



ViPNet Client [Деловая почта] 3.1

Руководство пользователя

1991–2011 ОАО «Инфотекс», Москва, Россия

ФРКЕ.00004-04 34 03

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

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

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «Инфотекс».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «Инфотекс»

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

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

Сайт компании «Инфотекс»: <http://www.infotecs.ru>

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение.....	7
О документе	8
Для кого предназначен документ	8
Соглашения документа.....	8
О программе.....	9
Системные требования.....	10
Информация о внешних устройствах хранения данных.....	11
Обратная связь	14
Дополнительная информация	14
Контактная информация.....	14
Глава 1. Быстрый старт.....	15
Перед началом работы	16
Как написать письмо	17
Как подписать письмо цифровой подписью	18
Как прочитать письмо	19
Как ответить на письмо.....	20
Как перенести письмо в Microsoft Outlook	21
Как удалить письмо.....	22
Глава 2. Начало работы с программой ViPNet Client [Деловая почта].....	23
Запуск и завершение работы с программой.....	24
Смена пользователя	26
Смена каталога ключей пользователя	27
Конвертация ключей на внешнем устройстве	27
Режимы авторизации.....	30
Интерфейс программы	34
Работа с папками программы ViPNet Client [Деловая почта]	37
Специальные папки.....	37
Работа с пользовательскими папками	38
Адресная книга	41
Уровни адресации	41

Создание групп адресатов	42
Глава 3. Работа с письмами	44
Создание нового письма	45
Окно создания и просмотра писем	45
Создание письма.....	46
Запрос извещения о доставке и прочтении в виде отдельного письма.....	48
Отправка письма в виде вложения	49
Создание и использование шаблонов	51
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.....	63
Экспорт писем	63
Импорт писем	64
Перенос писем в другую папку	65
Удаление писем	66
Архивация писем	67
Работа с архивами писем	69
Глава 4. Цифровая подпись и шифрование.....	72
Цифровая подпись в программе «Деловая почта»	73
Работа с цифровой подписью писем.....	74
Подписание письма.....	74
Подписание выбранным сертификатом	76
Использование сертификата, изданного сторонним удостоверяющим центром	78
Проверка цифровой подписи письма	79
Удаление цифровой подписи письма	80
Работа с цифровой подписью файлов.....	82
Подписание файла.....	82
Отсоединение и присоединение подписи файла	83
Проверка цифровой подписи файла	84
Удаление цифровой подписи файла	85
Шифрование и расшифрование писем	86

Глава 5. Автопроцессинг	88
Принцип работы автопроцессинга.....	89
Настройка параметров автопроцессинга.....	92
Создание правила для исходящих файлов.....	93
Создание правила для входящих писем.....	96
Оптимизация работы автопроцессинга	101
Просмотр журнала автопроцессинга	102
Настройка параметров журнала автопроцессинга	106
Глава 6. Настройка программы	108
Общие настройки.....	109
Настройка архивации	111
Настройка параметров работы с письмами.....	114
Настройка транспортного модуля.....	116
Настройка печати.....	118
Настройка внешних программ	119
Работа в программе с правами администратора.....	121
Дополнительные настройки и возможности «Деловой почты».....	122
Дополнительные настройки параметров безопасности.....	123
Изменение режима авторизации пользователя	124
Глава 7. Настройка параметров безопасности	126
Смена пароля пользователя.....	127
Выбор собственного пароля.....	128
Выбор пароля на основе парольной фразы.....	129
Выбор цифрового пароля	130
Настройка параметров шифрования.....	131
Задание параметров шифрования с использованием асимметричных ключей.....	132
Просмотр журнала событий, связанных с асимметричными ключами	133
Настройка параметров работы криптопровайдера ViPNet CSP.....	135
Управление внешними устройствами хранения данных	137
Инициализация устройства	138
Смена ПИН-кода устройства	140
Глава 8. Работа с сертификатами	142
Общие сведения о сертификатах открытых ключей.....	143

Определение и назначение	143
Структура	143
Роль РКІ для криптографии с открытым ключом.....	146
Использование сертификатов для шифрования электронных документов	147
Зашифрование	147
Расшифрование	148
Использование сертификатов для подписания электронных документов.....	149
Подписание.....	149
Проверка подписи	150
Использование сертификатов для подписания и шифрования электронных документов.....	151
Подписание и зашифрование.....	151
Расшифрование и проверка.....	152
Просмотр сертификатов.....	154
Просмотр текущего сертификата пользователя	155
Просмотр личных сертификатов пользователя	155
Просмотр доверенных корневых сертификатов.....	156
Просмотр изданных сертификатов	156
Просмотр цепочки сертификации.....	157
Просмотр полей сертификата и печать сертификата	157
Установка сертификатов в хранилище	159
Установка в хранилище автоматически	159
Установка в хранилище вручную	160
Экспорт сертификата.....	164
Управление сертификатами.....	166
Смена текущего сертификата.....	166
Обновление сертификата.....	167
Ввод сертификатов в действие.....	175
Ввод в действие автоматически.....	175
Ввод в действие вручную	176
Работа с запросами на сертификаты.....	176
Просмотр запроса на сертификат	177
Удаление запроса на сертификат.....	178
Работа с контейнером закрытого ключа.....	179
Смена пароля к контейнеру.....	180
Удаление сохраненного пароля	182
Проверка контейнера	183

Удаление закрытого ключа	183
Установка нового и смена текущего контейнера	184
Перенос контейнера	185
Приложение А. Глоссарий.....	187
Приложение В. Указатель	193



Введение

О документе	8
О программе	9
Системные требования	10
Информация о внешних устройствах хранения данных	11
Обратная связь	14

О документе

Для кого предназначен документ

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

Соглашения документа

Соглашения данного документа представлены в таблице ниже.

Таблица 1. Условные обозначения

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

О программе

Программа ViPNet Client [Деловая почта] (или просто «Деловая почта») предназначена для организации электронного документооборота в защищенной сети ViPNet (см. «[Сеть ViPNet](#)»). С помощью «Деловой почты» пользователи сети ViPNet, у которых есть связь друг с другом, могут обмениваться электронными письмами.

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

«Деловая почта» обладает стандартными функциями почтового клиента:

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

«Деловая почта» также имеет ряд особенностей:

- Доступ к программе на сетевом узле ViPNet имеет только пользователь этого сетевого узла.
- Письма «Деловой почты» передаются по защищенным каналам в сети ViPNet с помощью транспортного модуля MFTR (см. «[Настройка транспортного модуля](#)» на стр. 116).
- Письма «Деловой почты» зашифрованы на ключах адресата (см. «[Уровни адресации](#)» на стр. 41) и не могут быть прочитаны кем-либо другим.
- «Деловая почта» имеет мощную систему автоматической обработки входящих писем и исходящих файлов (см. «[Автопроцессинг](#)» на стр. 88).

Системные требования

Минимальные требования к аппаратным средствам для установки ViPNet Client [Деловая почта]:

- Процессор – не менее Pentium IV;
- ОЗУ – не менее 512 Мбайт.
- Свободное место на жестком диске – не менее 100 Мбайт (рекомендуется 200 Мбайт).
- Internet Explorer версии 6.0 и выше.
- Операционная система – Windows 2000 SP4 (32 бит)/XP SP3 (32 бит)/Server 2003 (32 бит)/ Vista SP2 (32/64 бит)/Server 2008 (32/64 бит)/Windows 7 (32/64 бит)/Server 2008 R2 (64 бит);
- Наличие сетевого адаптера.

Информация о внешних устройствах хранения данных

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

Ниже в таблице перечислены устройства и ключи, с которыми может работать ПО ViPNet. Приведенная таблица содержит следующие данные:

- в колонке **Тип устройства** представлены все типы устройств считывания, доступные для выбора в ПО ViPNet;
- в колонке **Тип ключа** представлены типы ключей, используемые для данных устройств;
- в колонке **Необходимые условия работы с ключом** описаны необходимые условия и важные моменты для использования каждого ключа;
- в последней колонке содержится информация о поддержке стандарта PKCS#11.



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

Тип устройства	Тип ключа	Необходимые условия работы с ключом	Поддержка стандарта PKCS#11
eToken Aladdin	eToken PRO (персональные электронные ключи, eToken PRO (Java), eToken PRO, смарт-карты eToken PRO (Java), eToken PRO компании Aladdin)	<ul style="list-style-type: none">• На компьютере должно быть установлено программное обеспечение PKI Client версии 5.1 и выше.• Поддерживаемые ОС: Windows XP SP3 (32 бит), Server 2003 SP2 (32 бит), Vista SP2 (32/64 бит), Server 2008 (32/64 бит), Windows 7 (32/64 бит), Server 2008 R2.	Да

		<ul style="list-style-type: none"> • Замечание: Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым USB-устройством считывания с карт. 	
iButton	iButton (Dallas) (электронные ключи iButton типа DS1993, DS1994, DS1995 и DS1996)	<ul style="list-style-type: none"> • К компьютеру должно быть подключено устройство считывания. • На компьютере должно быть установлено программное обеспечение обмена информации с iButton, 1-Wire Drivers версии 3.6.2. • Поддерживаемые ОС: Windows XP SP3 (32 бит), Server 2003 (32 бит), Vista SP2 (32 бит), Server 2008 (32 бит), Windows 7 (32 бит). 	Нет
Smartcard Athena	Смарт-карты с памятью типа I2C (ASE M4), синхронные смарт-карты с шиной 2/3 и защищенной памятью, удовлетворяющие стандарту ISO7816-3 (ASE MP42)	<ul style="list-style-type: none"> • Чтение и запись на смарт-карту осуществляется через считыватель ASEDrive III PRO-S компании Athena. • На компьютере должны быть установлены драйверы версии 2.6. • Поддерживаемые ОС: Windows 2000 SP4 (32 бит), Windows XP SP3 (32 бит), Server 2003 (32 бит), Vista SP2 (32/64 бит). 	Нет
SmartCard RIK	Российская интеллектуальная карта компании Атлас-Телеком.	<ul style="list-style-type: none"> • Работа с картой ПО ViPNet может производиться через любой PS\CS-совместимый считыватель. 	Нет
Shipka	ПСКЗИ ШИПКА компании ОКБ САПР	<ul style="list-style-type: none"> • Перед началом работы с устройством ШИПКА убедитесь, что на АП установлено программное обеспечение ACShipka Environment версии не ниже 3.3.2.6. Поддерживаемые ОС: Windows XP SP3 (32 бит), Server 2003 (32 бит), Vista SP2 (32/64 бит), Server 2008 (32/64 бит). Проведите инициализацию устройства при помощи утилиты производителя «Параметры авторизации». 	Да
ruToken	Rutoken S , электронный идентификатор	<ul style="list-style-type: none"> • На компьютере должны быть установлены драйверы Rutoken версий не ниже используемых в 	

	компании Актив	установочном комплекте версии 2.25.03.0267.	
		<ul style="list-style-type: none"> Поддерживаемые ОС: Windows 2000 SP4 (32 бит), Windows XP SP3 (32 бит), Server 2003 (32 бит), Vista SP2 (32/64 бит), Server 2008 (32/64 бит), Windows 7 (32/64 бит). 	
ruTokenЕСР	Rutoken ЭЦП , электронный идентификатор компании Актив	<ul style="list-style-type: none"> На компьютере должны быть установлены драйверы версии не ниже 2.25.03.0267. Поддерживаемые ОС: Windows 2000 SP4 (32 бит), Windows XP SP3 (32 бит), Server 2003 (32 бит), Vista SP2 (32/64 бит), Server 2008 (32/64 бит), Windows 7 (32/64 бит). 	Да
Siemens CardOS (не поддерживает ПО VipNet CSP)	смарт-карты Siemens (CardOS/M4.01a, CardOS V4.3B, CardOS V4.2B, CardOS V4.2B DI, CardOS V4.2C, CardOS V4.4)	<ul style="list-style-type: none"> Для работы на компьютере должно быть установлено ПО Siemens CardOS API V5.0 или выше Поддерживаемые ОС: Windows XP SP3 (32 бит), Server 2003 EE SP2 (32 бит), Vista SP2 (32/64 бит), Server 2008 SP2 (32/64 бит), Windows 7 (32/64 бит). 	Да
Аккорд-5MX	iButton типа DS1993, DS1994, DS1995 и DS1996	<ul style="list-style-type: none"> На компьютере должен быть установлен драйвер версии не ниже 3.18.0.0. Поддерживаемые ОС: Windows 2000 SP4 (32 бит), Windows XP SP3 (32 бит), Server 2003 (32 бит), Vista SP2 (32 бит), Server 2008 (32 бит). 	Нет



Внимание! Хранение ключевой информации нескольких пользователей на одном устройстве невозможно. Однако хранение ключей подписи нескольких пользователей на одном устройстве возможно. Перед записью ключевой информации на устройство убедитесь, что устройство отформатировано.

Обратная связь

Дополнительная информация

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

- Описание комплекса ViPNet CUSTOM <http://www.infotecs.ru/products/line/custom.php>.
- Сборник часто задаваемых вопросов (FAQ) <http://www.infotecs.ru/support/faq/>.
- Законодательная база в сфере защиты информации <http://www.infotecs.ru/laws/>.
- Описание технологии ViPNet <http://www.infotecs.ru/solutions/vpn/>.

Контактная информация

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

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



1

Быстрый старт

Перед началом работы	16
Как написать письмо	17
Как подписать письмо цифровой подписью	18
Как прочитать письмо	19
Как ответить на письмо	20
Как перенести письмо в Microsoft Outlook	21
Как удалить письмо	22

Перед началом работы

Данная глава содержит краткие указания по использованию основных возможностей программы «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. 24). Об основных действиях с письмами можно узнать далее в данной главе. В случае каких-либо затруднений обратитесь к разделу [Работа с письмами](#) (на стр. 44).

Использование криптографических возможностей программы описано в главе [Цифровая подпись и шифрование](#) (на стр. 72), автоматическая обработка писем и файлов — в главе [Автопроцессинг](#) (на стр. 88).

Как написать письмо

Чтобы написать письмо, выполните следующие действия:

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

Подробнее см. раздел [Создание нового письма](#) (на стр. 45).

Как подписать письмо цифровой подписью

Чтобы подписать письмо цифровой подписью, выполните следующие действия:

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

Подробнее см. раздел [Подписание письма](#) (на стр. 74).

Как прочитать письмо

При получении новых писем транспортный модуль MFTR выдает соответствующее сообщение. Непрочитанные письма выделяются в списке полужирным шрифтом. Папки «Деловой почты», в которых есть непрочитанные письма, также выделяются полужирным шрифтом, при этом в скобках после имени папки указано количество непрочитанных писем.

Чтобы прочитать письмо:

- 1 В окне программы ViPNet Client [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 Client [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. 17).

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

Как перенести письмо в Microsoft Outlook

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

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

Подробнее см. раздел [Экспорт и импорт писем](#) (на стр. 63).

Как удалить письмо

Чтобы удалить письмо, выполните следующие действия:

- 1 В окне программы ViPNet Client [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 будет перемещено в папку **Удаленные**, в подпапку с именем, которое совпадает с именем исходной папки письма.

Подробнее см. [Удаление писем](#) (на стр. 66).



2

Начало работы с программой ViPNet Client [Деловая почта]

Запуск и завершение работы с программой	24
Режимы авторизации	30
Интерфейс программы	34
Работа с папками программы ViPNet Client [Деловая почта]	37
Адресная книга	41

Запуск и завершение работы с программой

Чтобы запустить программу ViPNet Client [Деловая почта], выполните следующие действия:

- 1 Для запуска ViPNet Client [Деловая почта] используйте один из следующих способов:
 - Если запущена программа ViPNet Client [Монитор], в строке состояния в окне программы нажмите кнопку . Немедленно будет открыто окно программы ViPNet Client [Деловая почта]. Авторизация пользователя в этом случае не требуется.
 - Когда транспортный модуль MFTR получает новые почтовые конверты, он выдает уведомление о получении писем.

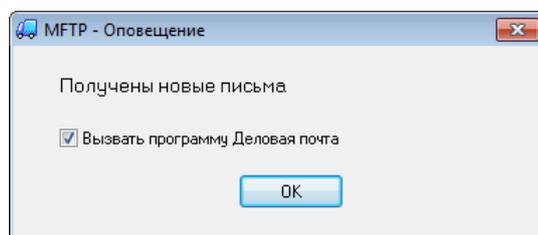


Рисунок 1: Уведомление о получении новых писем



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

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

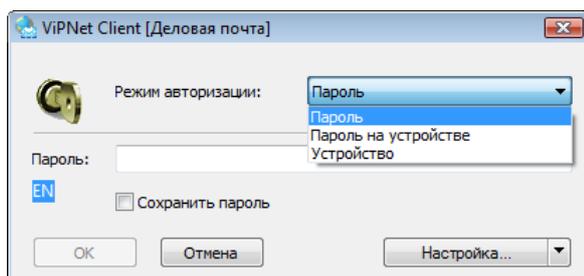


Рисунок 2: Окно входа в программу

- Чтобы запустить программу «Деловая почта» с помощью ярлыка, выполните одно из действий:
 - В меню **Пуск** выберите пункт **Программы**, затем **ViPNet**, затем **Client** и щелкните **ViPNet Деловая почта** (при установке путь к программе в меню **Пуск** мог быть изменен).
 - Дважды щелкните значок  на Рабочем столе (этот значок отображается, только если при установке программы была выбрана соответствующая опция).

Откроется окно входа в программу.

2 В окне входа в программу выполните следующие действия:

- 2.1** В зависимости от текущего режима авторизации, для входа в программу введите пароль пользователя либо подключите внешнее устройство хранения данных и введите ПИН-код.



Внимание! Если ПО ViPNet Client было обновлено с версии 3.0.x до текущей версии и до обновления использовался режим авторизации **Пароль на устройстве** или **Устройство**, то хранящиеся на внешнем устройстве ключи необходимо конвертировать в новый формат. При попытке войти в «Деловую почту» с помощью устройства, на котором хранятся ключи старого формата, будет автоматически запущена программа конвертации ключей (см. [«Конвертация ключей на внешнем устройстве»](#) на стр. 27).

Если по каким-либо причинам изменилось местонахождение каталога ключей пользователя, для успешной авторизации требуется указать путь к этому каталогу (см. [«Смена каталога ключей пользователя»](#) на стр. 27).

2.2 После ввода необходимых для авторизации данных нажмите **ОК**. Откроется окно программы ViPNet Client [Деловая почта].

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

Чтобы завершить работу с программой, выполните одно из действий:

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



Примечание. Если в окне **Настройка** в разделе **Общие** (см. «[Общие настройки](#)» на стр. 109) установлен флажок **По кнопке «Заккрыть» сворачивать окно почты в «трей»**, при нажатии на кнопку **Заккрыть**  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 Client [Деловая почта]. Для этого выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] в меню **Инструменты** выберите пункт **Смена пользователя**. Откроется окно входа в программу (см. Рисунок 2 на стр. 25).
- 2 Введите пароль пользователя, от имени которого требуется войти в программу, и нажмите **ОК**.



Примечание. На сетевом узле должна быть инициализирована справочно-ключевая информация пользователя, от имени которого выполняется вход в программу.

Смена каталога ключей пользователя

Чтобы изменить каталог ключей пользователя (см. «Папка (каталог) ключей пользователя»), выполните следующие действия:

- 1 Запустите программу ViPNet Client [Деловая почта] из меню **Пуск** или дважды щелкните ярлык программы на Рабочем столе (этот значок отображается, только если при установке программы была выбрана соответствующая опция).
- 2 В окне ввода пароля (см. рисунок на стр. **Error! Bookmark not defined.**) щелкните значок  справа от кнопки **Настройка** и в меню выберите пункт **Каталог ключей пользователя**.
- 3 В окне **Просмотр каталогов** укажите путь к каталогу ключей.



Примечание. Смена каталога ключей может понадобиться при входе в программу от имени нового пользователя.

Конвертация ключей на внешнем устройстве

Конвертер ключей ViPNet запускается автоматически в случае, когда требуется преобразование ключей ViPNet, хранящихся на внешних устройствах в старом формате, в новый формат.

Чтобы преобразовать ключи, хранящиеся на внешних устройствах в старом формате, в новый формат, выполните следующие действия:

- 1 В окне **Конвертер ключей ViPNet**, в списке **Устройство** выберите внешнее устройство хранения данных, на котором хранятся ключи в старом формате. Если список пуст, значит устройство не подключено либо для него неправильно установлены драйверы.
- 2 В поле **Введите ПИН-код** укажите ПИН-код выбранного внешнего устройства хранения данных.

- 3 Далее в списке **Ключи ViPNet на устройстве** напротив каждого из ключей в старом формате в столбце **Действие** выберите **Конвертировать**.

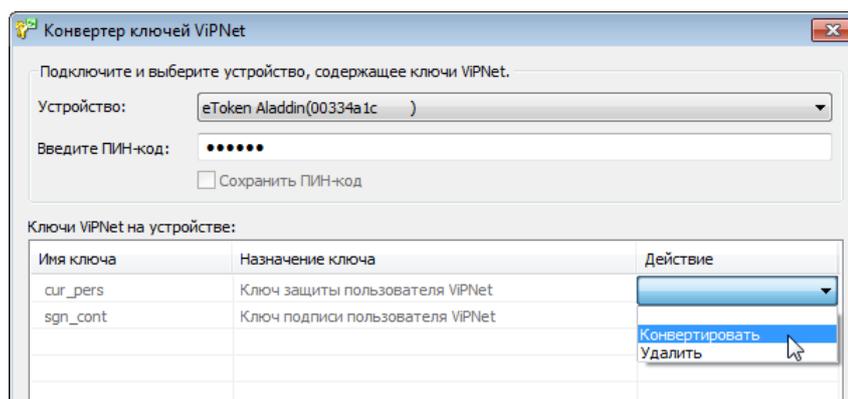


Рисунок 3: Выбор действия **Конвертировать** для ключей старого формата

- 4 Введите пароль доступа к ключу.

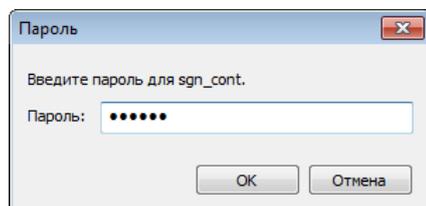


Рисунок 4: Окно ввода пароля

Если на устройстве уже имеется ключ с тем же именем и в новом формате, появится предупреждение об этом.

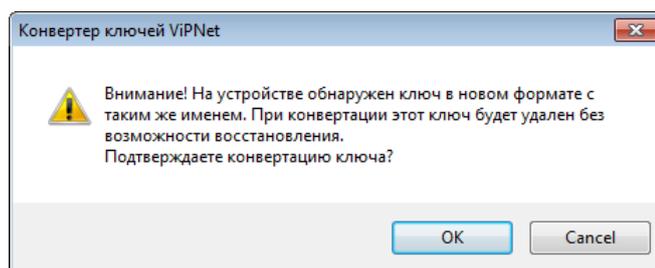


Рисунок 5: Предупреждение о совпадении имен ключей



Внимание! Если на устройстве уже имеется ключ в новом формате с точно таким же именем, что и ключ в старом формате, то при конвертации старого ключа ключ в новом формате будет удален без возможности восстановления.

Конвертирование осуществляется для всех ключей, хранящихся на устройстве. Ключи, которые не будут конвертированы в новый формат, будут удалены.

5 Нажмите кнопку **Конвертировать**.



Внимание! Если в процессе конвертации ключей в новый формат произошел сбой, есть возможность продолжить процесс конвертации. Для этого повторно запустите **Конвертер ключей ViPNet**. Нажмите кнопку **Да** в ответ на вопрос, хотите ли вы продолжить выполнение оставшихся действий.

Режимы авторизации

В программе «Деловая почта» предусмотрено три режима авторизации пользователя: **Пароль, Пароль на устройстве, Устройство**.

По умолчанию установлен режим авторизации **Пароль**. Администратор сетевого узла может изменить режим авторизации (см. «[Изменение режима авторизации пользователя](#)» на стр. 124) на вкладке **Ключи** в окне **Настройка параметров безопасности**.

В режимах **Пароль на устройстве** и **Устройство** авторизация осуществляется с помощью внешних устройств хранения данных (см. «[Информация о внешних устройствах хранения данных](#)» на стр. 11). Чтобы использовать какое-либо устройство для авторизации пользователя, нужно записать на это устройство необходимую ключевую информацию, а на компьютер нужно установить драйверы устройства. Записать ключевую информацию на внешнее устройство можно при изменении режима авторизации пользователя (см. «[Изменение режима авторизации пользователя](#)» на стр. 124) или в программе УКЦ при создании ключевого дистрибутива (в программе ViPNet Manager работа с внешними устройствами невозможна).

В зависимости от текущего режима авторизации для входа в программу «Деловая почта» выполните следующие действия:

1 Пароль.

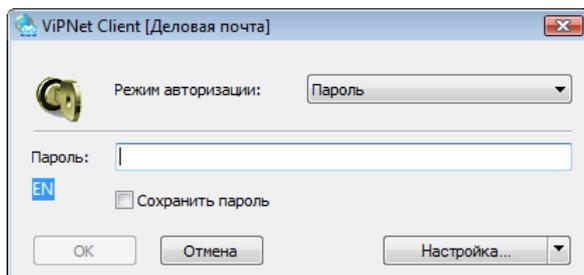


Рисунок 6: Режим авторизации «Пароль»

Для входа в программу:

1.1 В поле **Пароль** введите пароль пользователя сетевого узла.

Если сохранение пароля в реестре разрешено настройками программы (см. «[Дополнительные настройки параметров безопасности](#)» на стр. 123), для сохранения пароля можно установить соответствующий флажок.

1.1 Нажмите кнопку **ОК**.

2 Пароль на устройстве — в этом режиме для авторизации используется внешнее устройство хранения данных.

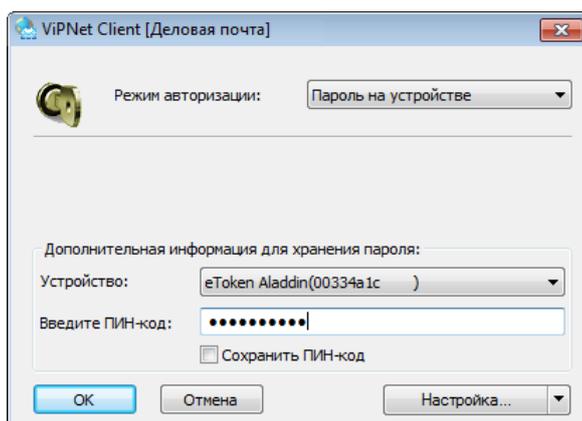


Рисунок 7: Режим авторизации «Пароль на устройстве»

Для входа в программу:

- 2.1** Подключите внешнее устройство хранения данных.
- 2.2** В списке **Устройство** выберите внешнее устройство хранения данных, на котором был сохранен парольный ключ пользователя.
- 2.3** Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства хранения данных (см. Рисунок 9 на стр. 33).
Чтобы сохранить ПИН-код и в дальнейшем не вводить его при авторизации, установите соответствующий флажок.
- 2.4** Нажмите кнопку **ОК**.

При использовании данного режима авторизации возможен вход в систему без использования внешнего устройства, посредством ввода пароля. Для этого в списке **Режим авторизации** выберите **Пароль**.

Такая особенность обеспечивает возможность входа в программу в случае потери или поломки внешнего устройства, но сохраняет возможность не сообщать пароль пользователю в целях обеспечения безопасности.



Внимание! Потерю устройства необходимо расценивать как компрометацию ключей пользователя.

- 3 Устройство** — в этом режиме для авторизации используются внешнее устройство и пароль пользователя ViPNet.

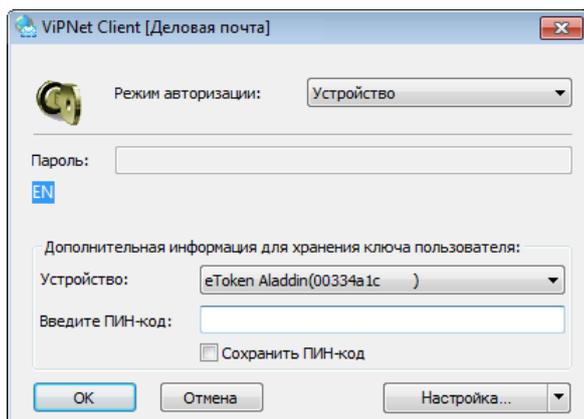
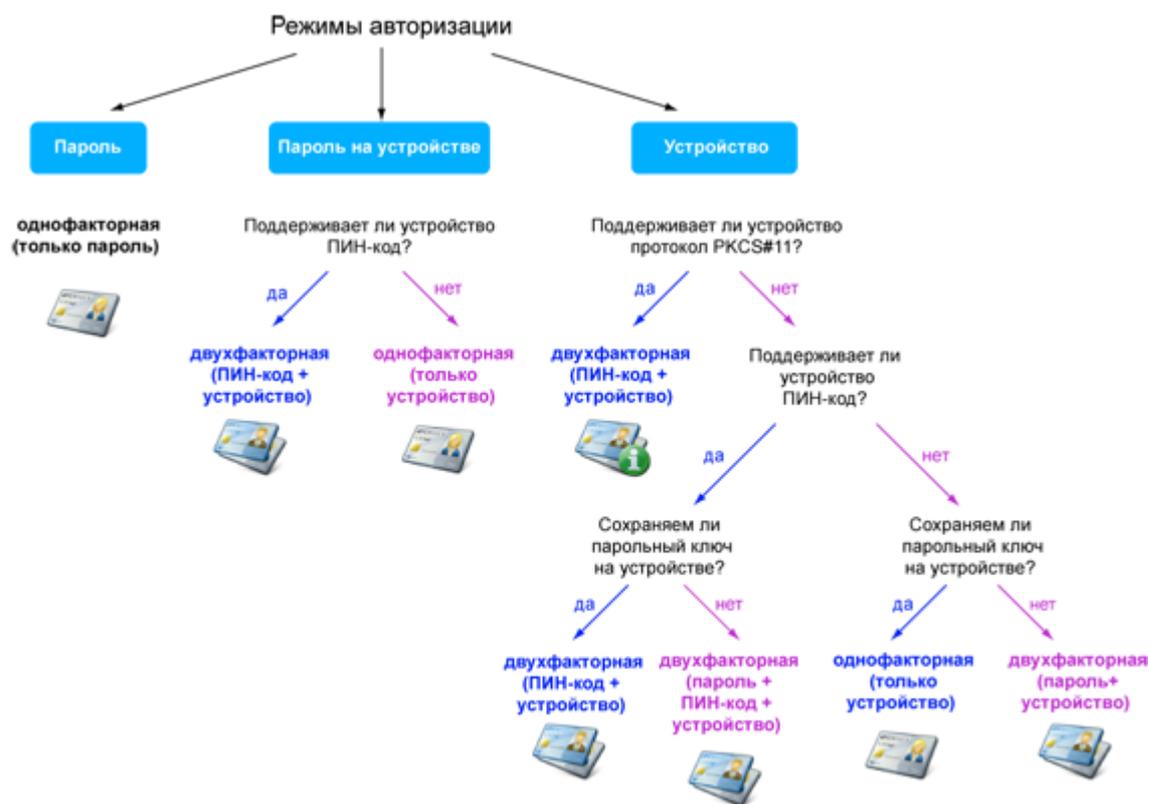


Рисунок 8: Режим авторизации «Устройство»

Для входа в программу:

- 3.1** Подключите внешнее устройство хранения данных
- 3.2** Если требуется, в поле **Пароль** введите пароль пользователя сетевого узла. Необходимость ввода пароля зависит от типа используемого внешнего устройства хранения данных (см. Рисунок 9 на стр. 33).
- 3.3** В списке **Устройство** выберите внешнее устройство хранения данных, на котором была сохранена личная ключевая информация пользователя.
- 3.4** Если требуется, введите ПИН-код. Чтобы сохранить ПИН-код и в дальнейшем не вводить его при авторизации, установите соответствующий флажок.
- 3.5** Нажмите кнопку **ОК**.

