параметры подписи B OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001 Параметры подписи C 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»	512

Алгоритм и его описание	Параметры алгоритма	Длина ключа проверки электронной подписи
	ГОСТ Р 34.10 - 2001. EDH Параметры обмена B OID «1.2.643.2.2. 36.1»	
ГОСТ Р 34.10-2012/512 Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 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 Параметры подписи B OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001 Параметры подписи C OID «1.2.643.2.2. 35.3»	512
ГОСТ Р 34.10-2012/1024 Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 512 бит OID «1.2.643.7.1.1.1.2»	ГОСТ Р 34.10 - 2012/1024 Набор параметров A ГОСТ Р 34.10 - 2012/1024 Набор параметров B	1024

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

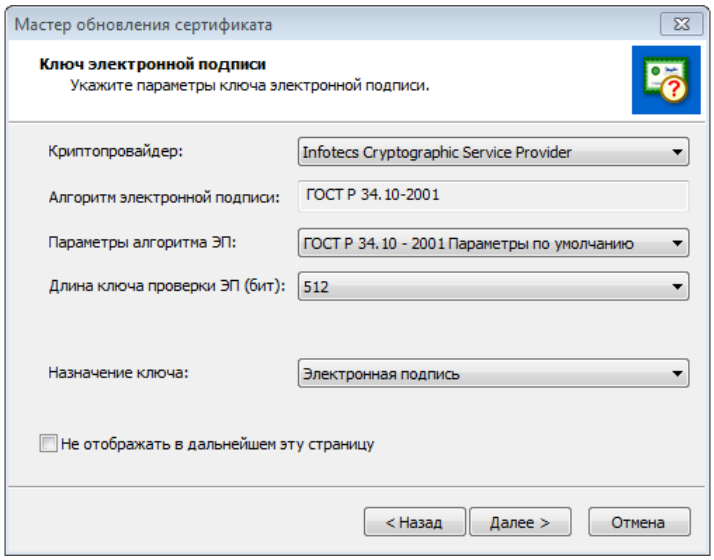


Рисунок 29. Выбор алгоритма и его параметров

2.3 Нажмите кнопку **Далее**.

3 На странице **Контейнер с ключом электронной подписи** укажите место хранения контейнера:

- 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. 190).

После этого нажмите кнопку **Далее**.

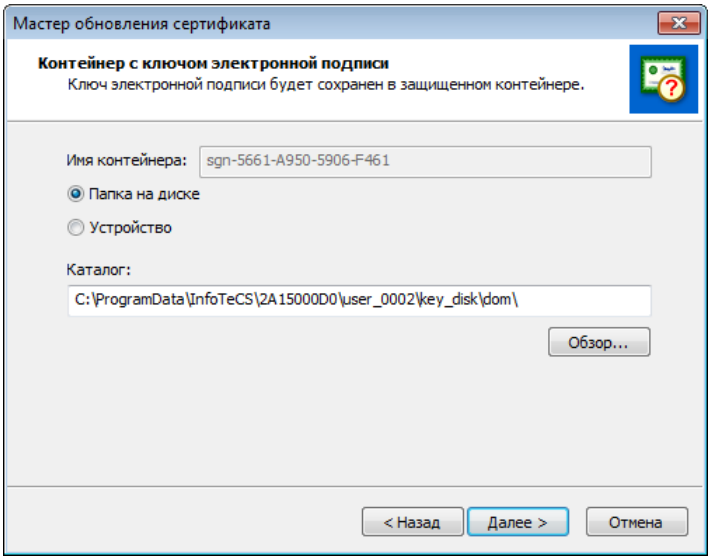


Рисунок 30. Указание места хранения контейнера ключей

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

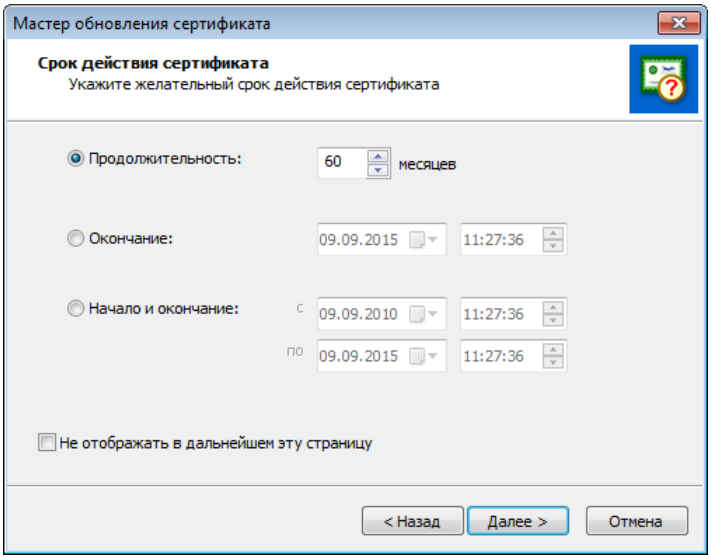


Рисунок 31. Указание желаемого срока действия сертификата

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. Если изданный сертификат был введен в действие и назначен текущим автоматически (см. Ввод в действие автоматически на стр. 104), 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. 105).

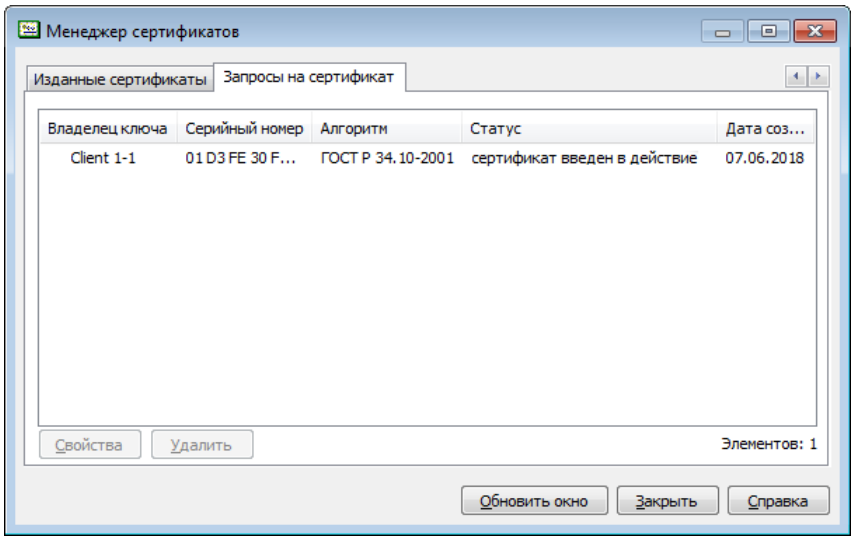


Рисунок 32. Статус запроса в случае ввода сертификата в действие

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. 105).

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. При этом сертификат сопоставляется с закрытым ключом и устанавливается в контейнер.

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 **Электронная 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 ключами электронной подписи. В противном случае они могут быть введены в действие только вручную (см. Ввод в действие вручную на стр. 105).

Внимание! Если контейнер с ключом электронной подписи хранится в папке на диске, то он доступен всегда. Если контейнер хранится на внешнем устройстве, то он будет доступен, если устройство подключено и сохранен ПИН-код к нему или ПИН-код уже вводился в рамках текущей сессии.

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 ключом электронной подписи.

Чтобы вручную ввести в действие полученный сертификат, выполните следующие действия:

1. В окне **Настройка параметров безопасности** откройте вкладку **Электронная 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. 95).

Работа с запросами на сертификаты

Работа с запросами на сертификаты (см. глоссарий, стр. 205) выполняется в окне **Менеджер сертификатов** на вкладке **Запросы на сертификат**.

Для вызова окна **Менеджер сертификатов**:

1. В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**.
2. Нажмите кнопку **Запросы на сертификат**.

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**.

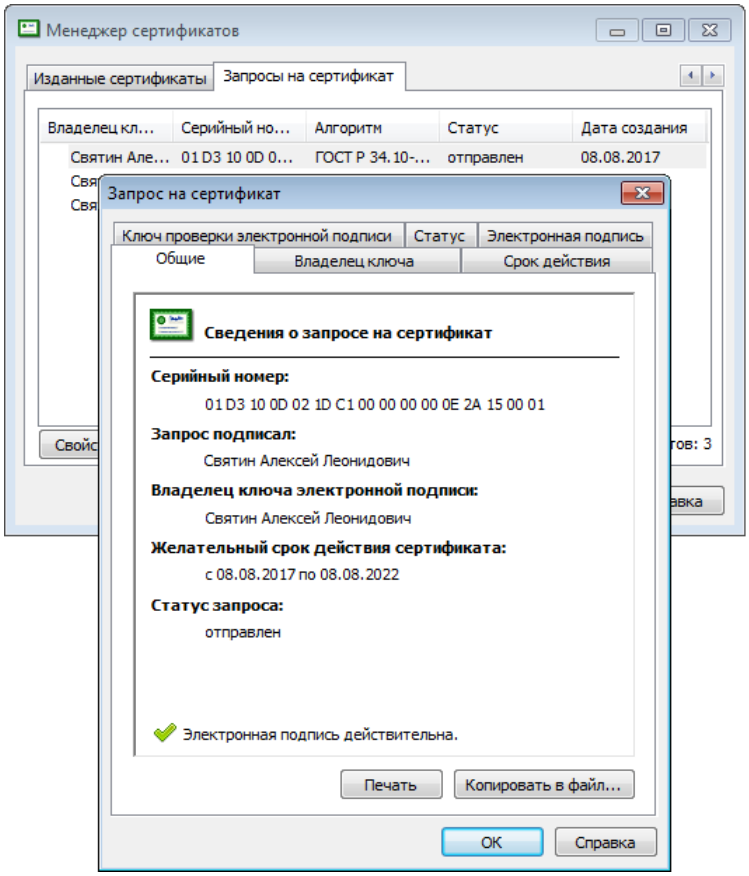


Рисунок 33. Просмотр подробной информации о запросе на сертификат

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 сертификат**, при этом сертификат, изданный по этому запросу, сохранится.

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. 85).

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. 108), после чего нажмите кнопку **Далее**.

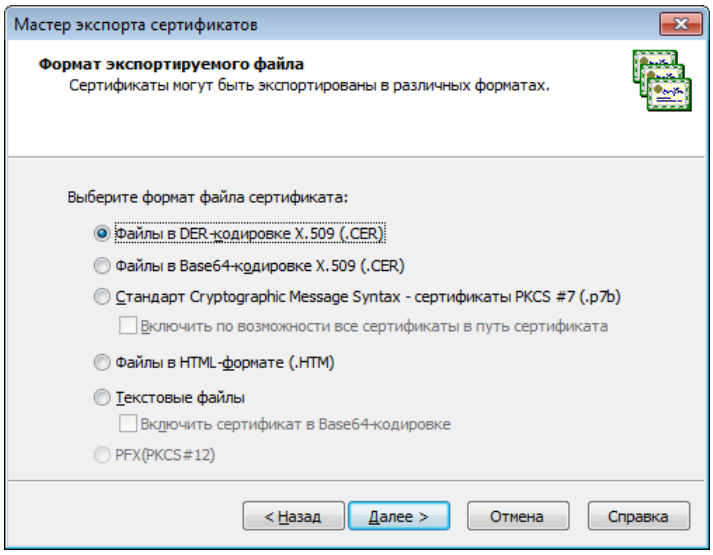


Рисунок 34. Выбор формата файла

5 На странице **Имя файла экспорта** 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 предпочтительный формат экспорта — PKCS #7, поскольку этот формат обеспечивает сохранение цепочки центров сертификации (пути сертификации). 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 веб-сайте RSA Laboratories.

- **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.

- **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, что обеспечивает целостность информации при ее передаче по сети. 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 в кодировке ANSI для просмотра в любом текстовом редакторе и вывода на печать.

- **Файлы в формате PFX (PKCS #12)**

  Формат PFX (PKCS#12) поддерживает безопасное хранение сертификата и закрытого ключа, соответствующего сертификату пользователя, может содержать все сертификаты в цепочке доверия от сертификата пользователя до корневого сертификата удостоверяющего центра и CRL.

Работа с контейнером ключей

Контейнер ключей (см. глоссарий, стр. 206) содержит ключ электронной подписи (см. глоссарий, стр. 205) и соответствующий ему сертификат ключа проверки электронной подписи (см. глоссарий, стр. 207), если он установлен в контейнер.

В программе ViPNet Деловая почта вы можете выполнять следующие операции с контейнером ключей:

- Установка (см. Установка контейнера ключей на стр. 114).

  Установка нового контейнера ключей указанным способом требуется в том случае, если у вас есть новый контейнер ключей, и вы хотите его использовать.

  Вы также можете установить контейнер ключей с помощью программы ViPNet CSP, входящей в состав ViPNet Деловая почта. Но при этом использовать ключ и сертификат из такого контейнера ключей вы сможете только в том случае, если вам разрешено использование внешних сертификатов (см. Дополнительные настройки параметров безопасности на стр. 151). В противном случае, они будут вам недоступны, даже если контейнер ключей будет установлен.

- Смена и удаление сохраненного пароля к контейнеру (см. Смена пароля к контейнеру на стр. 112).

  Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль. Удаление сохраненного пароля может потребоваться, если изменился регламент безопасности вашей организации и хранение пароля на компьютере стало недопустимым.

- Изменение расположения контейнера (см. Перенос контейнера ключей на стр. 116).

  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 электронной 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. 152).

Внимание! В сети ViPNet, управляемой с помощью ПО ViPNet Administrator, выполнять различные операции с контейнером ключей может только пользователь, который обладает правом подписи. Такое право предоставляется пользователям сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр.

Для работы с контейнером ключей:

1 Откройте вкладку **Ключи**.

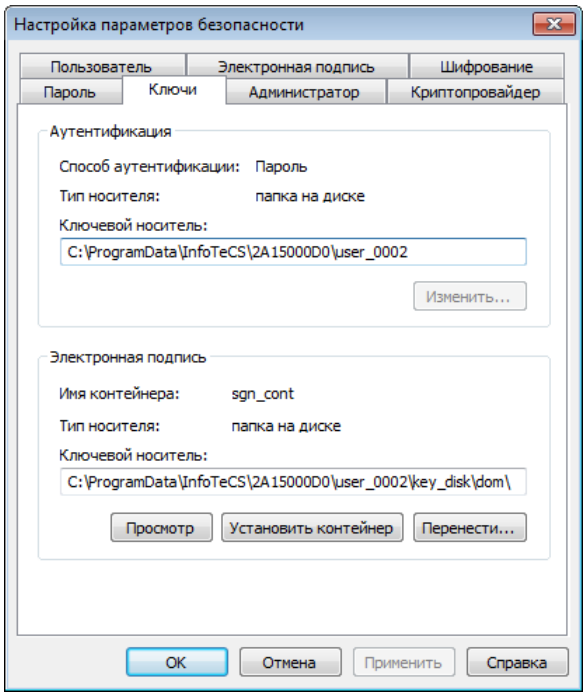


Рисунок 35. Работа с контейнером ключей

2 В группе **Электронная 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. 112);
  - удаления пароля (см. Удаление сохраненного на компьютере пароля к контейнеру ключей на стр. 113);
  - проверки соответствия ключа электронной подписи сертификату (см. Проверка контейнера ключей на стр. 114);
  - удаления ключа электронной подписи.
- **Установить контейнер** — для установки нового контейнера ключей (см. Установка контейнера ключей на стр. 114).
- **Перенести** — для изменения расположения контейнера ключей (см. Перенос контейнера ключей на стр. 116).

