# ViPNet Client for Windows 4

## Руководство пользователя

infotecs

ФРКЕ.00116-04 34 01



ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

# Содержание

**Введение** ..... **12**
О документе ..... 13
Для кого предназначен документ ..... 13
Соглашения документа ..... 13
О программе ..... 15
Назначение ПО ViPNet Client ..... 15
Состав ПО ViPNet Client ..... 15
ViPNet-драйвер ..... 15
ViPNet Монитор ..... 16
ViPNet MFTP ..... 16
ViPNet Контроль приложений ..... 16
ViPNet Деловая почта ..... 17
ViPNet CSP ..... 17
Система обновления ViPNet ..... 18
Принцип работы ViPNet-драйвера ..... 18
Новые возможности версии 4.3.2 ..... 21
Системные требования ..... 22
Комплект поставки ..... 23
Обратная связь ..... 24
Дополнительная информация ..... 24
Контактная информация ..... 24

**Глава 1. Установка, обновление и удаление ПО ViPNet Client** ..... **25**
Установка ПО ViPNet Client ..... 26
Установка в неинтерактивном режиме ..... 29
Дополнительные параметры установки в неинтерактивном режиме ..... 30
Установка ViPNet Client с помощью групповых политик ..... 31
Обновление ПО ViPNet Client ..... 40
Обновление, отправленное из ЦУСа или ViPNet Network Manager ..... 41
Обновление с помощью групповых политик ..... 41
Обновление с помощью Центра обновления Windows ..... 42
Обновление с помощью установочного файла ..... 42
Добавление, удаление и восстановление компонентов ПО ViPNet Client ..... 44
Удаление ПО ViPNet Client ..... 46
Перенос сетевого узла на другой компьютер ..... 47

**Глава 2. Установка и обновление справочников и ключей ... 50**
Установка справочников и ключей ... 51
Установка справочников и ключей одного пользователя ... 52
Установка справочников и ключей нескольких пользователей на одном сетевом узле ... 54
Расширенный режим установки справочников и ключей ... 54
Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet ... 56
Установка справочников и ключей в неинтерактивном режиме ... 57
Повторная установка справочников и ключей после сбоя программы ... 58
Использование справочников и ключей, установленных ранее ... 60
Обновление справочников, ключей и политик безопасности ... 61
Прием централизованных обновлений ... 61
Обновление справочников и ключей с помощью дистрибутива ключей ... 62
Удаление справочников и ключей ... 64
Действия при компрометации ключей ... 65

**Глава 3. Начало работы с ПО ViPNet Client ... 67**
Запуск программы ViPNet Монитор ... 68
Способы аутентификации пользователя ... 70
Пароль ... 72
Пароль на устройстве ... 72
Устройство ... 73
Особенности аутентификации с помощью сертификата ... 74
Смена пользователя ... 76
Завершение работы с программой ViPNet Монитор ... 77
Интерфейс программы ViPNet Монитор ... 78
Работа со списком защищенных узлов ViPNet ... 80
Использование программы ViPNet Монитор в условиях ограниченных полномочий ... 81

**Глава 4. Система обновления ViPNet ... 83**
О системе обновления ViPNet ... 84
Автоматическая установка обновлений ... 85
Установка обновлений вручную ... 87
Просмотр журнала установленных обновлений ... 89

**Глава 5. Подключение к защищенной сети ViPNet ... 90**
Протоколы соединений в защищенной сети ... 91
Принципы осуществления соединений в защищенной сети ... 93

Использование виртуальных IP-адресов ..... 96
Общие принципы назначения виртуальных адресов ..... 96
Настройка подключения к защищенной сети ..... 98
Настройка доступа к защищенным узлам ..... 101
Настройка приоритета IP-адресов доступа к координатору ..... 104
Настройка доступа к туннелируемым узлам ..... 107
Использование псевдонимов для защищенных узлов ..... 109
Просмотр информации о сетевом узле ..... 110

**Глава 6. Настройка и использование служб имен DNS и WINS в сети ViPNet ..... 111**
Службы DNS и WINS ..... 112
DNS ..... 112
WINS ..... 113
Службы DNS и WINS в сети ViPNet ..... 115
DNS (WINS) сервер на защищенном или туннелируемом узле ..... 116
Особенности использования ..... 116
Рекомендации по настройке ..... 117
Незащищенный DNS (WINS) сервер ..... 118
Особенности использования ..... 118
Рекомендации по настройке ..... 119
Использование защищенного DNS (WINS) сервера для удаленной работы с корпоративными ресурсами ..... 120
Автоматическая регистрация DNS (WINS) серверов ..... 120
Создание списка DNS (WINS) серверов вручную ..... 121
Если корпоративный DNS (WINS) сервер установлен непосредственно на сетевом узле ViPNet ..... 122
Если корпоративный DNS (WINS) сервер туннелируется координатором ..... 123
Пример составления файла DNS.TXT ..... 123
Использование DNS-серверов на контроллерах домена ..... 125

**Глава 7. Интегрированный сетевой экран ..... 126**
Основные принципы фильтрации трафика ..... 127
Общие сведения о сетевых фильтрах ..... 129
Использование групп объектов ..... 133
Системные группы объектов ..... 135
Пользовательские группы объектов, настроенные по умолчанию ..... 135
Создание и изменение групп объектов ..... 136
Добавление сетевых узлов ..... 139
Добавление IP-адресов и DNS-имен ..... 140

Добавление протоколов ... 141
Добавление расписаний ... 142
Создание сетевых фильтров ... 144
Создание фильтров для защищенной сети ... 146
Создание фильтров для открытой сети ... 147
Рекомендации по созданию сетевых фильтров ... 149
Восстановление предустановленных фильтров и групп объектов ... 150
Практический пример использования групп объектов и сетевых фильтров ... 151
Блокировка IP-трафика ... 154
Отключение защиты трафика ... 155

**Глава 8. Обработка прикладных протоколов ... 156**
Общие сведения о прикладных протоколах ... 157
Описание прикладных протоколов ... 159
Настройка параметров обработки прикладных протоколов ... 160

**Глава 9. Интеграция с программой ViPNet SafeDisk-V ... 162**
Общие сведения о программе ViPNet SafeDisk-V ... 163
Обеспечение интеграции ViPNet Client с ViPNet SafeDisk-V: порядок действий ... 165
Работа с интегрированной программой ViPNet SafeDisk-V ... 167

**Глава 10. Встроенные средства коммуникации ... 169**
Общие сведения ... 170
Обмен защищенными сообщениями ... 171
Интерфейс программы обмена защищенными сообщениями ... 172
Отправка сообщений ... 174
Прием сообщений ... 174
Отправка файлов и писем из программы обмена защищенными сообщениями ... 175
Прекращение обмена сообщениями ... 176
Отправка писем программы ViPNet Деловая почта ... 178
Файловый обмен ... 179
Интерфейс программы «Файловый обмен» ... 179
Отправка файлов из программы ViPNet Монитор ... 181
Отправка файлов с помощью контекстного меню Windows ... 182
Отправка файлов из программы обмена защищенными сообщениями ... 183
Прием файлов ... 184
Вызов внешних приложений ... 185
Просмотр веб-ресурсов сетевого узла ... 186
Обзор общих ресурсов сетевого узла ... 187

Проверка соединения с сетевым узлом ... 188

**Глава 11. Административные функции ... 192**

Работа с журналом IP-пакетов ... 193

Настройка параметров поиска IP-пакетов ... 193

Просмотр результатов поиска ... 195

Просмотр журнала IP-пакетов в интернет-браузере или в Microsoft Excel ... 197

Выбор IP-пакетов ... 198

Рекомендации по анализу открытых (нешифрованных) и зашифрованных соединений ... 198

Создание сетевого фильтра при просмотре журнала IP-пакетов ... 199

Просмотр журнала IP-пакетов другого сетевого узла ... 200

Просмотр архива журналов IP-пакетов ... 200

Настройка параметров регистрации IP-пакетов в журнале ... 201

Просмотр статистики фильтрации IP-пакетов ... 204

Просмотр информации о клиенте, времени работы программы и числе соединений ... 205

Управление конфигурациями программы ... 206

Конфигурация «Открытый Интернет» ... 208

Конфигурации «Внутренняя сеть» и «Интернет» ... 208

Настройка расписания смены конфигураций программы ... 209

Запуск программы удаленного доступа ... 211

Установка программного обеспечения для удаленного управления ... 212

Настройка терминального сервера при удаленном управлении ... 213

Настройка автоматического входа в ОС и программу ViPNet Монитор ... 214

Настройка автоматического входа в ОС Windows ... 215

Работа в программе в режиме администратора ... 219

Дополнительные настройки программы ViPNet Монитор ... 220

Ограничение интерфейса пользователя ... 221

Параметры запуска программы ... 222

Параметры блокировки компьютера ... 223

Параметры защиты трафика ... 223

Дополнительные настройки параметров безопасности ... 224

Изменение способа аутентификации пользователя ... 226

Просмотр журнала событий ... 227

Настройка параметров записи событий в журнал Windows ... 229

Настройка параметров запуска и аварийного завершения программы ViPNet Монитор ... 232

**Глава 12. Настройка параметров безопасности ... 234**

Смена пароля пользователя ... 235
Выбор собственного пароля ... 236
Выбор пароля на основе парольной фразы ... 236
Выбор цифрового пароля ... 238
Настройка параметров шифрования ... 239
Настройка параметров криптопровайдера ViPNet CSP ... 241

**Глава 13. Работа с сертификатами и ключами ... 243**
Просмотр сертификатов ... 244
Просмотр текущего сертификата пользователя ... 245
Просмотр личных сертификатов пользователя ... 245
Просмотр доверенных корневых сертификатов ... 246
Просмотр изданных сертификатов ... 246
Просмотр цепочки сертификации ... 247
Просмотр полей сертификата и печать сертификата ... 247
Управление сертификатами ... 249
Установка сертификатов в хранилище операционной системы ... 250
Установка в хранилище автоматически ... 250
Установка в хранилище вручную ... 252
Смена текущего сертификата ... 255
Обновление ключа электронной подписи и сертификата ... 256
Настройка оповещения об истечении срока действия ключа электронной подписи и сертификата ... 257
Процедура обновления ключа электронной подписи и сертификата ... 257
Ввод сертификата в действие ... 263
Ввод в действие автоматически ... 264
Ввод в действие вручную ... 264
Работа с запросами на сертификаты ... 265
Просмотр запроса на сертификат ... 265
Удаление запроса на сертификат ... 266
Экспорт сертификата ... 266
Форматы экспорта сертификатов ... 268
Работа с контейнером ключей ... 270
Смена пароля к контейнеру ... 272
Удаление сохраненного на компьютере пароля к контейнеру ключей ... 273
Проверка контейнера ключей ... 274
Установка контейнера ключей ... 275
Перенос контейнера ключей ... 276
Установка сертификата в контейнер ключей ... 277

**Приложение А. Возможные неполадки и способы их устранения ... 278**
Сбор диагностической информации при возникновении неполадок ... 279
Возможные неполадки ... 280
Невозможно проверить сертификат, которым подписан файл установки программы ... 280
Невозможно установить или обновить программу ... 280
Установка программы не выполняется в неинтерактивном режиме ... 281
Невозможно запустить программу ... 282
Не найдены ключи пользователя или неверный пароль ... 282
Не удается выполнить аутентификацию с помощью сертификата ... 283
Невозможно сохранить пароль ... 283
Невозможно подключиться к ресурсам в Интернете ... 283
Невозможно установить соединение с защищенным узлом ... 284
Невозможно обратиться к узлам домена по DNS-имени ... 284
Невозможно получить удаленный доступ к защищенным узлам по DNS-имени ... 284
Невозможно установить соединение с открытым узлом в локальной сети ... 285
Невозможно установить соединение по протоколу SSL ... 285
Невозможно установить соединение по протоколу PPPoE ... 285
В сети зарегистрирован узел с таким же идентификатором, как у вашего узла ... 286
Обнаружен конфликт IP-адресов или DNS-имен ... 286
Невозможно запустить службу MSSQLSERVER ... 287
Невозможно изменить настройки в программе ViPNet Монитор ... 287
Не удается использовать аппаратный датчик случайных чисел ... 288
Нарушение работоспособности сторонних приложений ... 289
Не проходит обновление ПО, отправленное из Центра управления сетью ... 289
Предупреждения сервиса безопасности ... 290
Срок действия пароля истек ... 290
Текущий сертификат не найден или недействителен ... 291
Срок действия текущего ключа электронной подписи или соответствующего сертификата близок к концу ... 293
Срок действия текущего ключа электронной подписи уже истек ... 294
Действительный список аннулированных сертификатов не найден ... 295
Сертификат, изданный по инициативе администратора, введен в действие ... 296
Срок действия сертификата, используемого при аутентификации, подходит к концу ... 297
Срок сертификата, используемого при аутентификации, истек ... 299
Сертификат, используемый при аутентификации, недействителен ... 299
Сертификат, используемый при аутентификации, не найден ... 300

**Приложение B. Общие сведения о сертификатах и ключах ..... 302**
Основы криптографии ..... 303
Симметричное шифрование ..... 303
Асимметричное шифрование ..... 304
Сочетание симметричного и асимметричного шифрования ..... 305
Сочетание хэш-функции и асимметричного алгоритма электронной подписи ..... 306
Общие сведения о сертификатах ключей проверки электронной подписи ..... 309
Определение и назначение ..... 309
Структура ..... 312
PKI и асимметричная криптография ..... 314
Использование сертификатов для шифрования электронных документов ..... 316
Зашифрование ..... 316
Расшифрование ..... 317
Использование сертификатов для подписания электронных документов ..... 318
Подписание ..... 318
Проверка подписи ..... 319
Использование сертификатов для подписания и шифрования электронных документов ..... 320
Подписание и зашифрование ..... 320
Расшифрование и проверка ..... 321
Ключевая система ViPNet ..... 323
Симметричные ключи в ПО ViPNet ..... 323
Асимметричные ключи в ПО ViPNet ..... 325

**Приложение C. События, отслеживаемые ПО ViPNet ..... 327**
Блокированные IP-пакеты ..... 328
Пропущенные IP-пакеты и служебные события ..... 333

**Приложение D. Региональные настройки ..... 335**
Региональные настройки в ОС Server 2003 ..... 336
Региональные настройки в ОС Windows Vista, Server 2008, Windows 7, Server 2008 R2 ..... 337
Региональные настройки в ОС Windows 8.1, Server 2012 ..... 341

**Приложение E. Внешние устройства ..... 345**
Общие сведения ..... 345
Список поддерживаемых внешних устройств ..... 346
Алгоритмы и функции, поддерживаемые внешними устройствами ..... 348

**Приложение F. Рекомендации по обеспечению совместной работы ПО ViPNet Client с другими приложениями ..... 351**

Совместное использование программы ViPNet Монитор и технологии Hyper-V ..... 352
Совместное использование ПО ViPNet Client и Secret Net ..... 354
Настройка доступа к папкам справочников и ключей ..... 355
Совместное использование ПО ViPNet Client и Cisco Agent Desktop ..... 357
Совместное использование ПО ViPNet Монитор и ESET NOD32 Smart Security ..... 358
Совместное использование ПО ViPNet Монитор и Avast ..... 361
Совместное использование ПО ViPNet Монитор и AVG Internet Security ..... 363

**Приложение G. История версий ..... 364**
Что нового в версии 4.3.1 ..... 364
Что нового в версии 4.3.0 ..... 365
Что нового в версии 4.2 ..... 365
Что нового в версии 4.1 ..... 371
Что нового в версии 4.0 ..... 372
Что нового в версии 3.2.11 ..... 377
Что нового в версии 3.2.10 ..... 377
Что нового в версии 3.2.9 ..... 378
Что нового в версии 3.1.5 ..... 384
Что нового в версии 3.1.4 ..... 386
Что нового в версии 3.1.3 ..... 389
Что нового в версии 3.1.2 ..... 390

**Приложение H. Глоссарий ..... 396**

**Приложение I. Указатель ..... 405**

# Введение


О документе 13

О программе 15

Что нового в версии 4.3.1 21

Системные требования 22

Комплект поставки 23

Обратная связь 24

# О документе

## Для кого предназначен документ

Данное руководство предназначено для пользователей программного обеспечения ViPNet Client. В нем содержится информация о назначении и составе ПО ViPNet Client, а также рекомендации по настройке и использованию возможностей программы ViPNet Монитор.

**Примечание.** В данном документе возможности программы ViPNet Монитор описаны с точки зрения пользователя, полномочия которого не ограничены. Если для вас недоступны какие-либо функции или настройки программы, обратитесь к администратору вашей сети ViPNet.

Предполагается, что читатель данного руководства имеет общее представление о сетевых технологиях, IP-протоколах, межсетевых экранах и информационной безопасности.

## Соглашения документа

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

*Таблица 1. Обозначения, используемые в примечаниях*

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

*Таблица 2. Обозначения, используемые для выделения информации в тексте*

| Обозначение | Описание |
|---|---|
| **Название** | Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши. |
| **Клавиша+Клавиша** | Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу. |

| | |
|---|---|
| **Меню > Подменю > Команда** | Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации. |
| `Код` | Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки. |

# О программе

## Назначение ПО ViPNet Client

Программное обеспечение ViPNet Client предназначено для использования в сетях ViPNet, управляемых с помощью ПО ViPNet Administrator и ПО ViPNet Network Manager. ViPNet Client выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях.

Программное обеспечение ViPNet Client может быть установлено для защиты трафика на любом компьютере с ОС Windows, будь то стационарный, удаленный, мобильный компьютер или сервер.

## Состав ПО ViPNet Client

Программное обеспечение ViPNet Client состоит из следующих компонентов:

- Низкоуровневый драйвер сетевой защиты ViPNet-драйвер.
- Программа ViPNet Монитор.
- Транспортный модуль ViPNet MFTP.
- Программа ViPNet Контроль приложений.
- Программа ViPNet Деловая почта.
- Криптопровайдер ViPNet CSP.
- Система обновления ViPNet.

### ViPNet-драйвер

ViPNet-драйвер (см. «Принцип работы ViPNet-драйвера» на стр. 18) — это низкоуровневый драйвер сетевой защиты, осуществляющий шифрование и фильтрацию IP-трафика. ViPNet-драйвер взаимодействует непосредственно с драйверами сетевых интерфейсов компьютера (реальных или их эмулируемых), что обеспечивает независимость программы от операционной системы и ее недокументированных возможностей. ViPNet-драйвер перехватывает и контролирует весь входящий и исходящий IP-трафик компьютера.

Одна из важнейших функций драйвера — эффективный контроль IP-трафика во время загрузки операционной системы. В ОС Windows для инициализации загрузки компьютера используется только одна служба. Инициализация ViPNet-драйвера и ключей шифрования ViPNet выполняется перед входом пользователя в Windows, то есть до инициализации остальных служб и драйверов операционной системы.

В результате ViPNet-драйвер первым получает контроль над стеком протоколов TCP/IP. К моменту инициализации драйверов сетевых интерфейсов ViPNet-драйвер подготовлен к шифрованию и фильтрации трафика, тем самым обеспечивается защищенное соединение с контроллером домена, контроль сетевой активности запущенных на компьютере приложений и блокирование нежелательных пакетов извне. В момент загрузки операционной системы ПО ViPNet проверяет собственные контрольные суммы, гарантирующие целостность программного обеспечения, наборов ключей и списка приложений, которым разрешена сетевая активность.

## ViPNet Монитор

Основной функцией программы ViPNet Монитор является настройка различных параметров ViPNet-драйвера (см. «Принцип работы ViPNet-драйвера» на стр. 18) и запись событий, возникающих в процессе обработки трафика драйвером, в журнал регистрации IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 193). Если выгрузить программу ViPNet Монитор из памяти компьютера, ViPNet-драйвер продолжит работу и будет обеспечивать безопасность компьютера, но в журнале регистрации IP-пакетов может отсутствовать информация о трафике, обработанном драйвером при закрытой программе ViPNet Монитор (ViPNet-драйвер может хранить в памяти не более 10000 записей журнала).

На компьютере программа ViPNet Монитор:

- Позволяет настраивать параметры встроенного сетевого экрана (см. «Интегрированный сетевой экран» на стр. 126).
- Позволяет управлять параметрами обработки прикладных протоколов (см. «Обработка прикладных протоколов» на стр. 156).
- Предоставляет встроенные функции для защищенного обмена сообщениями, проведения конференций, файлового обмена и так далее (см. «Встроенные средства коммуникации» на стр. 169).

## ViPNet MFTP

На клиентском узле (см. «Клиент (ViPNet-клиент)» на стр. 399) транспортный модуль ViPNet MFTP обеспечивает обмен управляющими конвертами, конвертами программы ViPNet Деловая почта и файлами с другими сетевыми узлами ViPNet. Подробнее о программе см. документ «ViPNet MFTP. Руководство администратора».

## ViPNet Контроль приложений

Программа «Контроль приложений» является необязательным модулем программного обеспечения ViPNet Client. Чтобы иметь возможность контролировать сетевую активность приложений на каждом компьютере, необходима специальная лицензионная запись в регистрационном файле на ПО ViPNet.

Программа «Контроль приложений» позволяет:

- Получать информацию обо всех приложениях, которые запрашивали доступ в сеть.
- Ограничивать (разрешить или запретить) доступ приложений к сети.
- Просматривать журнал событий по сетевой активности приложений.

Подробнее о программе см. документ «ViPNet Контроль приложений. Руководство пользователя».

## ViPNet Деловая почта

ViPNet Деловая почта — это программа в составе ПО ViPNet Client, предназначенная для обмена электронной почтой между пользователями сети ViPNet. С помощью программы ViPNet Деловая почта можно отправлять и получать сообщения с вложенными файлами, шифровать сообщения и вложения, подписывать сообщения и вложения электронной подписью. В программе предусмотрена система автоматической обработки входящих сообщений и файлов в соответствии с заданными правилами (автопроцессинг).

Подробная информация о программе ViPNet Деловая почта содержится в документе «ViPNet Деловая почта. Руководство пользователя».

## ViPNet CSP

Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций через интерфейс Microsoft CryptoAPI 2.0. Она позволяет использовать криптографические функции, реализованные в соответствии с российскими стандартами, в различных приложениях, например Microsoft Office.

С помощью криптопровайдера ViPNet CSP вы можете выполнять следующие операции:

- Формирование и проверка электронной подписи.
- Шифрование данных, в том числе сообщений электронной почты.
- Аутентификация и защита соединений по протоколу TLS/SSL.

---

**Внимание!** При установке программы ViPNet CSP в составе ПО ViPNet Client поддержка протокола TLS/SSL отключена. Чтобы включить поддержку протокола, в меню **Пуск** выберите **Все программы > ViPNet > ViPNet CSP**, щелкните **Установка ViPNet CSP**, в открывшемся окне выберите **Добавить и удалить компоненты**, нажмите кнопку **Продолжить**, в следующем окне раскройте список **Поддержка работы ViPNet CSP через MS Crypto API** и добавьте компонент **Поддержка протокола TLS/SSL**.

---

Подробнее об использовании криптопровайдера ViPNet CSP см. документ «ViPNet CSP. Руководство пользователя».

## Система обновления ViPNet

Система обновления ViPNet обеспечивает получение и установку в ViPNet Client обновлений ПО, справочников и ключей, отправляемых администратором сети из программы ViPNet Administrator или ViPNet Network Manager, а также обновлений политик безопасности, отправленных из программы ViPNet Policy Manager. Подробнее о работе системы обновления ViPNet см. в разделе Система обновления ViPNet (на стр. 83).

# Принцип работы ViPNet-драйвера

Ядром программного обеспечения ViPNet является ViPNet-драйвер, основной функцией которого является фильтрация, шифрование и расшифрование входящих и исходящих IP-пакетов.

Каждый исходящий пакет обрабатывается ViPNet-драйвером одним из следующих способов:

- шифруется и отправляется;
- отправляется в исходном виде (без шифрования);
- блокируется (в соответствии с установленными сетевыми фильтрами).

Каждый входящий пакет обрабатывается следующим образом:

- пропускается (если он не зашифрован и это разрешено сетевыми фильтрами для нешифрованного трафика);
- расшифровывается (если пакет был зашифрован);
- блокируется (в соответствии с установленными сетевыми фильтрами).

ViPNet-драйвер работает между канальным уровнем и сетевым уровнем модели OSI, что позволяет осуществлять обработку IP-пакетов до того, как они будут обработаны стеком протоколов TCP/IP и переданы на прикладной уровень. Таким образом, ViPNet-драйвер защищает IP-трафик всех приложений, не нарушая привычный порядок работы пользователей.


*Рисунок 1. ViPNet-драйвер в модели OSI*

Благодаря такому подходу внедрение технологии ViPNet не требует изменения сложившихся бизнес-процессов, а затраты на развертывание сети ViPNet невелики.

---

**Примечание.** На приведенной схеме модели OSI допущены следующие упрощения:

- Транспортный и сеансовый уровни объединены в транспортный уровень.
- Прикладной уровень и уровень представления объединены в прикладной уровень.

---

Следующая схема иллюстрирует работу ViPNet-драйвера при обработке запроса на просмотр веб-страницы. Страница размещена на IIS-сервере, который работает на компьютере Б.

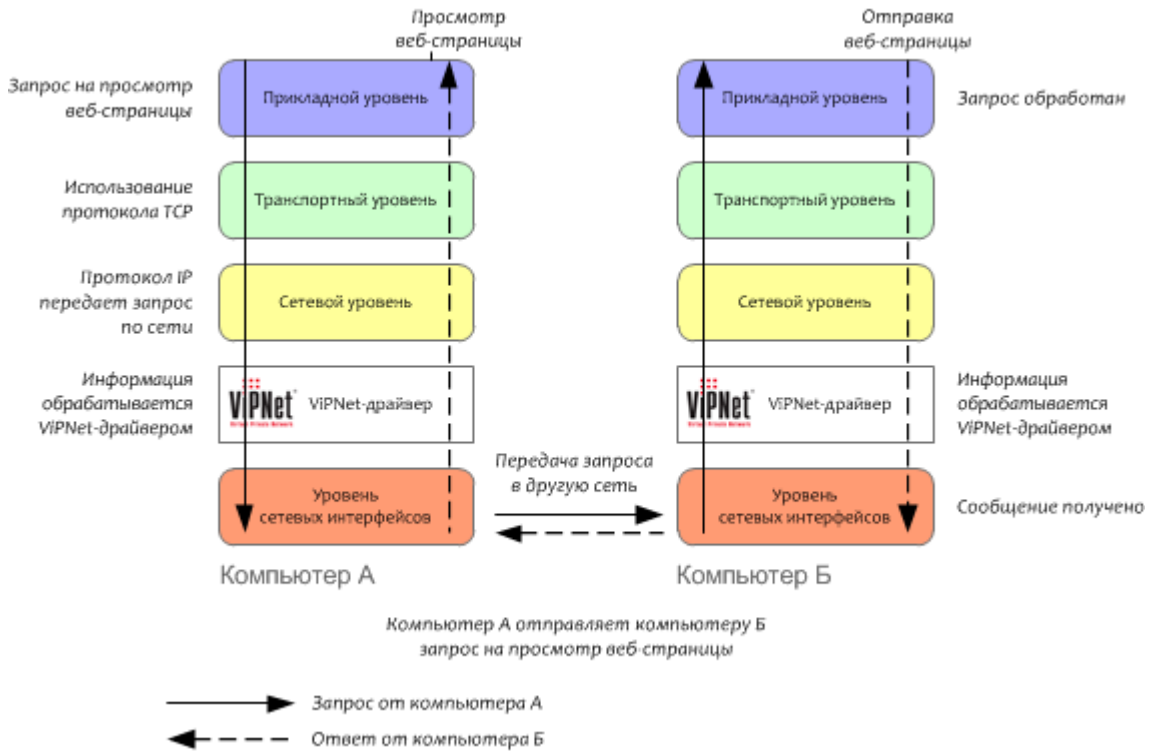



*Рисунок 2. Схема работы сети TCP/IP, защищенной ПО ViPNet*

Компьютер А отправляет на компьютер Б запрос по протоколу HTTP. Запрос передается на нижние уровни стека TCP/IP, при этом на каждом уровне к нему добавляется служебная информация. Когда запрос достигает ViPNet-драйвера, он зашифровывает запрос и добавляет к нему собственную информацию. ViPNet-драйвер, работающий на компьютере В, принимает запрос и удаляет из него служебную информацию ViPNet. Затем ViPNet-драйвер расшифровывает запрос и передает по стеку TCP/IP на прикладной уровень для обработки.

# Новые возможности версии 4.3.2

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.2 по сравнению с версией 4.3.1. Информация об изменениях в предыдущих версиях содержится в приложении История версий (на стр. 364).

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

  Раньше выполнения аутентификации с помощью сертификата необходимым условием являлось наличие назначения «Проверка подлинности клиента» в поле сертификата **Расширенное использование ключа**. Теперь для аутентификации вы можете использовать сертификат с назначением «Шифрование ключей» в поле **Использование ключа** (см. «Особенности аутентификации с помощью сертификата на устройстве» на стр. 74).

- **Изменение, касающееся поддержки операционных систем**

  Начиная с версии 4.3.2, прекращена поддержка ОС Windows XP и Windows Server 2003.

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

# Системные требования

Требования к компьютеру для установки программы ViPNet Client:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 1 Гбайт.
- Свободное место на жестком диске — не менее 150 Мбайт (рекомендуется 250 Мбайт).
- Сетевой интерфейс или модем.
- Операционная система — Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Server 2008 R2 (64-разрядная), Small Business Server 2008 (64 разрядная), Small Business Server 2008 SP2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Windows 8.1 (32/64-разрядная), Small Business Server 2011 (64 разрядная), Server 2012 (64-разрядная), Server 2012 R2 (64-разрядная), Windows 10 (32/64 разрядная).

  Для операционной системы должен быть установлен самый последний пакет обновлений.
- При использовании более ранних версий Windows, чем Windows 8, на компьютере должен быть установлен накопительный пакет обновления часовых поясов KB2570791.
- При использовании Internet Explorer — версия 6.0 или выше.

---

**Примечание.** На компьютере не должны быть установлены другие сетевые экраны (также называемые брандмауэрами).

---

# Комплект поставки

Комплект поставки ViPNet Client включает:

- Установочный файл программы.
- Документацию в формате PDF:
  - «ViPNet Client Монитор. Руководство пользователя».
  - «ViPNet Client. Быстрый старт».
  - «ViPNet Деловая почта. Руководство пользователя».
  - «ViPNet MFTP. Руководство администратора».
  - «ViPNet Контроль приложений. Руководство пользователя».
  - «ViPNet CSP. Руководство пользователя».
  - «Развертывание сети ViPNet 4.x. Руководство администратора».
  - «Классификация полномочий. Приложение к документации ViPNet 4.x».
  - «Новые возможности ViPNet Client и ViPNet Coordinator версии 4.x. Приложение к документации ViPNet».
  - «Основные термины и определения. Приложение к документации ViPNet 4.x».
  - «ViPNet Client/Coordinator. Лицензионные соглашения на компоненты сторонних производителей».
  - «ViPNet CSP. Лицензионные соглашения на компоненты сторонних производителей».

# Обратная связь

## Дополнительная информация

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

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

## Контактная информация

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

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6196,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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

# 1

# Установка, обновление и удаление ПО ViPNet Client


Установка ПО ViPNet Client 26

Установка в неинтерактивном режиме 29

Установка ViPNet Client с помощью групповых политик 31

Обновление ПО ViPNet Client 40

Добавление, удаление и восстановление компонентов ПО ViPNet Client 44

Удаление ПО ViPNet Client 46

Перенос сетевого узла на другой компьютер 47

# Установка ПО ViPNet Client

**Внимание!** На компьютере, где устанавливается ПО ViPNet Client, не должны быть установлены сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT). Использование ViPNet Client одновременно с такими программами может привести к конфликтам и вызвать проблемы с доступом в сеть.

Перед установкой ПО ViPNet Client убедитесь, что на компьютере выполнены стандартные сетевые настройки, а также правильно заданы часовой пояс, дата и время.

Если ViPNet Client устанавливается на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе ViPNet Client нужно изменить региональные настройки Windows (см. «Региональные настройки» на стр. 335).

Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

Для установки ViPNet Client требуются:

- Установочный EXE-файл программы.

  **Внимание!** Не используйте MSI-пакеты при локальной установке ПО ViPNet Client на компьютер. Эти компоненты предназначены только для сетевой установки ПО ViPNet Client с помощью групповых политик Active Directory (см. «Установка ViPNet Client с помощью групповых политик» на стр. 31).

- Дистрибутив ключей (на стр. 398) для сетевого узла (файл *.dst). Если на узле планируется работа нескольких пользователей, для каждого из них нужен отдельный дистрибутив ключей.
- Пароль пользователя сетевого узла или внешнее устройство аутентификации (см. «Внешние устройства» на стр. 345).

  Дистрибутив ключей и пароль пользователя (либо внешнее устройство) можно получить у администратора сети ViPNet.

Для установки ViPNet Client выполните следующие действия:

1 Запустите установочный файл  . Начнется установка ViPNet CSP (на стр. 17). Дождитесь, пока завершится установка ViPNet CSP и подготовка к установке ViPNet Client.

**Примечание.** После запуска файла установки может появиться предупреждение системы безопасности о невозможности проверить сертификат подписи файла установки. В этом случае см. указания раздела Невозможно проверить сертификат, которым подписан файл установки программы (на стр. 280).

2 Ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку **Продолжить**.

3 Если вы хотите, чтобы после завершения установки компьютер был перезагружен автоматически, установите соответствующий флажок.

4 Если вы хотите настроить параметры установки, нажмите кнопку **Настроить** и укажите:

- компоненты ViPNet Client, которые необходимо установить;
- путь к папке установки компонентов ViPNet Client на компьютере;
- имя пользователя и название организации;
- название папки для программы ViPNet Client в меню **Пуск**.

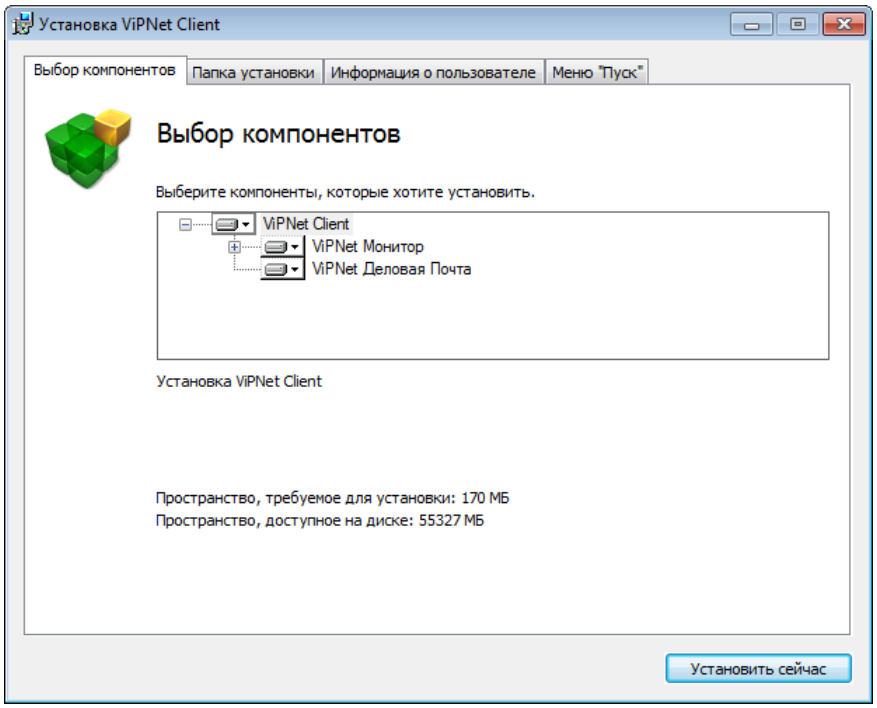



*Рисунок 3. Выбор компонентов программы ViPNet Client для установки*

5 Чтобы начать установку ViPNet Client, нажмите кнопку **Установить сейчас**.

**Примечание.** ViPNet Client можно установить в неинтерактивном режиме (см. «Установка в неинтерактивном режиме» на стр. 29). В этом случае процесс установки не будет отображаться на экране.

6 В зависимости от наличия на компьютере справочников и ключей, установленных ранее, выполните одно из действий:

- Если справочники и ключи еще не установлены на компьютере, выполните их установку (см. «Установка справочников и ключей» на стр. 51).
- Если на компьютере уже имеется ПО ViPNet, для которого ранее были установлены справочники и ключи, при запуске программы ViPNet Монитор укажите путь к папке ключей пользователя и папке ключей сетевого узла (см. «Использование справочников и ключей, установленных ранее» на стр. 60).

**Внимание!** В данном случае получать новый файл дистрибутива ключей для ПО ViPNet Client у администратора сети ViPNet и устанавливать ключи из этого файла крайне не рекомендуется, поскольку это может привести к сбоям в работе программного обеспечения ViPNet.

Если для управления сетью ViPNet используется программа ViPNet Network Manager версии ниже 4.3 или ПО ViPNet Administrator версии ниже 4.4.1, то при первом запуске программы ViPNet Монитор стандартный сетевой экран Windows будет автоматически отключен. При использовании более поздних версий состоянием сетевого экрана Windows управляет администратор сети ViPNet, поэтому при первом запуске программы ViPNet Монитор сетевой экран Windows будет включен или отключен в зависимости от настроек, заданных администратором сети ViPNet.

КС3

Соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КС3

Если в вашей организации требуется использовать средства криптографической защиты, соответствующие классу КС3, необходимо выполнить следующее:

Установите ViPNet CSP

Установите ViPNet SysLocker

# Установка в неинтерактивном режиме

В неинтерактивном режиме процесс установки ViPNet Client не отображается на экране компьютера. Установку в данном режиме можно запустить с помощью командной строки Windows. Параметры, которые обычно могут быть заданы в процессе установки, в неинтерактивном режиме следует указать заранее в командной строке.

Использование неинтерактивного режима позволяет вам выполнять удаленную установку ПО или создавать программы, которые обращаются к командной строке Windows и запускают автоматическую установку ПО с заданными параметрами.

Например, вы можете создать сценарий входа в систему (logon script), который запустит автоматическую установку ПО после загрузки системы (информацию о создании сценариев входа в систему можно найти на сайте компании Microsoft http://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx).

Чтобы запустить программу установки ПО в неинтерактивном режиме, в командной строке Windows выполните одну из команд:

- `<название установочного файла> /qn` — для установки в неинтерактивном режиме (без отображения процесса установки на экране);
- `<название установочного файла> /qb` — установка в неинтерактивном режиме с отображением индикатора выполнения установки.

При необходимости можно задать дополнительные параметры установки ViPNet Client в командной строке. После начала установки изменить параметры установки уже нельзя.

**Примечание.** Если после начала установки в неинтерактивном режиме по прошествии нескольких минут не появляется признаков завершения установки (появление ярлыка установленной программы на рабочем столе, перезагрузка компьютера), см. указания раздела Установка программы не выполняется в неинтерактивном режиме (на стр. 281).

В неинтерактивном режиме ПО ViPNet Client устанавливается в следующие папки:

- Если ПО ViPNet Client устанавливается на данный компьютер впервые:
  - В папку `C:\Program Files\InfoTeCS\ViPNet Client` при использовании 32-разрядных версий ОС Windows.
  - В папку `C:\Program Files (x86)\InfoTeCS\ViPNet Client` при использовании 64-разрядных версий ОС Windows.
- В текущую папку установки, если ПО ViPNet Client уже было установлено на компьютере.

# Дополнительные параметры установки в неинтерактивном режиме

При необходимости в командной строке укажите дополнительные параметры установки:

- Если вы хотите установить только часть компонентов ПО ViPNet Client, в командной строке задайте список нужных компонентов. Для этого используйте параметр

  `ADDLOCAL="<список компонентов>"`

  Компоненты ПО ViPNet Client:

  - Core — базовый компонент ПО (обязательный для установки).
  - Monitor — ViPNet Монитор.
  - RF — ViPNet Контроль приложений. Данный компонент может быть установлен только вместе с компонентом ViPNet Монитор.
  - BM — ViPNet Деловая почта.

  Если вы не зададите компоненты ПО с помощью параметра `ADDLOCAL`, будут установлены все компоненты.

- Если вы хотите, чтобы на рабочем столе были созданы ярлыки для установленных компонентов, используйте параметр

  `CREATESHORTCUT_DESKTOP="Yes"`

- В командной строке вы также можете указать параметры перезапуска компьютера после завершения установки:

  - `/forcerestart` — принудительная перезагрузка компьютера по окончании установки (в неинтерактивном режиме выполняется по умолчанию);
  - `/norestart` — отключение принудительной перезагрузки компьютера по окончании установки.

Пример команды для установки в неинтерактивном режиме без перезагрузки, без установки компонента ViPNet Контроль приложений и с созданием ярлыков:

```
<название установочного файла> /qn /norestart ADDLOCAL="Core,Monitor,BM"
CREATESHORTCUT_DESKTOP="Yes"
```

# Установка ViPNet Client с помощью групповых политик

**Примечание.** Подробнее об установке программного обеспечения с помощью групповых политик см. на сайте Microsoft http://support.microsoft.com/kb/816102/.

Вы можете автоматизировать установку программного обеспечения ViPNet Client на компьютеры пользователей вашей корпоративной сети с помощью групповых политик Active Directory. Настройка установки программы ViPNet Client с помощью групповых политик выполняется на контроллере домена Active Directory системным администратором домена. Необходимо обеспечить установку следующих компонентов:

- MSI-пакета программы ViPNet Client.
- MSI-пакета программы ViPNet CSP, которая является необходимым компонентом ViPNet Client. Установка ViPNet CSP должна выполняться перед установкой ViPNet Client, иначе работа ViPNet Client будет невозможна.
- MSI-пакетов, содержащих распространяемые компоненты Visual C++ (redistributables).

**Примечание.** Все указанные компоненты входят в комплект поставки ViPNet Client.

Все перечисленные компоненты имеют версии для 32-разрядных и 64-разрядных систем, поэтому для разных типов систем следует предусмотреть установку соответствующих версий программного обеспечения.

Вы можете установить только часть компонентов программ ViPNet Client и ViPNet CSP. Для этого необходимо использовать соответствующие файлы настроек в формате MST (файлы трансформации), которые содержат параметры установки и входят в комплект поставки ViPNet Client:

- `monitor_only.mst` — установка только компонента ViPNet Монитор.
- `monitor_and_bm.mst` — установка компонентов ViPNet Монитор и ViPNet Деловая почта.
- `csp_only_base.mst` — установка только базовых компонентов программы ViPNet CSP.

Рассмотрим вариант, когда в корпоративной сети одновременно используются 32-разрядные и 64-разрядные системы.

**Примечание.** Описание пользовательского интерфейса в данном разделе относится к Windows Server 2008 R2. Интерфейс других версий Windows Server может незначительно отличаться.

Чтобы установить ViPNet Client с помощью групповых политик Active Directory, создайте объект групповой политики (GPO) для всех компьютеров вашей сети. Для этого выполните следующие действия:

1 Создайте точку распространения. Для этого в общей папке по умолчанию `Netlogon` на контроллере домена создайте четыре папки и скопируйте в них следующие файлы и папки:

- MSI-пакеты ViPNet Client и ViPNet CSP для 32-разрядных систем.
- MSI-пакеты ViPNet Client и ViPNet CSP для 64-разрядных систем.
- MST-файлы, содержащие параметры установки для MSI-пакетов ViPNet Client и ViPNet CSP.
- Папки `\2008_x86`, `\2008_x64`, `\2010_x86`, содержащие MSI-пакеты и соответствующие CAB-архивы 32-разрядных и 64-разрядных версий распространяемых компонентов Visual C++ (redistributables).

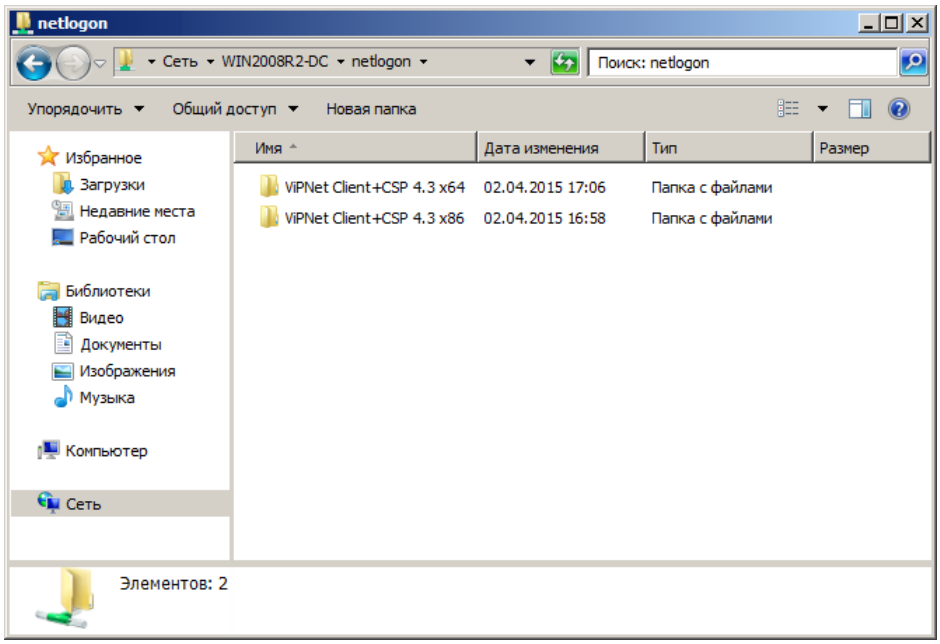



*Рисунок 4. Папки с установочными пакетами*

2 В домене Active Directory создайте отдельные группы для 32-разрядных и 64-разрядных систем, включающих компьютеры, на которые вы хотите установить ViPNet Client с помощью групповых политик. Параметры создаваемых групп оставьте по умолчанию.

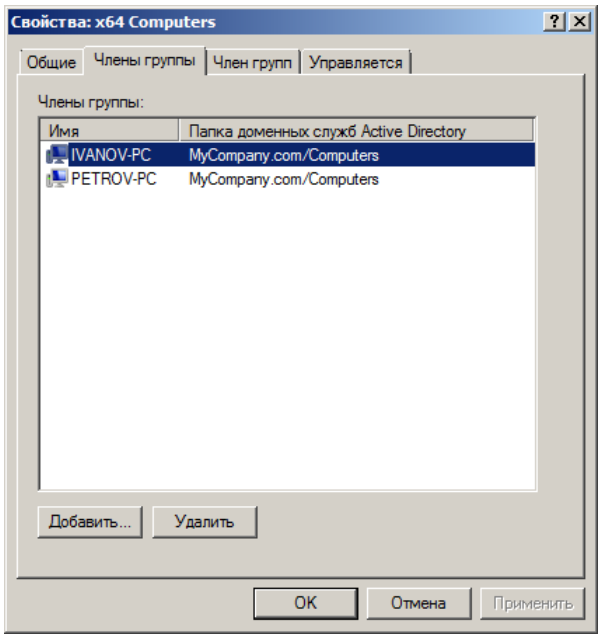



*Рисунок 5. Состав группы компьютеров с 64-разрядной операционной системой*

3 Создайте новый объект групповой политики (GPO) и свяжите его с доменом.

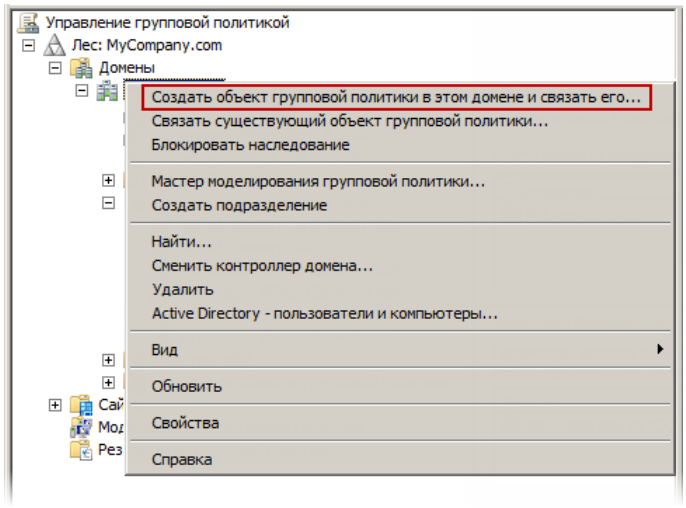



*Рисунок 6. Создание нового объекта групповой политики*

4 Откройте окно свойств объекта групповой политики и на вкладке **Область** в разделе **Фильтры безопасности** нажмите кнопку **Добавить**, чтобы добавить созданные ранее группы компьютеров.

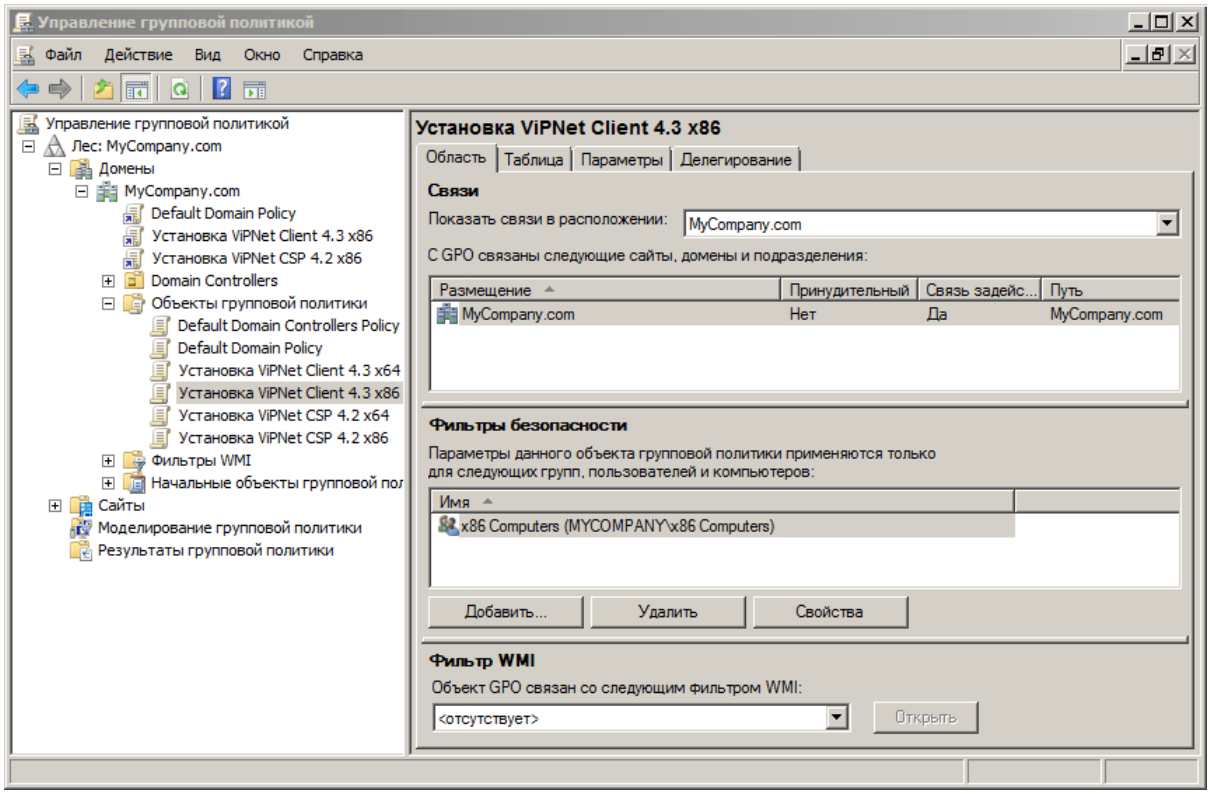



*Рисунок 7. Свойства объекта групповой политики*

5 Щелкните объект групповой политики правой кнопкой мыши и в контекстном меню выберите команду **Изменить**.