На схеме ниже представлены факторы авторизации, используемые в каждом режиме в зависимости от типа используемого внешнего устройства.



 В данном режиме авторизации личная ключевая информация пользователя защищается ПИН-кодом внешнего устройства хранения данных. Во всех остальных режимах личная ключевая информация защищается парольным ключом.

Рисунок 9: Схема соответствия между факторами и режимами авторизации



Примечание. Если на компьютере одновременно установлены ViPNet Client [Монитор] и ViPNet Client [Деловая почта], то в этих программах всегда используется один и тот же режим авторизации. Если изменить режим авторизации в программе ViPNet Client [Монитор], также изменится режим авторизации в программе ViPNet Client [Деловая почта], и наоборот.

Интерфейс программы

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

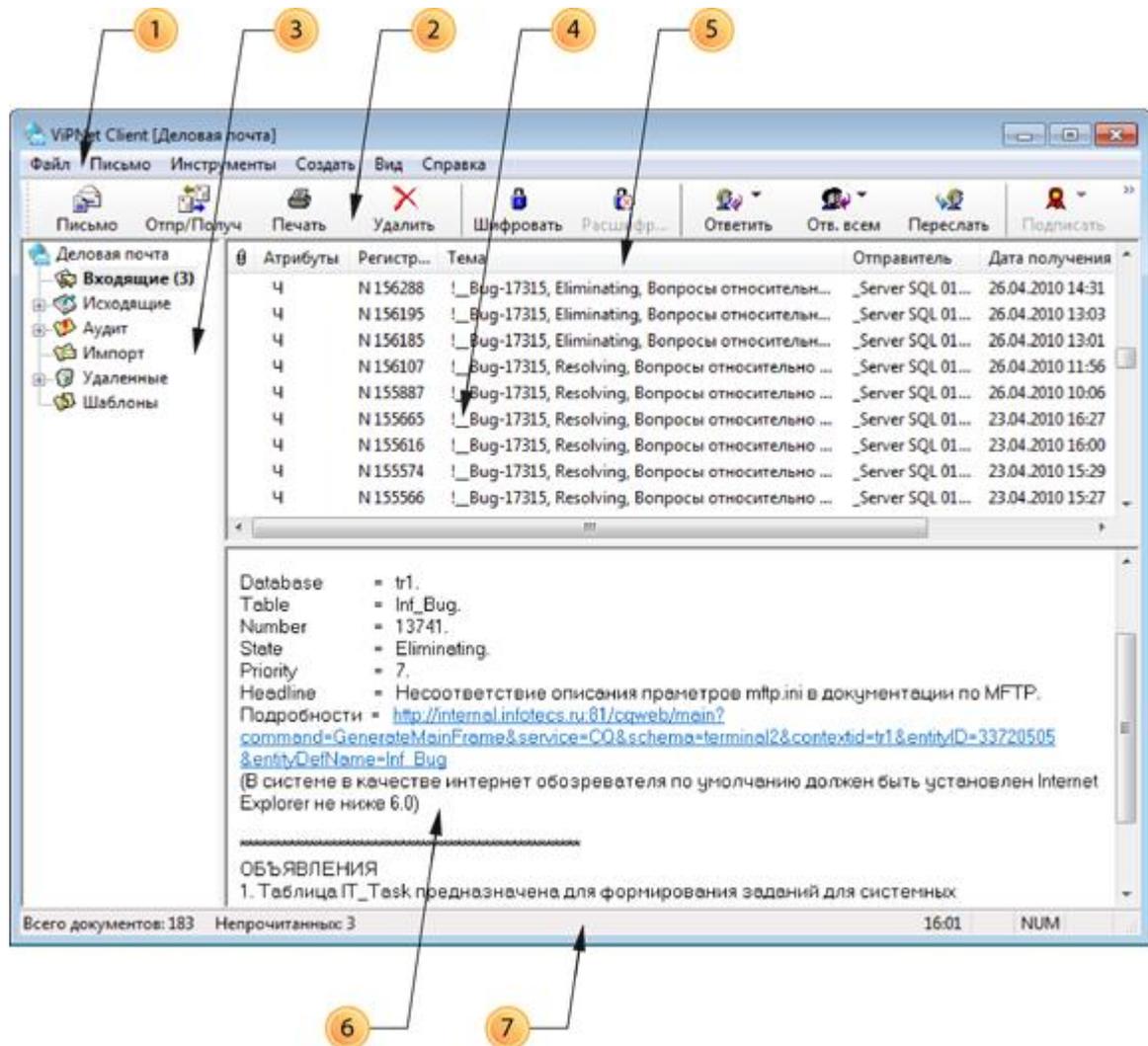


Рисунок 10: Интерфейс программы ViPNet Client [Деловая почта]

Цифрами на рисунке обозначены:

- 1 Главное меню программы «Деловая почта».

- 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 «Деловая почта».

Если в папке или ее подпапках есть непочитанные письма, количество таких писем указано после имени папки в скобках.
- 4 Панель писем. На этой панели отображается список писем, находящихся в выбранной на панели (3) папке.
- 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 **Атрибут** отображаются коды статуса письма. Описание кодов статуса представлено в следующей таблице:

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 абонентский пункт, на который отправлено письмо, отключен от сервера-маршрутизатора или удален из сети.



Примечание. Текст письма считается прочитанным, если письмо было открыто в отдельном окне. Вложение считается прочитанным, если оно было просмотрено.

Кроме того, после ответа на письмо текст этого письма считается прочитанным. При пересылке письма 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, а также количество непрочитанных (в папке **Входящие**) или неотправленных (в папке **Исходящие**) писем.

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

Работа с папками программы ViPNet Client [Деловая почта]

Хранение писем в программе «Деловая почта» можно упорядочить с помощью иерархической структуры папок. Папки отображаются на левой панели окна программы (см. [«Интерфейс программы»](#) на стр. 34).

Папки в «Деловой почте» делятся на две категории:

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

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

Специальные папки

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

- **Входящие** — папка, в которую по умолчанию помещаются входящие письма (см. [«Просмотр письма и вложений в отдельном окне»](#) на стр. 56).
- **Входящие > Извещения** — папка, в которую помещаются извещения о доставке и прочтении в виде отдельных писем (см. [«Запрос извещения о доставке и прочтении в виде отдельного письма»](#) на стр. 48).

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

- **Исходящие** — папка, в которую помещаются создаваемые письма (см. [«Создание нового письма»](#) на стр. 45).
- **Исходящие > Извещения** — папка, в которую помещаются извещения, отправляемые в виде отдельных писем.

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

- **Удаленные** — папка, в которую помещаются удаленные письма (см. «[Удаление писем](#)» на стр. 66).

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. 121).

- **Шаблоны** — папка, в которую помещаются шаблоны писем (см. «[Создание и использование шаблонов](#)» на стр. 51).
- **Импорт** — папка, в которую помещаются импортированные письма (см. «[Экспорт и импорт писем](#)» на стр. 63).

Работа с пользовательскими папками

При работе с пользовательскими папками возможны следующие действия:

1 Создание папки. Для создания папки:

1.1 На панели папок (см. «[Интерфейс программы](#)» на стр. 34) 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**.

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



Примечание. В одной папке нельзя создать две подпапки с одинаковыми именами. В папках **Удаленные** и **Аудит** (см. «[Специальные папки](#)» на стр. 37) создание новых папок невозможно.

2 Переименование папки. Чтобы переименовать папку:

2.1 На панели папок (см. «[Интерфейс программы](#)» на стр. 34) выберите папку, внутри которой требуется переименовать папку, и выполните одно из действий:

- Щелкните имя папки.
- Щелкните папку правой кнопкой мыши и в контекстном меню выберите пункт **Переименовать папку**.

На месте имени папки появится поле ввода.

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



Примечание. В одной папке нельзя создать две подпапки с одинаковыми именами. Невозможно переименовать специальные папки (см. «[Специальные папки](#)» на стр. 37).

3 Перенос папки. 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**.

4 Очистка содержимого папки. Для этого:

4.1 Щелкните папку правой кнопкой мыши и в контекстном меню выберите пункт **Очистить содержимое папки**.

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

Все письма из папки будут удалены (см. «[Удаление писем](#)» на стр. 66).

5 Удаление папки. Чтобы удалить папку:

5.1 Выберите папку, которую требуется удалить, и выполните одно из действий:

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

5.2 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 будет 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. 121).

Адресная книга

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

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

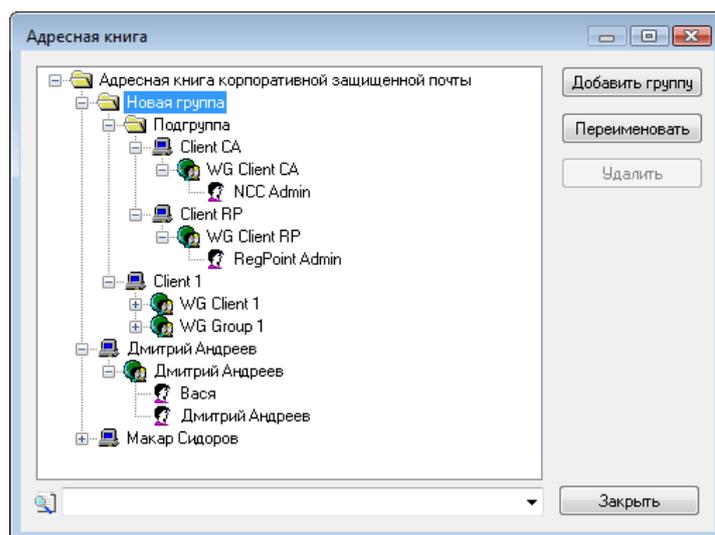


Рисунок 11: Адресная книга «Деловой почты»

Адресная книга используется для выбора адресатов при создании писем (см. «[Создание нового письма](#)» на стр. 45). Письмо можно адресовать сетевому узлу, типу коллектива или пользователю сети ViPNet. Таким образом, в программе «Деловая почта» существует три уровня адресации (см. «[Уровни адресации](#)» на стр. 41).

Для удобства абонентские пункты в адресной книге можно распределить по группам (см. «[Создание групп адресатов](#)» на стр. 42).

Уровни адресации

Каждому абонентскому пункту, с которым связан данный абонентский пункт, в адресной книге «Деловой почты» (см. Рисунок 11 на стр. 41) соответствует три уровня адресации:

- 1 Абонентский пункт. Данный уровень адресации соответствует всем пользователям абонентского пункта. То есть зашифрованное письмо, адресованное абонентскому пункту, могут прочитать все его пользователи.
- 2 Коллектив. Данный уровень адресации соответствует одному из коллективов пользователей, зарегистрированных на абонентском пункте (в сетях ViPNet CUSTOM на одном абонентском пункте может быть несколько коллективов). Зашифрованное письмо, адресованное коллективу, могут прочитать только члены этого коллектива.
- 3 Пользователь. Данный уровень соответствует конкретному пользователю абонентского пункта. Письмо, адресованное пользователю, могут прочесть все члены коллектива этого пользователя. Таким образом, этот уровень адресации не может использоваться для разграничения доступа к зашифрованным письмам, а служит только для определения адресата.



Примечание. Если пользователь является единственным членом своего коллектива и его имя совпадает с именем коллектива, то в адресной книге «Деловой почты» отображается только коллектив, а пользователь не отображается.

Создание групп адресатов

По умолчанию в адресной книге «Деловой почты» присутствует одна группа, которая называется **Адресная книга корпоративной защищенной почты**. Эту группу нельзя переименовать или удалить.

Чтобы создать новую группу, выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] в меню **Инструменты** выберите пункт **Адресная книга** либо в окне создания письма (см. «[Создание нового письма](#)» на стр. 45) нажмите кнопку **Получатели** .
- 2 В окне **Адресная книга** (см. Рисунок 11 на стр. 41) выберите группу абонентских пунктов, в которой требуется создать новую группу.
- 3 Нажмите кнопку **Добавить группу**. В адресной книге появится папка и поле для ввода имени группы.
- 4 Введите имя для созданной группы и нажмите клавишу **Enter**.
- 5 Чтобы перенести в новую группу абонентский пункт, щелкните этот абонентский пункт, его коллектив или пользователя мышью и перетащите в группу.

Чтобы переименовать группу:

- 1 Выберите группу в окне **Адресная книга**.
- 2 Нажмите кнопку **Переименовать**. На месте имени группы появится поле ввода.
- 3 Введите новое имя группы и нажмите клавишу **Enter** или щелкните мышью за пределами поля ввода.

Чтобы удалить группу:

- 1 Если в группе есть абонентские пункты, перенесите их в другие группы.
- 2 Выберите группу в списке.
- 3 Нажмите кнопку **Удалить**.



3

Работа с письмами

Создание нового письма	45
Создание и использование шаблонов	51
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	63
Перенос писем в другую папку	65
Удаление писем	66
Архивация писем	67
Работа с архивами писем	69

Создание нового письма

Окно создания и просмотра писем

Внешний вид окна, в котором осуществляется создание новых писем (см. «[Создание письма](#)» на стр. 46) и просмотр отправленных и полученных писем (см. «[Просмотр письма и вложений в отдельном окне](#)» на стр. 56), представлен на следующем рисунке:

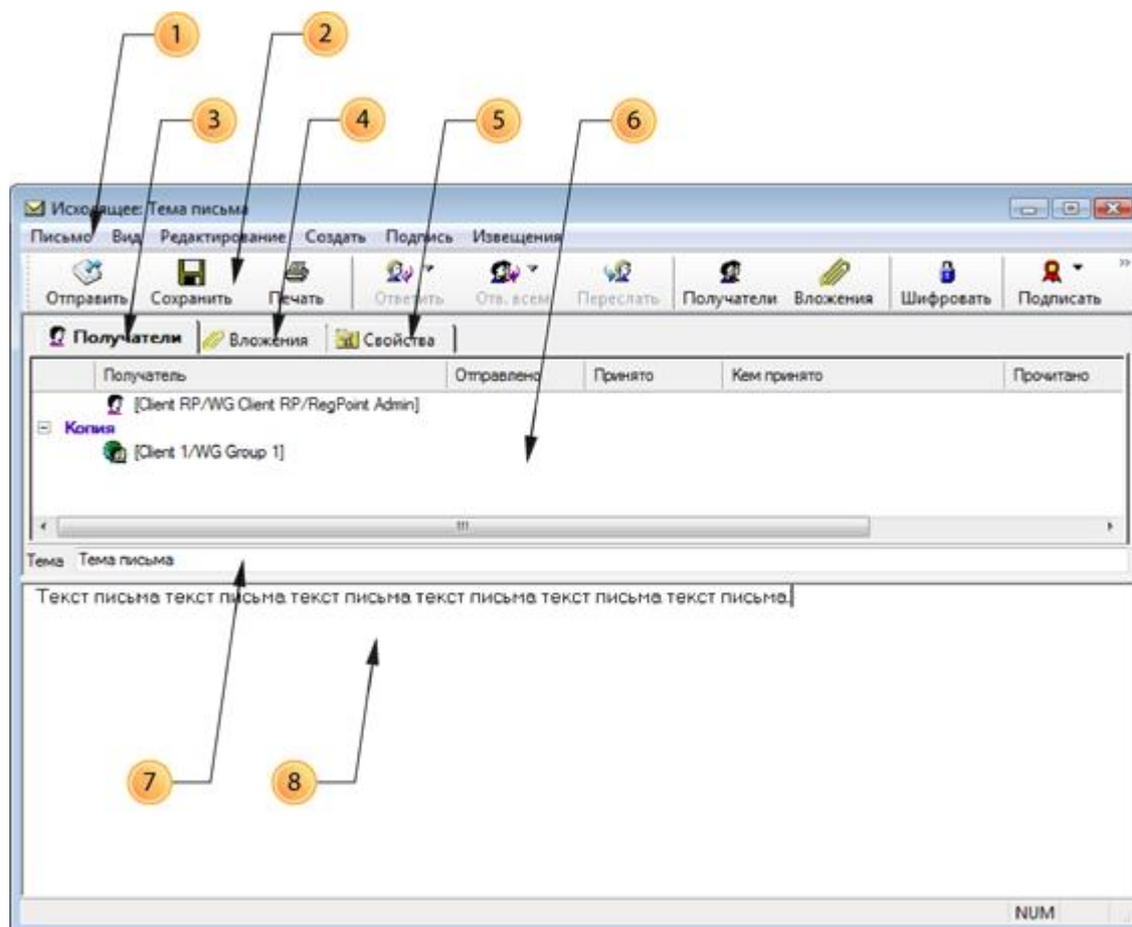


Рисунок 12: Интерфейс окна создания и просмотра писем

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 цифровой подписи (если она есть).
- 6 Панель, предназначенная для отображения содержимого вкладок **Получатели**, **Вложения** и **Свойства**.
- 7 Поле **Тема**. В этом поле отображается тема письма.
- 8 Панель, на которой отображается текст письма.

Создание письма

Чтобы написать письмо, выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] на панели инструментов нажмите кнопку **Письмо** . Откроется окно создания письма (см. «[Окно создания и просмотра писем](#)» на стр. 45).
- 2 В поле **Тема** введите тему письма.
- 3 На нижней панели окна введите текст письма.
- 4 Если в письмо требуется добавить вложения:
 - Выполните одно из действий:
 - Перетащите файлы в окно создания письма.
 - Нажмите кнопку **Вложения**  на панели инструментов. В окне **Открыть** выберите один или несколько файлов.
Для каждого файла будет открыто окно **Введите имя вложения**.
 - Чтобы добавить все файлы, сохранив их имена, нажмите кнопку **Добавить все**. Чтобы изменить имена файлов, для каждого файла введите имя и нажмите кнопку **Добавить**.
Выбранные файлы будут добавлены в письмо.

Чтобы удалить вложения из письма:

- В окне создания письма откройте вкладку **Вложения**.
 - Выберите вложение, которое нужно удалить, и нажмите клавишу **Delete**.
- 5** Если необходимо зашифровать письмо, на панели инструментов нажмите кнопку **Шифровать** . Если необходимо подписать письмо цифровой подписью, нажмите кнопку **Подписать** . Подробнее об использовании шифрования и цифровой подписи см. раздел [Цифровая подпись и шифрование](#) (на стр. 72).
- 6** Чтобы указать получателей письма:
- На панели инструментов нажмите кнопку **Получатели** . Откроется окно адресной книги (см. «[Адресная книга](#)» на стр. 41).

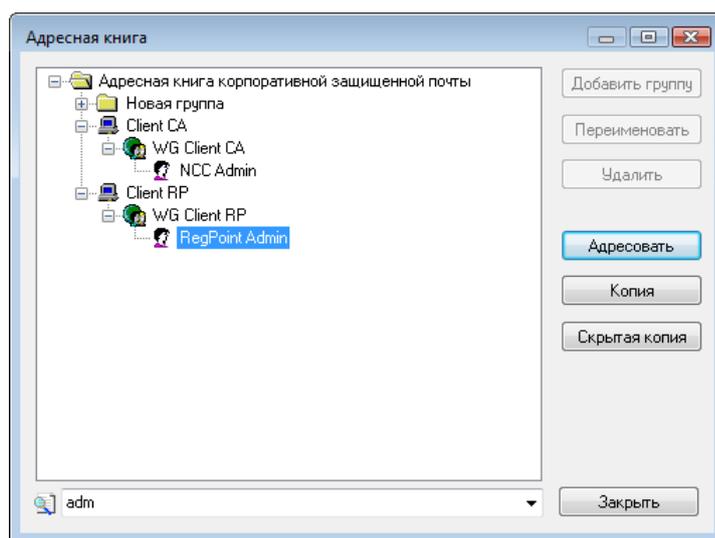


Рисунок 13: Выбор адресатов

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

Выбрав одного или несколько получателей, выполните одно из действий:

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

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

Чтобы удалить получателя, выберите его на вкладке **Получатели** (см. «[Окно создания и просмотра писем](#)» на стр. 45) и нажмите клавишу **Delete**.

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

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

- 8 Закончив создание нового письма, выполните одно из действий:

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



Примечание. Статус отправленного письма можно посмотреть в папке **Исходящие** в столбце **Атрибуты** (см. «[Интерфейс программы](#)» на стр. 34). Также можно запросить извещение о доставке и прочтении письма (см. «[Запрос извещения о доставке и прочтении в виде отдельного письма](#)» на стр. 48).

Запрос извещения о доставке и прочтении в виде отдельного письма

При отправке письма «Деловой почты» можно запросить извещение о доставке и прочтении письма. Чтобы запросить извещение:

- 1 Выполните действия, описанные в разделе [Создание письма](#) (на стр. 46).
- 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 «Деловой почты». 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 «Деловая почта» на абонентском пункте получателя исходящие извещения помещаются в папку **Исходящие > Извещения**, на абонентском пункте 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 цифровой подписи отправителя.
- Регистрационный номер письма.
- Результаты проверки цифровых подписей для подписанного текста письма и каждого из подписанных вложений.
- Контрольные суммы цифровых подписей для подписанного текста письма и каждого из подписанных вложений.

Отправка письма в виде вложения

Чтобы отправить письмо «Деловой почты» в виде вложения, выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) на левой панели выберите папку с письмами, которые требуется отправить в виде вложений.
- 2 На панели писем выберите одно или несколько писем.
- 3 Выполните одно из действий:
 - Щелкните письма правой кнопкой мыши и в контекстном меню выберите пункт **Переслать как вложения**.
 - В меню **Письмо** выберите пункт **Переслать как вложения**.

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

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

Выбранные письма будут добавлены в виде вложений.

- 5 Завершите создание письма и отправьте его, как описано в разделе [Создание письма](#) (на стр. 46).

Создание и использование шаблонов

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

1 Создать шаблон на основе существующего письма. Для этого выполните следующие действия:

1.1 Выберите письмо, на основе которого требуется создать шаблон.

1.1 Перенесите письмо (см. «[Перенос писем в другую папку](#)» на стр. 65) 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, цифровой подписи и атрибутов отправки, получения и прочтения. В качестве отправителя будет указан пользователь, создавший шаблон.

2 Создать новый шаблон. Для этого выполните следующие действия:

2.1 В окне программы «Деловая почта» в меню **Создать** выберите пункт **Новый шаблон**.

2.2 Откроется окно **Шаблон**, аналогичное окну создания письма (см. «[Окно создания и просмотра писем](#)» на стр. 45).

2.3 Введите текст и тему письма, укажите получателей и задайте другие параметры, как описано в разделе [Создание письма](#) (на стр. 46).

2.4 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 «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. 46) и отправьте его.

Просмотр письма и его свойств в основном окне программы

Чтобы просмотреть письмо:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) на левой панели выберите папку с письмом, которое требуется прочесть.



Примечание. Если в папке или ее подпапках есть непрочитанные письма, имя папки выделено полужирным шрифтом. Количество непрочитанных писем указано рядом с именем папки в скобках.

Непрочитанные письма, находящиеся в выбранной папке, выделены на панели писем полужирным шрифтом.

- 2 На панели писем выберите нужное письмо.

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

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

- Нажмите кнопку **Расшифровать**  на панели инструментов. Текст письма отобразится на панели чтения. Если письмо не прочитано, после этого оно не считается прочитанным.
 - Откройте письмо в отдельном окне (см. «[Просмотр письма и вложений в отдельном окне](#)» на стр. 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 **Атрибуты** появится атрибут **Ч** (см. «[Интерфейс программы](#)» на стр. 34).

- 2 Чтобы пометить прочитанное письмо как непрочитанное, щелкните письмо правой кнопкой мыши и в контекстном меню выберите пункт **Пометить как непрочтенные**. При этом атрибуты письма не изменятся.
- 3 Для неотправленного письма можно изменить регистрационный номер (см. «[Настройка параметров работы с письмами](#)» на стр. 114). 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**.

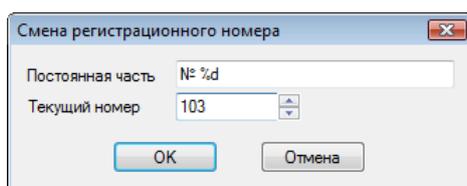


Рисунок 14: Изменение регистрационного номера

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

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. 114). 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**.

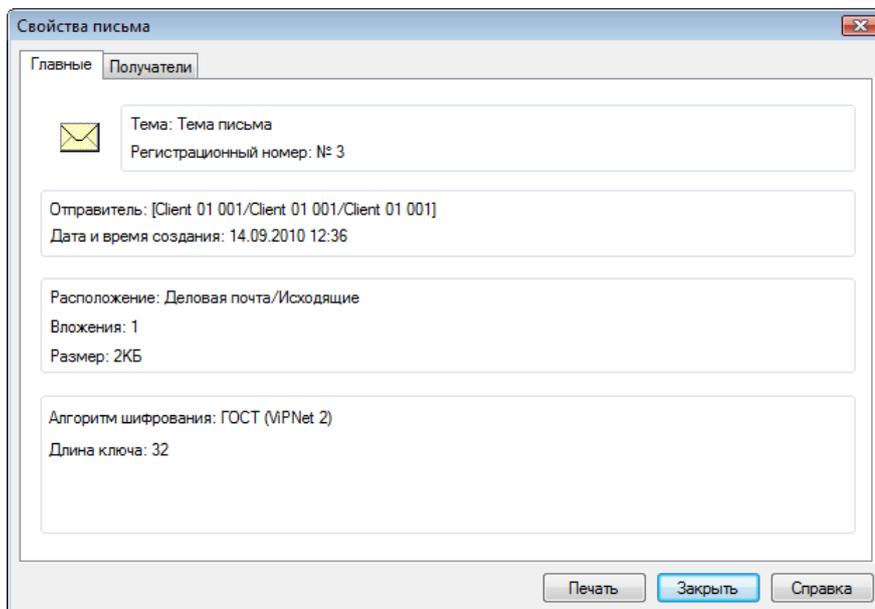


Рисунок 15: Свойства письма

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

Просмотр письма и вложений в отдельном окне

Чтобы просмотреть письмо в отдельном окне:

- 1 На панели писем дважды щелкните нужное письмо либо выберите письмо и нажмите клавишу **Enter**. Откроется окно просмотра письма (см. «[Окно создания и просмотра писем](#)» на стр. 45). Текст письма отобразится на нижней панели окна. При этом непрочитанное письмо станет прочитанным.

Если открыто исходящее письмо, которое еще не отправлено и не подписано цифровой подписью, его можно редактировать (см. «[Создание письма](#)» на стр. 46).



Примечание. Чтобы редактировать неотправленное письмо, подписанное цифровой подписью, удалите цифровую подпись (см. «[Удаление цифровой подписи письма](#)» на стр. 80).

- 2 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**.
- 3 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 **ОК**, вложение будет открыто в отдельном окне.



Примечание. Изменения, внесенные в открытое вложение, невозможно сохранить.

- Если письмо не отправлено и вложение не подписано цифровой 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.
 - Чтобы скопировать вложение для вставки в другое письмо «Деловой почты», 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 **Просмотр каталогов** 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**.
- 4** Чтобы распечатать текст письма, нажмите кнопку **Печать**  на панели инструментов.

Ответ на письмо и пересылка письма

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

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) 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. 45).
- 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 «Деловой почты» или на панели инструментов окна просмотра писем нажмите кнопку **Ответить автору** , 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 «Деловой почты» или на панели инструментов окна просмотра писем нажмите кнопку **Ответить 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 «Деловой почты» 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. 46).

Поиск писем

Для поиска писем «Деловой почты» выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «Интерфейс программы» на стр. 34) в меню **Инструменты** выберите пункт **Поиск документа**. Откроется окно **Поиск документа**.

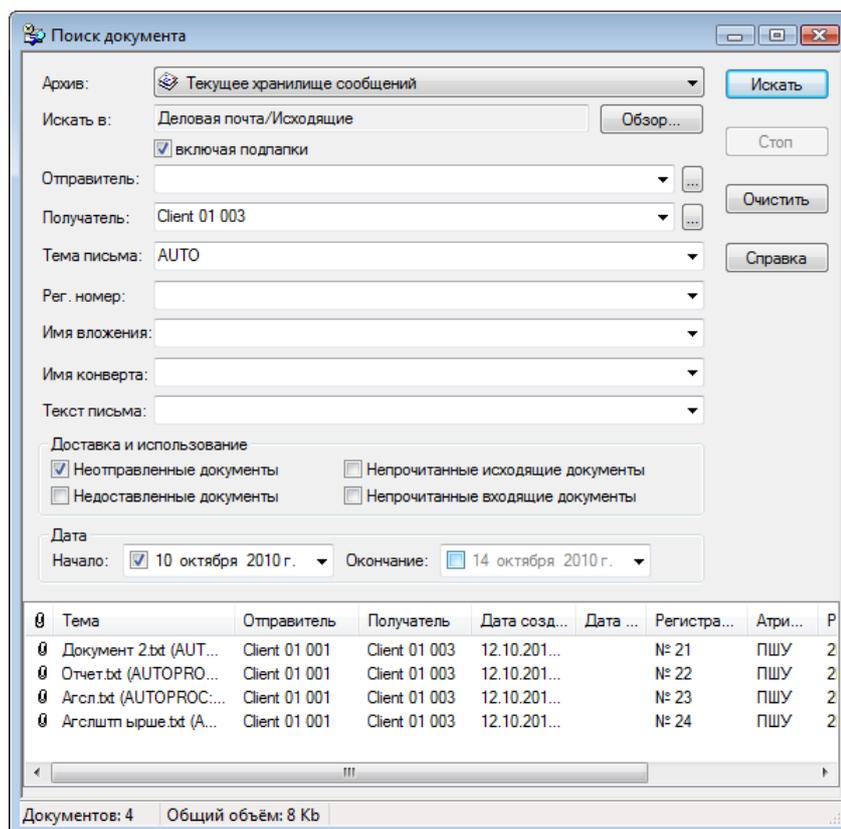


Рисунок 16: Окно поиска писем

- 2 Из списка **Архив** выберите хранилище сообщений или архив, в котором требуется найти письма.
- 3 Нажмите кнопку **Обзор** рядом с полем **Искать в** и в окне **Укажите папку** выберите папку, в которой требуется найти письма.
- 4 Для поиска писем в выбранной папке и ее подпапках установите флажок **включая подпапки**.