Примечание. В группе **Электронная подпись** отображается информация о ключе электронной подписи, соответствующем текущему сертификату.

Смена пароля к контейнеру

Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль. Описанный ниже сценарий смены пароля к контейнеру ключей применяется только для контейнеров, которые были созданы в программе ViPNet Registration Point, либо были перенесены из папки ключей пользователя (по умолчанию `C:\ProgramData\InfoTeCS\<идентификатор узла>\<идентификатор пользователя>\key_disk\dom`) в другую папку. В остальных случаях смена пароля к контейнеру предполагает смену пароля пользователя ViPNet (см. Смена пароля пользователя на стр. 155).

Для смены пароля к контейнеру ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 35 на стр. 111) нажмите кнопку **Просмотр**.
2. В окне **Свойства контейнера ключей** нажмите кнопку **Сменить пароль**.

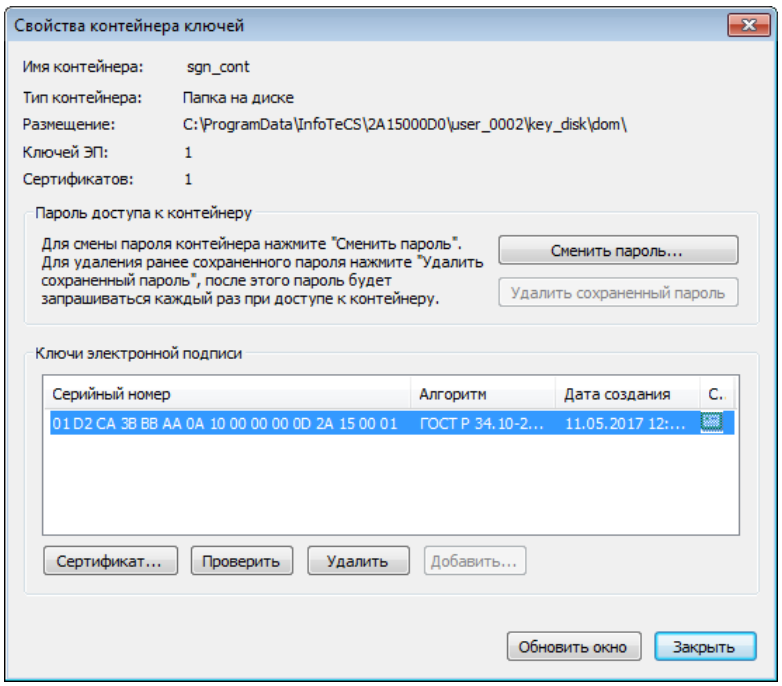


Рисунок 36: Смена пароля к контейнеру ключей

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. 155).
4. 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 - смена пароля контейнера ключей** укажите текущий пароль, задайте и подтвердите новый пароль. Нажмите кнопку **OK**.

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

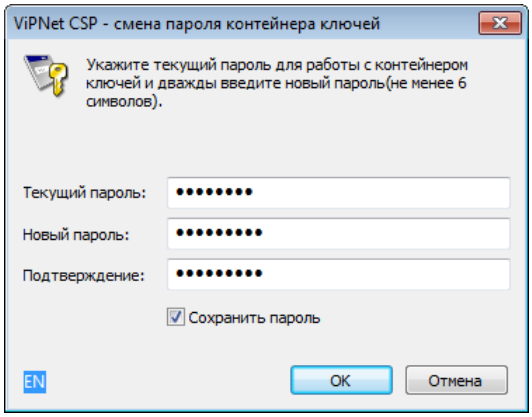


Рисунок 37. Смена пароля доступа к контейнеру ключей

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

Пароль доступа к контейнеру ключей изменен.

Удаление сохраненного на компьютере пароля к контейнеру ключей

Удаление сохраненного пароля к контейнеру ключей может потребоваться, 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 35 на стр. 111) нажмите кнопку **Просмотр**.

2 В окне **Свойства контейнера ключей** 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 ключ электронной подписи соответствуют друг другу и могут быть использованы для работы с защищенными документами.

Чтобы проверить контейнер ключей, выполните следующие действия:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 35 на стр. 111) нажмите кнопку **Просмотр**.

2 В окне **Свойства контейнера ключей** нажмите кнопку **Проверить**.

Программа сформирует фрагмент данных, который будет подписан с помощью ключа электронной подписи. После чего будет выполнена проверка электронной подписи. Таким образом, можно выяснить пригодность ключа электронной подписи и его соответствие сертификату ключа проверки электронной подписи, хранящемуся в контейнере.

Примечание. Проверка возможна только в том случае, если в контейнере ключей есть сертификат, соответствующий ключу электронной подписи. 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 ключа электронной подписи проверка действительности сертификата (срок его действия, отсутствие в списках аннулированных сертификатов и прочее) не выполняется.

Установка контейнера ключей

Если у вас есть контейнер ключей с сертификатом, который вы хотите использовать в программе ViPNet Деловая почта, то вы можете его установить в окне **Настройка параметров безопасности** на вкладке **Ключи**. Данная ситуация может возникнуть в следующих случаях:

- Вы переносите контейнер ключей с другого компьютера.
- Вы сформировали запрос на сертификат (см. Процедура обновления ключа электронной подписи и сертификата на стр. 98) и получили на него сертификат из программы ViPNet Удостоверяющий и ключевой центр не по сети, а в отдельном файле.
- У вас есть контейнер ключей, сформированный с помощью ViPNet CSP. О том, как сформировать контейнер ключей в ViPNet CSP, см. в документе «ViPNet CSP. Руководство пользователя».

Внимание! Нельзя установить контейнер ключей, сформированный в ПО ViPNet версии ниже 3.2.x.

Вы также можете установить контейнер ключей с помощью программы ViPNet CSP, входящей в состав ViPNet Деловая почта. Но при этом использовать ключ и сертификат из такого контейнера ключей вы сможете только в том случае, если вам разрешено использование внешних сертификатов (см. Дополнительные настройки параметров безопасности на стр. 151). В противном случае, они будут недоступны вам, даже если контейнер ключей будет установлен.

Для установки контейнера ключей выполните следующие действия:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 35 на стр. 111) 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.

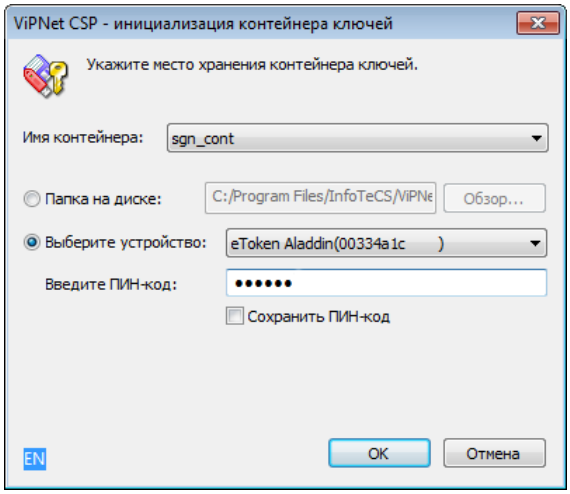


Рисунок 38. Установка контейнера ключей

Нажмите кнопку **OK**.

3. В окне **Назначение сертификата текущим** выберите соответствующий сертификат и нажмите кнопку **OK**.

В результате ключ электронной подписи и сертификат, которые хранятся в выбранном контейнере, будут назначены текущими. Информация о сертификате, который хранится в установленном контейнере, отобразится на вкладке **Электронная 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 рекомендуется переносить контейнер вручную, меняя его расположение на диске. Если это произошло, выполните установку контейнера (см. Установка контейнера ключей на стр. 114).

Не поддерживается перенос контейнера ключей на устройства с аппаратной реализацией криптографических функций.

Для того чтобы поменять расположение контейнера ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 35 на стр. 111) нажмите кнопку **Перенести**.
2. В окне **ViPNet CSP – инициализация контейнера ключей** 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. 190).

   Укажите пароль для доступа к контейнеру ключей, если появилось соответствующее сообщение.

Контейнер ключей будет перенесен по указанному пути.

Установка сертификата в контейнер ключей

Если по каким-то причинам ваш сертификат не находится в контейнере ключей, вы можете установить его в контейнер ключей вручную. Установить сертификат в контейнер можно как в программе ViPNet CSP, так и в окне **Настройка параметров безопасности**. При этом в обоих случаях контейнер ключей должен быть установлен в программу.

Совет. Сохранение сертификата в одном контейнере с ключом электронной подписи удобно, если контейнер планируется переносить и устанавливать на

другом компьютере.

Установка сертификата в контейнер с помощью программы ViPNet CSP описана в документе «ViPNet CSP. Руководство пользователя». Чтобы установить сертификат в контейнер ключей в окне **Настройка параметров безопасности**, выполните следующие действия:

1. Перейдите на вкладку **Ключи** (см. Рисунок 35 на стр. 111).
2. Установите контейнер ключей, если он не установлен (см. Установка контейнера ключей на стр. 114).
3. Перейдите в свойства контейнера с помощью кнопки **Просмотр**.
4. В окне **Свойства контейнера ключей** нажмите кнопку **Добавить**.
5. Укажите файл сертификата, который соответствует ключу электронной подписи, находящемуся в контейнере. Если будет установлено, что указанный сертификат соответствует ключу электронной подписи, он будет добавлен в контейнер. В противном случае, появится соответствующее сообщение.

6

Автопроцессинг

Принцип работы автопроцессинга 119

Настройка правил автопроцессинга 122

Оптимизация работы автопроцессинга 132

Просмотр журнала автопроцессинга 133

Настройка параметров журнала автопроцессинга 136

Принцип работы автопроцессинга

Автопроцессингом называется автоматическая обработка писем и файлов по определенным правилам.

Правила автопроцессинга делятся на следующие категории:

- Правила обработки исходящих файлов.

  Правила предназначены для автоматической отправки файлов с определенной маской имени, находящихся в заданной папке, одному или нескольким пользователям сети ViPNet. Например, вы можете настроить такое правило для отправки из заданной папки файлов, в имени которых содержится слово «отчет», коллеге, проверяющему отчеты.

- Правила обработки входящих писем.

  Правила предназначены для обработки входящих писем, соответствующих заданным параметрам, одним из способов:

  - Перемещение в определенную папку программы ViPNet Деловая почта. Например, вы можете настроить такое правило для переноса в отдельную папку программы писем, полученных от одного или нескольких коллег.
  - Копирование письма и вложений в определенную папку на диске. Например, вы можете настроить такое правило для копирования в отдельную папку писем, в имени которых содержится слово «отчет», от одного или нескольких своих коллег.

  Также возможна отправка квитанции о прочтении письма.

Правила автопроцессинга можно создать в окне **Настройка** в разделе **Автопроцессинг** (см. Настройка правил автопроцессинга на стр. 122).

Схема работы автопроцессинга представлена на следующем рисунке:

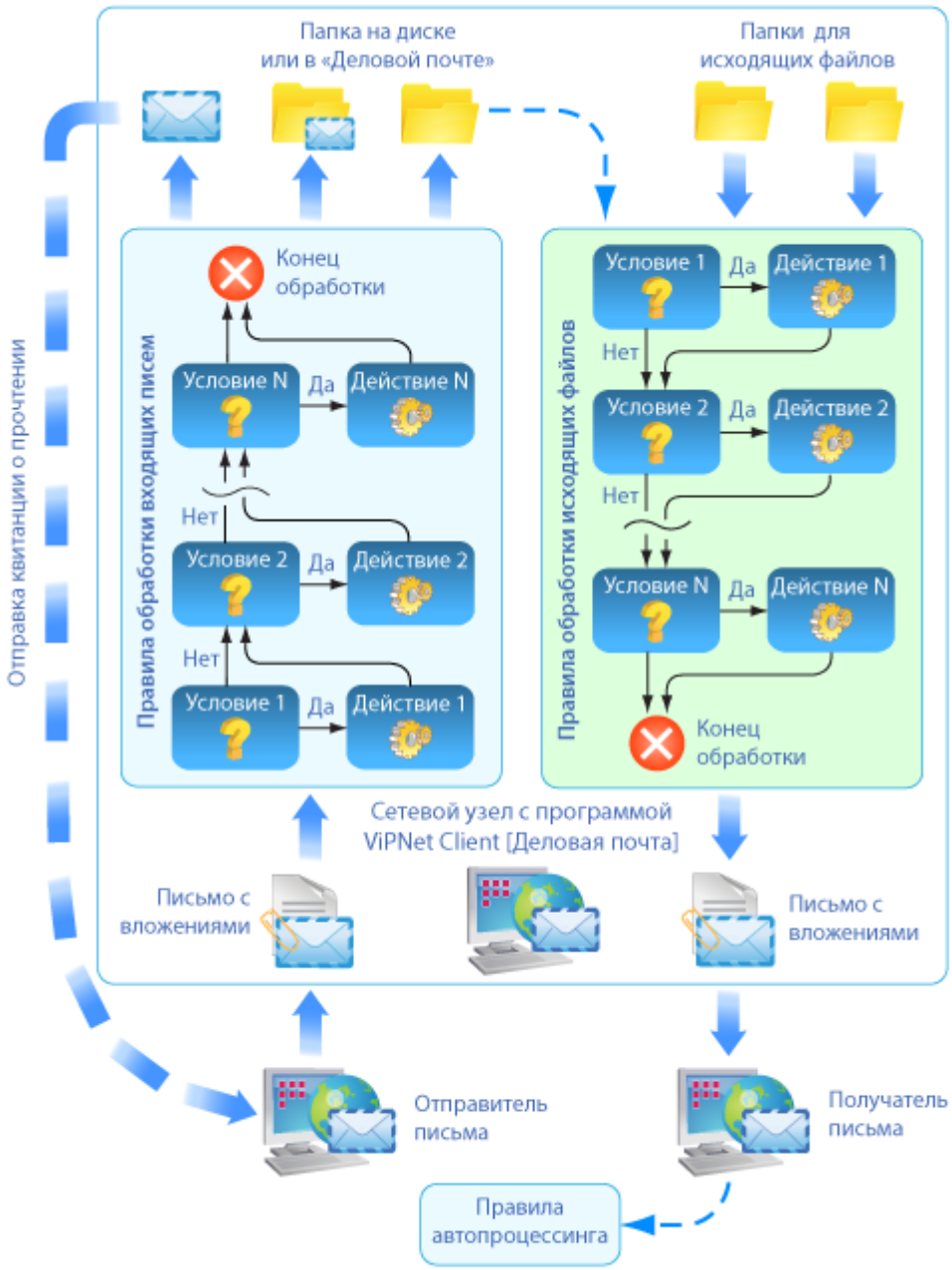


Рисунок 39. Схема работы автопроцессинга

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 периодически проверяются на наличие файлов.
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.