6 В открывшемся окне редактора групповых политик на панели навигации выберите раздел **Конфигурация компьютера** > **Политики** > **Конфигурация программ** > **Установка программ.**

7 Щелкните правой кнопкой мыши раздел **Установка программ**, в контекстном меню выберите **Создать** > **Пакет** и в открывшемся окне укажите путь к одному из установочных пакетов, помещенных в созданную вами точку распространения. Путь к установочным пакетам должен быть сетевым: `\\<Имя сервера>\Netlogon\<Имя_папки_с_установочным_пакетом>\`. Нажмите кнопку **Открыть**.

8 В окне **Развертывание программ** выберите один из методов развертывания:

- Если необходимо установить все компоненты установочного пакета, выберите метод развертывания **Назначенный** и нажмите кнопку **ОК**. Установочный пакет будет добавлен в раздел **Установка программ**.

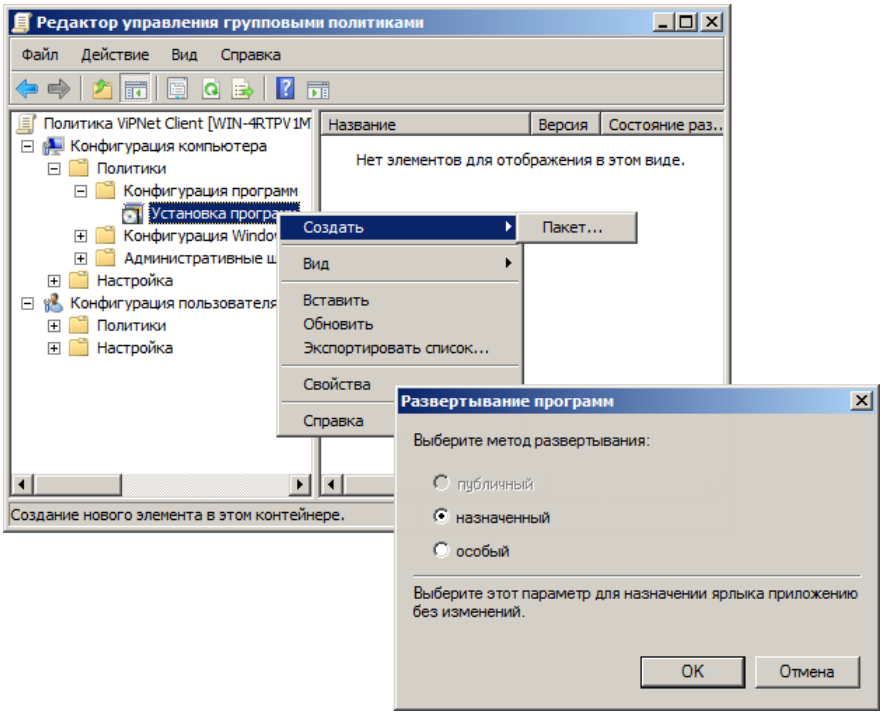



*Рисунок 8. Добавление установочного пакета*

---

**Внимание!** При добавлении установочных пакетов 32-разрядных и 64-разрядных версий распространяемых компонентов Visual C++ всегда выбирайте метод развертывания **Назначенный**.

---

- Если необходимо установить только отдельные компоненты программ ViPNet Client и ViPNet CSP, выберите метод развертывания **Особый**, нажмите кнопку **ОК** и в открывшемся окне свойств установочного пакета на вкладке **Модификации** укажите путь к соответствующему файлу MST (путь к этому файлу также должен быть сетевым).

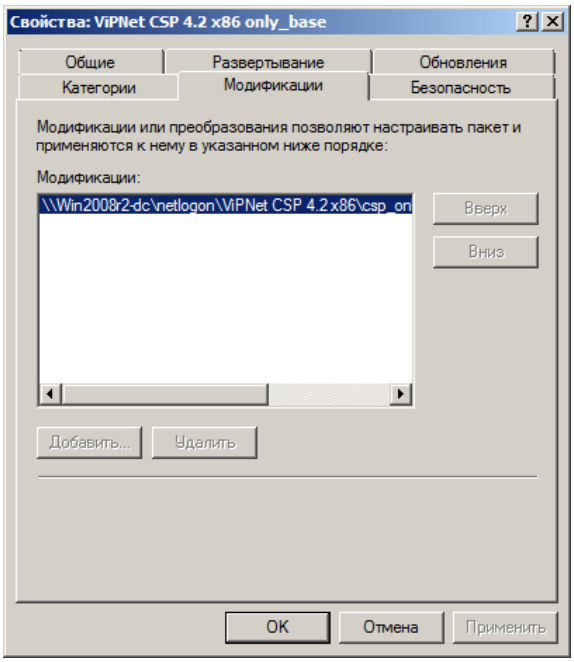



*Рисунок 9. Добавление файлов настроек MST*

9 Если окно свойств установочного пакета не открылось автоматически, дважды щелкните нужный установочный пакет  и в открывшемся окне в зависимости от выбранного установочного пакета выполните одно или несколько следующих действий:

- При добавлении установочных пакетов ViPNet Client и ViPNet CSP разной разрядности для каждого пакета на вкладке **Общие** в поле **Название** рекомендуется изменить заданное по умолчанию имя приложения, указав разрядность.

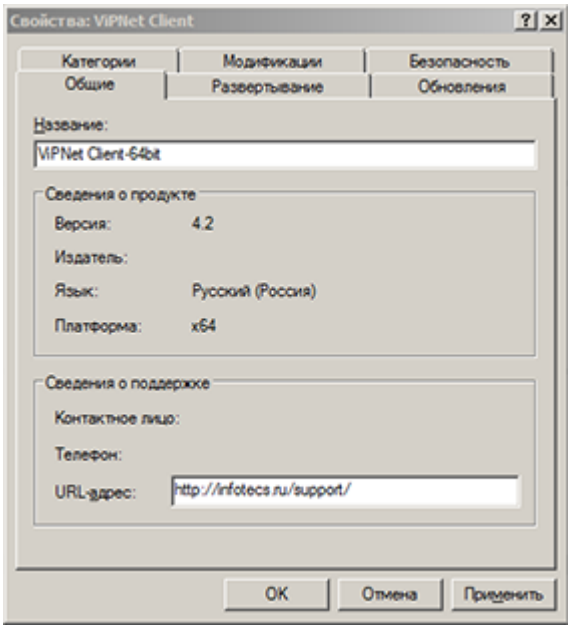



*Рисунок 10. Указание разрядности в имени добавляемого установочного пакета*

- Когда вы добавляете два установочных пакета разной разрядности для одного приложения, второй пакет по умолчанию определяется как обновление для первого. Чтобы избежать двойной установки одного пакета поверх другого и установить пакеты

нужной разрядности на соответствующие компьютеры, сделайте установочные пакеты одного приложения независимыми. Для этого при добавлении второго пакета в окне его свойств на вкладке **Обновления** выберите первый добавленный пакет и нажмите кнопку **Удалить**.

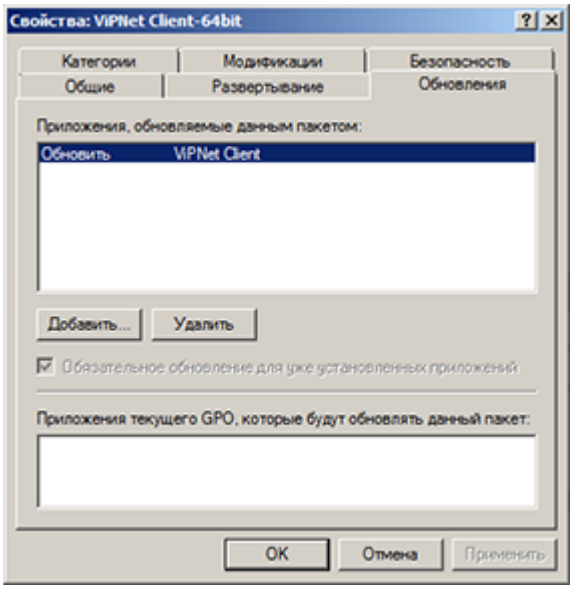



*Рисунок 11. Удаление связи между установочными пакетами*

- Для 32-разрядных версий ViPNet Client и ViPNet CSP отключите возможность установки на компьютеры с 64-разрядными системами. Для этого с помощью контекстного меню откройте окно свойств 32-разрядной версии ViPNet Client и ViPNet CSP, на вкладке **Развертывание** нажмите кнопку **Дополнительно**, в открывшемся окне снимите флажок **Сделать это 32-разрядное X86 приложение доступным для компьютеров с архитектурой Win64**.

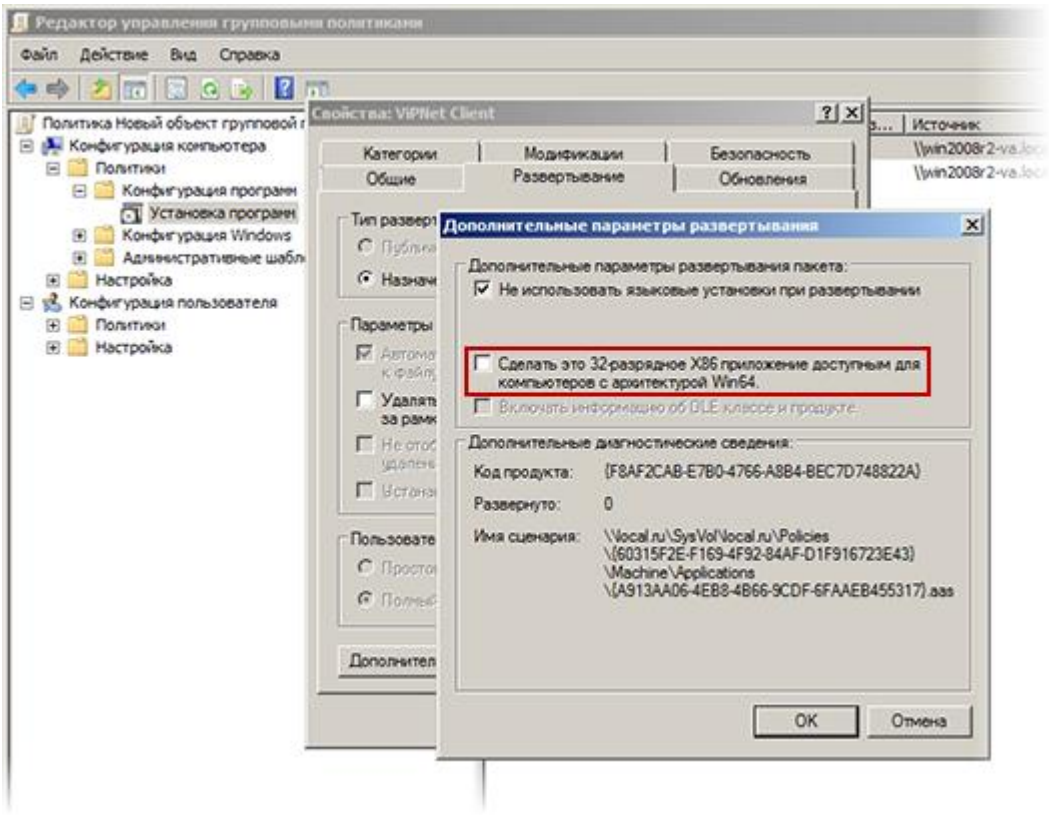



*Рисунок 12. Дополнительные настройки для 32-разрядных компонентов*

- Если языки локализации операционной системы и устанавливаемого приложения не совпадают, установите для пакета этого приложения флажок **Не использовать языковые установки при развертывании**.
- Убедитесь, что для 32-разрядных версий распространяемых компонентов Visual C++ установлен флажок **Сделать это 32-разрядное X86 приложение доступным для компьютеров с архитектурой Win64**.

10 Нажмите кнопку **OK**, чтобы сохранить выполненные настройки.

11 Повторите шаги 9-11 для каждого установочного пакета, помещенного в созданную вами точку распространения.

12 Если вы хотите вести журналирование процесса установки программ ViPNet Client и ViPNet CSP, выполните следующие действия:

12.1 Щелкните правой кнопкой мыши созданный объект групповой политики и выберите в контекстном меню команду **Изменить**.

12.2 В открывшемся окне редактора групповых политик на панели навигации выберите раздел **Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Установщик Windows**.

12.3 На панели просмотра дважды щелкните параметр **Ведение журнала событий** и в открывшемся окне установите переключатель в положение **Включить**.

12.4 Нажмите кнопку **OK**, чтобы сохранить выполненные настройки.
Журналы установки будут располагаться на компьютерах пользователей в папке `C:\ProgramData\InfoTeCS\InstallerData`.

После того как вы создадите объект групповой политики, для автоматической установки программного обеспечения ViPNet Client и других компонентов необходимо перезагрузить компьютеры пользователей.

---

**Примечание.** Обновление групповых политик на компьютерах пользователей может происходить не сразу, если на контроллере домена задан большой интервал времени для обновления политик (по умолчанию — 90 минут). Если на одном или нескольких компьютерах необходимо инициировать немедленное обновление с помощью групповых политик, на этих компьютерах в командной строке ОС Windows выполните команду `gpupdate`, а затем перезагрузите их.

---

На компьютерах пользователей установка ПО ViPNet Client будет выполняться в невидимом для пользователя режиме во время загрузки операционной системы. После установки программного обеспечения ViPNet Client и загрузки ОС на каждом сетевом узле появится сообщение с предложением установить дистрибутив ключей ViPNet.

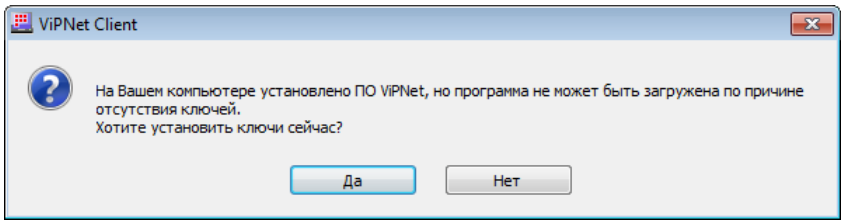



*Рисунок 13. Предложение установить ключи*

Для установки дистрибутива ключей ViPNet в окне с сообщением нажмите кнопку **Да**. Откроется окно программы установки ключей, следуйте инструкциям в разделе Установка справочников и ключей одного пользователя. При необходимости вы можете отказаться от установки дистрибутива ключей и выполнить ее позже, для этого в окне с сообщением нажмите кнопку **Нет**.

# Обновление ПО ViPNet Client

Если выпущена новая версия программы ViPNet Client, вы можете обновить программу, установленную на сетевом узле.

---

**Внимание!** Обновить программу до версии 4.x вы можете только с версии 3.2.x и выше.

Если у вас установлена программа более ранней версии, то выполните следующие действия:

- Сначала обновите программу до версии 3.2.x.
- Запустите и войдите в программу, сконвертировав ключи на устройстве, если таковые используются.
- После этого закройте и обновите программу до версии 4.x.

При несоблюдении указанных действий корректное обновление программы ViPNet Client до версии 4.x будет невозможно.

---

Перед началом обновления убедитесь, что ваша лицензия на сеть ViPNet разрешает использовать новую версию программного обеспечения. Если вы установите на сетевом узле недопустимую версию программного обеспечения, его невозможно будет запустить. В этом случае для восстановления работоспособности сетевого узла удалите новую версию программного обеспечения, затем установите версию, использование которой разрешено лицензией.

Если обновление ПО ViPNet Client выполняется на узле с установленной ОС Windows 10 либо на узле, где установлено ПО ViPNet Client, планируется обновление операционной системы до Windows 10, перед началом обновления убедитесь, что в программе ViPNet CSP отключена поддержка протокола TLS/SSL. Для этого:

1. Запустите установочный файл  программы ViPNet CSP.
2. В окне **Изменения установленных компонентов** выберите **Добавить или удалить компоненты** и нажмите кнопку **Продолжить**.
3. В окне **Выбор компонентов** убедитесь, что в списке **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** компонент **Поддержка протокола TLS/SSL** не установлен. В противном случае удалите его и нажмите кнопку **Продолжить**.

   Изменения полностью вступят в силу после перезагрузки компьютера.

Вы можете выполнить обновление несколькими способами:

- Прием обновления, отправленного централизованно на сетевые узлы администратором сети ViPNet с помощью программы ViPNet Центр управления сетью или ViPNet Network Manager. Такое обновление принимается автоматически (см. «Обновление, отправленное из ЦУСа или ViPNet Network Manager» на стр. 41).
- Обновление групповых политик Windows (см. «Обновление с помощью групповых политик» на стр. 41) либо обновление с помощью центра обновления Windows (на стр. 42). Обновления

данного типа централизованно отправляются на сетевые узлы администратором сети ViPNet с помощью средств создания групповых политик Windows.

- Обновление вручную с помощью нового установочного файла (см. «Обновление с помощью установочного файла» на стр. 42).

**Примечание.** На компьютере с операционной системой Windows Vista после начала обновления может появиться предупреждение системы безопасности о невозможности проверить сертификат подписи файла установки. В этом случае см. указания раздела Невозможно проверить сертификат, которым подписан файл установки программы (на стр. 280).

# Обновление, отправленное из ЦУСа или ViPNet Network Manager

Обновление ПО ViPNet Client, отправленное из ViPNet Administrator или ViPNet Network Manager, можно принять на сетевом узле с помощью системы обновления ViPNet (см. «О системе обновления ViPNet» на стр. 84). В зависимости от настроек системы обновления, обновление ПО принимается на сетевом узле автоматически, либо вам необходимо принять его вручную (см. «Установка обновлений вручную» на стр. 87).

# Обновление с помощью групповых политик

Администратор сети ViPNet может отправить на ваш сетевой узел обновление ПО ViPNet Client в виде обновления групповых политик. Для этого администратор использует средства управления групповыми политиками.

Полученные таким образом обновления ПО ViPNet Client устанавливаются в рамках обновления групповых политик в вашей сети и не требуют от вас каких-либо дополнительных действий.

Чтобы узнать о том, что такое групповые политики и для чего их можно использовать, перейдите по ссылке http://technet.microsoft.com/ru-ru/windowsserver/bb310732.aspx. О настройке установки с помощью групповых политик см. раздел Установка ViPNet Client с помощью групповых политик (на стр. 31).

# Обновление с помощью Центра обновления Windows

Администратор сети ViPNet может отправить на ваш сетевой узел обновление ViPNet Client, устанавливаемое с помощью Центра обновления Windows. Для этого администратор использует средства управления обновлениями (например, Microsoft System Center Essentials).

Чтобы установить полученные обновления, выполните следующие действия:

4 В меню **Пуск** выберите **Все программы** > **Центр обновления Windows**.

5 В открывшемся окне **Центр обновления Windows** проверьте наличие обновлений. При наличии обновлений будет отображаться кнопка **Установить обновления**.

6 Чтобы обновить ПО ViPNet Client, выберите для установки обновления ViPNet Client и ViPNet CSP. Затем нажмите кнопку **Установить обновления**.

7 Дождитесь завершения процесса обновления. При необходимости перезагрузите компьютер.

# Обновление с помощью установочного файла

Получите установочный файл новой версии ПО. Затем выполните следующие действия:

8 Запустите установочный файл  . Дождитесь завершения подготовки к установке ViPNet Client.

9 В окне **Обновление ViPNet Client** задайте настройки обновления:

- Если версия установленной на сетевом узле программы ViPNet CSP совпадает с версией в файле установки, в окне будет также отображен флажок **Восстановить ViPNet CSP**. Если вы установите данный флажок, то при обновлении ПО будет переустановлена программа ViPNet CSP.

---

**Совет.** Если программа ViPNet CSP на сетевом узле работает без сбоев, данный флажок можно не устанавливать. В этом случае обновление ПО будет выполнено быстрее.

---

  Если версия программы ViPNet CSP на сетевом узле не совпадает с версией в файле установки, то указанный флажок будет отсутствовать, и программа ViPNet CSP будет автоматически переустановлена.

- Если вы хотите, чтобы после обновления ViPNet Client была автоматически выполнена перезагрузка компьютера, установите соответствующий флажок.

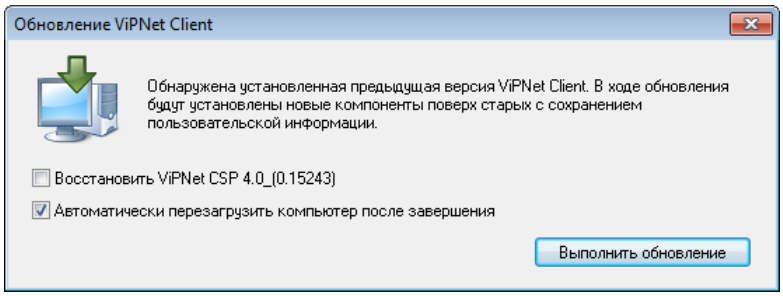



*Рисунок 14. Параметры обновления ПО*

10 Нажмите кнопку **Выполнить обновление**.

11 Если с некоторыми приложениями ViPNet работа не была завершена, может появиться сообщение о невозможности их обновления. В этом случае завершите работу с ними, после чего вы сможете продолжить обновление.

12 Дождитесь завершения обновления ПО.

Если ранее вы выбрали автоматическую перезагрузку компьютера, то после завершения установки компьютер будет автоматически перезагружен. В противном случае в окне завершения установки нажмите кнопку **Закрыть**.

# Добавление, удаление и восстановление компонентов ПО ViPNet Client

При необходимости вы можете установить или удалить компоненты ПО ViPNet Client, а также восстановить ПО при обнаружении повреждений. Например, таким образом вы можете установить программу ViPNet Деловая почта на компьютер в сети ViPNet VPN. Для выполнения данных операций вам необходимо получить установочный файл версии программы, с которой вы работаете.

---

**Примечание.** При удалении компонентов ПО ViPNet Client пользовательские данные (справочники и ключи ViPNet, настройки параметров работы программы и другие данные) сохраняются и могут использоваться после повторной установки соответствующего ПО.

---

Для установки, удаления компонентов и для восстановления ПО ViPNet Client выполните следующие действия:

13 Запустите установочный файл  , с помощью которого была выполнена первая установка ПО ViPNet Client. Дождитесь завершения подготовки к установке компонентов ViPNet Client.

14 В окне **Изменение установленных компонентов** выберите нужный пункт:

- для установки или удаления компонентов выберите **Добавить или удалить компоненты**;
- для восстановления ПО выберите **Восстановить**.

Если вы хотите, чтобы после завершения изменений в ПО перезагрузка была выполнена автоматически, установите соответствующий флажок.

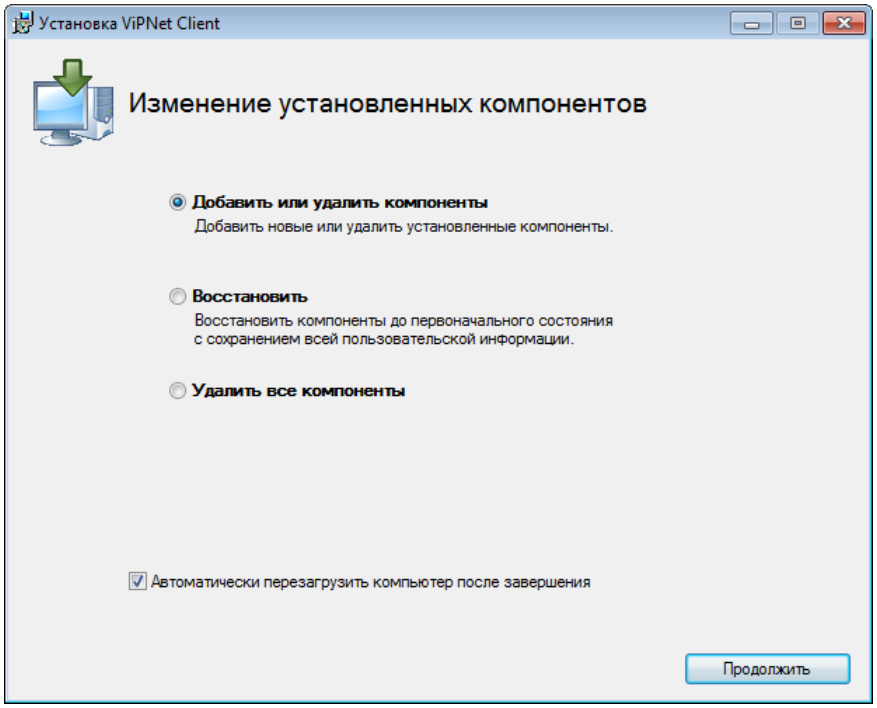



*Рисунок 15. Изменение установленных компонентов*

Затем нажмите кнопку **Продолжить**.

15 Если вы устанавливаете или удаляете компоненты ПО, на странице выбора компонентов укажите те, которые необходимо добавить или удалить. Затем нажмите кнопку **Продолжить**.

16 Дождитесь завершения установки (восстановления, удаления) компонентов ПО ViPNet Client. Затем нажмите кнопку **Закрыть**.

17 Если ранее вы выбрали автоматическую перезагрузку компьютера, компьютер будет автоматически перезагружен.

Если вы не выбрали автоматическую перезагрузку, в окне завершения обновления ПО нажмите кнопку **Закрыть**, затем самостоятельно перезагрузите компьютер.

# Удаление ПО ViPNet Client

При необходимости вы можете полностью удалить с компьютера программу ViPNet Client и все ее компоненты.

При удалении программы ViPNet Client вы можете сохранить пользовательские данные, сформированные и используемые во время работы: справочники и ключи ViPNet, настройки параметров работы программы, письма программы ViPNet Деловая почта и другие.

Чтобы полностью удалить ПО ViPNet Client с компьютера, выполните следующие действия:

1. Запустите установочный файл. Дождитесь завершения подготовки к удалению ViPNet Client.
2. На странице изменения установленных компонентов выберите пункт **Удалить все компоненты**.

   Если вы хотите, чтобы перезагрузка после удаления ПО была выполнена автоматически, установите соответствующий флажок.
3. Нажмите кнопку **Продолжить**.
4. В зависимости от того, хотите ли вы сохранить пользовательские данные, установите или снимите флажок **Удалить пользовательские данные**.
5. Для продолжения нажмите кнопку **Удалить**.

**Примечание.** Если при удалении ПО ViPNet Client вы также выбрали удаление пользовательских данных и при этом данные используются запущенными приложениями ViPNet, появится соответствующее предупреждение. В этом случае закройте все приложения ViPNet и нажмите кнопку **Повтор**.

6. Дождитесь завершения удаления программного обеспечения.

   Если ранее вы выбрали автоматическую перезагрузку компьютера, то после завершения удаления ПО компьютер будет автоматически перезагружен.

   Если вы не выбрали автоматическую перезагрузку, то в окне завершения удаления ПО нажмите кнопку **Закрыть**, затем самостоятельно перезагрузите компьютер.

**Совет.** Вы также можете полностью удалить ViPNet Client, выбрав в меню **Пуск** или на начальном экране пункт **Установка ViPNet Client**. При этом пользовательские данные будут сохранены.

# Перенос сетевого узла на другой компьютер

Чтобы перенести функционирующий узел сети ViPNet с одного компьютера на другой (например, в случае замены устаревшего компьютера), сохранив при этом текущие настройки программы ViPNet Монитор и письма программы ViPNet Деловая почта, необходимо скопировать на новый компьютер справочники и ключи, хранилище писем и другие данные из папки программы ViPNet Client.

Путем переноса справочников и ключей также можно восстановить сетевой узел после переустановки операционной системы.

**Внимание!** Не следует использовать данный сценарий для переноса сетевого узла с 32-разрядной версии операционной системы Windows на 64-разрядную версию Windows и наоборот, поскольку в этом случае возможна некорректная работа программного обеспечения ViPNet. Если есть потребность в подобном переносе, то в корректной форме его можно осуществить только путем установки на узле ПО ViPNet и справочников и ключей с помощью дистрибутива ключей.

После переноса справочников и ключей следует удалить их исходный экземпляр. Недопустима ситуация, когда на разных компьютерах установлены одни и те же ключи.

Для переноса справочников и ключей выполните следующие действия:

1. Скопируйте на съемный носитель или в другое надежное место следующие папки и файлы, находящиеся в папке установки программы ViPNet Client:
   - `\d_station`;
   - `\databases`;
   - `\Protocol` (если требуется скопировать сохраненные протоколы сеансов обмена сообщениями);
   - `\TaskDir` (если требуется сохранить файлы, принятые по файловому обмену);
   - Папки ключей пользователей, обычно `\user_AAAA` (где AAAA — шестнадцатеричный идентификатор пользователя ViPNet без номера сети).

     В некоторых случаях папка ключей пользователя может совпадать с папкой установки программы ViPNet Client, тогда следует скопировать папку `\key_disk`.
   - `\MS`;
   - `\MSArch` (папка хранения архивов программы ViPNet Деловая почта по умолчанию);
   - `autoproc.dat` (этот файл присутствует, если настроены правила автопроцессинга);
   - `wmail.ini`;

- файлы `AP*.TXT: APAXXXX.TXT`, `APCXXXX.TXT`, `APIXXXX.TXT`, `APLXXXX.TXT`, `APNXXXX.CRC`, `APNXXXX.CRG`, `APNXXXX.TXT`, `APSXXXX.TXT`, `APUXXXX.TXT` (где XXXX — шестнадцатеричный идентификатор сетевого узла без номера сети);
- `infotecs.re`;
- `iplir.cfg, iplirmain.cfg`;
- `ipliradr.do$`;
- `linkXXXX.txt`, `nodeXXXX.tun` (где XXXX — шестнадцатеричный идентификатор сетевого узла без номера сети);
- `mftp.ini`.

---

**Примечание.** По умолчанию программа ViPNet Client устанавливается в папку `C:\Program Files\InfoTeCS\ViPNet Client` в 32-битных версиях Windows и в папку `C:\Program Files (x86)\InfoTeCS\ViPNet Client` — в 64-битных версиях.

Некоторые из перечисленных файлов и папок могут отсутствовать в папке программы ViPNet Client.

---

2 Перед переносом справочников и ключей на новый компьютер установите на этот компьютер программу ViPNet Client, но не выполняйте установку справочников и ключей.

3 При переносе справочников и ключей на компьютер, на котором уже установлена программа ViPNet Client, убедитесь, что на этом компьютере не установлены справочники и ключи другого сетевого узла. Если эти данные присутствуют, удалите их, как это описано в разделе Удаление справочников и ключей (на стр. 64) либо вручную удалите следующие папки и файлы:

- папки ключей пользователей `\user_BBBB` (где BBBB — шестнадцатеричный идентификатор пользователя ViPNet без номера сети).
- файлы `AP*.TXT`, `APNYYYY.CRC`, `APNYYYY.CRG` (где YYYY — шестнадцатеричный идентификатор сетевого узла без номера сети).

4 Файлы и папки, скопированные на шаге **1**, поместите в новую папку установки программы ViPNet Client с заменой файлов.

5 Если требуется, в файле `wmail.ini` в качестве значений параметров `MSDir` и `MSArchDir` укажите путь к новой папке установки программы ViPNet Client.

6 Если требуется, в файле `mftp.ini` укажите путь к новой папке установки программы ViPNet Client в значениях всех параметров, где он встречается.

7 Удалите файл `certlist.sst`, находящийся в подпапке `\d_station\abn_AAAA` (где AAAA — шестнадцатеричный идентификатор пользователя ViPNet без номера сети).

8 Запустите программу ViPNet Монитор. В окне ввода пароля щелкните значок  справа от кнопки **Настройка** и выберите пункт **Папка ключей пользователя**. Укажите путь к папке ключей пользователя.

9 Выполните вход в программу ViPNet Монитор.

10 Установите контейнер ключей (см. «Установка контейнера ключей» на стр. 275).

11 На компьютере, с которого вы осуществили перенос сетевого узла, удалите исходные экземпляры справочников и ключей (см. «Удаление справочников и ключей» на стр. 64).

После выполнения перечисленных действий программа ViPNet Client готова к работе.

# 2

# Установка и обновление справочников и ключей


Установка справочников и ключей 51

Использование справочников и ключей, установленных ранее 60

Обновление справочников, ключей и политик безопасности 61

Удаление справочников и ключей 64

Действия при компрометации ключей 65

# Установка справочников и ключей

Установка справочников и ключей выполняется при развертывании ПО ViPNet на сетевом узле, при добавлении новых пользователей ViPNet на сетевой узел, а также в других случаях, когда справочники и ключи, установленные на узле, были повреждены или являются устаревшими.

Если вы хотите выполнить первоначальную установку справочников и ключей на сетевом узле с одним пользователем, выполните рекомендации раздела Установка справочников и ключей одного пользователя (на стр. 52).

В случаях, описанных ниже, перед установкой дополнительно ознакомьтесь с соответствующими разделами:

- Если вы хотите организовать работу нескольких пользователей на одном сетевом узле или добавить нового пользователя на сетевой узел, на котором уже работают другие пользователи, см. раздел Установка справочников и ключей нескольких пользователей на одном сетевом узле (на стр. 54).
- Если вы хотите самостоятельно задать папки, в которых будут храниться справочники и ключи, см. раздел Расширенный режим установки справочников и ключей (на стр. 54).
- Если на сетевом узле имеется несколько программ ViPNet, но ни для одной из них не установлены справочники и ключи, см. раздел Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet (на стр. 56).

**Примечание.** Если на узле уже установлены справочники и ключи для какой-либо программы ViPNet, выполните указания раздела Использование справочников и ключей, установленных ранее (на стр. 60).

- Если вы хотите установить справочники и ключи с использованием командной строки Windows, см. раздел Установка справочников и ключей в неинтерактивном режиме (на стр. 57).
- Если в результате программного или системного сбоя вы не можете войти в программу ViPNet Монитор и необходимо выполнить повторную установку справочников и ключей, см. раздел Повторная установка справочников и ключей после сбоя программы (на стр. 58).

В сети ViPNet, управляемой с помощью ПО ViPNet Administrator, в составе первоначального дистрибутива ключей каждому пользователю передается резервный набор персональных ключей (РНПК) (на стр. 402). Файл, в котором содержится резервный набор ключей, имеет вид `AAAA.pk` (где `AAAA` — идентификатор пользователя в сети ViPNet). Во время установки справочников и ключей он помещается в папку ключей пользователя (см. «Папка ключей пользователя» на стр. 401).

Из соображений безопасности после первичной установки справочников и ключей рекомендуется переместить файл резервного набора из папки ключей пользователя на внешнее устройство для хранения в безопасном месте, не доступном для посторонних лиц (например, в сейфе). После получения резервного набора ключей пользователи сети ViPNet несут личную ответственность за его хранение.

**Внимание!** Если обнаружен факт доступа посторонних лиц к вашему резервному набору ключей либо если вы подозреваете, что такой факт имел место, следуйте рекомендациям раздела Действия при компрометации ключей (на стр. 65).

# Установка справочников и ключей одного пользователя

Для установки справочников и ключей выполните следующие действия:

1. Получите дистрибутив ключей у администратора сети ViPNet.
2. Завершите работу всех компонентов программы ViPNet Client (см. «Завершение работы с программой ViPNet Монитор» на стр. 77).
3. Запустите программу установки ключей сети ViPNet одним из двух способов:
   - Дважды щелкните файл дистрибутива ключей.
   - Запустите программу ViPNet Монитор. Затем в окне ввода пароля щелкните значок справа от кнопки **Настройка** и в меню выберите пункт **Установить ключи**.

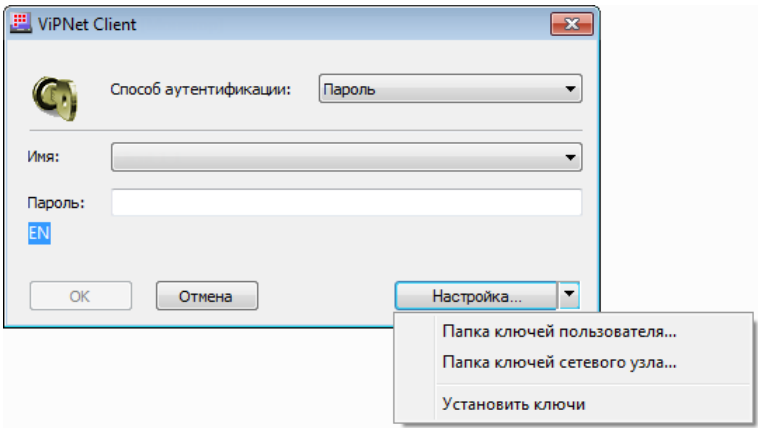



*Рисунок 16. Запуск программы установки ключей*

4. Если при запуске программы установки ключей будут обнаружены работающие приложения ViPNet, будет выведено сообщение о необходимости завершить их работу. Закройте указанные приложения и нажмите кнопку **Повтор**.
5. Если на странице **Укажите файл дистрибутива ключей** не указано местоположение файла дистрибутива, задайте его с помощью кнопки **Обзор**.
6. Убедитесь, что выбран дистрибутив ключей, предназначенный именно для текущего сетевого узла. Имя сетевого узла и имя пользователя отображаются ниже поля для указания пути к файлу дистрибутива. При необходимости укажите другой дистрибутив ключей.

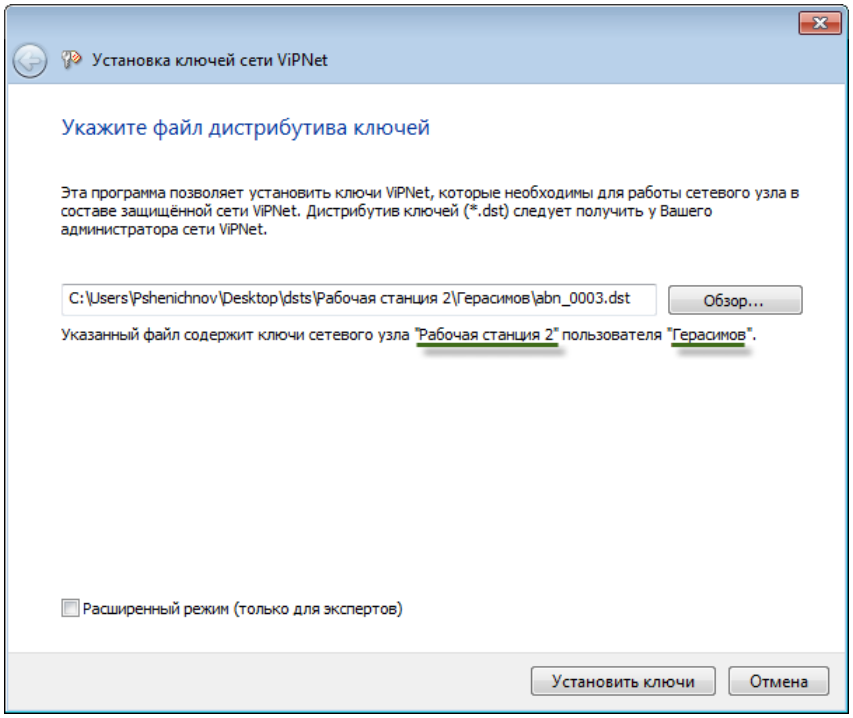



*Рисунок 17. Выбор файла дистрибутива ключей*

По умолчанию справочники и ключи устанавливаются в ту же папку, что и программа ViPNet Client. При необходимости вы можете указать другие папки для их установки (см. «Расширенный режим установки справочников и ключей» на стр. 54).

7 Нажмите кнопку **Установить ключи**.

---

**Примечание.** Кнопка **Установить ключи** может быть скрыта в том случае, если на сетевом узле установлено несколько программ ViPNet (см. «Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet» на стр. 56).

---

8 Если установка ключей прошла успешно, появится соответствующее сообщение.

9 Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях**. Для завершения установки ключей нажмите кнопку **Закрыть**.

Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

После успешной установки ключей можно запустить ПО ViPNet Client.

# Установка справочников и ключей нескольких пользователей на одном сетевом узле

Если на сетевом узле планируется работа нескольких пользователей, установите ключи для каждого пользователя.

Если на сетевом узле уже работают пользователи, и вы хотите добавить на узел новых пользователей, для установки вам понадобятся только ключи новых пользователей.

**Примечание.** Справочники и ключи нескольких пользователей из разных сетей ViPNet не могут быть установлены на одном компьютере.

Для установки справочников и ключей нескольких пользователей на одном компьютере выполните следующие действия:

1. Для каждого нового пользователя получите дистрибутив ключей у администратора сети ViPNet.
2. Последовательно выполните установку справочников и ключей (см. «Установка справочников и ключей одного пользователя» на стр. 52) с использованием дистрибутива каждого нового пользователя.

В результате в окне входа в программу в списке учетных записей будут отображаться пользователи, справочники и ключи которых вы установили.

# Расширенный режим установки справочников и ключей

По умолчанию справочники и ключи устанавливаются в папку установки программы. При необходимости вы можете использовать расширенный режим установки, который позволяет вам самостоятельно задать папки для установки справочников и ключей. Такая необходимость может возникнуть, если:

- из соображений безопасности вы хотите хранить справочники и ключи на специальном съемном носителе;
- у вас нет прав на изменение и запись файлов в папке `C:\Program Files\` или `C:\Program Files (x86)\` (в том числе в папке установки программы).

Папки, в которые производится установка справочников и ключей в расширенном режиме установки, должны отвечать следующим требованиям:

- В папках не должны находиться справочники и ключи другой программы ViPNet.
- У вас должно быть право на изменение и запись файлов в данных папках.

- Информационная защита папок должна отвечать требованиям безопасности вашей организации.
- ПО ViPNet Client должно иметь постоянный доступ к данным папкам.

---

**Внимание!** Неправильно заданные параметры установки могут привести к сбоям в работе программы. Не рекомендуется использовать данный режим без необходимости.

---

Для установки ключей в расширенном режиме выполните следующие действия:

1 Получите новый дистрибутив ключей у администратора сети ViPNet.

2 Следуйте указаниям раздела Установка справочников и ключей одного пользователя (на стр. 52).

На странице указания файла дистрибутива ключей (см. Рисунок 10 на стр. 53) установите флажок **Расширенный режим (только для экспертов)** и нажмите кнопку **Далее**.

3 На следующей странице мастера:

- В поле **Папка ключей сетевого узла** укажите папку для установки справочников и ключей сетевого узла.
- В поле **Папка ключей пользователя** (на стр. 401) укажите папку для установки ключей пользователя.

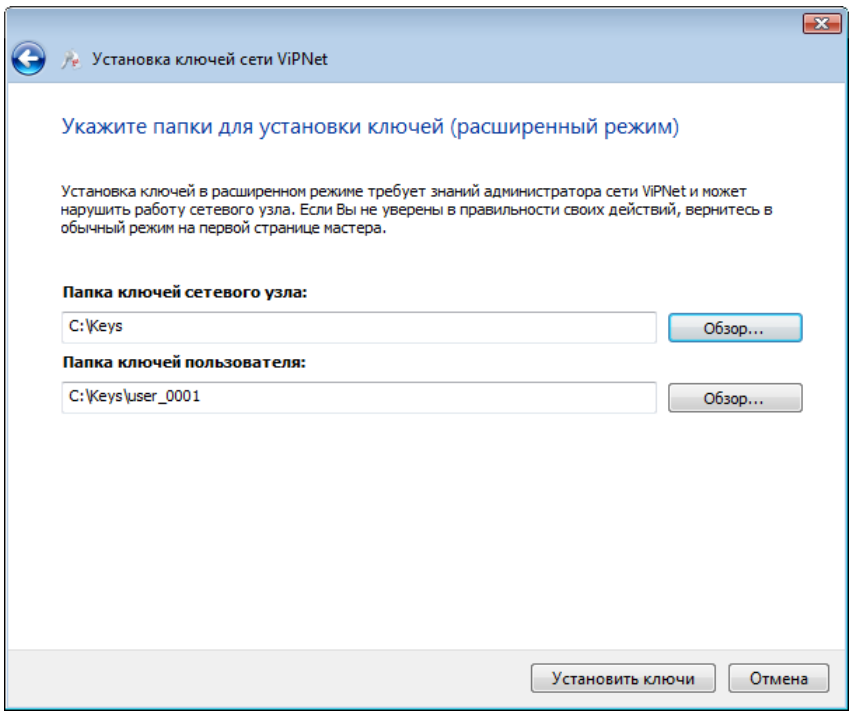



*Рисунок 18. Указание папок для установки ключей узла и ключей пользователя в расширенном режиме*

4 Для начала установки нажмите кнопку **Установить ключи**.

5 Если установка ключей прошла успешно, в завершающем окне будет выведено соответствующее сообщение. Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях**. Для завершения установки ключей нажмите кнопку **Закрыть**.

   Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

6 При первом запуске программы ViPNet Client укажите папки, в которые были установлены ключи сетевого узла и пользователя:

   - В окне ввода пароля щелкните значок  справа от кнопки **Настройка** и выберите пункт **Папка ключей сетевого узла**. В окне **Обзор папок** укажите путь к папке ключей узла.
   - Снова щелкните значок  справа от кнопки **Настройка** и выберите пункт **Папка ключей пользователя**. Укажите путь к папке ключей пользователя.

# Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet

Если на сетевом узле установлено несколько программ ViPNet, но при этом ни для одной из них не установлены справочники и ключи, то необходимо указать приложение, в папке установки которого будут храниться справочники и ключи.

**Внимание!** Если на узле уже имеются справочники и ключи для какой-либо из программ ViPNet, устанавливать новые справочники и ключи нельзя. В этом случае выполните указания раздела Использование справочников и ключей, установленных ранее (на стр. 60).

Для установки справочников и ключей выполните следующие действия:

1 Начните установку справочников и ключей (см. «Установка справочников и ключей одного пользователя» на стр. 52). После указания файла дистрибутива ключей нажмите кнопку **Далее**.

2 В окне выбора приложения ViPNet выберите **ViPNet Client**. В результате для установки справочников и ключей будет использована папка установки ПО ViPNet Client.

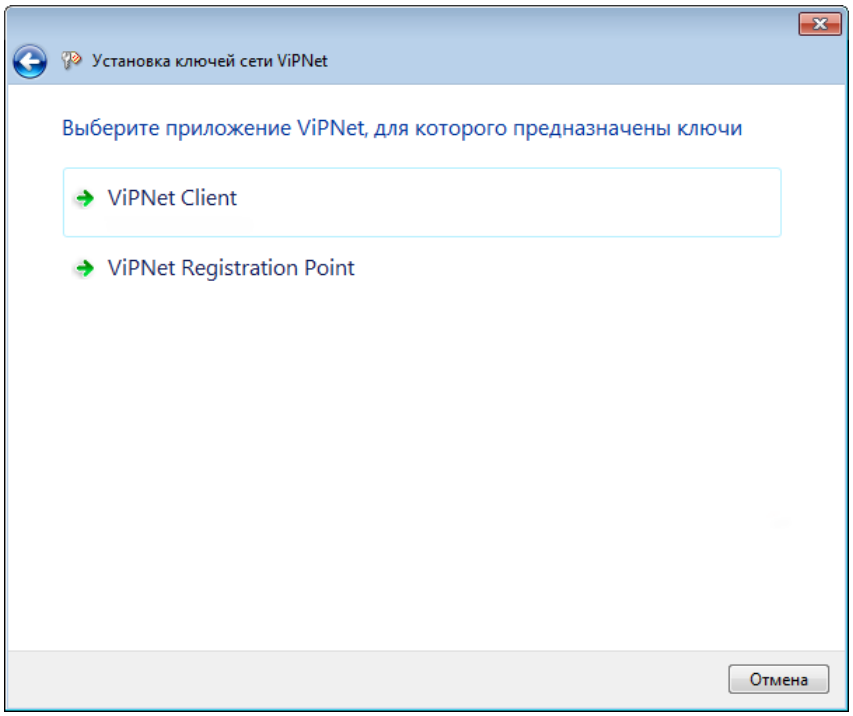



*Рисунок 19. Выбор программы, для которой устанавливаются ключи*

**Примечание.** В расширенном режиме установки ключей (см. «Расширенный режим установки справочников и ключей» на стр. 54) данное окно не отображается.

3 Если установка ключей прошла успешно, в завершающем окне будет выведено соответствующее сообщение. Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях**. Для завершения установки ключей нажмите кнопку **Закрыть**.

   Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

4 При первом запуске других программ ViPNet, установленных на узле, в качестве папки ключей узла укажите папку установки программы ViPNet Client.

После успешной установки ключей можно запустить ПО ViPNet Client.

# Установка справочников и ключей в неинтерактивном режиме

В неинтерактивном режиме процесс установки справочников и ключей не отображается на экране компьютера. Установку в данном режиме можно запустить с помощью командной строки Windows. Параметры установки, которые обычно могут быть заданы в процессе установки (см. «Установка

справочников и ключей одного пользователя» на стр. 52), в неинтерактивном режиме следует указать заранее в командной строке.

Использование неинтерактивного режима позволяет вам выполнять удаленную установку справочников и ключей или создавать программы, которые обращаются к командной строке Windows и запускают автоматическую установку справочников и ключей с заданными параметрами.

Например, вы можете создать сценарий входа в систему (logon script), который запустит автоматическую установку справочников и ключей после загрузки системы (информацию о создании сценариев входа в систему можно найти на сайте компании Microsoft http://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx).

Чтобы запустить программу установки справочников и ключей в неинтерактивном режиме, в командной строке Windows выполните команду:

```
keysetup <файл *.dst> /td <путь к папке для установки справочников и ключей> /term
/check
```

Например:

```
"C:\Program Files (x86)\InfoTeCS\ViPNet Client\keysetup" "C:\keys\abn_0002.dst" /td
"C:\Program Files (x86)\InfoTeCS\ViPNet Client" /term /check
```

**Внимание!** В качестве папки для установки справочников и ключей можно указывать только существующую папку. При указании несуществующей папки установка ключей произведена не будет.

После успешного выполнения данной команды можно запустить ПО ViPNet Client.

**Совет.** Чтобы узнать больше о возможностях использования командной строки Windows для установки справочников и ключей, выполните команду:

```
keysetup /?
```

# Повторная установка справочников и ключей после сбоя программы

Если в результате программного или системного сбоя вы не можете войти в программу ViPNet Монитор, рекомендуется обратиться в службу поддержки для восстановления доступа к программе. В исключительных случаях вы можете получить у администратора сети ViPNet новый дистрибутив ключей и выполнить повторную установку справочников и ключей.

**Внимание!** Крайне не рекомендуется проводить повторную установку справочников и ключей без особой необходимости, поскольку в этом случае не гарантируется сохранность пользовательских данных, сформированных компонентами ПО ViPNet Client (например, писем программы ViPNet Деловая почта).

Если с момента установки ключей до момента сбоя имели место смена мастер-ключей в сети ViPNet или компрометация ключей, при повторной установке ключей будет потерян доступ к зашифрованным письмам программы ViPNet Деловая почта (в том числе в архивах), защищенным сообщениям и другим пользовательским данным, сформированным компонентами ViPNet Client.

Если перечисленных выше событий не происходило, то повторная установка ключей будет выполнена как обновление справочников и ключей с помощью дистрибутива ключей (на стр. 62), и пользовательские данные сохранятся.

Для повторной установки справочников и ключей на сетевом узле выполните следующие действия:

1. Получите у администратора сети ViPNet новый дистрибутив ключей.
2. Установите справочники и ключи (см. «Установка справочников и ключей одного пользователя» на стр. 52), используя полученный дистрибутив.

# Использование справочников и ключей, установленных ранее

В момент установки программы ViPNet Client на сетевом узле уже могут иметься другие программы ViPNet, для работы которых установлены справочники, ключи сетевого узла и транспортный модуль MFTP. В этом случае задайте в программе ViPNet Client папку ключей сетевого узла, которую используют установленные ранее программы ViPNet.

---

**Примечание.** Если на сетевом узле не установлены справочники и ключи ни для одной из программ ViPNet, выполните указания раздела Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet (на стр. 56).

---

Чтобы указать папку ключей сетевого узла, выполните следующие действия:

1. Запустите программу ViPNet Монитор.
2. В окне ввода пароля щелкните значок справа от кнопки **Настройка** и выберите пункт **Папка ключей сетевого узла**.
3. В окне **Обзор папок** укажите путь к нужной папке ключей узла.

---

**Примечание.** По умолчанию папка ключей сетевого узла совпадает с папкой установки программного обеспечения ViPNet.

---

После задания папки ключей сетевого узла вы можете приступать к работе с программой ViPNet Client.

# Обновление справочников, ключей и политик безопасности

Для поддержания работоспособности узла следует регулярно обновлять справочники, ключи и политики безопасности.