- 5 Чтобы указать отправителя писем, которые требуется найти, нажмите кнопку  рядом с полем **Отправитель** и в адресной книге (см. «[Адресная книга](#)» на стр. 41) выберите нужного отправителя.
- 6 Чтобы указать получателя писем, которые требуется найти, нажмите кнопку  рядом с полем **Получатель** и в адресной книге (см. «[Адресная книга](#)» на стр. 41) выберите нужного получателя.
- 7 Для поиска писем, в теме которых содержится определенная строка, введите эту строку в поле **Тема письма**.
- 8 Для поиска писем по регистрационному номеру в поле **Рег. номер** введите номер или постоянную часть регистрационного номера.
- 9 Для поиска писем, содержащих вложения с определенными именами, в поле **Имя вложения** введите часть имени вложения.
- 10 Для поиска писем по именам транспортных конвертов (см. «[Транспортный конверт](#)») в поле **Имя конверта** введите часть имени конверта.
- 11 Для поиска писем, в тексте которых содержится определенная строка, введите эту строку в поле **Текст**.
- 12 Для поиска писем по статусу доставки и прочтения, в группе **Доставка и использование** установите нужные флажки:
- **Неотправленные документы.**
 - **Недоставленные документы.**
 - **Непрочитанные исходящие документы.**
 - **Непрочитанные входящие документы.**
- 13 Для поиска писем в определенном интервале дат выполните следующие действия:
- Чтобы указать начало интервала, установите флажок в поле **Начало**, затем нажмите кнопку  в правой части поля и выберите дату с помощью календаря.
 - Чтобы указать конец интервала, установите флажок в поле **Окончание**, затем нажмите кнопку  в правой части поля и выберите дату с помощью календаря.
- 14 Если требуется сбросить параметры поиска, нажмите кнопку **Очистить**.
- 15 Чтобы начать поиск писем с заданными параметрами, нажмите кнопку **Искать**.
Чтобы остановить процесс поиска, нажмите кнопку **Стоп**.

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

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

Экспорт и импорт писем

Экспорт писем

Письма «Деловой почты» можно экспортировать в формат BML. При экспорте вместе с письмами сохраняется атрибут цифровой подписи и время последней успешной проверки цифровой подписи. Если письма зашифрованы, при экспорте они автоматически расшифровываются.

Чтобы сохранить письма «Деловой почты» в файле *.bml, выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) 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 **Просмотр каталогов** 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 «Деловой почты» в программу Microsoft Outlook или Outlook Express (Windows Mail), выполните одно из следующих действий:

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



Примечание. Если в выбранной папке отсутствует доступ на создание сообщений, будет открыто окно создания нового сообщения, в которое будет вложено письмо «Деловой почты».

- Вложите в сообщение Microsoft Outlook или Outlook Express письмо деловой почты, экспортированное в файл *.bml.

Импорт писем

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

- В программе «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 «Деловой почты» в папку **Импорт**.

Импортированные письма появятся в папке **Импорт**.

Чтобы перенести в программу «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 «Деловой почты» (см. «[Интерфейс программы](#)» на стр. 34).
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. 46).

Перенос писем в другую папку

Перенести письма в другую папку «Деловой почты» можно двумя способами:

- 1 На панели писем выберите одно или несколько писем и перетащите их в папку назначения.
- 2 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](#)» на стр. 65).

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. 121).



Примечание. При работе в режиме администратора в контекстном меню письма доступен пункт **Полное удаление** (см. «[Дополнительные настройки и возможности „Деловой почты“](#)» на стр. 122).

Архивация писем

Под архивацией понимается перемещение определенных категорий писем из рабочего хранилища «Деловой почты» в заданную папку на диске. Архивация позволяет уменьшить объем рабочего хранилища и ускорить работу с письмами.



Внимание! Если в хранилище «Деловой почты» накопилось более 100 000 писем, мы настоятельно рекомендуем выполнить архивацию.

Архивация писем может осуществляться вручную либо автоматически. Автоматическая архивация запускается при выполнении определенных условий. Категории писем, подлежащие архивации, и параметры автоматической архивации можно задать в окне **Настройка** в разделе **Архивация** (см. «[Настройка архивации](#)» на стр. 111).

При архивации письма помещаются в архив, который представляет собой папку, имя которой формируется на основе даты и времени создания архива, например 21092010_163539. По умолчанию архив создается в папке \ViPNet Client\MSArch. Папку для хранения архивов можно изменить (см. «[Работа с архивами писем](#)» на стр. 69).

Письма, помещенные в архив, удаляются из рабочего хранилища «Деловой почты» и не отображаются в окне программы, однако их можно просматривать, открыв соответствующий архив (см. «[Работа с архивами писем](#)» на стр. 69).

Для архивации писем выполните следующие действия:

- 1 В зависимости от режима архивации:
 - Для запуска архивации вручную в окне программы ViPNet Client [Деловая почта] в меню **Файл** выберите пункт **Архивировать почту**.
 - Автоматическая архивация запускается в соответствии с заданными параметрами (см. «[Настройка архивации](#)» на стр. 111).
- 2 Перед началом архивации «Деловая почта» запросит подтверждение. В окне подтверждения нажмите **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 «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 «Деловой почты», выполните следующие действия:

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

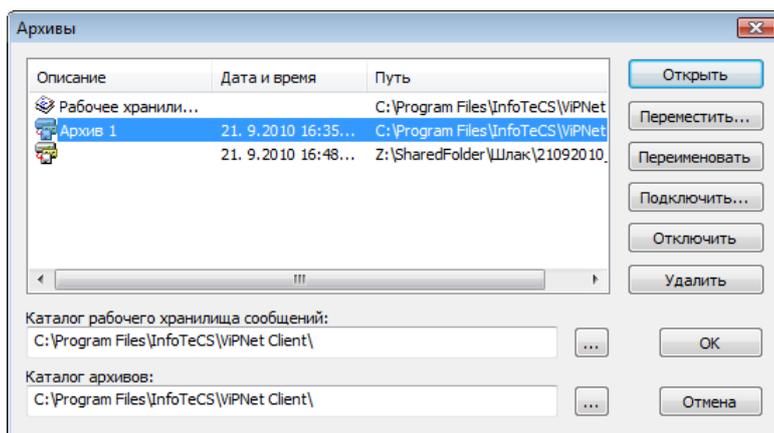


Рисунок 17: Окно управления архивами

- 2 В списке выберите архив, который требуется просмотреть.
- 3 Нажмите кнопку **Открыть**.

Письма, содержащиеся в выбранном архиве, будут отображены в окне программы «Деловая почта». Эти письма будут доступны только для чтения.

Во время работы с архивом писем рабочее хранилище «Деловой почты» 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 «Деловая почта» откроется рабочее хранилище, в котором возможна полноценная работа с защищенной почтой.

Чтобы просмотреть архив писем другого пользователя сети ViPNet:

- 1 В меню **Файл** выберите пункт **Выбрать архив**. Откроется окно **Архивы**.
- 2 Нажмите кнопку **Подключить**. Откроется окно **Просмотр каталогов**.
- 3 В окне **Просмотр каталогов** укажите папку, содержащую архив писем, и нажмите **ОК**.

Указанный архив будет добавлен в список в окне **Архивы**.

- 4 Выберите архив в списке и нажмите кнопку **Открыть**.

Письма, содержащиеся в архиве, будут отображены в окне программы «Деловая почта». Зашифрованные письма будут недоступны для просмотра, остальные письма будут доступны только для чтения.

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

- Чтобы задать папку, в которую помещаются создаваемые архивы писем:
 - В окне **Архивы** нажмите кнопку  рядом с полем **Каталог архивов**.
 - В окне **Просмотр каталогов** укажите папку, в которую будут помещаться архивы писем, и нажмите **ОК**.
- Чтобы переместить архив в другую папку:
 - В окне **Архивы** выберите архив и нажмите кнопку **Переместить**.
 - В окне **Просмотр каталогов** укажите папку, в которую требуется переместить архив, и нажмите кнопку **ОК**. Архив будет перемещен в указанную папку.
- Чтобы переименовать архив:
 - В окне **Архивы** 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:
 - В окне **Архив** выберите архив, который требуется удалить.

- Нажмите кнопку **Удалить**, в окне подтверждения нажмите **ОК**.



4

Цифровая подпись и шифрование

Цифровая подпись в программе «Деловая почта»	73
Работа с цифровой подписью писем	74
Работа с цифровой подписью файлов	82
Шифрование и расшифрование писем	86

Цифровая подпись в программе «Деловая почта»

Электронная цифровая подпись (ЭЦП, или цифровая подпись) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи.

Цифровая подпись позволяет:

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

С помощью программы «Деловая почта» можно подписать цифровой подписью текст письма и его вложения (см. [«Работа с цифровой подписью писем»](#) на стр. 74) или отдельные файлы (см. [«Работа с цифровой подписью файлов»](#) на стр. 82). Также можно проверить и удалить цифровую подпись письма или файла.

Для подписания писем и файлов можно использовать следующие типы сертификатов (см. [«Сертификат открытого ключа подписи пользователя»](#)):

- Сертификат цифровой подписи текущего пользователя абонентского пункта.
- Сертификат пользователя другого сетевого узла или сертификат внешнего пользователя сети ViPNet (см. [«Подписание выбранным сертификатом»](#) на стр. 76), находящийся во внешнем контейнере закрытого ключа (см. [«Контейнер закрытого ключа»](#)). Контейнер может храниться на диске или на внешнем устройстве (см. [«Информация о внешних устройствах хранения данных»](#) на стр. 11).
- Сертификат цифровой подписи, изданный сторонним удостоверяющим центром (см. [«Использование сертификата, изданного сторонним удостоверяющим центром»](#) на стр. 78).

Работа с цифровой подписью писем

Подписание письма

По умолчанию в программе «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. 114).

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

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) 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 цифровой подписи текущего пользователя.
 - **Выбранным сертификатом**, чтобы подписать письма сертификатом из определенного контейнера закрытого ключа.
 - Щелкните выбранные письма правой кнопкой мыши и в контекстном меню выберите пункт **Подписать**, затем щелкните **Текущим сертификатом** или **Выбранным сертификатом**.
- 3 Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе [Подписание выбранным сертификатом](#) (на стр. 76).

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

Чтобы подписать цифровой подписью письмо, открытое в окне создания и просмотра писем (см. «[Окно создания и просмотра писем](#)» на стр. 45), выполните следующие действия:

- 1 Создайте новое письмо (см. «[Создание письма](#)» на стр. 46) 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 цифровой подписи текущего пользователя.
 - **Выбранным сертификатом**, чтобы подписать письмо сертификатом из определенного контейнера закрытого ключа.
 - В меню **Подпись** выберите пункт **Подписать все письмо**, затем выберите **Текущим сертификатом** или **Выбранным сертификатом**.
- 3 Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе [Подписание выбранным сертификатом](#) (на стр. 76).

Письмо и его вложения будут подписаны цифровой подписью.

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

- 1 Создайте новое письмо (см. [«Создание письма»](#) на стр. 46) либо откройте неотправленное письмо в отдельном окне.
- 2 Выполните одно из действий:
 - В меню **Подпись** выберите пункт **Подписать текст письма**, затем выберите **Текущим сертификатом** или **Выбранным сертификатом**.
 - Щелкните текст письма правой кнопкой мыши, в контекстном меню выберите пункт **Подписать текст письма**, затем выберите **Текущим сертификатом** или **Выбранным сертификатом**.
- 3 Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе [Подписание выбранным сертификатом](#) (на стр. 76).

Текст письма будет подписан цифровой подписью.

Чтобы подписать цифровой подписью только вложения письма:

- 1 Создайте новое письмо (см. [«Создание письма»](#) на стр. 46) либо откройте неотправленное письмо в отдельном окне.
- 2 Добавьте в письмо одно или несколько вложений.
- 3 На вкладке **Вложения** выберите одно или несколько вложений.

- Щелкните выбранные вложения правой кнопкой мыши и в контекстном меню выберите пункт **Подписать**, затем щелкните **Текущим сертификатом** или **Выбранным сертификатом**.
- Если выбрана подпись сертификатом из внешнего контейнера, выполните действия, описанные в разделе [Подписание выбранным сертификатом](#) (на стр. 76).
Выбранные вложения будут подписаны цифровой подписью.

Подписание выбранным сертификатом

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

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

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

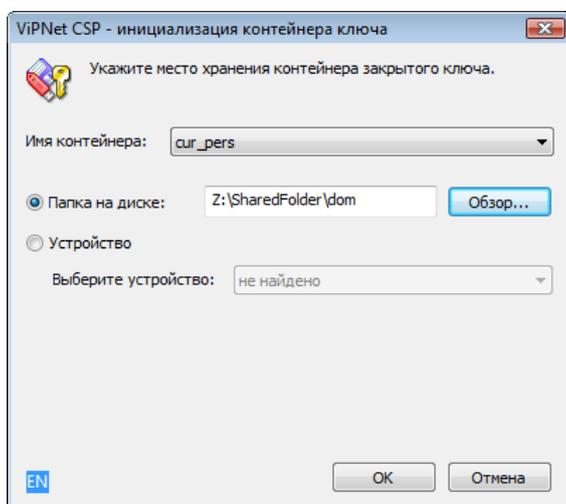


Рисунок 18: Контейнер хранится на диске

- Нажмите кнопку **Обзор** и укажите путь к папке, в которой хранится контейнер.
- Если в папке хранится несколько контейнеров, в списке **Имя контейнера** выберите нужный контейнер.
- Нажмите кнопку **ОК**.
- Если в контейнере хранится несколько сертификатов, откроется окно **Выбор сертификата**. Выберите сертификат и нажмите **ОК**.

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

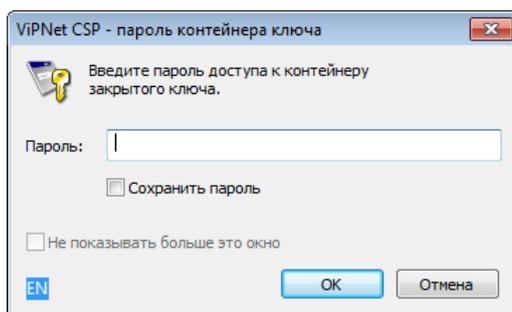


Рисунок 19: Ввод пароля доступа к контейнеру закрытого ключа

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

Если контейнер хранится на внешнем устройстве (см. [«Информация о внешних устройствах хранения данных»](#) на стр. 11), выполните следующие действия:

- 1 В окне **ViPNet CSP - инициализация контейнера ключа** выберите пункт **Устройство**.
- 2 Подключите устройство, на котором хранится контейнер. Если подключено несколько устройств, в списке **Выберите устройство** укажите нужное устройство.

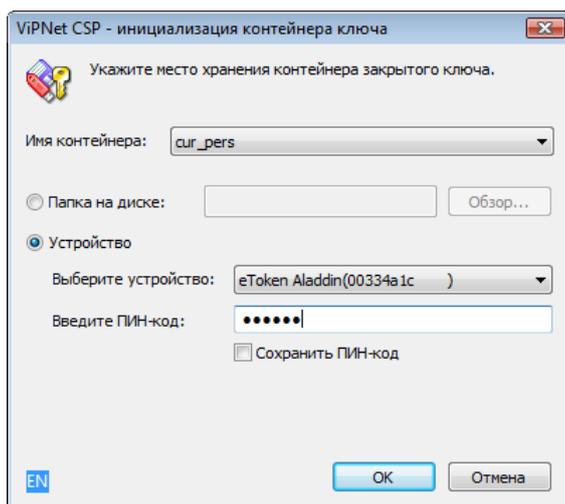


Рисунок 20: Контейнер хранится на внешнем устройстве

- 3 Если на устройстве хранится несколько контейнеров, в списке **Имя контейнера** выберите нужный контейнер.
- 4 В поле **Введите ПИН-код** укажите ПИН-код устройства и нажмите **ОК**.

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

Использование сертификата, изданного сторонним удостоверяющим центром

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

Чтобы использовать такой сертификат, выполните следующие действия:

- 1 Если сертификат и соответствующий ему закрытый ключ созданы с помощью криптопровайдера стороннего производителя (не входящего в состав ПО ViPNet):
 - В настройках параметров безопасности отключите криптопровайдер ViPNet CSP (см. [«Настройка параметров работы криптопровайдера ViPNet CSP»](#) на стр. 135).
 - Установите на компьютер криптопровайдер, необходимый для работы с внешним сертификатом.
- 2 Импортируйте сертификат и соответствующий закрытый ключ в системное хранилище сертификатов пользователя с помощью оснастки «Сертификаты — текущий пользователь» (certmgr.msc).

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

- 3 В окне **Настройка параметров безопасности** убедитесь, что на вкладке **Администратор** установлен флажок **Разрешить использование внешних сертификатов** (см. [«Дополнительные настройки параметров безопасности»](#) на стр. 123).



Примечание. Изменять настройки на вкладке **Администратор** может только администратор сетевого узла (см. [«Работа в программе с правами администратора»](#) на стр. 121).

- 4 На вкладке **Подпись** выберите нужный сертификат в качестве текущего (см. [«Смена текущего сертификата»](#) на стр. 166).
- 5 При подписании писем (см. [«Подписание письма»](#) на стр. 74) и файлов (см. [«Подписание файла»](#) на стр. 82) в меню выберите пункт **Текущим сертификатом**.

Проверка цифровой подписи письма

Чтобы проверить цифровую подпись письма, выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) на панели писем выберите подписанное письмо (с атрибутом **П** или **Н**), для которого требуется проверить цифровую 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 цифровой подписи**.

Чтобы проверить цифровую подпись вложения в окне просмотра письма (см. «[Окно создания и просмотра писем](#)» на стр. 45):

- 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 цифровой подписи**
- .

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

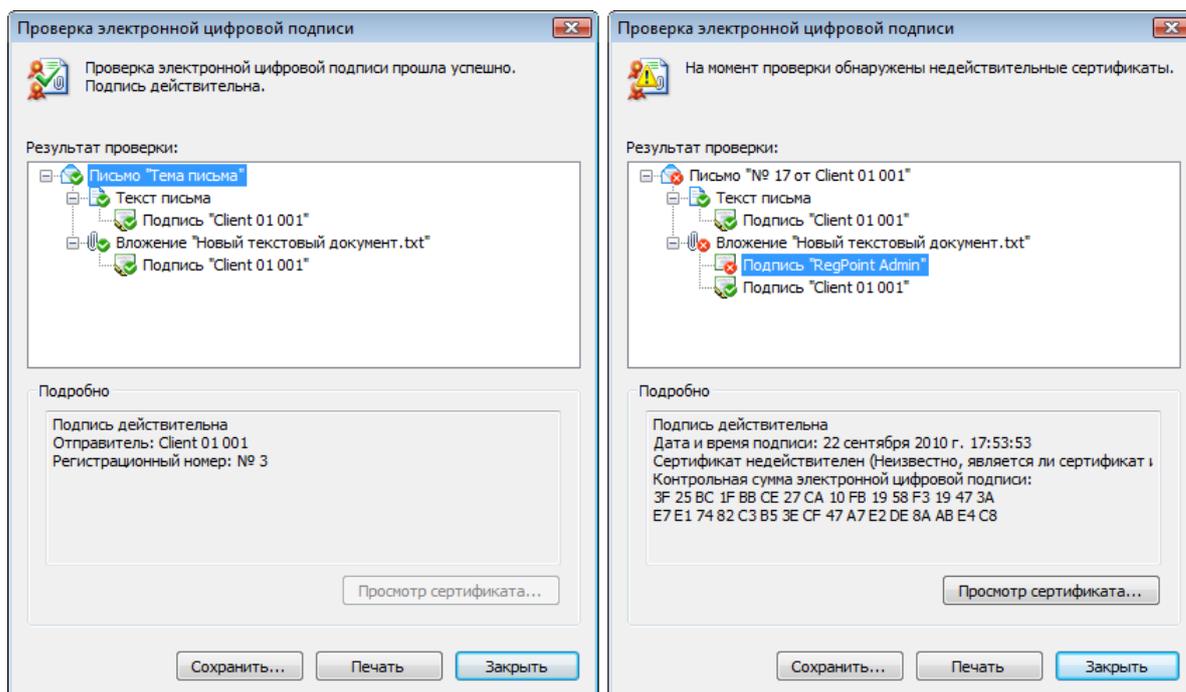


Рисунок 21: Результат проверки подписи

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

- Чтобы просмотреть сведения о цифровой подписи какого-либо элемента письма (всего письма, текста, какого-либо вложения или цифровой 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** цифровую подпись и нажмите кнопку **Просмотр сертификата**.

Удаление цифровой подписи письма

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

- 1 В окне программы ViPNet Client [Деловая почта] (см. «**Интерфейс программы**» на стр. 34) в папке **Исходящие** или какой-либо ее подпапке выберите одно или

несколько неотправленных писем с цифровой подписью (они имеют атрибут **П** или **Н**).

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**.

Цифровые подписи выбранных писем и их вложений будут удалены.

Чтобы удалить цифровую подпись письма, открытого в окне создания и просмотра писем (см. «[Окно создания и просмотра писем](#)» на стр. 45):

- Чтобы удалить цифровую подпись текста письма и всех вложений, нажмите кнопку **Удалить**  на панели инструментов.
- Чтобы удалить цифровую подпись вложения, на вкладке **Вложения** щелкните подписанное вложение правой кнопкой мыши и в контекстном меню выберите пункт **Удалить подпись**.
- Чтобы удалить цифровую 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 цифровой подписью файлов

Подписание файла

Программа «Деловая почта» позволяет подписать цифровой подписью файл, не являющийся вложением письма «Деловой почты». 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 цифровой подписи (см. «[Проверка цифровой подписи файла](#)» на стр. 84). Чтобы была возможность просматривать подписанные файлы, нужно отсоединить их цифровые подписи (см. «[Отсоединение и присоединение подписи файла](#)» на стр. 83). Если файл с присоединенной или отсоединенной цифровой подписью каким-либо образом изменить, цифровая подпись станет недействительной.

Чтобы подписать цифровой подписью один или несколько файлов, не являющихся вложениями «Деловой почты», выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] в меню **Файл** выберите пункт **Подпись файлов**, затем выберите:
 - **Подписать файл текущим сертификатом**, чтобы использовать для подписи текущий сертификат цифровой подписи.
 - **Подписать файл выбранным сертификатом**, чтобы использовать для подписи сертификат цифровой подписи из внешнего контейнера.
- 2 Если выбрана подпись внешним сертификатом, выполните действия, описанные в разделе [Подписание выбранным сертификатом](#) (на стр. 76).
- 3 Откроется окно **Открыть**. В этом окне укажите один или несколько файлов, которые требуется подписать цифровой 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 80 на стр. 185) введите пароль.

Файлы будут подписаны выбранным сертификатом.



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

Если подписать файл, уже имеющий отсоединенную цифровую подпись (см. «Отсоединение и присоединение подписи файла» на стр. 83), новая подпись будет присоединена к файлу, а отсоединенная подпись не изменится.

Отсоединение и присоединение подписи файла

При подписании файла одной или несколькими цифровыми подписями создается файл *.v7s, содержащий исходный файл и цифровые подписи.

Чтобы отсоединить подписи файла, выполните следующие действия:

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

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

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



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

Чтобы присоединить отсоединенную цифровую подпись, выполните следующие действия:

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

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



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

Проверка цифровой подписи файла

Для проверки цифровой подписи файла выполните следующие действия:

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

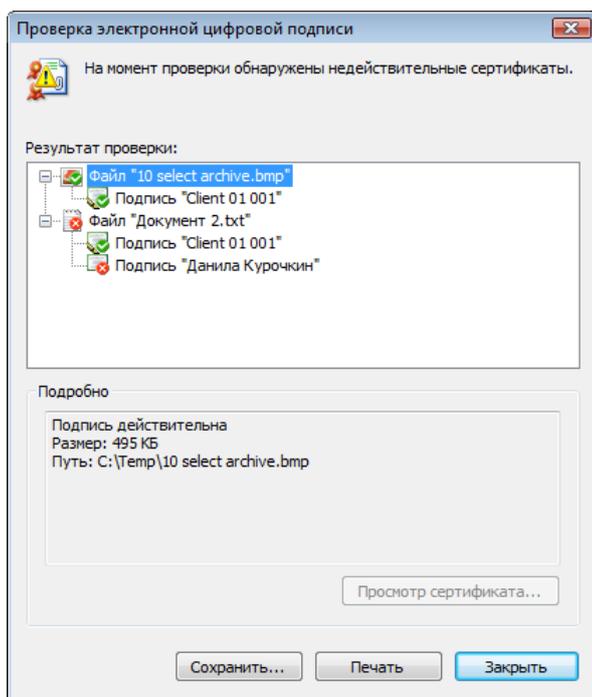


Рисунок 22: Проверка подписей нескольких файлов

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



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

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

- Чтобы просмотреть сведения о файле или цифровой 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** цифровую подпись и нажмите кнопку **Просмотр сертификата**.

Удаление цифровой подписи файла

Чтобы удалить цифровую подпись файла, выполните следующие действия:

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



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

Шифрование и расшифрование писем

По умолчанию в программе «Деловая почта» настроено автоматическое шифрование писем и вложений при отправке. Эти настройки можно изменить (см. «[Настройка параметров работы с письмами](#)» на стр. 114).

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

1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) 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**.

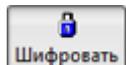
Выбранные письма будут расшифрованы вместе с вложениями.

Чтобы зашифровать или расшифровать письмо, открытое в окне создания и просмотра писем (см. «[Окно создания и просмотра писем](#)» на стр. 45), выполните следующие действия:

1 Создайте новое письмо (см. «[Создание письма](#)» на стр. 46) 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 следующим образом:





5

Автопроцессинг

Принцип работы автопроцессинга	89
Настройка параметров автопроцессинга	92
Оптимизация работы автопроцессинга	101
Просмотр журнала автопроцессинга	102
Настройка параметров журнала автопроцессинга	106

Принцип работы автопроцессинга

Автопроцессингом называется автоматическая обработка писем и файлов по определенным правилам.

Правила автопроцессинга делятся на две категории:

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

Правила автопроцессинга можно создать в окне **Настройка** в разделе **Автопроцессинг** (см. «[Настройка параметров автопроцессинга](#)» на стр. 92).

Схема работы автопроцессинга представлена на следующем рисунке:

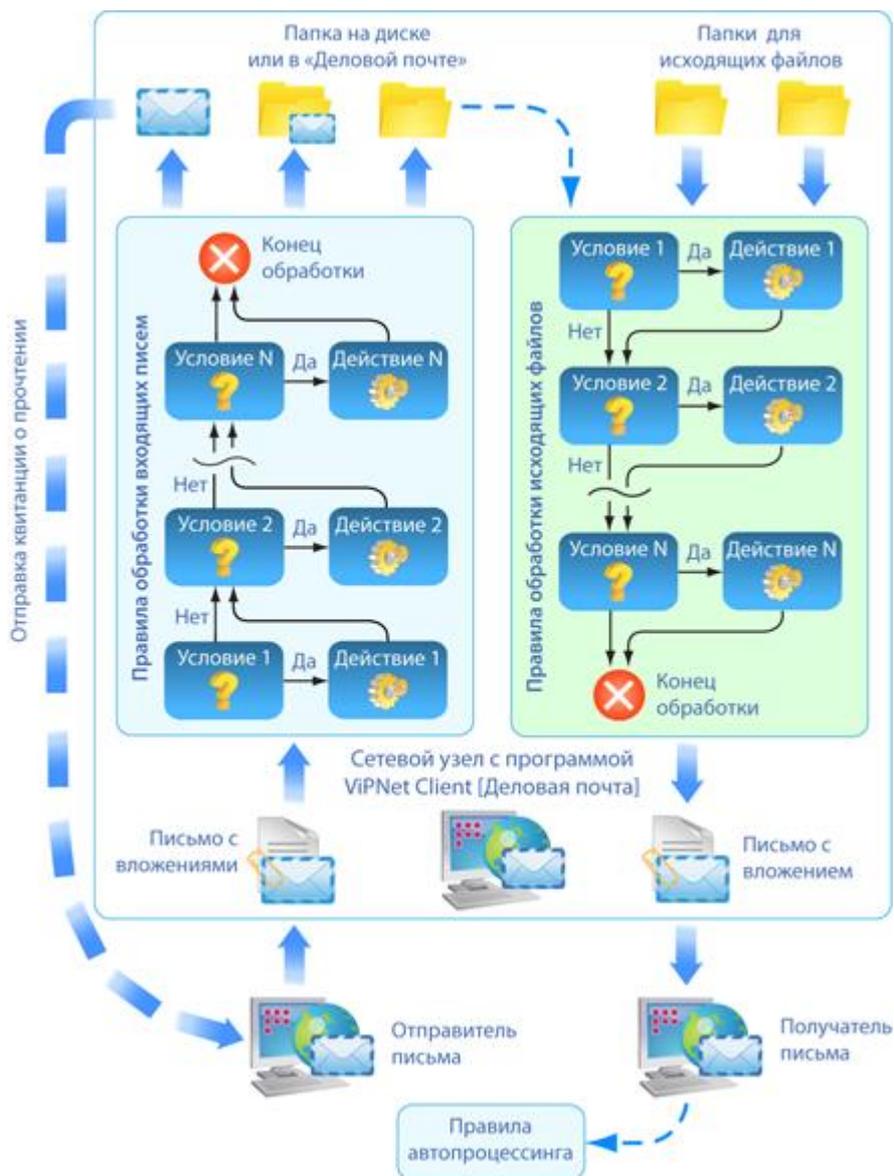


Рисунок 23: Схема работы автопроцессинга

Обработка писем и файлов осуществляется следующим образом:

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

- 2 Начинается обработка письма или файла соответствующими правилами автопроцессинга. Обработка выполняется в порядке расположения правил в списке в разделе **Автопроцессинг**.
- 3 Каждое правило автопроцессинга состоит из условия и действия. Если письмо или файл удовлетворяет условиям правила:
 - Над ним выполняется заданное действие.
 - Если в действии правила не задано прекращение дальнейшей обработки, письмо или файл обрабатывается следующим правилом.
- 4 Обработка письма или файла прекращается после проверки всех правил или если выполняется действие, прекращающее дальнейшую обработку.



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

Настройка параметров автопроцессинга

Для настройки параметров автопроцессинга выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне **Настройка** на левой панели выберите раздел **Автопроцессинг**.