5 Обработанные автопроцессингом файлы автоматически удаляются.

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** или не совершать никаких действий более 20 секунд, правило не отключается, но программа больше не будет пытаться отправить данный файл. При повторной загрузке программа ViPNet Деловая почта в любом случае 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**.

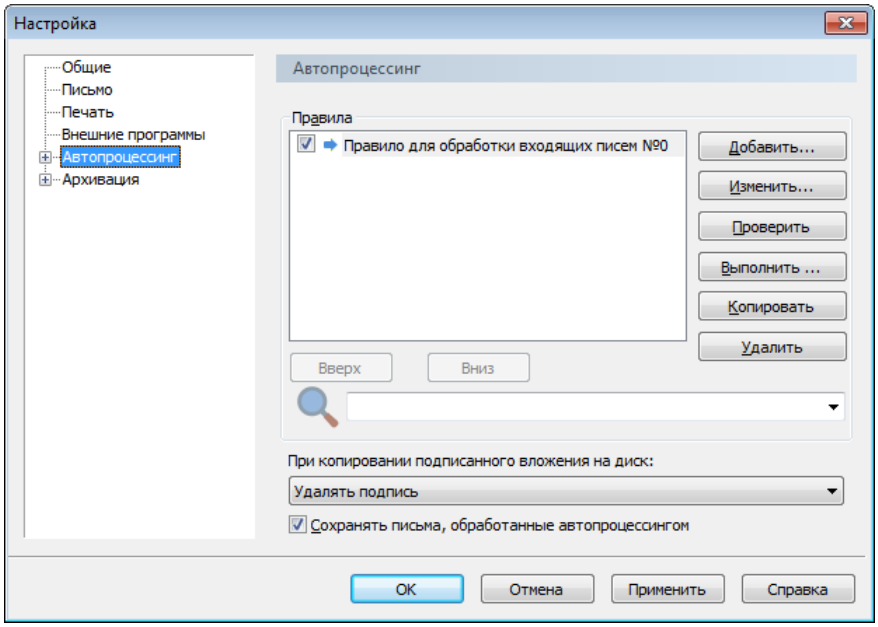


Рисунок 40. Настройка правил автопроцессинга

3 Чтобы настроить правило для обработки файлов, выполните указания одного из следующих разделов:

- Создание правила для исходящих файлов (на стр. 123).
- Создание правила для входящих писем (на стр. 126).

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 следующих разделах:

   - Создание правила для исходящих файлов (на стр. 123).
   - Создание правила для входящих писем (на стр. 126).

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 удаленных письмах по умолчанию сохраняется в папке **Аудит**. Подробнее о настройке сохранения информации в папке **Аудит** см. в разделе Дополнительные настройки и возможности программы (на стр. 150).

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 40 на стр. 122).

3 На панели просмотра **Автопроцессинг** нажмите кнопку **Добавить**.

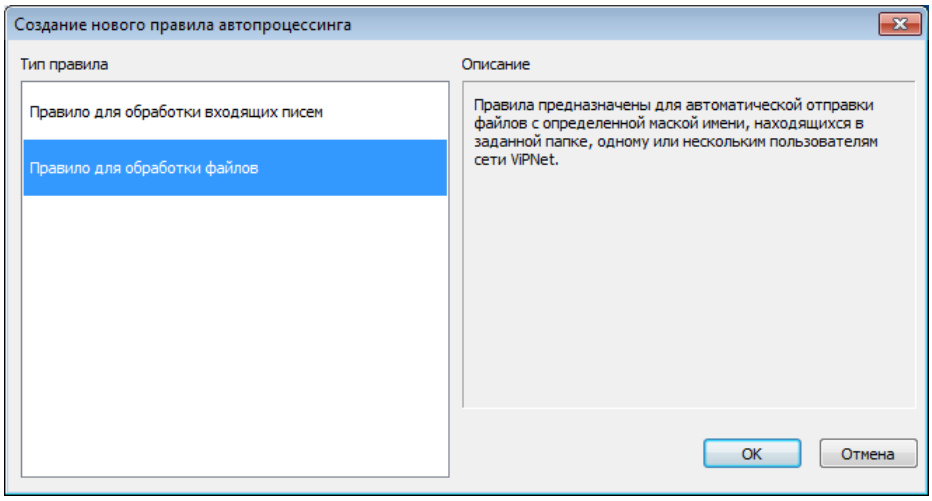


Рисунок 41. Выбор типа правила

4 В окне **Создание нового правила автопроцессинга** выберите тип правила **Правило для обработки файлов** и нажмите кнопку **OK**.

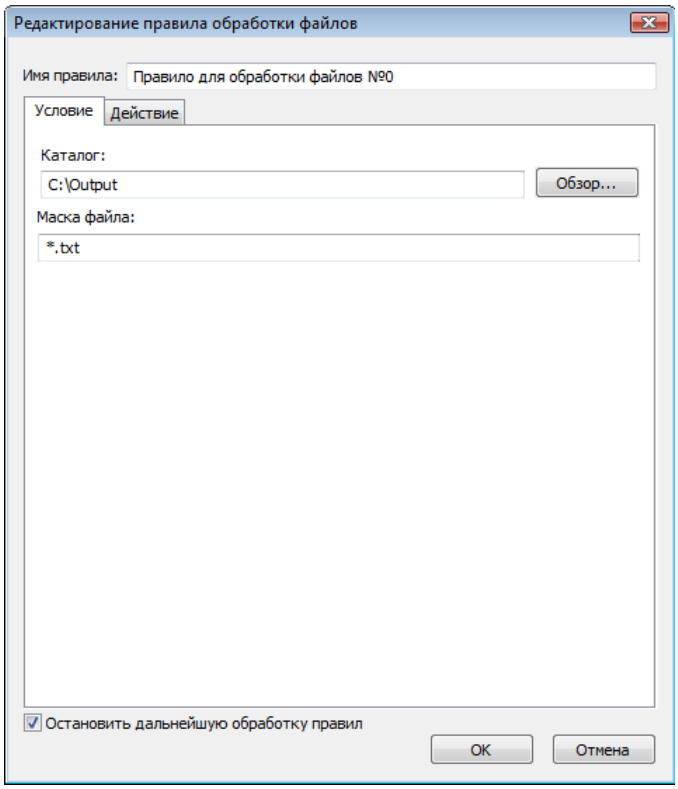


Рисунок 42. Условие для правила обработки исходящих файлов

5 В окне **Редактирование правила обработки файлов** 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 Перейдите на вкладку **Действие**.

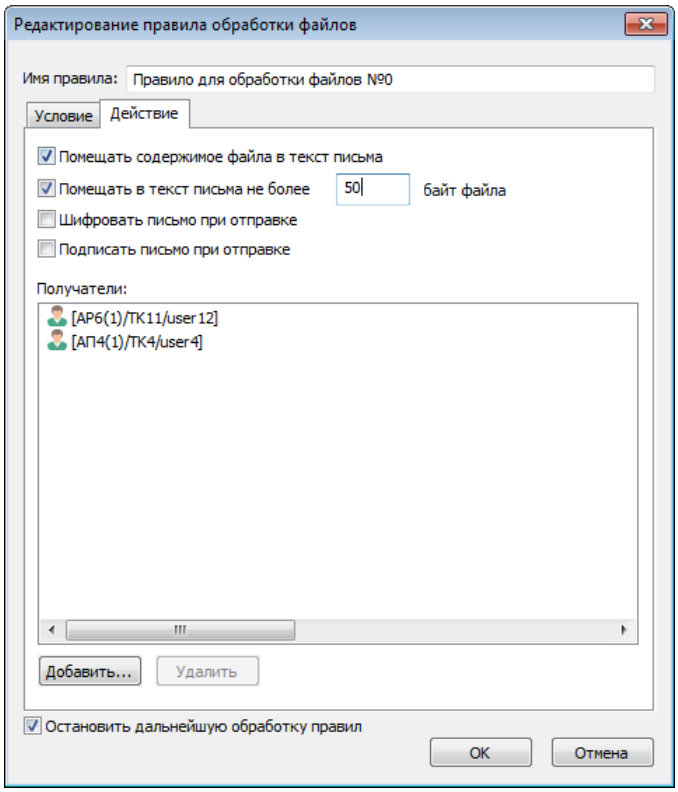


Рисунок 43. Действие правила обработки файлов

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 в формате 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.

Примечание. При отправке писем с помощью правил автопроцессинга вы можете задать тему письма. Для этого:

1. В окне **Редактирование правила обработки файлов** на вкладке **Действие** установите флажок **Помещать содержимое файла в текст письма**.
2. Создайте текстовый файл и в первой строке введите "Subject_Subject:" и тему письма.
3. После темы письма вставьте символ переноса строки и напечатайте содержимое письма.
4. Поместите файл в папку, указанную на вкладке **Условие** окна **Редактирование правила обработки файлов**.

Таким образом, с помощью этого правила будет автоматически рассылаться письмо с указанной темой и содержимым.

10. Чтобы шифровать письмо, установите флажок **Шифровать письмо при отправке**.
11. Чтобы подписывать письмо электронной подписью, установите флажок **Подписать письмо при отправке**.
12. Чтобы добавить получателей, которым будет отправлен файл, нажмите кнопку **Добавить** и выберите из адресной книги одного или несколько пользователей с помощью кнопки **Выбрать**. Затем 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 40 на стр. 122).
3. На панели просмотра **Автопроцессинг** нажмите кнопку **Добавить**.
4. В окне **Создание нового правила автопроцессинга** выберите **Правило для обработки входящих писем** и нажмите **OK**.

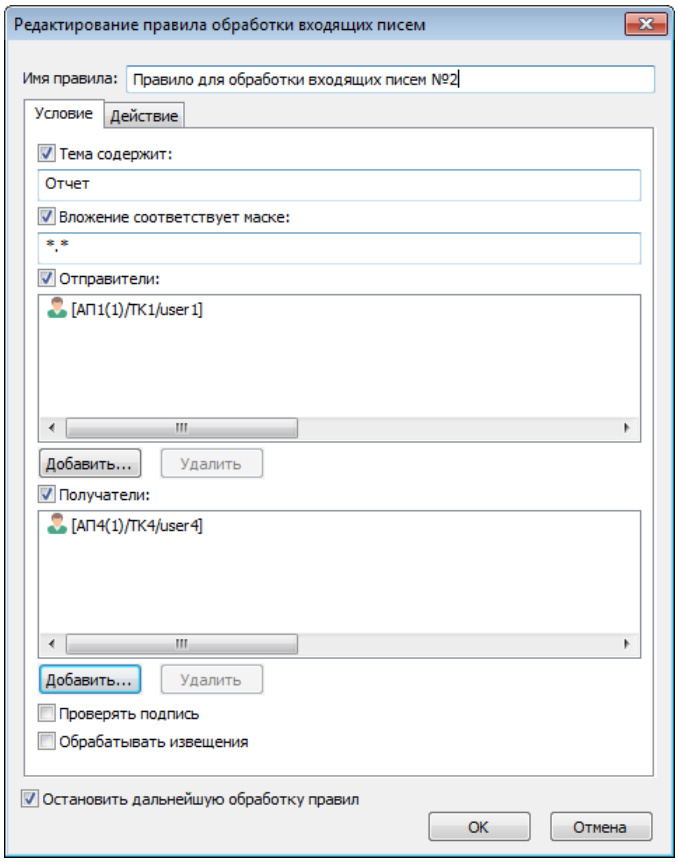


Рисунок 44. Условие правила обработки входящих писем

5 В окне **Редактирование правила обработки входящих писем** в поле **Имя правила** укажите произвольное имя.

6 На вкладке **Условие** укажите, в каких случаях письмо будет обработано данным правилом:

- Для обработки писем, в теме которых содержится определенная последовательность символов, установите флажок **Тема содержит** и в поле под флажком введите эту последовательность.
- Для обработки писем с вложениями, имена которых содержат определенные символы, установите флажок **Вложение соответствует маске** и в поле под этим флажком введите нужные символы. 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 имя файла во вложении соответствовало заданной маске. Файлы того же вложения, не соответствующие маске, обработаны не будут.

Примечание. Чтобы применить правило ко всему вложению, в котором есть хотя бы один файл, соответствующий маске, в папке программы ViPNet Client откройте файл

---

wmail.ini, в секции [AutoprocSettings] найдите параметр ProcessFilesByMaskOnly и замените заданное по умолчанию значение 1 на 0. Если в файле wmail.ini нет параметра ProcessFilesByMaskOnly, создайте его и укажите нужное значение.

- Для обработки писем от определенных отправителей или получателей, установите нужный флажок, нажмите кнопку **Добавить** и выберите из адресной книги одного или несколько пользователей с помощью кнопки **Выбрать**. Затем нажмите кнопку **ОК**.

  Для удаления отправителей или получателей, выберите их в соответствующем списке и нажмите кнопку **Удалить**.

  Если флажки **Отправители** и **Получатели** не установлены, правило будет выполняться для писем любых пользователей.

- Если необходимо обрабатывать письма, подписанные электронной подписью, установите флажок **Проверять подпись**.

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

- Если необходимо применить правила к извещениям (см. Запрос извещений о доставке и прочтении в виде отдельного письма на стр. 50) установите флажок **Обрабатывать извещения**.

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

7 Откройте вкладку **Действие**.

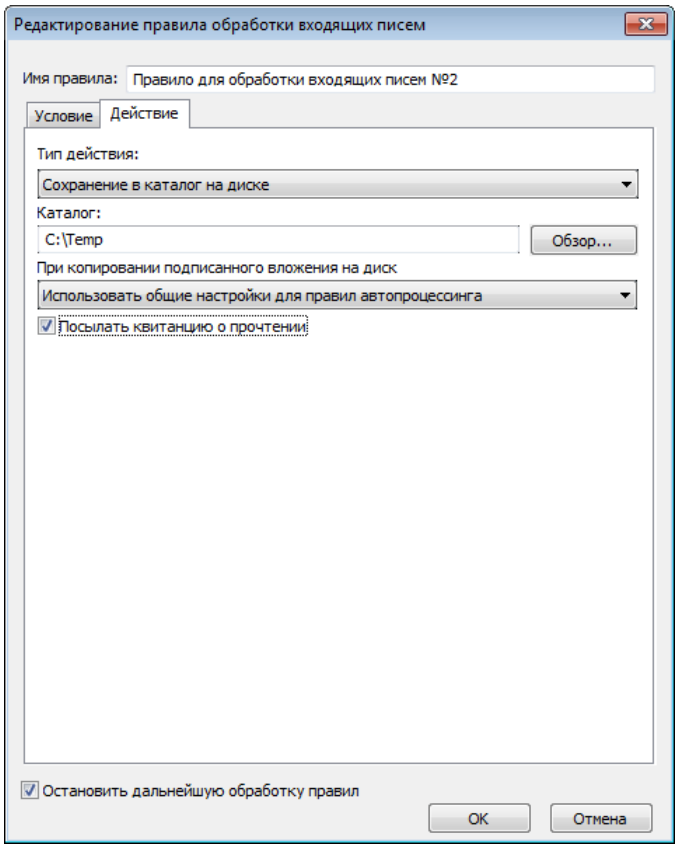


Рисунок 45. Действие правила обработки входящих писем

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

- **Сохранение в каталог на диске**.