Если администратор сети ViPNet вносит какие-либо изменения в структуру сети или настройки отдельных сетевых узлов, например, создает новые связи между сетевыми узлами, то автоматически изменяются справочники и ключи для сетевых узлов. Обновления справочников и ключей создаются администратором сети в программе ViPNet Administrator или ViPNet Network Manager.

При изменениях правил безопасности в сети ViPNet администратор безопасности рассылает на сетевые узлы обновленные политики безопасности. Политика безопасности, полученная сетевым узлом из программы ViPNet Policy Manager, определяет текущую политику безопасности узла, совместно с сетевыми фильтрами, настроенными на самом узле (см. «Общие сведения о сетевых фильтрах» на стр. 129). Текущая политика безопасности узла действительна для всех пользователей, зарегистрированных на узле, и для всех конфигураций программы ViPNet Монитор. При добавлении новых пользователей или конфигураций к ним также применяется текущая политика.

Обновления справочников, ключей и политик безопасности могут быть приняты на сетевом узле с помощью системы обновления ViPNet (см. «О системе обновления ViPNet» на стр. 84). Если по каким-либо причинам обновление справочников и ключей с помощью системы обновления не может быть выполнено, вы можете выполнить его вручную с помощью дистрибутива ключей (см. «Обновление справочников и ключей с помощью дистрибутива ключей» на стр. 62).

## Прием централизованных обновлений

Обновления справочников и ключей передаются на сетевые узлы из программы ViPNet Administrator или ViPNet Network Manager, а обновления политик безопасности — из программы ViPNet Policy Manager.

Обновления справочников, ключей и политик безопасности можно принять на сетевом узле с помощью системы обновления ViPNet (см. «О системе обновления ViPNet» на стр. 84). В зависимости от настроек системы обновления, данные обновления могут быть приняты на сетевом узле автоматически сразу после их получения либо обновление потребуется выполнить вручную.

# Обновление справочников и ключей с помощью дистрибутива ключей

Если по каким-либо причинам обновление справочников и ключей не может быть принято по сети (см. «Обновление справочников, ключей и политик безопасности» на стр. 61), вы можете выполнить обновление вручную с помощью дистрибутива ключей. Для этого:

1 Получите новый дистрибутив ключей у администратора сети ViPNet.

Следуйте указаниям раздела Установка справочников и ключей одного пользователя (на стр. 52) с использованием нового дистрибутива.

При указании дистрибутива ключей (см. Рисунок 10 на стр. 53) автоматически проверяется соответствие между установленными ранее ключами и новыми ключами, которые находятся в указанном файле дистрибутива ключей (например, предназначены ли данные ключи для одного и того же сетевого узла).

**Внимание!** При установке ключей в расширенном режиме (см. «Расширенный режим установки справочников и ключей» на стр. 54) данное сопоставление ключей производиться не будет.

2 Для установки справочников и ключей нажмите кнопку **Установить ключи** (см. Рисунок 10 на стр. 53).

Если кнопка недоступна, это значит, что обнаружены несоответствия между новыми и установленными ранее ключами. Для получения информации о выявленных несоответствиях нажмите кнопку **Далее**. В зависимости от характера несоответствия появится сообщение одного из двух типов:

- Если выбранный дистрибутив содержит ключи другого сетевого узла, формат ключей в дистрибутиве отличается от формата текущих ключей, а также в ряде других случаев будет выведено предупреждение, содержащее описание выявленного несоответствия.

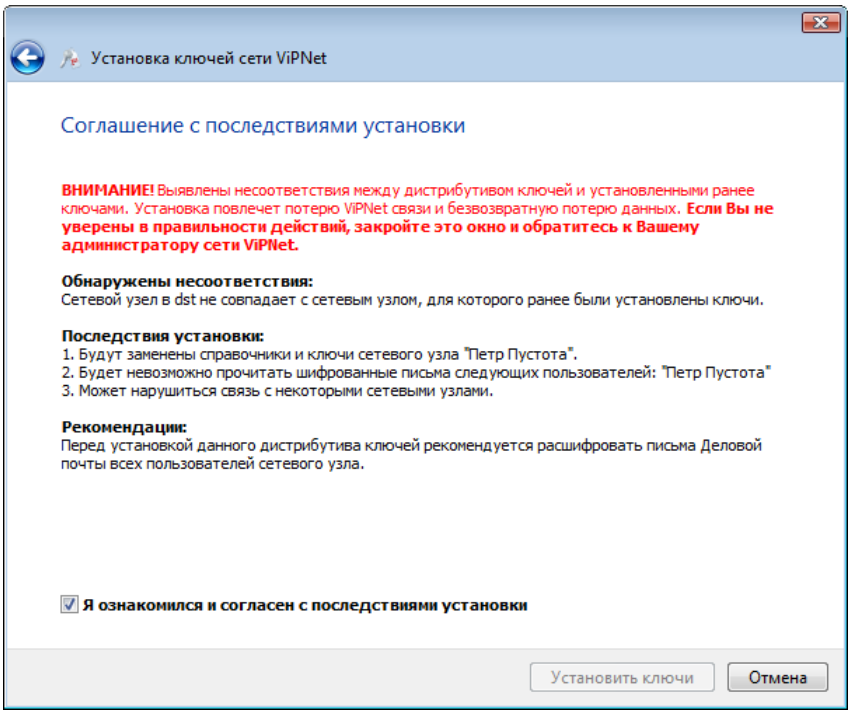



*Рисунок 20. Обнаружено несоответствие между дистрибутивом и текущими ключами на узле*

- Чтобы отказаться от установки ключей, нажмите кнопку **Отмена**, затем в окне подтверждения нажмите кнопку **Да**.

---

**Внимание!** Если вы хотите продолжить установку, ознакомьтесь с информацией о возможных последствиях и проконсультируйтесь у администратора вашей сети ViPNet. Перед продолжением установки рекомендуется завершить работу мастера с помощью кнопки **Отмена**, расшифровать письма программы ViPNet Деловая почта и затем повторно запустить мастер установки ключей.

---

- Для продолжения установите флажок **Я ознакомился и согласен с последствиями установки**, затем нажмите кнопку **Установить ключи**.

- Если выбранный дистрибутив не может быть установлен (например, он создан для другой программы ViPNet), будет выведено сообщение об ошибке, и дальнейшая установка будет невозможна. Ознакомьтесь с информацией о выявленном несоответствии и нажмите кнопку **Закрыть**.

В случае отказа от установки в результате несоответствий новых и установленных ранее ключей обратитесь за помощью к администратору сети ViPNet.

3 Завершите установку согласно указаниям раздела Установка справочников и ключей одного пользователя (на стр. 52).

После успешного обновления ключей можно запустить ПО ViPNet.

# Удаление справочников и ключей

Удаление справочников и ключей может потребоваться при переносе сетевого узла на другой компьютер (см. «Перенос сетевого узла на другой компьютер» на стр. 47).

Чтобы удалить справочники и ключи, завершите работу с программой (см. «Завершение работы с программой ViPNet Монитор» на стр. 77), затем в командной строке Windows выполните команду:

```
keysetup /clean /td <папка, в которой находятся справочники и ключи>
```

Например:

```
"C:\Program Files (x86)\InfoTeCS\ViPNet Client\keysetup" /clean / td "C:\Program Files (x86)\InfoTeCS\ViPNet Client"
```

В результате выполнения данной команды все справочники и ключи, находящиеся в указанной папке, будут удалены.

# Действия при компрометации ключей

Под компрометацией ключей подразумевается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Различают явную и неявную компрометацию ключей:

- Явной называют компрометацию, факт которой становится известным в течение срока действия данного ключа.
- Неявной называют компрометацию ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа. Неявная компрометация представляет наибольшую опасность.

Основные события, при которых ключи можно считать скомпрометированными, перечислены ниже:

1. Посторонним лицам мог стать доступным файл дистрибутива ключей.
2. Посторонним лицам могло стать доступным внешнее устройство с ключами пользователя.
3. Посторонним лицам мог стать доступным пароль пользователя, и эти лица могли иметь доступ к компьютеру пользователя.
4. Посторонние лица могли получить неконтролируемый физический доступ к ключам пользователя, хранящимся на компьютере.
5. На компьютере, подключенном к сети, не установлена программа ViPNet Монитор или в программе была отключена защита трафика. При этом:
   - в локальной сети возможно присутствие посторонних лиц;
   - на границе локальной сети отсутствует (отключен) межсетевой экран.
6. Был уволен сотрудник, имевший доступ к ключам.
7. Входящий документ подписан аннулированным сертификатом, находящимся в списке аннулированных сертификатов (см. «Список аннулированных сертификатов (CRL)» на стр. 403).
8. Случаи, когда нельзя достоверно установить, что произошло с внешними устройствами (например, внешнее устройство вышло из строя, и существует возможность того, что это произошло в результате несанкционированных действий злоумышленника).

К событиям, требующим проведения расследования и принятия решения о факте компрометации, также относится возникновение подозрений в утечке информации или ее искажение в системе конфиденциальной связи.

При наступлении любого из перечисленных выше событий:

- Немедленно прекратите работу на сетевом узле и сообщите о факте компрометации (или предполагаемом факте компрометации) администратору сети ViPNet.
- Если скомпрометированы только ключи подписи, прекратите использование этих ключей для подписи документов и сообщите администратору сети ViPNet.
- Если есть подозрение, что посторонние лица могут знать пароль пользователя ViPNet, но эти посторонние лица не имеют доступа к компьютеру, смените пароль и продолжайте работу. Если доступ посторонних лиц к компьютеру пользователя возможен, то следует считать ключи скомпрометированными.

В сети ViPNet, управляемой с помощью ПО ViPNet Administrator, на случай компрометации ключей пользователя предусмотрена возможность дистанционного обновления ключей с помощью резервного набора персональных ключей (РНПК). Файл резервного набора (`AAAA.pk`, где AAAA — идентификатор пользователя в сети ViPNet) входит в состав первоначального дистрибутива ключей и при установке справочников и ключей помещается в папку ключей пользователя (см. «Установка справочников и ключей» на стр. 51).

Если текущий персональный ключ пользователя оказался скомпрометирован, администратор программы ViPNet Удостоверяющий и ключевой центр высылает пользователю новые ключи, защищенные с помощью очередного варианта персонального ключа, который не нужно передавать по сети, так как он уже содержится в резервном наборе. Если при обновлении файл резервного набора не найден, требуется указать путь к этому файлу. Если резервный набор персональных ключей отсутствует или не подходит пароль, откажитесь от ввода данных и обратитесь к администратору программы ViPNet Удостоверяющий и ключевой центр, чтобы получить его копию.

# 3

# Начало работы с ПО ViPNet Client


Запуск программы ViPNet Монитор 68

Завершение работы с программой ViPNet Монитор 77

Интерфейс программы ViPNet Монитор 78

# Запуск программы ViPNet Монитор

ViPNet-драйвер активирует фильтрацию трафика во время загрузки операционной системы Windows еще до аутентификации в программе ViPNet Монитор. При этом работа ViPNet-драйвера определяется предустановленными фильтрами защищенной сети и фильтрами открытой сети, которые использовались в предыдущем сеансе работы. Полную защиту трафика, включающую его шифрование, ViPNet-драйвер обеспечивает после аутентификации в программе ViPNet Монитор.

Перед окончанием загрузки Windows появится окно входа в программу ViPNet Монитор. Для запуска программы введите пароль или подключите внешнее устройство аутентификации (см. «Способы аутентификации пользователя» на стр. 70).

---

**Примечание.** Чтобы выполнить аутентификацию в программе ViPNet Монитор во время загрузки Windows, вы можете использовать экранную клавиатуру. Для этого нажмите кнопку  и в меню выберите пункт **Экранная клавиатура**.

---

Чтобы отказаться от запуска программы ViPNet Монитор, нажмите кнопку **Отмена**, в этом случае шифрование трафика будет отключено.

---

**Внимание!** В зависимости от уровня полномочий пользователя, который определяется в ViPNet Центр управления сетью (см. «Использование программы ViPNet Монитор в условиях ограниченных полномочий» на стр. 81), возможность отказа от запуска ViPNet Монитор и отключения шифрования трафика может быть недоступна. **З**агрузка Windows не будет завершена, пока вы не выполните вход в программу ViPNet Монитор.

В случае если вы забыли пароль входа в программу ViPNet Монитор или внешнее устройство аутентификации повреждено, обратитесь к администратору вашей сети ViPNet за дистрибутивом ключей, загрузите операционную систему Windows в безопасном режиме и повторно установите ключи пользователя (см. Установка справочников и ключей одного пользователя на стр. 52).

---

Если вы вышли из программы (см. «Завершение работы с программой ViPNet Монитор» на стр. 77) или отказались от аутентификации при загрузке Windows, то для запуска программы ViPNet Монитор:

1. Выполните одно из действий:
   - Если вы используете операционную систему Windows 7, Windows Server 2008 R2 или более ранней версии, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Client** > **Монитор.**
   - Если вы используете операционную систему Windows 8 или Windows Server 2012, на начальном экране откройте список приложений и выберите **ViPNet** > **Монитор**.

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

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

Откроется окно входа в программу.

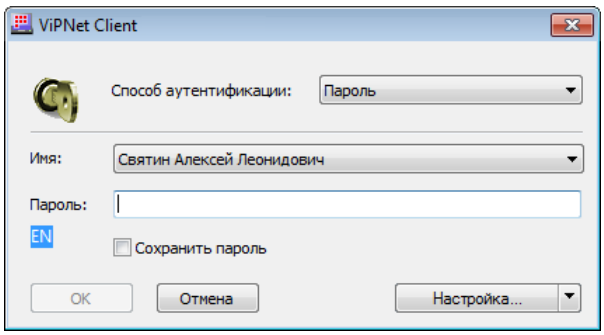



*Рисунок 21. Окно входа в программу*

2 Выберите способ аутентификации для входа в программу (см. «Способы аутентификации пользователя» на стр. 70) и в зависимости от выбранного способа введите пароль пользователя либо подключите внешнее устройство и введите ПИН-код.

Если на вашем компьютере работает несколько пользователей ViPNet Client и для аутентификации вы используете пароль, в списке **Имя** выберите ваше имя пользователя.

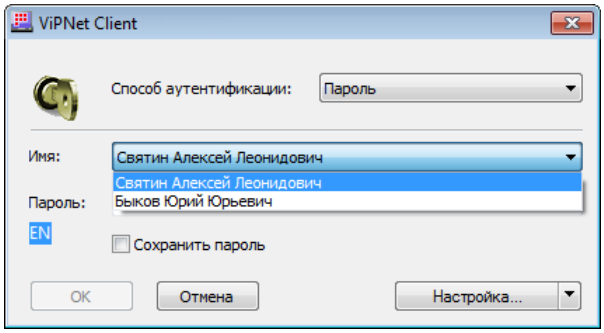



*Рисунок 22. Выбор учетной записи пользователя*

3 После ввода необходимых для аутентификации данных нажмите кнопку **OK**. Откроется окно программы ViPNet Монитор (см. «Интерфейс программы ViPNet Монитор» на стр. 78).

# Способы аутентификации пользователя

В программе ViPNet Монитор предусмотрено три способа аутентификации:

- Пароль (на стр. 72). Для входа в программу вам следует ввести свой пароль. Каждый раз после ввода пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу.
- Пароль на устройстве (на стр. 72). Для входа в программу вам следует подключить устройство и ввести ПИН-код.

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

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

- Устройство (на стр. 73). Для входа в программу вам следует подключить устройство и ввести ПИН-код (и в некоторых случаях пароль).

По умолчанию установлен способ аутентификации **Пароль**. В режиме администратора можно изменить способ аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 226).

При использовании способов **Пароль на устройстве** и **Устройство** аутентификация пользователя осуществляется с помощью внешних устройств (см. «Внешние устройства» на стр. 345). Чтобы использовать какое-либо устройство для аутентификации пользователя, на компьютер необходимо установить драйверы этого устройства и затем записать ключи на это устройство. Записать ключи на внешнее устройство можно при изменении способа аутентификации пользователя или в программе ViPNet Удостоверяющий и ключевой центр при создании дистрибутива ключей (в программе ViPNet Network Manager работа с внешними устройствами невозможна).

**Внимание!** Если при использовании способов аутентификации **Пароль на устройстве** или **Устройство** внешнее устройство будет отключено, может произойти автоматическая блокировка компьютера — в соответствии с настройками, заданными в режиме администратора (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220). Для продолжения работы необходимо вновь подключить это внешнее устройство.

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

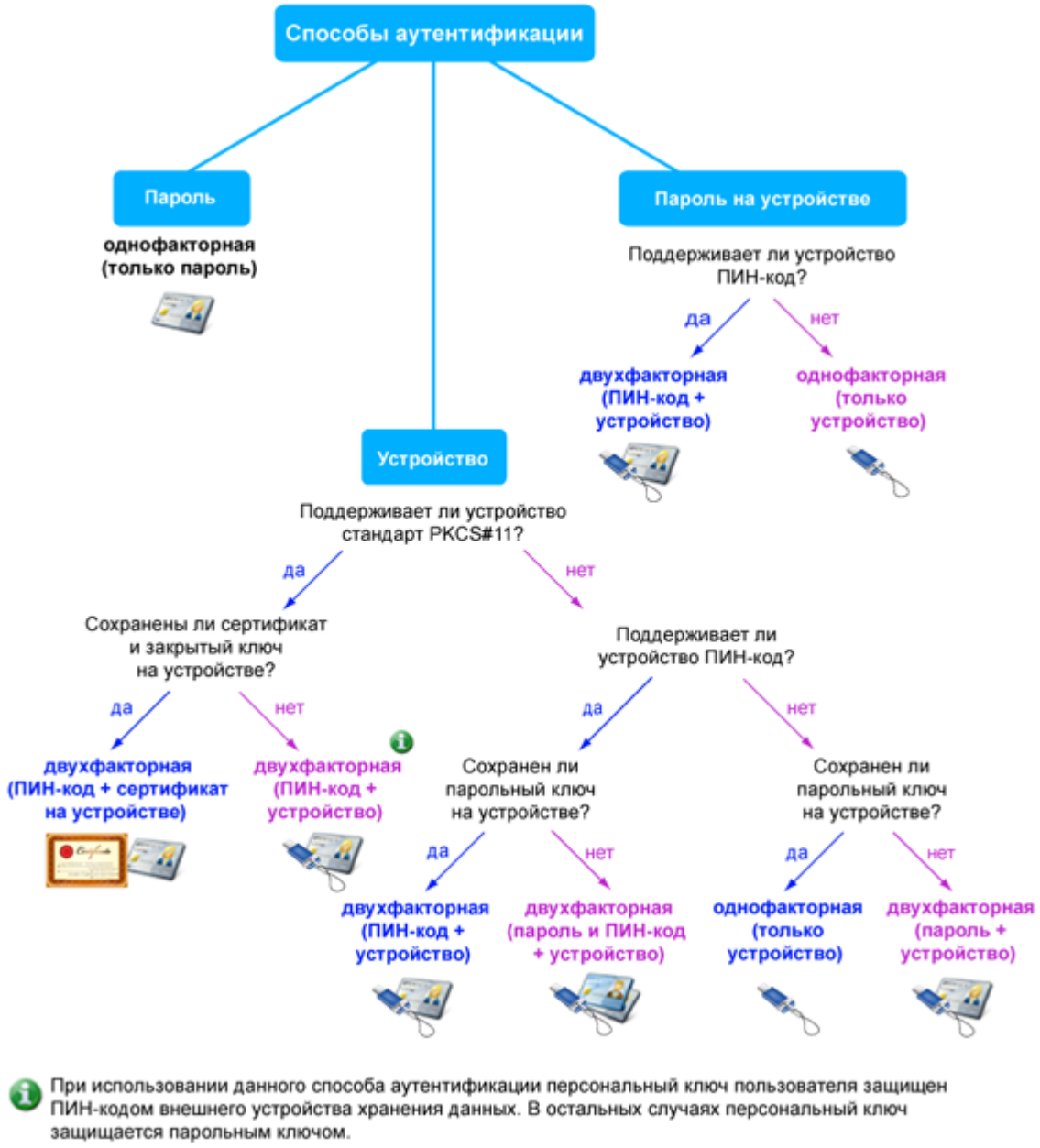



*Рисунок 23. Схема соответствия между факторами и способами аутентификации*

## Пароль

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

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

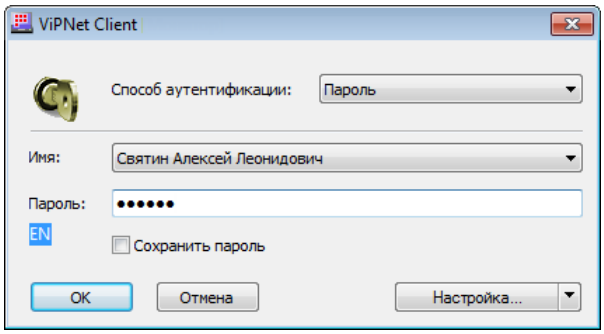



*Рисунок 24. Способ аутентификации «Пароль»*

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

**Примечание.** В данном списке отображаются имена всех пользователей, ключи которых были установлены на данном сетевом узле (см. «Установка справочников и ключей» на стр. 51). Если на узле не установлены ключи ни одного пользователя, список будет пуст.

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

Если сохранение пароля в реестре разрешено настройками программы (см. «Дополнительные настройки параметров безопасности» на стр. 224), для сохранения пароля можно установить соответствующий флажок.

4 Нажмите кнопку **OK**.

## Пароль на устройстве

**Внимание!** Во избежание неполадок в работе ПО ViPNet не следует использовать способ аутентификации **Пароль на устройстве**. При использовании данного способа аутентификации рекомендуется его изменить на **Пароль** или **Устройство** (см. «Изменение способа аутентификации пользователя» на стр. 226).

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

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

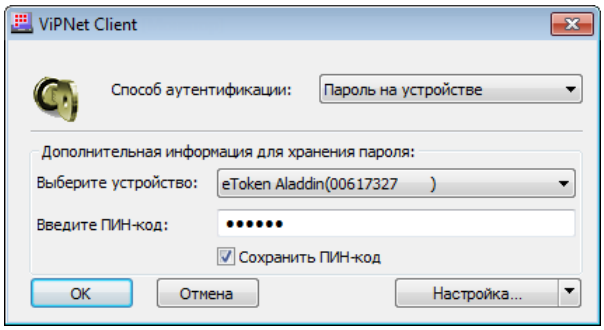



*Рисунок 25. Способ аутентификации «Пароль на устройстве»*

2 Подключите внешнее устройство, на котором находится ваш пароль.

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

4 Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства (см. Рисунок 16 на стр. 71).

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

5 Нажмите кнопку **OK**.

## Устройство

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

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

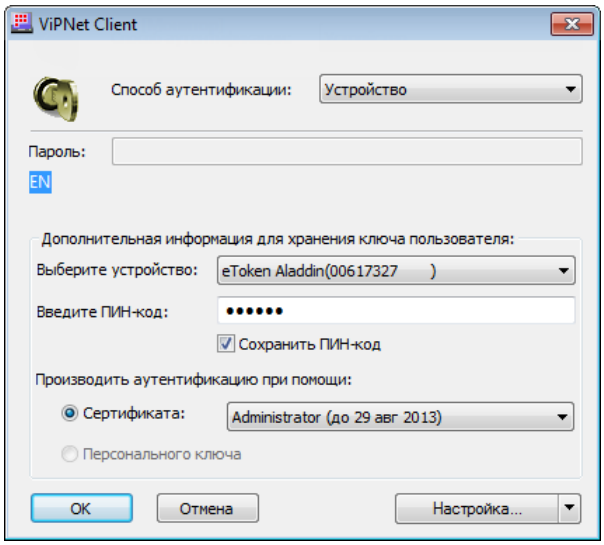



*Рисунок 26. Способ аутентификации «Устройство»*

2 Подключите внешнее устройство.

3 Если требуется, в списке ниже выберите ваше имя пользователя и в поле **Пароль** введите свой пароль. Необходимость ввода пароля зависит от типа используемого внешнего устройства (см. Рисунок 16 на стр. 71).

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

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

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

- **Сертификата** — чтобы выполнить аутентификацию с помощью сертификата, хранящегося на используемом устройстве. В списке сертификатов, обнаруженных на устройстве, выберите нужный сертификат. Подробнее о требованиях, предъявляемых к сертификату, используемому для аутентификации см. в разделе Особенности аутентификации с помощью сертификата (на стр. 74). В случае возникновения затруднений при аутентификации с помощью сертификата см. раздел Не удается выполнить аутентификацию с помощью сертификата (на стр. 283).
- **Персонального ключа** — чтобы выполнить аутентификацию с помощью персонального ключа (который входит в состав ключей пользователя и хранится на используемом устройстве).

7 Нажмите кнопку **OK**.

## Особенности аутентификации с помощью сертификата

Для возможности аутентификации в программе ViPNet Монитор с помощью сертификата должны быть выполнены следующие условия:

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

---

**Примечание.** Информация о том, какие внешние устройства обеспечивают аппаратную поддержку алгоритмов ГОСТ и поддержку стандарта PKCS#11, содержится в разделе Алгоритмы и функции, поддерживаемые внешними устройствами (на стр. 348). В таблице такие устройства вы можете найти по содержимому столбцов **Аппаратная поддержка российских криптографических алгоритмов (на устройстве)** и **Поддержка PKCS#11**.

---

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

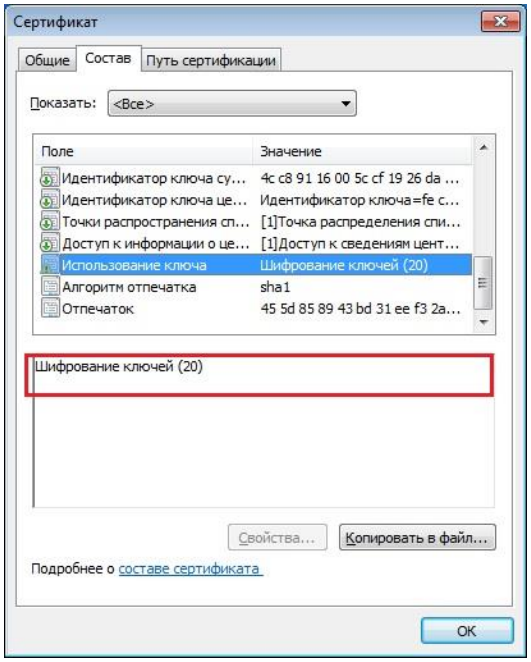



*Рисунок 27. Проверка наличия назначения «Шифрование ключей» в сертификате для аутентификации*

- В контейнере на устройстве находится закрытый ключ, которому соответствует используемый сертификат.
- Сертификат действителен, то есть срок его действия не истек, он не находится в списке аннулированных сертификатов доверенного удостоверяющего центра, соответствующая ему цепочка сертификации полна, и все входящие в нее сертификаты также действительны.
- Если требуется выполнять аутентификацию в программе ViPNet Монитор до загрузки ОС Windows, в хранилище операционной системы **Локальный компьютер** должны быть установлены соответствующие действительный список аннулированных сертификатов и все сертификаты из цепочки сертификации, включая корневой сертификат.

---

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

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

---

Чтобы получить сертификат ГОСТ, подходящий для аутентификации в программе ViPNet Монитор, выполните следующие действия:

1 Создайте запрос на сертификат. При этом сохраните контейнер ключей на внешнее устройство (см. «Обновление ключа электронной подписи и сертификата» на стр. 256).

2 Предупредите администратора программы ViPNet Удостоверяющий и ключевой центр о том, что при издании сертификата в него необходимо добавить назначение «Проверка подлинности клиента». Если в УКЦ обработка запросов на сертификаты производится в автоматическом режиме, администратору нужно будет отключить этот режим и обработать ваш запрос вручную.

3 Установите изданный сертификат в контейнер ключей, сохраненный на устройстве (см. «Установка сертификатов в хранилище операционной системы» на стр. 250).

# Смена пользователя

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

1 В главном меню программы выберите пункт **Файл** > **Сменить пользователя**. Откроется окно входа в программу.

2 Выберите способ аутентификации для входа в программу (см. «Способы аутентификации пользователя» на стр. 70) и в зависимости от выбранного способа введите пароль пользователя либо подключите внешнее устройство и введите ПИН-код.

   Если на вашем компьютере работает несколько пользователей ViPNet Client и для аутентификации вы используете пароль, в списке **Имя** выберите ваше имя пользователя.

**Примечание.** На сетевом узле должны быть предварительно установлены ключи пользователя (см. «Установка справочников и ключей» на стр. 51), от имени которого выполняется вход в программу.

3 Нажмите кнопку **OK**.

# Завершение работы с программой ViPNet Монитор

Существует несколько способов завершения работы с программой ViPNet Client:

1 Чтобы свернуть окно программы, выполните одно из действий:

- Нажмите кнопку **Закрыть**  в правом верхнем углу окна.
- Нажмите сочетание клавиш **Alt+F4**.

Чтобы снова развернуть окно программы, щелкните значок  в области уведомлений на панели задач.

2 Чтобы выйти из программы, в главном меню программы выберите пункт **Файл** > **Выход** либо в области уведомлений в контекстном меню программы ViPNet Client выберите пункт **Выход**. В окне подтверждения нажмите **Да**.

**Примечание.** После выхода из программы ViPNet Client работа ViPNet-драйвера продолжается: он фильтрует IP-трафик в соответствии с фильтрами, заданными в настройках интегрированного сетевого экрана.

# Интерфейс программы ViPNet Монитор

Окно программы ViPNet Монитор представлено на следующем рисунке:

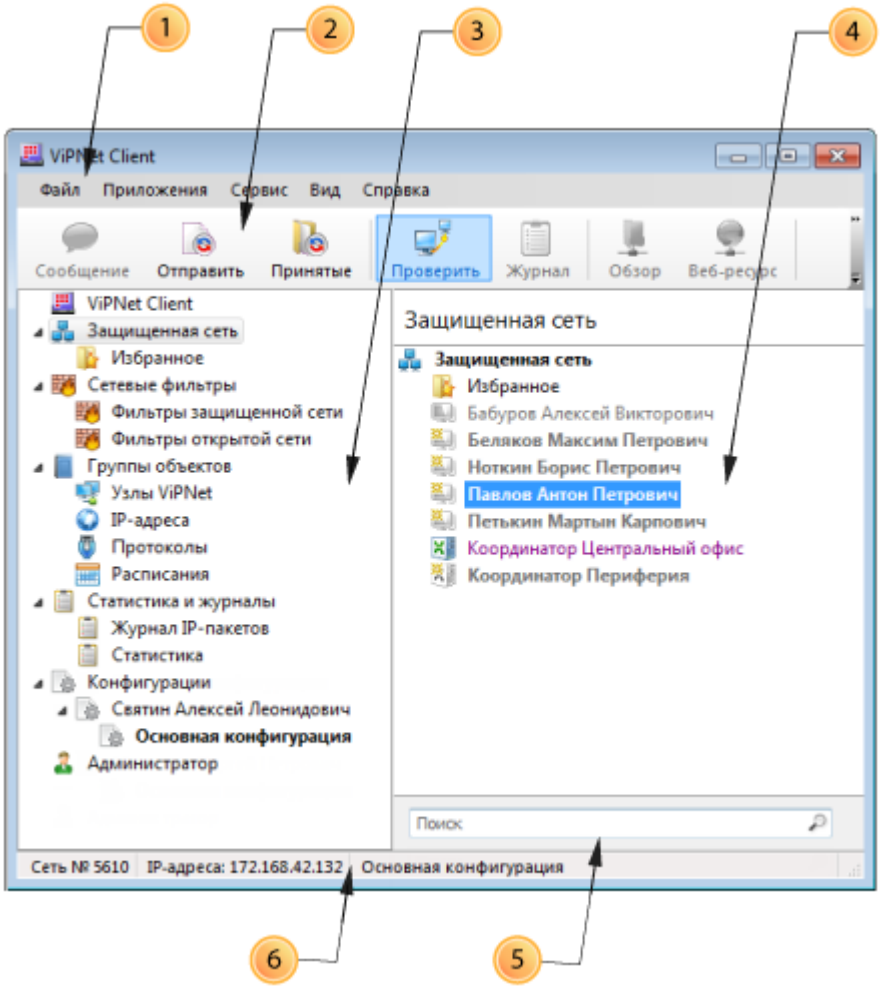



*Рисунок 28. Окно программы ViPNet Монитор*

Цифрами на рисунке обозначены:

1 Главное меню программы.

2 Панель инструментов. Чтобы отобразить или скрыть панель инструментов, в меню **Вид** выберите пункт **Панель инструментов**. Добавить или удалить кнопки на панель инструментов вы можете с помощью кнопки  . Чтобы изменить расположение кнопок на панели инструментов, перетащите их в нужном порядке, удерживая нажатой клавишу **Alt**.

3 Панель навигации. Содержит перечень разделов, предназначенных для настройки различных параметров ViPNet Монитор:

- **Защищенная сеть** (этот раздел выбран по умолчанию) — содержит список сетевых узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью или ViPNet Network Manager. Подробнее см. Работа со списком защищенных узлов ViPNet (на стр. 80).
- **Сетевые фильтры**. Содержит подразделы с фильтрами IP-трафика:
  - **Фильтры защищенной сети** — предназначен для настройки фильтров защищенного трафика (см. «Создание фильтров для защищенной сети» на стр. 146).
  - **Фильтры открытой сети** — предназначен для настройки фильтров открытого трафика (см. «Создание фильтров для открытой сети» на стр. 147).
- **Группы объектов —** содержит списки объектов, которые могут быть использованы при создании сетевых фильтров: группы узлов ViPNet, группы IP-адресов и так далее (см. «Использование групп объектов» на стр. 133).
- **Статистика и журналы**. Содержит подразделы:
  - **Журнал IP-пакетов —** предназначен для поиска записей в журнале IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 193).
  - **Статистика —** предназначен для просмотра статистики фильтрации IP-пакетов (см. «Просмотр статистики фильтрации IP-пакетов» на стр. 204).
- **Конфигурации** — предназначен для управления конфигурациями программы ViPNet Монитор (см. «Управление конфигурациями программы» на стр. 206).
- **Администратор** — отображается только после входа в программу в режиме администратора и служит для настройки дополнительных параметров программы (см. «Работа в программе в режиме администратора» на стр. 219).

---

**Примечание.** Количество и порядок расположения разделов на панели навигации зависит от уровня полномочий пользователя, который определяется в ViPNet Центр управления сетью (в сетях ViPNet, управляемых с помощью ПО ViPNet Administrator) (см. «Использование программы ViPNet Монитор в условиях ограниченных полномочий» на стр. 81). В сетях ViPNet, управляемых с помощью ПО ViPNet Network Manager, уровень полномочий для пользователей не задается.

---

4 Панель просмотра. Предназначена для отображения раздела, выбранного на панели навигации (**3**).

5 Строка поиска. Отображается в разделах **Защищенная сеть**, **Сетевые фильтры** и **Группы объектов**. Для поиска по разделу введите в этой строке часть адреса, имени сетевого узла или другие параметры.

В разделе **Защищенная сеть** поиск выполняется по следующим параметрам:

- Имя узла (отображается в разделе **Защищенная сеть** и в окне **Свойства узла** на вкладке **Общие**).
- Имя компьютера (окно **Свойства узла**, вкладка **Общие**).
- Псевдоним (окно **Свойства узла**, вкладка **Общие**).

- Реальные и виртуальные IP-адреса (окно **Свойства узла**, вкладка **IP-адреса**, список **IP-адреса**).
- DNS-имя (окно **Свойства узла**, вкладка **IP-адреса**, список **DNS-имя**).
- Идентификатор узла (окно **Свойства узла**, вкладка **Общие**).

Чтобы очистить строку поиска, нажмите кнопку **Показать все**.

6 Строка состояния. Содержит следующие сведения: номер сети ViPNet, IP-адреса, назначенные узлу, и текущая конфигурация программы. При изменении сетевых фильтров или групп объектов вместо указанных сведений в строке состояния появляется сообщение о том, что фильтры или группы объектов были изменены, но не применены.

Чтобы показать или скрыть строку состояния, в меню **Вид** выберите пункт **Строка состояния**. При изменении фильтров или групп объектов строка состояния отображается всегда, даже если она была ранее скрыта.

# Работа со списком защищенных узлов ViPNet

Раздел **Защищенная сеть** (см. «Интерфейс программы ViPNet Монитор» на стр. 78) содержит список защищенных узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью или ViPNet Network Manager.

Значок рядом с именем сетевого узла, а также цвет имени обозначают тип сетевого узла и его текущий статус:

*Таблица 3. Обозначение статуса сетевых узлов*

| Значок | Цвет имени | Статус сетевого узла |
|---|---|---|
|  | Серый | Клиент в данный момент отключен от сети либо нет данных о его статусе |
|  | Фиолетовый | Клиент в данный момент подключен к сети |
|  | Серый или фиолетовый, полужирный | Новый клиент, с которым была создана связь |
|  | Серый или фиолетовый, полужирный | Новый координатор, с которым была создана связь |
|  | Серый | Координатор в данный момент отключен от сети либо нет данных о его статусе |
|  | Фиолетовый | Координатор в данный момент подключен к сети |

**Примечание.** Чтобы настроить параметры внешнего вида раздела **Защищенная сеть**, выберите в окне программы ViPNet Монитор в меню **Сервис** пункт **Настройка приложения** и далее перейдите к разделу **Общие**.

Для удобства просмотра списка и поиска сетевые узлы в разделе **Защищенная сеть** можно сгруппировать по папкам:

- Чтобы создать новую папку, в окне программы ViPNet Монитор на панели навигации или на панели просмотра в контекстном меню элемента **Защищенная сеть** выберите пункт **Создать папку**.

  Новая папка появится на панели навигации, а также в разделе **Защищенная сеть**.
- Чтобы перенести сетевые узлы в какую-либо папку, в разделе **Защищенная сеть** выберите один или несколько сетевых узлов и перетащите их в нужную папку.
- Чтобы переименовать папку, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт **Переименовать**.
- Чтобы удалить папки:
  - Убедитесь, что папки, которые требуется удалить, не содержат сетевых узлов. В противном случае перенесите сетевые узлы в другие папки.
  - Выберите одну или несколько папок на панели навигации или в разделе **Защищенная сеть**.
  - Нажмите клавишу **Delete** либо воспользуйтесь пунктом **Удалить** в контекстном меню.

Для поиска сетевого узла в списке введите в строку поиска часть имени, IP-адреса или другие параметры узла.

Для просмотра свойств сетевого узла дважды щелкните имя узла. Откроется окно **Свойства узла**, в котором приведены общие сведения о сетевом узле и содержатся параметры доступа к узлу.

Чтобы проверить соединение с другим узлом, начать сеанс обмена защищенными сообщениями, отправить файл или использовать другие встроенные функции программы ViPNet Монитор (см. «Встроенные средства коммуникации» на стр. 169), выполните одно из действий:

- Выберите сетевой узел в списке и нажмите соответствующую кнопку на панели инструментов.
- Выберите соответствующий пункт в контекстном меню сетевого узла.

# Использование программы ViPNet Монитор в условиях ограниченных полномочий

Возможности использования программы ViPNet Монитор и изменения ее параметров на узлах сетей ViPNet, управляемых с помощью ПО ViPNet Administrator, могут быть ограничены уровнем полномочий пользователя. Кроме этого, интерфейс программы ViPNet Монитор может быть ограничен в режиме администратора сетевого узла (см. «Работа в программе в режиме

администратора» на стр. 219). В сетях ViPNet, управляемых с помощью ПО ViPNet Network Manager, уровень полномочий не задается: на координаторах всегда используется максимальный уровень полномочий, на клиентах — уровень полномочий, при котором интерфейс программы ограничен.

Если полномочия пользователя ограничены, могут быть скрыты определенные элементы интерфейса программы ViPNet Монитор, может быть заблокировано изменение параметров программы, сетевых фильтров и так далее. При входе в программу в режиме администратора все ограничения снимаются.

В данном документе возможности программы ViPNet Монитор описаны с точки зрения пользователя, полномочия которого не ограничены. Если для вас недоступны какие-либо функции или настройки программы, обратитесь к администратору вашей сети ViPNet.

Подробная информация о полномочиях пользователя содержится в документе «Классификация полномочий. Приложение к документации ViPNet».

# 4

# Система обновления ViPNet


О системе обновления ViPNet 84

Автоматическая установка обновлений 85

Установка обновлений вручную 87

Просмотр журнала установленных обновлений 89

# О системе обновления ViPNet

Система обновления ViPNet обеспечивает получение и установку обновлений следующих типов:

- обновления ПО ViPNet Client, полученные из программы ViPNet Administrator или ViPNet Network Manager;
- обновления справочников и ключей, полученные из программы ViPNet Administrator или ViPNet Network Manager;
- обновления политик безопасности, полученные из программы ViPNet Policy Manager.

Установка обновлений может осуществляться как в автоматическом режиме (см. «Автоматическая установка обновлений» на стр. 85), так и вручную (см. «Установка обновлений вручную» на стр. 87).

Если на узле настроена установка обновлений вручную, то при поступлении файлов обновления в области уведомлений отображается значок **Система обновления ViPNet** и соответствующая информация.

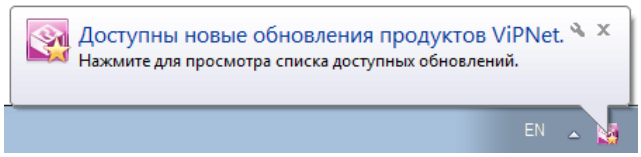



*Рисунок 29. Отображение наличия обновлений в области уведомлений*

Значок **Система обновления ViPNet** в области уведомлений может принимать следующий вид:

- — доступны новые обновления;
- — обновления успешно установлены;
- — обновления успешно установлены, необходима перезагрузка.

После установки обновлений, если не требуется перезагрузка, значок системы перестает отображаться в области уведомлений.

Если же на узле настроена автоматическая установка обновлений, то все операции система обновления ViPNet будет производить в «тихом» режиме без каких-либо сообщений. В области уведомлений значок системы будет отображаться, только если требуется перезагрузка компьютера (значок будет иметь вид ).

# Автоматическая установка обновлений

**Примечание.** Если вместе с ViPNet Client у вас установлена программа ViPNet SafeDisk-V (см. «Работа с интегрированной программой ViPNet SafeDisk-V» на стр. 167), то во время работы с защищенными контейнерами SafeDisk-V и независимо от выбранного режима установки обновлений, поступающие обновления можно установить только вручную.

Если вы хотите, чтобы обновления устанавливались на узле автоматически, выполните следующие действия:

1. Войдите в операционную систему с правами администратора.

   Без прав администратора вы не сможете изменить настройки системы обновления ViPNet.

2. Выполните одно из действий:

   - Если вы используете операционную систему Windows 7, Windows Server 2008 R2 или более ранней версии, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления**.
   - Если вы используете операционную систему Windows 8, Windows Server 2012 или более поздней версии, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet Система обновления**.

3. В открывшемся окне на вкладке **Параметры** установите флажок **Устанавливать обновления автоматически**.

4. Если вы хотите, чтобы, когда это необходимо, после обновления перезагрузка выполнялась автоматически, установите соответствующий флажок.

5. Для сохранения настроек нажмите кнопку **OK**.

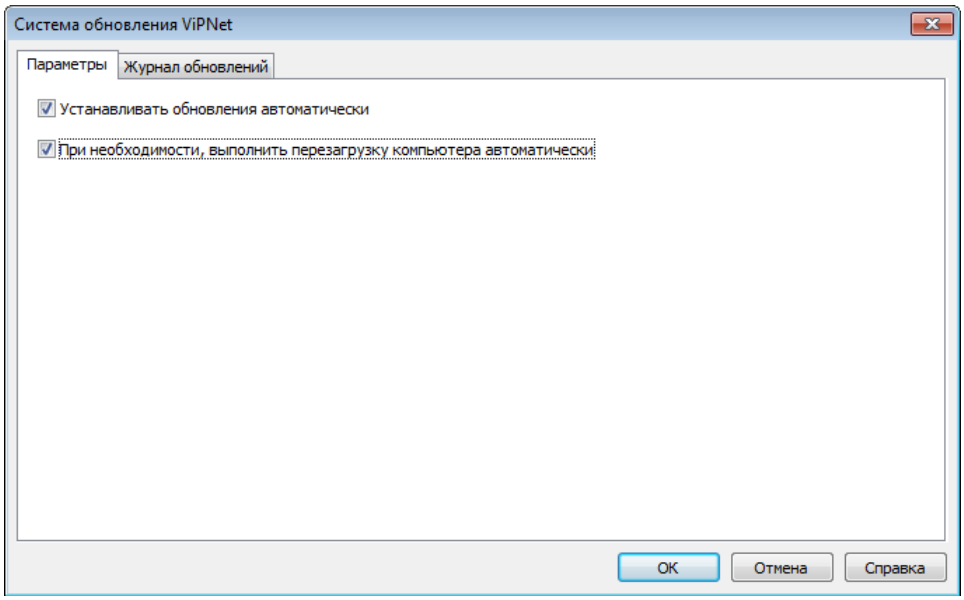



*Рисунок 30. Настройка автоматической установки обновлений*

# Установка обновлений вручную

Если вы хотите самостоятельно контролировать установку обновлений на сетевом узле, отключите автоматическую установку обновлений. Для этого выполните следующие действия (см. Рисунок 22 на стр. 86):

1. Войдите в операционную систему с правами администратора.

   Без прав администратора вы не сможете изменить настройки системы обновления ViPNet.

2. Выполните одно из действий:

   - Если вы используете операционную систему Windows 7, Windows Server 2008 R2 или более ранней версии, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления**.
   - Если вы используете операционную систему Windows 8, Windows Server 2012 или более поздней версии, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet Система обновления**.

3. В открывшемся окне на вкладке **Параметры** снимите флажок **Устанавливать обновления автоматически**.

4. Если вы хотите, чтобы, когда это необходимо, после обновления перезагрузка выполнялась автоматически, установите соответствующий флажок.

5. Для сохранения настроек нажмите кнопку **OK**.

Если автоматическая установка обновлений отключена, то после получения обновлений выполните их установку вручную:

1. В области уведомлений щелкните значок **Система обновления ViPNet** правой кнопкой мыши и в контекстном меню выберите пункт **Доступные обновления**.

2. В открывшемся окне проверьте список устанавливаемых обновлений (они отмечены флажком). Если какое-либо обновление устанавливать не нужно, снимите соответствующий флажок.

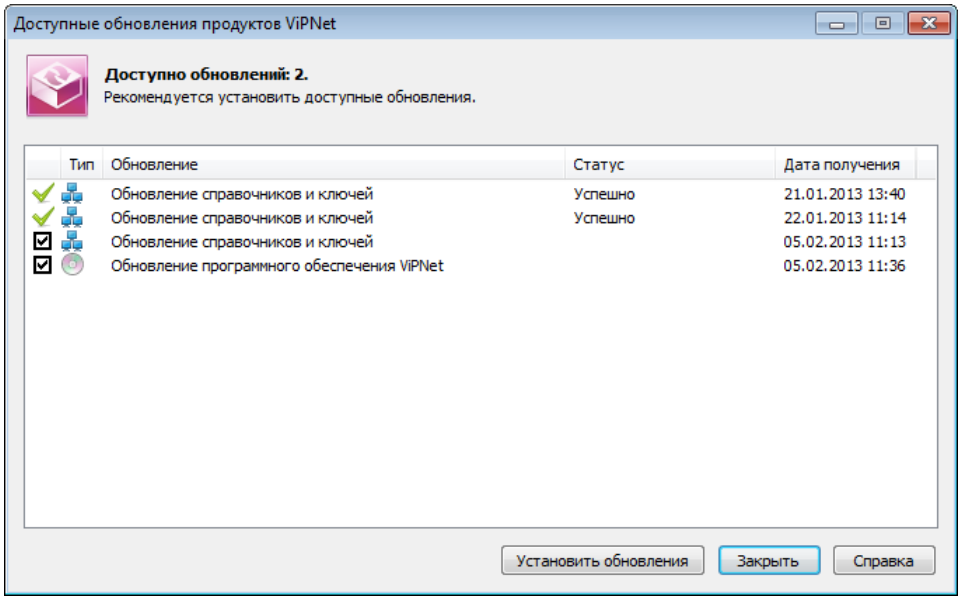



*Рисунок 31. Просмотр полученных обновлений*

3 Нажмите кнопку **Установить обновления**.

4 Если для продолжения установки обновлений должны быть закрыты какие-либо работающие приложения ViPNet, в окне **Установка обновлений продуктов ViPNet** появится соответствующее сообщение. Нажмите кнопку **Продолжить**. При этом нужные приложения будут автоматически закрыты, и установка обновлений будет продолжена.

После запуска установки программа ViPNet Монитор выгружается из памяти компьютера, и начинается процесс обновления. При этом в области уведомлений отображается соответствующая информация.

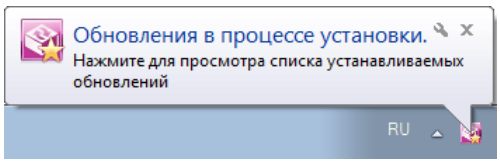



*Рисунок 32. Отображение установки обновлений в области уведомлений*

**Внимание!** Обновление ПО может занять значительное время. Не прерывайте процесс обновления и не выполняйте перезагрузку компьютера до окончания процесса обновления.

5 Если после завершения обновления необходимо выполнить перезагрузку, соответствующая информация появится в области уведомлений.

# Просмотр журнала установленных обновлений

Информация об установленных обновлениях отображается в журнале обновлений. Для просмотра журнала обновлений выполните следующее:

1 Выполните одно из действий:

- Если вы используете операционную систему Windows 7, Windows Server 2008 R2 или более ранней версии, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления.**
- Если вы используете операционную систему Windows 8 или Windows Server 2012, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet Система обновления**.

2 Выберите вкладку **Журнал обновлений**.

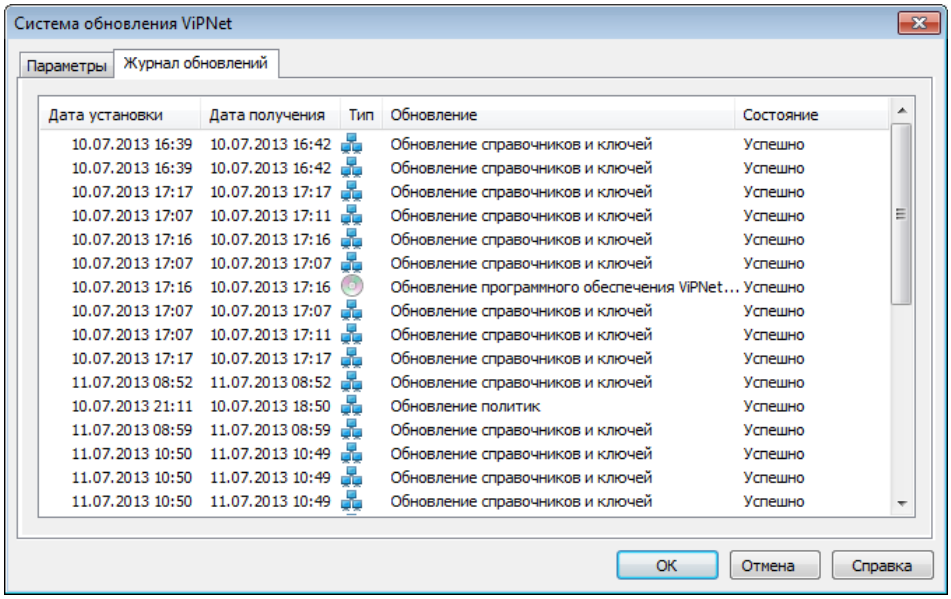



*Рисунок 33. Журнал обновлений*

# 5

# Подключение к защищенной сети ViPNet


Протоколы соединений в защищенной сети 91

Принципы осуществления соединений в защищенной сети 93

Использование виртуальных IP-адресов 96

Настройка подключения к защищенной сети 98

Настройка доступа к защищенным узлам 101

Настройка приоритета IP-адресов доступа к координатору 104

Настройка доступа к туннелируемым узлам 107

Использование псевдонимов для защищенных узлов 109

Просмотр информации о сетевом узле 110

# Протоколы соединений в защищенной сети

Сетевые узлы ViPNet могут располагаться в сетях любого типа, поддерживающих IP-протокол. Способ подключения к сети может быть любой: сеть Ethernet, PPPoE через XDSL-подключение, PPP через подключение Dial-up или ISDN, сеть сотовой связи GPRS или UMTS, устройства Wi-Fi, сети MPLS или VLAN. ПО ViPNet поддерживает разнообразные протоколы канального уровня. Для создания защищенных соединений между сетевыми узлами используются IP-протоколы трех типов (IP/241, UDP и TCP), в которые упаковываются пакеты любых других IP-протоколов.