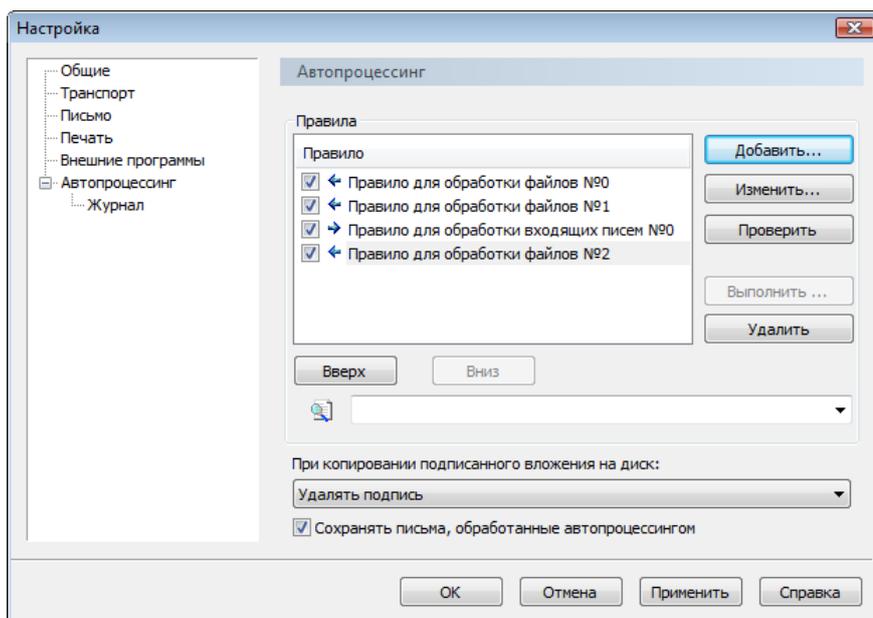


Рисунок 24: Настройка параметров автопроцессинга

- 3 Чтобы настроить правило для обработки файлов, следуйте указаниям раздела [Создание правила для исходящих файлов](#) (на стр. 93).
Чтобы настроить правило для обработки писем, следуйте указаниям раздела [Создание правила для входящих писем](#) (на стр. 96).
- 4 Для поиска правила в списке введите часть имени правила в строку поиска, расположенную под списком.
- 5 Чтобы выключить или включить правило автопроцессинга, снимите или установите флажок слева от имени правила в списке.

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



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

- 7 Чтобы изменить параметры правила, выберите его в списке и нажмите кнопку **Изменить**. Настройка правил описана в разделах [Создание правила для исходящих файлов](#) (на стр. 93) и [Создание правила для входящих писем](#) (на стр. 96).
- 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 «Деловой почты».
- 10 Чтобы удалить правило, выберите его в списке и нажмите кнопку **Удалить**.
- 11 Чтобы указать, как следует поступать с цифровой подписью файлов, копируемых на диск, выберите нужный вариант из списка **При копировании подписанного вложения на диск**.
- 12 Чтобы сохранять письма, обработанные автопроцессингом в папках «Деловой почты» или удалять их, установите или снимите соответствующий флажок.
Если данный флажок снят, обработанные письма автоматически удаляются, информация об этих письмах сохраняется в папке **Аудит**.

Создание правила для исходящих файлов

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

- 1 В окне программы ViPNet Client [Деловая почта] в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне **Настройка** на левой панели выберите раздел **Автопроцессинг** (см. Рисунок 24 на стр. 92).

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

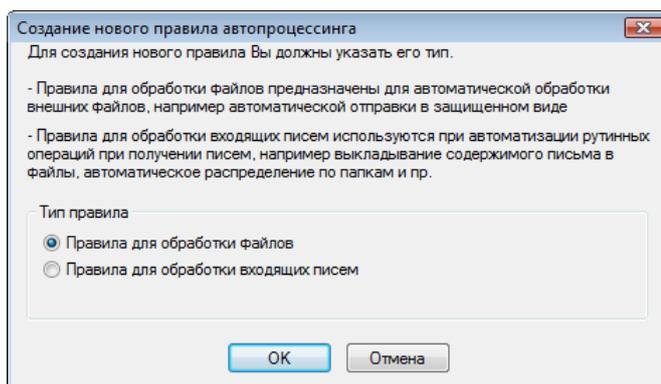


Рисунок 25: Выбор типа правила

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

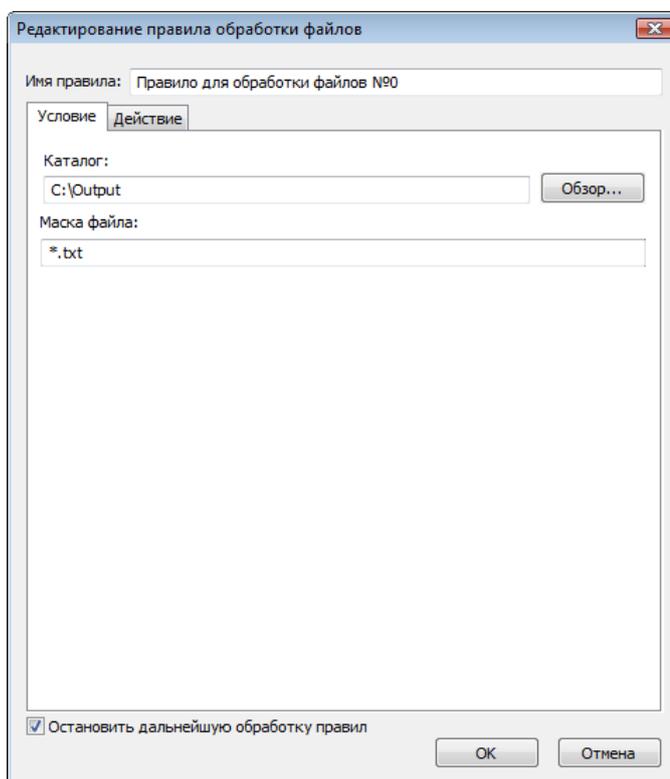


Рисунок 26: Условие для правила обработки исходящих файлов

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

6 На вкладке **Условие** нажмите кнопку **Обзор** и в окне **Просмотр каталогов** 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.

Для задания маски имени файла используются следующие специальные символы:

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

8 Откройте вкладку **Действие**.

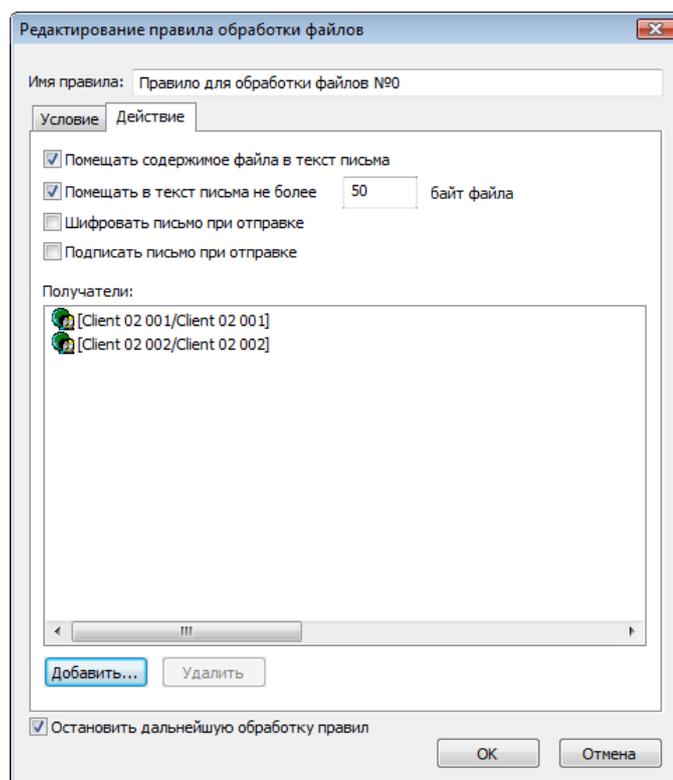


Рисунок 27: Действие правила обработки файлов

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



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

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

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

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

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

11 Чтобы подписывать вложенный файл цифровой подписью, установите флажок **Подписывать письмо при отправке**.

12 Чтобы добавить получателей, которым будет отправлен файл:

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

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 **ОК**.

Создание правила для входящих писем

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

- 1** В окне программы ViPNet Client [Деловая почта] в меню **Инструменты** выберите пункт **Настройка**.
- 2** В окне **Настройка** на левой панели выберите раздел **Автопроцессинг** (см. Рисунок 24 на стр. 92).

- 3 На вкладке **Автопроцессинг** нажмите кнопку **Добавить**, откроется окно **Создание нового правила автопроцессинга**.
- 4 Выберите тип правила **Правило для обработки входящих писем** и нажмите кнопку **ОК**. Откроется окно **Редактирование правила обработки входящих писем**.

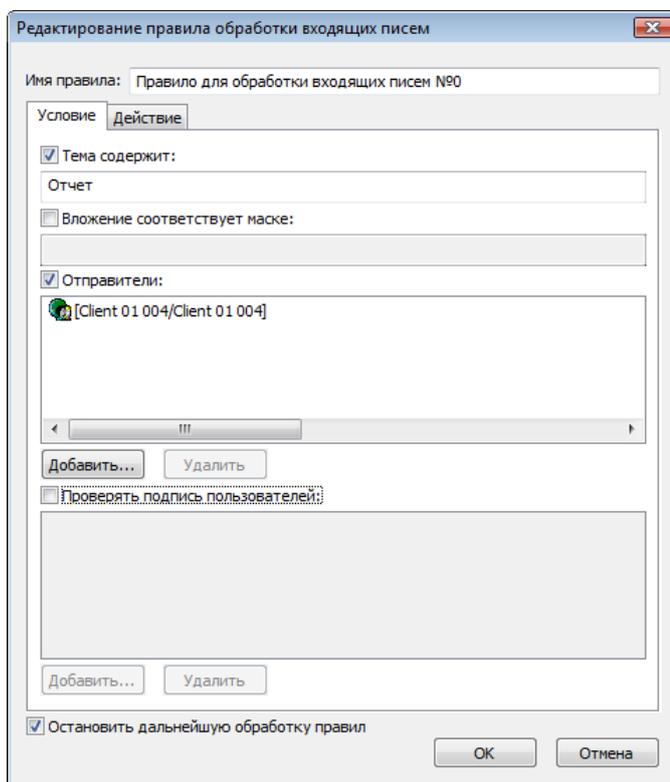


Рисунок 28: Условие правила обработки входящих писем

- 5 В поле **Имя правила** укажите имя для создаваемого правила.
- 6 На вкладке **Условие** задайте условия, при выполнении которых письмо будет обработано данным правилом:
 - Если необходимо обрабатывать письма, в теме которых содержится определенная последовательность символов, установите флажок **Тема содержит** и в поле под этим флажком введите требуемые символы.
 - Если необходимо обрабатывать письма с вложениями, имена которых соответствуют определенной маске, установите флажок **Вложение соответствует маске** и в поле под этим флажком введите маску имени вложения. Можно задать только одну маску.

Для задания маски имени файла используются следующие специальные символы:

- * — соответствует любой последовательности символов.

- ? — соответствует любому единичному символу.
- Если необходимо обрабатывать письма от определенных отправителей:
 - Установите флажок **Отправители**.
 - Нажмите кнопку **Добавить**. Откроется **Адресная книга** (на стр. 41).
 - В адресной книге выберите одного или несколько отправителей и нажмите кнопку **Выбрать**.
 - Выбрав нужных отправителей, нажмите кнопку **Заккрыть**.
 - Если требуется удалить каких-либо отправителей, выберите их в списке и нажмите кнопку **Удалить**.
- Если необходимо обрабатывать письма, подписанные цифровой подписью определенных пользователей:
 - Установите флажок **Проверять подпись пользователей**.
 - Нажмите кнопку **Добавить**. Откроется **Адресная книга**.
 - В адресной книге выберите одного или несколько пользователей и нажмите кнопку **Выбрать**.
 - Выбрав нужных пользователей, нажмите кнопку **Заккрыть**.
 - Если требуется удалить каких-либо пользователей, выберите их в списке и нажмите кнопку **Удалить**.



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

7 Откройте вкладку **Действие**.

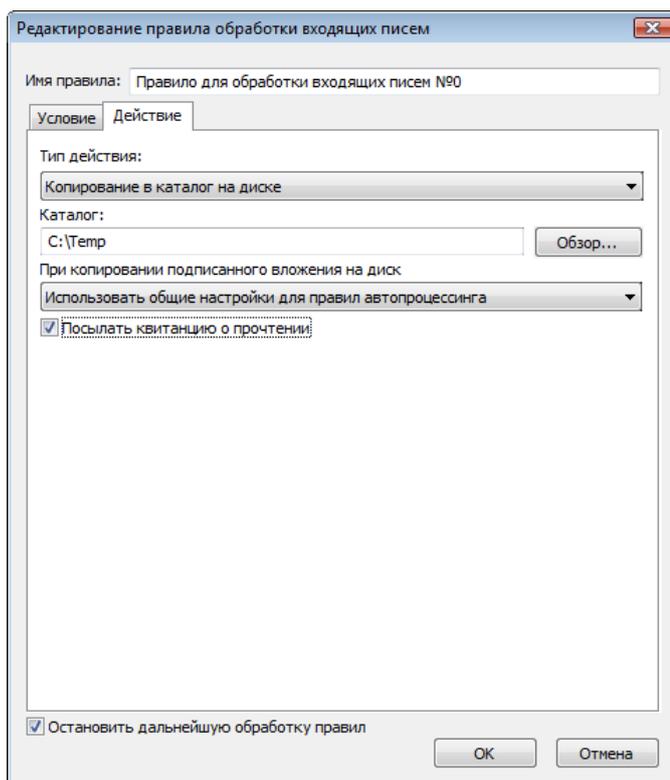


Рисунок 29: Действие правила обработки входящих писем

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

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

При копировании письма на диске в указанной папке сохраняются файлы вложений и текст письма в виде файла `blank.txt`. На этот файл распространяется тип действия, выбранный в списке. По умолчанию файл `blank.txt` создается даже в том случае, если в письме нет текста.



Примечание. Чтобы не создавать файл `blank.txt` в случае отсутствия текста в письме, следует в файле `wmail.ini` (этот файл находится в папке установки «Деловой Почты») присвоить параметру `ProcessEmptyBlankTxt` значение 0. По умолчанию параметр имеет значение 1.

- 9** Если выбрано копирование письма в каталог на диске, выполните следующие действия:
- Нажмите кнопку **Обзор** и в окне **Просмотр каталогов** укажите папку, в которую будут скопированы текст письма и его вложения.
 - Из списка **При копировании подписанного вложения на диск** выберите один из вариантов:
 - **Использовать общие настройки для правил автопроцессинга.** При выборе этого варианта будет выполнено действие, заданное в разделе **Автопроцессинг** (см. «[Настройка параметров автопроцессинга](#)» на стр. 92).
 - **Удалять подпись.**
 - **Сохранять в виде файла с присоединенной подписью.**
 - **Отсоединять подпись в отдельный файл.**
- Подробнее о присоединенной и отсоединенной цифровой подписи файла см. [Отсоединение и присоединение подписи файла](#) (на стр. 83).
- Если после обработки письма данным правилом требуется отправлять уведомление о прочтении письма, установите флажок **Посылать квитанцию о прочтении**.
- 10** Если выбрано копирование письма в папку «Деловой почты», нажмите кнопку **Обзор** и в окне **Укажите папку** выберите папку «Деловой почты» для сохранения писем. Это должна быть какая-либо подпапка папки **Входящие**.
- 11** Если требуется, чтобы после обработки письма данным правилом это письмо могло быть обработано последующими правилами, снимите флажок **Остановить дальнейшую обработку правил** (по умолчанию установлен).
- 12** Чтобы сохранить правило, нажмите кнопку **ОК**.

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 «Деловой почты», приостановить прием текущей корреспонденции, вызвать непредвиденные ошибки.

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

- 1 Войдите в программу «Деловая почта» с правами администратора (см. [«Работа в программе с правами администратора»](#) на стр. 121).
- 2 В окне программы в меню **Инструменты** выберите пункт **Настройка**.
- 3 В окне **Настройка** на левой панели выберите раздел **Администратор**.
- 4 В разделе **Администратор** снимите флажок **Сохранять историю в папке «Аудит»**.
- 5 На левой панели выберите раздел **Автопроцессинг**.
- 6 В разделе **Автопроцессинг** (см. [«Настройка параметров автопроцессинга»](#) на стр. 92) снимите флажок **Сохранять письма, обработанные автопроцессингом**.

Данные настройки позволят существенно повысить скорость обработки писем правилами автопроцессинга.

Просмотр журнала автопроцессинга

Информация о событиях, возникающих при работе автопроцессинга, фиксируется в журнале автопроцессинга. Настройка параметров журнала описана ниже (см. «[Настройка параметров журнала автопроцессинга](#)» на стр. 106).

Для просмотра журнала автопроцессинга выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) в меню **Файл** выберите пункт **Журнал автопроцессинга**. Откроется окно **Просмотр журналов**.

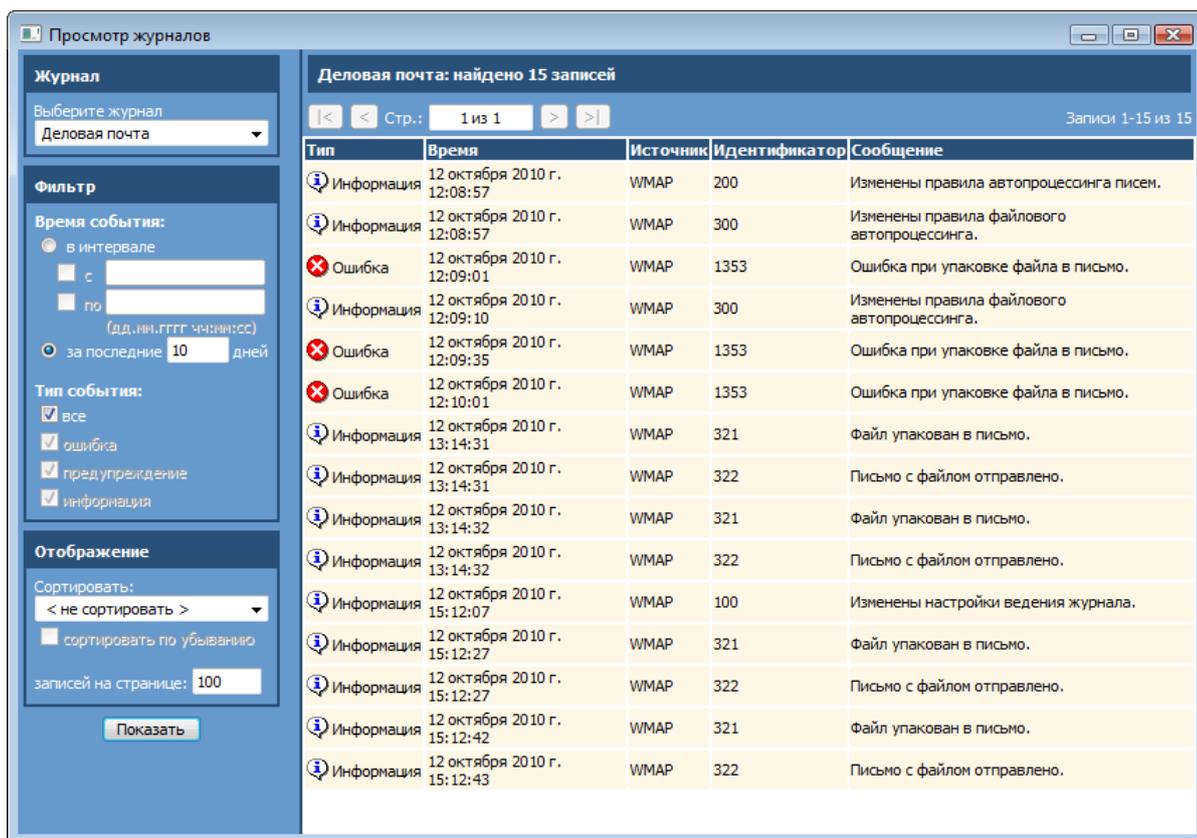


Рисунок 30: Просмотр журнала автопроцессинга

- 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 интервала, установите флажок **с** и в поле справа введите дату и время начала интервала в формате `дд.мм.гггг чч:мм:сс`. Чтобы указать конец интервала, установите флажок **по** и в поле справа введите дату и время конца интервала.
- 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 30 на стр. 102).

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**.

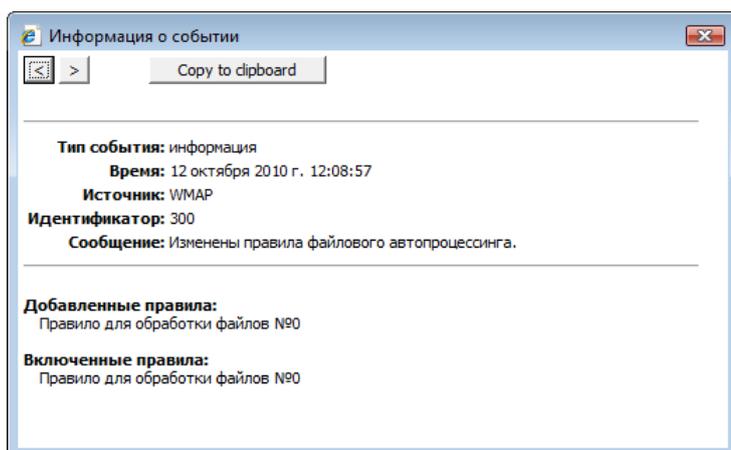


Рисунок 31: Подробная информация о событии

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 в следующей таблице:

Тип события	Идентификатор события	Описание события
	100	Изменены настройки ведения журнала
	200	Изменены правила автопроцессинга писем
	210	Сработало правило автопроцессинга писем
	211	Письмо перемещено
Информация	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

Тип события	Идентификатор события	Описание события
	1251	Ошибка при обработке письма
	1252	Ошибка при поиске правила
	1253	Ошибка при применении правила
	1254	Ошибка при перемещении письма
Ошибка	1255	Ошибка при сохранении текста письма
	1256	Ошибка при сохранении вложения
	1351	Ошибка при поиске файлов
	1352	Ошибка при обработке файла
	1353	Ошибка при упаковке файла в письмо
	1354	Ошибка при отправке письма с файлом

Настройка параметров журнала автопроцессинга

Для настройки параметров журнала автопроцессинга выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне **Настройка** на левой панели разверните пункт **Автопроцессинг** и щелкните пункт **Журнал**. На правой панели отобразится раздел **Журнал**.

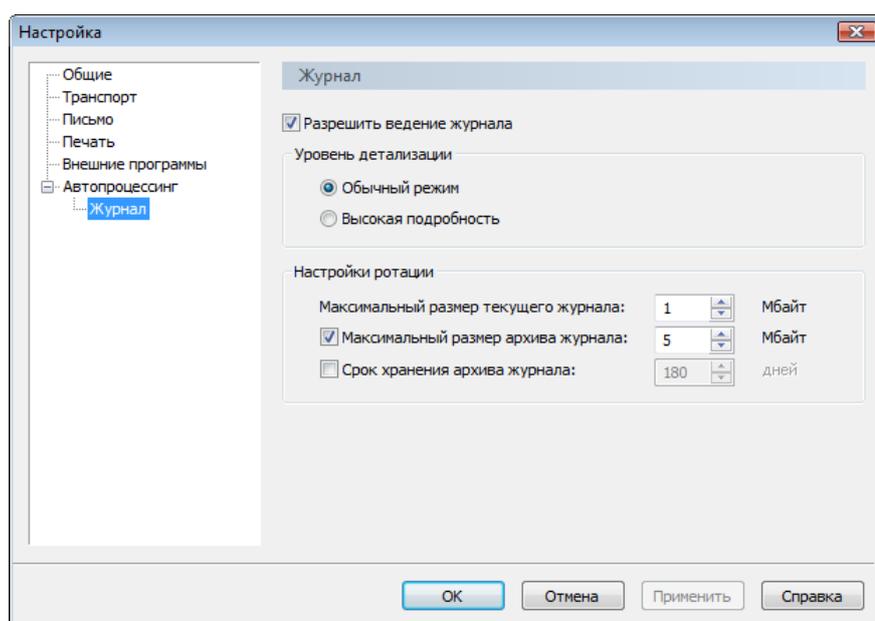


Рисунок 32: Настройка журнала автопроцессинга

- 3 Если требуется отключить ведение журнала автопроцессинга, снимите флажок **Разрешить ведение журнала** (по умолчанию установлен).
Если данный флажок снят, настройка остальных параметров журнала автопроцессинга недоступна.
- 4 В группе **Уровень детализации** выберите один из пунктов:
 - **Обычный режим** (выбран по умолчанию) — фиксируется наиболее важная информация.
 - **Высокая подробность** — фиксируется вся информация.

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

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

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

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

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

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

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



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

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



6

Настройка программы

Общие настройки	109
Настройка архивации	111
Настройка параметров работы с письмами	114
Настройка транспортного модуля	116
Настройка печати	118
Настройка внешних программ	119
Работа в программе с правами администратора	121

Общие настройки

Для настройки общих параметров «Деловой почты» выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне настройки на левой панели выберите раздел **Общие**.

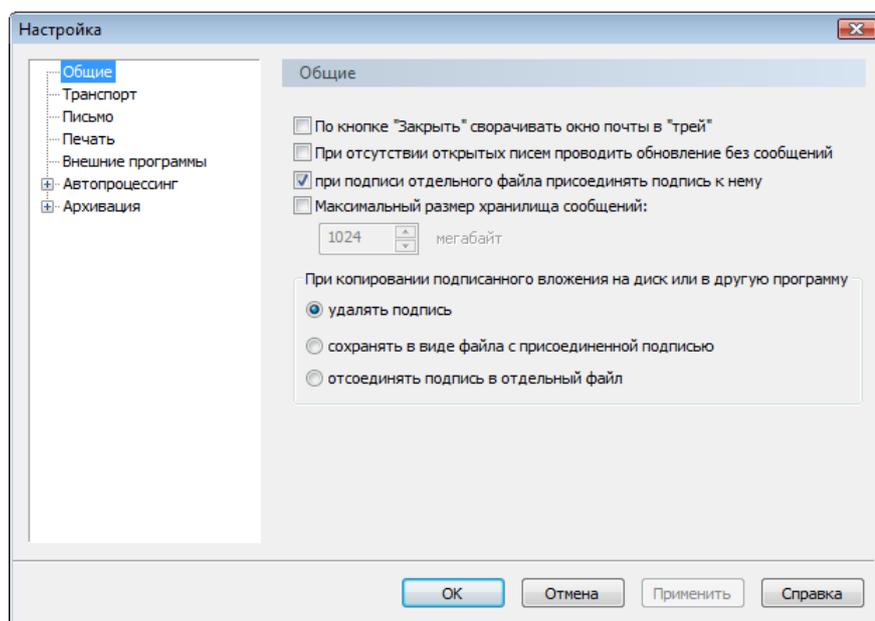


Рисунок 33: Общие настройки «Деловой почты»

- 3 Чтобы при нажатии на кнопку **Закреть**  программа сворачивалась в область уведомлений, установите флажок **По кнопке «Закреть» сворачивать окно почты в «трей»** (по умолчанию снят).
- 4 Чтобы при отсутствии открытых писем проводить обновление справочно-ключевой информации и программного обеспечения без уведомлений, установите флажок **При отсутствии открытых писем проводить обновление без сообщений** (по умолчанию снят).
- 5 Если требуется отсоединять цифровую подпись при подписании отдельного файла (см. «[Подписание файла](#)» на стр. 82), 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 перестает забирать почтовые конверты из папки транспортного модуля.

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

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

Подробнее о присоединенной и отсоединенной цифровой подписи файла см. [Отсоединение и присоединение подписи файла](#) (на стр. 83).

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

Настройка архивации

Чтобы указать, какие письма следует помещать в архив при ручной или автоматической архивации писем (см. «[Архивация писем](#)» на стр. 67), выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне **Настройка** на левой панели выберите раздел **Архивация**.

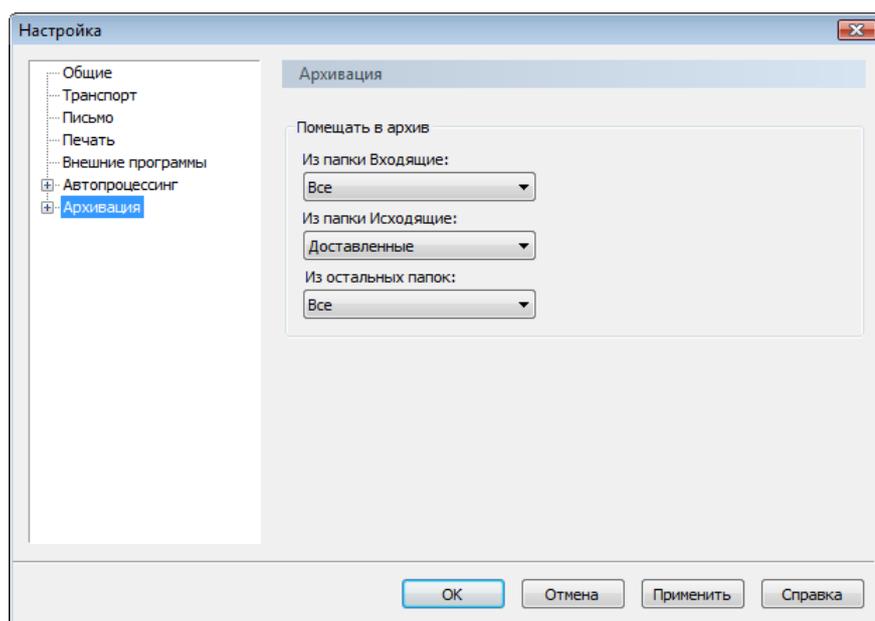


Рисунок 34: Настройка параметров архивации

- 3 В разделе **Архивация** выполните следующие действия:
 - 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**).
- 4 Выполнив необходимые настройки, нажмите кнопку **Применить**.