> **Внимание!** Если у вас настроено автоматическое сохранение входящих писем в каталог на диске, в случае обработки письма с файлом вложения, имя которого совпадает с именем ранее сохраненного в каталог файла, новый файл вложения не сохранится.

- **Сохранение в каталог с заменой существующих файлов**. При совпадении имен файл, уже находящийся в папке назначения, заменяется файлом вложения из обработанного письма.
- **Сохранение 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.
- **Сохранение 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 сохранении письма на диск в выбранной папке сохраняются файлы вложений и текст письма в виде файла `BODY-<регистрационный номер>.rtf` или `blank.txt`, если вы работаете с письмами без применения форматирования (см. Настройка общих параметров на стр. 139). Если письмо не содержит текста, файлы в формате RTF и TXT не создаются.

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

- Нажмите кнопку **Обзор** и в окне **Обзор папок** укажите папку, в которую будут скопированы файлы письма.
- В списке **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. 122).
  - **Удалять подпись**.
  - **Сохранять в виде файла с присоединенной подписью**.
  - **Отсоединять подпись в отдельный файл**.

  Подробнее о прикрепленной и открепленной электронных подписях файла см. Открепление и прикрепление подписи файла (на стр. 80).
- Если требуется отправлять квитанцию о прочтении письма в случае, когда обработаны только некоторые файлы вложения письма, установите флажок **Посылать квитанцию о прочтении.**

Примечание. После обработки письма со всеми файлами вложений квитанция о прочтении отправляется всегда.

---

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 созданная вами подпапка папки **Входящие** или **Деловая почта**.

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**.

Копирование правил автопроцессинга

Если вам необходимо создать множество однотипных правил, незначительно отличающихся друг от друга (например, чтобы организовать индивидуальную рассылку файлов вашим контактам), вы можете скопировать существующее правило и отредактировать его. Для этого 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 40 на стр. 122).

3 На панели просмотра **Автопроцессинг** выберите правило, которое нужно скопировать, и нажмите кнопку **Копировать**. Созданная копия выбранного правила будет выделена серым цветом.

4 Чтобы изменить параметры скопированного правила, нажмите кнопку **Изменить**. Настройка правил описана в следующих разделах:

- Создание правила для исходящих файлов (на стр. 123).
- Создание правила для входящих писем (на стр. 126).

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. 150).
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. 122) снимите флажок **Сохранять письма, обработанные автопроцессингом**.

Данные настройки позволят существенно повысить скорость обработки писем правилами автопроцессинга.

Внимание! Если вы отключите сохранение писем, обработанных автопроцессингом, и сохранение истории в папке **Аудит**, обработанные письма с необработанными файлами вложений, а также информация об их наличии будут утеряны.

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. 136).

Для просмотра журнала автопроцессинга выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. Интерфейс программы на стр. 32) в меню **Файл** выберите пункт **Журнал автопроцессинга**. Откроется окно **Просмотр журналов**.

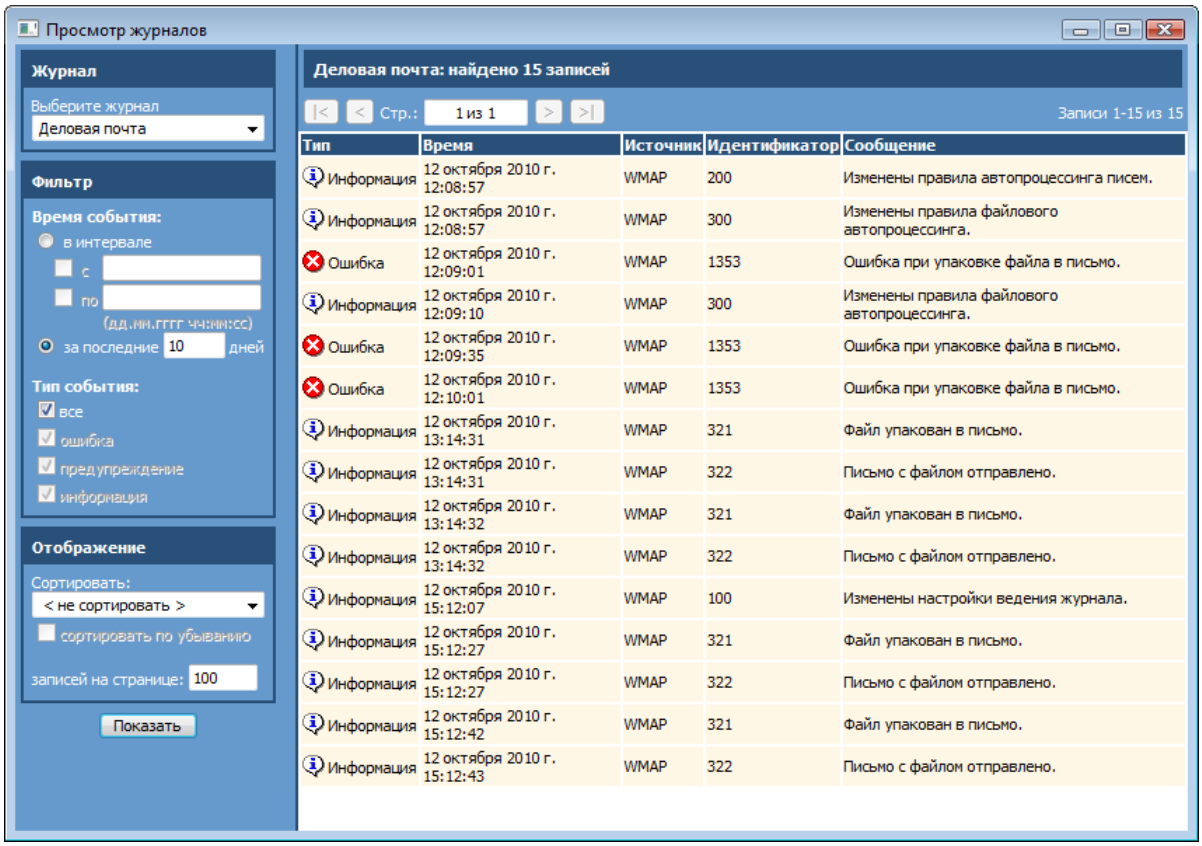


Рисунок 46. Просмотр журнала автопроцессинга

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 46 на стр. 133).

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**.

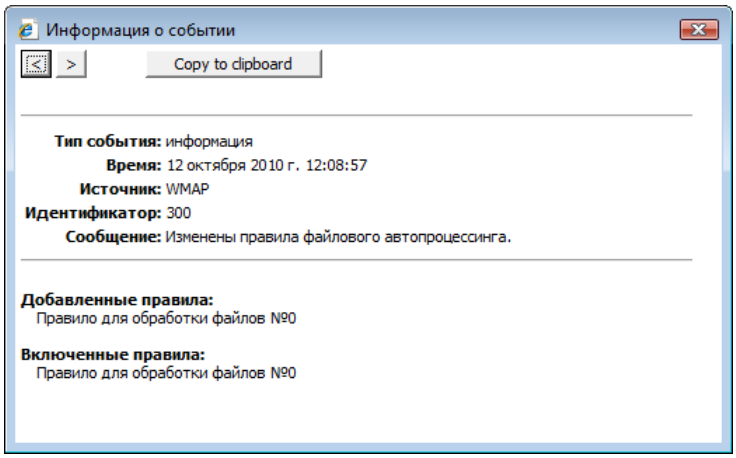


Рисунок 47. Подробная информация о событии

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 7. События автопроцессинга

Тип события	Идентификатор события	Описание события
	200	Изменены правила автопроцессинга писем

Тип события	Идентификатор события	Описание события
Информация	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
	1355	Ошибка при удалении обработанного файла

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**.

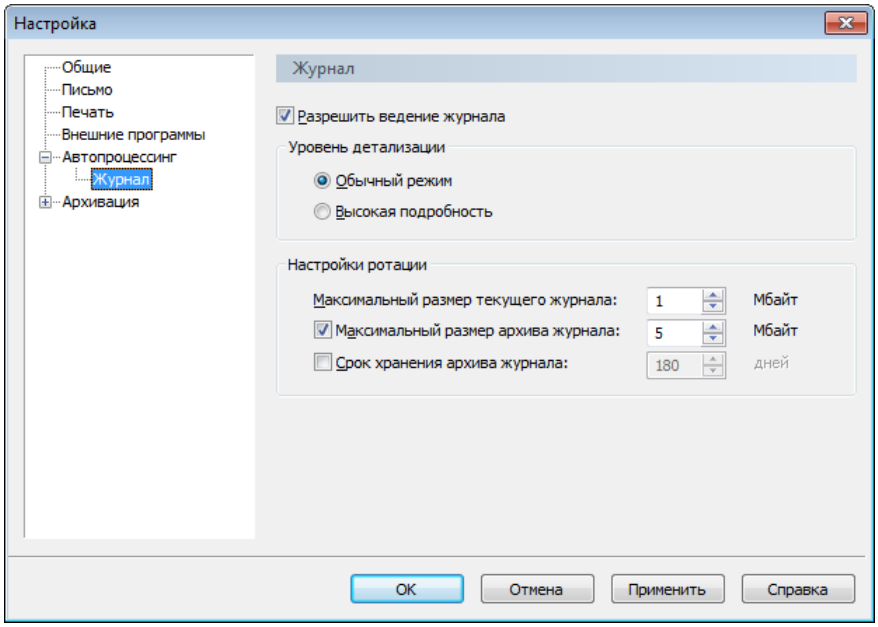


Рисунок 48. Настройка журнала автопроцессинга

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**.

7

Настройка программы

Настройка общих параметров 139

Настройка архивации писем 141

Настройка параметров работы с письмами 145

Настройка печати 147

Настройка внешних программ 148

Работа в программе с правами администратора 150

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. 32) в меню **Инструменты** выберите пункт **Настройка**.

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

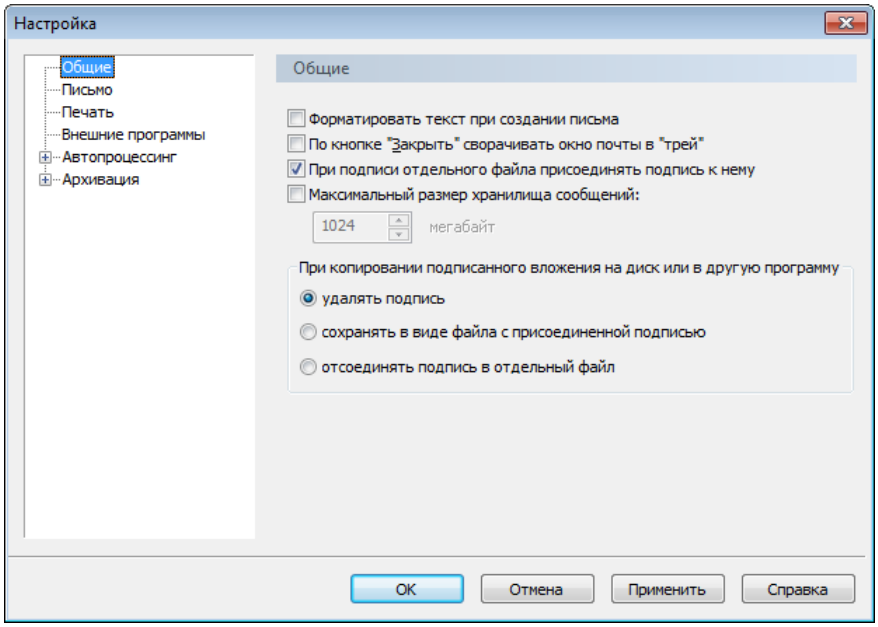


Рисунок 49. Общие настройки программы ViPNet Деловая почта

3 Если при создании писем вы хотите использовать возможности форматирования текста, установите флажок **Форматировать текст при создании письма** (по умолчанию снят). При этом в окне создания писем (см. Окно создания и просмотра писем на стр. 46) будет отображаться панель форматирования.

Отправлять письма без применения форматирования рекомендуется в случае, когда получатели письма используют программу ViPNet Деловая почта более ранних версий, в которой не поддерживается форматирование текста. Если вы отправите такому получателю письмо с применением форматирования, он получит текст вашего письма в виде файла вложения BODY-<регистрационный номер письма>.rtf и сможет прочесть его с помощью текстового редактора, например Microsoft Office Word или Microsoft WordPad.

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

5 Если требуется отсоединять электронную подпись при подписании отдельного файла (см. Подписание файла на стр. 79), 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);
- перестанет отправлять файлы с помощью правил автопроцессинга, если они были настроены.

Примечание. Программа не сможет обработать только те письма и файлы, размер которых превышает оставшееся в хранилище место. Письма и файлы меньшего размера будут приниматься и отправляться.

---

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 прикрепленной и открепленной электронных подписях файла см. Открепление и прикрепление подписи файла (на стр. 80).

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. 32) в меню **Инструменты** выберите пункт **Настройка**.

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

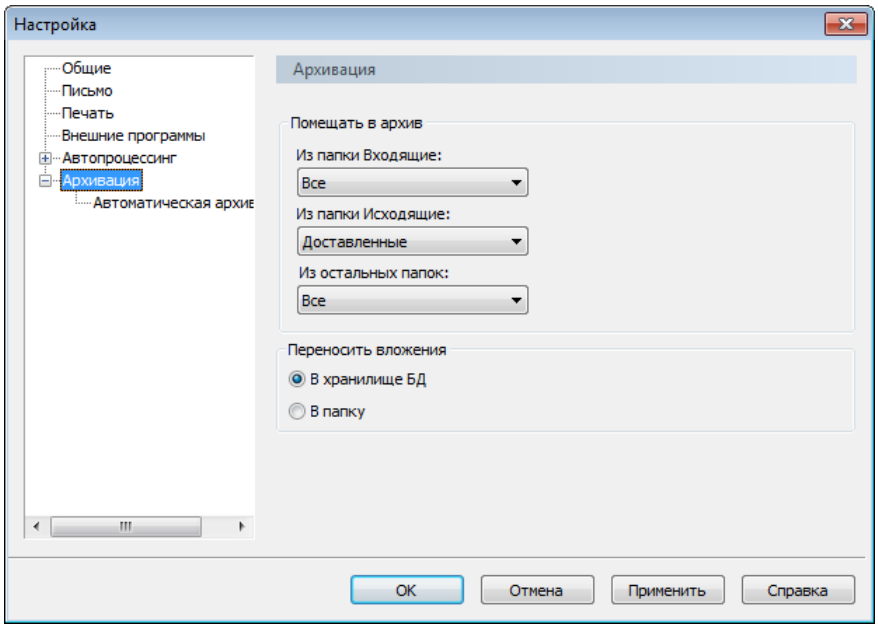


Рисунок 50. Настройка параметров архивации

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**.