При взаимодействии любых узлов ViPNet между собой, если они расположены в одном сегменте локальной сети и доступны по широковещательным адресам, используется протокол IP/241. Этот протокол более экономичен, так как не имеет UDP-заголовка размером 8 байт. Исходный пакет после шифрования упаковывается в пакет IP-протокола номер 241.


*Рисунок 34. Сетевые узлы расположены в одном сегменте локальной сети*

Если узлы ViPNet располагаются в разных сегментах сети, то автоматически используется протокол UDP, который позволяет IP-пакетам проходить через межсетевые экраны. Исходный пакет после шифрования упаковывается в UDP-пакет.


*Рисунок 35. Сетевые узлы соединяются через межсетевой экран*

Если на пути следования IP-пакета расположено устройство NAT, на этом устройстве должны быть настроены динамические или статические правила трансляции адресов, которые разрешают обмен UDP-трафиком с узлами сети ViPNet. При настройке статических правил должен быть указан порт инкапсуляции UDP-пакетов. По умолчанию используется порт 55777, но при необходимости он может быть изменен на любой другой. Если пакеты проходят напрямую через координатор, то номер порта узлов, расположенных за этим координатором, значения не имеет. После прохождения через координатор пакетам присваиваются IP-адреса соответствующего сетевого интерфейса координатора, то есть осуществляется трансляция адресов.

Бывают случаи, когда взаимодействие защищенных узлов по UDP-протоколу невозможно, передача UDP-пакетов провайдером услуг запрещена. Например, при удаленном подключении к

сети ViPNet из гостиниц или других общественных мест. В таком случае весь IP-трафик может передаваться через TCP-туннель, настроенный на сервере соединений узла, являющегося инициатором соединения. При настройке TCP-туннеля на сервере соединений (см. «Сервер соединений» на стр. 402) может быть указан произвольный порт. По умолчанию используется порт 443.


*Рисунок 36. Сетевые узлы соединяются через межсетевой экран*

На сервере соединений полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узел назначения по UDP-протоколу.

# Принципы осуществления соединений в защищенной сети

Клиентские узлы в сети ViPNet автоматически выполняют соединения с другими узлами по кратчайшим доступным маршрутам. Для установки соединений они используют серверы соединений (см. «Сервер соединений» на стр. 402). Информацию о других узлах, параметрах доступа и их активности в данный момент клиенты получают от своего сервера IP-адресов (см. «Сервер IP-адресов» на стр. 402). По умолчанию сервер IP-адресов является сервером соединений для клиента, но при необходимости сервером соединений может быть назначен другой координатор.

Параметры подключения к сети определяются клиентами автоматически также с помощью серверов соединений.

Организация соединений между клиентскими узлами осуществляется следующим образом:

- Перед установкой соединения с другим узлом клиент определяет канал доступа к своему серверу соединений. Если клиент определил, что работает через устройство NAT, то он продолжает поддерживать канал путем периодической отправки на сервер IP-пакетов. Интервал отправки IP-пакетов на сервер соединений по умолчанию равен 25 секундам. Этого, как правило, достаточно для работы через большинство устройств NAT. При необходимости интервал (тайм-аут) может быть изменен.
- После того, как связь между клиентом и его сервером соединений будет установлена, клиент начинает устанавливать соединение с другим узлом. Он начинает передавать тестовые IP-пакеты удаленному узлу через свой сервер соединений. Одновременно с этим клиент передает тестовые IP-пакеты на сервер соединений удаленного узла и напрямую на удаленный узел.
- Если тестовые IP-пакеты дошли до удаленного узла, то удаленный узел регистрирует соединение и начинает ответный IP-трафик передавать напрямую. Клиент при получении ответного IP-трафика от удаленного узла свой последующий IP-трафик ему также начинает передавать напрямую.

  Если тестовые IP-пакеты дошли только до сервера соединений удаленного узла, то сервер соединений регистрирует это соединение и отправляет напрямую клиенту ответные IP-пакеты удаленного узла.

  То есть с удаленным узлом устанавливается прямое соединение или соединение через его сервер соединений. Если ответный IP-трафик так и не поступил от удаленного узла или его сервера соединений, то клиент по-прежнему осуществляет соединение с удаленным узлом через свой сервер соединений.


*Рисунок 37. Взаимодействие между сетевыми узлами*

Таким образом, если существует возможность, узлы устанавливают взаимодействие друг с другом по кратчайшим маршрутам без участия координаторов, за счет чего повышается скорость обмена шифрованным IP-трафиком и снижается нагрузка на координаторы.

---

**Примечание.** Описанный порядок установления соединения применим в полном объеме только в том случае, если на всех узлах используется ПО ViPNet версии не ниже 4.2.x.

---

Кроме этого, существуют следующие особенности при установлении соединений в сети:

- Если узлы находятся в маршрутизируемой сети, то соединение между клиентами будет производиться в соответствии с заданными маршрутами через шлюзы сети, а не координаторы.
- Если удаленный узел, с которым устанавливается соединение, не расположен за устройством NAT, то информация о возможности прямого доступа к нему запоминается и при следующих соединениях с этим узлом, если не изменилось его местоположение, тестовые IP-пакеты не отправляются, IP-трафик начинает сразу передаваться по прямому маршруту.
- Если клиенты, между которыми устанавливается соединение, расположены за устройствами с динамической трансляцией адресов, то они также в состоянии соединиться друг с другом напрямую. Это происходит за счет того, что серверы соединений передают клиентам информацию об IP-адресах и портах, по которым они могут получить доступ к другим узлам через устройства NAT. Данную информацию серверы определяют по полученным от клиентов IP-пакетам.

  Имея эту информацию, клиенты отправляют друг другу тестовые IP-пакеты на зарегистрированные IP-адреса и порты. Если тестовые пакеты будут получены хотя бы одной стороной, весь IP-трафик начинает передаваться между клиентами напрямую. То есть технология установления прямого соединения между клиентами будет применена, если хотя бы одно из устройств NAT при отправке IP-пакетов от узла по разным адресам сохраняет для данного узла выделенный порт.

Прямое соединение между клиентами будет невозможно, если устройства NAT обоих клиентов при отправке IP-пакетов от них по разным адресам каждый раз выделяют случайный порт. Таким образом работает так называемый симметричный NAT. В этом случае соединение между двумя такими клиентами установится через один из серверов соединений.

- Возможность прямого соединения с удаленным узлом, стоящим за устройством с динамической трансляцией адресов, сохраняется по умолчанию в течение 75 секунд (трех тайм-аутов или интервалов отправки IP-пакетов) с момента окончания предыдущего соединения.
- Если клиент расположен за устройством со статической трансляцией адресов, то в его настройках необходимо зафиксировать нужный порт инкапсуляции UDP-пакетов. В противном случае порт будет изменяться, а вследствие этого соединение клиента с другими узлами будет невозможно.

# Использование виртуальных IP-адресов

В различных локальных сетях и сетях интернет-провайдеров довольно часто возникает проблема с пересечением IP-адресов. Технология виртуальных адресов позволяет эффективно решить эту проблему при организации защищенных соединений.

Виртуальные адреса также можно использовать, чтобы установить правила доступа к ресурсу на основе виртуальных адресов. Для чего это нужно? Известно, что если IP-адрес используется для идентификации пользователя, то одной из сетевых угроз является подделка IP-адреса. Однако в сети ViPNet подделка адреса невозможна. В момент приема пакета из сети ViPNet-драйвер подставляет вместо реального адреса отправителя соответствующий виртуальный адрес, затем пакет передается приложению. Это происходит только в случае успешной расшифровки пакета на ключах отправителя, то есть после идентификации отправителя пакета. Это обеспечивает защиту от подмены адреса отправителя и надежное разграничение доступа к ресурсам на основе виртуальных адресов.

Каждый сетевой узел ViPNet автоматически формирует один или несколько виртуальных IP-адресов для каждого сетевого узла ViPNet и туннелируемого узла, с которым он связан. Каждому реальному адресу узла ставится в соответствие виртуальный IP-адрес. То есть число формируемых виртуальных адресов зависит от числа реальных адресов узла и числа туннелируемых этим узлом адресов.

У каждого сетевого узла собственный список виртуальных адресов для других узлов. Все приложения при работе в сети могут использовать эти виртуальные адреса для соединения с соответствующими узлами. ViPNet-драйвер подменяет адреса в момент отправки и получения IP-пакетов (включая пакеты служб DNS, WINS, NetBIOS, SCCP, SIP и другие).

По умолчанию сетевой узел автоматически использует виртуальные адреса для соединения с другими сетевыми узлами, если эти узлы недоступны по широковещательным IP-адресам. Для туннелируемых узлов по умолчанию используются реальные IP-адреса. При необходимости можно принудительно установить для любых узлов реальную или виртуальную видимость.

## Общие принципы назначения виртуальных адресов

По умолчанию начальный адрес для генератора виртуальных адресов — 11.0.0.1 (маска подсети: 255.0.0.0). Начальный адрес можно изменить в окне **Настройка**, в разделе **Защищенная сеть** > **Дополнительные параметры**. Автоматическое формирование виртуальных IP-адресов для сетевых узлов ViPNet и одиночных туннелируемых адресов начинается с этого адреса.

Для диапазонов туннелируемых адресов начальным виртуальным адресом по умолчанию является 12.0.0.1 либо адрес, в котором значение первого октета на 1 больше, чем значение первого октета начального адреса для генератора виртуальных адресов.

**Примечание.** Одиночный туннелируемый адрес — это адрес, который явно (а не в составе диапазона адресов) указан в настройках туннелируемых адресов узла.

Следует учитывать, что по умолчанию для виртуальных адресов используется один из интернет-диапазонов. Поэтому при взаимодействии узла с открытыми ресурсами Интернета может возникнуть конфликт, если у некоторого открытого ресурса IP-адрес совпадет с используемым виртуальным адресом. Соединение с таким открытым ресурсом будет невозможно. Если доступ к открытому ресурсу все же необходим, следует либо сменить диапазон назначаемых виртуальных адресов, либо работать с этим ресурсом через прокси-сервер. С защищенными узлами работать через прокси-сервер при этом нельзя. Поэтому при использовании прокси-сервера требуется IP-адреса защищенных узлов указать в качестве исключений.

Виртуальные адреса сетевых узлов отображаются на вкладке **IP-адреса** в окне **Свойства узла** для каждого сетевого узла. Виртуальные адреса туннелируемых узлов отображаются на вкладке **Туннель** в окне **Свойства узла** для координатора, осуществляющего туннелирование.

Виртуальные адреса для сетевых узлов закрепляются не за конкретными реальными адресами, а за уникальными идентификаторами сетевых узлов, присвоенными в ViPNet Центр управления сетью или ViPNet Network Manager. Виртуальные адреса для одиночных туннелируемых узлов закрепляются за каждым реальным туннелируемым IP-адресом. Виртуальные адреса закрепляются за сетевыми узлами и одиночными туннелируемыми адресами до тех пор, пока сетевые узлы или туннелируемые адреса не будут удалены.

**Внимание!** Чтобы избежать ошибок при назначении начальных адресов для генератора виртуальных адресов, следует иметь в виду следующее:

- Значение первого (младшего) октета должно быть в диапазоне 1–254.
- Значение четвертого октета должно быть в диапазоне 1–239.
- Значение второго и третьего октетов должно быть в диапазоне 0–255.

Вновь добавленным сетевым узлам, реальным IP-адресам узлов и одиночным туннелируемым адресам ставятся в соответствие новые свободные виртуальные адреса. Виртуальные адреса, выделенные для туннелируемых диапазонов адресов, могут измениться при добавлении новых диапазонов туннелируемых адресов.

При смене начального адреса для генератора виртуальных адресов все виртуальные адреса формируются заново.

# Настройка подключения к защищенной сети

Для подключения клиента к защищенной сети ViPNet в общем случае не требуется никаких настроек. Дополнительные настройки при подключении могут быть нужны только в некоторых особых ситуациях. Например, вы со своим мобильным компьютером подключаетесь к локальной сети другой организации. В этой сети нет доступа к вашему серверу соединений (см. «Сервер соединений» на стр. 402), но в ней есть координатор, имеющий связь с вашим узлом. В этом случае в настройках подключения к сети ViPNet вам потребуется изменить сервер соединений.

---

**Совет.** Если вы часто подключаетесь к другой локальной сети, то для удобства вы можете создать конфигурацию, в которой этот вариант настройки подключения будет сохранен. Информацию по созданию конфигурации см. в разделе Управление конфигурациями программы (на стр. 206).

---

Выбрать другой сервер соединений вы также можете, если ваш координатор по каким-то причинам оказался недоступным.

Чтобы назначить сервер соединений, выполните следующие действия:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. На панели навигации окна **Настройка** выберите раздел **Защищенная сеть**.
3. В списке **Сервер соединений** выберите координатор, с помощью которого клиент будет устанавливать соединения с другими узлами. Если нужного координатора нет в списке, нажмите кнопку  и выберите координатор в окне **Выбор сетевого узла**.

   Этот координатор должен быть доступен либо напрямую, либо через межсетевой экран со статической трансляцией адресов.
4. Чтобы сохранить настройки, нажмите кнопку **Применить**.

При необходимости вы также можете выполнить расширенную настройку подключения к сети:

- В разделе **Защищенная сеть** нажмите кнопку **Показать дополнительные настройки** и выполните следующие действия:
  - Если требуется направлять весь входящий и исходящий трафик через сервер соединений, установите флажок **Весь трафик направлять через сервер соединений**.

**Примечание.** Направлять IP-трафик через сервер соединений может потребоваться в том случае, если есть необходимость в контроле всего передаваемого IP-трафика. При этом стоит учитывать, что передача IP-трафика через сервер соединений может привести к существенному снижению скорости обмена данными между узлами.

- Если требуется установить клиент за межсетевой экран со статической трансляцией адресов, установите флажок **Зафиксировать порт UDP** и в поле ниже укажите порт инкапсуляции UDP-пакетов. Для этого порта на устройстве NAT должно быть создано соответствующее статическое правило.
- Если требуется изменить интервал отправки IP-пакетов серверу соединений при работе через межсетевой экран с динамической трансляцией адресов, в поле **Тайм-аут поддержки соединений через устройства с динамическим NAT** укажите новое значение. По умолчанию отправка IP-пакетов производится каждые 25 секунд. Как правило, этого интервала достаточно, чтобы поддерживать связь с сервером соединений при работе через большинство устройств NAT.
- Если требуется изменить сервер IP-адресов, в списке **Сервер IP-адресов** выберите другой координатор.

**Внимание!** Изменять сервер IP-адресов без согласования с администратором сети ViPNet крайне не рекомендуется.

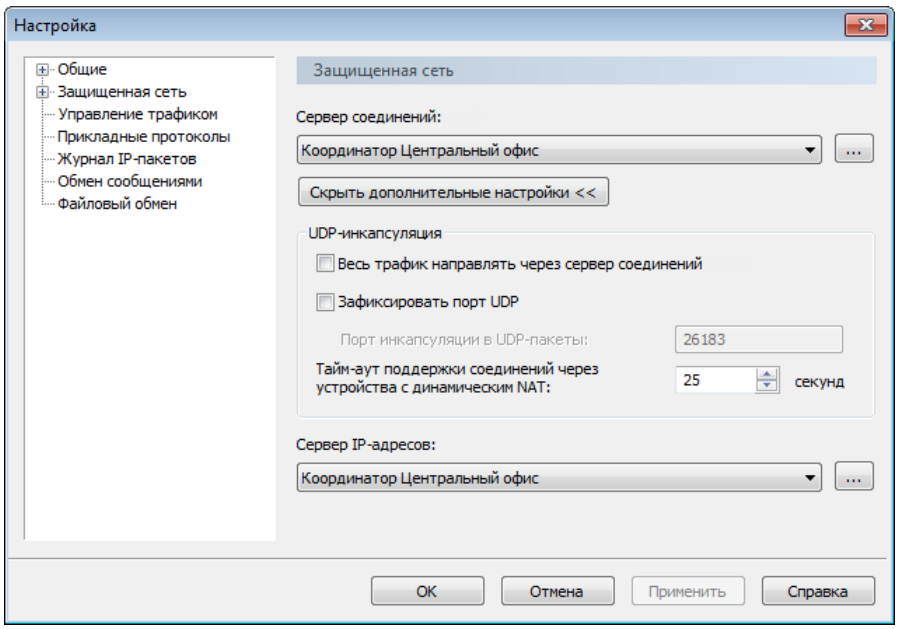



*Рисунок 38. Настройка подключения клиента к защищенной сети ViPNet*

- Если при работе с некоторыми устройствами NAT не проходит передача длинных пакетов, перейдите в подраздел **Защищенная сеть** > **Дополнительные параметры** и уменьшите значение MSS (максимальный размер сегмента).

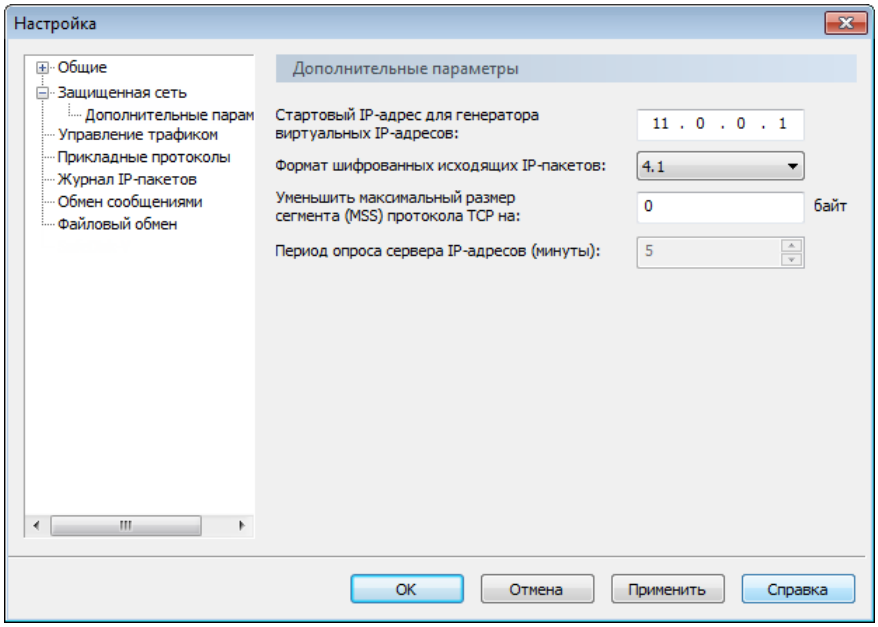



*Рисунок 39. Настройка дополнительных параметров*

Для сохранения параметров расширенной настройки подключения, нажмите кнопку **Применить**.

# Настройка доступа к защищенным узлам

Для возможности соединения с другими узлами в сети ViPNet должны быть настроены параметры доступа. На клиенте достаточно настроить параметры доступа только для координатора, который является сервером IP-адресов и сервером соединений. При этом данная настройка требуется в том случае, если в программе ViPNet Administrator или ViPNet Network Manager IP-адреса и параметры подключения координаторов не были заданы централизованно.

Необходимые параметры доступа к другим сетевым узлам автоматически будут получены у сервера IP-адресов сразу после того, как с ним будет установлено соединение. В программе ViPNet Монитор вы можете их изменить, например, при возникновении конфликта IP-адресов. В других случаях изменять их не рекомендуется.

Чтобы настроить доступ к сетевому узлу, выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.

2 В разделе **Защищенная сеть** дважды щелкните нужный сетевой узел.

3 В окне **Свойства узла** на вкладке **IP-адреса** добавьте в список реальный IP-адрес сетевого узла. Автоматически новому адресу будет сопоставлен виртуальный IP-адрес.

   Если вам не известен IP-адрес узла, то вы можете определить его по имени компьютера. Для этого нажмите кнопку **Определить имя/IP-адрес**  и в появившемся окне выполните поиск IP-адреса по указанному имени.

   При добавлении IP-адреса будет автоматически выполнена его проверка на наличие конфликта с IP-адресами, уже заданными в списке, и IP-адресами других сетевых узлов (в том числе, туннелируемых), если для узлов не установлена видимость по виртуальным IP-адресам. Данная проверка позволит избежать задания одинаковых IP-адресов. Если в ходе проверки будет обнаружен конфликт IP-адресов, появится соответствующее сообщение. Устраните конфликт IP-адресов (см. «Обнаружен конфликт IP-адресов или DNS-имен» на стр. 286).

   Вы также можете выполнить проверку на конфликт IP-адресов вручную. Для этого нажмите кнопку **Проверить конфликты**  .

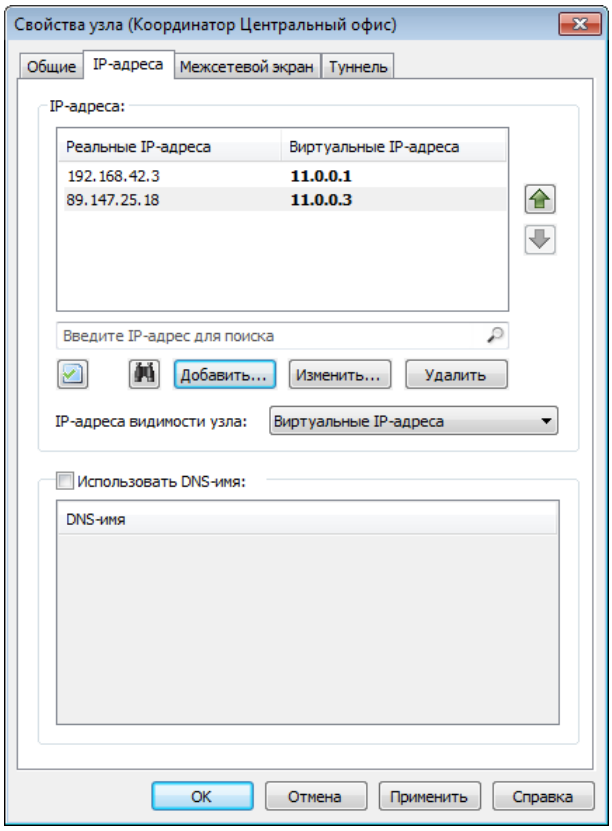



*Рисунок 40. Задание IP-адреса сетевого узла*

4 В списке **IP-адреса видимости узла** укажите, по каким адресам должен быть доступен сетевой узел. По умолчанию IP-адреса видимости выбираются автоматически. Если возможен конфликт реальных IP-адресов с адресами других узлов в сети, в списке выберите **Виртуальные IP-адреса**.

При изменении IP-адресов видимости в свойствах координатора вам будет предложено установить аналогичные IP-адреса видимости на всех узлах, использующих данный координатор в качестве сервера соединений.

5 Если для доступа к сетевому узлу необходимо использовать DNS-имя, установите флажок **Использовать DNS-имя** и добавьте в список DNS-имя сетевого узла. При добавлении DNS-имени также будет автоматически выполнена его проверка на наличие конфликта с DNS-именами, уже заданными в программе. Если в ходе проверки будет обнаружен конфликт DNS-имен, устраните его (см. «Обнаружен конфликт IP-адресов или DNS-имен» на стр. 286). Вы также можете выполнить проверку на конфликт DNS-имен с помощью кнопки **Проверить конфликты**  .

Для любого сетевого узла можно задать несколько DNS-имен. При настройке параметров доступа к координатору DNS-имена узлов, туннелируемых этим координатором, также следует добавить в список на вкладке **IP-адреса** (см. «Настройка доступа к туннелируемым узлам» на стр. 107).

Для клиента порядок DNS-имен в списке не имеет значения. Для координатора в первой строке списка нужно указать DNS-имя, соответствующее IP-адресу координатора. Подробная информация об использовании службы DNS в сети ViPNet см. в разделе Настройка и использование служб имен DNS и WINS в сети ViPNet (на стр. 111).

6 При настройке параметров доступа к координатору на вкладке **Межсетевой экран** добавьте IP-адрес межсетевого экрана, если он используется. При необходимости укажите дополнительные IP-адреса. Если будет указано несколько IP-адресов доступа через межсетевой экран, то вы можете указать приоритет этих адресов с помощью метрик (см. «Настройка приоритета IP-адресов доступа к координатору» на стр. 104).

В поле **Порт UDP** укажите порт доступа через межсетевой экран.

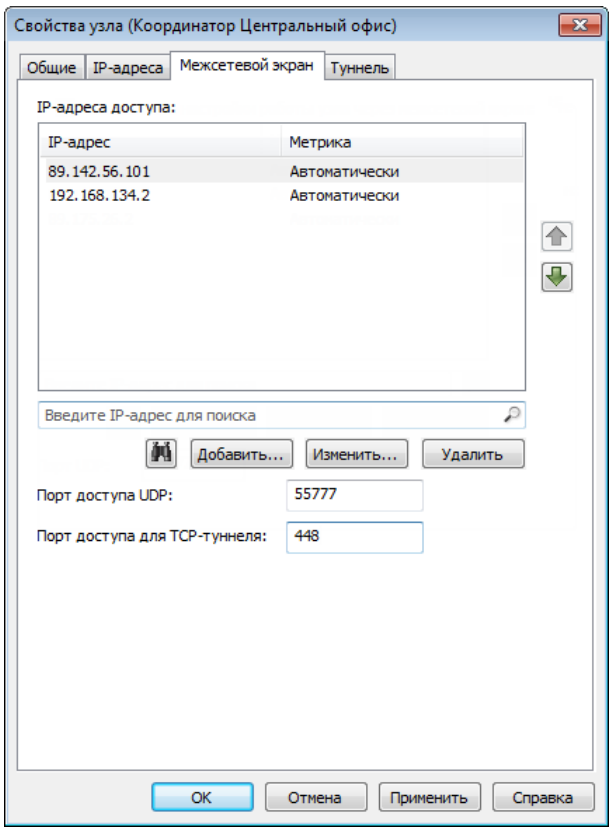



*Рисунок 41. Настройка доступа к координатору через межсетевой экран*

7 При настройке параметров доступа к координатору на вкладке **Межсетевой экран** в поле **Порт доступа для TCP-туннеля** вы можете указать порт, по которому ваш узел сможет соединяться с координатором по TCP-протоколу (через TCP-туннель). Порт рекомендуется задавать в том случае, если в свойствах координатора он не задан, но при этом известно, что на данном координаторе развернут TCP-туннель для соединений по TCP-протоколу.

Как правило, информация о номере порта доступа по TCP-протоколу поступает на сетевой узел автоматически сразу после развертывания на координаторе TCP-туннеля. Поэтому если в свойствах координатора порт доступа по TCP-протоколу указан, изменять его не следует.

8 Чтобы сохранить указанные настройки, нажмите кнопку **Применить**.

# Настройка приоритета IP-адресов доступа к координатору

Если координатор имеет несколько адресов доступа (например, по разным каналам связи), то можно настроить приоритет каналов для установления соединения с координатором. Если самый приоритетный канал по каким-то причинам недоступен, то канал связи будет выбран в соответствии с приоритетами оставшихся каналов. Когда самый приоритетный канал станет доступен, соединение с координатором вновь будет установлено через него.

**Примечание.** Следует учитывать, что эффективной данная настройка может быть только в случае, если узел связывается с координатором по нескольким разным каналам, например, через Интернет и выделенную сеть (то есть при маршрутизации через разные шлюзы).

Приоритет каналов задается с помощью метрики для каждого адреса доступа координатора. По умолчанию метрика назначается автоматически. При назначении метрик нужно придерживаться следующих принципов:

- Метрика определяет задержку (в миллисекундах) отправки тестовых IP-пакетов при выполнении опроса для определения доступности адреса. Соединение устанавливается по тому адресу, доступность которого быстрее определяется в результате опроса.
- Опросы осуществляются в следующих случаях:
  - При запуске программы ViPNet Монитор.
  - При проверке соединения с узлом вручную.
  - Периодически. Период опросов задается на координаторе в окне **Настройка** в разделе **Защищенная сеть** > **Дополнительные параметры**. По умолчанию период опроса координаторами других координаторов равен 15 минутам, период опроса своего координатора клиентами равен 5 минутам.
- Адрес с наименьшей метрикой считается самым приоритетным. Соединение с координатором устанавливается по адресу с наименьшей метрикой всегда, когда этот адрес доступен.
- Если для всех адресов доступа узла метрика назначена автоматически, то значение метрики равно 0. Если для части адресов метрика назначена вручную, а для остальных — автоматически, то значение автоматически назначенной метрики всегда на 100 миллисекунд больше максимального значения метрики, присвоенной вручную.
- Чем больше разница между наименьшей метрикой и остальными метриками, тем меньше вероятность того, что в случае кратковременного сбоя самого приоритетного канала будет выбран менее приоритетный канал. При использовании менее приоритетного канала сетевой узел быстрее сможет вернуться к работе через самый приоритетный канал, когда он станет доступен.

- Если все метрики равны, то для работы будет выбран тот канал, через который соединение с координатором будет установлено быстрее. После того как канал выбран, определение доступности других каналов связи выполняется только при потере соединения по текущему каналу. Этот же механизм действует в случае, если выбран канал связи с наименьшей метрикой.
- Если хотя бы для одного адреса доступа значение метрики задано вручную и выбран не самый приоритетный канал, то определение доступности других каналов связи с целью возвращения к каналу с наименьшей метрикой начнется одновременно с периодическим опросом по выбранному каналу.
- После определения канала доступа текущий адрес доступа отобразится в окне свойств координатора в первой строке списка IP-адресов на вкладке **Межсетевой экран**.

Чтобы назначить метрики для адресов доступа к координатору, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** дважды щелкните координатор, для которого требуется задать приоритет IP-адресов доступа.
3. В окне **Свойства узла** откройте вкладку **Межсетевой экран**.
4. В случае необходимости настройте параметры доступа к координатору через межсетевой экран (см. «Настройка доступа к защищенным узлам» на стр. 101).
5. Чтобы назначить IP-адресу доступа метрику, выберите в списке адрес и нажмите кнопку **Изменить**.

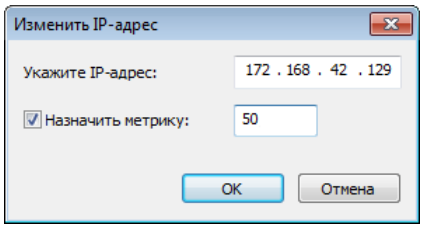



*Рисунок 42. Назначение метрики*

6. В появившемся окне установите флажок **Назначить метрику** и в поле рядом введите значение метрики в миллисекундах (допустимые значения от 1 до 9999), после чего нажмите кнопку **OK**.

Рассмотрим пример использования метрики. Предположим, координатор имеет четыре адреса доступа по каналам связи A, B, C и D. Требуется задать метрики для этих каналов.

Пусть каналы имеют следующий приоритет:

1. A — самый быстрый и безопасный канал. Используется в первую очередь.
2. C и D — безопасные, но менее быстрые каналы. Используются, если канал A недоступен.
3. B — менее безопасный канал. Используется в последнюю очередь.

Чтобы канал A стал самым приоритетным, зададим для него самую маленькую метрику, например 1. Для канала B зададим максимальную метрику 9999, так как работа через этот канал нежелательна. Для каналов C и D зададим одинаковую метрику, причем такую, чтобы разница с метрикой для канала A была небольшой, например 500.

При указанных значениях метрик канал A будет использоваться всегда, когда доступен. Если в момент проверки он недоступен или его качество ухудшилось (он стал медленнее), то соединение с координатором будет установлено по каналу C или D. И только в крайнем случае, если в момент проверки каналы A, C или D недоступны или их качество значительно ухудшилось, для работы может быть выбран канал B.

Если для соединения с координатором используются каналы B, C или D, то по истечении периода опроса, при перезапуске программы ViPNet Монитор или при проверке соединения с координатором сетевой узел будет пытаться установить соединение с координатором по каналу A. Чем меньше период опроса, тем быстрее происходит переход на другой канал в случае сбоев и возвращение на более приоритетный канал.

# Настройка доступа к туннелируемым узлам

Если настройки параметров туннелирования для всех координаторов были сделаны в программе ViPNet Administrator или ViPNet Network Manager, то в программе ViPNet Монитор на сетевом узле ничего дополнительно настраивать не требуется. Сетевой узел сможет устанавливать соединения с туннелируемыми узлами. Если предварительных настроек не было сделано, то на сетевом узле настройте параметры соединения с туннелируемыми узлами вручную. Для этого выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.

2 В разделе **Защищенная сеть** дважды щелкните координатор, который осуществляет туннелирование требуемых открытых узлов.

3 В окне **Свойства узла** на вкладке **Туннель** установите флажок **Использовать IP-адреса для туннелирования** и с помощью соответствующих кнопок сформируйте список IP-адресов туннелируемых узлов. Заданным адресам автоматически будут сопоставлены виртуальные IP-адреса.

   Если вам не известен IP-адрес туннелируемого узла, то вы можете определить его по имени компьютера. Для этого нажмите кнопку **Определить имя/IP-адрес**  и в появившемся окне выполните поиск IP-адреса по указанному имени.

---

**Примечание.** Если необходимо указать DNS-имена туннелируемых узлов, эти имена следует добавить в список DNS-имен туннелирующего координатора (см. «Настройка доступа к защищенным узлам» на стр. 101). Следует иметь в виду, что на первом месте в этом списке должно стоять зарегистрированное на DNS-сервере имя координатора.

---

При добавлении IP-адреса будет автоматически выполнена его проверка на пересечение с IP-адресами, уже заданными в списке, и IP-адресами других сетевых узлов (в том числе, туннелированных). Данная проверка позволит исключить возможность задания одинаковых IP-адресов. Если в ходе проверки будет обнаружено пересечение IP-адресов, появится соответствующее сообщение. Устраните пересечение IP-адресов (см. «Обнаружен конфликт IP-адресов или DNS-имен» на стр. 286).

Вы также можете выполнить проверку на пересечение IP-адресов вручную. Для этого нажмите кнопку **Проверить конфликты**  .

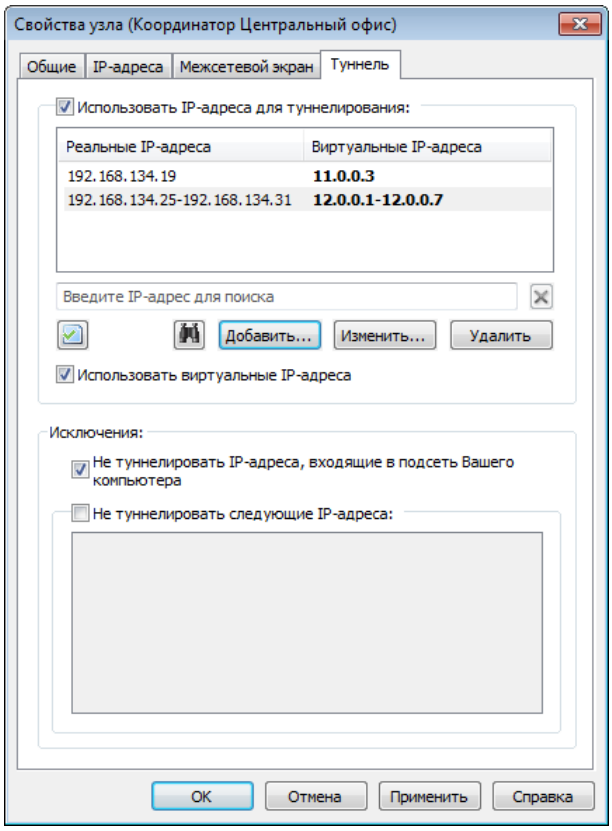



*Рисунок 43. Задание адресов туннелируемых узлов*

4 Если возможен конфликт IP-адресов в подсетях, установите флажок **Использовать виртуальные IP-адреса**.

5 Если туннелируемый узел находится в одной подсети с вашим узлом и на нем не настроена специальная маршрутизация, убедитесь, что установлен флажок **Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера**. Иначе соединение с туннелируемым узлом будет невозможно.

6 Если при соединении с какими-либо туннелированными узлами шифрование данных не требуется, рекомендуется установить флажок **Не туннелировать следующие IP-адреса** и добавить в список ниже IP-адреса этих узлов.

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

Настройки, описанные в данном разделе, должны быть выполнены на сетевом узле для всех координаторов, с туннелируемыми узлами которых требуется устанавливать соединения.

# Использование псевдонимов для защищенных узлов

Для удобства любому сетевому узлу в разделе **Защищенная сеть** можно задать произвольный псевдоним. Этот псевдоним будет отображаться вместо имени сетевого узла в разделе **Защищенная сеть**. Чтобы найти сетевой узел в списке, в строку поиска можно ввести как псевдоним, так и имя сетевого узла.

Чтобы задать псевдоним для сетевого узла, выполните следующие действия:

1. В программе ViPNet Монитор выберите раздел **Защищенная сеть** и дважды щелкните узел, для которого требуется задать псевдоним.
2. В окне **Свойства узла** на вкладке **Общие** в поле **Псевдоним** введите имя, которое нужно присвоить данному сетевому узлу.
3. Нажмите кнопку **OK**.
4. При необходимости добавьте псевдонимы для других защищенных сетевых узлов.

---

**Примечание.** Если после добавления псевдонима в списке по-прежнему указано имя сетевого узла, включите функцию отображения псевдонимов. Для этого:

- В программе ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
- В окне **Настройка** в разделе **Общие** установите флажок **Отображать псевдонимы ViPNet-пользователей**.

---

# Просмотр информации о сетевом узле

При организации доступа к узлу или при возникновении проблем с доступом, администратор сети ViPNet или служба технической поддержки может запросить информацию об этом сетевом узле, а также о вашем сетевом узле.

Чтобы просмотреть информацию о чужом сетевом узле ViPNet, выполните следующие действия:

1. В окне программы ViPNet Монитор в разделе **Защищенная сеть** дважды щелкните нужный сетевой узел.
2. В окне **Свойства узла** перейдите на вкладку **Общие**.
3. Если необходимо, скопируйте нужный текст, чтобы передать его администратору или службе технической поддержки.

Для просмотра информации о своем сетевом узле в главном окне программы в меню **Файл** выберите пункт **Свойства моего узла**.

# 6

# Настройка и использование служб имен DNS и WINS в сети ViPNet


Службы DNS и WINS 112

Службы DNS и WINS в сети ViPNet 115

DNS (WINS) сервер на защищенном или туннелируемом узле 116

Незащищенный DNS (WINS) сервер 118

Использование защищенного DNS (WINS) сервера для удаленной работы с корпоративными ресурсами 120

Использование DNS-серверов на контроллерах домена 125

# Службы DNS и WINS

К компьютерам удобнее обращаться не по цифровым адресам, а по каким-либо осмысленным именам, которые соответствуют функциям и местоположению компьютеров. Людям проще запомнить буквенное имя, чем последовательность цифр. Локальные сети и Интернет объединяют огромное количество компьютеров, поэтому необходимы специализированные службы имен, обеспечивающие сопоставление имен компьютеров с их IP-адресами. В настоящее время в сетях используются две службы имен — DNS и WINS.

## DNS

В сетях TCP/IP используется система доменных имен (Domain Name System, DNS), которая служит для преобразования IP-адреса в доменное имя и наоборот: например, 79.11.15.23 — в `www.company.ru`.

Следующий рисунок иллюстрирует использование DNS, то есть обнаружение IP-адреса компьютера по его имени.


*Рисунок 44. Общий принцип работы службы DNS*

Компьютер-клиент запрашивает у DNS-сервера IP-адрес компьютера с доменным именем `www.company.ru`. Поскольку DNS-сервер может ответить на запрос с помощью своей локальной базы данных, он возвращает ответ, содержащий запрашиваемую информацию, то есть запись об узле, в которой содержится IP-адрес, соответствующий имени `www.company.ru`.

Этот пример демонстрирует простой запрос DNS от клиента к DNS-серверу. На практике запросы DNS могут потребовать привлечения других серверов и выполнения дополнительных шагов, не показанных в этом примере.

Система именования, используемая DNS, носит иерархический характер. Доменное имя складывается из нескольких частей, расположенных справа налево. Первая часть (домен верхнего уровня) является фиксированной и назначается централизованно Сетевым Информационным Центром (Network Information Center, NIC). Домены остальных уровней присваиваются на серверах доменных имен произвольно.

# WINS

Аналогично DNS работает служба WINS (Windows Internet Name Service, служба имен сети Интернет для Windows), которая преобразует IP-адрес в NetBIOS-имя и наоборот: например, 192.168.1.20 — в HOST-A. Служба WINS является наиболее удобным средством разрешения имен NetBIOS в маршрутизируемых сетях, использующих NetBIOS через стек TCP/IP.

---

**Примечание.** NetBIOS (Network Basic Input Output System, сетевая базовая система ввода-вывода) — протокол сеансового уровня для работы в локальных сетях, обеспечивающий доступ компьютера как к собственным локальным ресурсам, так и к ресурсам удаленных компьютеров. Поскольку NetBIOS применяет рассылку широковещательных сообщений, он не поддерживает передачу информации через маршрутизаторы. Но с другой стороны, усовершенствования, внесенные в NetBIOS, позволяют этой системе работать поверх протоколов маршрутизации, таких как IP и IPX.

---

Служба WINS упрощает управление пространством имен NetBIOS в сетях на основе стека протоколов TCP/IP. Следующий рисунок иллюстрирует типичную последовательность событий, связанных с клиентами и серверами WINS.


*Рисунок 45. Общий принцип работы службы WINS*

Этот пример демонстрирует следующие события:

- (1) WINS-клиент HOST-A регистрирует любое из своих локальных имен NetBIOS на своем WINS-сервере WINS-A.

  В случае, если компьютер HOST-A не имеет в своем распоряжении IP-адреса WINS-сервера, он передает в широковещательной рассылке свое имя NetBIOS, объявляя тем самым о своем присутствии в сети. Когда происходит подобное событие, локальный WINS-сервер принимает такое широковещательное сообщение и вводит содержащееся в нем имя и соответствующий IP-адрес в свою базу данных.

- (2) Другой WINS-клиент HOST-B запрашивает сервер WINS-A найти IP-адрес компьютера HOST-A в сети.

- (3) Сервер WINS-A возвращает 192.168.1.20 — IP-адрес компьютера HOST-A.

Службы WINS и DNS могут бесконфликтно работать в пределах одной сети. Пространства имен той и другой службы не совпадают. DNS использует иерархическую структуру именования, в то время как WINS — одноранговую. Служба WINS особенно актуальна для сетей, на узлах которых установлена ОС Windows Server 2003. В сетях, в которых применяются и доменные имена, и имена NetBIOS, рекомендуется использовать обе службы.

# Службы DNS и WINS в сети ViPNet

В сетях ViPNet приложения могут использовать виртуальные IP-адреса, реально не существующие в сети и уникальные на каждом сетевом узле, что позволяет избежать конфликтов при наличии пересекающихся адресов в разных сетях.

Для обеспечения работы служб DNS и WINS в сети ViPNet с виртуальными адресами программное обеспечение ViPNet автоматически выполняет специальную обработку IP-пакетов этих служб. Такая обработка требуется для того, чтобы на защищенных узлах приложения, которые обращаются к службам DNS и WINS, использовали для доступа к другим защищенным и туннелируемым узлам правильные IP-адреса (реальные или виртуальные).

Если на DNS (WINS) сервере, к которому обращаются приложения, установлено ПО ViPNet или этот сервер туннелируется координатором, поддержка DNS (NetBIOS) имен для виртуальных адресов обеспечивается без дополнительных настроек ПО ViPNet при соблюдении определенных правил (см. «DNS (WINS) сервер на защищенном или туннелируемом узле» на стр. 116).

DNS-имена для защищенных узлов можно задать вручную в программе ViPNet Монитор на сетевом узле либо в программе ViPNet Центр управления сетью или ViPNet Network Manager. В этом случае при использовании службы DNS появляются дополнительные возможности:

- Обеспечивается безопасная работа приложений с удаленными защищенными узлами ViPNet по DNS-именам при использовании открытых (публичных) DNS-серверов (см. «Незащищенный DNS (WINS) сервер» на стр. 118).
- Появляется возможность взаимодействия защищенного узла ViPNet со своим координатором по DNS-имени путем публикации на DNS-сервере IP-адреса, не принадлежащего координатору (например, IP-адреса доступа к координатору через NAT-устройство). При автоматической публикации адреса доступа к координатору на публичном DNS-сервере (технология динамического DNS, или DYN DNS) можно организовать безопасный доступ к координатору, адрес доступа к которому динамически изменяется.

# DNS (WINS) сервер на защищенном или туннелируемом узле

## Особенности использования

Использование DNS (WINS) сервера, расположенного на защищенном или туннелируемом узле, имеет следующие особенности:

- Для обеспечения работоспособности служб имен DNS и WINS не нужно выполнять никаких дополнительных настроек ПО ViPNet.
- Если DNS (NetBIOS) имена и соответствующие им IP-адреса защищенных и туннелируемых узлов автоматически регистрируются на DNS (WINS) сервере, то технология ViPNet обеспечивает автоматическую публикацию на этом сервере требуемых реальных или виртуальных IP-адресов защищенных и туннелируемых узлов. ViPNet-драйвер на DNS (WINS) сервере (или на координаторе, туннелирующем этот сервер) выполняет подмену адреса в IP-пакете на виртуальный или реальный IP-адрес.
- Если к DNS (WINS) серверу обращается защищенный или туннелируемый узел, к ответу добавляется идентификатор запрашиваемого узла в сети ViPNet (или идентификатор координатора, который туннелирует запрашиваемый узел). По этому идентификатору программное обеспечение ViPNet на узле, с которого был отправлен запрос (или на координаторе, его туннелирующем), определяет правильный адрес доступа к запрашиваемому узлу — реальный или виртуальный.
- Если к защищенному DNS (WINS) серверу обращается открытый компьютер, программное обеспечение ViPNet на DNS (WINS) сервере или на туннелирующем координаторе обрабатывает ответ таким образом, чтобы сообщить открытому компьютеру реальные IP-адреса защищенных и туннелируемых узлов, даже если для них опубликованы виртуальные IP-адреса.

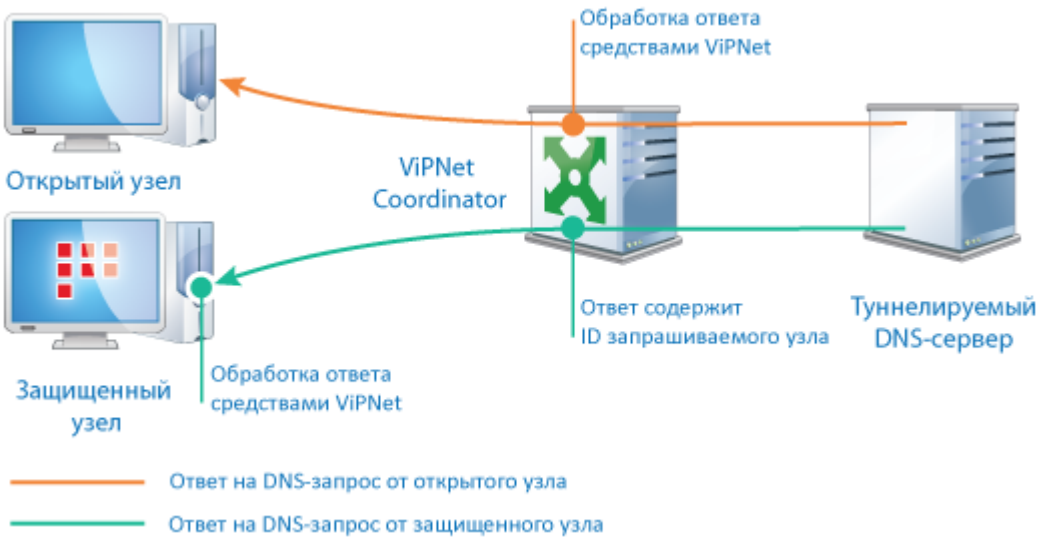



*Рисунок 46. DNS-сервер на защищенном или туннелируемом узле*

# Рекомендации по настройке

При использовании DNS (WINS) сервера, расположенного на защищенном или туннелируемом узле, и при необходимости публикации виртуальных IP-адресов следует соблюдать следующие рекомендации:

- При регистрации вручную на DNS (WINS) сервере IP-адресов защищенных и туннелируемых узлов следует указывать их виртуальные или реальные IP-адреса, по которым эти узлы видны в программе ViPNet Монитор, установленной на DNS (WINS) сервере, или на координаторе, осуществляющем туннелирование этого сервера.
- Если DNS (WINS) сервер расположен на узле с ПО ViPNet, то в подсети этого сервера не следует размещать туннелируемые каким-либо координатором узлы, с которых будут поступать запросы на сервер (или адреса которых будут запрашиваться другими узлами). Если сервер расположен на координаторе, то данное требование относится к туннелируемым узлам других координаторов.
- Если DNS (WINS) сервер туннелируется координатором, то в подсети этого сервера не следует размещать узлы с ПО ViPNet, с которых будут поступать запросы на сервер (или адреса которых будут запрашиваться другими узлами).
- Если возникает необходимость размещения узлов в нарушение приведенных рекомендаций, то на узлах с ПО ViPNet следует снять флажок **Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера** (см. «Настройка доступа к туннелируемым узлам» на стр. 107), а на туннелируемых узлах настроить частный маршрут на узлы с ПО ViPNet через координатор.

# Незащищенный DNS (WINS) сервер

## Особенности использования

Часто возникает задача получения доступа к координатору с динамически изменяющимся внешним адресом доступа (например, координатор подключен к сети через DSL-модем) со стороны других защищенных узлов. Для решения данной задачи можно опубликовать адрес этого координатора на публичном DNS-сервере, расположенном в Интернете, и задать DNS-имя координатора в программе ViPNet Монитор на других узлах. В корпоративной сети может возникнуть необходимость в использовании публичного DNS-сервера и в других случаях.

Однако публичные DNS-серверы могут быть подвержены различным сетевым атакам, в результате которых происходит подмена IP-адреса запрашиваемого сетевого ресурса с целью заставить защищенный компьютер обратиться на атакующий компьютер. Если такая атака удастся, при обращении к защищенному узлу по DNS-имени он установит с атакующим компьютером открытое соединение, так как IP-адрес атакующего компьютера не известен ViPNet-драйверу. В результате злоумышленник может получить интересующую его информацию с защищенного компьютера.


*Рисунок 47. Атака на публичный DNS-сервер*

Чтобы предотвратить атаки подобного рода, для защищенных прикладных серверов (см. «Защищенные прикладные серверы» на стр. 399), регистрируемых на публичном DNS-сервере и доступных с защищенного узла, в программе ViPNet Монитор на этом узле следует указать DNS-имена (см. «Настройка доступа к защищенным узлам» на стр. 101). Тогда при обращении к серверу по DNS-имени независимо от адреса, подставленного злоумышленником, при приеме ответа на DNS-запрос ViPNet-драйвер подставит уже известный ему IP-адрес видимости узла (реальный или виртуальный), соответствующий заданному в программе ViPNet Монитор DNS-имени.

# Рекомендации по настройке

При использовании открытого DNS-сервера следует выполнять следующие рекомендации:

- Если внешний IP-адрес доступа к координатору может изменяться, для организации доступа к этому координатору по DNS-имени, зарегистрированному на открытом DNS-сервере, в программе ViPNet Монитор на защищенных узлах для данного координатора следует указать DNS-имя.
- Если на узле с установленным ПО ViPNet другие защищенные узлы доступны по виртуальным IP-адресам, и необходимо обеспечить доступ к этим узлам по DNS-именам, зарегистрированным на открытом DNS-сервере, то эти DNS-имена следует указать в программе ViPNet Монитор. При этом на открытом DNS-сервере может быть зарегистрирован любой адрес (реальный или виртуальный). Технология ViPNet обеспечит защищенное соединение по виртуальному адресу видимости узла вне зависимости от типа опубликованного адреса.
- Как было сказано выше, даже если доступ к защищенным узлам обеспечивается по реальным адресам, для обеспечения безопасности важно указать их DNS-имена в программе ViPNet Монитор.