Для настройки параметров автоматической архивации выполните следующие действия:

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

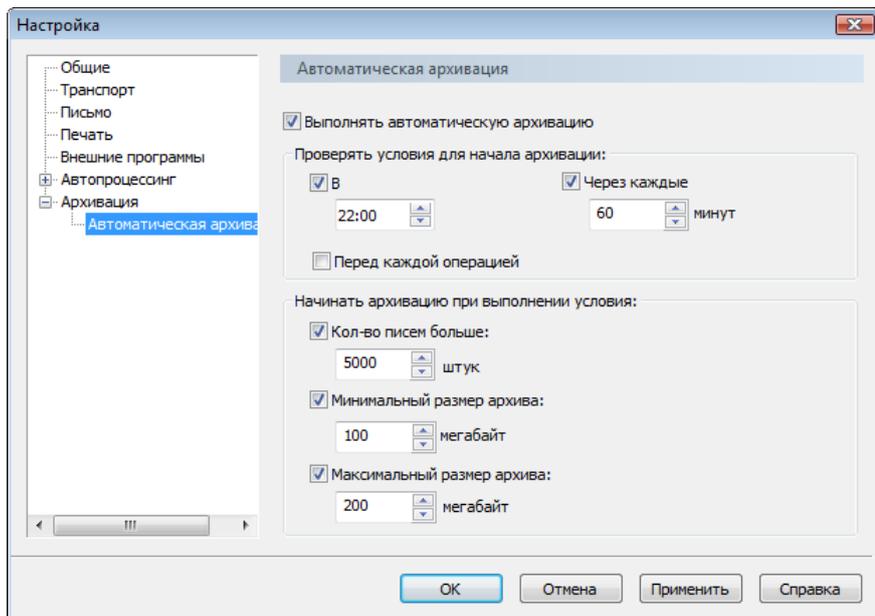


Рисунок 35: Параметры автоматической архивации

- 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** укажите, когда требуется проверять условия архивации:
 - 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).
- 4 Если автоматическая архивация включена, в группе **Начинать архивацию при выполнении условия** задайте условия выполнения автоматической архивации:
 - Чтобы выполнять автоматическую архивацию при накоплении определенного количества писем, установите флажок **Кол-во писем больше** и в поле под флажком укажите количество писем (по умолчанию 5000).

- Чтобы выполнять автоматическую архивацию при достижении определенного размера хранилища, установите флажок **Минимальный размер архива** и в поле под флажком укажите размер в мегабайтах (по умолчанию 100).

Если задан минимальный размер архива, то при проверке условий архивации подсчитывается текущий размер хранилища писем. Если он меньше заданного минимального размера архива, дальнейшие проверки не выполняются.

В противном случае подсчитывается суммарный размер писем, подлежащих архивации (задаются в группе **Помещать в архив**). Если полученное значение больше заданного минимального размера архива, запускается автоматическая архивация.

- Чтобы задать максимальный размер архива, установите флажок **Максимальный размер архива** 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 Выполнив необходимые настройки, нажмите кнопку **Применить**.

Настройка параметров работы с письмами

Для настройки параметров работы с письмами выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне **Настройка** на левой панели выберите раздел **Письмо**.

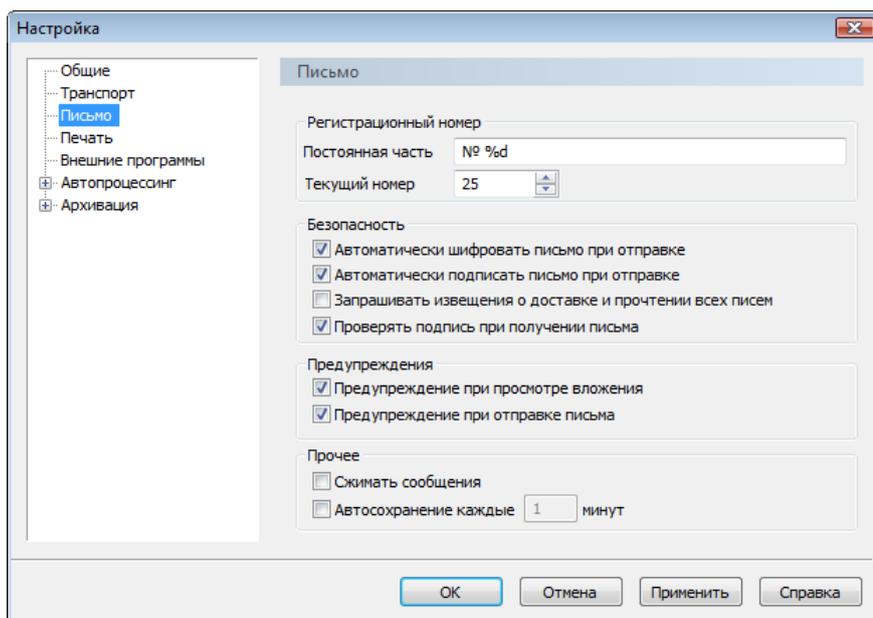


Рисунок 36: Параметры работы с письмами

- 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. 34).
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 цифровой 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. «[Цифровая подпись в программе „Деловая почта“](#)» на стр. 73).
 - Установите или снимите флажок **Запрашивать извещения о доставке и прочтении всех писем** (см. «[Запрос извещения о доставке и прочтении в виде отдельного письма](#)» на стр. 48).
 - Установите или снимите флажок **Проверять подпись при получении письма**.
- 5** Чтобы изменить параметры уведомления при просмотре вложений и отправке писем, в группе **Предупреждения** выполните следующие действия:
- Установите или снимите флажок **Предупреждение при просмотре вложения**.
Если этот флажок установлен, перед просмотром вложения программа выдаст предупреждение.
 - Установите или снимите флажок **Предупреждение при отправке письма**.
Если этот флажок установлен, при отправке письма программа запросит подтверждение.
- 6** В группе **Прочие** доступны следующие настройки:
- Чтобы уменьшить размер передаваемых конвертов, установите флажок **Сжимать сообщения** (по умолчанию снят). Перед отправкой письма будут обрабатываться алгоритмом сжатия.
 - Чтобы включить автоматическое сохранение редактируемых писем, установите флажок **Автосохранение каждые** (по умолчанию снят) и в поле справа укажите интервал автоматического сохранения в минутах.

Настройка транспортного модуля

Для настройки параметров транспортного модуля MFTR выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «Интерфейс программы» на стр. 34) в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне **Настройка** на левой панели выберите раздел **Транспорт**.

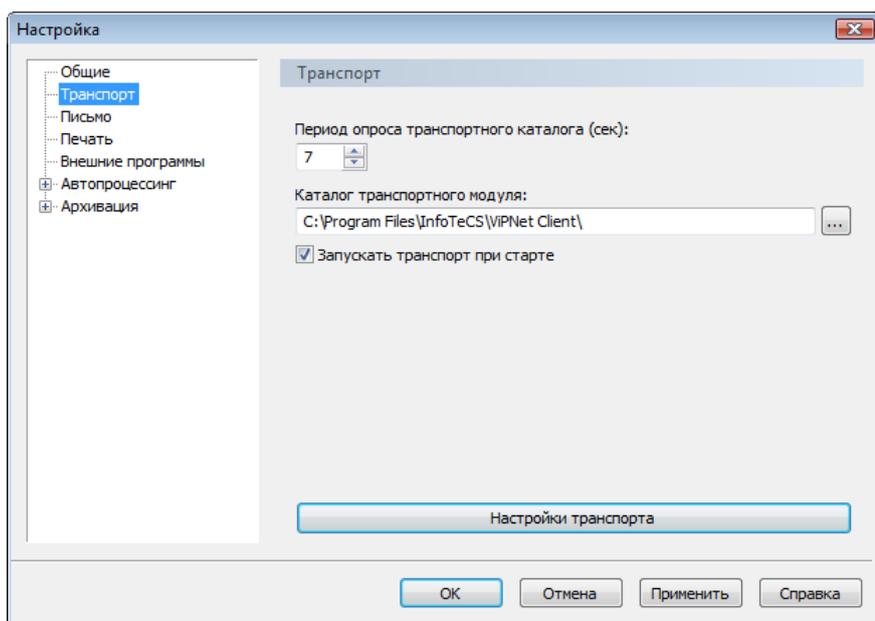


Рисунок 37: Настройки транспортного модуля

- 3 В разделе **Транспорт** при необходимости можно изменить следующие параметры:
 - В поле **Период опроса транспортного каталога (сек)** укажите нужный период в секундах.
 - Чтобы изменить транспортный каталог, нажмите кнопку  и в окне **Просмотр каталогов** укажите папку, в которой находится транспортный модуль MFTR.



Внимание! Не следует изменять папку транспортного модуля без необходимости.

- Если не требуется запускать транспортный модуль при запуске «Деловой почты», снимите флажок **Запускать транспорт при старте** (по умолчанию установлен).
- 4** Чтобы вызвать окно настройки, доступное из основного окна транспортного модуля, нажмите кнопку **Настройки транспорта**.
- Подробная информация о транспортном модуле и его настройке содержится в документе «ViPNet MFTP. Руководство администратора».
- 5** Выполнив необходимые настройки, нажмите кнопку **ОК**.

Настройка печати

Чтобы настроить параметры печати писем, выполните следующие действия:

- 1 В окне программы ViPNet Client [Деловая почта] (см. «Интерфейс программы» на стр. 34) в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне **Настройка** на левой панели выберите раздел **Печать**.

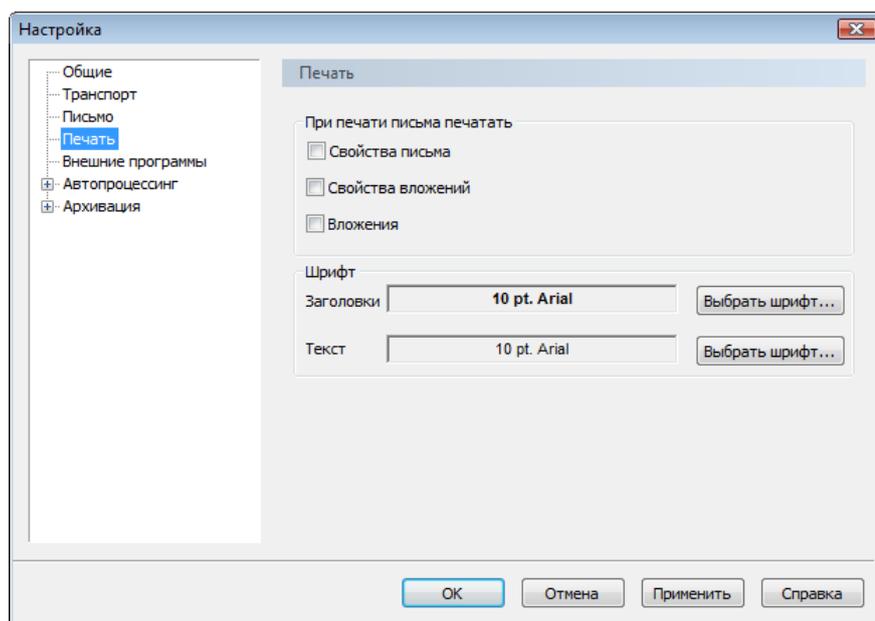


Рисунок 38: Настройки печати

- 3 В группе **При печати письма печатать** укажите, какую дополнительную информацию требуется добавлять к тексту письма, установив соответствующие флажки (по умолчанию все флажки сняты):
 - **Свойства письма.**
 - **Свойства вложений.**
 - **Вложения.**
- 4 Чтобы изменить шрифт заголовка или текста при печати, нажмите кнопку **Выбрать шрифт** напротив поля **Заголовки** или **Текст** и в окне **Шрифт** задайте параметры шрифта.
- 5 Выполнив необходимые настройки, нажмите кнопку **Применить**.

Настройка внешних программ

В программе ViPNet Client [Деловая почта] существует возможность вызова внешних программ с помощью меню **Инструменты > Запуск внешних программ** или кнопки  на панели инструментов.

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

- 1 В окне программы ViPNet Client [Деловая почта] (см. «[Интерфейс программы](#)» на стр. 34) в меню **Инструменты** выберите пункт **Настройка**.
- 2 В окне **Настройка** на левой панели выберите раздел **Внешние программы**.

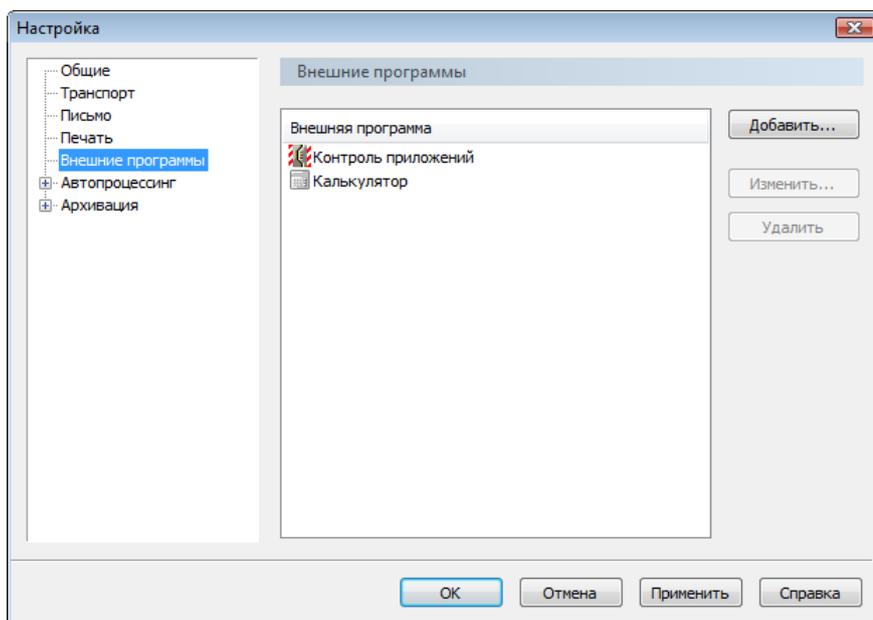


Рисунок 39: Настройка внешних программ

- 3 Чтобы добавить программу в список программ, доступных для вызова из «Деловой почты»:
 - 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 «Деловой почты», 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**.

Чтобы вызвать одну из внешних программ, добавленных в список, в окне программы «Деловая почта» на панели инструментов нажмите кнопку **Запуск внешних программ**  и выберите нужную программу из списка.

Работа в программе с правами администратора

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

- [Дополнительные настройки и возможности «Деловой почты»](#) (на стр. 122).
- [Дополнительные настройки параметров безопасности](#) (на стр. 123).
- [Изменение режима авторизации пользователя](#) (на стр. 124).

При работе в режиме администратора все ограничения, накладываемые уровнем полномочий пользователя (см. [«Полномочия пользователя»](#)), снимаются.

Чтобы войти в программу в качестве администратора:

- 1 В окне программы ViPNet Client [Деловая почта] (см. [«Интерфейс программы»](#) на стр. 34) 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 (см. «Администратор сетевого узла ViPNet»).

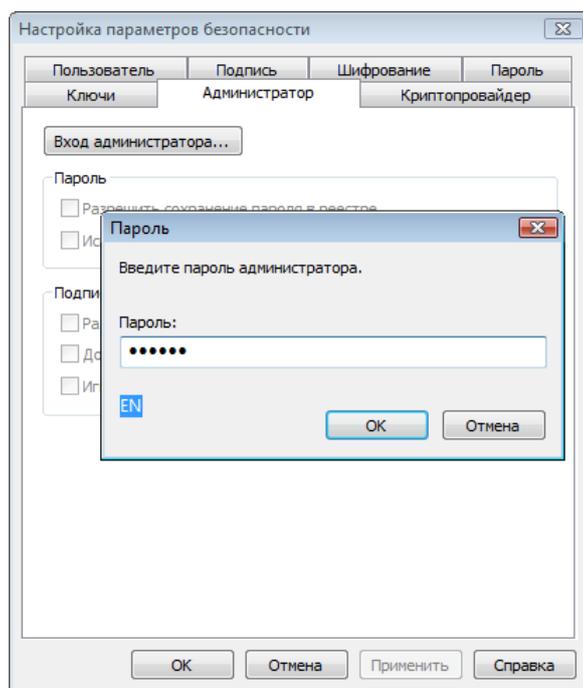


Рисунок 40: Ввод пароля администратора сетевого узла

- 4 Нажмите кнопку **ОК**. Если введен верный пароль, программа будет перезапущена и станут доступны дополнительные настройки.

Дополнительные настройки и возможности «Деловой почты»

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

Если полномочия пользователя в программе «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 «Деловая почта» в качестве администратора (см. «Работа в программе с правами администратора» на стр. 121).

- 2 В окне программы в меню **Инструменты** выберите пункт **Настройка**.
- 3 В окне **Настройка** на левой панели выберите раздел **Администратор**.

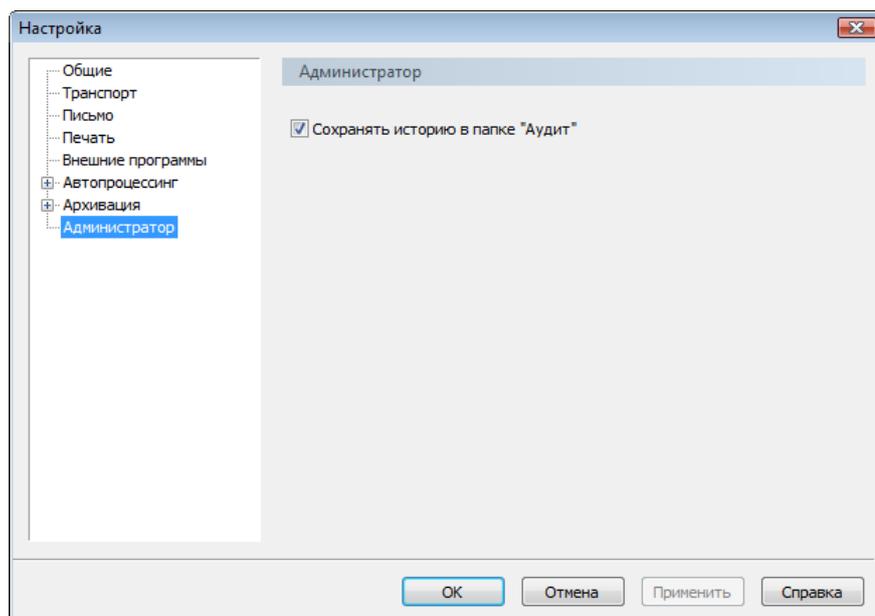


Рисунок 41: Дополнительные настройки в разделе «Администратор»

- 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 настроек в разделе **Администратор**, во время работы с правами администратора сетевого узла доступны следующие настройки 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 «Деловая почта». Если этот флажок установлен, пароль пользователя хранится в реестре Windows и автоматически подставляется в поле ввода пароля при запуске программ ViPNet [Монитор] и ViPNet Client [Деловая почта].



Примечание. Если администратор сети ViPNet, построенной на базе комплекса ViPNet OFFICE, в программе ViPNet Manager на вкладке **Полномочия** установил для данного сетевого узла параметры **Разрешить сохранять пароль** или

Запретить сохранять пароль, то изменить состояние флажка **Разрешить сохранение пароля в реестре** невозможно. Чтобы изменить этот параметр, обратитесь к администратору сети ViPNet.

Для сетей, построенных на базе комплекса ViPNet CUSTOM, такая функциональность не предусмотрена.

- **Использовать цифровой пароль** — если ПО ViPNet установлено на компьютере с сенсорным экраном, который не имеет клавиатуры, эта настройка позволяет использовать для ввода пароля экранную клавиатуру ОС. Если этот флажок установлен, при следующем запуске программы «Деловая почта» будет отображена экранная клавиатура.



Примечание. Данная настройка не имеет никакого действия, если в операционной системе компьютера нет встроенной экранной клавиатуры.

- **Разрешить использование внешних сертификатов** — данная настройка позволяет использовать сертификаты не только из личного хранилища (хранилища программы), но также из хранилища операционной системы.
- **Доверять только спискам сертификатов из ЦУС** — если этот флажок снят, при проверке сертификата поиск корневого сертификата выполняется не только во внутреннем хранилище ПО ViPNet, но и в хранилищах **Доверенные корневые центры сертификации** и **Промежуточные центры сертификации**.
- **Игнорировать отсутствие списков отозванных сертификатов** — этот флажок следует установить, если в системе используются сертификаты, изданные внешними удостоверяющими центрами (вне сети ViPNet), так как в таких сертификатах эта информация может отсутствовать.
-

Изменение режима авторизации пользователя

Режим авторизации определяет, какие данные должен предоставить пользователь для входа в программу «Деловая почта». Чтобы изменить режим авторизации, выполните следующие действия:

- 1 Выполните вход в программу в качестве администратора.

- 2 В окне программы «Деловая почта» в меню **Инструменты** выберите пункт **Настройка параметров безопасности**.
- 3 В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите кнопку **Изменить**.
- 4 В окне **Режим авторизации** выберите из списка один из режимов:
 - **Пароль**. Для входа в программу «Деловая почта» требуется ввести пароль пользователя. Каждый раз после ввода пароля вычисляется парольный ключ, который используется для доступа к персональной ключевой информации пользователя.
 - **Пароль на устройстве**. При выборе этого режима авторизации необходимо подключить внешнее устройство для сохранения парольного ключа пользователя.

Для входа в программу «Деловая почта» пользователь должен обеспечить контакт устройства со считывателем и ввести ПИН-код.
 - **Устройство**. При выборе этого режима авторизации необходимо подключить внешнее устройство для сохранения персональной ключевой информации пользователя.



Примечание. Персональная ключевая информация включает парольный ключ и персональный ключ.

Для входа в программу «Деловая почта» пользователь должен обеспечить контакт устройства со считывателем и ввести ПИН-код (и в некоторых случаях пароль пользователя).

- 5 Выбрав режим авторизации, нажмите **ОК**.
- 6 На вкладке **Ключи** в группе **Авторизация** значения полей **Режим авторизации** и **Тип носителя** изменятся в соответствии с выбранным режимом.



Настройка параметров безопасности

Смена пароля пользователя	127
Настройка параметров шифрования	131
Настройка параметров работы криптопровайдера ViPNet CSP	135
Управление внешними устройствами хранения данных	137

Смена пароля пользователя

Смена текущего пароля пользователя требуется в следующих случаях:

- По истечении срока действия текущего пароля (в случае, если этот срок действия ограничен).
- При поступлении на используемый сетевой узел обновления из программы ViPNet Administrator [УКЦ], содержащего новый пароль пользователя. В этом случае появится окно с сообщением «Рекомендуется сменить пароль пользователя», однако пароль не будет изменен автоматически, поэтому процедуру смены пароля необходимо выполнить вручную.



Примечание. В программе ViPNet Manager смена пароля пользователя функционирующего сетевого узла невозможна.

Для того чтобы сменить пароль пользователя:

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

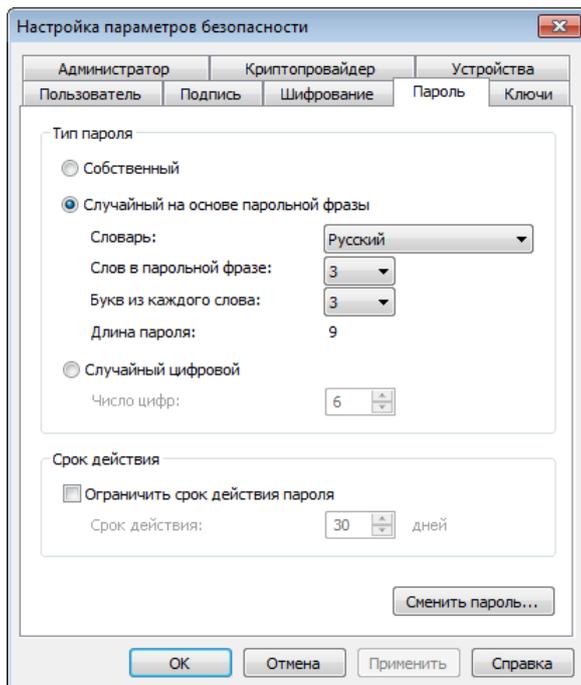


Рисунок 42: Смена текущего пароля пользователя

- 2 В разделе **Тип пароля** выберите тот тип, которому должен соответствовать новый пароль:
 - **Собственный** — пароль, определяемый пользователем (см. «[Выбор собственного пароля](#)» на стр. 128);
 - **Случайный на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы, по заданным параметрам (см. «[Выбор пароля на основе парольной фразы](#)» на стр. 129);
 - **Случайный цифровой** — пароль, формируемый автоматически из заданного числа цифр (см. «[Выбор цифрового пароля](#)» на стр. 130).
- 3 При необходимости ограничения срока действия нового пароля установите флажок **Ограничить срок действия пароля**, после чего укажите желаемое число дней.

Выбор собственного пароля

Для того чтобы сменить текущий пароль пользователя на собственный:

- 1 На вкладке **Пароль** (см. Рисунок 42 на стр. 128) выберите **Собственный**.

- 2 Нажмите кнопку **Сменить пароль**.
- 3 При появлении электронной рулетки поведите указателем в пределах окна.



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

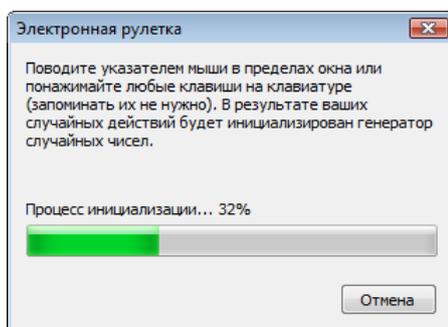


Рисунок 43: Электронная рулетка

- 4 В окне **Смена пароля** введите новый пароль (длиной не менее 6-ти символов) поочередно в каждом из полей, учитывая регистр и раскладку клавиатуры.
После этого нажмите кнопку **ОК**.

Теперь при запуске программы ViPNet Client [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 42 на стр. 128) 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 будет пароль.
 - В списке **Букв из каждого слова** выберите число начальных букв каждого слова (3 или 4), которые войдут в пароль.

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

- 2 Нажмите кнопку **Сменить пароль**.
- 3 Запомните пароль и (или) парольную фразу, отображенную в окне **Смена пароля**.
При необходимости измените парольную фразу и пароль на другие, также соответствующие указанным параметрам, с помощью кнопки **Другой пароль**.
После этого нажмите кнопку **ОК**.

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

Выбор цифрового пароля

Для того чтобы сменить текущий пароль пользователя на цифровой (ПИН-код):

- 1 На вкладке **Пароль** выберите **Случайный цифровой**, после чего в поле **Число цифр** укажите длину пароля.
- 2 Нажмите кнопку **Сменить пароль**.
- 3 Запомните ПИН-код, отображенный в окне **Смена пароля**.
При необходимости измените этот ПИН-код на другой, также содержащий указанное число цифр, с помощью кнопки **Другой ПИН-код**.
После этого нажмите кнопку **ОК**.

Теперь при запуске программы ViPNet Client [Деловая почта] от имени того же пользователя следует вводить предложенный ПИН-код.

Настройка параметров шифрования

Для настройки параметров шифрования:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Шифрование**.

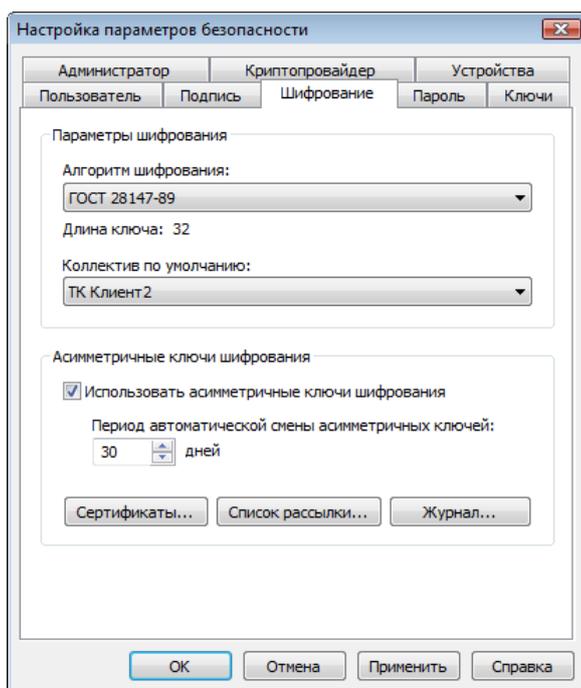


Рисунок 44: Настройка параметров шифрования

- 3 В разделе **Параметры шифрования** измените, при необходимости, используемые параметры шифрования:
 - в списке **Алгоритм шифрования** выберите алгоритм ГОСТ или AES (по умолчанию ГОСТ);
 - в списке **Коллектив по умолчанию** выберите тот коллектив, от имени которого необходимо осуществлять шифрование в случае, если коллектив отправителя сообщения невозможно однозначно определить по получателю.
- 4 При необходимости, перейдите на использование асимметричных ключей шифрования (см. «[Задание параметров шифрования с использованием асимметричных ключей](#)» на стр. 132).

Задание параметров шифрования с использованием асимметричных ключей

Внимание! Использование асимметричных ключей шифрования доступно при выполнении следующих условий:



- используемый абонентский пункт не является Центром управления сетью или Удостоверяющим и ключевым центром;
 - пользователь, от имени которого выполнен запуск программы ViPNet Client [Деловая почта], обладает правом подписи.
-

Для перехода на использование асимметричных ключей и задания параметров шифрования с использованием асимметричных ключей, на вашем абонентском пункте, а также на всех тех абонентских пунктах, обмен информацией с которыми необходимо организовать с использованием асимметричных ключей, выполните следующее:

- 1 В настройках модуля ViPNet [MFTP] выберите тип канала **Через сервер** (см. документ «ViPNet [MFTP]. Руководство пользователя»).
- 2 Вызовите окно **Настройка параметров безопасности**, после чего откройте вкладку **Шифрование** (см. Рисунок 44 на стр. 131).
- 3 В разделе **Асимметричные ключи шифрования** установите флажок **Использовать асимметричные ключи шифрования**, после чего в поле **Период автоматической смены асимметричных ключей шифрования** задайте число суток, по истечении которого будет выполняться автоматическая смена асимметричных ключей.



Примечание. Если флажок **Использовать асимметричные ключи шифрования** будет снят, данный абонентский пункт не сможет устанавливать новые соединения на основе асимметричных ключей. Асимметричные ключи будут использовать для обмена информацией только с теми абонентскими пунктами, с которыми он был настроен ранее.

- 4 Нажмите кнопку **Применить**.
- 5 Нажмите кнопку **Список рассылки**, после чего в появившемся окне **Список рассылки АКШ** выберите с помощью флажков те абонентские пункты, обмен информацией с которыми необходимо организовать с использованием асимметричных ключей.



Примечание. Если для обмена информацией с тем или иным абонентским пунктом необходимо вновь использовать симметричные ключи, следует в окне **Список рассылки АКШ** снять соответствующий флажок.

- 6 В окне подтверждения рассылки асимметричных ключей нажмите кнопку **ОК**.
- 7 В окне **Список рассылки АКШ** нажмите кнопку **ОК**.
- 8 При необходимости просмотра сертификатов асимметричных ключей для каждого из коллективов используемого абонентского пункта на вкладке **Шифрование** нажмите кнопку **Сертификаты**.
Откроется окно **Сертификаты АКШ** с информацией об этих сертификатах.
- 9 При необходимости просмотра журнала событий, связанных с асимметричными ключами, на вкладке **Шифрование** нажмите кнопку **Журнал событий** (см. [«Просмотр журнала событий, связанных с асимметричными ключами»](#) на стр. 133).
- 10 По завершении настройки параметров использования асимметричных ключей на вкладке **Шифрование** нажмите кнопку **ОК**.