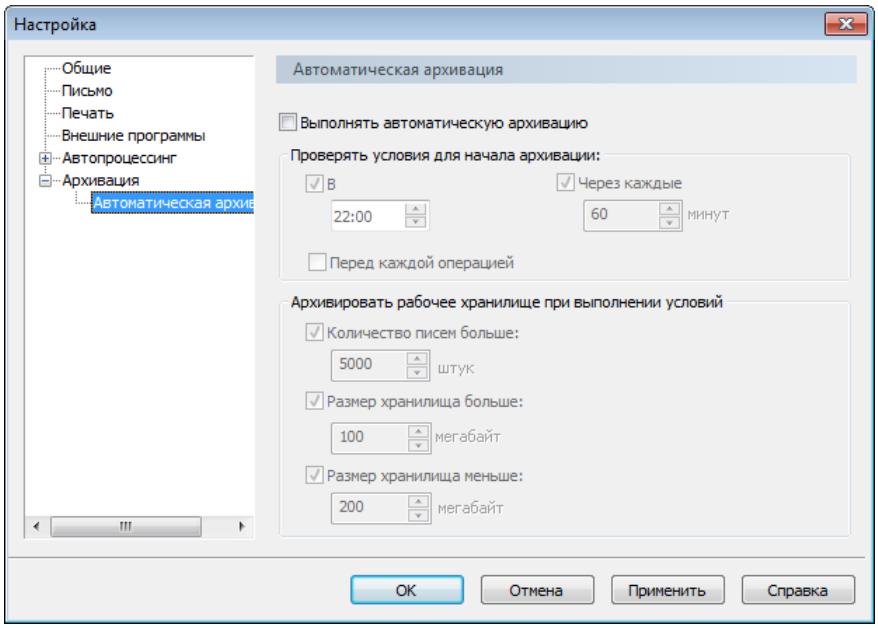


Рисунок 51. Параметры автоматической архивации

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. 32) в меню **Инструменты** выберите пункт **Настройка**.

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

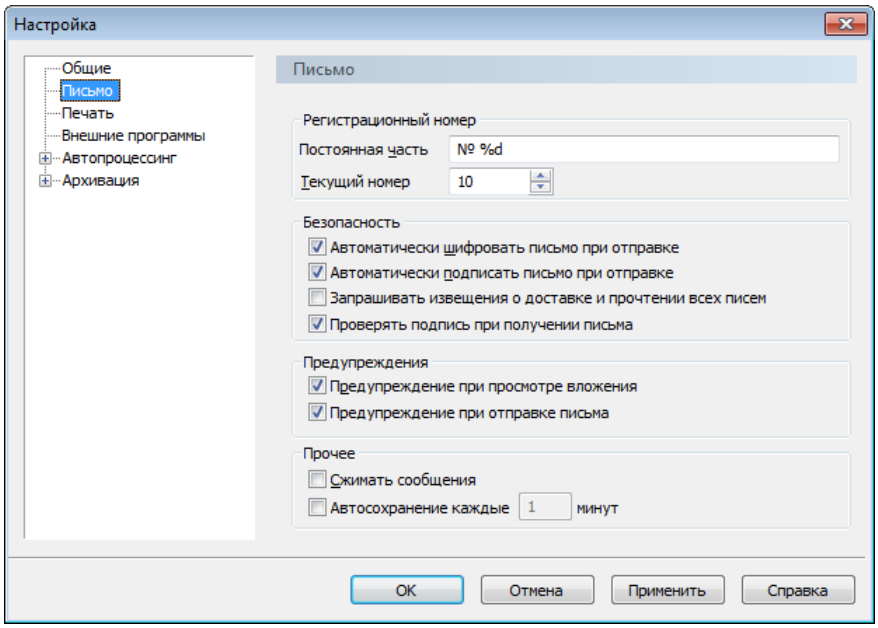


Рисунок 52. Параметры работы с письмами

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. 32).

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. 71).
- 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. 50).
- 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 печати

Чтобы настроить параметры печати писем выполните следующие действия:

1 В окне программы ViPNet Деловая почта (см. Интерфейс программы на стр. 32) в меню **Инструменты** выберите пункт **Настройка**.

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

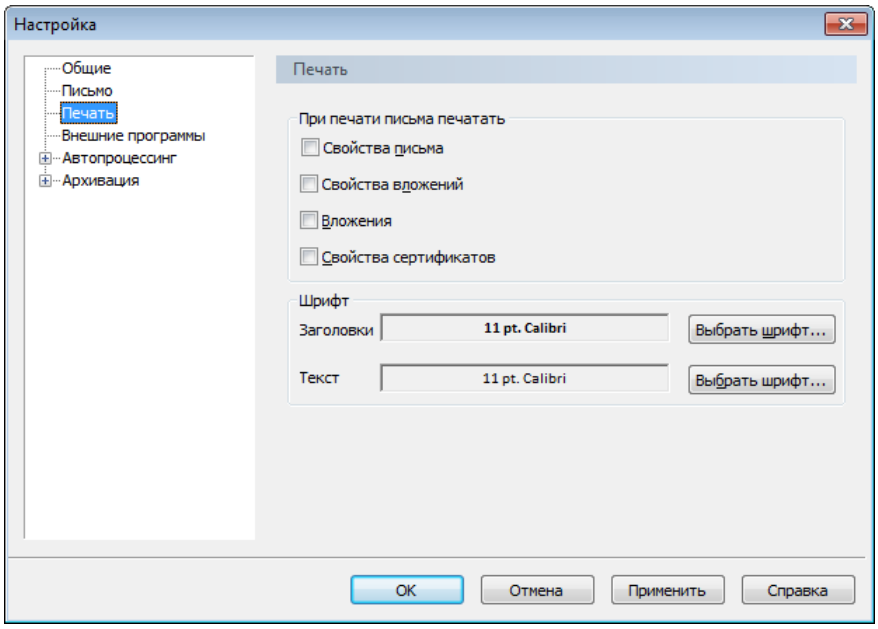


Рисунок 53. Настройки печати

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**.
- **Свойства сертификатов.**

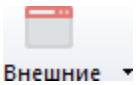
Этот флажок включает печать свойств сертификата, которыми подписаны письмо и (или) его вложения. Поэтому для того, чтобы свойства сертификатов выводились на печать, необходимо также установить флажки **Свойства письма** и (или) **Свойства вложений**.

4 Чтобы изменить шрифт заголовков и текста при печати писем, созданных без применения форматирования, и описанной выше дополнительной информации, 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 выполните одно из действий:

- в меню **Инструменты** выберите **Запуск внешних программ** и затем нужную программу из списка;
- на панели инструментов нажмите кнопку 

и выберите нужную программу из списка.

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

1 В окне программы ViPNet Деловая почта (см. Интерфейс программы на стр. 32) в меню **Инструменты** выберите пункт **Настройка**.

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

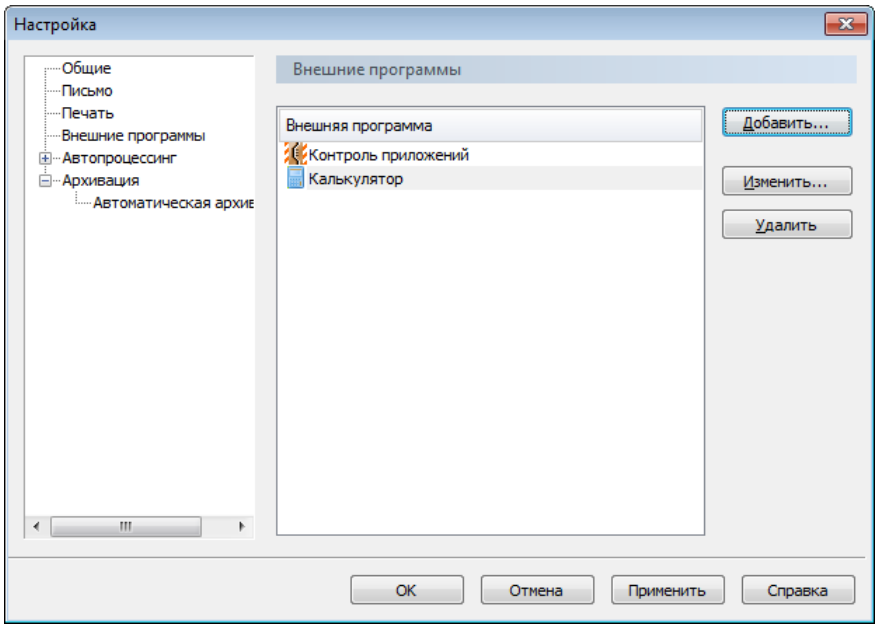


Рисунок 54. Настройка внешних программ

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. 150).
- Дополнительные настройки параметров безопасности (на стр. 151).
- Изменение способа аутентификации пользователя (на стр. 152).

При работе в режиме администратора все ограничения, накладываемые уровнем полномочий пользователя (см. глоссарий, стр. 206), снимаются.

Чтобы войти в программу в качестве администратора:

1 В окне программы ViPNet Деловая почта (см. Интерфейс программы на стр. 32) 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.

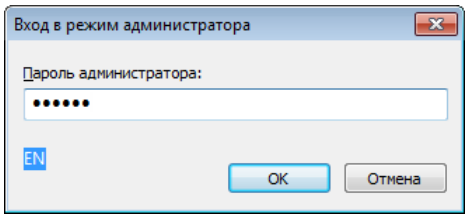


Рисунок 55. Ввод пароля администратора сетевого узла

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 (см. глоссарий, стр. 206) 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. 150).

2 В окне программы в меню **Инструменты** выберите пункт **Настройка**.

3 В окне **Настройка** на панели навигации выберите раздел **Администратор**.

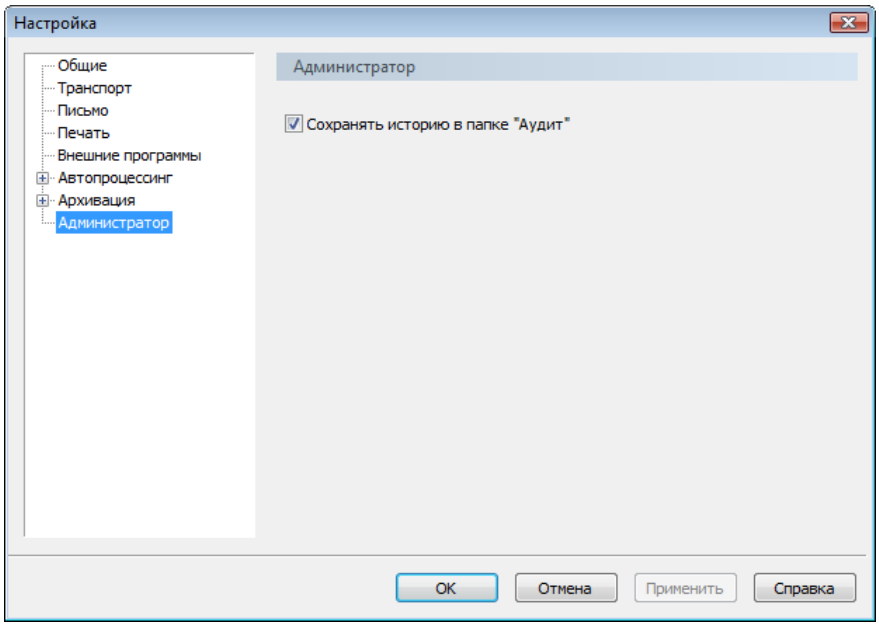


Рисунок 56. Дополнительные настройки в разделе «Администратор»

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. Данный параметр задается администратором сети ViPNet в программе ViPNet Administrator и передается на узел в составе дистрибутива ключей или в составе обновления справочников и ключей. Администратор сетевого узла может изменить состояние флажка **Разрешить сохранение пароля в реестре**, это изменение будет действительно до следующего обновления справочников и ключей. После следующего обновления состояние флажка будет соответствовать настройкам, заданным администратором сети ViPNet.

- **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 сертификатов из хранилища ОС** — 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 аннулированных сертификатов** — этот флажок следует установить, если в системе используются сертификаты, изданные внешними удостоверяющими центрами, так как в таких сертификатах информация о списках аннулированных 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. 25).

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. 165).

При выборе способа аутентификации по персональному ключу подключите внешнее устройство для сохранения на нем персонального ключа пользователя. Если вы выбрали способ аутентификации по персональному ключу, также необходимо перенести на это же внешнее устройство ключи подписи пользователя (контейнер ключей (см. глоссарий, стр. 206)). 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 **ОК**.

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

В сетях ViPNet, управляемых с помощью ПО ViPNet Administrator, 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. 28). После назначения пользователю нового способа аутентификации администратор вышлет обновление ключей узла. Приняв данное обновление ключей, пользователь сможет выполнить аутентификацию на узле только выбранным способом.

8

Настройка параметров безопасности

Смена пароля пользователя 155

Настройка параметров шифрования 159

Настройка параметров криптопровайдера ViPNet CSP 161

Настройка автоматической установки сертификатов в системное хранилище 163

Смена пароля пользователя

Пароль пользователя рекомендуется менять раз в 3 месяца. Как правило, 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 оповещение о необходимости сменить пароль пользователя. В этом случае при входе в программу 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 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. 112), 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**.

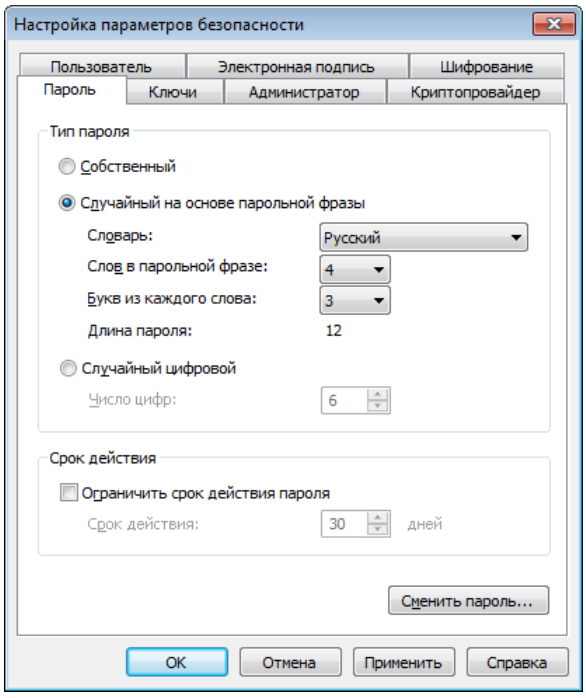


Рисунок 57. Смена текущего пароля пользователя

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

- **Собственный** — пароль, определяемый пользователем (см. Выбор собственного пароля на стр. 156);
- **Случайный на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы по заданным параметрам (см. Выбор пароля на основе парольной фразы на стр. 156);
- **Случайный цифровой** — пароль, формируемый автоматически из заданного числа цифр (см. Выбор цифрового пароля на стр. 158).

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 число дней.

5 Нажмите кнопку **OK**.

Выбор собственного пароля

Для того чтобы сменить текущий пароль пользователя на собственный:

1 На вкладке **Пароль** (см. Рисунок 57 на стр. 155) выберите **Собственный**.