Во всех описанных случаях DNS-имена защищенных узлов могут быть заданы вручную на каждом сетевом узле (см. «Настройка доступа к защищенным узлам» на стр. 101), однако рекомендуется указывать DNS-имена централизованно в программе ViPNet Центр управления сетью или ViPNet Network Manager.

# Использование защищенного DNS (WINS) сервера для удаленной работы с корпоративными ресурсами

Удаленные пользователи подключаются к сети ViPNet через Интернет. Они могут работать дома, в интернет-кафе, в гостинице или других местах, где IP-адреса и используемые DNS (WINS) серверы определяются поставщиком услуг Интернета. Однако для работы со многими корпоративными приложениями требуется использовать DNS (WINS) сервер корпоративной сети. Использование корпоративного DNS (WINS) сервера позволяет обращаться к серверам и другим узлам корпоративной сети по их именам, а не по IP-адресам. При этом преобразование DNS (WINS) имен в IP-адреса обеспечивается как для адресов корпоративной сети, так и для адресов Интернета.

## Автоматическая регистрация DNS (WINS) серверов

Для удаленного доступа к узлам корпоративной сети по DNS-именам должны быть выполнены следующие условия:

- В системном файле `hosts`, который устанавливает соответствие между IP-адресами и именами компьютеров, не должно быть записей об узлах корпоративной сети. Этот файл расположен в папке `%systemroot%\System32\drivers\etc\` (по умолчанию это `C:\Windows\System32\drivers\etc\`).
- В свойствах подключения к сети должен быть указан адрес корпоративного DNS (WINS) сервера.

**Внимание!** Если защищенный узел зарегистрирован и на корпоративном DNS-сервере, и на открытом, то могут возникнуть проблемы с доступом к нему. Для решения его DNS-имя требуется задать в свойствах узла на вкладке **IP-адреса** (см. «Настройка доступа к защищенным узлам» на стр. 101).

Вы можете указать адрес корпоративного DNS-сервера в свойствах подключения к сети вручную. Однако рекомендуется задать адреса корпоративных DNS-серверов централизованно. Для этого администратору сети ViPNet следует указать сетевые узлы или туннелируемые узлы, на которых расположены DNS-серверы, в программе ViPNet Центр управления сетью или ViPNet Network Manager. В этом случае список корпоративных DNS-серверов будет передан на сетевые узлы

ViPNet вместе с ключами и справочниками. На сетевых узлах программа ViPNet Монитор будет определять текущие IP-адреса видимости корпоративных DNS-серверов (реальные или виртуальные) и автоматически изменять адреса DNS-серверов в настройках сетевых интерфейсов компьютера.

Рассмотрим следующий пример. Сотрудник, работающий в главном офисе на ноутбуке с установленным ПО ViPNet Client, подключается к защищенному корпоративному DNS-серверу по одному адресу (например, 10.0.0.25). В какой-то момент времени этот сотрудник отправляется со своим ноутбуком в командировку в другой офис, и DNS-сервер главного офиса становится доступен по другому IP-адресу (например, 11.0.0.3). При этом сотруднику нужно подключиться через Интернет к корпоративным ресурсам главного офиса.

При регистрации DNS-сервера средствами операционной системы сотруднику потребуется на ноутбуке изменять настройки подключения к сети, что неудобно, поскольку после возвращения в главный офис эти настройки нужно будет вернуть в исходное состояние. Если узлы, на которых расположены DNS-серверы, заданы в программе ViPNet Центр управления сетью или ViPNet Network Manager, изменять настройки подключения к сети вручную не требуется.

Если по какой-либо причине адреса корпоративных DNS-серверов не заданы в программе ViPNet Центр управления сетью или ViPNet Network Manager, на сетевом узле вы можете задать список защищенных DNS-серверов вручную, как описано ниже.

# Создание списка DNS (WINS) серверов вручную

Если список корпоративных DNS (WINS) серверов не был задан централизованно в программе ViPNet Центр управления сетью или ViPNet Network Manager (см. «Автоматическая регистрация DNS (WINS) серверов» на стр. 120), вы можете создать такой список вручную на вашем сетевом узле. В этом случае программа ViPNet Монитор также будет определять текущие IP-адреса видимости корпоративных DNS-серверов и автоматически изменять настройки сетевых интерфейсов компьютера.

Для регистрации корпоративного DNS (WINS) сервера вручную выполните следующие действия:

1. В любом текстовом редакторе (лучше «Блокнот») создайте пустой текстовый файл `DNS.TXT`.
2. Внесите в него запись о корпоративном DNS (WINS) сервере. О том, как указать информацию о сервере, см. в разделах ниже. Формат записей в файле `DNS.TXT` отличается в зависимости от того, установлен ли корпоративный DNS (WINS) сервер на защищенном узле или туннелируется координатором.
3. Сохраните файл в папке `\DATABASES\DNSWINSLIST`, находящейся в папке установки ПО ViPNet (если папка не существует, создайте ее).

**Примечание.** Все операции по созданию и редактированию файла `DNS.TXT` можно производить без выгрузки программы ViPNet Монитор из памяти компьютера.

В файле `DNS.TXT` можно зарегистрировать сразу несколько DNS (WINS) серверов. В этом случае на всех сетевых интерфейсах компьютера списки IP-адресов DNS (WINS) серверов будут дополнены IP-адресами, по которым в данный момент доступны указанные серверы. Одновременно в настройках сетевых интерфейсов сохранятся IP-адреса, полученные по DHCP или заданные на сетевых интерфейсах вручную, если эти IP-адреса не принадлежат указанным в `DNS.TXT` серверам.

**Примечание.** Если используемые DNS (WINS) серверы перечислены в файле `DNS.TXT`, задавать их адреса в сетевых настройках Windows не требуется.

## Если корпоративный DNS (WINS) сервер установлен непосредственно на сетевом узле ViPNet

Если корпоративный DNS (WINS) сервер установлен на защищенном сетевом узле, то в файле `DNS.TXT` укажите следующую информацию:

- Для DNS-сервера:

  ```
  [DNSLIST]
  ID00=<идентификатор>;
  ```

- Для WINS-сервера:

  ```
  [WINSLIST]
  ID00=<идентификатор>;
  ```

  где: `<идентификатор>` — шестнадцатеричный идентификатор сетевого узла ViPNet, на котором установлен DNS (WINS) сервер, с номером сети;

  **Примечание.** Чтобы узнать идентификатор узла, в программе ViPNet Монитор в разделе **Защищенная сеть** дважды щелкните сетевой узел, на котором установлен DNS (WINS) сервер. Откроется окно **Свойства узла**. На вкладке **Общие** в первой строке будет указан идентификатор сетевого узла.

  `ID00` — идентификатор номера строки, где после ID допустимы любые цифры.

В разделе ниже вы можете ознакомиться с примером составления файла `DNS.TXT` (см. «Пример составления файла DNS.TXT» на стр. 123).

## Если корпоративный DNS (WINS) сервер туннелируется координатором

Если корпоративный DNS (WINS) сервер туннелируется координатором, то в файле `DNS.TXT` укажите следующую информацию:

- Для DNS-сервера:

  ```
  [DNSLIST]
  ID00=<идентификатор>-<IP-адрес>;
  ```

- Для WINS-сервера:

  ```
  [WINSLIST]
  ID00=<идентификатор>-<IP-адрес>;
  ```

  где: `<идентификатор>` — шестнадцатеричный идентификатор координатора, туннелирующего DNS (WINS) сервер, с номером сети;

  **Примечание.** Чтобы узнать идентификатор координатора, который туннелирует DNS (WINS) сервер, в программе ViPNet Монитор дважды щелкните его в разделе **Защищенная сеть**. Откроется окно **Свойства узла**. На вкладке **Общие** в первой строке будет указан идентификатор координатора.

  `ID00` — идентификатор номера строки, где после ID допустимы любые цифры.

В отличие от ситуации, когда корпоративный DNS (WINS) сервер установлен непосредственно на сетевом узле ViPNet, здесь указывается идентификатор координатора, который туннелирует DNS (WINS) сервер, и через дефис непосредственно IP-адрес DNS (WINS) сервера. Если имеется несколько DNS (WINS) серверов, которые туннелируются одним координатором, их IP-адреса можно перечислить в одной строке через точку с запятой без пробелов после идентификатора координатора: `ID00=<идентификатор>-<IP-адрес 1>;<IP-адрес 2>`.

При этом следует убедиться, что в списке туннелируемых адресов данного координатора эти IP-адреса также присутствуют.

В разделе ниже вы можете ознакомиться с примером составления файла `DNS.TXT` (см. «Пример составления файла DNS.TXT» на стр. 123).

## Пример составления файла DNS.TXT

Ниже приведен пример того, как может быть составлен файл `DNS.TXT`:

```
[DNSLIST]
ID00=000100CA-10.0.0.25;
ID01=0001000b;
ID02=000110bc-10.0.0.20;10.0.0.21;10.0.2.132;
[WINSLIST]
ID00=0001000b;
ID01=000101fa-10.0.1.132;10.0.1.133;10.0.1.134;
```

Обратите внимание, что в одном файле `DNS.TXT` могут содержаться записи как для DNS (WINS) серверов, установленных на сетевых узлах ViPNet, так и туннелируемых тем или иным координатором. Число записей не ограничивается.

# Использование DNS-серверов на контроллерах домена

Если в сети ViPNet вашей организации используется служба Active Directory и при этом защищенные контроллеры домена с DNS-серверами, которые в рамках домена синхронизируются между собой, защищены разными узлами ViPNet, то могут возникнуть проблемы разрешения IP-адресов при обращении к ним с других защищенных узлов. Для предотвращения проблем в этом случае необходимо обеспечить регистрацию на всех резервируемых DNS-серверах одного и того же адреса каждого узла.

Воспользуйтесь одним из следующих вариантов:

- Разместите DNS-серверы без установленного ПО ViPNet за отдельным сетевым интерфейсом координатора и настройте туннелирование этих серверов данным координатором (см. «Если корпоративный DNS (WINS) сервер туннелируется координатором» на стр. 123). Другие защищенные и открытые узлы, которые обращаются к DNS-серверам, во избежание конфликтов не должны находиться со стороны данного интерфейса координатора.

  Если регистрация IP-адресов узлов осуществляется на защищенном DNS-сервере автоматически, будут зарегистрированы IP-адреса, соответствующие видимости узлов с данного координатора. Если регистрация IP-адресов узлов осуществляется на DNS-сервере вручную, на каждом DNS-сервере зарегистрируйте IP-адреса видимости узлов (виртуальные или реальные) с этого координатора. Открытые узлы, которые обращаются к DNS-серверу за IP-адресом защищенного узла через координатор, получат реальный IP-адрес этого узла.

- Если размещение DNS-серверов за одним координатором затруднительно или на них установлена программа ViPNet Client, на координаторах, за которыми расположены DNS-серверы, или в программе ViPNet Client настройте видимость узлов (туннелируемых узлов, клиентов и координаторов), зарегистрированных на этих DNS-серверах, по реальным IP-адресам.

  Чтобы изменить IP-адрес видимости всех клиентов, стоящих за координатором, достаточно изменить IP-адрес видимости координатора на одном из клиентов в программе ViPNet Client Монитор, после чего появится сообщение с предложением изменить аналогичным образом IP-адреса видимости клиентов, расположенных за данным координатором.

# 7

# Интегрированный сетевой экран


Основные принципы фильтрации трафика 127

Общие сведения о сетевых фильтрах 129

Использование групп объектов 133

Создание сетевых фильтров 144

Восстановление предустановленных фильтров и групп объектов 150

Практический пример использования групп объектов и сетевых фильтров 151

Блокировка IP-трафика 154

Отключение защиты трафика 155

# Основные принципы фильтрации трафика

Фильтрации подвергается весь IP-трафик, который проходит через сетевой узел:

- открытый (незашифрованный) трафик;
- защищенный (зашифрованный) трафик.

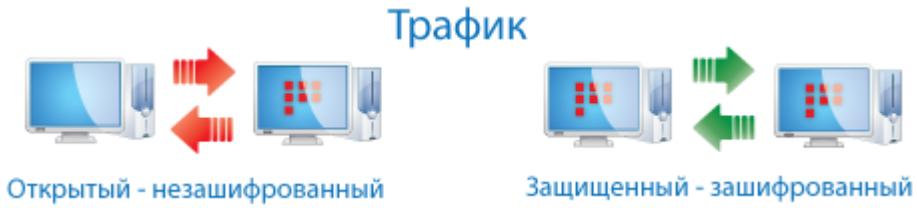



*Рисунок 48. Виды IP-трафика*

Наибольшую опасность представляет трафик из открытой сети, поскольку в случае атаки достаточно сложно обнаружить ее источник и принять оперативные меры по ее пресечению.

И открытый, и защищенный трафик может быть локальным или широковещательным. Под локальным трафиком понимается входящий или исходящий трафик конкретного узла (то есть когда сетевой узел является отправителем или получателем IP-пакетов). Под широковещательным трафиком имеется в виду передача узлом IP-пакетов, у которых IP-адрес или MAC-адрес назначения является широковещательным адресом (то есть передача пакетов всем узлам определенного сегмента сети).


*Рисунок 49. Виды защищенного и открытого трафика*

Для того чтобы правильно настроить сетевые фильтры, необходимо понимать основные принципы фильтрации трафика.

Все входящие и исходящие открытые и защищенные IP-пакеты проходят комплексную проверку в соответствии с сетевыми фильтрами (см. «Общие сведения о сетевых фильтрах» на стр. 129). Если IP-пакет соответствует параметрам одного из имеющихся сетевых фильтров, то он пропускается или блокируется в соответствии с этим фильтром. Если пакет не соответствует ни одному из заданных фильтров, то он блокируется.

Такой принцип фильтрации обеспечивает высокий уровень безопасности, разрешая соединения только с нужными узлами по заданным протоколам и портам. IP-пакет последовательно проходит ряд фильтров, пока не будет пропущен или заблокирован одним из них. Как только пакет пропускается или блокируется, все последующие фильтры уже не действуют. Если пакет не был обработан ни одним фильтром, то он блокируется.

Сетевые фильтры к зашифрованным IP-пакетам применяются только после их успешной расшифровки и идентификации сетевого узла-источника. В этом случае IP-адреса сетевых узлов не имеют никакого значения.

**Примечание.** В ПО ViPNet Client версии 3.2 и ниже принцип фильтрации определялся выбранным режимом безопасности.

Схематично последовательность фильтрации IP-пакетов представлена ниже:


*Рисунок 50. Уровни фильтрации трафика*

# Общие сведения о сетевых фильтрах

Существуют сетевые фильтры как для защищенного, так и для открытого трафика. Они выполняют следующие функции:

- Фильтры открытой сети на защищенном узле могут разрешать либо запрещать обмен IP-трафиком с открытыми узлами.

  **Примечание.** Под открытыми узлами понимаются узлы, на которых не установлено программное обеспечение ViPNet с функцией шифрования трафика. К ним относятся также компьютеры с программным обеспечением ViPNet CryptoService и ViPNet Registration Point.

- Фильтры защищенной сети могут ограничивать обмен IP-трафиком с защищенными узлами ViPNet, с которыми данный узел имеет связь.

При запуске программы ViPNet Client, при включении защиты трафика или смене конфигурации программы сетевые фильтры загружаются в ViPNet-драйвер (на стр. 15). При этом выполняется контроль целостности базы сетевых фильтров. Если целостность сетевых фильтров будет нарушена, появится соответствующее предупреждение, и будут загружены предустановленные сетевые фильтры.

Все сетевые фильтры делятся на следующие категории:

- Фильтры, определенные специальными конфигурациями.
- Фильтры, поступившие в составе политик безопасности (см. «Политика безопасности» на стр. 402) из программы ViPNet Policy Manager.

  С помощью специальной опции в режиме администратора можно исключить данные фильтры из списков сетевых фильтров (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220).
- Предустановленные фильтры и фильтры, заданные пользователем.

  В том случае если программа ViPNet Монитор была обновлена до версии 4.x с версии 3.x, предустановленных фильтров не будет. В списках сетевых фильтров будут присутствовать только фильтры, которые действовали в программе до обновления (в сконвертированном формате).
- Фильтры по умолчанию.

Фильтры, определенные специальными конфигурациями программы, имеют более высокий приоритет, чем все остальные фильтры, и применяются в первую очередь. Они ограничивают трафик, который запрещен в конфигурациях «Открытый Интернет» (см. «Конфигурация „Открытый Интернет“» на стр. 208), «Внутренняя сеть» или «Интернет» (см. «Конфигурации „Внутренняя сеть“ и «Интернет»» на стр. 208). Их нельзя редактировать и удалять.

**Примечание.** При работе с защищенными контейнерами SafeDisk-V действуют специальные запрещающие фильтры. Они формируются при запуске программы ViPNet SafeDisk-V (см. «Работа с интегрированной программой ViPNet SafeDisk-V» на стр. 167) и по приоритету становятся выше всех остальных фильтров, в том числе и фильтров специальных конфигураций. Поскольку в процессе работы в ViPNet SafeDisk-V действуют ограничения на интерфейс программы ViPNet Монитор, данные фильтры просмотреть нельзя, переключиться в специальные конфигурации также невозможно.

После фильтров конфигураций следуют фильтры, поступившие из ViPNet Policy Manager, которые также недоступны для редактирования. Далее размещаются предустановленные фильтры и фильтры, заданные пользователем в программе ViPNet Монитор. При определенных полномочиях их всегда можно изменить или удалить. Самыми последними фильтрами являются фильтры по умолчанию. Данная категория представлена одним сетевым фильтром, блокирующим IP-трафик, который не соответствует ни одному из сетевых фильтров из категорий выше.

Последовательность применения сетевых фильтров согласно приоритету изображена на схеме ниже.

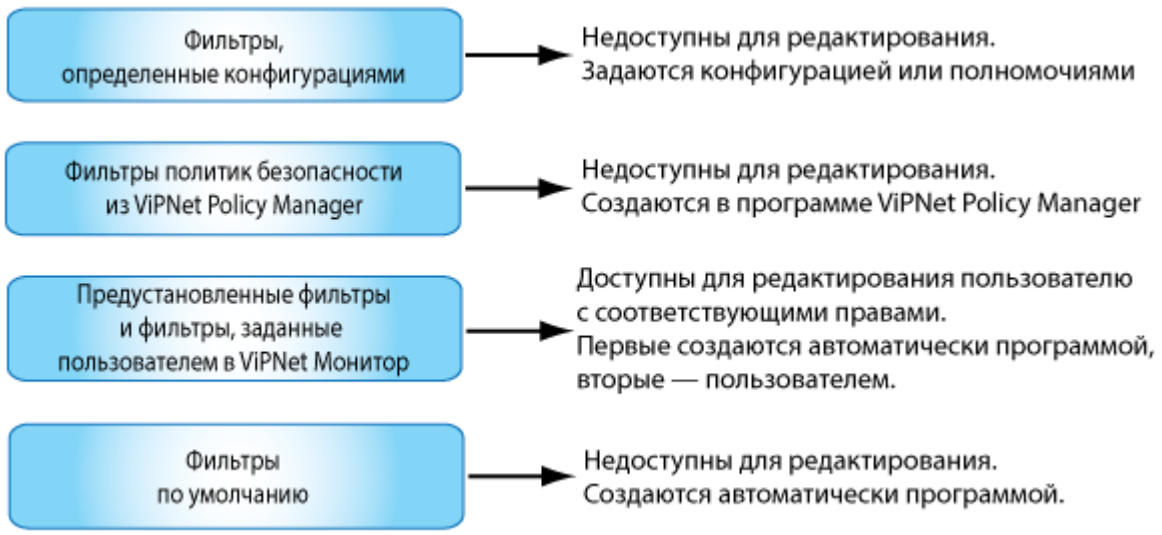



*Рисунок 51. Приоритет применения сетевых фильтров*

Списки сетевых фильтров представлены на панели просмотра в окне программы ViPNet Client Монитор в разделах **Фильтры защищенной сети** и **Фильтры открытой сети**.

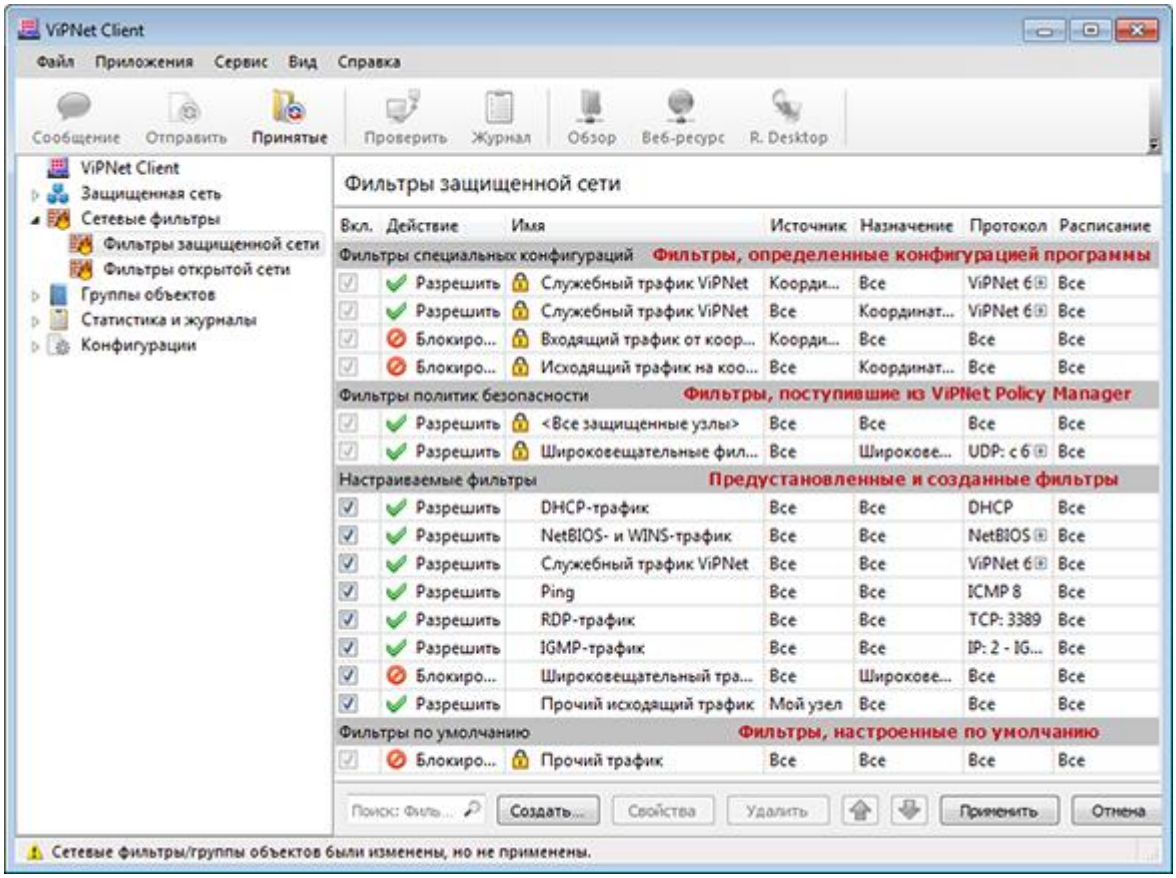



*Рисунок 52. Пример отображения фильтров для защищенного трафика разных категорий*

Сетевые фильтры имеют следующие особенности:

- Фильтры включают в себя следующие параметры:
  - Действие, применяемое к IP-пакетам. Фильтры могут пропускать (✔) или блокировать (⊘) IP-пакеты, соответствующие заданным параметрам.
  - Источник и назначение IP-пакетов, на которые распространяется действие фильтра.
  - Протоколы фильтрации IP-пакетов.
  - Расписание действия.

  Для задания параметров фильтра могут использоваться группы объектов (см. «Использование групп объектов» на стр. 133).
- Фильтры, созданные пользователем, влияют как на новые, так и на уже существующие соединения. Таким образом, если фильтр, блокирующий трафик соединения, добавлен после установления соединения, то оно будет разорвано.
- IP-пакеты проверяются в соответствии с расположением фильтров в списке, по порядку сверху вниз. Когда пакет блокируется или пропускается первым подходящим фильтром, последующие фильтры уже не оказывают никакого влияния на данный пакет.
- В программе ViPNet Монитор фильтры различных категорий в списках фильтров отображаются в соответствующих группах и располагаются в порядке их приоритета согласно схеме выше.

Порядок фильтров, определенных конфигурацией программы, фильтров, поступивших из ViPNet Policy Manager, и фильтров по умолчанию изменить нельзя. Порядок предустановленных фильтров и фильтров, заданных в ViPNet Монитор, вы можете изменять с помощью кнопок  и  .

Фильтры, которые нельзя отредактировать и удалить, отмечены значком  .

- Чтобы изменить действие фильтра, двойным щелчком откройте свойства фильтра и в разделе **Основные параметры** выберите требуемое значение. Чтобы включить или отключить фильтр, установите или снимите флажок рядом с именем фильтра.
- При изменении настроек сетевых фильтров или создании новых фильтров в строке состояния появляется сообщение о том, что фильтры были изменены, но не применены. Измененные или новые фильтры вступят в действие после того, как вы нажмете кнопку **Применить** и в течение 30 секунд подтвердите сохранение изменений.

---

**Примечание.** Для гарантированного применения фильтров, блокирующих трафик, также требуется перезагрузить компьютер.

---

Если вам не требуется сохранять новые настройки фильтров, нажмите кнопку **Отмена**. В этом случае произойдет возврат к тем настройкам фильтров, которые действовали на момент их изменения.

При необходимости вы можете отменить все произведенные изменения и восстановить предустановленные фильтры (см. «Восстановление предустановленных фильтров и групп объектов» на стр. 150).

# Использование групп объектов

Группы объектов — это средство, позволяющее упростить создание сетевых фильтров в программе ViPNet Монитор. Они объединяют несколько значений одного типа и могут быть заданы при настройке параметров фильтра вместо отдельных объектов.

Группы объектов делятся на несколько видов:

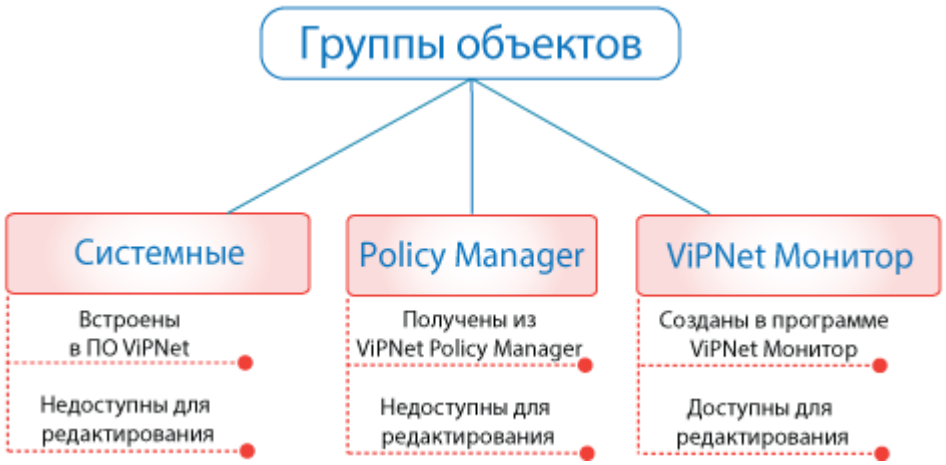



*Рисунок 53. Виды групп объектов*

Системные группы объектов — встроенные в ПО ViPNet Client объекты с фиксированными именами, которые могут использоваться в создаваемых сетевых фильтрах для задания отправителей и получателей IP-пакетов, а также в других пользовательских группах объектов. Системные группы объектов не отображаются в списках групп и их нельзя изменить или удалить. Список системных групп объектов см. в разделе Системные группы объектов (на стр. 135).

Группы объектов, создаваемые в ПО ViPNet Policy Manager, — группы, которые рассылаются вместе с политиками безопасности. Они недоступны для редактирования и использования в создаваемых сетевых фильтрах, других пользовательских группах объектов. В программе ViPNet Монитор можно только просмотреть состав данных групп.

Пользовательские группы объектов — группы объектов, создаваемые пользователем непосредственно в программе ViPNet Монитор, а также некоторые группы, настроенные по умолчанию. Подробнее о группах по умолчанию см. в разделе Пользовательские группы объектов, настроенные по умолчанию (на стр. 135). У каждой группы объектов есть свой состав, при этом из состава могут быть заданы некоторые исключения. В состав и исключения группы могут быть включены другие группы объектов той же категории или некоторые системные группы объектов. Работа с такими группами объектов осуществляется в окне программы ViPNet Client Монитор в разделе **Группы объектов**.

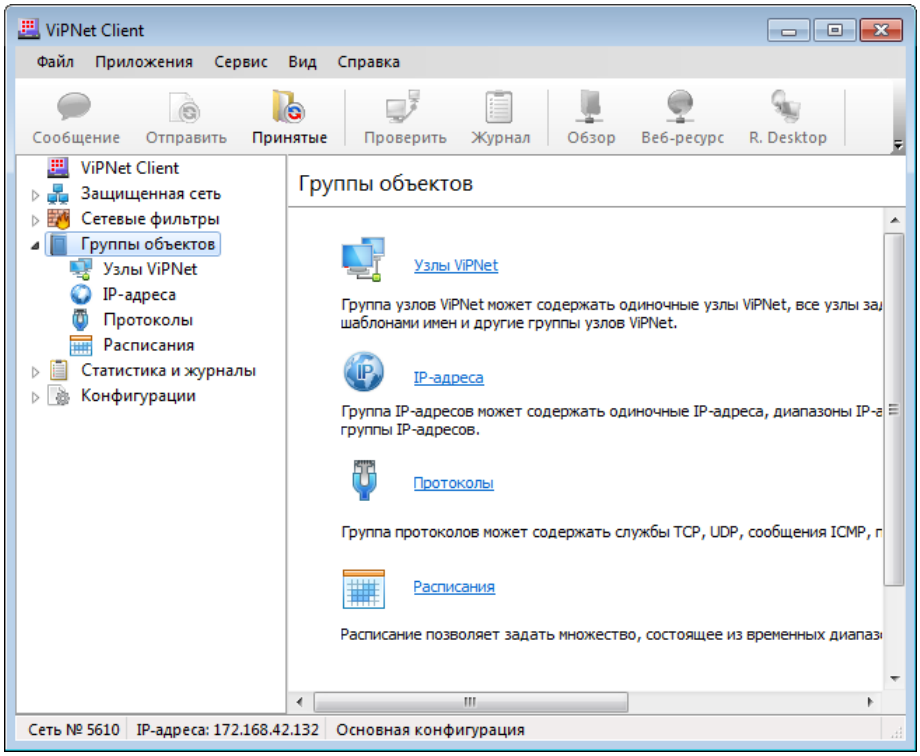



*Рисунок 54: Работа с пользовательскими группами объектов*

Пользовательские группы объектов делятся на следующие типы:

- **Узлы ViPNet** — группа узлов защищенной сети. Используется в фильтрах защищенной сети.
- **IP-адреса** — любая комбинация отдельных IP-адресов и диапазонов IP-адресов или DNS-имен. Используется в фильтрах открытой сети.
- **Протоколы** — любая комбинация протоколов и портов. Используется во всех фильтрах.
- **Расписания** — любая комбинация условий применения сетевых фильтров по времени и дням недели. Используется во всех фильтрах.

Вы можете создать группу объектов любой категории. Имеет смысл создавать группы из часто используемых наборов объектов. Подробнее о создании групп см. в разделе Создание и изменение групп объектов (на стр. 136).

# Системные группы объектов

В таблице ниже приведен список системных групп объектов и их значений.

*Таблица 4. Системные группы объектов*

| Имя группы объектов | Значение |
|---|---|
| Все клиенты | Все клиенты из справочников узла |
| Все координаторы | Все координаторы из справочников узла |
| Все объекты | Совокупность всех объектов в группе конкретного типа. Задается только в составе группы объектов. Предназначена для создания групп, состоящих из всех объектов, кроме некоторых исключений |
| Координаторы Открытого Интернета | Множество координаторов открытого Интернета, присутствующих в сети ViPNet<br>Используется только в фильтрах, определенных конфигурацией «Открытый Интернет». В создаваемых фильтрах ее указать нельзя |
| Широковещательные адреса | Все широковещательные адреса<br>Используется при создании фильтров широковещательных пакетов |
| Мой узел | Свой узел<br>Можно указать в качестве источника IP-пакетов для исходящих соединений узла или в качестве назначения для входящих соединений |
| Другие узлы | Другие сетевые узлы (любые узлы, кроме своего)<br>Можно указать в качестве источника IP-пакетов для входящих соединений узла или в качестве назначения для исходящих соединений |
| Групповые адреса | Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255)<br>Можно указать только в качестве назначения для открытых соединений |

# Пользовательские группы объектов, настроенные по умолчанию

В составе программы ViPNet Client имеется ряд предварительно настроенных групп объектов:

- Две группы IP-адресов по умолчанию:

- **Публичные IP-адреса** — группа, в составе которой указаны все IP-адреса, за исключением частных IP-адресов.
- **Частные IP-адреса** — группа, в составе которой указаны IP-адреса локальных сетей: 10.0.0.0; 172.16.0.0; 192.168.0.0.

- Множество групп протоколов по умолчанию. В данном множестве представлены группы протоколов, которые чаще всего используются при создании сетевых фильтров. Одними из них являются группы: **DHCP**, **ViPNet базовые службы**, **ViPNet удаленный просмотр журнала** и другие.
- Две группы расписаний по умолчанию:
  - **Рабочие дни** — группа с расписанием, в котором заданы рабочие дни недели (понедельник — пятница).
  - **Выходные дни** — группа с расписанием, в котором заданы выходные дни (суббота и воскресенье).

# Создание и изменение групп объектов

Чтобы создать новую группу объектов, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Группы объектов**.
2. На панели просмотра щелкните ссылку с названием типа группы объектов, которую вы хотите создать, или на панели навигации выберите соответствующий подраздел.
3. На панели просмотра нажмите кнопку **Создать**.

   Откроется окно свойств группы объектов, в котором вы можете задать параметры новой группы.
4. В разделе **Основные параметры** задайте имя группы объектов. Имя группы должно быть уникальным.
5. В разделе **Состав** определите состав создаваемой группы.

   При формировании состава группы типа:

   - **Узлы ViPNet —** укажите защищенные узлы, которые необходимо включить в создаваемую группу. Подробнее см. раздел Добавление сетевых узлов (на стр. 139).

     В состав группы узлов защищенной сети вы также можете включить системные группы объектов **Все координаторы** и **Все клиенты** (см. «Системные группы объектов» на стр. 135).

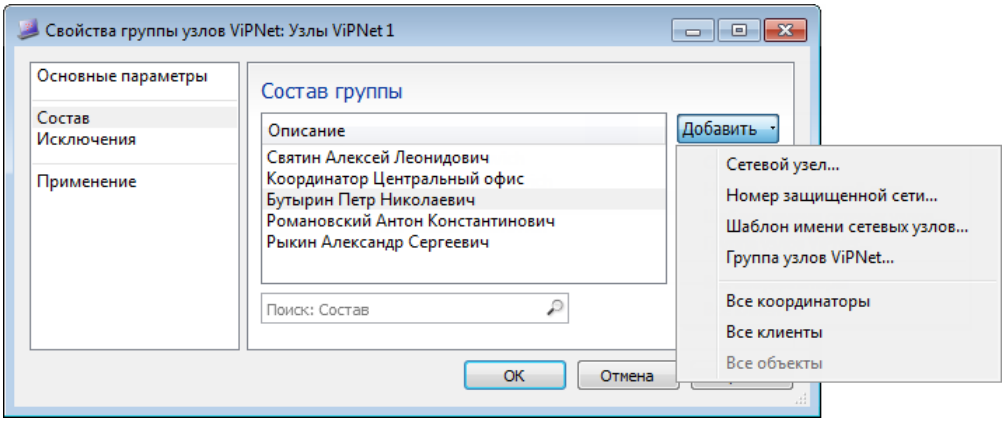



*Рисунок 55. Формирование состава группы узлов*

- **IP-адреса** — задайте отдельные IP-адреса, диапазон адресов или подсеть либо DNS-имена. Подробнее см. раздел Добавление IP-адресов и DNS-имен (на стр. 140).

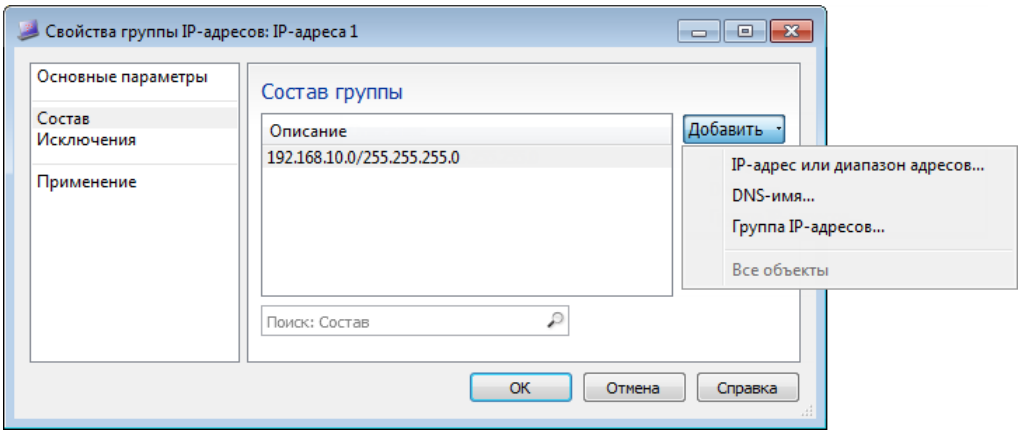



*Рисунок 56. Формирование состава группы IP-адресов*

- **Протоколы** — задайте протоколы и при необходимости номера портов. Подробнее см. раздел Добавление протоколов (на стр. 141).

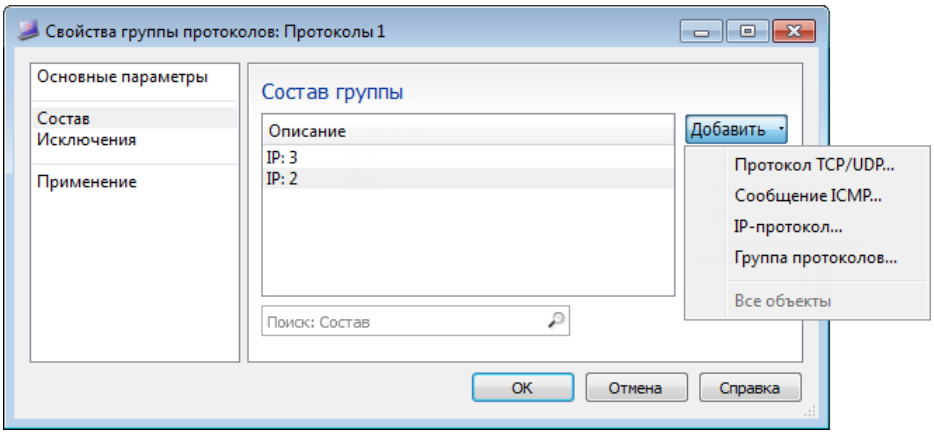



*Рисунок 57. Формирование состава группы протоколов*

- **Расписания** — задайте расписание, состоящее из дней недели или временных диапазонов. Впоследствии такие расписания можно использовать для ограничения времени действия сетевых фильтров. Подробнее см. раздел Добавление расписаний (на стр. 142).

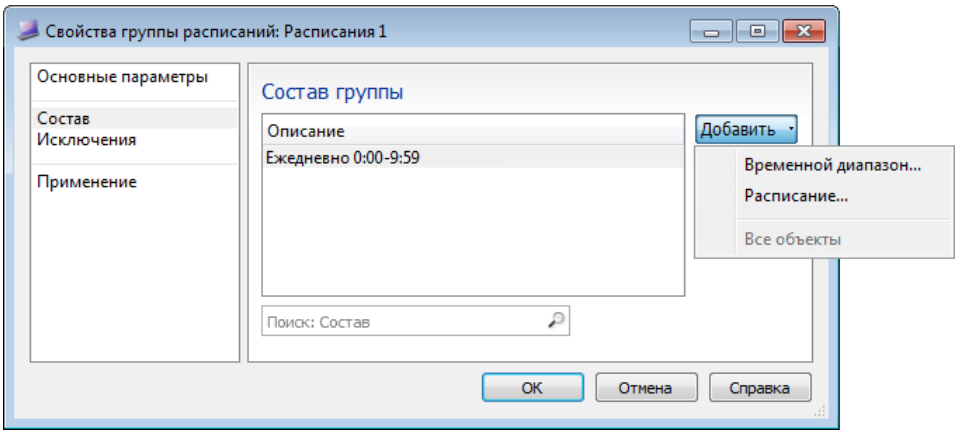



*Рисунок 58. Формирование состава группы расписаний*

---

**Примечание.** В каждую группу объектов могут входить группы объектов этого же типа, то есть можно организовать вложенность однотипных групп.

Кроме этого, в составе любой группы объектов вы можете задать системную группу **Все объекты**, например при создании группы, состоящей из всех объектов, кроме некоторых исключений.

---

6 В разделе **Исключения** задайте исключения из состава группы объектов, то есть те элементы, которые в группу объектов не должны входить. Например, чтобы создать группу защищенных узлов, состоящую из всех координаторов, кроме одного, добавьте в состав системную группу **Все координаторы**, а в качестве исключения задайте конкретный сетевой узел — координатор.

В качестве исключения можно задать также другую группу объектов такого же типа.

Формирование исключений осуществляется аналогично формированию состава групп объектов.

---

**Примечание.** В разделе **Применение** ничего задавать не требуется. В нем отображается список фильтров, в которых используется группа объектов. При создании группы объектов данный раздел пустой.

---

7 По завершении нажмите кнопку **OK**.

В результате в списке групп объектов выбранного типа появится новая группа.

Если при создании группы объектов не был определен ее состав, то такая группа будет считаться пустой. Пустые группы не рекомендуется использовать в сетевых фильтрах, поскольку фильтры в этом случае не будут применяться.

Чтобы изменить параметры группы объектов, выберите ее в соответствующем разделе групп объектов, затем дважды щелкните или нажмите кнопку **Свойства**. После изменения основных параметров группы или ее состава в окне свойств группы нажмите кнопку **OK**.

Чтобы удалить группу объектов, выберите ее в соответствующем разделе групп объектов и нажмите кнопку **Удалить**. В появившемся окне подтвердите удаление группы. Если удаляемая

группа объектов используется в каких-либо сетевых фильтрах либо входит в другие группы объектов, то появится сообщение об этом и она не будет удалена. В данном случае с помощью кнопки **Показать подробности** в окне сообщения просмотрите, в каких элементах используется данная группа, и повторите удаление, предварительно исключив группу из состава данных элементов.

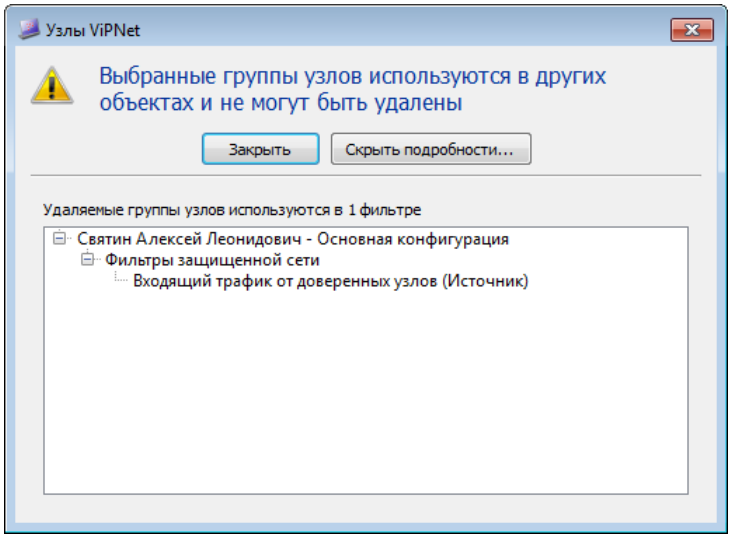



*Рисунок 59. Невозможность удаления группы объектов*

Чтобы новые или измененные группы объектов вступили в действие, в разделе групп объектов нажмите кнопку **Применить** и в течение 30 секунд подтвердите сохранение изменений. Если вы не хотите сохранять внесенные изменения в группы объектов, нажмите кнопку **Отмена**.

## Добавление сетевых узлов

Сетевые узлы могут быть добавлены в состав и исключения групп узлов, а также выбраны в качестве источника или назначения при создании фильтров защищенной сети следующим образом:

- При создании группы узлов или сетевых фильтров вы можете добавить выбранное множество сетевых узлов. Для этого в окне свойств группы узлов или сетевого фильтра в соответствующем разделе нажмите **Добавить** и в меню выберите **Сетевой узел**. После этого в появившемся окне выберите один или несколько узлов из списка и нажмите кнопку **ОК**.

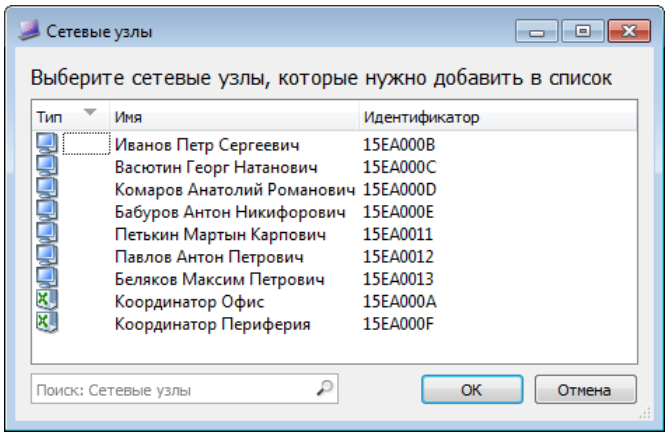



*Рисунок 60. Выборочное добавление сетевых узлов*

В результате будут добавлены выбранные узлы.

- При создании группы узлов вы можете добавить множество узлов определенной сети ViPNet. Для этого в нужных разделах окна свойств группы нажмите кнопку **Добавить** и в меню выберите **Номер защищенной сети**. В появившемся окне введите номер нужной сети.

  В результате будут добавлены все узлы из заданной сети.

- При создании группы узлов вы можете добавить множество узлов, имя которых соответствует заданной маске. Для этого в нужных разделах окна свойств группы нажмите кнопку **Добавить** и в меню выберите **Шаблон имени сетевых узлов**. В появившемся окне задайте маску имен узлов. Маска задается стандартным образом с использованием символов «*» и «?».

  В результате будут добавлены все узлы, имена которых соответствуют заданной маске.

## Добавление IP-адресов и DNS-имен

IP-адреса или DNS-имена могут быть добавлены в состав и исключения групп IP-адресов, а также заданы при определении источника и назначения в локальных фильтрах открытой сети.

Чтобы добавить IP-адреса в одном из указанных случаев:

1. В окне свойств группы IP-адресов или сетевого фильтра в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **IP-адрес или диапазон адресов**.
2. В появившемся окне выполните следующие действия:
   - Если требуется добавить один конкретный IP-адрес (в том случае, если он известен), установите переключатель в положение **IP-адрес** и в поле напротив введите данный IP-адрес.
   - Если требуется задать IP-адреса в рамках некоторой подсети, установите переключатель в положение **Подсеть**, после чего в соответствующих полях задайте адрес и маску данной подсети.
   - Если требуется задать диапазон IP-адресов, установите переключатель в положение **Диапазон IP-адресов**, после чего в соответствующих полях задайте начальный и конечный адрес диапазона.

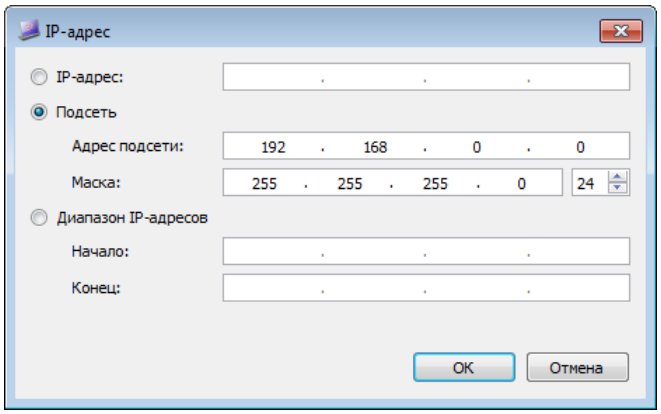



*Рисунок 61. Добавление IP-адресов*

После ввода необходимых данных нажмите кнопку **OK**.

В результате указанный IP-адрес или IP-адреса будут добавлены.

Чтобы добавить DNS-имя, в окне свойств группы IP-адресов или сетевого фильтра в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **DNS-имя**. В появившемся окне задайте DNS-имя и нажмите кнопку **OK**.

В результате DNS-имя будет добавлено.

## Добавление протоколов

Протоколы могут быть добавлены в состав и исключения групп протоколов, а также заданы при создании любых сетевых фильтров.

Чтобы добавить протоколы в одном из указанных случаев, в окне свойств группы протоколов или сетевого фильтра в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите:

- **Протокол TCP/UDP** — для добавления TCP- или UDP-протокола с номером порта источника и назначения. В появившемся окне выполните следующие действия:
  - В зависимости от того, какой протокол вам требуется добавить, установите переключатель **Протокол** в нужное положение.
  - Если требуется, задайте номера порта источника. Для этого выберите:
    - **Все порты** — для задания всех портов, например если вы не знаете конкретного номера.
    - **Номер порта** — для задания номера конкретного порта. В списке напротив выберите нужный номер.
    - **Диапазон** — для задания диапазона номеров портов. В полях напротив укажите начальный и конечный адреса диапазона.
  - При необходимости аналогичным образом задайте порт назначения.

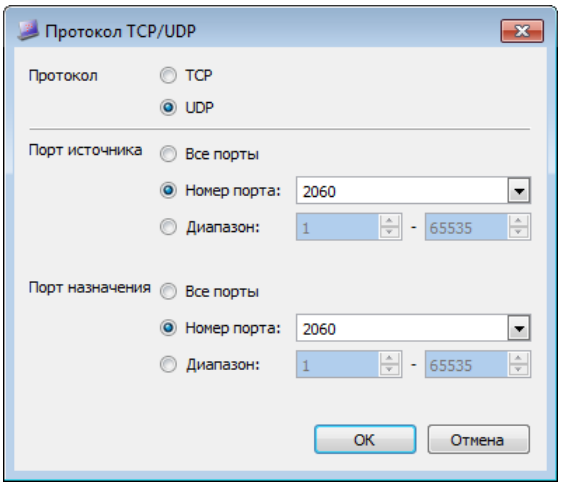



*Рисунок 62. Добавление TCP- или UDP-протокола*

По завершении ввода данных нажмите кнопку **OK**.

- **Сообщение ICMP** — для добавления ICMP-протокола. В появившемся окне в соответствующих списках выберите тип и код ICMP-протокола (если требуется) и нажмите кнопку **OK**.
- **IP-протокол** — для добавления других протоколов. В появившемся окне в списке выберите нужный протокол либо введите код протокола (если он известен) и нажмите кнопку **OK**.

## Добавление расписаний

Расписания действия сетевых фильтров могут быть добавлены в состав и исключения групп расписаний, а также заданы при создании любых сетевых фильтров (если требуется, чтобы фильтр действовал в конкретное время или в определенные промежутки времени).

Чтобы добавить расписание в одном из указанных случаев, выполните следующие действия:

1. В окне свойств группы расписаний или сетевого фильтра в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **Временной диапазон**.
2. В появившемся окне задайте параметры расписания:
   - В группе **Время выполнения фильтра** укажите временной интервал, в течение которого будет действовать сетевой фильтр.
   - Установите переключатель в положение:
     - **Ежедневно**, если сетевой фильтр должен действовать каждый день в указанное время. Если требуется, чтобы фильтр действовал в некоторый период времени (например, в течение двух недель), установите соответствующий флажок и задайте нужный период.
     - **Еженедельно**, если сетевой фильтр должен действовать в определенные дни недели. Установите флажки напротив нужных дней недели.