Просмотр журнала событий, связанных с асимметричными ключами

Для просмотра журнала событий, связанных с асимметричными ключами:

- 1 В окне **Настройка параметров безопасности** на вкладке **Шифрование** (см. Рисунок 44 на стр. 131) нажмите кнопку **Журнал событий**.

Откроется окно **Просмотр журналов**.

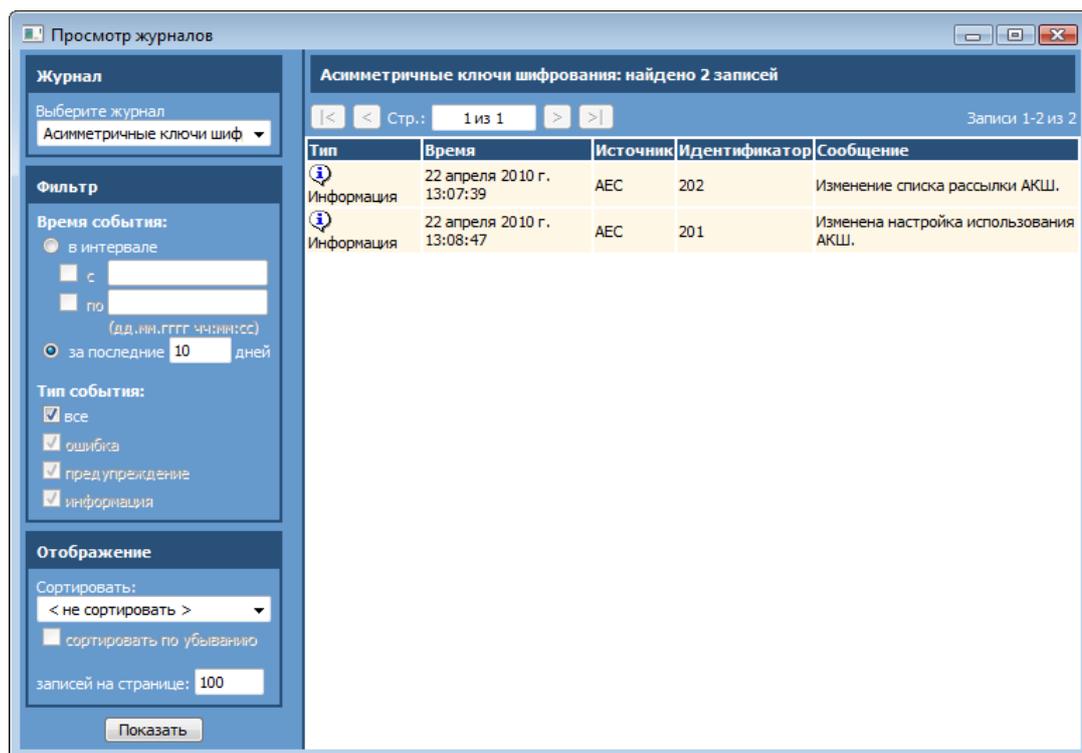


Рисунок 45: Просмотр журнала событий, связанных с асимметричными ключами

2 В окне **Просмотр журналов** на левой панели задайте значения параметров фильтрации событий:

- по времени регистрации,
- по типу.

После этого нажмите кнопку **Показать**. На правой панели отобразятся события, соответствующие заданным параметрам фильтрации.

3 При необходимости просмотра подробной информации о том или ином событии выберите это событие двойным щелчком мыши.

Откроется окно **Информация о событии**.

Настройка параметров работы криптопровайдера ViPNet CSP

Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций через интерфейс Microsoft CryptoAPI 2.0. Это позволяет вызывать криптографические функции из различных приложений Microsoft и другого ПО, использующего данный интерфейс.

Для настройки параметров работы с криптопровайдером ViPNet CSP:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Криптопровайдер**.

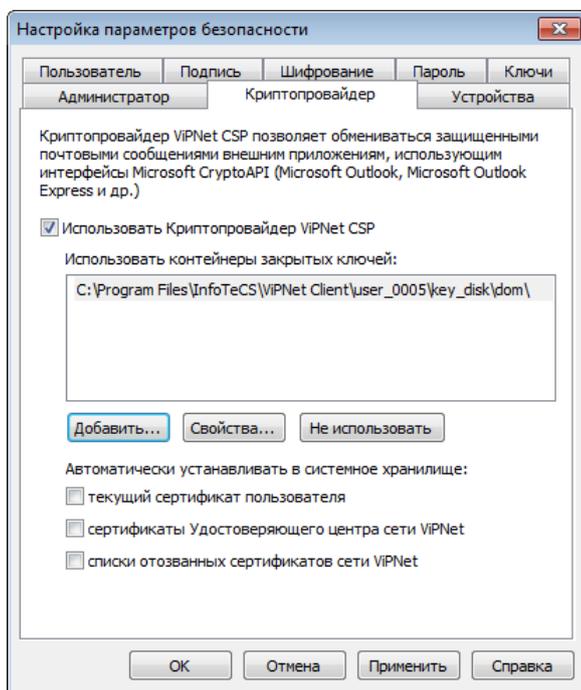


Рисунок 46: Настройка параметров работы с криптопровайдером ViPNet CSP

- 3 Убедитесь в том, что установлен флажок **Использовать Криптопровайдер ViPNet CSP**.
- 4 Добавьте контейнер закрытых ключей, который будет использоваться криптопровайдером, с помощью кнопки **Добавить**.

- 5 В окне **ViPNet CSP – инициализация контейнера ключа** укажите расположение контейнера закрытого ключа:
- папку на диске,
 - устройство с указанием его параметров.



Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).



Внимание! В случае, если на выбранном устройстве хранятся ключи, сформированные в ПО ViPNet версии ниже 3.1.X, появится окно программы **Конвертер ключей ViPNet** с предложением конвертировать ключи в новый формат. Подробная информация о работе с программой **Конвертер ключей ViPNet** содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).

После этого нажмите кнопку **ОК**. Полный путь к выбранному контейнеру отобразится в списке **Использовать контейнеры закрытых ключей**.

- 6 При дальнейшей работе с контейнером:
- Для просмотра и (или) изменения свойств контейнера закрытого ключа нажмите кнопку **Свойства** (см. «[Работа с контейнером закрытого ключа](#)» на стр. 179).
 - Для удаления контейнера из списка контейнеров, используемых криптопровайдером, нажмите кнопку **Не использовать**.
- 7 Выберите сертификаты, которые, в случае их отсутствия в хранилище программы, необходимо устанавливать в это хранилище автоматически (см. «[Установка в хранилище автоматически](#)» на стр. 159):
- **текущий сертификат пользователя;**
 - **сертификаты Удостоверяющего центра сети ViPNet;**
 - **списки отозванных сертификатов сети ViPNet.**
- 8 Нажмите кнопку **Применить** и (или) **ОК**.

Управление внешними устройствами хранения данных

Управление внешними устройствами хранения данных упрощает работу с контейнерами закрытых ключей, которые хранятся на этих устройствах (см. «[Работа с контейнером закрытого ключа](#)» на стр. 179), — например, установку нового контейнера или перенос контейнера на устройство с помощью окна **ViPNet CSP – инициализация контейнера ключа** (см. Рисунок 79 на стр. 184).

Для управления внешними устройствами:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 Откройте вкладку **Устройства**.

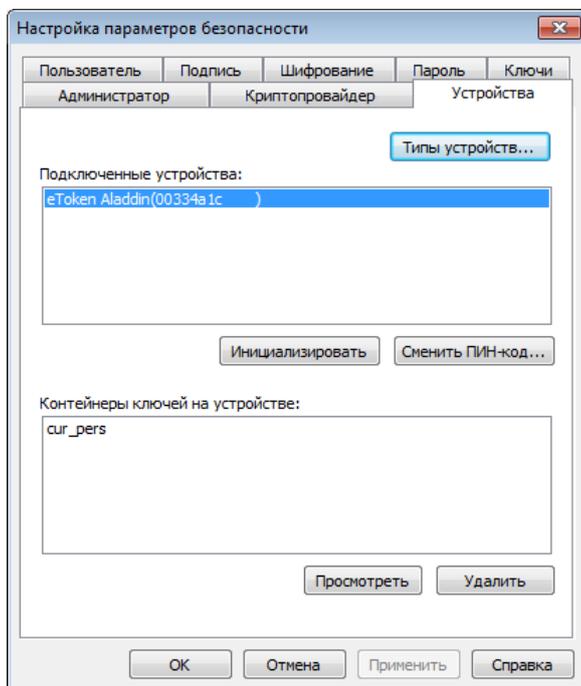


Рисунок 47: Управление внешними устройствами хранения данных

- 3 Подключите нужные устройства.



Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).

Наименования подключенных устройств отобразятся в списке **Подключенные устройства**, а наименования контейнеров закрытых ключей, которые хранятся на выбранном устройстве, — в списке **Контейнеры ключей на устройстве**.

- 4 Задайте типы устройств, на которых необходимо выполнять поиск контейнеров закрытых ключей, с помощью кнопки **Типы устройств**.
В появившемся окне **Настройка списка опрашиваемых устройств** выберите типы устройств с помощью флажков, после чего нажмите кнопку **ОК**.
- 5 Инициализируйте подключенное устройство (см. [«Инициализация устройства»](#) на стр. 138).
- 6 При необходимости измените ПИН-код администратора и (или) ПИН-код пользователя для подключенного устройства (см. [«Смена ПИН-кода устройства»](#) на стр. 140).
- 7 При необходимости просмотрите и (или) измените свойства контейнера закрытого ключа, который хранится на подключенном устройстве, с помощью кнопки **Просмотреть** (см. [«Работа с контейнером закрытого ключа»](#) на стр. 179).
- 8 Если контейнер, который хранится на подключенном устройстве, не нужно использовать для авторизации в ПО ViPNet, удалите этот контейнер с помощью кнопки **Удалить**.

Инициализация устройства

Для инициализации подключенного устройства:

- 1 Убедитесь в том, что устройство, которое необходимо инициализировать, не содержит ценной информации. При необходимости перенесите все данные, хранящиеся на устройстве, на другой съемный носитель или жесткий диск компьютера.
- 2 На вкладке **Устройства** (см. Рисунок 47 на стр. 137) в списке **Подключенные устройства** выберите нужное устройство.



Внимание! В случае, если на выбранном устройстве хранятся ключи, сформированные в ПО ViPNet версии ниже 3.1.X, появится окно программы **Конвертер ключей ViPNet** с предложением конвертировать ключи в новый формат. Подробная информация о работе с программой **Конвертер ключей ViPNet** содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).

- 3 Нажмите кнопку **Инициализировать**.



Внимание! В процессе инициализации выполняется форматирование устройства. Все данные, хранящиеся на устройстве, удаляются.

- 4 В окне с предупреждением об удалении данных с устройства нажмите кнопку **Да**.
- 5 В появившемся окне **Инициализация** введите ПИН-код администратора.
- 6 При необходимости смены ПИН-кода пользователя введите в двух других полях окна также новый ПИН-код пользователя.
- 7 После этого нажмите кнопку **ОК**.



Внимание! В случае, если вы используете устройство ОКБ САПР Шипка (Shipka) и произвели инициализацию в приложении ViPNet, для корректной работы устройства вам так же необходимо выполнить инициализацию с помощью утилиты ОКБ САПР «Параметры авторизации» (см. [«Информация о внешних устройствах хранения данных»](#) на стр. 11).

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

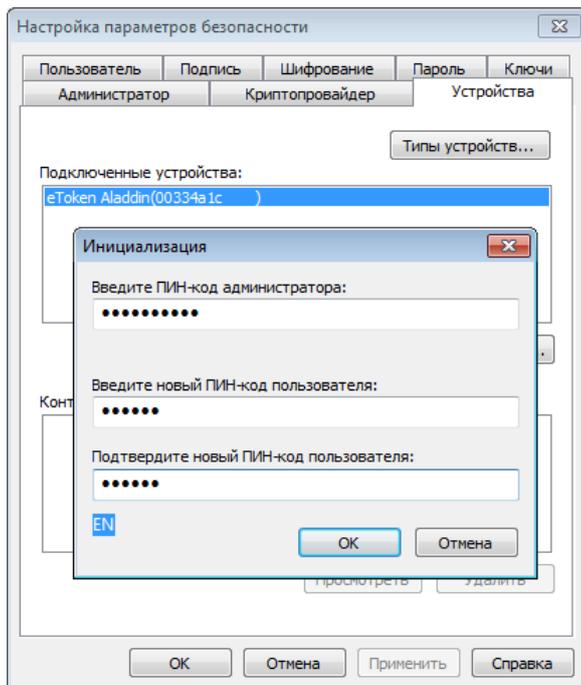


Рисунок 48: Инициализация устройства

Смена ПИН-кода устройства

Для того чтобы сменить ПИН-код администратора и (или) ПИН-код пользователя (в зависимости от уровня полномочий на доступ к устройству) для подключенного устройства:

- 1 Нажмите кнопку **Смена ПИН-кода**.
- 2 В окне **Смена ПИН-кода** выберите тип изменяемого ПИН-кода.

- 3 В поле **Введите старый ПИН-код** укажите прежний ПИН-код, а в оставшихся двух полях — новый ПИН-код, после чего нажмите кнопку **ОК**.

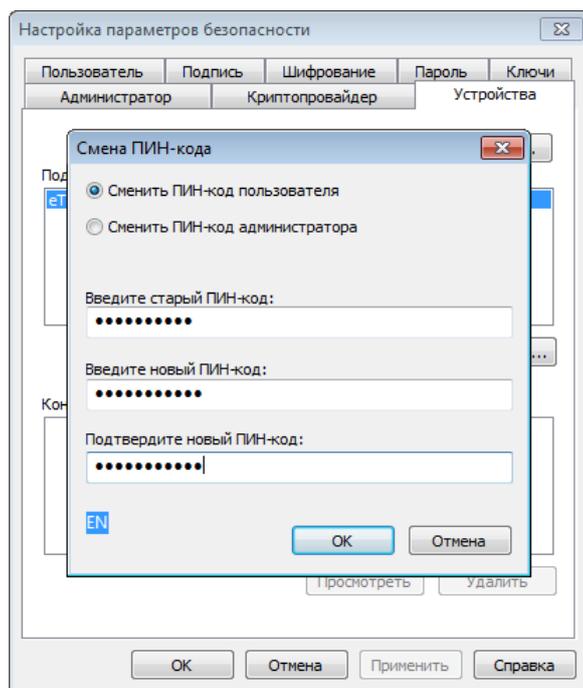


Рисунок 49: Смена ПИН-кода устройства



8

Работа с сертификатами

Общие сведения о сертификатах открытых ключей	143
Просмотр сертификатов	154
Установка сертификатов в хранилище	159
Экспорт сертификата	164
Управление сертификатами	166
Работа с контейнером закрытого ключа	179

Общие сведения о сертификатах открытых ключей

Определение и назначение

Сертификат открытого ключа (далее — сертификат) является цифровым документом, который подтверждает личность владельца открытого ключа электронной цифровой подписи. Сертификат содержит информацию, которая идентифицирует субъекта (владельца открытого ключа), а также другие вспомогательные данные. Сертификат издается полномочной организацией — Удостоверяющим центром (согласно Федеральному закону № 1 «Об электронной цифровой подписи» от 10.01.2002 г.). Удостоверяющий центр гарантирует подлинность информации, указанной в сертификате, в течение срока действия сертификата.

Сертификаты поддерживают механизм криптографии с открытым ключом — сертификат содержит открытый ключ того субъекта, который определен в сертификате. Сертификат открытого ключа используется для идентификации субъекта и уточнения операций, которые субъекту разрешается совершать с использованием закрытого ключа, соответствующего открытому ключу, удостоверяемому данным сертификатом. Для криптографии с открытым ключом важно, что сертификат обеспечивает хранение и распространение открытого ключа субъекта и подтверждает, что этот ключ действителен. Пользователь А получает открытый ключ пользователя В из сертификата пользователя В. Пользователь А видит, что сертификат действителен, так как издан доверенным Удостоверяющим центром.

Удостоверяющий центр, являющийся издателем сертификата, подписывает издаваемый сертификат собственным закрытым ключом. Таким образом, чтобы подтвердить подлинность того или иного сертификата, пользователю необходим сертификат издателя (корневой сертификат).

Структура

Чтобы сертификат можно было использовать, он должен обладать доступной универсальной структурой, позволяющей извлечь из него нужную информацию и легко ее понять. Например, благодаря тому, что паспорта имеют простую однотипную структуру, можно легко понять информацию, изложенную в паспорте любого государства, даже если вы никогда не видели раньше таких паспортов. Так же дело

обстоит и с сертификатами: стандартизация форматов сертификатов позволяет читать и понимать их независимо от того, кем они были изданы.

Один из форматов сертификата открытого ключа определен в рекомендациях Международного Союза по телекоммуникациям (International Telecommunications 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 т. д.).

Сертификат содержит элементы данных, сопровождаемые цифровой 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 субъекта,
- имя издателя,
- период действия,
- открытый ключ субъекта,
- имя субъекта сертификата.



Примечание. Под субъектом понимается сторона, контролирующая закрытый ключ, соответствующий данному открытому ключу. Субъектом сертификата может быть конечный пользователь или Удостоверяющий центр.

К необязательным полям относятся:

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



Рисунок 50: Структура сертификата, соответствующего стандарту X.509 версии 3

Сертификат ключа подписи

Кому выдан: TDC, Alena V. Laskarzhetskaya
 Кем выдан: Lidiya V. Rodkina (adm)
 Действителен с 4 февраля 2010 г. по 4 февраля 2015 г.

Назначение:

- Подтверждает удаленному компьютеру идентификацию Вашего компьютера.
- Защищает сообщения электронной почты.

Версия: V3
 Серийный номер: 01 CA A5 89 9F 85 5B 20 00 00 04 B1 10 E1 07 BC
 Алгоритм подписи: ГОСТ Р 34.10/34.11-2001
 Издатель: Имя: Lidiya V. Rodkina (adm)
 Должность: Администратор
 Подразделение: Удостоверяющий и Ключевой центр
 Организация: Infotecs, TDC

Действителен с: 4 февраля 2010 г. 15:03:03 (GMT+04:00)
 Действителен по: 4 февраля 2015 г. 15:03:03 (GMT+04:00)
 Владелец: Имя: TDC, Alena V. Laskarzhetskaya
 Организация: Infotecs, TDC

Открытый ключ: ГОСТ Р 34.10-2001 (512 бит)
 04 40 26 52 F7 BF 65 7C AA 53 E4 9F 74 9C BB 66
 D1 13 7C 80 F7 42 B2 D7 52 60 9B AD 6C EB FB CE
 1E 4D 46 57 D3 70 D1 05 FB BC A2 0D D4 71 93 47
 16 61 75 9C DC 7A BC 9E 57 9A 8D 3E 85 B0 57 A8
 BE B3

Расширения сертификата X.509

Использование ключа: Цифровая 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 субъекта: 95 65 BE D6 15 A5 65 00 3D F8 A0 CB 47 CA 04 16 E9 10 C0 C1

Срок действия закрытого ключа: С 4 февраля 2010 г. 15:03:03 (GMT+04:00)
 по 4 февраля 2011 г. 15:03:03 (GMT+04:00)

Идентификатор ключа центра сертификатов: Идентификатор ключа=40 72 76 98 C8 37 45 D2 D6 77 E8 C3 34 F4
 2A 65 AC 48 10 E8

Основные ограничения: Тип субъекта=Пользователь

Результат проверки сертификата
 Сертификат действителен.
 Проверен 26 июля 2010 г. 11:57:39 (GMT+04:00).

Рисунок 51: Пример сертификата ViPNet, соответствующего стандарту X.509 версии 3

Роль PKI для криптографии с открытым ключом

Для сертификатов требуется инфраструктура, которая позволяла бы управлять ими в той среде, в которой эти сертификаты предполагается использовать. Технология управления сертификатами должна учитывать природу сертификатов открытых ключей, которые предназначены для широкого распространения. Одной из реализаций такой инфраструктуры, позволяющей проверить подлинность электронной цифровой подписи документа, является технология PKI (Public Key Infrastructure — инфраструктура открытых ключей). PKI обслуживает жизненный цикл сертификата: издание

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

Кроме того, PKI позволяет осуществлять проверку подлинности и действительности сертификатов.

Для защиты электронных документов может потребоваться доступ к открытым ключам как отправителей, так и получателей сообщений. Поскольку эта информация содержится в сертификате, для организации защиты электронных документов важна доступность сертификатов пользователей. PKI предоставляет доступ к сертификатам — сертификаты хранятся в общедоступной папке, откуда приложения могут их извлекать по мере необходимости. Таким образом PKI решает проблему обмена ключами вручную.

Как сказано выше, подлинность сертификата гарантируется Удостоверяющим центром, который подписывает сертификат своим открытым ключом. Проверка подлинности сертификата подразумевает проверку цифровой подписи Удостоверяющего центра. PKI упрощает эту проверку.

Ни один из методов защиты не является совершенным. Цифровой сертификат может быть скомпрометирован — например, вследствие утери закрытого ключа. Чтобы цифровые сертификаты по-прежнему могли обеспечивать доверие, предусмотрен механизм аннулирования, или отзыва, сертификатов до истечения срока их действия.

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 (для однократного использования в рамках данного сеанса).
- 4 Подписанный документ зашифровывается с использованием сеансового ключа.
- 5 Сеансовый ключ зашифровывается с использованием открытого ключа получателя.
- 6 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

7 Документ отправляется.

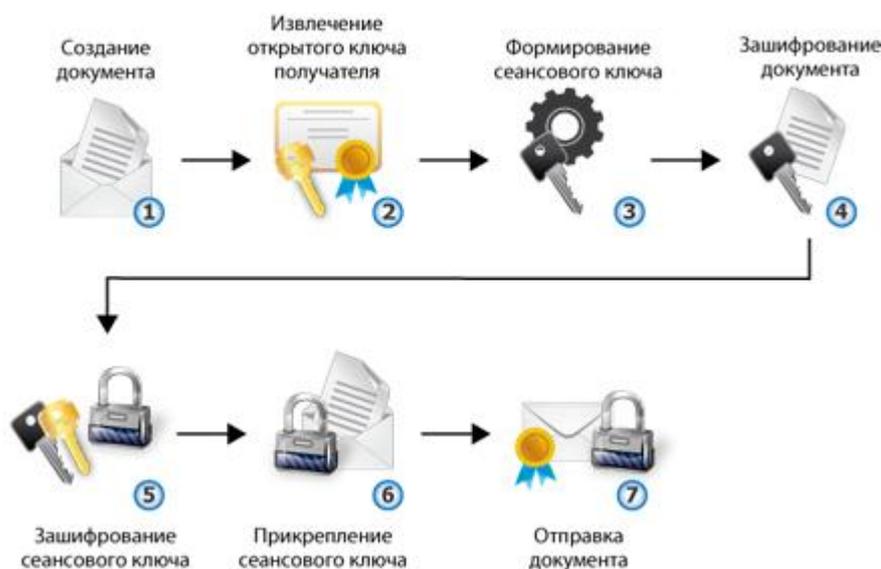


Рисунок 52: Процесс зашифрования электронных документов

Расшифрование

- 1 Пользователь получает электронный документ.
- 2 Зашифрованное содержимое документа и зашифрованный сеансовый ключ извлекаются из документа.
- 3 Закрытый ключ получателя документа извлекается из ключевого контейнера.
- 4 Сеансовый ключ расшифровывается с использованием закрытого ключа получателя.
- 5 Документ расшифровывается с использованием расшифрованного сеансового ключа.
- 6 Расшифрованный документ доступен получателю.



Рисунок 53: Процесс расшифровки электронных документов

Использование сертификатов для подписания электронных документов

Когда отправитель подписывает документ, он использует закрытый ключ, соответствующий открытому ключу, который хранится в сертификате. Когда получатель проверяет электронную цифровую подпись (ЭЦП) сообщения, он извлекает открытый ключ из сертификата отправителя.

Подписание

- 1 Пользователь создает электронный документ.
- 2 Вычисляется хэш-сумма документа.
- 3 Закрытый ключ отправителя извлекается из ключевого контейнера.
- 4 С использованием закрытого ключа отправителя на основе хэш-суммы формируется ЭЦП.
- 5 ЭЦП прикрепляется к документу.
- 6 Зашифрованный документ отправляется.



Рисунок 54: Процесс подписания электронного документа

Проверка подписи

- 1 Пользователь получает электронный документ.
- 2 ЭЦП (зашифрованная хэш-сумма) извлекается из документа.
- 3 Вычисляется хэш-сумма документа.
- 4 Открытый ключ отправителя извлекается из сертификата отправителя.
- 5 ЭЦП расшифровывается с использованием открытого ключа отправителя.
- 6 Хэш-сумма ЭЦП сравнивается с полученной хэш-суммой документа.
- 7 Если значения хэш-сумм совпадают, ЭЦП документа считается действительной.

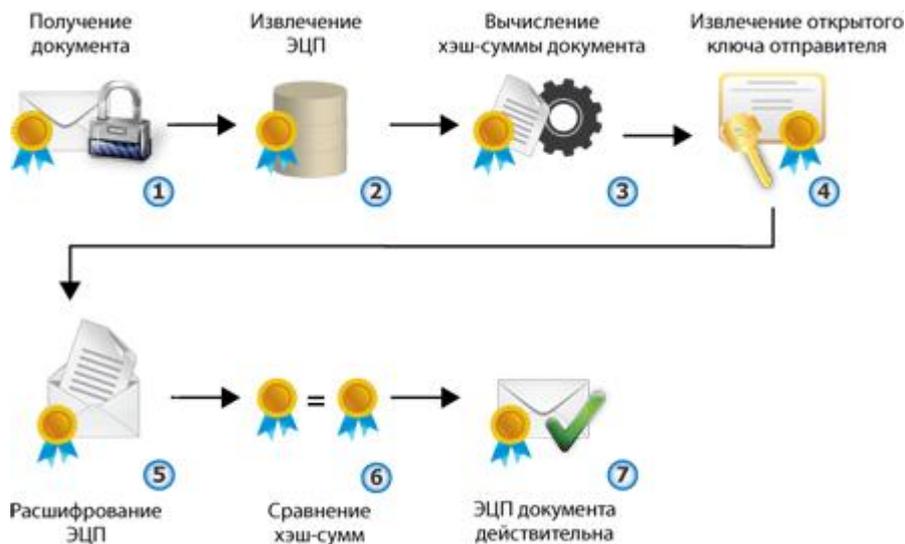


Рисунок 55: Процесс проверки подписи

Использование сертификатов для подписания и шифрования электронных документов

Подписание и зашифрование

- 1 Пользователь создает электронный документ.
- 2 Вычисляется хэш-сумма документа.
- 3 Закрытый ключ отправителя извлекается из ключевого контейнера.
- 4 Открытый ключ получателя извлекается из сертификата получателя.
- 5 С использованием закрытого ключа отправителя на основе хэш-суммы формируется ЭЦП.
- 6 ЭЦП прикрепляется к документу.
- 7 Формируется симметричный сеансовый ключ (для однократного использования в рамках данного сеанса).
- 8 Подписанный документ зашифровывается с использованием сеансового ключа.
- 9 Сеансовый ключ зашифровывается с использованием открытого ключа получателя.
- 10 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

11 Документ отправляется.

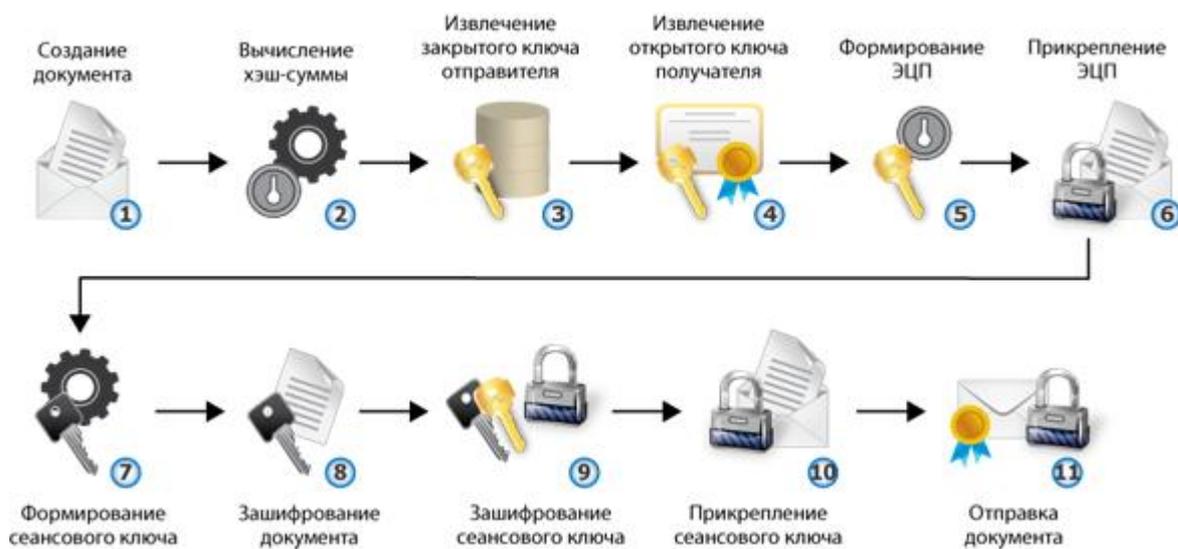


Рисунок 56: Процесс подписания и зашифрования электронных документов

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 ключевого контейнера.
- 4 Сеансовый ключ расшифровывается с помощью закрытого ключа получателя.
- 5 Документ расшифровывается с использованием расшифрованного сеансового ключа.
- 6 ЭЦП (зашифрованная хэш-сумма) извлекается из документа.
- 7 Вычисляется хэш-сумма документа.
- 8 Открытый ключ отправителя извлекается из сертификата отправителя.
- 9 ЭЦП расшифровывается с использованием открытого ключа отправителя.
- 10 Хэш-сумма ЭЦП сравнивается с полученной хэш-суммой документа.
- 11 Если значения хэш-сумм совпадают, ЭЦП документа считается действительной.
- 12 Расшифрованный документ доступен получателю.