2 Нажмите кнопку **Сменить пароль**.

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

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

4 Нажмите кнопку **OK**.

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 57 на стр. 155) 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.

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

---

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.

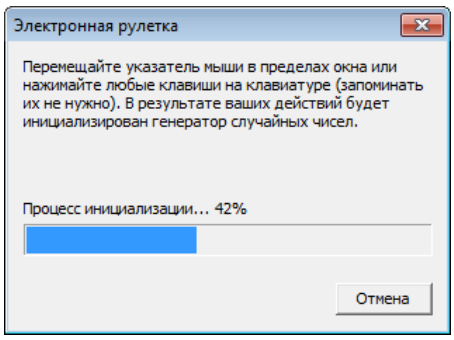


Рисунок 58. Электронная рулетка

4 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 **OK**.

Теперь при запуске программы ViPNet Деловая почта от имени того же пользователя следует вводить указанное число букв каждого слова парольной фразы, без пробелов. Например, для парольной фразы «кипучий фазан скрутил разгильдяя» с параметрами пароля по умолчанию (4 буквы из каждого слова) при запуске программы следует, используя английскую раскладку клавиатуры, вводить буквы «кипуфазаскруразг».

Выбор цифрового пароля

Для того чтобы сменить текущий пароль пользователя на цифровой:

1 На вкладке **Пароль** (см. Рисунок 57 на стр. 155) выберите **Случайный цифровой**, после чего в поле **Число цифр** укажите длину пароля.

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

2 Нажмите кнопку **Сменить пароль**.

3 Выполните действия, предлагаемые в окне **Электронная рулетка** (см. Рисунок 58 на стр. 157).

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

4 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 исходящих писем. Для этого выполните следующие действия:

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

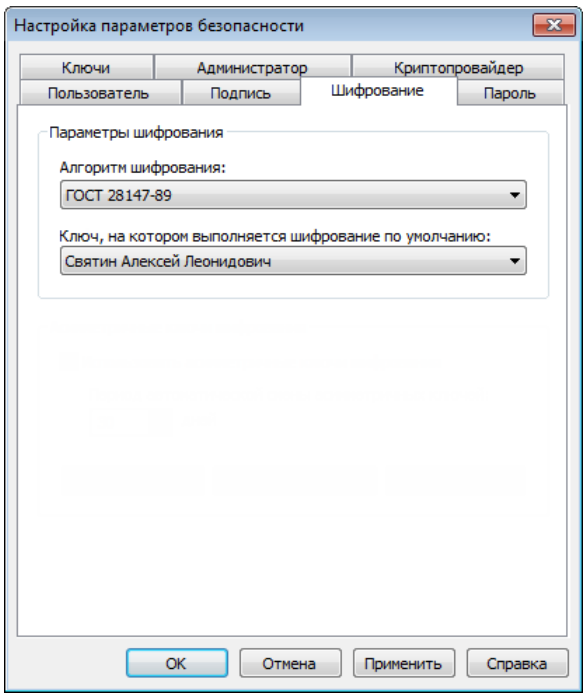


Рисунок 59. Настройка параметров шифрования

2 В списке **Алгоритм шифрования** выберите алгоритм шифрования исходящих писем.

По умолчанию выбран алгоритм ГОСТ 28147-89. В соответствии с выбранным алгоритмом будет осуществляться зашифрование исходящих писем. Расшифрование входящих писем производится в соответствии с тем алгоритмом, который был задан при их зашифровании отправителем.

Если для управления сетью ViPNet используется программа ViPNet Network Manager версии 4.3 и выше или ПО ViPNet Administrator версии 4.4.1 и выше, администратор сети ViPNet может изменить алгоритм шифрования. В этом случае после обновления справочников и ключей на сетевом узле будет выбран алгоритм, заданный администратором сети ViPNet.

3 В следующем списке укажите ключи, на которых должно выполняться шифрование исходящих писем. 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 переписке в программе ViPNet Деловая почта. То есть если исходящее письмо 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. Это криптопровайдер, который позволяет использовать российские криптографические алгоритмы в приложениях Microsoft и других программах, использующих интерфейс Microsoft CryptoAPI 2.0. Кроме этого, программа ViPNet CSP обеспечивает работу с контейнерами ключей (см. глоссарий, стр. 206) и поддержку различных внешних устройств хранения ключей (см. Внешние устройства на стр. 190).

Чтобы настроить программу ViPNet CSP, выполните следующие действия:

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

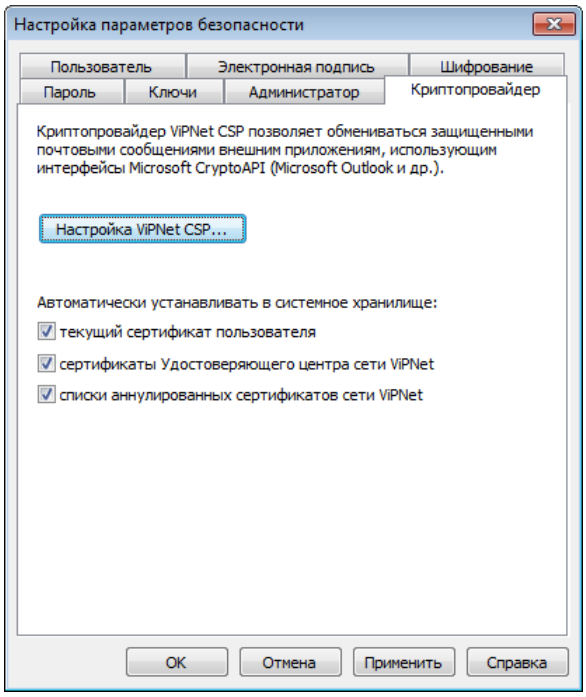


Рисунок 60. Настройка параметров криптопровайдера ViPNet CSP

2 Нажмите кнопку **Настройка ViPNet CSP**. Откроется окно **ViPNet CSP**, в котором вы можете:

- Задать необходимые параметры криптопровайдера ViPNet CSP.
- 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 Если необходимо, настройте параметры автоматической установки сертификатов в хранилище (см. Настройка автоматической установки сертификатов в системное хранилище на стр. 163).

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

Настройка автоматической установки сертификатов в системное хранилище

Чтобы задать параметры автоматической установки сертификатов в системное хранилище, выполните следующие действия:

1. В окне **Настройка параметров безопасности** откройте вкладку **Криптопровайдер** (см. Рисунок 60 на стр. 161).
2. При необходимости укажите, какие сертификаты и списки аннулированных сертификатов следует устанавливать в системное хранилище автоматически (см. Установка в хранилище автоматически на стр. 90), 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 в составе обновления ключей;
   - **списки аннулированных сертификатов сети ViPNet** — для установки в системное хранилище списков аннулированных сертификатов, получаемых из программы ViPNet Удостоверяющий и ключевой центр в составе обновления ключей.
3. Выполнив необходимые настройки, нажмите кнопку **OK**.

Подробнее об автоматической установке сертификатов в хранилище см. раздел «Установка в хранилище автоматически (на стр. 90)».

A

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 ключ электронной подписи, которые хранятся на внешнем устройстве, это может быть вызвано одной из следующих причин:

- Внешнее устройство не обеспечивает аппаратную поддержку алгоритмов ГОСТ.
- Внешнее устройство хранения данных не поддерживает стандарт PKCS#11. Проверить, поддерживает ли ваше устройство этот стандарт, можно в разделе Внешние устройства (на стр. 190).
- 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 аннулированных сертификатов, который установлен в хранилище данного узла. При выборе аннулированного сертификата появится соответствующее сообщение. В этом случае следует обратиться к администратору вашего удостоверяющего центра.
- Выбранный сертификат не имеет назначения «Шифрование ключей». Это расширение должно отображаться в окне **Сертификат**, на вкладке **Состав**, в поле **Использование ключа**. В этом случае следует обратиться к администратору вашего удостоверяющего центра для переиздания сертификата.

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.

Входящее письмо перемещено в папку Проблемные или Поврежденные

Если при обработке входящего письма программой ViPNet Деловая почта произошла ошибка, в зависимости от типа ошибки входящее письмо будет автоматически помещено в одну из двух основных подпапок (см. Основные папки на стр. 35) в папке **Аудит,** а на экране появится соответствующее предупреждение. Если выбрать такое письмо, вместо текста письма на панели чтения (см. Интерфейс программы на стр. 32) будет отображаться информация о номере, теме, отправителе письма и коде ошибки.

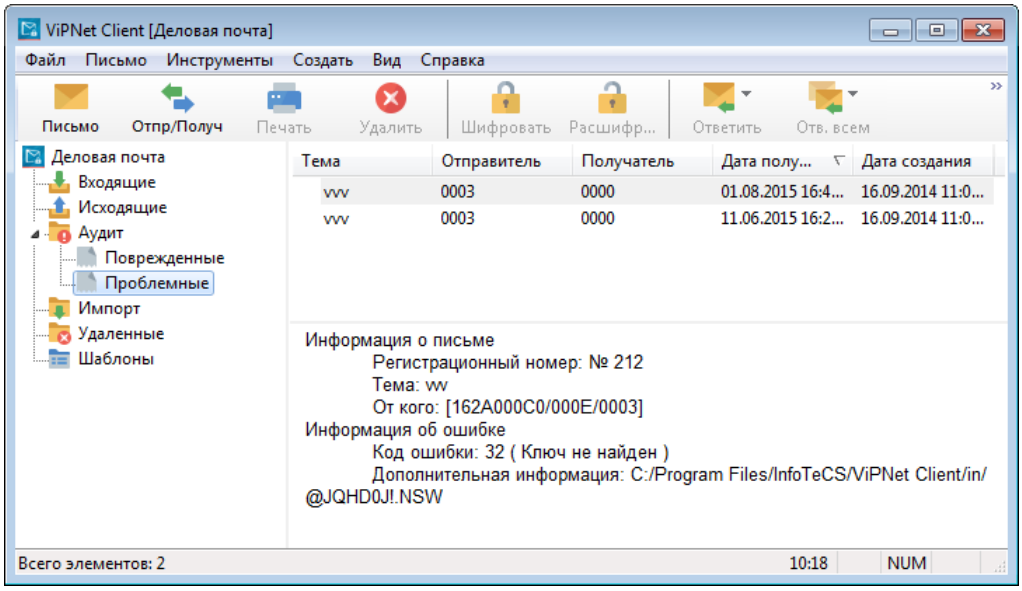


Рисунок 61. Просмотр письма в папке Проблемные

В папку **Поврежденные** перемещаются входящие письма, если:

- при обработке письма произошла критическая ошибка;
- письмо было отправлено 30 дней назад, но не доставлено, потому что программа ViPNet Деловая почта не запускалась в течение 30 дней.

Письмо в папке **Поврежденные** невозможно восстановить. Если в папке **Поврежденные** появилась новая запись, сообщите о ней администратору сети ViPNet.

В папку **Проблемные** перемещаются входящие письма, которые не удалось расшифровать. Если в папке **Проблемные** появилась новая запись, выполните одно или несколько следующих действий:

- Перезапустите программу ViPNet Деловая почта. После повторного запуска программа выполнит повторную обработку проблемного письма. В случае успешной обработки письма в папке **Входящие** появится новое письмо. При этом проблемное письмо также останется в папке **Проблемные**.
- Если на одном сетевом узле зарегистрировано несколько пользователей, возможно, проблемное входящее письмо адресовано другому пользователю. Сообщите другому пользователю, который зарегистрирован на этом узле, чтобы он попытался открыть проблемное письмо, когда войдет в программу ViPNet Деловая почта под своим именем (см. Смена пользователя на стр. 24).
- Если письмо все же не удалось открыть, возможно, на вашем сетевом узле необходимо обновить справочники и ключи. Сообщите о проблемном письме и типе ошибки администратору сети ViPNet и следуйте его рекомендациям.

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.

Ошибка отправки письма: Ключ не найден

При попытке отправить письмо с электронной подписью появляется следующее сообщение:

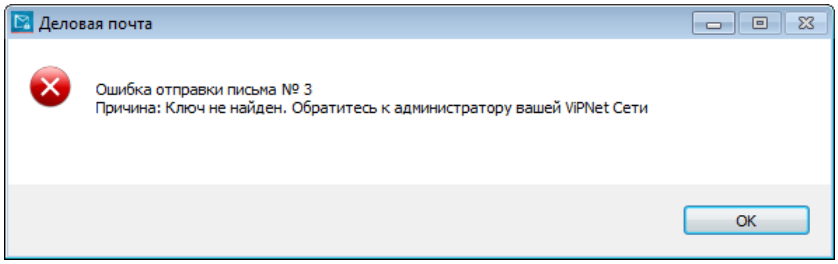


Рисунок 62. Сообщение об ошибке при отправке письма

Данная ошибка может возникать после смены мастер-ключей в вашей сети ViPNet. Для решения проблемы выберите в качестве текущего сертификат (см. Смена текущего сертификата на стр. 95), выпущенный вместе с новыми ключами. Как правило, это сертификат с самой поздней датой выпуска. Если подходящего сертификата нет, обратитесь к администратору вашей сети ViPNet.

Невозможно выполнить правило автопроцессинга

При отправке письма с помощью автопроцессинга появляется следующее сообщение:

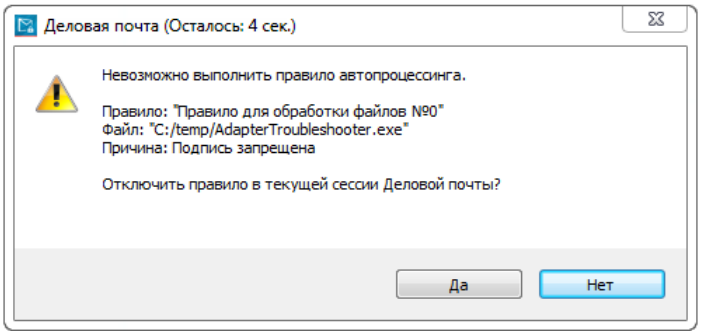


Рисунок 63. Ошибка при выполнении правила автопроцессинга

Данное сообщение означает, что ваш сертификат не позволяет заверять письма с помощью электронной подписи. Для продолжения работы выполните одно из действий:

- Если подпись не нужна, измените правило автопроцессинга (см. Создание правила для исходящих файлов на стр. 123), сняв флажок **Подписывать письмо при отправке**.
- Если подпись нужна, обратитесь к администратору сети ViPNet за обновлением сертификата.

B

Общие сведения о сертификатах ключей проверки электронной подписи

Определение и назначение

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

- Ключ электронной подписи — для формирования электронной подписи (см. глоссарий, стр. 208) и расшифрования сообщения. Ключ электронной подписи хранится в тайне и не подлежит распространению.
- Ключ проверки электронной подписи — для проверки электронной подписи и зашифрования сообщения. Ключ проверки электронной подписи известен всем участникам информационного обмена и может передаваться по незащищенным каналам связи.

Таким образом, криптография с ключом проверки электронной подписи 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.