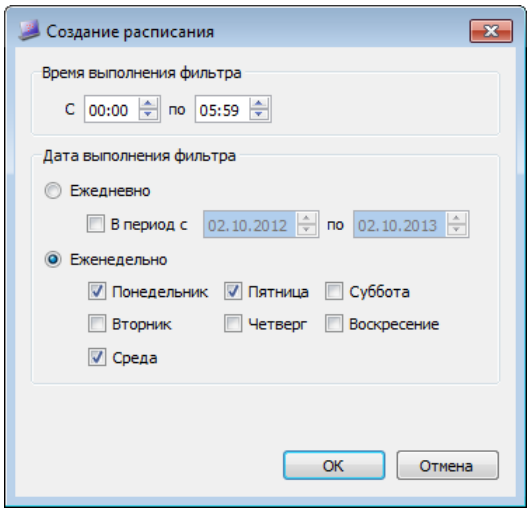



*Рисунок 63. Добавление расписания*

3 По завершении ввода данных нажмите кнопку **OK**.

В результате будет добавлено расписание с заданными параметрами.

# Создание сетевых фильтров

В программе ViPNet Client предусмотрена возможность создания следующих фильтров:

- фильтров для защищенной сети,
- фильтров для открытой сети.

Для создания любого из перечисленных фильтров выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел того типа фильтров, который вы хотите создать.

2 На панели просмотра нажмите кнопку **Создать**. Откроется окно свойств сетевого фильтра, в котором вы можете задать параметры нового фильтра.

3 В разделе **Основные параметры** выполните следующие действия:

   - Введите имя фильтра в соответствующем поле.
   - Укажите действие нового фильтра (блокировать или пропускать трафик), установив переключатель **Действие** в нужное положение. По умолчанию выбрано действие **Блокировать трафик**.

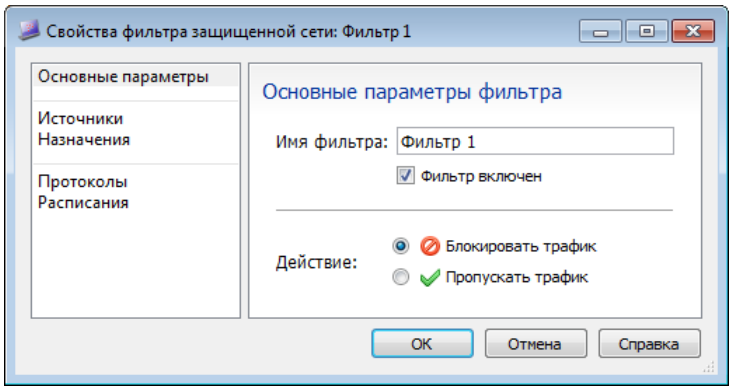



*Рисунок 64. Задание основных параметров фильтра*

4 В разделе **Источники** задайте отправителя IP-пакетов, на которые будет распространяться действие фильтра.

5 В разделе **Назначения** задайте получателя IP-пакетов, на которые будет распространяться действие фильтра.

6 В разделе **Протоколы** укажите протокол для фильтрации. Фильтром в данном случае будут обрабатываться только IP-пакеты, переданные с помощью указанного протокола. Вы можете добавить нужный протокол (см. «Добавление протоколов» на стр. 141) или сразу группу протоколов.

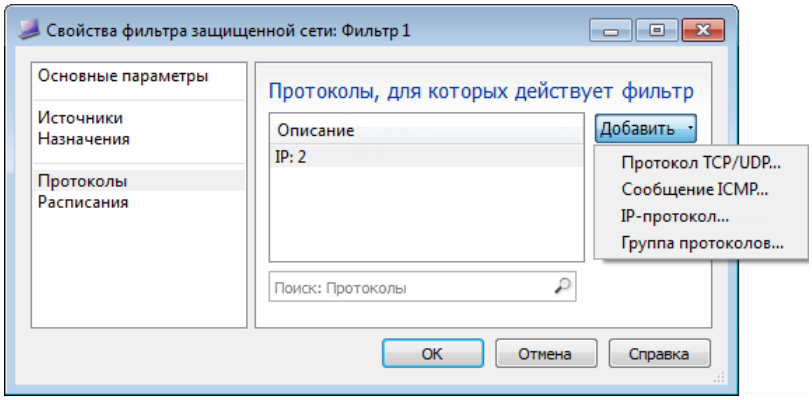



*Рисунок 65. Добавление протоколов при создании фильтра*

7 В разделе **Расписания** укажите расписание действия фильтра, если требуется. Вы можете добавить новое расписание (см. «Добавление расписаний» на стр. 142) или группу расписаний.

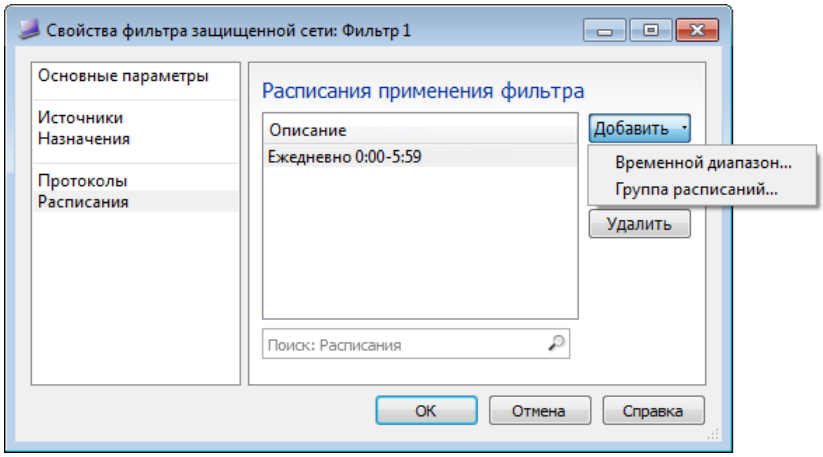



*Рисунок 66. Добавление расписания при создании фильтра*

8 Для сохранения параметров нового фильтра нажмите кнопку **OK**. В результате в списке на панели просмотра появится новый фильтр.

Созданный фильтр будет включен, если при задании его основных параметров не был снят соответствующий флажок. Если потребуется отключить фильтр, снимите флажок слева от его имени.

9 Задайте приоритет созданного фильтра, установив его положение в списке с помощью кнопок  и  .

10 Чтобы созданный фильтр вступил в действие, по завершении всех операций с ним нажмите кнопку **Применить** и в появившемся окне в течение 30 секунд подтвердите сохранение изменений.

---

**Примечание.** Для гарантированного применения фильтров, блокирующих трафик, также требуется перезагрузить компьютер.

---

Подробнее о создании каждого типа фильтров см. соответствующие разделы ниже.

# Создание фильтров для защищенной сети

Чтобы создать фильтр для защищенного трафика (см. «Общие сведения о сетевых фильтрах» на стр. 129), выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Фильтры защищенной сети**.

2 На панели просмотра нажмите кнопку **Создать**, после чего в появившемся окне задайте параметры нового фильтра защищенного трафика.

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик (см. Рисунок 56 на стр. 144).

4 В разделе **Источники** задайте отправителя защищенных IP-пакетов. Для этого добавьте:

- Один или несколько узлов защищенной сети (см. «Добавление сетевых узлов» на стр. 139).
- Одну или несколько групп узлов сети ViPNet, если такие созданы (см. «Создание и изменение групп объектов» на стр. 136).
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для исходящих соединений вашего сетевого узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для входящих соединений вашего сетевого узла.
- Системные группы объектов **Все координаторы** и **Все клиенты** (см. «Системные группы объектов» на стр. 135).

Если вы не укажете отправителя, то действие фильтра будет распространяться на IP-пакеты, отправленные любыми защищенными узлами, и вашим в том числе.

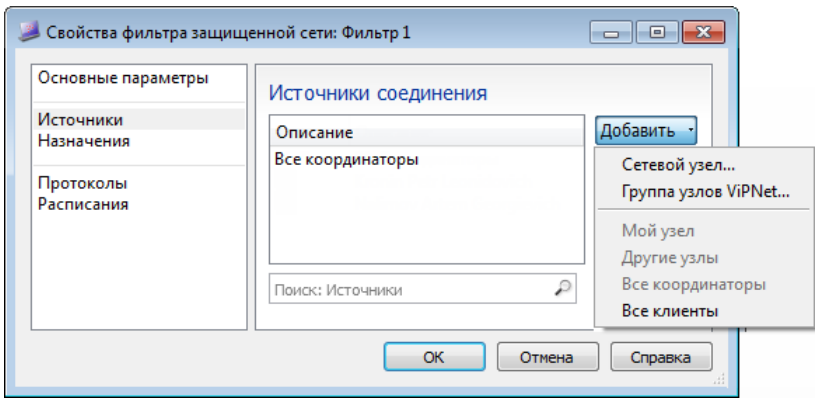



*Рисунок 67. Задание отправителя защищенных IP-пакетов*

5 В разделе **Назначения** задайте получателя защищенных IP-пакетов. Для этого добавьте:

- Один или несколько узлов защищенной сети (см. «Добавление сетевых узлов» на стр. 139).

- Одну или несколько групп узлов сети ViPNet, если такие созданы (см. «Создание и изменение групп объектов» на стр. 136).
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для входящих соединений вашего сетевого узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для исходящих соединений вашего сетевого узла.
- Системные группы объектов **Все координаторы** и **Все клиенты** (см. «Системные группы объектов» на стр. 135).
- Системную группу объектов **Широковещательные адреса**. В этом случае действие фильтра будет распространяться на широковещательные пакеты.

  Если в качестве получателя указать **Широковещательные адреса**, в качестве отправителя — **Мой узел** или **Другие узлы** (см. пункт выше), то будут созданы фильтры для исходящих или входящих широковещательных IP-пакетов соответственно.

Если вы не укажете узел назначения, то действие фильтра будет распространяться на IP-пакеты, отправленные на любой узел сети, и ваш узел в том числе.

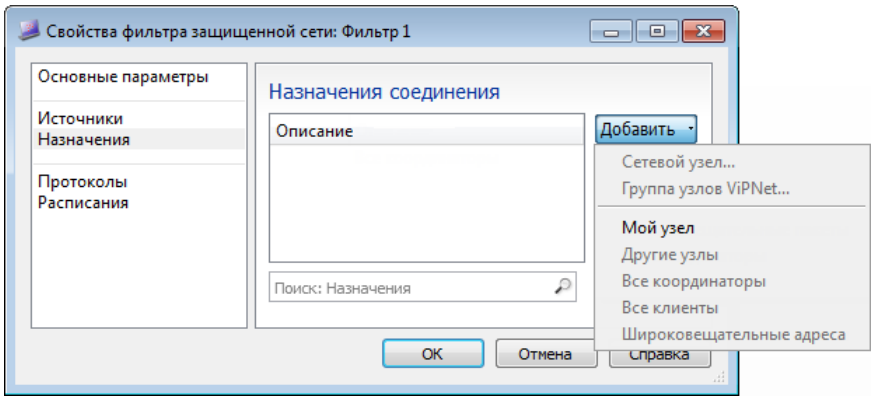



*Рисунок 68. Задание получателя защищенных IP-пакетов*

6 В разделе **Протоколы** укажите протокол для фильтрации.

7 В разделе **Расписания** укажите расписание действия фильтра.

8 Нажмите кнопку **OK**. В результате в списке на панели просмотра появится новый фильтр.

# Создание фильтров для открытой сети

Чтобы создать фильтр для локального открытого трафика (см. «Общие сведения о сетевых фильтрах» на стр. 129), выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Фильтры открытой сети**.

2 На панели просмотра нажмите кнопку **Создать**, после чего в появившемся окне задайте параметры нового фильтра открытого трафика.

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик (см. Рисунок 56 на стр. 144).

4 В разделе **Источники** задайте отправителя открытых IP-пакетов. Для этого добавьте:

- IP-адрес или DNS-имя отправителя либо диапазон адресов, если их несколько (см. «Добавление IP-адресов и DNS-имен» на стр. 140).
- Группы IP-адресов отправителей, если такие созданы (см. «Создание и изменение групп объектов» на стр. 136).
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для исходящих открытых соединений вашего узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для входящих открытых соединений вашего узла.

Если вы не укажете отправителя, то действие фильтра будет распространяться на IP-пакеты, отправленные любыми открытыми узлами, и вашим узлом в том числе.

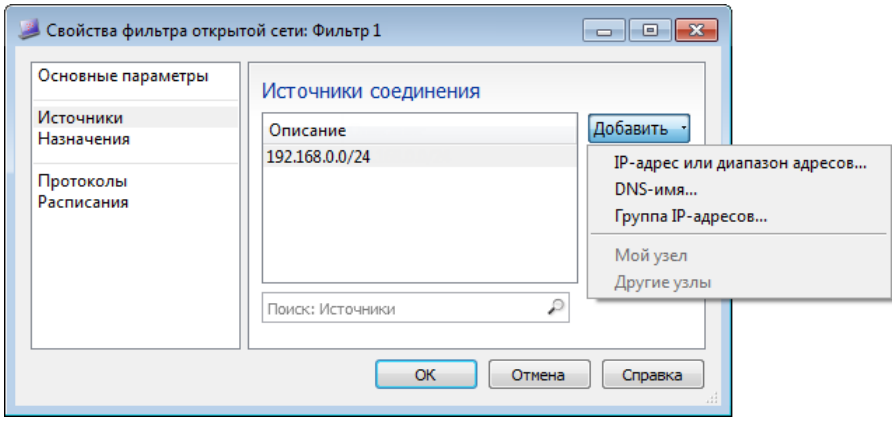



*Рисунок 69. Указание источника отправки IP-пакетов в открытой сети*

5 В разделе **Назначения** задайте получателя открытых IP-пакетов. Для этого добавьте:

- IP-адрес или DNS-имя получателя либо диапазон адресов, если их несколько.
- Группы IP-адресов получателей, если такие созданы.
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для входящих открытых соединений вашего узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для исходящих открытых соединений вашего узла.
- Широковещательные адреса, выбрав системную группу объектов **Широковещательные адреса**. В этом случае действие фильтра будет распространяться на широковещательные пакеты.
- Системную группу объектов **Групповые адреса**. В этом случае действие фильтра будет распространяться на пакеты, отправленные по групповой рассылке.

Если вы не укажете получателя, то действие фильтра будет распространяться на IP-пакеты, отправленные на любой открытый узел.

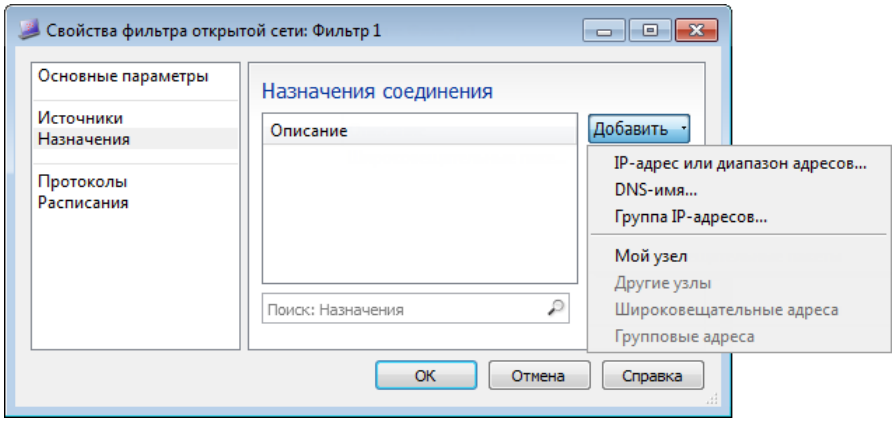



*Рисунок 70. Указание получателя IP-пакетов в открытой сети*

6 В разделе **Протоколы** укажите протокол для фильтрации.

7 В разделе **Расписания** укажите расписание действия фильтра.

8 Нажмите кнопку **OK**. В результате в списке на панели просмотра появится новый фильтр.

# Рекомендации по созданию сетевых фильтров

Чтобы обеспечить стабильную работу программы ViPNet Монитор, необходимо контролировать число создаваемых фильтров, потому что оно зависит от количества узлов, на которые будет распространяться действие каждого из фильтров.  Мы рекомендуем придерживаться следующих ограничений:

- Если действие каждого из создаваемых фильтров распространяется на один сетевой узел или IP-адрес, общее количество фильтров не должно превышать 3000.
- Если действие каждого из создаваемых фильтров распространяется на два или большее количество сетевых узлов или IP-адресов, общее количество сетевых узлов или IP-адресов, на которые будут распространяться действия всех созданных фильтров, не должно превышать 700. При этом действие одного фильтра не должно распространяться более чем на 500 сетевых узлов или IP-адресов.

# Восстановление предустановленных фильтров и групп объектов

Если вы создали неудачный список сетевых фильтров, то вы можете восстановить предустановленные фильтры. В этом случае списки настроенных фильтров всех типов будут заменены на предустановленные. Вместе с фильтрами также будут восстановлены предустановленные группы объектов.

Для восстановления предустановленных фильтров и групп объектов выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры**.
2. На панели просмотра нажмите кнопку **Восстановить фильтры по умолчанию**.
3. В появившемся окне **Сброс фильтров** нажмите кнопку **Да**.

   В результате во всех разделах сетевых фильтров в группе **Настраиваемые фильтры** будут присутствовать только предустановленные фильтры, в разделе **Группы объектов** — только предустановленные группы.

# Практический пример использования групп объектов и сетевых фильтров

Рассмотрим следующий пример использования групп объектов и сетевых фильтров. Допустим, в организации развернут почтовый сервер, на котором установлена программа ViPNet Монитор. Этот защищенный почтовый сервер выполняет следующие функции:

- Обмен сообщениями электронной почты с внешними почтовыми серверами;
- Передача сообщений электронной почты, отправленных удаленными сотрудниками или адресованных им.

Отправка сообщений на почтовый сервер внешними почтовыми серверами и пользователями осуществляется по протоколу SMTP. Передача сообщений электронной почты пользователям производится по протоколам POP3 и IMAP.

Чтобы организовать обмен сообщениями с внешними почтовыми серверами и пользователями и доступ пользователей к электронной почте из Интернета, на защищенном почтовом сервере необходимо создать сетевой фильтр, разрешающий прием и передачу IP-пакетов по 25-му порту протокола TCP (стандартный порт для протокола SMTP), а также по 110-му и 143-му порту (для протоколов POP3 и IMAP соответственно).

Вы можете создать группу протоколов, в которую будут входить все указанные выше протоколы. Данную группу вы сможете использовать при создании сетевого фильтра. Кроме этого, вы сможете использовать ее повторно в дополнительных фильтрах для почтового сервера, если такие в дальнейшем потребуется создать.

Чтобы создать группу протоколов, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Группы объектов** > **Протоколы**.
2. На панели просмотра нажмите кнопку **Создать** и в окне свойств создаваемой группы в разделе **Состав** добавьте все нужные протоколы.
3. Для добавления протокола SMTP в меню кнопки **Добавить** выберите пункт **Протокол TCP/UDP**, после чего в появившемся окне укажите:
   - в качестве протокола — **TCP**;
   - в качестве порта источника — **Все порты**;
   - в качестве порта назначения — номер порта **25-smtp**.

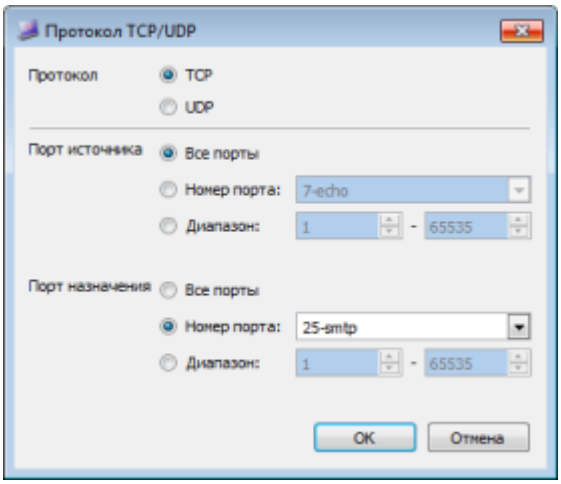



*Рисунок 71. Пример добавления протокола SMTP в группу*

4 Аналогичным образом добавьте протоколы POP3 и IMAP, указав вместо порта назначения номер порта 110 и 143 соответственно.

5 По завершении добавления протоколов в окне свойств группы нажмите кнопку **OK**.

В результате будет создана группа протоколов. Используйте данную группу при создании фильтра.

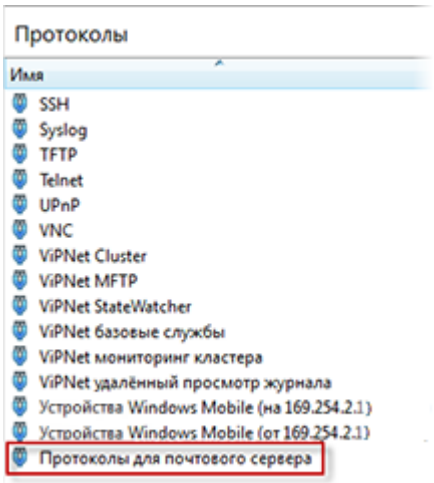



*Рисунок 72. Результат создания группы протоколов для почтового сервера*

Чтобы создать сетевой фильтр для обмена почтовыми сообщениями с внешними серверами и пользователями, на защищенном почтовом сервере выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Фильтры открытой сети**.

2 В разделе **Фильтры открытой сети** создайте сетевой фильтр для всех IP-адресов, так как IP-адреса внешних почтовых серверов заранее неизвестны и создаваемый фильтр должен распространяться на IP-адреса всех пользователей. Для этого на панели просмотра нажмите кнопку **Создать** и в появившемся окне свойств создаваемого фильтра задайте его параметры.

3 В разделе **Основные параметры** установите переключатель **Действие** в положение **Пропускать трафик**.

4 Чтобы действие фильтра распространялось на все IP-адреса, в разделах **Источники** и **Назначения** не задавайте отправителей и получателей соответственно.

5 В разделе **Протоколы** в меню кнопки **Добавить** выберите пункт **Группа протоколов**, после чего в появившемся окне выберите группу протоколов, которая была создана предварительно.

6 Расписание для данного фильтра формировать не следует.

7 Нажмите кнопку **OK**.

В результате будет создан сетевой фильтр.

Таким образом, на защищенном почтовом сервере будет разрешен обмен сообщениями с внешними серверами и сотрудниками организации и доступ сотрудников к электронной почте.

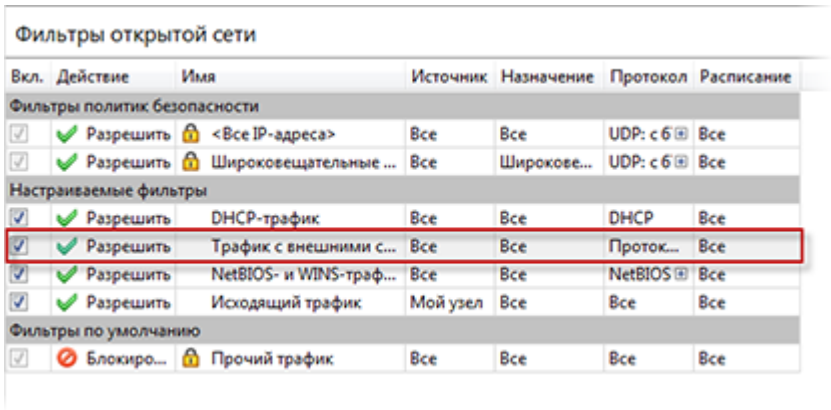



*Рисунок 73. Результат создания разрешающего фильтра для протоколов SMTP, POP3, IMAP*

# Блокировка IP-трафика

С помощью программы ViPNet Монитор вы можете заблокировать весь IP-трафик компьютера. В этом случае любые соединения с защищенными и открытыми узлами будут запрещены.

Чтобы заблокировать IP-трафик, выполните следующие действия:

1. В программе ViPNet Монитор включите блокировку одним из следующих способов:
   - В меню **Файл** выберите пункт **Конфигурации** > **Блокировать IP-трафик**.
   - На панели задач щелкните правой кнопкой мыши значок программы и в меню выберите пункт **Блокировать IP-трафик**.
2. Если вы хотите, чтобы после блокировки трафика при определенных условиях трафик был автоматически разблокирован, в окне **Блокирование IP-трафика**:
   - Установите флажок **Разрешить IP-трафик автоматически**.
   - Из списка под флажком выберите условие для автоматической разблокировки IP-трафика: после перезагрузки компьютера или по истечении определенного промежутка времени.

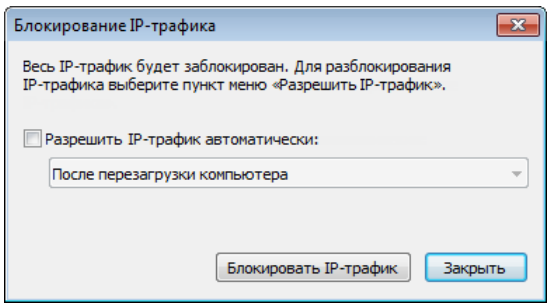



*Рисунок 74. Включение блокировки IP-трафика*

3. Нажмите кнопку **Блокировать IP-трафик**. Весь открытый и защищенный трафик компьютера будет заблокирован, значок программы ViPNet Монитор в области уведомлений примет следующий вид .
4. Чтобы снять блокировку IP-трафика, в меню **Файл** выберите пункт **Конфигурации** > **Разрешить IP-трафик**.

# Отключение защиты трафика

При необходимости вы можете отключить защиту трафика с помощью программного обеспечения ViPNet Client. В этом случае будет прекращена любая обработка трафика и ведение журнала регистрации IP-пакетов. Соединение с защищенными узлами ViPNet будет невозможно. Также будет невозможно запустить программу ViPNet SafeDisk-V, если вы используете ее совместно с программой ViPNet Client.

---

**Внимание!** Не следует работать на сетевом узле с отключенной защитой трафика, так как в этом случае компьютер не защищен от попыток несанкционированного доступа из сети.

---

Чтобы отключить защиту трафика, выполните следующие действия:

1. В программе ViPNet Монитор в меню **Файл** выберите пункт **Конфигурации** > **Отключить защиту**.
2. Если вы хотите, чтобы после отключения защиты трафика при определенных условиях защита была автоматически включена, в окне **Отключение защиты**:
   - Установите флажок **Включить защиту IP-трафика автоматически**.
   - Из списка под флажком выберите условие для автоматического включения защиты трафика: после перезагрузки компьютера или по истечении определенного промежутка времени.

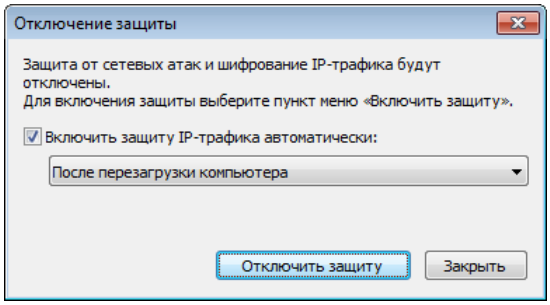



*Рисунок 75. Отключение защиты трафика*

3. Нажмите кнопку **Отключить защиту**. Защита трафика будет отключена, значок программы ViPNet Монитор в области уведомлений примет следующий вид .
4. Чтобы включить защиту трафика, в меню **Файл** выберите пункт **Конфигурации** > **Включить защиту**.

# 8

# Обработка прикладных протоколов


Общие сведения о прикладных протоколах 157

Описание прикладных протоколов 159

Настройка параметров обработки прикладных протоколов 160

# Общие сведения о прикладных протоколах

Функционирование сетевых сервисов, например таких как, IP-телефония, DNS-служба, FTP-служба, обеспечивается прикладными протоколами. При использовании прикладных протоколов IP-адреса часто передаются в теле IP-пакета. Поведение подобного рода может привести к отсутствию сервиса на защищаемых ресурсах в случае использования технологии виртуальных IP-адресов. Кроме того, некоторые протоколы, помимо основного (управляющего) соединения, открывают для передачи данных дополнительные соединения на случайно выбранный порт. Для IP-пакетов, следующих на порт назначения, номер которого заранее не известен, невозможно создать разрешающий фильтр, следовательно, соединение будет заблокировано.

Решить перечисленные проблемы позволяет функция обработки прикладных протоколов, которая обеспечивает:

- Подмену виртуального IP-адреса в теле пакета на реальный IP-адрес в случае использования технологии виртуальных IP-адресов.
- Активацию разрешающего сетевого фильтра для дополнительного соединения на случайно выбранный порт, открываемый прикладным протоколом.

---

**Примечание.** В программе ViPNet Монитор обработка прикладных протоколов осуществляется для открытого и защищенного трафика.

---

Следует учитывать, что обработка прикладных протоколов не предполагает автоматического разрешения на установление управляющего соединения с открытыми узлами. Установление управляющего соединения с открытыми узлами осуществляется в соответствии с настроенными фильтрами трафика (см. «Общие сведения о сетевых фильтрах» на стр. 129).

Рассмотрим обработку прикладного протокола на примере протокола FTP.

При передаче файлов между FTP-клиентом и FTP-сервером протокол регламентирует установление двух TCP-соединений: управляющее соединение (для отправки команд FTP-серверу и получения ответов от него) и дополнительное соединение (для передачи данных). Соединение клиента с сервером осуществляется в одном из двух режимов: активном и пассивном. В активном режиме клиент инициирует управляющее соединение с порта из диапазона 1024–65535 на порт с номером 21 на сервере. По номеру порта, с которого клиент инициировал соединение, сервер подключается к клиенту и устанавливает соединение для передачи данных. При этом со стороны сервера соединение происходит через порт с номером 20. В пассивном режиме после установления управляющего соединения сервер сообщает клиенту случайно выбранный номер порта из диапазона 1024–65535, к которому можно подключиться при установлении соединения для передачи данных. Таким образом, в активном режиме клиент должен принять соединение для передачи данных от сервера, в пассивном режиме соединение для передачи данных всегда инициирует клиент.

Для установления управляющего и дополнительного соединений в активном или пассивном режиме работы протокола FTP в программе ViPNet Монитор выполните следующие настройки:

- Если действуют предустановленные фильтры открытой сети, которые разрешают любые исходящие соединения, то для разрешения исходящего управляющего соединения дополнительные настройки не требуются.

  Если фильтры открытой сети не разрешают исходящие соединения, то в таком случае создайте фильтр открытой сети (см. «Создание фильтров для открытой сети» на стр. 147), разрешающий исходящее соединение по протоколу TCP на 21 порт FTP-сервера.

- Для разрешения дополнительного соединения в активном режиме работы должна быть включена обработка протокола FTP, которая активирует необходимый фильтр трафика. Убедитесь, что она включена.

- Для разрешения дополнительного соединения в пассивном режиме работы специальные настройки не требуются.

Рассмотрим еще один пример — обработку прикладного протокола на примере протокола SIP.

Протокол SIP предназначен для организации, модификации и завершения сеансов связи — мультимедийных конференций, телефонных соединений — и распределения мультимедийной информации.

Вызывающий SIP-клиент отправляет запрос (например, приглашение к сеансу связи, подтверждение приема ответа на запрос, завершение сеанса связи) вызываемому SIP-клиенту с указанием его SIP-адреса. В зависимости от способа установления соединения запрос направляется вызываемому клиенту либо напрямую, либо с участием прокси-сервера SIP, либо с участием сервера переадресации. Вызываемый клиент в зависимости от типа полученного запроса передает вызывающему клиенту ответ на запрос (например, информацию об ошибке при обработке запроса, запрос успешно обработан, отклонение входящего вызова).

Для установления сеанса связи между SIP-клиентами протокол SIP регламентирует установление соединений TCP и UDP через порт 5060.

Чтобы установить сеанс связи между SIP-клиентами, убедитесь, что включена обработка протокола SIP, и выполните дополнительные настройки в программе ViPNet Монитор:

1. Чтобы SIP-клиент мог принять запрос на установление сеанса связи или принять ответ на запрос, создайте фильтр открытой сети, разрешающий входящее соединение по протоколам TCP и UDP на порт 5060.
2. Чтобы SIP-клиент мог отправить запрос на установление сеанса связи или ответ на запрос:
   - Если действуют предустановленные фильтры открытой сети, которые разрешают любые исходящие соединения, настройка дополнительных фильтров не требуется.
   - Если фильтры открытой сети не разрешают любые исходящие соединения, создайте фильтр открытой сети, разрешающий исходящее соединение по протоколам TCP и UDP на порт 5060.

# Описание прикладных протоколов

**Примечание.** В программе ViPNet Монитор версии 3.2 и выше удалена веб-фильтрация и обработка прикладного протокола HTTP.

В программе ViPNet Монитор реализована возможность настройки параметров обработки следующих прикладных протоколов:

- Протокол FTP обеспечивает передачу файлов между FTP-клиентом и FTP-сервером.
- Протокол DNS (Domain Name System) обеспечивает разрешение DNS-имен сетевых узлов в IP-адреса.
- Протокол H.323 обеспечивает работу программ для проведения мультимедийных конференций через IP-сети, в том числе Интернет.
- Протокол SCCP (Skinny Client Control Protocol) обеспечивает передачу сообщений между Skinny-клиентами (проводными и беспроводными IP-телефонами Cisco) и сервером голосовой почты Cisco Unity и Cisco CallManager.
- Протокол SIP (Session Initiation Protocol) обеспечивает установление сеансов связи при передаче голосовых звонков, видеоконференций, а также мультимедийной информации.

**Примечание.** Список поддерживаемых программой ViPNet Монитор прикладных протоколов задан по умолчанию, нельзя добавить протоколы или удалить протоколы из списка.

# Настройка параметров обработки прикладных протоколов

**Внимание!** В сетях, где используется обработка прикладных протоколов средствами ViPNet, на сетевом оборудовании (маршрутизаторах, шлюзах) необходимо отключить функцию DPI (deep packet inspection — глубокий анализ пакетов). Применение DPI может привести к сбоям в работе приложений, использующих протоколы FTP, DNS, H.323, SCCP, SIP.

Чтобы настроить параметры обработки прикладных протоколов для открытого и защищенного трафика, выполните следующие действия:

1 В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2 На панели навигации окна **Настройка** выберите раздел **Прикладные протоколы**.

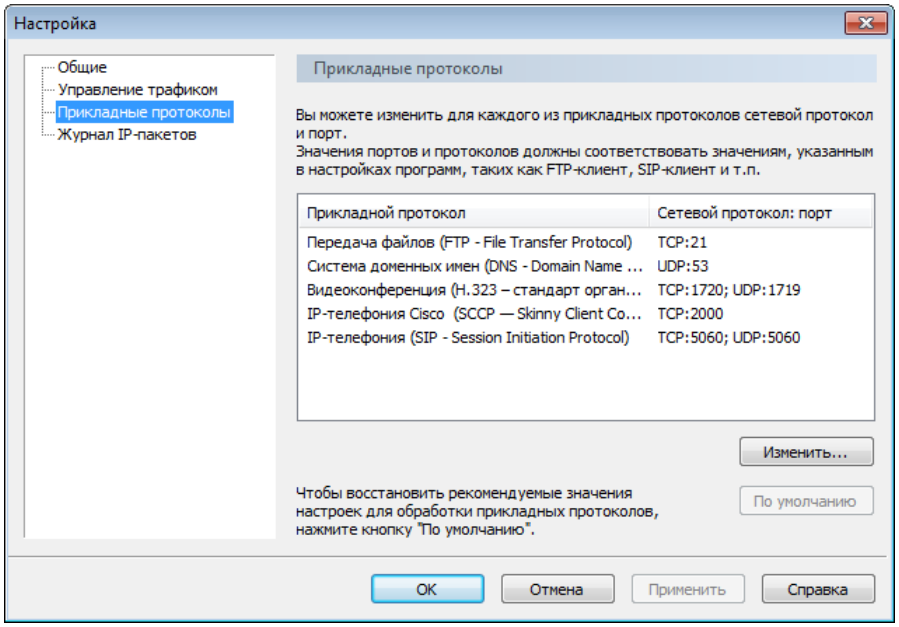



*Рисунок 76. Раздел «Прикладные протоколы»*

В разделе **Прикладные протоколы** приведен список поддерживаемых программой прикладных протоколов (см. «Описание прикладных протоколов» на стр. 159).

**Примечание.** По умолчанию для всех прикладных протоколов заданы наиболее часто используемые сетевые протоколы и порты.

Список поддерживаемых программой ViPNet Монитор прикладных протоколов задан по умолчанию, нельзя добавить протоколы или удалить протоколы из списка.

3 В разделе **Прикладные протоколы** выберите протокол, параметры обработки которого требуется отредактировать, затем нажмите кнопку **Изменить**.

4 Если требуется, в окне **Настройка прикладного протокола: <название прикладного протокола>** выполните следующие действия:

- Чтобы включить сетевой протокол, установите соответствующий флажок и задайте порты.

**Примечание.** Заданные параметры обработки прикладных протоколов должны соответствовать параметрам, указанным в настройках различных приложений, таких как FTP-клиент, DNS-клиент, SIP-клиент и других.

При вводе номеров портов, диапазонов номеров портов их необходимо разделять запятыми.

- Чтобы отключить сетевой протокол, снимите соответствующий флажок.
- Чтобы отключить обработку прикладного протокола:
  - Отключите все сетевые протоколы.
  - В окне предупреждения нажмите кнопку **OK**.

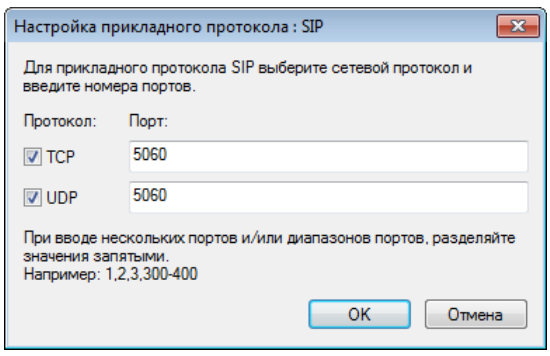



*Рисунок 77. Настройка параметров обработки прикладного протокола*

По окончании настройки нажмите кнопку **OK**.

**Внимание!** Не рекомендуется отключать обработку прикладных протоколов, в противном случае работа прикладных программ может быть затруднена.

5 Чтобы сохранить настройки, в окне **Настройка** нажмите кнопку **Применить**.

6 Чтобы восстановить настройки по умолчанию, в разделе **Прикладные протоколы** нажмите кнопку **По умолчанию**.

# 9

# Интеграция с программой ViPNet SafeDisk-V


Общие сведения о программе ViPNet SafeDisk-V 163

Обеспечение интеграции ViPNet Client с ViPNet SafeDisk-V: порядок действий 165

Работа с интегрированной программой ViPNet SafeDisk-V 167

# Общие сведения о программе ViPNet SafeDisk-V

Программа ViPNet SafeDisk-V предназначена для защиты конфиденциальной информации, которая хранится на диске или съемном носителе.

Информация, которую требуется защитить, помещается в контейнер SafeDisk-V (см. «Файл контейнера» на стр. 404). Контейнер представляет собой зашифрованный файл. При подключении контейнера в программе ViPNet SafeDisk-V он отображается как логический диск в операционной системе.

Данные, которые записываются в подключенный контейнер, автоматически зашифровываются и также автоматически расшифровываются в процессе чтения. Шифрование осуществляется незаметно для пользователя, не требуя от него никаких дополнительных действий.

При отключении контейнер перестает отображаться в системе, и установить сам факт наличия конфиденциальной информации и получить к ней доступ невозможно.

Программа ViPNet SafeDisk-V, интегрированная с ViPNet Client, имеет по сравнению с программой ViPNet SafeDisk следующие преимущества:

- Доступ к защищенной информации, хранящейся в контейнерах SafeDisk-V, имеет только пользователь программы ViPNet Client. При работе с контейнерами обеспечивается дополнительная защита средствами ViPNet Client (см. «Работа с интегрированной программой ViPNet SafeDisk-V» на стр. 167).
- Ключи контейнеров SafeDisk-V не надо обновлять самостоятельно. Обновление ключей контейнеров поступает в составе ключей узла и ключей пользователя, которыми они защищены.

---

**Примечание.** Во время работы с защищенными контейнерами SafeDisk-V независимо от выбранного режима установки обновлений (см. «Автоматическая установка обновлений» на стр. 85) поступающие обновления можно установить только вручную.

---

- При работе с контейнерами SafeDisk-V в программе ViPNet Монитор действуют специальные фильтры, ограничивающие защищенные и открытые соединения сетевого узла. Данные фильтры формируются при запуске программы ViPNet SafeDisk-V, имеют наиболее высокий приоритет и не отображаются в интерфейсе программы ViPNet Client (см. Работа с интегрированной программой ViPNet SafeDisk-V (на стр. 167)). Кроме того, для обеспечения дополнительной безопасности на время работы с контейнерами в программе ViPNet Монитор блокируются возможности переключения в конфигурацию «Открытый Интернет» или «Интернет», смены пользователя и выхода из программы.

Подробная информация о программе ViPNet SafeDisk-V содержится в документе «ViPNet SafeDisk-V. Руководство пользователя».

# Обеспечение интеграции ViPNet Client с ViPNet SafeDisk-V: порядок действий

**Внимание!** ПО ViPNet Client версий 4.x может быть интегрировано только с версией ViPNet SafeDisk-V 4.2.

Для того чтобы использовать программу ViPNet SafeDisk-V совместно с программой ViPNet Client, необходимо выполнить действия из приведенного ниже списка.

*Таблица 5. Порядок действий при интеграции ПО ViPNet Client с ViPNet SafeDisk-V*

| | Действие | Ссылка |
|---|---|---|
| ☐ | Администратору сети ViPNet следует:<br>• В сети ViPNet, управляемой с помощью программы ViPNet Administrator, — в программе ViPNet Центр управления сетью добавить на сетевой узел роль «SafeDisk».<br>• В сети ViPNet, управляемой с помощью ПО ViPNet Network Manager, — в программе ViPNet Network Manager выбрать сетевой узел и на вкладке **Ключи** установить флажок **Использовать SafeDisk-V**. | «ViPNet Administrator Центр управления сетью. Руководство администратора»<br>«ViPNet VPN. Руководство пользователя» |
| ☐ | Администратору сети ViPNet следует:<br>• В сети ViPNet, управляемой с помощью программы ViPNet Administrator, — при создании нового сетевого узла в программе ViPNet Удостоверяющий и ключевой центр сформировать дистрибутив ключей и установить его на узле. Для созданного ранее сетевого узла в программе ViPNet Центр управления сетью сформировать справочники и отправить их на узел.<br>• В сети ViPNet, управляемой с помощью ПО ViPNet Network Manager, — в программе ViPNet Network Manager отправить на сетевой узел ключи или сохранить ключи в файл и установить их на узле вручную. | «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора»<br>«ViPNet Administrator Центр управления сетью. Руководство администратора»<br>«ViPNet VPN. Руководство пользователя» |

| | Действие | Ссылка |
|---|---|---|
| ☐ | Пользователю, обладающему правами администратора в ОС Windows, следует установить на сетевой узел программу ViPNet SafeDisk-V. | «ViPNet SafeDisk-V. Руководство пользователя» |
| ☐ | Ознакомиться с принципом взаимодействия программ ViPNet Client и ViPNet SafeDisk-V. | Работа с интегрированной программой ViPNet SafeDisk-V (на стр. 167) |
| ☐ | Удостовериться, что ViPNet Client не находится в конфигурации «Открытый Интернет» или «Интернет» и что защита IP-трафика включена. При работе в данных конфигурациях или при отключенной защите IP-трафика программа ViPNet SafeDisk-V не может быть запущена. | Управление конфигурациями программы (на стр. 206)<br>Отключение защиты трафика (на стр. 155) |

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

# Работа с интегрированной программой ViPNet SafeDisk-V

Если выполнены все условия совместной работы программы ViPNet Client и ViPNet SafeDisk-V:

- Запустите программу ViPNet Монитор, после чего запустите программу ViPNet SafeDisk-V.

  Если программа ViPNet Монитор не будет запущена, либо будет запущена в конфигурации «Интернет» или «Открытый Интернет», либо в программе будет отключена защита IP-трафика, то появится соответствующее сообщение и запустить программу ViPNet SafeDisk-V вы не сможете.

- При запуске программы ViPNet SafeDisk-V появится окно **ViPNet SafeDisk-V**, в котором вы сможете задать параметры защиты трафика в программе ViPNet Client. В результате в программе ViPNet Client будут добавлены соответствующие сетевые фильтры, которые будут действовать только во время работы программы ViPNet SafeDisk-V.

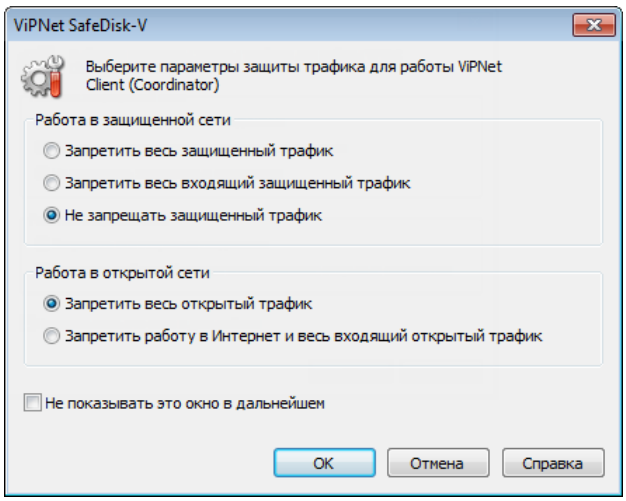



*Рисунок 78. Настройка параметров защиты трафика для работы ViPNet Client*

  Данные параметры невозможно изменить в программе ViPNet Монитор, что обеспечивает дополнительную защиту от несанкционированного доступа к защищенным контейнерам пользователей как открытой, так и защищенной сети (например, системный администратор или администратор сети ViPNet не смогут получить доступ к контейнеру).

  По умолчанию при работе с защищенными контейнерами независимо от настроек ViPNet Client всегда запрещаются любые открытые соединения (в группе **Работа в открытой сети** установлен режим **Запретить весь открытый трафик**). Крайне не рекомендуется изменять настройки работы в открытой сети, установленные по умолчанию, так как даже разрешение только исходящих открытых соединений (установка режима **Запретить работу в Интернет и весь входящий открытый трафик** в группе **Работа в открытой сети**) является потенциально опасным при работе с информацией в защищенных контейнерах.

- После того как в окне **ViPNet SafeDisk-V** будут заданы параметры защиты трафика, в области уведомлений над значком программы ViPNet Монитор появится уведомление о переходе в

режим работы SafeDisk-V. В названии главного окна программы ViPNet Монитор будет указано **Режим SafeDisk-V**, интерфейс программы будет ограничен (например, работа с сетевыми фильтрами будет невозможна и так далее) и будут заблокированы следующие возможности:

- возможность входа в программу в режиме администратора;
- возможность отключения защиты IP-трафика;
- возможность переключиться в конфигурацию «Интернет» или «Открытый Интернет»;
- выход и смена пользователя.

Также перед фильтрами, заданными в ViPNet Client, автоматически будут установлены запрещающие фильтры в соответствии с настройками в окне SafeDisk-V. Данные фильтры не отображаются в интерфейсе ViPNet Client.

- После завершения программы SafeDisk-V (в том числе при запуске команд **Срочное отключение контейнеров** в режиме **«Опасность»** и **Ликвидировать все контейнеры** в режиме **«Большая опасность»**) в программе ViPNet Client будут выполнены следующие действия:
  - будут выгружены все фильтры, автоматически созданные при запуске SafeDisk-V;
  - программа ViPNet Client продолжит работу с фильтрами конфигурации, в которой находилась до запуска программы ViPNet SafeDisk-V;
  - ограничение на интерфейс будет снято и станут доступными следующие возможности:
    - возможность входа в программу в режиме администратора;
    - возможность отключения защиты IP-трафика;
    - возможность переключиться в конфигурацию «Интернет» или «Открытый Интернет»;
    - выход и смена пользователя.

# 10

# Встроенные средства коммуникации


Общие сведения 170

Обмен защищенными сообщениями 171

Отправка писем программы ViPNet Деловая почта 178

Файловый обмен 179

Вызов внешних приложений 185

Просмотр веб-ресурсов сетевого узла 186

Обзор общих ресурсов сетевого узла 187

Проверка соединения с сетевым узлом 188

# Общие сведения

В состав программы ViPNet Монитор входит несколько дополнительных инструментов, предоставляющих возможность быстрого и защищенного обмена информацией:

- Обмен защищенными сообщениями / Защищенная конференция.
- Быстрая отправка электронных писем.
- Файловый обмен.
- Вызов внешних приложений.
- Функция «Открыть веб-ресурс сетевого узла».
- Функция «Обзор общих ресурсов сетевого узла».
- Проверка соединения с другим сетевым узлом ViPNet.

# Обмен защищенными сообщениями

Пользователи сети ViPNet могут в режиме реального времени обмениваться мгновенными сообщениями с другими пользователями ViPNet или участвовать в конференции с несколькими пользователями:

- Вы можете начать сеанс обмена сообщениями, чтобы отправлять сообщения одному или нескольким пользователям одновременно и получать от них ответы. При этом все участники сеанса будут получать ваши сообщения, но не будут получать ответные сообщения от других пользователей.

  Чтобы начать сеанс обмена сообщениями, в окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**, затем на панели просмотра выберите один или несколько сетевых узлов. В контекстном меню узлов выберите пункт **Послать сообщение** или на панели инструментов нажмите кнопку **Сообщение**  .

- Вы можете начать конференцию с несколькими пользователями, чтобы все участники сеанса могли получать сообщения от других пользователей и отвечать на них. В этом заключается отличие конференции от сеанса обмена сообщениями.

  Чтобы начать конференцию, в окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**, затем на панели просмотра выберите несколько сетевых узлов. В контекстном меню узлов выберите пункт **Конференция** или на панели инструментов нажмите кнопку **Конференция**  (по умолчанию эта кнопка скрыта).

Пользователь ViPNet может участвовать в нескольких сеансах обмена сообщениями одновременно. Если получено сообщение, которое не относится ни к одному из текущих сеансов, будет открыт новый сеанс обмена сообщениями.

Все сообщения, полученные и отправленные в течение сеанса, записываются в протокол сеанса. Если в рамках сеанса отправить сообщение какому-либо пользователю, его ответ придет в том же сеансе и будет сохранен в том же протоколе. При необходимости вы можете сохранить протокол сеанса как текстовый файл.

Во время сеанса обмена сообщениями вы можете отправлять пользователям файлы и письма (см. «Отправка файлов и писем из программы обмена защищенными сообщениями» на стр. 175).

---

**Примечание.** Если на вашем сетевом узле обмен сообщениями недоступен, обратитесь к администратору сети ViPNet с просьбой разрешить обмен сообщениями.