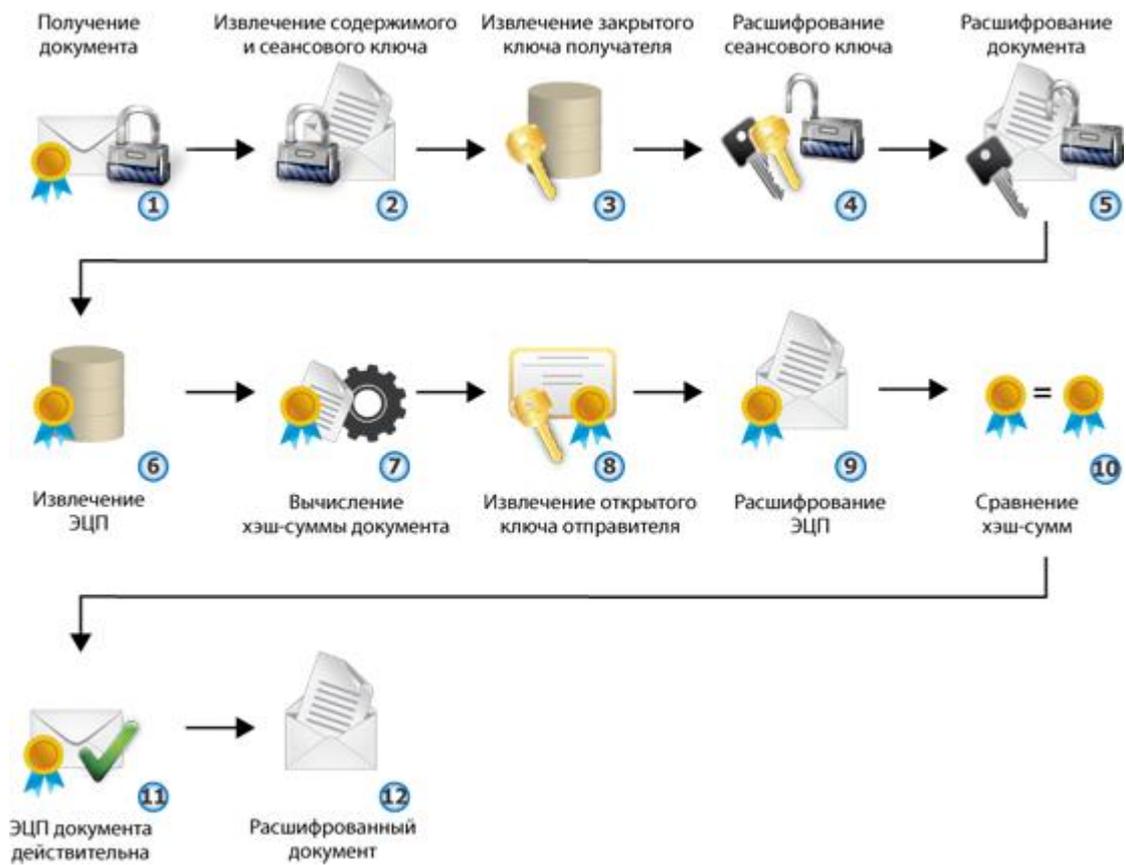


Рисунок 57: Процесс расшифрования и проверки электронного документа

Просмотр сертификатов

В программе ViPNet Client [Деловая почта] можно просматривать следующие типы сертификатов:

- текущий сертификат пользователя (см. [«Просмотр текущего сертификата пользователя»](#) на стр. 155),
- личные сертификаты пользователя (см. [«Просмотр личных сертификатов пользователя»](#) на стр. 155),
- доверенные корневые сертификаты (см. [«Просмотр доверенных корневых сертификатов»](#) на стр. 156),
- изданные сертификаты (см. [«Просмотр изданных сертификатов»](#) на стр. 156).

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

- назначение сертификата;
- имя субъекта (владельца открытого ключа), которому выдан сертификат;
- имя издателя сертификата;
- срок действия сертификата;
- срок действия закрытого ключа, соответствующего данному сертификату;
- информация о политиках применения сертификата, отображаемая при нажатии кнопки **Заявление издателя**.



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

В сертификате пользователя сети ViPNet OFFICE кнопка **Заявление издателя** всегда недоступна.

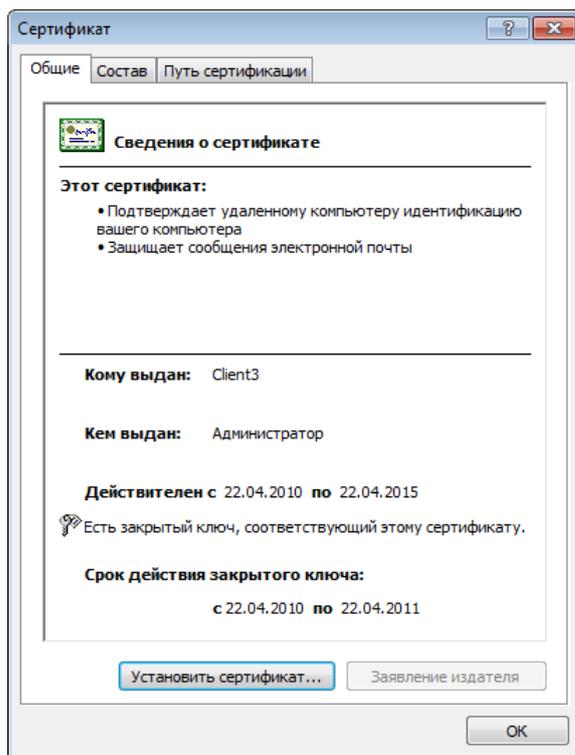


Рисунок 58: Просмотр основной информации о сертификате

Просмотр текущего сертификата пользователя

Для просмотра текущего сертификата пользователя:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Подробнее**.

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

Просмотр личных сертификатов пользователя

Для просмотра личных сертификатов пользователя:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.

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

Откроется окно **Менеджер сертификатов** с информацией обо всех личных сертификатах пользователя, а также о сертификатах, установленных в хранилище операционной системы. Все данные сертификаты введены в действие. Один из сертификатов является текущим, о чем в столбце **Статус** свидетельствует сообщение **Текущий**.



Примечание. Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование внешних сертификатов** (см. «[Дополнительные настройки параметров безопасности](#)» на стр. 123).

- 3 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или выполните двойной щелчок мыши для этого сертификата.

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

Просмотр доверенных корневых сертификатов

Для просмотра доверенных корневых сертификатов:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Сертификаты**.
- 3 В окне **Менеджер сертификатов** откройте вкладку **Доверенные корневые сертификаты**.
- 4 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или выполните двойной щелчок мыши для этого сертификата.

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

Просмотр изданных сертификатов

Для просмотра изданных сертификатов:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Изданные сертификаты**.

Откроется окно **Менеджер сертификатов** с информацией о сертификатах, которые изданы в программе ViPNet Administrator [УКЦ] или ViPNet Manager по запросам на обновление сертификата, но еще не введены в действие.
- 3 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или выполните двойной щелчок мыши для этого сертификата.

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

Просмотр цепочки сертификации

Для просмотра цепочки сертификации 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 Выберите группу полей в выпадающем списке **Показать**:

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



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

- **Только критические расширения** — только те расширения, которые признаны издателем критическими;
 - **Только свойства** — параметры, которые не являются полями сертификата, но присваиваются сертификату при хранении его в системном хранилище используемой рабочей станции.
- 4** Выберите в таблице нужное поле, после чего в нижней части окна ознакомьтесь с содержимым этого поля.

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

Установка сертификатов в хранилище

Установка сертификатов в хранилище (хранилище программы ViPNet Client [Деловая почта] или хранилище операционной системы) позволяет использовать сертификаты во внешних приложениях (таких как Windows Live Mail, MS Outlook, MS Word и др.).

Установку можно выполнить автоматически или вручную.



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

Установка в хранилище автоматически

Установка сертификатов запускается автоматически при соблюдении следующих двух условий:

- сертификаты (текущий сертификат пользователя, корневой сертификат и списки отозванных сертификатов) отсутствуют в хранилище;
- в окне **Настройка параметров безопасности** на вкладке **Криптопровайдер** (см. **Рисунок 46 на стр. 135**) сняты флажки раздела **Автоматически устанавливать в системное хранилище** (см. рисунок на стр. **Error! Bookmark not defined.**).



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

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

Для автоматической установки корневого сертификата:

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

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



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

- если необходимо выполнить автоматическую установку корневого сертификата, нажмите кнопку **ОК**.

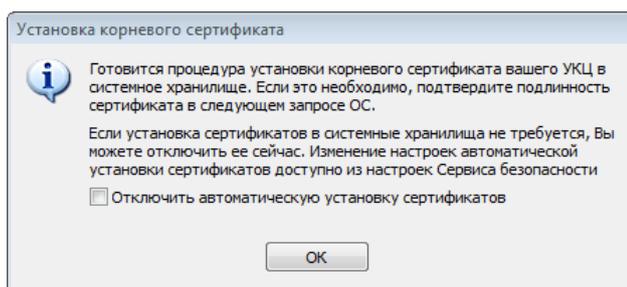


Рисунок 59: Установка корневого сертификата

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

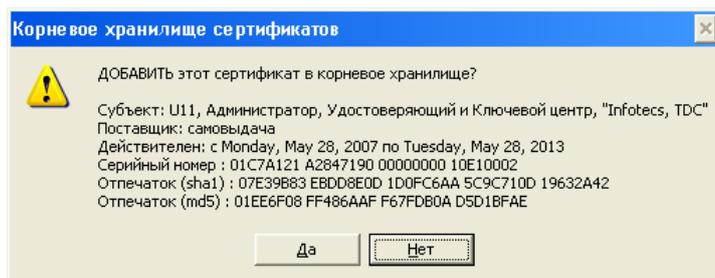


Рисунок 60: Подтверждение подлинности корневого сертификата

Корневой сертификат установлен в хранилище сертификатов текущего пользователя.

Установка в хранилище вручную

Для работы с защищенными документами и соединениями необходим закрытый ключ и соответствующий ему сертификат. Установка ключа и сертификата может выполняться

путем установки одного контейнера или путем установки сертификата и контейнера закрытого ключа по отдельности.

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



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

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

Для установки сертификата в хранилище пользователя:

- 1 Вызовите окно **Сертификаты** для того сертификата, который необходимо установить в хранилище (см. «[Просмотр сертификатов](#)» на стр. 154).
- 2 Нажмите кнопку **Установить сертификат**.
- 3 На странице приветствия мастера установки сертификатов нажмите кнопку **Далее**.
- 4 На странице **Выбор хранилища сертификатов** укажите, в какое хранилище будет установлен ваш сертификат, и нажмите кнопку **Далее**.

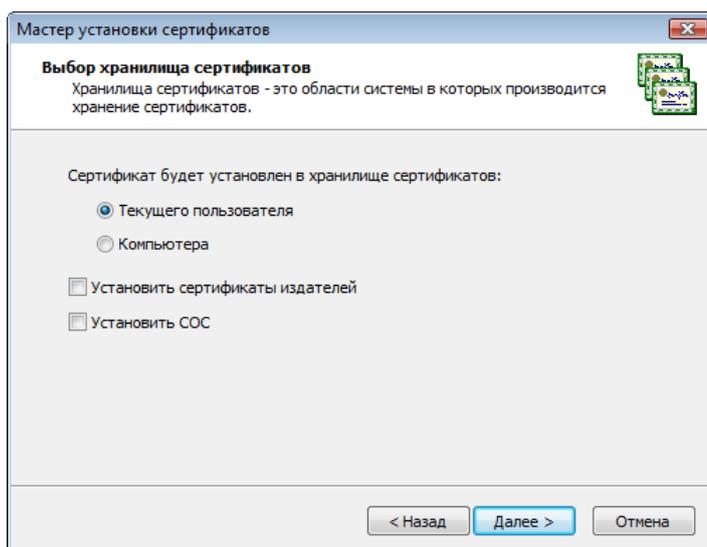


Рисунок 61: Выбор хранилища сертификатов

Примечание. Сертификат следует устанавливать в хранилище текущего пользователя для целей шифрования, расшифрования и подписания файлов, а также для доступа к защищенным ресурсам через браузер.



Для продукта ViPNet CSP сертификат следует устанавливать в хранилище компьютера при использовании ViPNet CSP на web-сервере для организации доступа к защищенным ресурсам.

Для продукта ViPNet CUSTOM сертификат следует устанавливать в хранилище компьютера в том случае, если сертификат необходим только для проверки ЭЦП и расшифрования файлов.

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.

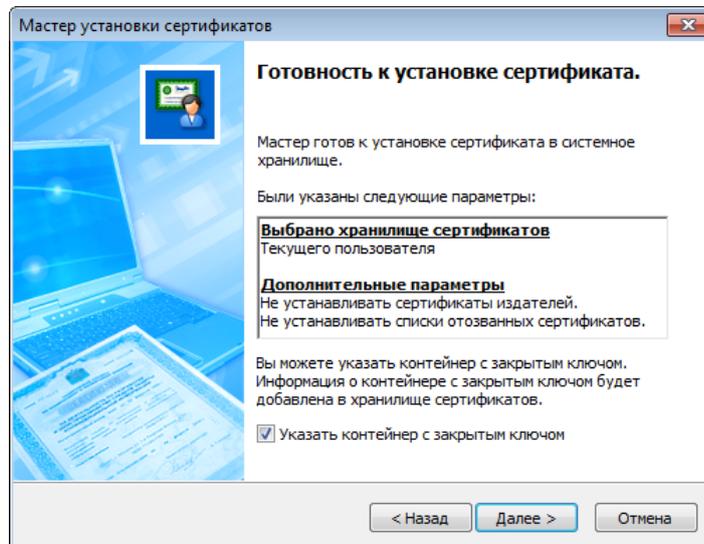


Рисунок 62: Страница **Готовность к установке сертификата**

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



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

- Нажмите кнопку **Далее**.
- 6** Если флажок **Указать контейнер с закрытым ключом** установлен и контейнер не найден либо недоступен, в появившемся окне **ViPNet CSP – инициализация контейнера ключа** укажите расположение контейнера закрытого ключа:
- папку на диске;
 - устройство с указанием его параметров и ПИН-кода.



Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).

После этого нажмите кнопку **ОК**.

- 7** В окне с сообщением «Вы желаете сохранить сертификат в контейнере с закрытым ключом?» нажмите **Да**, чтобы добавить сертификат в контейнер закрытого ключа, или **Нет**, чтобы оставить сертификат в виде отдельного файла.



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

- 8** Если флажок **Указать контейнер с закрытым ключом** установлен и контейнер доступен, в появившемся окне **ViPNet CSP – пароль контейнера ключа** в поле **Пароль** введите пароль доступа к контейнеру, после чего нажмите кнопку **ОК**.



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

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

Экспорт сертификата

Для экспорта сертификата в файл определенного формата:

- 1 Вызовите окно **Сертификат** для того сертификата, который необходимо экспортировать (см. «[Просмотр сертификатов](#)» на стр. 154).
- 2 Откройте вкладку **Состав**, после чего нажмите кнопку **Копировать в файл**.
- 3 На стартовой странице мастера экспорта сертификатов нажмите кнопку **Далее**.



Совет. Если при последующих запусках мастера желательно пропускать те или иные страницы, на этих страницах следует устанавливать флажок **Не отображать в дальнейшем эту страницу**.

- 4 На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов, после чего нажмите кнопку **Далее**.

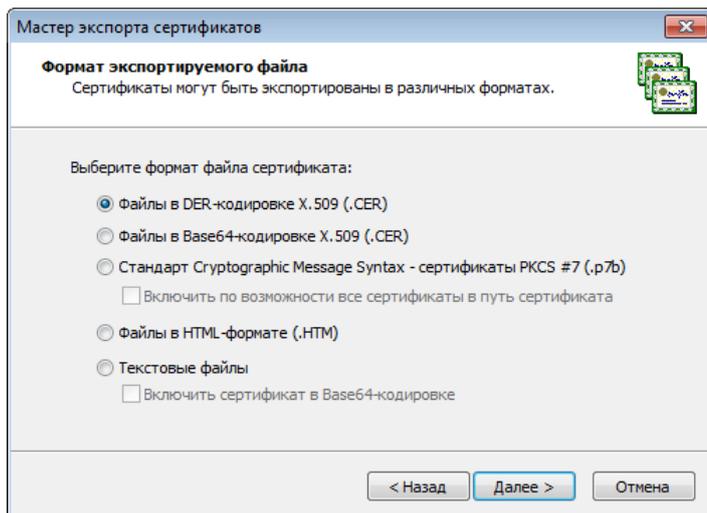


Рисунок 63: Выбор формата файла

- 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 «Экспорт успешно выполнен» нажмите кнопку **ОК**.

Управление сертификатами

Смена текущего сертификата

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



Внимание! Выбирать сертификат для использования в качестве текущего необходимо в том случае, когда новый сертификат получен в составе ключевой дискеты.

Для выбора действительного личного сертификата, который необходимо использовать в качестве текущего:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Выбрать**.

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



Примечание. Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование внешних сертификатов** (см. «[Дополнительные настройки параметров безопасности](#)» на стр. 123).

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

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



Примечание. В качестве текущего можно использовать только тот действительный личный сертификат, который введен в действие. Изданный, но не введенный в действие личный сертификат необходимо сперва ввести в действие, а затем назначить текущим.

При успешном выполнении описанных действий выбранный сертификат назначается текущим.

Обновление сертификата

Срок действия сертификата цифровой подписи пользователя определяет администратор УКЦ или ViPNet Manager при издании сертификата. По умолчанию срок действия сертификата составляет 5 лет. После истечения срока действия сертификат становится недействительным. Цифровые подписи на документах или файлах, подписанных этим сертификатом, также станут недействительными.

Сертификат цифровой подписи, у которого истекает срок действия, необходимо обновить. Рекомендуется сделать это заранее. По умолчанию ПО ViPNet [Монитор] или «Деловая почта» начинает выдавать предупреждения за 15 дней до истечения срока действия сертификата.

Чтобы изменить настройки оповещения, выполните следующие действия:

- 1 В программе ViPNet [Монитор] в меню **Сервис** выберите пункт **Настройка параметров безопасности** или в программе «Деловая почта» в меню **Инструменты** выберите **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**.

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

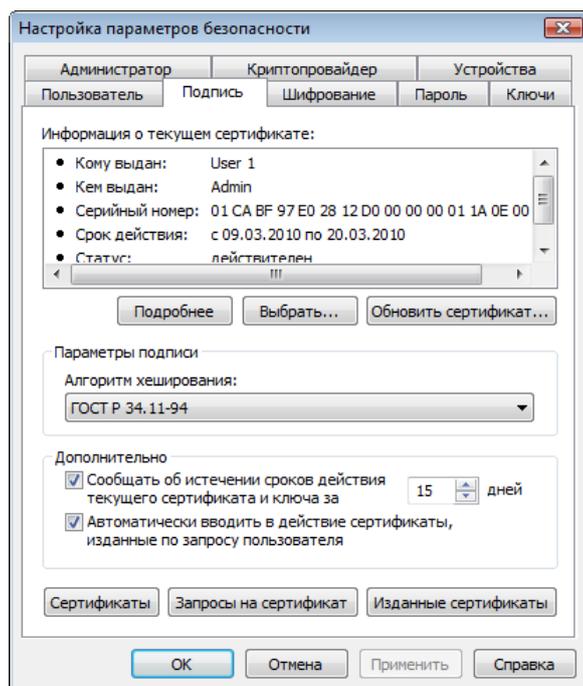


Рисунок 64: Вкладка «Подпись»

- 3 В группе **Дополнительно** установите или снимите флажок **Сообщать об истечении сроков действия текущего сертификата и ключа за** и в поле справа введите число дней не более 99.
- 4 Установите или снимите флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**.



Внимание! По умолчанию флажки **Сообщать об истечении сроков действия текущего сертификата и ключа за** и **Автоматически вводить в действие сертификаты, изданные по запросу пользователя** установлены. В этом случае обеспечивается своевременное и простое обновление истекающего сертификата. Не рекомендуется снимать эти флажки.

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

- Если включено оповещение об истечении срока действия сертификата:

- Когда до истечения срока остается заданное количество дней, программа ViPNet [Монитор] или «Деловая почта» выдаст соответствующее сообщение.

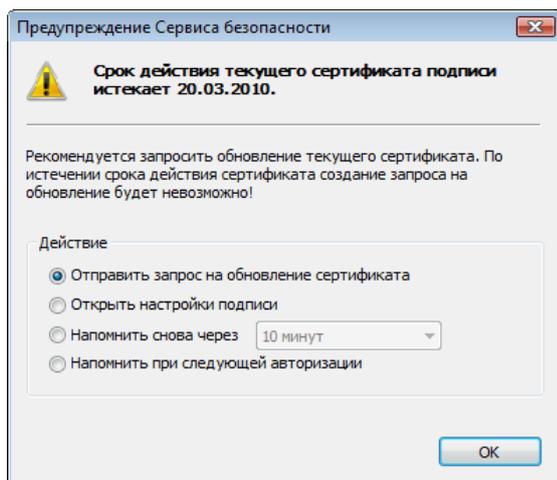


Рисунок 65: Сообщение об истечении срока действия сертификата

- В окне сообщения выберите **Отправить запрос на обновление сертификата** и нажмите **ОК**. Будет запущен **Мастер обновления сертификата**.



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

- Если оповещение об истечении срока действия сертификата отключено:
 - В окне программы ViPNet [Монитор] в меню **Сервис** выберите пункт **Настройка параметров безопасности** или в окне «Деловой почты» в меню **Инструменты** выберите **Настройка параметров безопасности**.
 - В окне **Настройка параметров безопасности** откройте вкладку **Подпись**.
 - На вкладке **Подпись** (см. Рисунок 64 на стр. 168) нажмите кнопку **Обновить сертификат**. Будет запущен **Мастер обновления сертификата**.

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

- 1 На стартовой странице мастера обновления сертификата нажмите кнопку **Далее**.

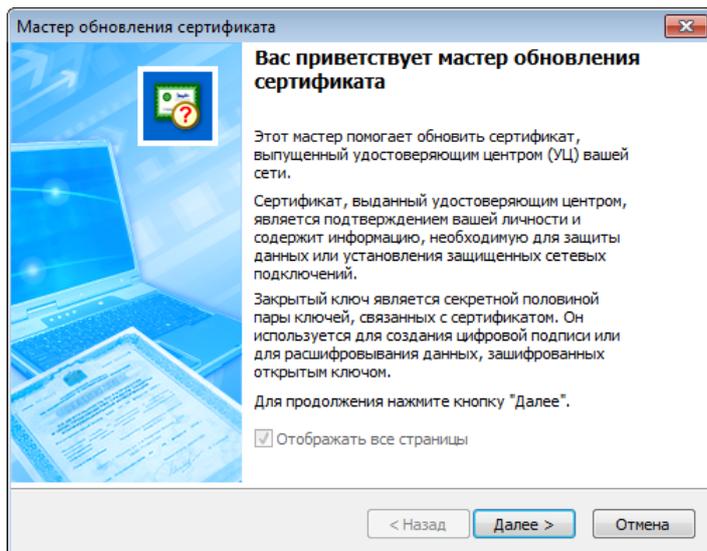


Рисунок 66: Стартовая страница мастера обновления сертификата

- 2 На странице **Открытый ключ** укажите параметры открытого ключа в соответствии с приведенной ниже таблицей:

Алгоритм подписи	Описание	Параметры алгоритма	Описание параметров	Длина ключа
ГОСТ Р 34.10-2001	Новый стандарт ЭЦП, основанный на арифметике эллиптических кривых. OID «1.2.643.2.2.19»	ГОСТ Р 34.10-2001	Параметры по умолчанию (рекомендуется). OID «1.2.643.2.2. 35.1»	512
		ГОСТ Р 34.10-2001	Параметры подписи 3 (Набор параметров «КриптоПРО»): OID «1.2.643.2.2. 35.3»	



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

После этого нажмите кнопку **Далее**.

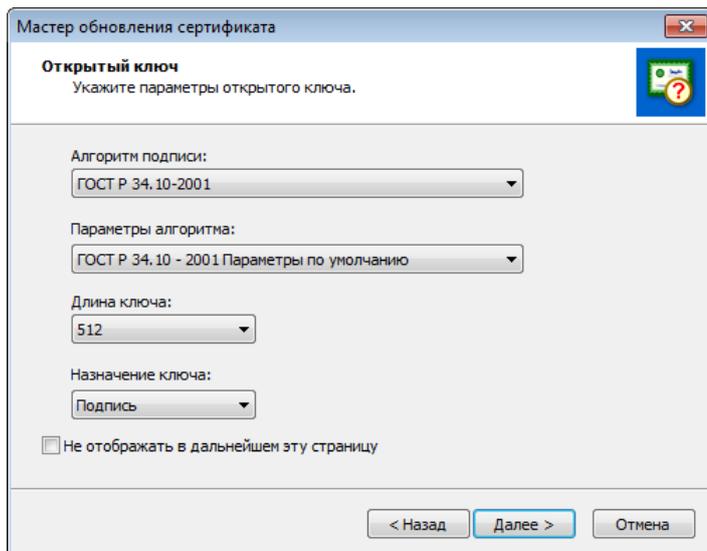


Рисунок 67: Выбор параметров открытого ключа

- 3 На странице **Контейнер с закрытым ключом** укажите место сохранения контейнера с закрытым ключом:
- папку на диске,
 - устройство с указанием его параметров и ПИН-кода.



Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).

После этого нажмите кнопку **Далее**.

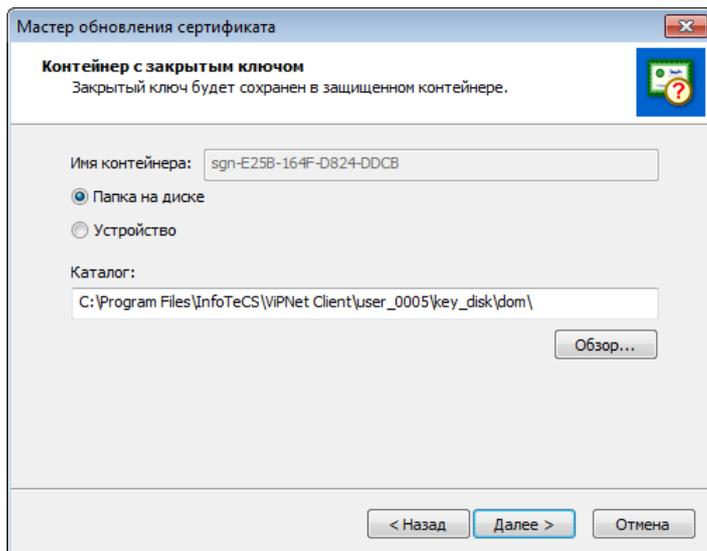


Рисунок 68: Указание места сохранения контейнера с закрытым ключом

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

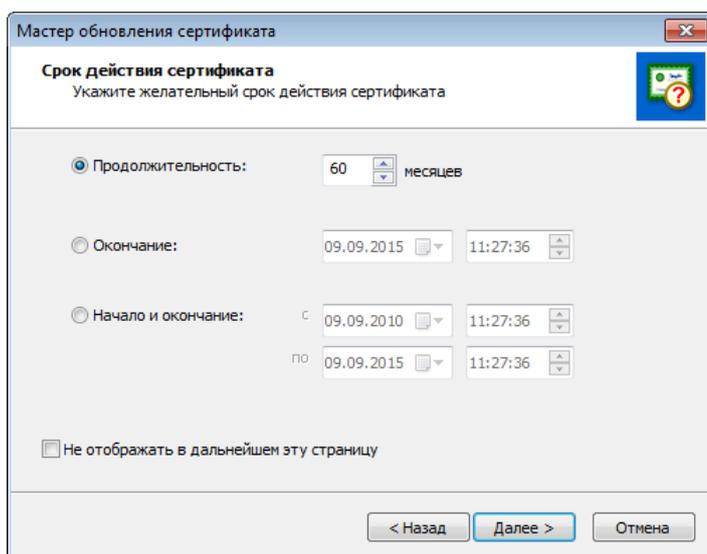


Рисунок 69: Указание желаемого срока действия сертификата

- 5 На странице **Способ передачи сертификата** выберите, каким образом запрос на обновление сертификата будет передан в программу ViPNet Administrator [УКЦ] или ViPNet Manager:

- **Передать через транспортный модуль** — отправка запроса через транспортный модуль ViPNet [MFTP].
- **Передать через файл** — сохранение запроса в файл (формата *.sok или другого формата) по пути, указанному с помощью кнопки **Обзор**. По завершении работы мастера обновления этот файл необходимо передать администратору вашей сети ViPNet.

После этого нажмите кнопку **Далее**.

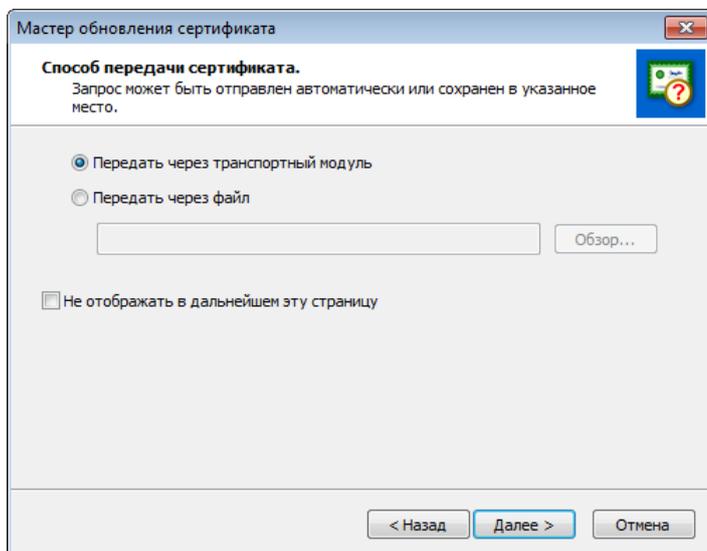


Рисунок 70: Выбор способа передачи сертификата в программу ViPNet Administrator [УКЦ] или ViPNet Manager

6 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 данной рабочей станции, убедитесь в том, что установлен флажок **Печатать информацию о запросе**. В противном случае снимите флажок.

После этого нажмите кнопку **Далее**.

7 При появлении электронной рулетки поведите указателем мыши в пределах появившегося окна.



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

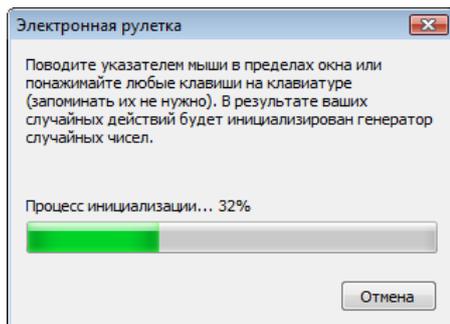


Рисунок 71: Электронная рулетка

8 На странице **Завершение работы мастера обновления сертификата:**

- В случае если ранее на странице **Способ передачи сертификата** выбран способ **Передать через транспортный модуль**, — нажмите кнопку **Готово**. Работа мастера обновления сертификата завершена. Созданный файл необходимо передать администратору вашей сети ViPNet.
- В случае если ранее на странице **Способ передачи сертификата** выбран способ **Передать через файл**, — задайте значения следующих параметров:
 - **Ожидать ответа на запрос** — для входа в режим ожидания ответа от программы ViPNet Administrator [УКЦ] или ViPNetManager.
 - **Ввести изданный сертификат в действие** — для ввода изданного сертификата в действие и назначения его текущим сразу после получения.