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

Поскольку ключ проверки электронной подписи распространяется публично, существует опасность того, что злоумышленник, подменив ключ проверки электронной подписи одного из пользователей, может выступать от его имени. Для обеспечения доверия к ключам проверки электронной подписи создаются удостоверяющие центры (согласно Федеральному закону РФ № 63 «Об электронной подписи» от 6 апреля 2011 года), которые играют роль доверенной третьей стороны и заверяют ключи проверки электронной подписи каждого из пользователей своими электронными подписями — иначе говоря, сертифицируют эти ключи.

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

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

Сертификат включает ключ проверки электронной подписи и список дополнительных атрибутов, принадлежащих пользователю (владельцу сертификата). К таким атрибутам относятся: имена владельца и издателя сертификата, номер сертификата, время действия сертификата, предназначение ключа проверки электронной подписи (электронная подпись, шифрование) и так далее. Структура и протоколы использования сертификатов определяются международными стандартами (см. Структура на стр. 176).

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 ключа электронной подписи, 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. PKI и асимметричная криптография на стр. 179), может использоваться либо как сертификат издателя (в иерархической модели), либо для проверки сертификатов пользователей другой сети (в распределенной модели).

Рисунок 64. 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 аннулирован, то сертификат считается действительным. Документы, подписанные действительным сертификатом и не изменявшиеся с момента их подписания, также считаются действительными.

Таким образом, криптография с ключом проверки электронной подписи и инфраструктура обмена сертификатами ключей проверки электронной подписи (см. PKI и асимметричная криптография на стр. 179) 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 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,
- ключ проверки электронной подписи владельца,
- имя владельца сертификата.

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

К необязательным полям относятся:

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

Рисунок 65. Структура сертификата, соответствующего стандарту X.509 версий 1, 2 и 3

Сертификат ключа проверки электронной подписи

Кому выдан: Client 2

Кем выдан: Кузнецов Виктор Петрович

Действителен с 19 июня 2014 г. по 19 июня 2019 г.

Назначение:	• Подтверждает удаленному компьютеру идентификацию вашего компьютера. • Защищает сообщения электронной почты.
Версия:	V3
Серийный номер:	01 CF 8B 9F 55 CA 35 90 00 00 00 01 15 EA 00 03
Алгоритм электронной подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Имя: Кузнецов Виктор Петрович Должность: Администратор Подразделение: Удостоверяющий и ключевой центр Организация: Infotecs
Действителен с:	19 июня 2014 г. 13:17:00 (GMT+04:00)
Действителен по:	19 июня 2019 г. 13:17:00 (GMT+04:00)
Субъект:	Имя: Client 2 Организация: Infotecs
Открытый ключ:	ГОСТ Р 34.10-2001 (512 Бит) 04 40 4B E4 FF 92 EA CB 7E 67 9C D4 6E E5 5C 68 96 59 F8 FC B7 34 2E B4 86 99 EA 3D 89 10 47 F5 9E 3D 40 BD 0F FC 7C 9E 4D 4C 9B 14 55 94 F0 59 79 11 50 A5 F5 C9 06 77 1E 94 E3 54 FE E8 BA B1 03 D3

Расширения сертификата X.509

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)
Идентификатор ключа центра сертификатов:	Идентификатор ключа=7D F1 CD 4A 8A 31 14 4F 43 55 59 05 63 77 A8 E4 82 12 5B 5B Издатель сертификата: O="Infotecs, Documentation, Prakhova" OU=Удостоверяющий и ключевой центр T=Администратор CN=Кузнецов Виктор Петрович Серийный номер сертификата=01 CE B8 44 20 0A AA E0 00 00 00 00 00 00 00 01
Идентификатор ключа субъекта:	DA 3C 23 13 22 21 FA D4 48 9F 3B E9 5E 05 65 46 C5 CF 6A D2
Срок действия закрытого ключа:	С 19 июня 2014 г. 13:17:00 (GMT+04:00) по 19 июня 2015 г. 13:17:00 (GMT+04:00)
Основные ограничения:	Тип субъекта=Пользователь

Результат проверки сертификата

Сертификат действителен.
Проверен 1 августа 2014 г. 5:46:03 (GMT+04:00).

Рисунок 66. Пример сертификата ViPNet, соответствующего стандарту X.509 версии 3

PKI и асимметричная криптография

Одной из реализаций инфраструктуры, позволяющей управлять сертификатами ключей проверки электронной подписи, является технология PKI (инфраструктура открытых ключей) (см. глоссарий, стр. 204). PKI обслуживает жизненный цикл сертификата: издание сертификатов, хранение, резервное копирование, печать, взаимную сертификацию, ведение списков аннулированных сертификатов (CRL), 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 CRL 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 (см. глоссарий, стр. 205). Головной удостоверяющий центр выдает кросс-сертификаты подчиненным ему центрам, тем самым обеспечивая доверие к ключам проверки электронной подписи этих центров. Каждый удостоверяющий центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие к сертификату каждого удостоверяющего центра основано на заверении его ключом вышестоящего центра. Сертификат головного удостоверяющего центра (корневой сертификат (см. глоссарий, стр. 206)) 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.

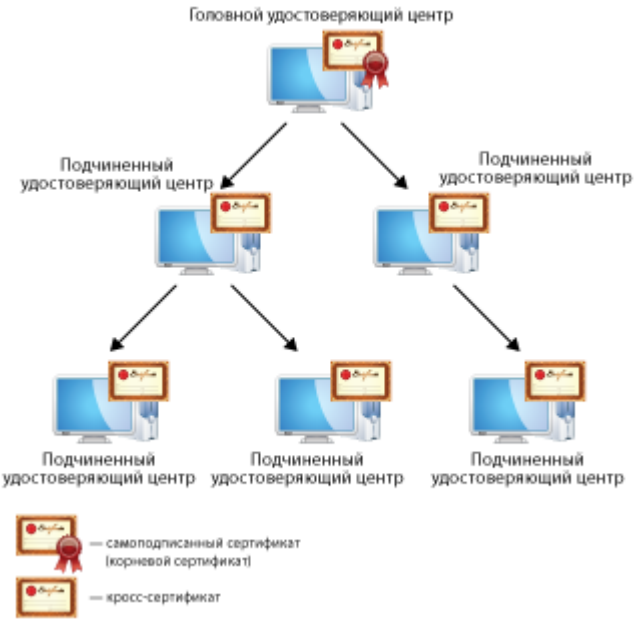


Рисунок 67. Иерархическая модель доверительных отношений

- 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 ключе проверки электронной подписи. Поэтому в сети, отправившей запрос, нет необходимости переиздавать сертификаты пользователей.

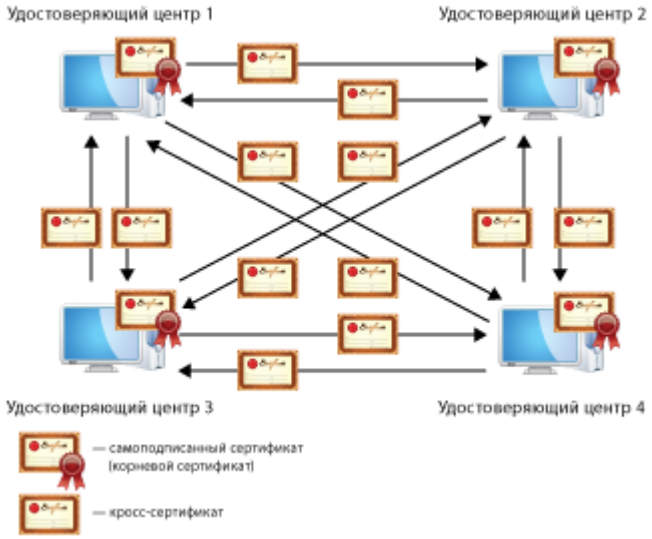


Рисунок 68. Распределенная модель доверительных отношений

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

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 (см. глоссарий, стр. 207), 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. глоссарий, стр. 206) с использованием открытого ключа получателя.
6. Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.
7. Документ отправляется.

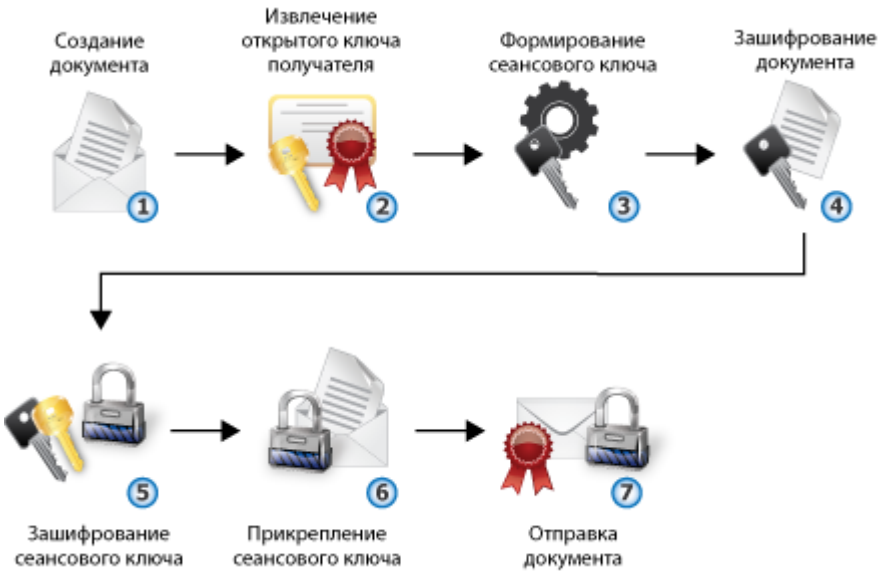


Рисунок 69. Зашифрование электронного документа

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 70. Расшифрование электронного документа

Использование сертификатов для подписания электронных документов

Когда отправитель подписывает документ, он использует ключ электронной подписи, соответствующий ключу проверки электронной подписи, который хранится в сертификате. Когда получатель проверяет электронную подпись (см. глоссарий, стр. 208) сообщения, он извлекает ключ проверки электронной подписи 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. Ключ электронной подписи отправителя извлекается из контейнера ключей.
4. С использованием ключа электронной подписи отправителя на основе значения хэш-функции формируется электронная подпись.
5. Электронная подпись прикрепляется к документу.
6. Зашифрованный документ отправляется.

Рисунок 71. 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. Ключ проверки электронной подписи отправителя извлекается из сертификата отправителя.
5. Электронная подпись расшифровывается с использованием ключа проверки электронной подписи 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. Электронная подпись считается недействительной также в том случае, если сертификат отправителя просрочен, аннулирован, искажен или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

Рисунок 72. Процесс проверки электронной подписи документа

Использование сертификатов для подписания и шифрования электронных документов

Подписание и зашифрование

1. Пользователь создает электронный документ.
2. Вычисляется значение хэш-функции документа.
3. Ключ электронной подписи отправителя извлекается из контейнера ключей.
4. Открытый ключ получателя извлекается из сертификата получателя.
5. С использованием ключа электронной подписи отправителя на основе значения хэш-функции формируется электронная подпись.
6. Электронная подпись прикрепляется к документу.
7. Формируется симметричный сеансовый ключ (см. глоссарий, стр. 207), 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. глоссарий, стр. 206) с открытого ключа получателя.
10. Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.
11. Документ отправляется.

Рисунок 73. 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 Ключ проверки электронной подписи отправителя извлекается из сертификата отправителя.

9 Электронная подпись расшифровывается с использованием ключа проверки электронной подписи 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, аннулирован, искажен или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

12 Расшифрованный документ доступен получателю.

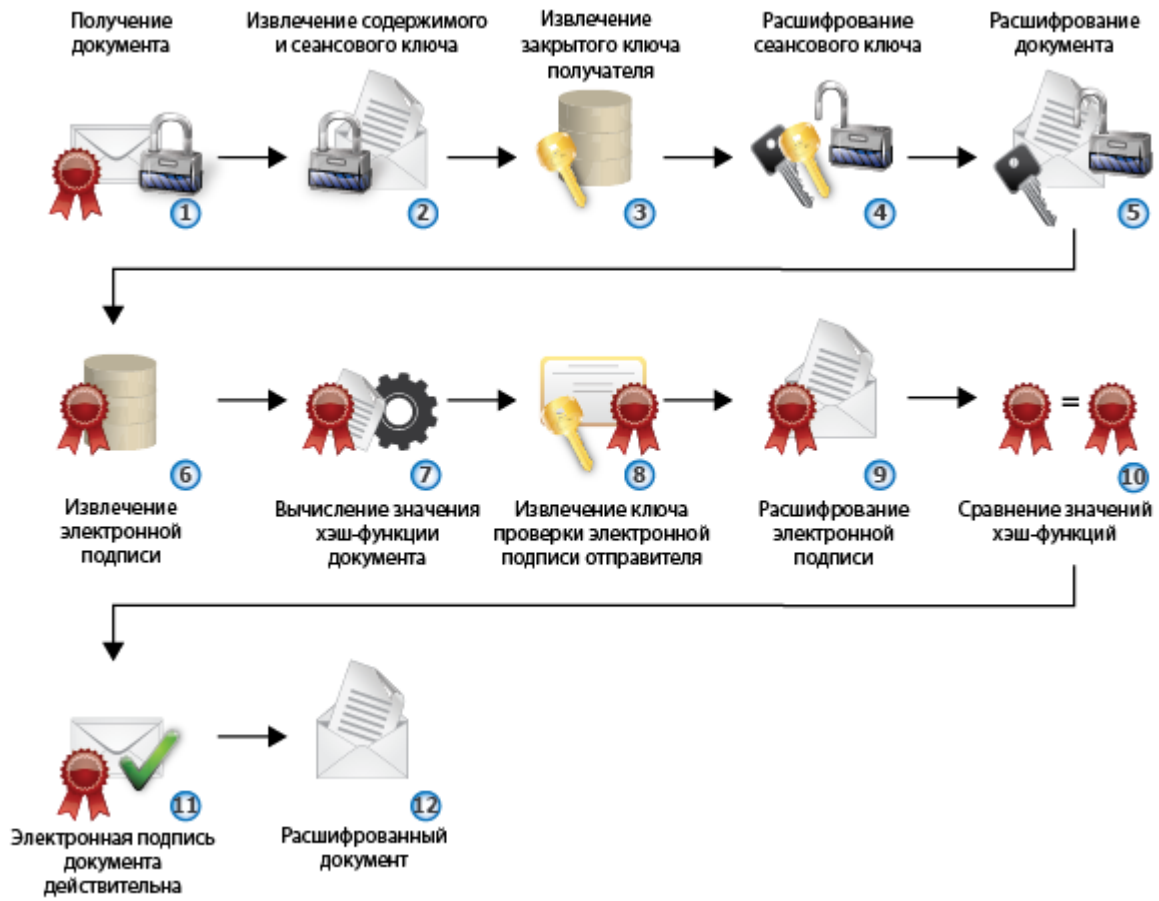


Рисунок 74. Процесс расшифрования и проверки электронной подписи документа

C

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей (см. глоссарий, стр. 206), которые вы можете использовать для аутентификации, формирования электронной подписи (см. глоссарий, стр. 208) 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. 25):

- 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. Требования к сертификату см. в разделе Особенности аутентификации с помощью сертификата (на стр. 29).