---

# Интерфейс программы обмена защищенными сообщениями

Прием и отправка сообщений выполняются в окне **Оперативный обмен защищенными сообщениями**, которое представлено на следующем рисунке:

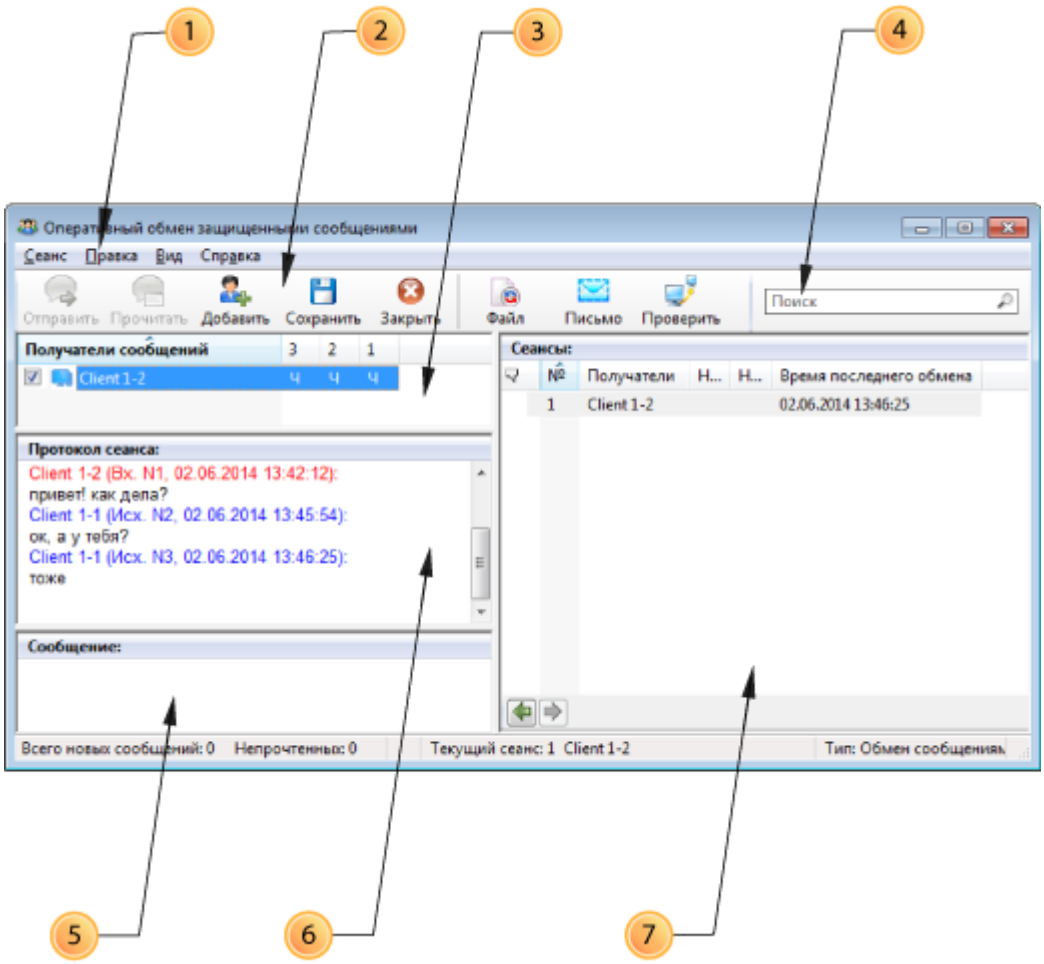



*Рисунок 79. Окно обмена защищенными сообщениями*

Цифрами на рисунке обозначены:

1. Главное меню программы обмена защищенными сообщениями.
2. Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Настроить панель**.
3. Панель **Получатели сообщений**. Содержит список пользователей, участвующих в данном сеансе. После отправки сообщения его статус отображается с помощью следующих символов:
   - О — сообщение отправлено, но еще не доставлено.
   - Д — сообщение доставлено, на экране получателя появилось уведомление о сообщении.
   - Ч — сообщение прочитано получателем.

- П — сообщение было прочитано, получатель собирается ответить.

Сообщения пронумерованы в порядке их отправки. Колонки со статусами отправленных сообщений расположены в обратном порядке (начиная с последнего отправленного сообщения). Сообщения отправляются пользователям, рядом с именами которых установлены флажки.

4 Строка поиска, предназначенная для фильтрации списка получателей на панели **Сеансы** и для поиска слов в сообщениях на панели **Протокол сеанса**. В протоколе сеанса все вхождения заданной строки поиска отмечаются желтым фоном.

5 Панель **Сообщение**. Предназначена для ввода новых сообщений.

6 Панель **Протокол сеанса**. На этой панели отображается история сообщений (протокол) текущего сеанса.

7 Панель **Сеансы**. Содержит список открытых сеансов и кнопки перехода между сеансами. Описание колонок на панели **Сеансы** приведено в следующей таблице:

| Колонка | Описание |
|---|---|
| | Статус сеанса:<br>Значки отсутствуют. Сеанс открыт, все сообщения были обработаны.<br>Сеанс открыт, получены новые сообщения.<br>Сеанс закрыт инициатором, однако в сеансе есть непрочитанные сообщения (этот значок отображается, только если сеанс инициирован другим пользователем).<br>Сеанс закрыт инициатором (этот значок отображается, только если сеанс инициирован другим пользователем). |
| **№** | Номер сеанса. |
| **Получатели** | Список участников сеанса. |
| **Новых** | Число новых (необработанных) сообщений. Если новых сообщений нет, это поле пусто. |
| **Не прочитано** | Число непрочитанных сообщений. Если непрочитанных сообщений нет, это поле пусто.<br>Если в сеансе есть непрочитанные сообщения, атрибуты этого сеанса выделены полужирным шрифтом. |
| **Время последнего обмена** | Дата и время последнего сообщения сеанса. |

Под списком открытых сеансов расположены кнопки  и  , с помощью которых можно перейти к предыдущему или к следующему просмотренному сеансу. В истории переходов между сеансами запоминается 10 последних сеансов, просмотр которых продолжался более 5 секунд.

# Отправка сообщений

Для обмена мгновенными сообщениями выполните следующие действия:

1. Если окно **Оперативный обмен защищенными сообщениями** закрыто, чтобы открыть его, в меню программы ViPNet Монитор выберите пункт **Приложения** > **Обмен сообщениями**. В окне **Оперативный обмен защищенными сообщениями** будут открыты все начатые ранее сеансы обмена сообщениями.
2. Чтобы начать новый сеанс обмена сообщениями или конференцию, в окне **Оперативный обмен защищенными сообщениями** выполните следующие действия:
   - В меню **Сеанс** выберите пункт **Новый**, а затем щелкните **Обмен сообщениями** или **Конференция**.
   - В окне **Выбор сетевого узла** укажите узлы, с пользователями которых вы хотите начать обмен сообщениями или конференцию. Затем нажмите кнопку **Выбрать**.

   Откроется новый сеанс обмена сообщениями. Если вы указали единственный сетевой узел, с которым сеанс обмена сообщениями уже был начат, то вместо нового сеанса откроется существующий сеанс.

   **Примечание.** Чтобы начать новый сеанс обмена сообщениями или конференцию, вы также можете выбрать сетевые узлы в разделе **Защищенная сеть** и выбрать в контекстном меню узлов соответствующий пункт (см. «Обмен защищенными сообщениями» на стр. 171).
3. В окне **Оперативный обмен защищенными сообщениями** выберите сеанс, в который вы хотите отправить новые сообщения.
4. На панели **Сообщение** введите текст сообщения.
5. Нажмите кнопку **Отправить** или клавишу **F5**.

   **Совет.** В настройках программы обмена сообщениями можно выбрать, какое действие выполняется по нажатию клавиши **Enter** на панели **Сообщение**: отправка сообщения или переход на новую строку. Для этого в программе ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**, откроется окно **Настройка**. В разделе **Обмен сообщениями** в группе **Назначить горячие клавиши** выберите **Ctrl+Enter: отправка сообщения, Enter: перевод строки** или наоборот.

# Прием сообщений

По умолчанию при поступлении новых сообщений в области уведомлений появляется значок , текст сообщения отображается во всплывающем окне над областью уведомлений. Чтобы прочитать новые сообщения, выполните одно из действий:

- Щелкните значок в области уведомлений.

- В окне **Оперативный обмен защищенными сообщениями** на панели инструментов нажмите кнопку **Прочитать** .

Вы можете изменить способ уведомления о новом сообщении. Для этого выполните следующие действия:

1 В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2 В окне **Настройка** в разделе **Обмен сообщениями** установите или снимите следующие флажки:

   - **Уведомлять о приходе сообщения полупрозрачным окном**.
   - **Уведомлять о приходе сообщения миганием кнопки на панели задач**.
   - **Уведомлять о приходе сообщения окном поверх всех окон**.
   - **Показывать новые сообщения в отдельном окне**.

     Если флажок **Показывать новые сообщения в отдельном окне** установлен, при получении сообщений откроется окно **Новые сообщения**.

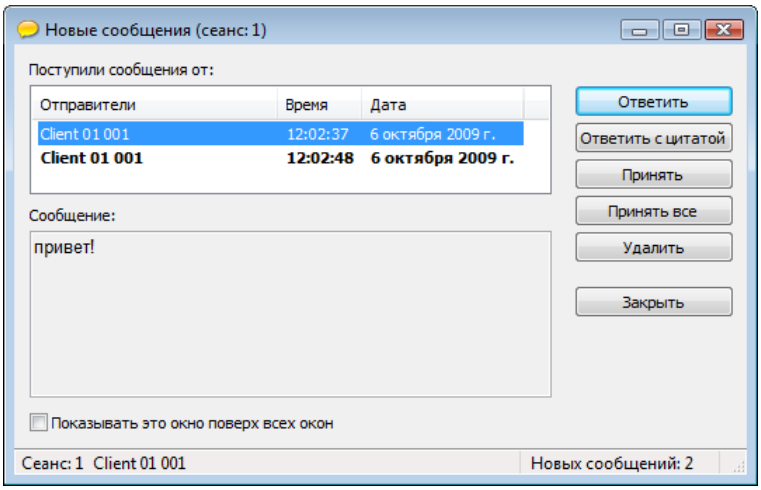



*Рисунок 80. Новые сообщения в отдельном окне*

В окне **Новые сообщения** отображается список новых сообщений в порядке поступления. С помощью кнопок в правой части окна вы можете принять сообщение (тогда оно будет сохранено в протоколе сеанса), ответить на сообщение или удалить его.

# Отправка файлов и писем из программы обмена защищенными сообщениями

Во время сеанса обмена сообщениями вы можете отправлять участникам сеанса файлы и письма по защищенному каналу VPN. Для этого используйте кнопки **Файл** и **Письмо** , расположенные на панели инструментов.

Отправка файлов осуществляется с помощью приложения «Файловый обмен» (см. «Отправка файлов из программы обмена защищенными сообщениями» на стр. 183).

Отправка писем возможна, только если вашему сетевому узлу назначена роль «Деловая почта» и на нем установлена программа ViPNet Деловая почта. Чтобы отправить письмо, выполните следующие действия:

1 В окне **Оперативный обмен защищенными сообщениями** на панели **Сеансы** выберите сеанс, участникам которого вы хотите отправить письмо.

2 На панели **Получатели сообщений** выберите участников и на панели инструментов нажмите кнопку **Письмо**  .

В результате будет запущена программа ViPNet Деловая почта и появится окно создания нового письма, в котором в качестве получателей будут указаны выбранные участники сеанса. Подробнее о том, как создать и отправить письмо, см. документ «ViPNet Деловая почта. Руководство пользователя».

**Примечание.** В список получателей нового письма будут включены только участники сеанса с ролью «Деловая почта», у которых установлена программа ViPNet Деловая почта. Если таких участников нет среди выбранных, то отправить письмо будет невозможно.

# Прекращение обмена сообщениями

Чтобы закрыть сеанс обмена сообщениями:

1 В окне **Оперативный обмен защищенными сообщениями** на панели **Сеансы** выберите сеанс, который требуется закрыть.

2 Если вы хотите сохранить протокол сеанса в виде текстового файла, щелкните сеанс правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить как**, затем укажите файл для сохранения протокола.

3 Выполните одно из действий:

- В меню **Сеанс** выберите пункт **Закрыть**.
- Нажмите клавишу **F8**.
- На панели инструментов нажмите кнопку **Закрыть**  .

4 После закрытия сеанс будет удален с панели **Сеансы**.

Чтобы закрыть программу обмена защищенными сообщениями, выполните одно из действий:

- В меню **Сеанс** выберите пункт **Выход**.
- Нажмите кнопку **Закрыть**  .

**Примечание.** При повторном открытии окна **Оперативный обмен защищенными сообщениями** все текущие сеансы будут восстановлены.

# Отправка писем программы ViPNet Деловая почта

В состав программного обеспечения ViPNet Client входит программа ViPNet Деловая почта, которая позволяет обмениваться электронными письмами в защищенной сети VPN. Если вашему сетевому узлу назначена роль «Деловая почта» и на нем установлена программа ViPNet Деловая почта, вы можете отправлять письма непосредственно из программы ViPNet Монитор. Для этого выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** выберите сетевой узел, на который требуется отправить письмо. Чтобы выбрать несколько сетевых узлов, зажмите клавишу **Ctrl** и по очереди щелкните нужные узлы. Чтобы отфильтровать список сетевых узлов, воспользуйтесь строкой поиска в нижней части раздела **Защищенная сеть**.
3. Выполните одно из действий:
   - Нажмите кнопку **Письмо**  на панели инструментов.
   - Щелкните сетевой узел правой кнопкой мыши и в контекстном меню выберите пункт **Отправить письмо**.

   В результате будет запущена программа ViPNet Деловая почта и появится окно создания нового письма, в котором в качестве получателей будут указаны выбранные сетевые узлы. Подробнее о том, как создать и отправить письмо, см. документ «ViPNet Деловая почта. Руководство пользователя».

---

**Примечание.** В список получателей нового письма будут включены только сетевые узлы с ролью «Деловая почта», у которых установлена программа ViPNet Деловая почта. Если таких узлов нет среди выбранных, то отправить письмо будет невозможно.

---

# Файловый обмен

С помощью приложения «Файловый обмен» пользователи сети ViPNet могут пересылать друг другу файлы по защищенному каналу VPN. Ограничения на размер и тип передаваемых файлов отсутствуют. Кроме этого обеспечивается контроль их целостности. Если целостность файла при передаче была нарушена, то данный файл автоматически удаляется.

**Примечание.** Для файлов, полученных от пользователей, у которых установлено ПО ViPNet более ранних версий, проверка целостности не выполняется. В окне **Файловый обмен** (см. Рисунок 73 на стр. 180) для таких файлов указан статус **Целостность не подтверждена**. Решение об использовании такого файла принимается на усмотрение пользователя.

Приложение «Файловый обмен» вы можете вызвать из программы ViPNet Монитор, из контекстного меню Windows или из программы обмена защищенными сообщениями.

**Примечание.** Если на вашем сетевом узле файловый обмен недоступен, обратитесь к администратору сети ViPNet с просьбой разрешить файловый обмен.

## Интерфейс программы «Файловый обмен»

Для просмотра файлов, отправленных и принятых по файловому обмену, откройте окно «Файловый обмен». Для этого в программе ViPNet Монитор выберите пункт меню **Приложения** > **Файловый обмен**.

Окно «Файловый обмен» также появляется каждый раз при отправке или приеме файлов.

Внешний вид окна программы «Файловый обмен» представлен на следующем рисунке.

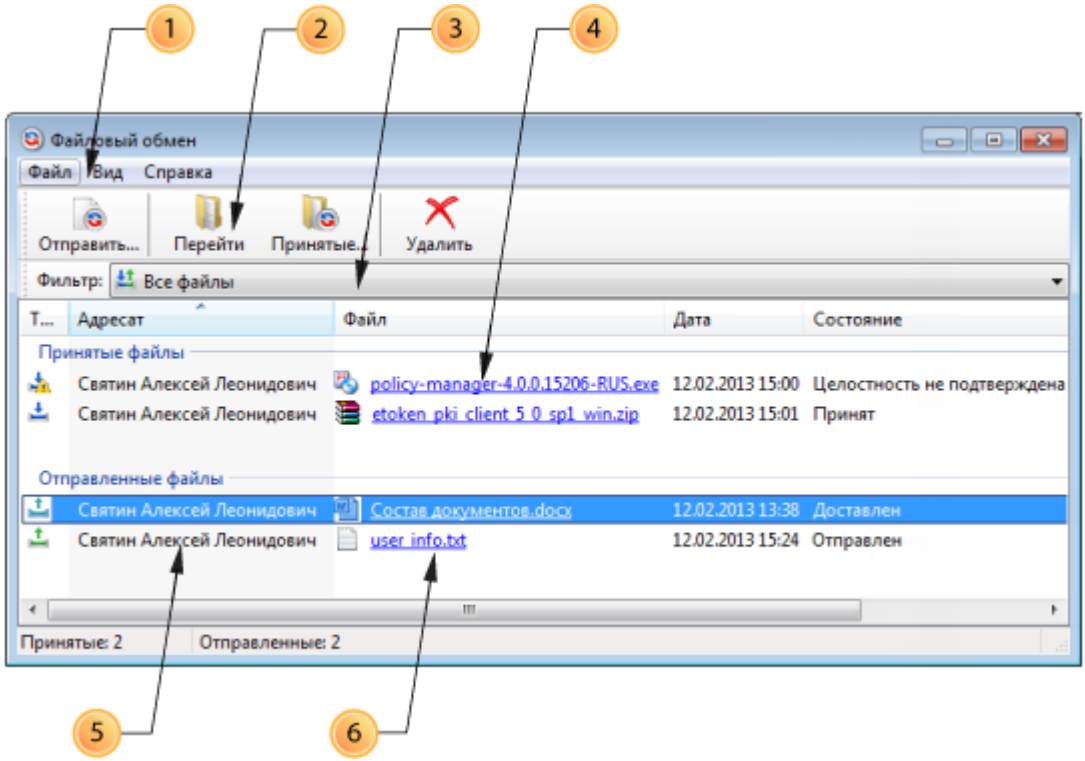



*Рисунок 81. Окно файлового обмена*

Цифрами на рисунке обозначены:

1 Главное меню программы.

2 Панель инструментов. С помощью кнопок на панели инструментов можно отправить новый файл, перейти к принятым файлам или удалить файл из списка.

Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Настроить панель**.

3 Фильтр списка файлов. Предусмотрено три режима отображения списка:

- Все файлы.
- Принятые файлы.
- Отправленные файлы.

4 Группа **Принятые файлы**. В этой группе отображаются файлы, полученные от пользователей других сетевых узлов ViPNet.

5 Группа **Отправленные файлы**. В этой группе отображаются файлы, переданные пользователям других сетевых узлов ViPNet.

6 Ссылка для перехода в папку, в которой находится файл.

# Отправка файлов из программы ViPNet Монитор

Чтобы отправить файл с помощью программы ViPNet Монитор:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** выберите сетевой узел, на который требуется отправить файл. Чтобы выбрать несколько сетевых узлов, зажмите клавишу **Ctrl** и по очереди щелкните нужные узлы. Чтобы отфильтровать список сетевых узлов, воспользуйтесь строкой поиска в нижней части раздела **Защищенная сеть**.
3. Выполните одно из действий:
   - Нажмите кнопку **Отправить**  на панели инструментов.
   - Щелкните сетевой узел правой кнопкой мыши и в контекстном меню выберите пункт **Отправить файл**.
4. В появившемся окне укажите файлы или папки, которые требуется отправить, и нажмите кнопку **Открыть**.

   Выбранные файлы будут отправлены адресату.

---

**Внимание!** При отправке файла длина его имени (включая путь) не должна превышать 130 символов. При отправке папки:

- Имя папки (включая путь) должно иметь длину не более 31 символа и не должно содержать восклицательный знак.
- Имена вложенных папок и файлов должны иметь длину не более 31 символа.

Если указанные ограничения нарушены, программа выдаст сообщение об ошибке, файлы и папки не будут отправлены.

---

5. Откроется окно **Файловый обмен** (см. Рисунок 73 на стр. 180), в котором отображается информация об отправленных файлах и их состоянии.
6. Когда отправленные файлы будут доставлены получателю, программа выдаст уведомление о доставке. Чтобы отключить уведомления, в окне сообщения установите флажок **Не показывать это сообщение в дальнейшем**.

---

**Примечание.** Для настройки уведомлений в окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения** и перейдите к разделу **Файловый обмен**.

---

# Отправка файлов с помощью контекстного меню Windows

Чтобы отправить файл пользователю ViPNet:

1 В Проводнике Windows выберите файл для отправки. Если нужно выбрать несколько файлов, удерживайте клавишу **Ctrl** и по очереди щелкните нужные файлы.

2 Щелкните один из выбранных файлов правой кнопкой мыши и в контекстном меню выберите пункт **Отправить файл адресату ViPNet**.

---

**Внимание!** При отправке файла длина его имени (включая путь) не должна превышать 130 символов. При отправке папки:

- Имя папки (включая путь) должно иметь длину не более 31 символа и не должно содержать восклицательный знак.
- Имена вложенных папок и файлов должны иметь длину не более 31 символа.

Если указанные ограничения нарушены, программа выдаст сообщение об ошибке, файлы и папки не будут отправлены.

---

3 В окне **Файловый обмен: Выбор сетевого узла** выберите из списка одного или нескольких получателей. Чтобы отфильтровать список пользователей, воспользуйтесь строкой поиска в нижней части окна.

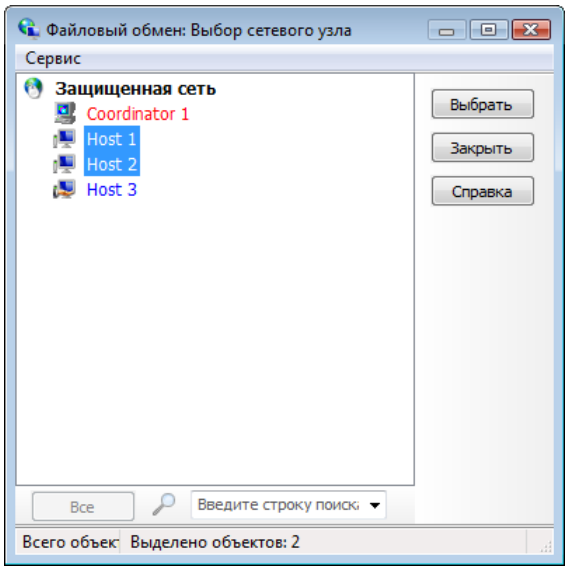



*Рисунок 82. Выбор получателя для отправляемых файлов*

4 Выбрав получателей, нажмите кнопку **Выбрать**. Файлы будут отправлены выбранным получателям.

5 Откроется окно **Файловый обмен** (см. Рисунок 73 на стр. 180), в котором отображается информация об отправленных файлах и их состоянии.

6 Когда отправленные файлы будут доставлены получателю, программа выдаст уведомление о доставке. Чтобы отключить уведомления, в окне сообщения установите флажок **Не показывать это сообщение в дальнейшем**.

---

**Примечание.** Для настройки уведомлений в окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения** и перейдите к разделу **Файловый обмен**.

---

# Отправка файлов из программы обмена защищенными сообщениями

Чтобы отправить файл во время обмена мгновенными сообщениями с пользователями ViPNet, выполните следующие действия:

1 В окне **Оперативный обмен защищенными сообщениями** на панели **Сеансы** выберите сеанс, участникам которого вы хотите отправить файл.

2 На панели **Получатели сообщений** выберите участников и на панели инструментов нажмите кнопку **Файл**  .

3 В появившемся окне укажите файлы, которые требуется отправить, и нажмите кнопку **Открыть**.

Выбранные файлы будут отправлены участникам сеанса.

---

**Внимание!** При отправке файла длина его имени (включая путь) не должна превышать 130 символов. Если указанное ограничение нарушено, программа выдаст сообщение об ошибке, файлы не будут отправлены.

---

4 Откроется окно **Файловый обмен** (см. Рисунок 73 на стр. 180), в котором отображается информация об отправленных файлах и их состоянии.

5 Когда отправленные файлы будут доставлены получателям, программа выдаст уведомление о доставке. Чтобы отключить уведомления, в окне сообщения установите флажок **Не показывать это сообщение в дальнейшем**.

---

**Примечание.** Для настройки уведомлений в окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения** и перейдите к разделу **Файловый обмен**.

---

# Прием файлов

При поступлении файлов от другого пользователя ViPNet:

1 Программа выдаст сообщение о принятом файле, в области уведомлений появится значок программы файлового обмена .

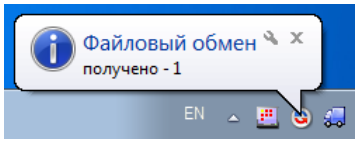



*Рисунок 83. Уведомление о принятом файле*

**Примечание.** Для настройки уведомлений в окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения** и перейдите к разделу **Файловый обмен**.

2 Чтобы просмотреть полученные файлы, щелкните значок файлового обмена в области уведомлений. Откроется окно **Файловый обмен** (см. Рисунок 73 на стр. 180).

3 В окне **Файловый обмен** в группе **Принятые файлы** выберите нужный файл и выполните одно из действий:

- Щелкните имя файла в столбце **Файл**.
- Нажмите кнопку **Принятые** на панели инструментов.

В новом окне будет открыта папка, содержащая выбранный файл.

Чтобы просмотреть файлы, полученные от определенного пользователя сети ViPNet:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.

2 В разделе **Защищенная сеть** выберите сетевой узел, от пользователя которого были приняты файлы, и нажмите кнопку **Принятые** на панели инструментов.

В новом окне будет открыта папка, содержащая файлы, поступившие с выбранного сетевого узла.

**Примечание.** Если в разделе **Защищенная сеть** выбрать несколько сетевых узлов и нажать кнопку **Принятые**, откроется папка, содержащая подпапки с файлами, которые были получены от разных пользователей ViPNet.

# Вызов внешних приложений

Программы ViPNet Client и ViPNet Coordinator поддерживают вызов внешних приложений, таких как:

- VNC Viewer.
- Remote Desktop Connection.
- Radmin Viewer.

Подробнее о работе с программами Radmin Viewer, VNC Viewer и Remote Desktop Connection можно прочесть в разделе Запуск программы удаленного доступа (на стр. 211).

С помощью внешних программ пользователи ViPNet могут пользоваться различными сервисами, предоставляемыми через Интернет, например, доступом к удаленному рабочему столу. Преимущество работы с внешними программами в сети ViPNet состоит в том, что весь трафик этих программ надежно шифруется.

Для взаимодействия с другим пользователем ViPNet с помощью внешнего приложения:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** щелкните нужный сетевой узел правой кнопкой мыши и в контекстном меню выберите пункт **Внешние программы**, затем щелкните команду вызова требуемой программы.

   Внешняя программа будет автоматически запущена в защищенном режиме, а пользователю выбранного сетевого узла ViPNet будет предложено подтвердить запуск той же программы на его компьютере.

# Просмотр веб-ресурсов сетевого узла

Если на компьютере, где установлено ПО ViPNet Client или ViPNet Coordinator, также установлен какой-либо веб-сервер или веб-приложение, то другие пользователи сети ViPNet могут осуществлять защищенное (шифрованное) соединение с этим веб-сервером.

При этом данный веб-сервер будет доступен только пользователям сети ViPNet, которым разрешено соединение с сетевым узлом, на котором установлен сервер. Это позволяет реализовать идею защищенного интернет-портала, в который могут быть интегрированы различные приложения — CRM, CMS, приложения на основе баз данных и многое другое.

Чтобы установить такое соединение:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** выберите сетевой узел, на котором организован защищенный Интернет-портал, и выполните одно из действий:
   - Нажмите кнопку **Веб-ресурс**  на панели инструментов.
   - Щелкните выбранный узел правой кнопкой мыши и в контекстном меню выберите пункт **Web-ссылка**.

# Обзор общих ресурсов сетевого узла

Функция «Обзор общих ресурсов сетевого узла» позволяет открыть сетевые ресурсы с общим доступом на сетевом узле ViPNet. Соединение устанавливается в защищенном режиме.

Чтобы открыть общий ресурс сетевого узла ViPNet:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** выберите нужный сетевой узел и выполните одно из действий:
   - Нажмите кнопку **Обзор**  на панели инструментов.
   - Щелкните выбранный узел правой кнопкой мыши и в контекстном меню выберите пункт **Открыть сетевой ресурс**.

В результате Проводник Windows в новом окне отобразит доступные сетевые ресурсы на выбранном сетевом узле. Пункт контекстного меню и кнопка на панели инструментов доступны, только если выбран один сетевой узел.

# Проверка соединения с сетевым узлом

С помощью программы ViPNet Монитор можно проверить текущий статус других сетевых узлов ViPNet из раздела **Защищенная сеть** — доступны они или нет, активны или нет и так далее. Для проверки соединения с сетевым узлом необходимо, чтобы этот узел имел версию ПО ViPNet не ниже 2.8.9.

Чтобы проверить соединение с одним или несколькими сетевыми узлами ViPNet и узнать статус их пользователей:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** выберите сетевой узел, соединение с которым требуется проверить. Чтобы выбрать несколько сетевых узлов, зажмите клавишу **Ctrl** и по очереди щелкните нужные узлы.
3. Выполните одно из действий:
   - Нажмите кнопку **Проверить** на панели инструментов.
   - Нажмите клавишу **F5**.
   - Щелкните один из выбранных сетевых узлов правой кнопкой мыши и в контекстном меню выберите пункт **Проверить соединение**.

   Откроется окно **Проверка соединения**, содержащее информацию о выбранных сетевых узлах.

Внешний вид окна **Проверка соединения** представлен на следующем рисунке:

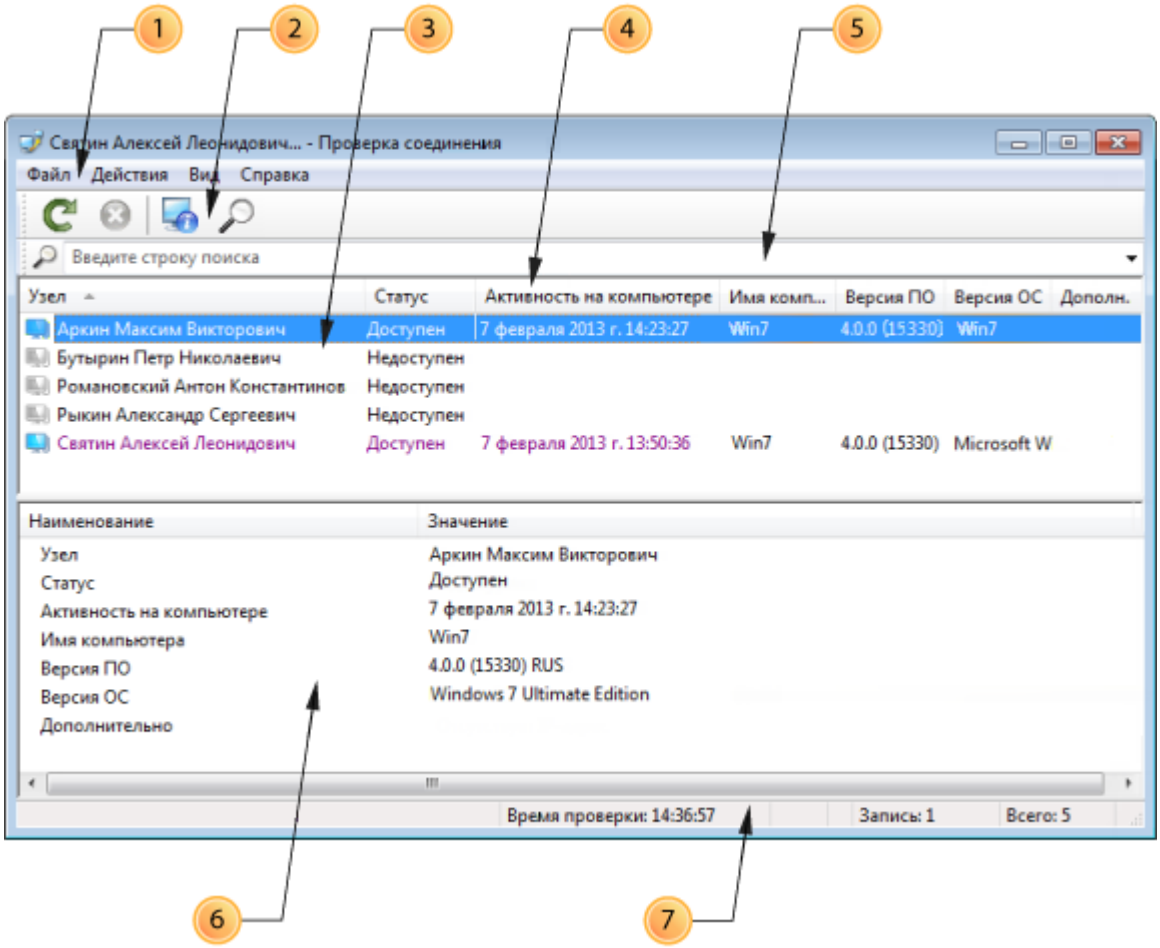



*Рисунок 84. Окно проверки соединения*

Цифрами на рисунке обозначены:

1 Главное меню программы проверки соединения.

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

3 Основная панель. Содержит список сетевых узлов, с которыми осуществляется проверка соединения.

Цвет и цветовое выделение (фон) имени сетевого узла обозначают его текущее состояние:

| Цвет имени | Состояние сетевого узла |
|---|---|
| Фиолетовый | Сетевой узел доступен, но последние 15 минут не проявлял активности на компьютере. |
| Черный на зеленом фоне | Сетевой узел доступен и проявлял активность за последние 15 минут. |
| Черный | Сетевой узел в данный момент не подключен к сети. |

- Чтобы посмотреть подробную информацию о сетевом узле в отдельном окне, выполните одно из действий:
  - Дважды щелкните нужный сетевой узел.
  - Выберите сетевой узел из списка и нажмите кнопку **Свойства** на панели инструментов.
  - Выберите сетевой узел из списка и нажмите клавишу **F3**.

  Откроется окно **Свойства узла**.

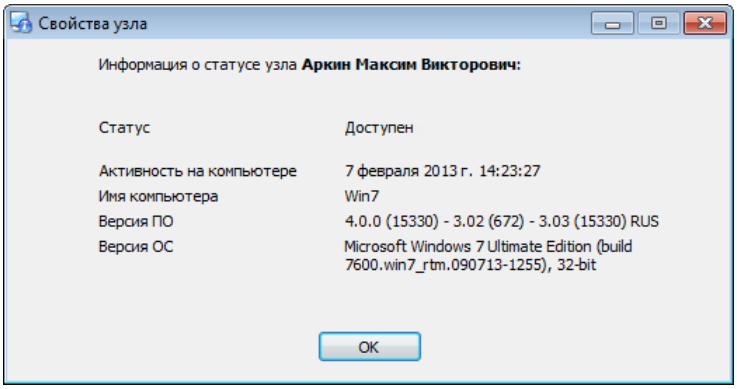



*Рисунок 85. Подробная информация о статусе сетевого узла*

- Чтобы отправить на один из сетевых узлов в окне **Проверка соединения** письмо программы ViPNet Деловая почта, начать сеанс обмена защищенными сообщениями или выполнить другое действие, доступное в разделе **Защищенная сеть**, щелкните выбранный узел правой кнопкой мыши и в контекстном меню выберите соответствующий пункт.

4 Столбцы основной панели. Статус сетевых узлов указан в столбце **Статус**. Описание возможных статусов приведено в таблице ниже.

| Статус | Описание |
|---|---|
| **Доступен** | Есть полноценная связь с сетевым узлом. |
| **Связь по VPN есть, но программа Монитор не доступна** | На сетевом узле не активна программа ViPNet Монитор, но сам узел доступен по защищенному каналу. В этом случае при взаимодействии с сетевым узлом недоступны встроенные средства коммуникации (такие как обмен защищенными сообщениями, файловый обмен и другие), но возможен просмотр общих ресурсов и веб-ресурсов сетевого узла, подключение через удаленный рабочий стол. |
| **Недоступен** | Связь с сетевым узлом отсутствует. |

В столбце **Активность на компьютере** указано время последней активности.

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

**5** Строка поиска. Предназначена для фильтрации списка сетевых узлов на основной панели (**3**).

**6** Панель свойств узла. Содержит подробную информацию о сетевом узле, выбранном на основной панели (**3**).

**7** Строка состояния.

---

**Примечание.** По умолчанию в окне **Проверка соединения** не отображаются панель инструментов (**2**), строка поиска (**5**), панель свойств узла (**6**) и строка состояния (**7**). Для отображения этих элементов интерфейса в меню **Вид** установите флажки в соответствующих пунктах.

---

# 11

# Административные функции


Работа с журналом IP-пакетов 193

Просмотр статистики фильтрации IP-пакетов 204

Просмотр информации о клиенте, времени работы программы и числе соединений 205

Управление конфигурациями программы 206

Запуск программы удаленного доступа 211

Работа в программе в режиме администратора 219

Настройка параметров запуска и аварийного завершения программы ViPNet Монитор 232

# Работа с журналом IP-пакетов

В разделе **Журнал IP-пакетов** на основе различных параметров поиска можно сформировать отчет о зарегистрированных программой IP-пакетах. Такие отчеты позволяют контролировать все входящие и исходящие соединения компьютера.

## Настройка параметров поиска IP-пакетов

Для просмотра журнала IP-пакетов:

1 В окне программы ViPNet Монитор выберите раздел **Статистика и журналы** > **Журнал IP-пакетов**.

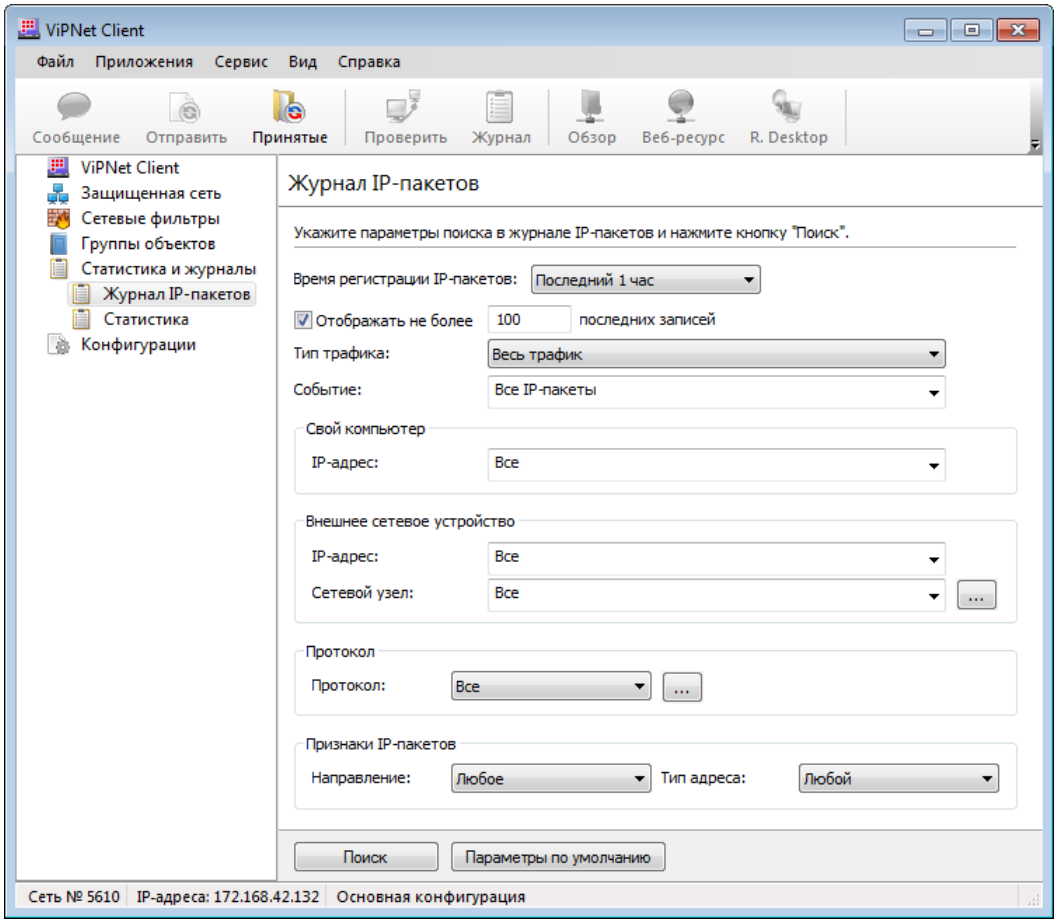



*Рисунок 86. Настройка параметров поиска по журналу IP-пакетов*

2 В разделе **Журнал IP-пакетов** задайте следующие параметры поиска:

- **Время регистрации IP-пакетов** (последние 24 часа, последний час, заданный интервал времени).

- **Число отображаемых записей журнала**. По умолчанию установлен флажок **Отображать не более** и заданное количество записей равно 100. Если снять этот флажок, будут показаны все записи, соответствующие параметрам поиска.
- В списке **Тип трафика** выберите один из пунктов:
  - **Весь трафик** — будут отображены записи обо всех IP-пакетах.
  - **Защищенный** — будут отображены записи о зашифрованных IP-пакетах, отправителем или получателем которых является данный сетевой узел.
  - **Открытый** — будут отображены записи об открытых IP-пакетах, отправителем или получателем которых является данный сетевой узел.
- В списке **Событие** укажите для поиска определенный тип или группу типов событий, которые ViPNet Монитор сопоставляет каждому IP-пакету (см. «События, отслеживаемые ПО ViPNet» на стр. 327).
- В группе **Свой компьютер** укажите IP-адрес своего компьютера.
- В группе **Внешнее сетевое устройство** укажите IP-адрес компьютера или имя сетевого узла ViPNet, являющегося вторым участником соединения.

**Примечание.** Задавать значения для обоих полей (**IP-адрес** и **Сетевой узел**) имеет смысл в случае, если участник соединения имеет несколько IP-адресов и необходимо получить статистику соединений с каким-либо конкретным IP-адресом, зарегистрированным на выбранном участнике.

- В списке **Протокол** выберите протокол передачи IP-пакетов, которые требуется найти. Если в списке нет нужного протокола, нажмите кнопку  и в окне **Список протоколов** добавьте требуемый протокол.
- В группе **Признаки IP-пакетов**:
  - В списке **Направление** выберите направление передачи IP-пакетов, которые требуется найти (**Любое**, **Входящие**, **Исходящие**).
  - В списке **Тип адреса** укажите, на какие адреса отправлялись IP-пакеты (**Любой**, **Одноадресный**, **Широковещательный**, **Групповой**).
- Чтобы восстановить начальные параметры поиска, нажмите кнопку **Параметры по умолчанию**.

3 Задав параметры поиска, нажмите кнопку **Поиск**.

**Примечание.** Если выполнить поиск с параметрами по умолчанию, в отчете будет показано не более 100 записей об IP-пакетах, зарегистрированных за последний час.

# Просмотр результатов поиска

После нажатия кнопки **Поиск** в разделе **Журнал IP-пакетов** будет выполнен поиск по журналу в соответствии с указанными параметрами. Результаты поиска отобразятся в окне **Журнал регистрации IP-пакетов**.

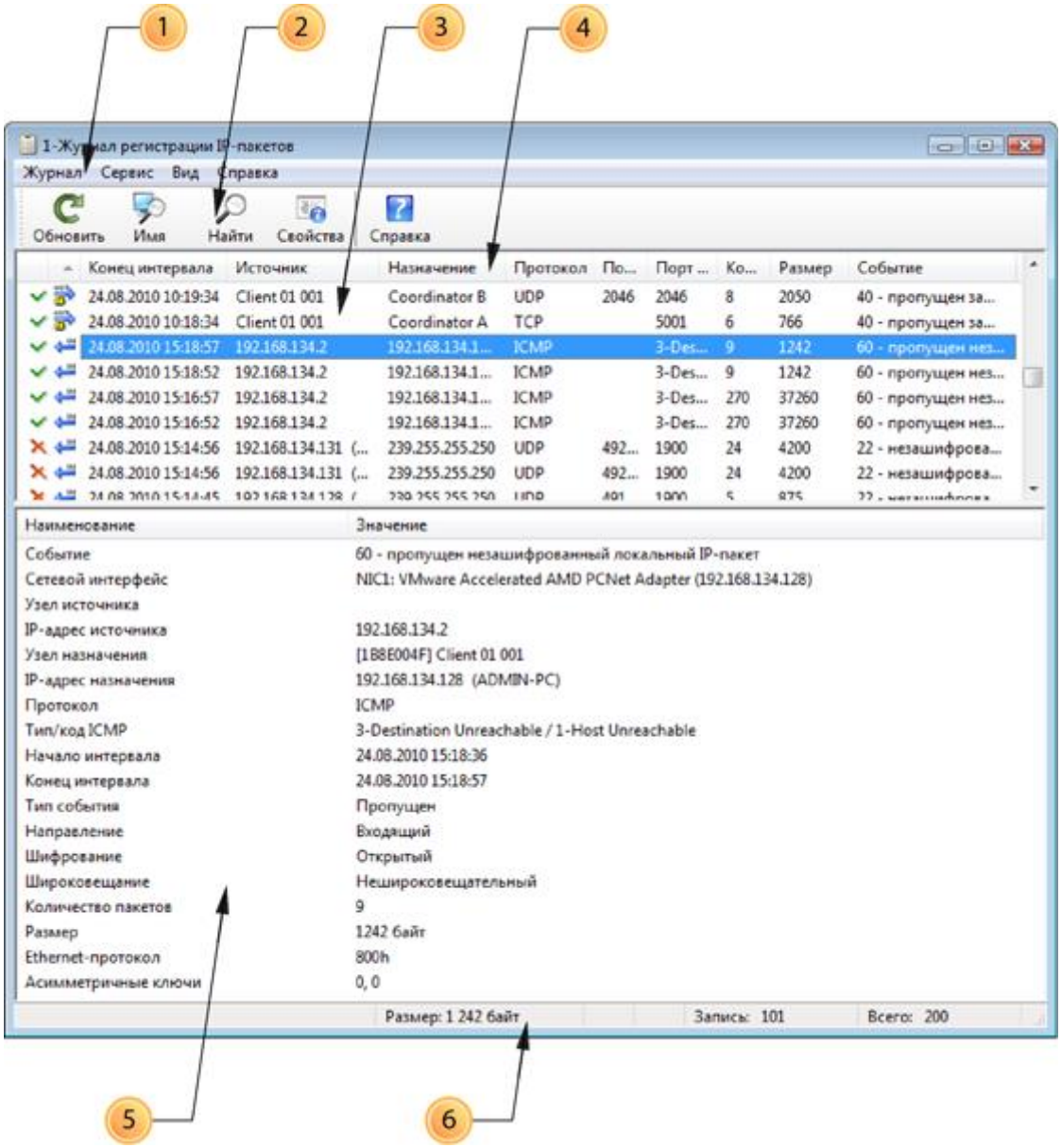



*Рисунок 87. Просмотр журнала IP-пакетов*

Цифрами на рисунке обозначены:

1 Главное меню.

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

3 Основная панель. Содержит список записей журнала, соответствующих заданным параметрам поиска.

- Чтобы просмотреть подробную информацию о выбранном IP-пакете в отдельном окне, нажмите кнопку **Свойства IP-пакетов** на панели инструментов окна **Журнал регистрации IP-пакетов**.
- Чтобы найти имя компьютера-отправителя или получателя выбранного пакета, нажмите кнопку **Определить имя компьютера** на панели инструментов или щелкните запись о пакете правой кнопкой мыши и в контекстном меню выберите пункт **Определить имя компьютера**.

4 Столбцы основной панели.

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

Описание столбцов приведено в таблице ниже.

*Таблица 6. Описание столбцов основной панели*

| Название столбца | Описание |
|---|---|
| **Тип события** | Типы событий обозначаются следующими значками:<br>— IP-пакеты заблокированы.<br>— IP-пакеты пропущены.<br>— IP-пакеты относятся к служебным событиям. |
| **Свойства пакета** | Свойства IP-пакетов обозначаются следующими значками:<br>— открытые входящие IP-пакеты.<br>— открытые исходящие IP-пакеты.<br>— зашифрованные входящие IP-пакеты.<br>— зашифрованные исходящие IP-пакеты. |
| **Начало интервала** | Дата и время создания записи для группы однотипных IP-пакетов (регистрация первого пакета).<br>Подробнее о регистрации однотипных пакетов в течение определенного интервала времени можно узнать в разделе Настройка параметров регистрации IP-пакетов в журнале (на стр. 201). |
| **Конец интервала** | Конец интервала регистрации группы однотипных IP-пакетов.<br>Если на данный момент интервал еще не закончился, то в этом столбце указано время регистрации последнего IP-пакета данного типа. Если будут зарегистрированы новые пакеты данного типа, значение данного параметра изменится. |
| **Источник** | Имя сетевого узла (для защищенных узлов ViPNet) или IP-адрес и имя компьютера (для открытых узлов) отправителя пакета. |
| **Узел источника** | Имя сетевого узла отправителя пакета (только для защищенных узлов). Если пакет отправлен открытым узлом, этот столбец будет пустым. |
| **IP-адрес источника** | IP-адрес и имя компьютера (если определилось) отправителя пакета. |

| | |
|---|---|
| **Порт источника** | Номер порта отправителя пакета. |
| **Назначение** | Имя сетевого узла (для защищенных узлов ViPNet) или IP-адрес и имя компьютера (для открытых узлов) получателя пакета. |
| **Узел назначения** | Имя сетевого узла получателя (только для защищенных узлов). Если пакет предназначен для открытого узла, этот столбец будет пустым. |
| **IP-адрес назначения** | IP-адрес и имя компьютера (если определилось) получателя пакета. |
| **Порт назначения (Тип / код ICMP)** | Номер порта получателя пакета. |
| **Протокол** | Протокол, по которому было установлено соединение. |
| **Событие** | Событие, соответствующее данной записи. Описание событий содержится в приложении События, отслеживаемые ПО ViPNet (на стр. 327). |
| **Количество пакетов** | Количество однотипных IP-пакетов, сгруппированных в одну запись в течение заданного интервала времени. |
| **Размер** | Размер (в байтах) всех IP-пакетов, сгруппированных в одну запись. |

5 Панель свойств IP-пакетов. Содержит подробную информацию о записи, выбранной на основной панели (**3**).

6 Строка состояния. Содержит размер выбранного пакета (или группы пакетов) в байтах, порядковый номер записи в списке и общее число найденных записей. Если на основной панели (**3**) выбрано несколько записей, в строке состояния отображается суммарный размер соответствующих IP-пакетов.

**Совет.** Чтобы определить суммарный объем IP-трафика, зарегистрированного на сетевом узле ViPNet, выполните поиск всех IP-пакетов в журнале. Затем в окне **Журнал регистрации IP-пакетов** с помощью сочетания клавиш **Ctrl+A** выберите все записи. В строке состояния будет показан суммарный размер найденных IP-пакетов.

## Просмотр журнала IP-пакетов в интернет-браузере или в Microsoft Excel

Чтобы экспортировать результаты поиска, в окне **Журнал регистрации IP-пакетов** щелкните меню **Журнал**, а затем выберите один из пунктов:

- **Просмотр в веб-браузере.** Таблица с результатами поиска будет открыта в вашем веб-браузере. В строке адреса будет указан путь к файлу отчета.

- **Просмотр в Excel.** Таблица с результатами поиска будет открыта в приложении Microsoft Excel (для этого приложение должно быть установлено на компьютере). Чтобы сохранить эту таблицу, в Microsoft Excel воспользуйтесь функцией **Сохранить как**.

## Выбор IP-пакетов

В журнале регистрации IP-пакетов можно выделить IP-пакеты:

- широковещательные;
- относящиеся к служебным событиям;
- принадлежащие одной сессии, установленной в начале взаимодействия между двумя узлами;
- принадлежащие одним и тем же IP-адресам вне зависимости от направления пакета и порта соединения.

**Примечание.** Под сессией подразумеваются все IP-пакеты, передаваемые между узлом 1 и узлом 2. Если при этом соединение осуществляется по протоколу TCP или UDP, то учитываются также и порты. Например, соединение между узлом 1 и узлом 2 по протоколу HTTP будет считаться одной сессией (узел 1 открывает веб-страницу с сервера IIS, установленного на узле 2). Однако если узел 1 подключится к узлу 2 по протоколу FTP (скачает файл с FTP-сервера, установленного на узле 2), то это уже будет считаться другой сессией.

Чтобы выделить IP-пакеты:

1. В окне **Журнал регистрации IP-пакетов** щелкните запись журнала правой кнопкой мыши.
2. В появившемся контекстном меню выберите:
   - **Выделить по IP-адресам**, чтобы выделить все записи IP-пакетов, имеющих те же IP-адреса, что выбранный пакет.
   - **Выделить сессию**, чтобы выделить все записи IP-пакетов, относящихся к сессии выбранного пакета.
   - **Выделить широковещательные**, чтобы выделить записи широковещательных пакетов.
   - **Выделить служебные**, чтобы выделить записи служебных событий.
3. Чтобы снять выделение, в контекстном меню выберите пункт **Отменить выделение**.