Примечание. Флажок **Ввести изданный сертификат в действие** можно не устанавливать, если в окне **Настройка параметров безопасности** на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**.

Нажмите кнопку **Готово**.

- 9** При появлении окна с сообщением «Ожидание ответа удостоверяющего центра» дождитесь отображения ответа от программы ViPNet Administrator [УКЦ] или ViPNet Manager:
- **Запрос на сертификат удовлетворен** — обновленный сертификат получен.

- **Запрос на сертификат отклонен** — сертификат не был обновлен. Обратитесь к администратору вашей сети ViPNet для уточнения причин отклонения запроса.

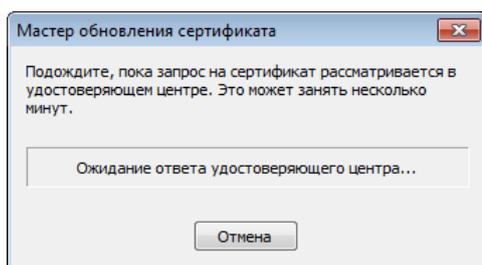


Рисунок 72: Ожидание ответа от программы ViPNet Administrator [УКЦ] или ViPNet Manager

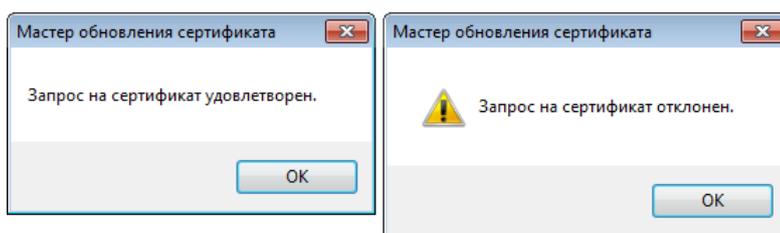


Рисунок 73: Возможные ответы от программы ViPNet Administrator [УКЦ] или ViPNet Manager

- 10** Убедитесь в том, что изданный сертификат введен в действие.
 - Вызовите окно **Настройка параметров безопасности**, после чего откройте вкладку **Подпись**.
 - Нажмите кнопку **Запросы на сертификат**.
 - Убедитесь в том, что для отправленного запроса отображается статус **сертификат введен в действие**.

Если сертификат издан, но не введен в действие автоматически, выполните ввод сертификата в действие вручную (см. «[Ввод в действие вручную](#)» на стр. 176).

Ввод сертификатов в действие

Ввод в действие автоматически

Для того чтобы ввод в действие сертификатов, полученных из программы ViPNet Administrator [УКЦ] или ViPNet Manager, выполнялся автоматически:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 Убедитесь в том, что установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**, после чего нажмите кнопку **Применить** или **ОК**.

Сертификаты будут вводиться в действие автоматически в течение часа с момента их получения.

Ввод в действие вручную

Для того чтобы ввести в действие сертификаты, изданные в программе ViPNet Administrator [УКЦ] или ViPNet Manager и переданные на используемую рабочую станцию в виде файлов:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Изданные сертификаты**.
- 3 В окне **Менеджер сертификатов** нажмите кнопку **Импорт**.
- 4 В окне **Открыть (Open)** выберите файл формата *.sok, полученный от администратора Вашей сети ViPNet.
Выбранный файл будет помещен в каталог установки программы ViPNet Client [Деловая почта], в папку From_KC. При этом информация об изданном сертификате отобразится на вкладке **Изданные сертификаты**.
- 5 Выберите сертификат, который необходимо ввести в действие, после чего нажмите кнопку **Ввести в действие**.

Работа с запросами на сертификаты

Работа с запросами на сертификаты выполняется в окне **Менеджер сертификатов** на вкладке **Запросы на сертификат**.

Для вызова окна **Менеджер сертификатов**:

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.
- 2 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**.

3 Нажмите кнопку **Запросы на сертификаты**.

Просмотр запроса на сертификат

Для просмотра подробной информации о запросе на сертификат:

- 1 В окне **Менеджер сертификатов** на вкладке **Запросы на сертификат** выберите нужный запрос, после чего нажмите кнопку **Свойства** или выполните двойной щелчок мыши по этому запросу.
- 2 В окне **Запрос на сертификат** просмотрите нужную информацию на соответствующих вкладках.

При необходимости запрос можно напечатать (на принтере, используемом по умолчанию на данной рабочей станции) с помощью кнопки **Печать**, а также сохранить в файл формата *.txt — с помощью кнопки **Копировать в файл**.

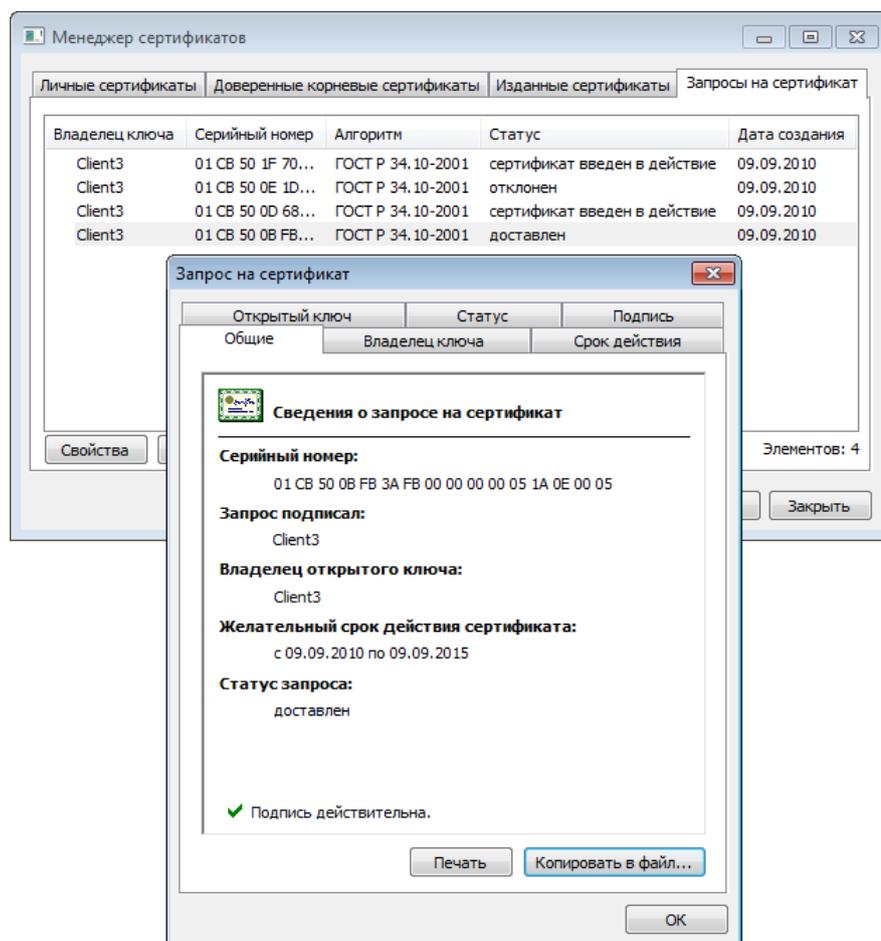


Рисунок 74: Просмотр подробной информации о запросе на сертификат

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**.

Работа с контейнером закрытого ключа

Контейнер закрытого ключа содержит сертификат (для проверки подлинности вашей подписи и зашифрования сообщений, адресованных вам) и соответствующий ему закрытый ключ подписи (для подписи и расшифровки документов).

В программе ViPNet Client [Деловая почта] доступны следующие операции с контейнером закрытого ключа:

- Установка.

Контейнер закрытого ключа может быть установлен как совместно с сертификатом (см. «[Установка сертификатов в хранилище](#)» на стр. 159), так и отдельно (см. «[Установка нового и смена текущего контейнера](#)» на стр. 184) (например, в случае, если закрытый ключ хранится в контейнере, а сертификат сформирован по запросу пользователя в программе ViPNet Administrator [УКЦ] или ViPNet Manager).

- Смена и удаление пароля к контейнеру, а также удаление закрытого ключа, который хранится в контейнере.
- Изменение расположения контейнера.



Внимание! В рамках ПО ViPNet CUSTOM выполнять различные операции с контейнером закрытого ключа может только пользователь, который обладает правом подписи. Такое право предоставляется пользователям сети ViPNet в программе ViPNet Administrator [ЦУС].

Для работы с контейнером закрытого ключа (см. «[Контейнер закрытого ключа](#)»):

- 1 Выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.

2 Откройте вкладку **Ключи**.

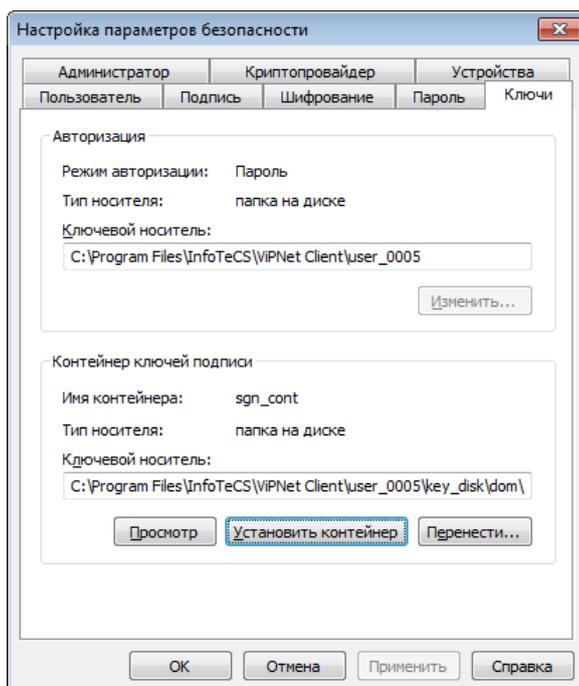


Рисунок 75: Работа с контейнером закрытого ключа

- 3 В разделе **Контейнер ключей подписи** нажмите одну из следующих кнопок:
- **Просмотр** — для просмотра подробной информации об используемом контейнере, а также для изменения свойств контейнера:
 - смены пароля (см. «Смена пароля к контейнеру» на стр. 180);
 - удаления пароля (см. «Удаление сохраненного пароля» на стр. 182);
 - проверки соответствия закрытого ключа сертификату (см. «Проверка контейнера» на стр. 183);
 - удаления закрытого ключа (см. «Удаление закрытого ключа» на стр. 183).
 - **Установить контейнер** — для установки нового и смены текущего контейнера (см. «Установка нового и смена текущего контейнера» на стр. 184).
 - **Перенести** — для смены пути к контейнеру (см. «Перенос контейнера» на стр. 185).

Смена пароля к контейнеру

Для смены пароля к контейнеру:

- 1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 75 на стр. 180) нажмите кнопку **Просмотр**.
- 2 В окне **Свойства контейнера** нажмите кнопку **Сменить пароль**.

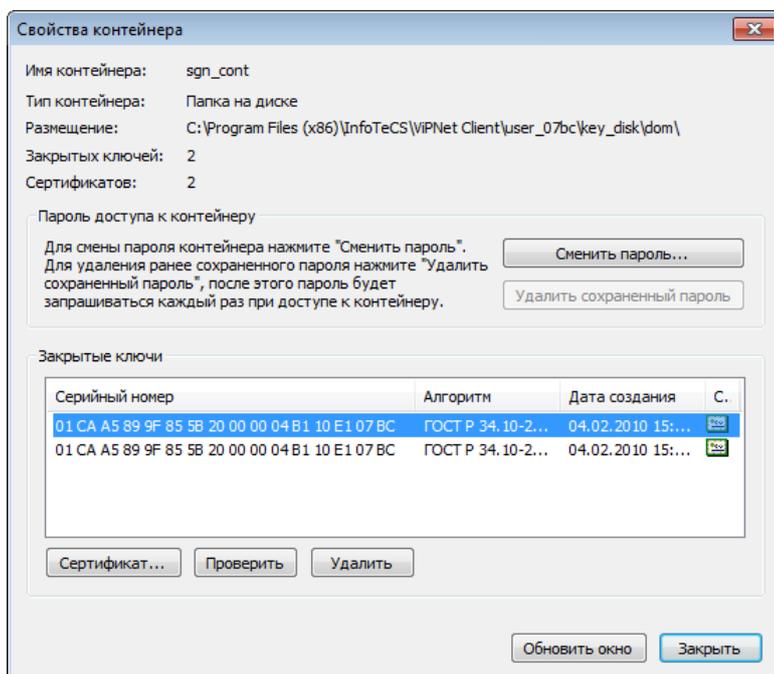


Рисунок 76: Окно *Свойства контейнера*

- 3 При появлении окна, изображенного на нижеследующем рисунке, нажмите кнопку **ОК**, после чего измените пароль пользователя (см. «[Смена пароля пользователя](#)» на стр. 127).

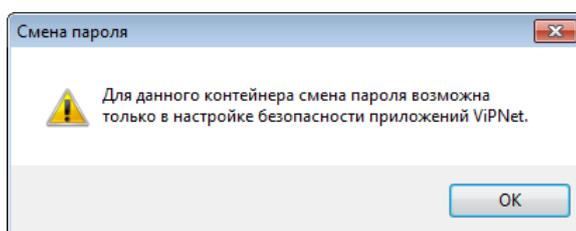


Рисунок 77: Сообщение о невозможности смены пароля для доступа к контейнеру



Примечание. Появление данного окна связано с тем, что контейнер закрытого ключа защищен с использованием не пароля, а персонального ключа пользователя. Поэтому изменение пароля к контейнеру возможно только вместе с изменением пароля пользователя.

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



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

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

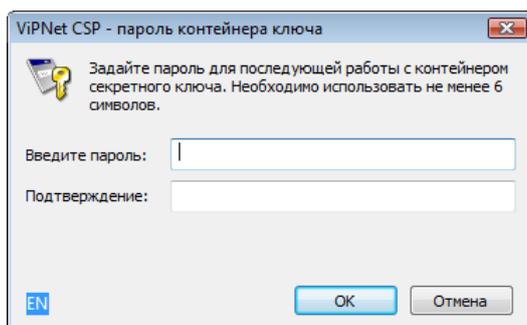


Рисунок 78: Смена пароля доступа к контейнеру

Пароль доступа к контейнеру изменен.

Удаление сохраненного пароля

Для удаления сохраненного пароля к контейнеру и отображения окна ввода пароля при доступе к контейнеру:

- 1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 75 на стр. 180) нажмите кнопку **Просмотр**.
- 2 В окне **Свойства контейнера** (см. Рисунок 76 на стр. 181) нажмите кнопку **Удалить сохраненный пароль**.

Сохраненный пароль удален.

Проверка контейнера

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

Чтобы проверить контейнер, выполните следующие действия:

- 1 В окне **Свойства контейнера** (см. Рисунок 76 на стр. 181) в списке **Закрытые ключи** выберите строку закрытого ключа.
- 2 Нажмите кнопку **Проверить**.
- 3 В окне **ViPNet CSP - пароль контейнера ключа** (см. Рисунок 80 на стр. 185) введите пароль доступа к контейнеру и нажмите **ОК**.

После этого будет сформирован фрагмент данных, который будет подписан с помощью закрытого ключа, после чего будет выполнена проверка цифровой подписи с помощью сертификата открытого ключа. Таким образом, будет проверена пригодность закрытого ключа и его совместимость с сертификатом, хранящимся в контейнере.



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

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

При успешной проверке закрытого ключа отобразится соответствующее сообщение.

Удаление закрытого ключа

Чтобы удалить закрытый ключ из контейнера:

- 1 В окне **Свойства контейнера** (см. Рисунок 76 на стр. 181) в списке **Закрытые ключи** выберите строку закрытого ключа.
- 2 Нажмите кнопку **Удалить**. Появится предупреждение о том, что удаленные закрытые ключи невозможно восстановить.
- 3 В окне предупреждения нажмите **Да**.

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

Установка нового и смена текущего контейнера

Для установки нового или смены текущего контейнера:

- 1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 75 на стр. 180) нажмите кнопку **Установить сертификат**.
- 2 В окне **ViPNet CSP – инициализация ключевого контейнера** укажите место хранения контейнера закрытого ключа:
 - папку на диске,
 - устройство с указанием его параметров и ПИН-кода.

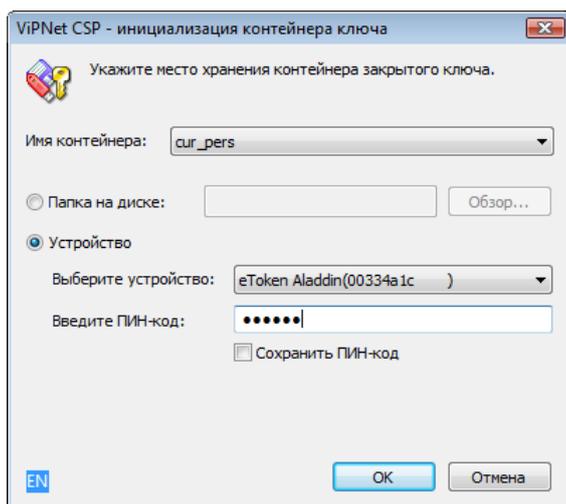


Рисунок 79: Инициализация контейнера ключа с внешнего устройства



Внимание! В случае, если на выбранном устройстве хранятся ключи, сформированные в ПО ViPNet версии ниже 3.1.X, появится окно программы **Конвертер ключей ViPNet** с предложением конвертировать ключи в новый формат. Подробная информация о работе с программой **Конвертер ключей ViPNet** содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).

После этого нажмите кнопку **ОК**.

- 3 В случае, если целостность контейнера нарушена (отсутствует закрытый ключ и (или) сертификат), в окне с сообщением об ошибке нажмите кнопку **ОК**, затем выберите другой контейнер.

- 4 При появлении окна ввода пароля укажите пароль к выбранному контейнеру, после чего нажмите кнопку **ОК**.

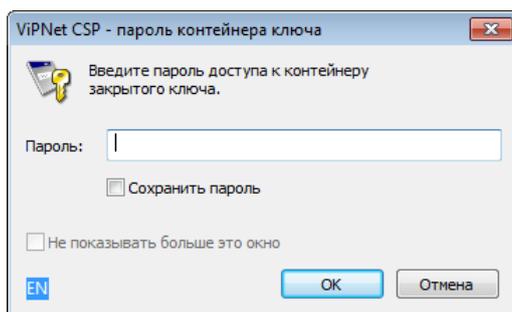


Рисунок 80: Ввод пароля доступа к контейнеру закрытого ключа

- 5 В случае, если в контейнере найдено несколько сертификатов, в окне **Выбор сертификата** назначьте один из них текущим, после чего нажмите кнопку **ОК**.

Выбранный контейнер закрытого ключа и соответствующий сертификат назначены текущими.

Перенос контейнера

Для того чтобы поменять расположение контейнера:

- 1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 75 на стр. 180) нажмите кнопку **Перенести**.
- 2 В окне **ViPNet CSP – инициализация контейнера ключа** укажите новое место хранения контейнера закрытого ключа:
 - папку на диске,
 - устройство с указанием его параметров и ПИН-кода.



Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).



Внимание! В случае, если на выбранном устройстве хранятся ключи, сформированные в ПО ViPNet версии ниже 3.1.X, появится окно программы **Конвертер ключей ViPNet** с предложением конвертировать ключи в новый

формат. Подробная информация о работе с программой **Конвертер ключей ViPNet** содержится в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 11).

Контейнер закрытого ключа будет перенесен по указанному пути.



Глоссарий

Р

PKI (инфраструктура открытых ключей)

PKI (инфраструктура открытых ключей) — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам в распределенных системах через создание сертификатов открытых ключей и поддержание их жизненного цикла.

См. также: [Открытый ключ](#).

А

Абонентский пункт (АП)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора абонентский пункт не выполняет функции маршрутизации трафика и служебной информации.

См. также: [Сетевой узел ViPNet \(СУ\)](#).

Администратор сетевого узла ViPNet

Лицо, ответственное за настройку программного обеспечения ViPNet на сетевом узле ViPNet.

См. также: [Сетевой узел ViPNet \(СУ\)](#).

Д

Дистрибутив справочно-ключевой информации

Файл с расширением .DST, создаваемый УКЦ для каждого пользователя сетевого узла ViPNet. В этом файле помещены адресные справочники, ключевая информация и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив справочно-ключевой информации необходимо установить на сетевой узел.

См. также: [Сетевой узел ViPNet \(СУ\)](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

К

Ключевая дискета (КД)

Совокупность файлов, необходимых пользователю для аутентификации в сети ViPNet, к которым имеет доступ только данный пользователь.

Ключевая дискета (КД) пользователя может содержать:

- действующий персональный ключ пользователя;
- случайный ключ защиты пользователя;
- контейнер с ключом (ключами) подписи;
- файл хэша пароля пользователя.

Содержимое ключевой дискеты формируется в зависимости от типа аутентификации пользователя.

Коллектив

Совокупность пользователей одного сетевого узла ViPNet, имеющих одни и те же ключи для шифрования конфиденциальной информации.

См. также: [Сетевой узел ViPNet \(СУ\)](#).

Контейнер закрытого ключа

Файл, в котором хранятся закрытый ключ и соответствующий ему сертификат открытого ключа.

При формировании запроса на обновление сертификата имя контейнера, в котором будет храниться новая пара ключей подписи (закрытый и сертификат), задается автоматически и имеет вид `sgn-<случайное число 16-ричного формата>`.

См. также: [Сертификат открытого ключа подписи пользователя](#).

О

Общий коллектив (коллектив сетевого узла, «нулевой» коллектив)

Коллектив, который зарегистрирован на отдельном сетевом узле и включает всех пользователей данного сетевого узла. Информация об общем коллективе сетевого узла отображается в программах ViPNet [Монитор] и ViPNet [Деловая почта] в окне **Настройка параметров безопасности > Пользователь > Коллективы, в которых зарегистрирован пользователь > Все коллективы**.

См. также: [Коллектив](#).

Открытый ключ

Последовательность символов, связанная с закрытым ключом определенным математическим соотношением. Открытый ключ доступен любым пользователям информационной системы и предназначен для подтверждения подлинности электронной цифровой подписи (или шифрования).

См. также: [Электронная цифровая подпись \(ЭЦП\)](#).

П

Папка (каталог) ключей пользователя

Папка, в которой находится ключевая дискета (КД).

См. также: [Ключевая дискета \(КД\)](#).

Папка справочно-ключевой информации

Папка, в которую устанавливается дистрибутив справочно-ключевой информации. Несколько программ ViPNet могут использовать одну и ту же папку справочно-ключевой информации.

См. также: [Дистрибутив справочно-ключевой информации](#).

Полномочия пользователя

Права, определяющие допустимость различных действий пользователей на сетевом узле ViPNet по изменению настроек установленного на нем ПО ViPNet.

Администратор ЦУС выставляет полномочия пользователей одного сетевого узла ViPNet в рамках прикладной задачи. Если полномочия пользователя ограничены, ввод пароля администратора сетевого узла ViPNet снимет эти ограничения, предоставив максимальные полномочия в приложениях.

См. также: [Прикладная задача](#), [Сетевой узел ViPNet \(СУ\)](#).

Прикладная задача

Совокупность программных средств, предназначенных для решения целевых и служебных задач сети ViPNet. Прикладная задача выполняет две основные функции: используется в лицензировании сети с помощью файла infotecs.reg и определяет допустимость выполнения какой-либо функциональности ПО ViPNet для заданного сетевого узла.

Прикладные задачи могут иметь атрибуты, например, в виде полномочий, которые также влияют на функциональность, и количественных характеристик.

Приложение ViPNet может включать в себя несколько прикладных задач. Каждая прикладная задача имеет свое название.

См. также: [Полномочия пользователя](#), [Сеть ViPNet](#).

С

Сертификат издателя

Сертификат, с помощью закрытого ключа которого подписывается другой сертификат.

Сертификат открытого ключа подписи пользователя

Цифровой документ заранее определенного формата, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Сертификат содержит информацию о владельце ключа, открытый ключ, сведения о его назначении и области применения, информацию о выпустившем сертификат удостоверяющем центре, период действия сертификата, а также некоторые дополнительные параметры. В сети ViPNet сертификат создается программой УКЦ и заверяется электронной цифровой подписью администратора УКЦ.

ЭЦП центра сертификации (администратора УКЦ), заверяющая содержимое каждого сертификата, обеспечивает подлинность и целостность указанной в нем информации, включая описание владельца и его открытый ключ. Спецификация содержимого и формат сертификата в сети ViPNet соответствует стандарту X.509 версии 3 и Федеральному закону РФ «Об электронной цифровой подписи».

См. также: [Открытый ключ](#), [Электронная цифровая подпись \(ЭЦП\)](#).

Сетевой узел ViPNet (СУ)

Узел с установленным ПО ViPNet, с помощью которого защищают информацию приложений ViPNet, хранимую локально на компьютере, и (или) трафик посредством шифрования, имитозащиты и ЭЦП.

См. также: [Сеть ViPNet](#), [Электронная цифровая подпись \(ЭЦП\)](#).

Сеть ViPNet

Логическая сеть, организованная с помощью ПО ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

См. также: [Сетевой узел ViPNet \(СУ\)](#).

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны администратором удостоверяющего центра и на данный момент недействительны.

Т

Транспортный конверт

Информация служб или приложений в защищенном виде, доставляемая узлам ViPNet транспортным модулем ViPNet MFTR.

См. также: [Транспортный модуль \(MFTR\)](#).

Транспортный модуль (MFTR)

Программный модуль, предназначенный для обмена информацией в сети ViPNet.

У

Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в ПО ViPNet Administrator. Администратор УКЦ формирует (и обновляет) ключевую информацию для объектов и пользователей сети ViPNet, а также выдает сертификаты пользователям сети ViPNet, удовлетворяет запросы на сертификаты и управляет списками корневых и отозванных сертификатов.

См. также: [Список отозванных сертификатов \(СОС\)](#).

Ц

Центр управления сетью (ЦУС)

Программа, входящая в ПО ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение конфигурации виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка защищенных адресных справочников;
- формирование информации о связях пользователей для УКЦ;
- определений полномочий пользователей сетевых узлов ViPNet.

См. также: [Полномочия пользователя Удостоверяющий и ключевой центр \(УКЦ\)](#).

Э

Электронная цифровая подпись (ЭЦП)

Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.



В

Указатель

А

- Автопроцессинг • 9, 16
- Администратор сетевого узла ViPNet • 122
- Адресная книга • 47, 61, 98
- Архивация писем • 111

В

- Ввод в действие вручную • 175
- Выбор пароля на основе парольной фразы • 128
- Выбор собственного пароля • 128
- Выбор цифрового пароля • 128

Д

- Дистрибутив справочно-ключевой информации • 190
- Дополнительные настройки и возможности • 66, 121
- Дополнительные настройки параметров безопасности • 30, 78, 121, 156, 166

З

- Задание параметров шифрования с использованием асимметричных ключей • 131
- Запрос извещения о доставке и прочтении в виде отдельного письма • 37, 48, 115

- Запуск и завершение работы с программой • 16

И

- Изменение режима авторизации пользователя • 30, 121
- Инициализация устройства • 138
- Интерфейс программы • 37, 38, 39, 48, 49, 53, 54, 58, 60, 63, 64, 74, 79, 80, 86, 102, 109, 111, 114, 116, 118, 119, 121
- Информация о внешних устройствах хранения данных • 30, 73, 77, 136, 138, 139, 163, 171, 184, 185
- Использование сертификата, изданного сторонним удостоверяющим центром • 73

К

- Как написать письмо • 20
- Ключевая дискета (КД) • 190
- Коллектив • 189
- Конвертация ключей на внешнем устройстве • 25
- Контейнер закрытого ключа • 73, 179

Н

- Настройка архивации • 67
- Настройка параметров автопроцессинга • 89, 100, 101
- Настройка параметров журнала автопроцессинга • 102
- Настройка параметров работы криптопровайдера ViPNet CSP • 78
- Настройка параметров работы с письмами • 54, 74, 86
- Настройка транспортного модуля • 9

О

- Общие настройки • 26
- Окно создания и просмотра писем • 46, 48, 51, 56, 58, 74, 79, 81, 86
- Ответ на письмо и пересылка письма • 20
- Открытый ключ • 187, 191
- Отсоединение и присоединение подписи файла • 82, 83, 100, 110

П

- Папка (каталог) ключей пользователя • 27
- Перенос контейнера • 180
- Перенос писем в другую папку • 51, 66
- Подписание выбранным сертификатом • 73, 74, 75, 76, 82
- Подписание письма • 18, 78
- Подписание файла • 78, 109
- Полномочия пользователя • 121, 122, 190, 192
- Прикладная задача • 190
- Проверка контейнера • 180
- Проверка цифровой подписи файла • 82
- Просмотр доверенных корневых сертификатов • 154
- Просмотр журнала событий, связанных с асимметричными ключами • 133
- Просмотр изданных сертификатов • 154
- Просмотр личных сертификатов пользователя • 154
- Просмотр письма и вложений в отдельном окне • 19, 37, 45, 53
- Просмотр сертификатов • 161, 164
- Просмотр текущего сертификата пользователя • 154

Р

- Работа в программе с правами администратора • 38, 40, 66, 78, 101, 122
- Работа с архивами писем • 67
- Работа с контейнером закрытого ключа • 136, 137, 138
- Работа с письмами • 16
- Работа с цифровой подписью писем • 73
- Работа с цифровой подписью файлов • 73

С

- Сертификат открытого ключа подписи пользователя • 73, 189
- Сетевой узел ViPNet (СУ) • 187, 188, 189, 190, 191
- Сеть ViPNet • 9, 190, 191
- Смена каталога ключей пользователя • 25
- Смена пароля к контейнеру • 180
- Смена пароля пользователя • 181
- Смена ПИН-кода устройства • 138
- Смена текущего сертификата • 78
- Создание групп адресатов • 41
- Создание и использование шаблонов • 38
- Создание нового письма • 17, 37, 41, 42
- Создание письма • 45, 48, 50, 51, 52, 56, 59, 64, 74, 75, 86
- Создание правила для входящих писем • 92, 93
- Создание правила для исходящих файлов • 92, 93
- Специальные папки • 38, 39
- Список отозванных сертификатов (СОС) • 192

Т

- Транспортный конверт • 61
- Транспортный модуль (MFTP) • 192

У

- Удаление закрытого ключа • 180
- Удаление писем • 22, 38, 39
- Удаление сохраненного пароля • 180
- Удаление цифровой подписи письма • 56
- Удостоверяющий и ключевой центр (УКЦ) • 188, 192
- Уровни адресации • 9, 41, 47
- Установка в хранилище автоматически • 136
- Установка нового и смена текущего контейнера • 179, 180
- Установка сертификатов в хранилище • 179

Ц

- Цифровая подпись в программе • 115
- Цифровая подпись и шифрование • 16, 47

Э

Экспорт и импорт писем • 21, 38

Электронная цифровая подпись (ЭЦП) •
189, 191