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP (см. Настройка параметров криптопровайдера ViPNet CSP на стр. 161). 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 семейства устройств в таблице приведено описание, указаны условия и особенности работы с устройствами.

Таблица 8. Поддерживаемые внешние устройства

Название семейства устройств в программе ViPNet CSP	**Полные названия и типы устройств**	**Необходимые и рекомендуемые условия работы с семейством устройств**
ESMART Token	Смарт-карты и токены типов **ESMART Token**, **ESMART Token ГОСТ**, **ESMART Token USB 64K**	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.3 R1). Устройства типа ESMART Token необходимо отформатировать с помощью ПО ESMART PKI Client для Windows с профилем ViPNet2. Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом. При использовании устройства типа ESMART Token ГОСТ возможна аутентификация только по персональному ключу на устройстве.
Infotecs Software Token	**Infotecs Software Token** — программная реализация стандарта PKCS#11	Необходимое ПО входит в поставку ViPNet CSP. С помощью программы token_manager.exe на компьютере должен быть создан виртуальный токен. Подробную информацию о работе с программным токеном см. в документе «Криптографический интерфейс ViPNet PKCS#11 VT. Руководство разработчика», раздел «Создание и удаление слотов и токенов в ViPNet PKCS#11 VT».
A-Key	Смарт-карты **aKey S1000**, **aKey S1003**, **aKey S1004** производства компании Ak Kamal Security	На компьютере должна быть установлена библиотека akpkcs11.dll, предоставленная компанией Ak Kamal Security. Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — `12345678`. Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. При использовании этих устройств возможна аутентификация только по персональному ключу на устройстве.
ViPNet HSM	Виртуальный токен **ViPNet HSM** производства ОАО «ИнфоТеКС»	Необходимо установить клиентское приложение ViPNet HSM и проинициализировать виртуальный токен.

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
JaCarta	Персональные электронные ключи и смарт-карты **JaCarta PKI**, **JaCarta Laser** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемые версии — 2.9.0.1531, 2.11.0.1754). Устройства JaCarta PKI/ГОСТ определяются как принадлежащие одновременно к семействам JaCarta и eToken GOST/JaCarta GOST. Во избежание возникновения проблем рекомендуется запретить опрос неиспользуемого семейства устройств. Для ОС Windows 10 (версия 1803) устройство JaCarta следует отключить. При использовании устройства JaCarta PKI/ГОСТ во избежание появления ошибок не следует сохранять ПИН-коды этого устройства на компьютере.
JCDS	Смарт-карты **Gemalto Optelio Contactless D72**, **KONA 131 72K** и токен **JaCarta LT** с апплетом от компании «Аладдин Р.Д.»	На карту или токен должен быть загружен апплет Datastore, позволяющий модулю jcpkcs11ds.dll (рекомендуемая версия — 1.1.3.20) производства компании «Аладдин Р.Д.» работать с картой или токеном. Для администрирования токенов JaCarta LT на компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемые версии — 2.9.0.1531, 2.11.0.1754). При использовании JaCarta LT возможна аутентификация только по персональному ключу на устройстве.
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. Смарт-карты должны быть особым образом размечены. Обратитесь к производителю устройств.

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
eToken GOST/ **JaCarta GOST**	Персональные электронные ключи **eToken ГОСТ** и **JaCarta ГОСТ** , а также персональные электронные ключи и смарт-карты **JaCarta PKI/ГОСТ** производства компании «Аладдин Р.Д.»	Для работы с указанными устройствами на компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемые версии — 2.9.0.1531, 2.11.0.1754). Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. Устройства JaCarta PKI/ГОСТ определяются как принадлежащие одновременно к семействам JaCarta и eToken GOST/JaCarta GOST. Во избежание возникновения проблем рекомендуется запретить опрос неиспользуемого семейства устройств. Для ОС Windows 10 (версия 1803) устройство JaCarta следует отключить. Перенос ключей подписи на данный тип устройств невозможен.
Rutoken ECP/ **Rutoken Lite**	Электронные идентификаторы **Рутокен ЭЦП** и **Рутокен Lite** производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.2.2.0). Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. При использовании Rutoken Lite возможна аутентификация только по персональному ключу на устройстве.
Rutoken/ **Rutoken S**	Электронные идентификаторы **Рутокен** и **Рутокен S** производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.2.2.0).

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
eToken Aladdin	Персональные электронные ключи **Gemalto SafeNet eToken 5100/5105**, **5200/5205**, **5110**, **7300**, смарт-карта **Gemalto SafeNet eToken 4100** производства компании Gemalto (SafeNet) Персональные электронные ключи **eToken PRO (Java)**, **eToken PRO**, смарт-карты **eToken PRO (Java)**, **eToken PRO**, **JaCarta PRO** производства компании «Аладдин Р.Д.»	Если компьютер работает под управлением ОС Windows 10, на нем должно быть установлено ПО SafeNet Authentication Client (рекомендуемая версия — 10.0.43). Если компьютер работает под управлением другой ОС, на нем должно быть установлено либо ПО PKI Client версии 5.1 SP1, либо ПО SafeNet Authentication Client (рекомендуемая версия — 10.0.43). Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт. Для работы смарт-карты JaCarta PRO на компьютере должно быть установлено ПО JC-PROClient версии 1.0.6 и должен быть включен режим совместимости с eToken. **Примечание**. Если вам необходимо работать с устройством из семейства **eToken Aladdin**, а также с устройством из семейства **JaCarta**, **JCDS** или **eToken GOST/JaCarta GOST**, то во избежание появления ошибок при выполнении криптографических операций не устанавливайте на компьютер одновременно ПО «Единый Клиент JaCarta» и ПО SafeNet Authentication Client.

Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

Алгоритмы и функции, поддерживаемые внешними устройствами

В следующей таблице перечислены криптографические алгоритмы, поддерживаемые внешними устройствами, приведена информация о возможности использования устройств в качестве датчиков случайных чисел, а также 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 ключа проверки электронной подписи), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Таблица 9. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств в программе ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	Поддержка PKCS#11
ESMART Token	**ESMART Token** — отсутствует; **ESMART Token ГОСТ** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (может не поддерживаться на старых устройствах)	**ESMART Token** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 **ESMART Token ГОСТ** — отсутствует	Нет	Да
Infotecs Software Token	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (изолированная программная реализация)	отсутствует	Нет	Да
A-Key	**aKey S1000**, **aKey S1003**, **aKey S1004** — ГОСТ Р 34.10-2012; **aKey S1000**, **aKey S1003** — ГОСТ Р 34.10-2001	отсутствует	Нет	Да
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да
JaCarta	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
JCDS	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
Siemens CardOS	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
eToken GOST/ JaCarta GOST	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ)	отсутствует	Да	Да
Rutoken ECP/ Rutoken Lite	**Рутокен ЭЦП** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ); **Рутокен Lite** — отсутствует	**Рутокен ЭЦП** — отсутствует; **Рутокен Lite** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	**ЭЦП** — да **Lite** — нет	Да

Название семейства устройств в программе ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	Поддержка PKCS#11
Rutoken/ Rutoken S	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
eToken Aladdin	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

Примечание. Шифрование поддерживается не всеми перечисленными устройствами. Для получения более подробной информации см. документацию по необходимому устройству.

D

История версий

В данном приложении описаны основные изменения в предыдущих версиях программы ViPNet Деловая почта.

Что нового 4.5.0

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.5.0 по сравнению с версией 4.3.4.

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

- **Изменения в документации**

  В документацию добавлена информация о том, что при ограничении размера хранилища программа не будет отправлять файлы с помощью правил автопроцессинга, если размер файла превышает размер оставшегося в хранилище места.

Что нового 4.3.4

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.4 по сравнению с версией 4.3.3.

- **Улучшение документации**

  В документацию добавлено ограничение по максимальному количеству писем, которое может храниться в базе данных ПО ViPNet Деловая почта.

Что нового 4.3.3

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.3 по сравнению с версией 4.3.2.

- **Поддержка Windows Server 2016**

  Начиная с версии 4.3.3, программа ViPNet Деловая почта поддерживает операционную систему Windows Server 2016.

- **Возможность ограничения размера вложений в сообщение электронной почты**

  Начиная с версии 4.3.3, администратор сети ViPNet может установить максимальный размер вложения, которое отправляется в программе ViPNet Деловая почта. Письма, имеющие во вложении файлы большего размера, отправлены не будут.

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

Что нового 4.3.2

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.2 по сравнению с версией 4.3.1.

- **Изменен список поддерживаемых операционных систем**

  Начиная с версии 4.3.2, прекращена поддержка ОС Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 в связи с прекращением их поддержки производителем.

- **Вывод свойств сертификата при печати письма**

  В версии 4.3.2 появилась возможность добавлять информацию о сертификате подписи при печати письма:

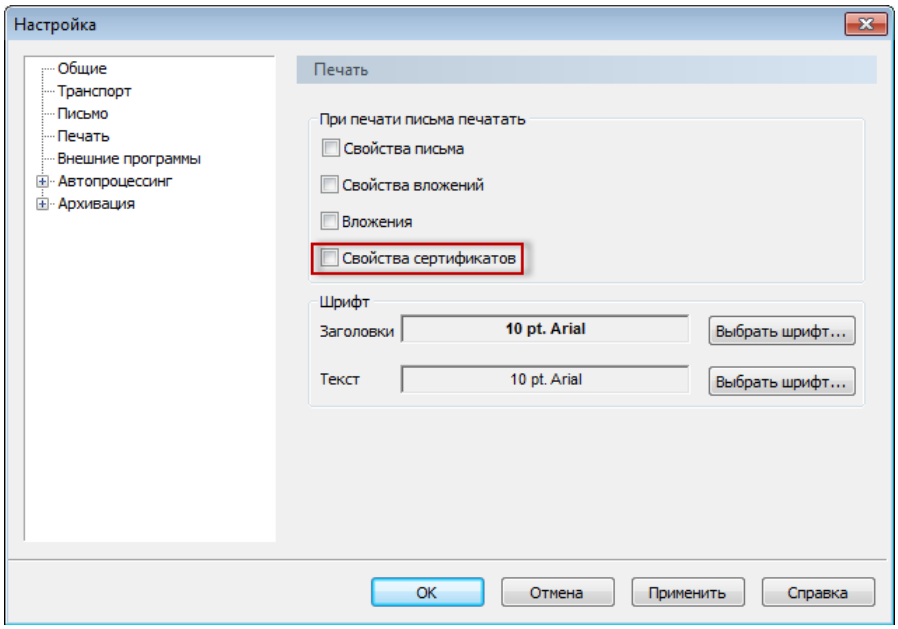


Рисунок 75. Флажок Свойства сертификатов в окне настройки печати

  Это позволит визуально подтвердить действительность электронной подписи при печати письма.

- **Новая адресная книга**

  В новой версии полностью переработана адресная книга программы. Теперь вы можете управлять списками контактов, создавая пользовательские адресные книги и группы рассылки, а также хранить в созданных адресных книгах дополнительные сведения о своих контактах.

- **Новые папки для проблемных писем**

  В папке **Аудит** для писем, при получении которых произошла ошибка, теперь предусмотрены две папки: **Поврежденные** и **Проблемные** (см. Основные папки на стр. 35). Они автоматически создаются при появлении первой ошибки.

- **Новый интерфейс программы**

Был изменен внешний вид программы ViPNet Деловая почта. Кроме того, были выполнены следующие изменения в интерфейсе программы:

Что изменено	Версия 4.3.1	Версия 4.3.2
Название окна, вызываемого при создании письма нажатием кнопки **Получатели**	**Адресная книга**	**Выбрать контакты**
Пункт меню **Подписать**	**Выбранным сертификатом**	**Другим сертификатом**
Флажок в окне **Настройка параметров безопасности** на вкладке **Администратор**	**Разрешить использование внешних сертификатов**	**Разрешить использование сертификатов из хранилища ОС**

- **Изменение требований к сертификатам, используемым при аутентификации**

  Раньше выполнения аутентификации с помощью сертификата необходимым условием являлось наличие назначения «Проверка подлинности клиента» в поле сертификата **Расширенное использование ключа**. Теперь для аутентификации вы можете использовать сертификат с назначением «Шифрование ключей» в поле **Использование ключа** (см. Особенности аутентификации с помощью сертификата на стр. 29).

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

Глоссарий

PKI (инфраструктура открытых ключей)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

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 аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

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.

Головной удостоверяющий центр

Удостоверяющий центр, который находится на вершине иерархической системы доверительных отношений между удостоверяющими центрами.

Дистрибутив ключей

Файл с расширением *.dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр 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.

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи 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).

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. Клиент должен быть зарегистрирован на координаторе. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключ проверки электронной подписи

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

Ключ электронной подписи

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

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Контейнер ключей

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

Корневой сертификат

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.

Открепленная подпись

Тип электронной подписи, при использовании которого электронная подпись и служебная информация помещаются в отдельный файл. Далее для проверки электронной подписи требуется не только данный контейнер, но и исходный файл, который в контейнер не входит.

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.

Прикрепленная подпись

Тип электронной подписи, при использовании которого исходный файл, электронная подпись и служебная информация помещаются совместно в один контейнер. Далее для проверки электронной подписи требуется только данный контейнер, который содержит и электронную подпись, и исходный файл.

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.

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии 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.

Сеансовый ключ

Случайный или производный ключ, предназначенный для шифрования одного сообщения.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

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

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

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).

Список аннулированных сертификатов (CRL)

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

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на сетевые узлы ViPNet транспортным модулем ViPNet MFTP.

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

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.

Электронная подпись

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

Указатель

А

Автопроцессинг - 118
  Журнал автопроцессинга - 133, 136
Администратор сетевого узла - 150
Адресная книга - 38, 47
Аннотация - 47, 56
Архив писем - 66, 68, 141
Аудит - 35, 65, 150
Аутентификация пользователя - 25, 152

В

Вложение - 47, 56, 126
Внешнее устройство - 25, 190
Внешние программы - 148

И

Извещение - 35, 50

К

Контейнер ключей - 73, 110, 206
Корневой сертификат - 206, 207
Криптопровайдер ViPNet CSP - 75, 161

П

Папки - 32, 35, 64
Печать - 53, 56, 147
Письмо - 45, 145
  Архивация писем - 66
  Атрибуты писем - 32
  Импорт писем - 63
  Поиск писем - 60
  Просмотр писем - 53, 56
  Создание писем - 46, 58
  Удаление писем - 65
  Экспорт писем - 62
Пользователь - 24, 25, 155, 206

Р

Регистрационный номер - 53, 145

С

Сертификат электронной подписи - 71, 172, 207
  Обновление сертификатов - 96, 104, 105
  Просмотр сертификатов - 85

Т

Транспортный модуль - 207, 208

Ф

Файл
  Автоматическая отправка файлов - 123
  Электронная подпись файлов - 79

Ш

Шаблон письма - 52
Шифрование - 83

Э

Электронная подпись - 17, 71, 72, 79, 208
    Подписание - 72, 73, 79
    Проверка подписи - 76, 80
    Удаление подписи - 77, 81