## Рекомендации по анализу открытых (нешифрованных) и зашифрованных соединений

Для удобства анализа открытых соединений в журнале регистрации IP-пакетов рекомендуется произвести следующие настройки:

1. В окне **Журнал регистрации IP-пакетов** щелкните правой кнопкой мыши по любому из заголовков столбцов.

2 В появившемся контекстном меню выберите **Свойства**.

3 Для анализа:

- открытых (нешифрованных) соединений:
  - в окне **Поля** настройте отображение следующих столбцов: **IP-адрес источника**, **IP-адрес назначения**.
  - в окне **Поля** скройте следующие столбцы: **Источник**, **Узел источника**, **Назначение**, **Узел назначения**.
- закрытых (зашифрованных) соединений:
  - в окне **Поля** настройте отображение следующих столбцов: **Узел источника**, **Узел назначения**.
  - в окне **Поля** скройте следующие столбцы: **IP-адрес источника**, **IP-адрес назначения**.

4 По окончании настройки нажмите кнопку **OK** для закрытия окна и сохранения изменений или кнопку **Отмена** для выхода без сохранения изменений.

# Создание сетевого фильтра при просмотре журнала IP-пакетов

Если требуется пропускать IP-пакеты в рамках запрещенных соединений либо блокировать IP-пакеты в рамках разрешенных соединений, вы можете создать сетевой фильтр для таких IP-пакетов при просмотре соединений в журнале IP-пакетов. Для этого выполните следующие действия:

1 В окне **Журнал регистрации IP-пакетов** (см. «Просмотр результатов поиска» на стр. 195) выберите запись о заблокированном соединении, которое должно быть разрешено, либо разрешенное соединение, которое должно быть заблокировано.

2 Щелкните выбранную запись правой кнопкой мыши и в контекстном меню выберите пункт **Создать фильтр**.

В зависимости от типа выбранного соединения появится окно создания:

- Фильтра открытой сети — если в рамках соединения передавались незашифрованные IP-пакеты.
- Фильтра защищенной сети — если в рамках соединения передавались зашифрованные IP-пакеты.

3 В разделах окна свойств сетевого фильтра будут автоматически заданы параметры, сформированные из записи выбранного соединения. При необходимости внесите соответствующие изменения (см. «Создание сетевых фильтров» на стр. 144).

4 В окне свойства сетевого фильтра нажмите кнопку **OK**. В результате созданный фильтр появится в списке сетевых фильтров.

# Просмотр журнала IP-пакетов другого сетевого узла

При работе в режиме администратора сетевого узла можно запросить журнал IP-пакетов другого сетевого узла ViPNet, с которым у данного узла есть связь. Для этого выполните следующие действия:

1 Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 219).

2 В окне программы ViPNet Монитор на панели навигации выберите раздел **Журнал IP-пакетов**.

3 В списке **Журнал сетевого узла** выберите сетевой узел, журнал которого требуется просмотреть. Если нужного сетевого узла нет в списке, нажмите кнопку  и в окне **Выбор сетевого узла** укажите нужный узел.

4 После выбора сетевого узла, журнал которого требуется просмотреть, с этим узлом будет установлено соединение. В случае успешного соединения имя выбранного узла появится в списке **Журнал сетевого узла**. Чтобы прервать процесс подключения, нажмите кнопку **Отмена**.

---

**Примечание.** Если сетевой узел, с которого запрашивается журнал IP-пакетов, имеет версию ПО ViPNet ниже 3.0, то параметры поиска будут существенно ограничены. Это связано с тем, что в версии 3.0 формат журнала IP-пакетов изменился. При ограничении параметров поиска появится соответствующее предупреждение.

Следует иметь в виду, что при просмотре журнала IP-пакетов другого сетевого узла параметры поиска соответствуют типу этого узла. То есть если в программе ViPNet Coordinator запросить журнал IP-пакетов клиента, можно указать только параметры, доступные на клиентах.

---

5 Задайте параметры поиска (см. «Настройка параметров поиска IP-пакетов» на стр. 193) и нажмите кнопку **Поиск**.

# Просмотр архива журналов IP-пакетов

Архивация журналов IP-пакетов применяется для оптимизации поиска по IP-пакетам и для рационального использования дискового пространства.

Новый архив создается, когда текущий журнал IP-пакетов достиг размера, определенного параметром **Максимальный размер журнала** (см. «Настройка параметров регистрации IP-пакетов в журнале» на стр. 201). Если данный параметр установлен в значение «0», архивирование журнала не происходит.

Для просмотра архива журнала IP-пакетов:

1 В окне программы ViPNet Монитор в разделе **Журнал IP-пакетов** выберите подраздел **Архив журналов** и далее архив с нужным интервалом дат.

**Примечание.** Если подраздел **Архив журналов** не отображается, значит, системой не было создано ни одного архива.

2 Укажите параметры поиска по архиву журнала (см. «Настройка параметров поиска IP-пакетов» на стр. 193).

3 Результаты поиска будут отображены в окне **Журнал регистрации IP-пакетов**.

**Совет.** Чтобы удалить неактуальные архивы журналов IP-пакетов, в подразделе **Архив журналов** выберите один или несколько архивов и воспользуйтесь клавишей **Delete** на клавиатуре или командой **Удалить** из контекстного меню.

# Настройка параметров регистрации IP-пакетов в журнале

Чтобы настроить параметры журнала IP-пакетов:

1 В главном окне ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2 На панели навигации окна **Настройка** выберите раздел **Журнал IP-пакетов**.

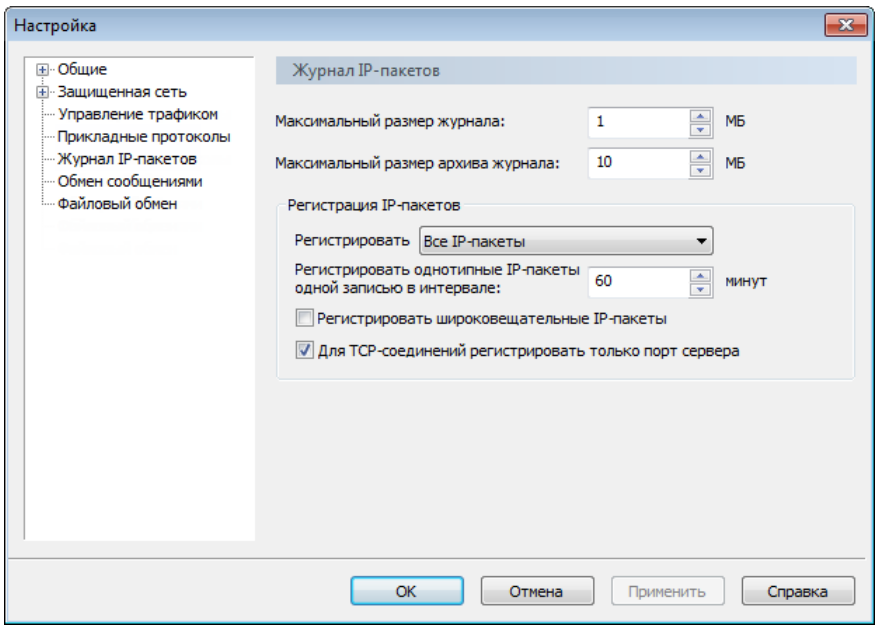



*Рисунок 88. Настройка параметров журнала IP-пакетов*

3 Задайте значения следующих параметров:

- В поле **Максимальный размер журнала** укажите размер журнала в мегабайтах (по умолчанию — 1 Мбайт). Если размер журнала превысит указанное значение, записи в хронологическом порядке будут переноситься в архив.

  Чтобы отключить ведение журнала, задайте значение 0. Записи о новых зарегистрированных IP-пакетах не будут добавляться в журнал. Однако записи, созданные до присвоения значения 0, будут сохранены.

  При первой архивации журнала IP-пакетов на панели навигации главного окна ViPNet Монитор создается раздел **Архив журналов**.

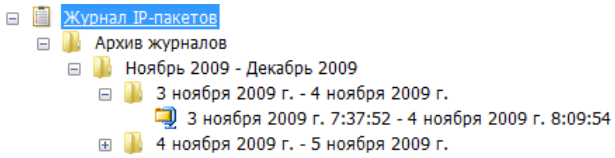



  *Рисунок 89. Архив журнала IP-пакетов*

- В поле **Максимальный размер архива журнала** укажите размер архива в мегабайтах (по умолчанию — 10 Мбайт). Если размер архива журнала превысит указанное значение, старые записи будут удаляться из архива в хронологическом порядке.

  Чтобы отключить перенос записей в архив, задайте значение 0. Однако данные, помещенные в архив до присвоения значения 0, будут сохранены.

- С помощью списка **Регистрировать** укажите, какие IP-пакеты следует регистрировать в журнале: **Все IP-пакеты** или **Только блокируемые IP-пакеты**.

- В поле **Регистрировать однотипные IP-пакеты одной записью в интервале** укажите интервал времени в минутах. По истечении указанного интервала для IP-пакетов определенного типа будет создаваться новая запись в журнале.

  Смысл данного параметра состоит в том, что при регистрации пакета с определенными параметрами (IP-адрес, протокол, порт и так далее) для него создается запись в журнале. В течение указанного интервала времени IP-пакеты, которые имеют те же IP-адрес, протокол, порт и другие параметры, регистрируются, но записи в журнале для них не создаются. Число таких пакетов, зарегистрированных в течение интервала, указано в столбце **Количество пакетов** в окне **Журнал регистрации IP-пакетов**.

  Когда заданный интервал времени истекает, для следующего IP-пакета создается новая запись в журнале, даже если этот пакет имеет параметры, которые уже зафиксированы в другой записи. Если поступает пакет другого типа, для него также создается новая запись в журнале. После создания новой записи снова начинается отсчет интервала времени для пакетов с одинаковыми параметрами. Данный механизм распространяется на все регистрируемые IP-пакеты.

  Начало и конец интервала времени, в течение которого были зарегистрированы IP-пакеты, объединенные одной записью, указаны в столбцах **Начало интервала** и **Конец интервала**.

  Данный механизм позволяет значительно сократить размер журнала IP-пакетов, сохранив его информативность. Чем больше заданный интервал времени, тем меньше размер

журнала. Однако с увеличением интервала регистрации уменьшается точность данных в журнале (невозможно определить время регистрации пакетов).

Если задать нулевое значение интервала регистрации пакетов, для каждого зарегистрированного IP-пакета будет создаваться запись в журнале. Однако размер журнала при этом может сильно увеличиться. Нулевое значение интервала рекомендуется задавать только для тестирования и на короткое время. ViPNet-драйвер может хранить не более 10000 записей журнала. По достижении этого ограничения более старые записи заменяются новыми. Если обмен трафиком достаточно интенсивен, часть информации может быть потеряна. Кроме того, обработка трафика может замедлиться, так как увеличится нагрузка на процессор компьютера.

- Установите флажок **Регистрировать широковещательные IP-пакеты**, чтобы такие пакеты фиксировались в журнале.
- Убедитесь, что установлен флажок **Для TCP-соединений регистрировать только порт сервера**. В этом случае IP-пакеты протокола TCP будут группироваться по порту сервера вне зависимости от порта клиента.

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

# Просмотр статистики фильтрации IP-пакетов

Чтобы просмотреть статистику фильтрации IP-пакетов, в окне программы ViPNet Монитор на панели навигации выберите раздел **Статистика и журналы** > **Статистика**.

В разделе **Статистика** представлены данные о количестве входящих и исходящих IP-пакетов, которые были пропущены или заблокированы в соответствии с заданными фильтрами трафика. Эта информация может быть полезна при первоначальной настройке программы ViPNet Монитор.

Чтобы обнулить статистику IP-пакетов, нажмите кнопку **Очистить**.

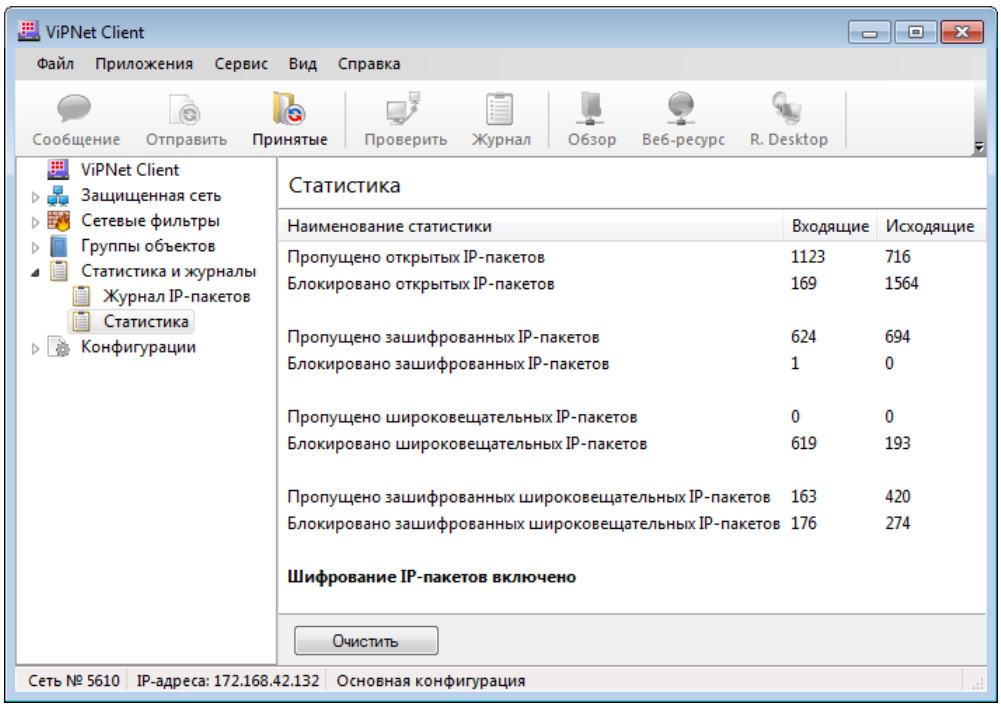



*Рисунок 90. Просмотр статистики IP-пакетов*

# Просмотр информации о клиенте, времени работы программы и числе соединений

Чтобы получить информацию о сети ViPNet, в которой находится данный узел ViPNet, о пользователе, который произвел вход в программу, сведения о соединениях узла и другую дополнительную информацию, в окне программы ViPNet Монитор выберите раздел **ViPNet Client**.

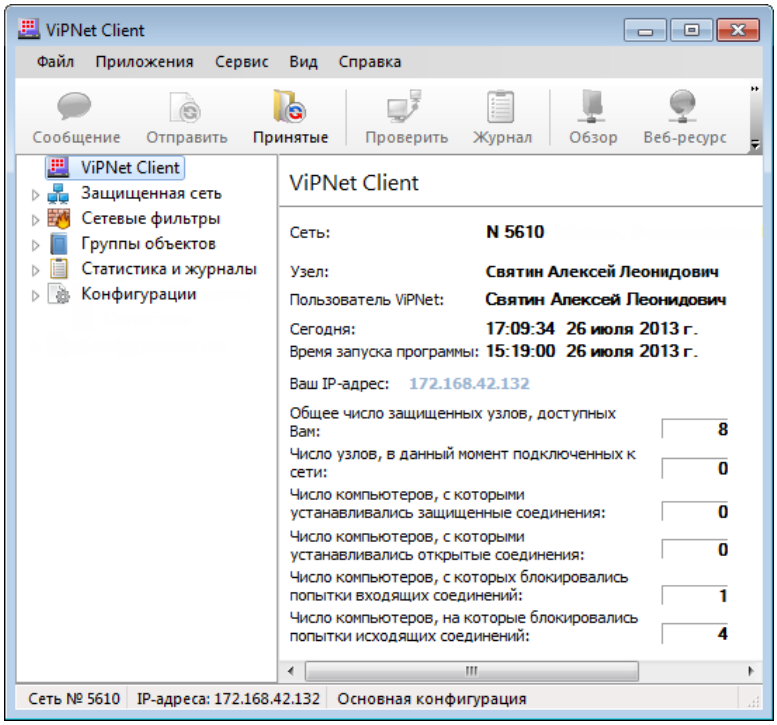



*Рисунок 91. Раздел общей информации об узле ViPNet*

# Управление конфигурациями программы

Конфигурация — это совокупность всех настроек ViPNet Монитор. В разделе **Конфигурации** можно создать несколько дополнительных конфигураций и установить требуемую конфигурацию в любой момент.

Использование нескольких конфигураций может быть полезно в следующих случаях. Предположим, что политика безопасности компании запрещает одновременно работать с локальными ресурсами и ресурсами Интернета. Тогда вам следует создать две конфигурации: в одной конфигурации должна быть разрешена работа в Интернете и запрещен доступ в локальную сеть, во второй конфигурации должна быть разрешена работа в локальной сети и запрещен доступ в Интернет. Либо, например, вам приходится периодически изменять настройки подключения к защищенной сети. Тогда для удобства вы можете создать несколько конфигураций с разными настройками подключения к защищенной сети. В дальнейшем вам не потребуется изменять настройки каждый раз, когда возникнет необходимость. Будет достаточно просто выбрать конфигурацию с нужными настройками.

При первом запуске программы создается **Основная конфигурация**, которая содержит настройки по умолчанию. Эту конфигурацию нельзя переименовать или удалить. Также в программе ViPNet Монитор могут по умолчанию присутствовать специальные конфигурации, предназначенные для работы в Интернете: «Открытый Интернет», «Внутренняя сеть» и «Интернет». Описание данных конфигураций приведено в разделах ниже.

---

**Примечание.** При использовании контейнеров SafeDisk-V работа в конфигурациях «Открытый Интернет» и «Интернет» существенно ограничивается — доступ в Интернет автоматически блокируется набором сетевых фильтров. Подробнее см. раздел Работа с интегрированной программой ViPNet SafeDisk-V (на стр. 167).

---

В программе ViPNet Монитор вы можете выполнить следующие действия по управлению конфигурациями:

1 Чтобы создать новую конфигурацию, в окне программы ViPNet Монитор на панели навигации щелкните правой кнопкой мыши раздел **Конфигурации** и в контекстном меню выберите **Создать конфигурацию**.

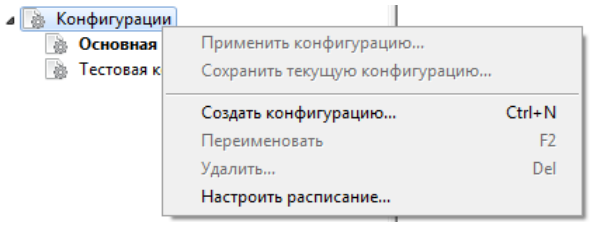



*Рисунок 92. Создание новой конфигурации*

В списке конфигураций появится элемент **Новая конфигурация**.

**Примечание.** В режиме администратора можно создать конфигурацию программы для любого пользователя, зарегистрированного на узле. В данном режиме отображаются все конфигурации, созданные в процессе работы с программой, причем они сгруппированы по пользователям, от имени которых были созданы.

2 Чтобы переименовать конфигурацию, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт **Переименовать**.

3 Чтобы загрузить (сделать активной) одну из конфигураций, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт **Применить конфигурацию**.

**Примечание.** Загрузить нужную конфигурацию вы также можете из главного меню программы **Файл** > **Конфигурации** либо из контекстного меню значка программы ViPNet Монитор в области уведомлений на панели задач.

4 Если в текущей конфигурации были изменены параметры программы (например, созданы новые сетевые фильтры, изменены настройки), то вы можете сохранить изменения в любой другой существующей конфигурации, кроме основной. Для этого щелкните нужную конфигурацию правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить текущую конфигурацию**. В окне подтверждения нажмите кнопку **Да**.

В текущей конфигурации все изменения сохраняются автоматически.

Если в программе создано несколько конфигураций и при этом в настройках установлен флажок **Вызывать окно выбора конфигурации** (см. «Настройка параметров запуска и аварийного завершения программы ViPNet Монитор» на стр. 232), то при запуске ViPNet Монитор откроется окно выбора конфигурации.

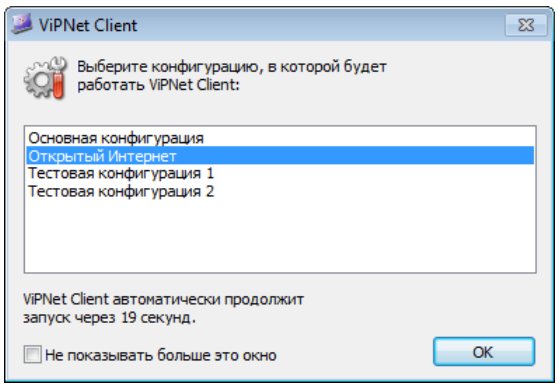



*Рисунок 93. Выбор конфигурации при запуске программы*

Для того чтобы загрузить одну из этих конфигураций, выберите ее в списке и нажмите кнопку **OK**.

Если в течение 30 секунд с момента появления окна не будет выбрана ни одна конфигурация, программа ViPNet Монитор продолжит работу в основной конфигурации.

Если в программе создано несколько конфигураций, которые используются в конкретные периоды времени, то для удобства вы можете настроить расписание автоматической смены данных конфигураций (см. «Настройка расписания смены конфигураций программы» на стр. 209).

# Конфигурация «Открытый Интернет»

Если клиент связан с координатором, для которого в программе ViPNet Центр управления сетью включена функция сервера открытого Интернета, в списке конфигураций программы ViPNet Монитор присутствует конфигурация «Открытый Интернет».

Если доступ клиентов в Интернет организован через сервер Открытого Интернета:

- Для работы в защищенной сети установите любую конфигурацию, кроме конфигурации «Открытый Интернет».

  В этом случае соединение с сервером открытого Интернета установить невозможно. Следовательно, невозможно получить доступ к Интернету.

- Для работы с ресурсами Интернета установите конфигурацию «Открытый Интернет».

  При загрузке конфигурации «Открытый Интернет» в раздел **Сетевые фильтры** будут автоматически добавлены фильтры трафика, запрещающие соединение с какими-либо сетевыми узлами ViPNet, кроме сервера открытого Интернета.

---

**Примечание.** Находясь в конфигурации «Открытый Интернет» вы не можете работать с защищенными контейнерами SafeDisk-V (см. «Интеграция с программой ViPNet SafeDisk-V» на стр. 162).

---

Таким образом, клиент может быть подключен либо только к защищенной сети ViPNet, либо только к Интернету. Это позволяет изолировать компьютер, обменивающийся потенциально опасным трафиком в Интернете, от остальных узлов сети ViPNet.

# Конфигурации «Внутренняя сеть» и «Интернет»

Если администратор сети ViPNet в программе ViPNet Центр управления сетью установил для пользователей сетевого узла уровень полномочий «h», в программе ViPNet Монитор автоматически создаются две конфигурации: «Внутренняя сеть» и «Интернет».

Подробная информация об уровнях полномочий пользователя содержится в документе «Классификация полномочий. Приложение к документации ViPNet».

Конфигурации «Внутренняя сеть» и «Интернет» имеют следующие особенности:

- Конфигурация «Внутренняя сеть» предназначена для работы в защищенной сети ViPNet и запрещает соединения с открытыми узлами.

При загрузке этой конфигурации в разделе **Фильтры открытой сети** автоматически добавляются фильтры, блокирующие любой открытый IP-трафик, кроме пакетов службы DHCP.

- Конфигурация «Интернет» предназначена для работы в открытой сети и запрещает соединения с защищенными узлами ViPNet.

  При загрузке этой конфигурации в разделе **Фильтры защищенной сети** автоматически добавляются фильтры, блокирующие любой защищенный IP-трафик.

**Примечание.** Находясь в конфигурации «Интернет», вы не можете работать с защищенными контейнерами SafeDisk-V (см. «Интеграция с программой ViPNet SafeDisk-V» на стр. 162).

# Настройка расписания смены конфигураций программы

Если в процессе работы в программе ViPNet Монитор используется несколько конфигураций, каждая из которых должна устанавливаться в конкретное время, вы можете настроить расписание автоматической смены конфигураций. Например, автоматическая смена будет удобна в том случае, если вам периодически в заданное время приходится переключаться в конфигурацию для работы в Интернете. В остальных случаях, как правило, рекомендуется менять конфигурации вручную.

Настроить расписание смены конфигураций можно только в том случае, если в программе создано более двух конфигураций. Основная конфигурация и специальные конфигурации при этом не учитываются, расписание их установки настроить нельзя. Основная конфигурация автоматически устанавливается и вступает в действие в те промежутки времени, в которые не действуют по расписанию остальные конфигурации. Специальные конфигурации можно установить только вручную.

**Внимание!** При пересечении расписаний автоматическая смена конфигураций не гарантируется. В процессе составления расписаний рекомендуется следить за тем, чтобы расписания смены конфигураций не пересекались.

Чтобы настроить расписание смены конфигураций, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации щелкните правой кнопкой мыши раздел **Конфигурации** или любую созданную конфигурацию и в контекстном меню выберите пункт **Настроить расписание**.
2. В окне **Настройка расписания смены конфигурации** установите флажок **Устанавливать конфигурации в соответствии с расписанием**, после чего добавьте в список конфигураций, которые требуется устанавливать автоматически.

   При добавлении конфигурации в окне **Параметры расписания** задайте следующие данные:

   - в поле **Начало действия** — время установки конфигурации (в часах);

- в поле **Длительность** — время, в течение которого должна действовать конфигурация после установки (количество часов);
- в группе **Повторение** — дни недели, в которые должна устанавливаться конфигурация.

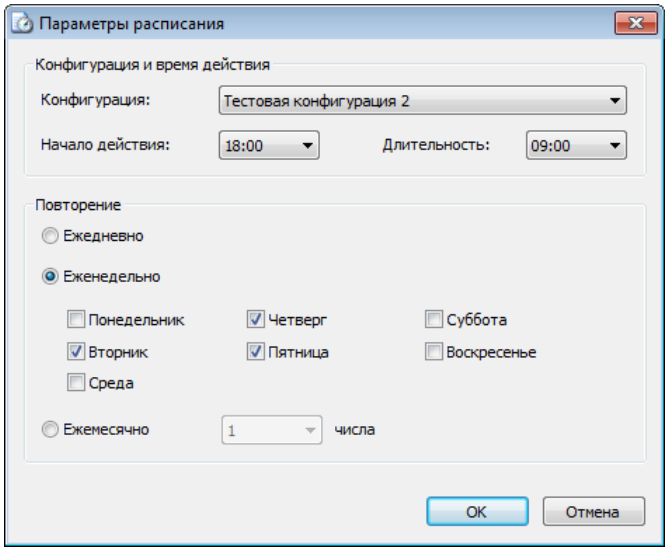



*Рисунок 94. Настройка расписания смены конфигураций*

3 Нажмите кнопку **OK**.

В результате расписание смены конфигураций будет настроено.

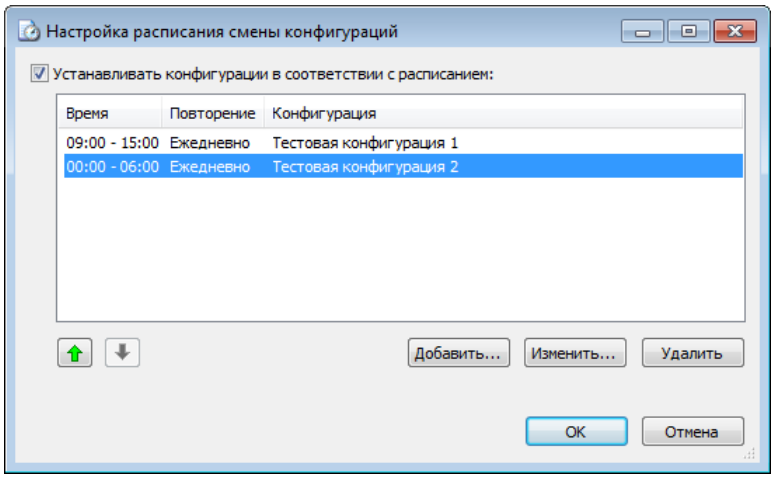



*Рисунок 95. Сформированное расписание смены конфигураций*

Чтобы установка конфигураций перестала производиться автоматически в соответствии с расписанием, в окне **Настройка расписания смены конфигурации** снимите соответствующий флажок.

Чтобы перед каждой сменой конфигурации по расписанию производилось оповещение, в настройках программы в разделе **Предупреждения** установите флажок **Выдавать предупреждение перед сменой конфигурации по расписанию**.

# Запуск программы удаленного доступа

Программа ViPNet Монитор позволяет получить удаленный доступ к сетевому узлу ViPNet с помощью внешних программ, таких как Remote Administrator (Radmin), VNC или Remote Desktop Connection. Удаленный доступ к сетевому узлу может потребоваться администратору этого узла, если физический доступ к компьютеру затруднен, или пользователю, например, для работы на компьютере, находящемся в офисе, из дома.

Чтобы запустить программу удаленного доступа:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. Щелкните правой кнопкой мыши сетевой узел, к которому требуется получить удаленный доступ, в контекстном меню выберите пункт **Внешние программы**, затем выберите команду запуска нужной программы удаленного доступа.

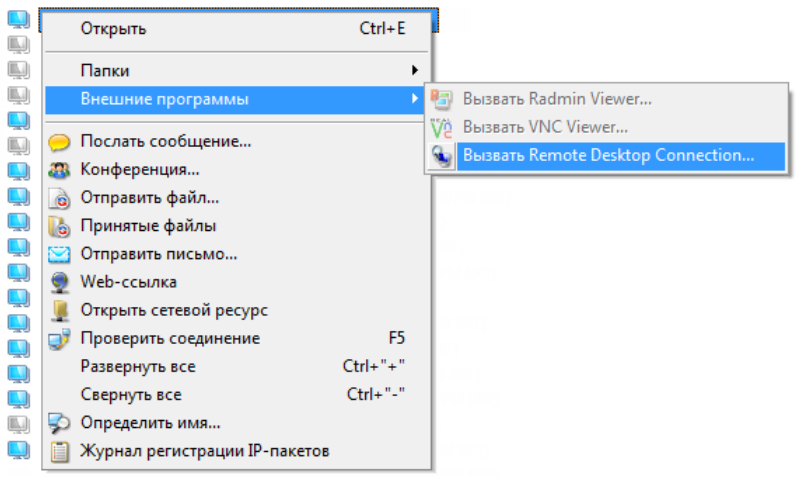



*Рисунок 96. Вызов внешней программы*

Команды подменю **Внешние программы** активны, только если на компьютере установлены соответствующие программы (см. «Установка программного обеспечения для удаленного управления» на стр. 212). Кроме того, выбранный сетевой узел должен иметь ненулевой IP-адрес доступа, и на этом узле должно быть установлено, запущено и настроено соответствующее серверное программное обеспечение (например, Radmin Server, VNC Server).

**Примечание.** При использовании программы Remote Desktop установка серверного программного обеспечения не требуется. С помощью Remote Desktop можно получить удаленный доступ к любому сетевому узлу ViPNet, работающему под управлением ОС Windows.

При соблюдении указанных условий откроется окно соединения. Если соединение установлено, появится окно ввода пароля доступа к выбранному узлу. После успешного ввода пароля откроется окно с отображением рабочего стола удаленного сетевого узла.

**Примечание.** Следует иметь в виду, что для успешного подключения к сетевому узлу ViPNet требуется правильно настроить используемое для удаленного доступа программное обеспечение.

Например, при использовании программы Remote Desktop на сетевом узле, к которому осуществляется подключение, должны быть выполнены следующие настройки:

- В свойствах системы должно быть разрешено удаленное подключение к компьютеру.
- Учетная запись внешнего пользователя должна быть добавлена в список удаленных пользователей.

# Установка программного обеспечения для удаленного управления

Если вы хотите осуществлять удаленное подключение к сетевым узлам ViPNet с помощью внешних программ Remote Administrator (Radmin), VNC или Remote Desktop Connection, то убедитесь, что указанные программы установлены на вашем компьютере.

Получить установочные комплекты данных программ вы можете, загрузив их со следующих страниц:

- Remote Administrator — со страницы Radmin http://www.radmin.com/download/. Пакет Remote Administrator включает клиентскую и серверную части.
- VNC — со страницы RealVNC http://www.realvnc.com/download.html. Пакет VNC включает клиентскую и серверную части.
- Remote Desktop Connection — с веб-сайта Microsoft http://www.microsoft.com/ru-ru/download/details.aspx?id=856. Программа Remote Desktop Connection установлена по умолчанию в операционных системах Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8. Устанавливать подключения можно с компьютеров, использующих любые версии указанных операционных систем. Однако подключаться можно только к компьютерам, использующим версии «Корпоративная», «Профессиональная» и «Максимальная». Подробная информация содержится на веб-сайте Microsoft http://windows.microsoft.com/ru-ru/windows-8/remote-desktop-connection-frequently-asked-questions.

# Настройка терминального сервера при удаленном управлении

Во время работы в терминальной сессии (например, при подключении к серверу с помощью программы Remote Desktop Connection) может возникнуть ситуация, когда после выхода из терминальной сессии программа ViPNet Монитор автоматически выгружается из памяти удаленного сервера и защита IP-трафика отключается. Если это произойдет на координаторе, у всех сетевых узлов ViPNet, использующих этот координатор в качестве межсетевого экрана или сервера IP-адресов, возникнут сбои подключения.

Эта проблема возникает, если терминальный сервер настроен таким образом, чтобы завершать все приложения пользователя после его выхода из терминальной сессии. На рисунке ниже показаны настройки в оснастке **Настройка служб терминалов**, которые приводят к нежелательному завершению программы ViPNet Монитор.

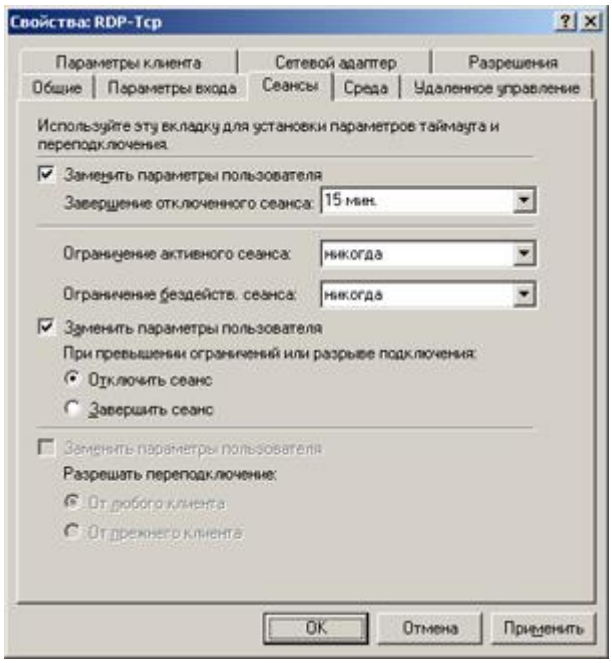



*Рисунок 97. Неверные настройки терминального сервера*

Для решения проблемы следует вернуть все настройки в состояние по умолчанию, сняв все флажки **Заменить параметры пользователя**.

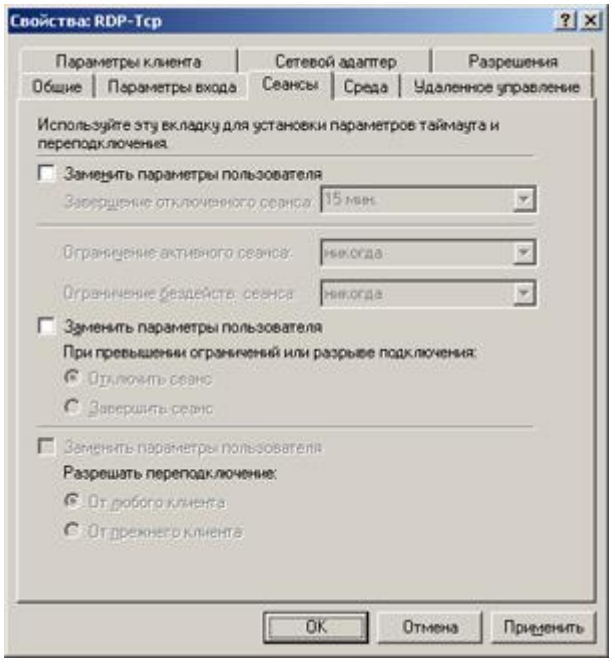



*Рисунок 98. Верные настройки терминального сервера*

**Примечание.** В операционной системе Windows Server 2008 R2 службы терминалов называются службами удаленных рабочих столов.

# Настройка автоматического входа в ОС и программу ViPNet Монитор

При администрировании удаленных компьютеров или компьютеров, физический доступ к которым по каким-либо причинам затруднен, возникает необходимость после перезагрузки выполнять автоматический вход в операционную систему и запуск программы ViPNet Монитор. Это представляет определенные трудности, так как перед загрузкой операционной системы и инициализацией драйвера ViPNet требуется ввести пароль пользователя сетевого узла.

Чтобы на сетевом узле вход в систему и запуск программы ViPNet Монитор осуществлялся автоматически, выполните на нем следующие действия:

1. Настройте параметры автоматического входа в ОС Windows (см. «Настройка автоматического входа в ОС Windows» на стр. 215).
2. В программе ViPNet Монитор:
   - Настройте параметры сохранения пароля при входе в программу. Для этого войдите в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 219). В меню **Сервис** выберите пункт **Настройка параметров безопасности** и в появившемся окне на вкладке **Администратор** установите флажок **Разрешить сохранение пароля в реестре** (см. «Дополнительные настройки параметров безопасности» на стр. 224).

**Примечание.** Подразумевается, что на удаленном узле используется аутентификация пользователя по паролю (см. «Способы аутентификации пользователя» на стр. 70).

- Включите опцию автоматической блокировки компьютера при запуске программы (см. «Настройка параметров запуска и аварийного завершения программы ViPNet Монитор» на стр. 232). Это поможет предотвратить несанкционированный доступ к компьютеру.

**Внимание!** Данные настройки должен выполнять пользователь, обладающий правами администратора в ОС Windows. При необходимости их можно выполнить в удаленной сессии.

В результате для загрузки операционной системы и инициализации драйвера ViPNet не требуется никаких действий пользователя.

## Настройка автоматического входа в ОС Windows

Для настройки автоматического входа в ОС Windows:

1. Нажмите сочетание клавиш **Win**+**R**.

   В меню **Пуск** (**Start**) также можно выбрать пункт **Выполнить** (**Run**).

2. В появившемся окне в поле **Открыть** (**Open**) введите команду `control userpasswords2` и нажмите кнопку **OK**.

   При использовании ОС Windows Vista/Server 2008/Windows 7 также можно использовать команду `netplwiz`.

3. В окне **Учетные записи пользователей** (**User Accounts**) выполните следующие действия:

   - На вкладке **Пользователи** (**Users**) в списке выберите пользователя, под учетной записью которого будет осуществляться вход в ОС и снимите флажок **Требовать ввод имени пользователя и пароля** (**Users must enter a username and password to use this computer**).

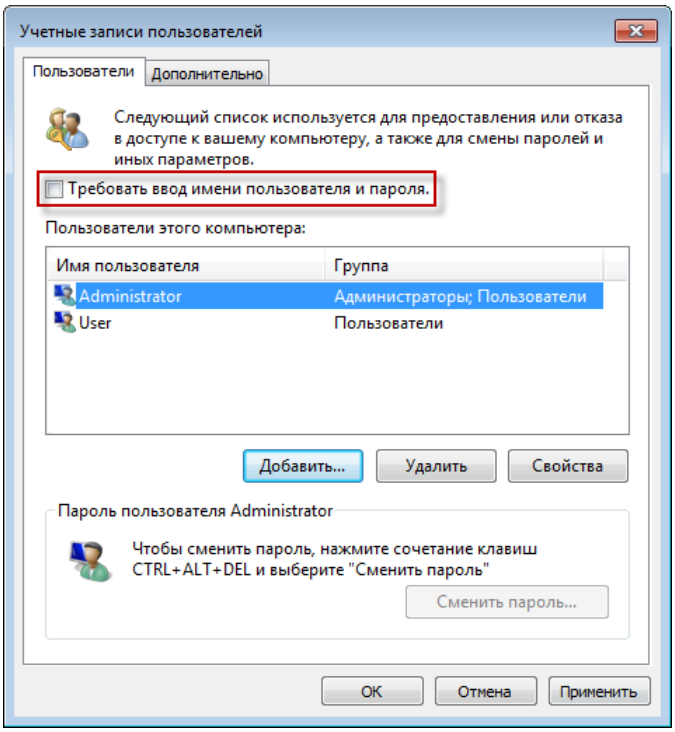



*Рисунок 99. Настройка автоматического входа в ОС на вкладке Пользователи*

- На вкладке **Дополнительно** (**Advanced**) снимите флажок **Требовать нажатия CTRL+ALT+DELETE** (**Require users to press Ctrl+Alt+Delete**).

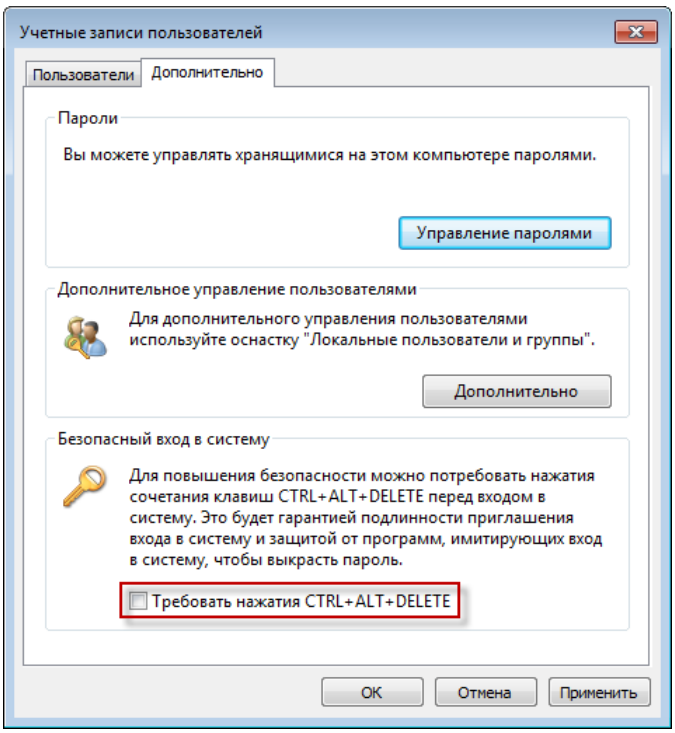



*Рисунок 100. Настройка автоматического входа в ОС на вкладке Дополнительно*

**Примечание.** Если компьютер находится в домене, то указанные флажки могут отсутствовать или быть недоступными в соответствии с групповой политикой безопасности. В этом случае для настройки автоматического входа в ОС потребуется правка реестра вручную.

Неправильное редактирование реестра может привести к возникновению неполадок в работе операционной системы, поэтому обязательно создайте резервную копию реестра. Это позволит восстановить реестр при возникновении неполадок.

Если отсутствует или недоступен флажок **Требовать ввод имени пользователя и пароля (Users must enter a username and password to use this computer**), то в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` задайте следующие значения параметрам:

- `AutoAdminLogon` — 1 («истина»). Данный параметр необходим для включения опции автоматического входа в ОС. При значении 0 автоматический вход в ОС выключен.
- `DefaultDomainName` — имя домена, в который входит компьютер пользователя.
- `DefaultUserName` — имя пользователя, под учетной записью которого будет осуществлять автоматический вход в ОС.
- `DefaultPassword` — пароля пользователя. Если значение этому параметру не будет присвоено, то значение параметра `AutoAdminLogon` автоматически изменится на 0 («ложь»), что не позволит осуществлять автоматический вход в ОС.

При отсутствии указанных параметров создайте их вручную, используя строковый тип (**REG_SZ**).

Если отсутствует или недоступен флажок **Требовать нажатия CTRL+ALT+DELETE (Require users to press Ctrl+Alt+Delete)**, то в разделе ветки реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` параметру `Disablecad` присвойте значение 1 («истина»). При отсутствии данного параметра создайте его вручную, используя тип **DWORD**.

- Нажмите кнопку **Применить** (**Apply**).

4 В окне **Автоматический вход в систему** (**Automatically Log On**) введите пароль и нажмите кнопку **OK**.

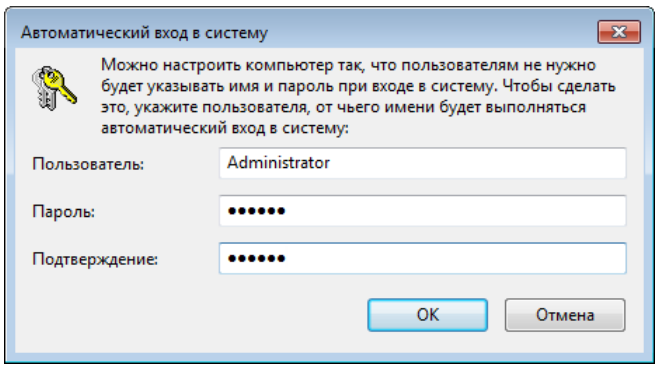



*Рисунок 101. Окно ввода пароля для автоматического входа в систему*

В результате при последующих запусках компьютера вход в ОС будет производиться под учетной записью выбранного пользователя, без ввода пароля и нажатия сочетания клавиш **Ctrl**+**Alt**+**Delete**.

# Работа в программе в режиме администратора

В программе ViPNet Монитор предусмотрена возможность работы в режиме администратора. В данном режиме доступны следующие дополнительные функции и настройки:

- Раздел **Администратор**, который появляется на панели навигации главного окна программы и в котором можно выполнить дополнительную настройку сетевого узла ViPNet (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220).
- Журнал событий, содержащий записи о различных действиях, совершенных пользователем или администратором (см. «Просмотр журнала событий» на стр. 227).
- Возможность просмотреть журнал IP-пакетов определенного сетевого узла ViPNet (см. «Просмотр журнала IP-пакетов другого сетевого узла» на стр. 200).
- Возможность просмотра и изменения конфигураций программы ViPNet Монитор (см. «Управление конфигурациями программы» на стр. 206), созданных всеми пользователями сетевого узла.

При работе в режиме администратора снимаются все ограничения, накладываемые уровнем полномочий пользователя.

Чтобы войти в программу в режиме администратора:

1 Выполните одно из действий:

   - В окне программы ViPNet Монитор в меню **Файл** выберите пункт **Войти в режим администратора**.
   - В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка параметров безопасности**.

     В окне **Настройка параметров безопасности** откройте вкладку **Администратор** и нажмите кнопку **Вход в режим администратора**.

2 В окне **Вход в режим администратора** введите пароль администратора сетевого узла ViPNet.

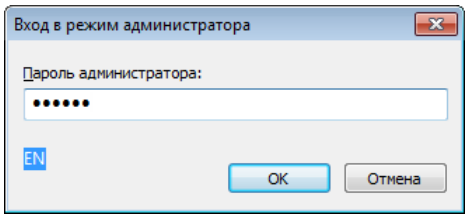



*Рисунок 102. Ввод пароля администратора сетевого узла*

3 Нажмите кнопку **OK**.

   Если введен верный пароль, будет выполнен перезапуск программы и станут доступны дополнительные настройки.

**Внимание!** В сети ViPNet, управляемой с помощью ПО ViPNet Administrator, пароли администратора для каждого сетевого узла создаются в программе ViPNet Удостоверяющий и ключевой центр.

В сети ViPNet, управляемой с помощью ПО ViPNet Network Manager, пароль администратора для всех сетевых узлов хранится в файле `ViPNet_a.txt`, который автоматически создается в папке с наборами ключей при их сохранении.

# Дополнительные настройки программы ViPNet Монитор

После входа в ViPNet Монитор в режиме администратора сетевого узла на панели навигации окна программы появляется раздел **Администратор**. В этом разделе можно настроить ряд дополнительных параметров. Для настройки этих параметров:

1 Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 219).

2 В окне программы ViPNet Монитор на панели навигации выберите раздел **Администратор**.

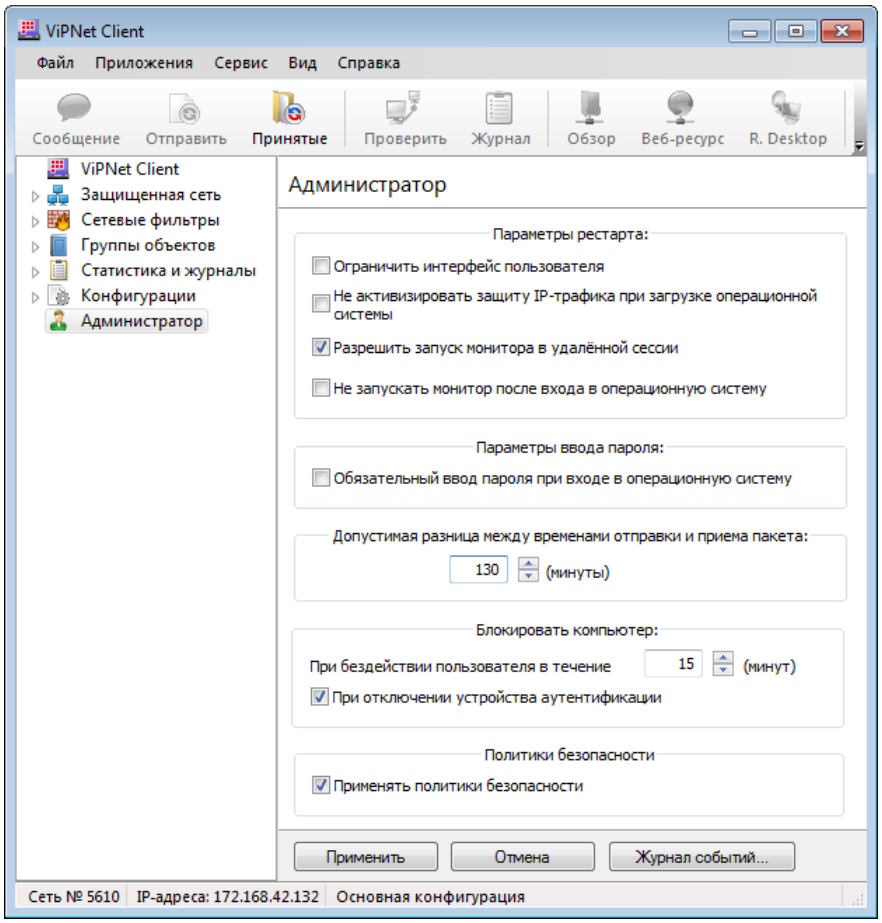



*Рисунок 103. Настройка дополнительных параметров в режиме администратора*

3 Для изменения параметров программы ViPNet Монитор следуйте указаниям следующих разделов:

   - Ограничение интерфейса пользователя (на стр. 221).
   - Параметры запуска программы (на стр. 222).
   - Параметры блокировки компьютера (на стр. 223).
   - Параметры защиты трафика (на стр. 223).

4 Чтобы сохранить настройки, нажмите кнопку **Применить**. Чтобы отказаться от изменений, нажмите кнопку **Отмена**.

## Ограничение интерфейса пользователя

Если вы хотите ограничить возможность изменения параметров программы ViPNet Монитор и скрыть панели навигации, в разделе **Администратор** (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220) установите флажок **Ограничить интерфейс пользователя**.

**Примечание.** Если для сетевого узла задан специальный уровень полномочий 3, данный флажок установлен по умолчанию и его невозможно снять.

Если этот флажок установлен, в программе ViPNet Монитор действуют следующие ограничения:

- В окне программы отображается только панель просмотра со списком сетевых узлов ViPNet.
- В меню **Файл** отсутствует пункт **Сменить пользователя**, но при этом доступны пункты **Сменить пароль пользователя** и **Сменить способ аутентификации пользователя**. Сменить пароль можно только на случайный пароль на основе парольной фразы.

  Пункт **Конфигурации** в меню **Файл** присутствует только в том случае, если в программе создано несколько конфигураций. С помощью данного пункта можно только переключать конфигурации. Пункты **Отключить защиту** и **Блокировать IP-трафик** в нем отсутствуют.

  Пользователь не имеет возможности создавать новые конфигурации. Если в режиме администратора сетевого узла будут созданы новые конфигурации, то они будут доступны пользователю. Если сетевой узел имеет связь с сервером открытого Интернета, на этом узле доступна конфигурация «Открытый Интернет».
- Недоступен пункт меню **Сервис**, в связи с этим невозможно изменение, сохранение и восстановление настроек программы ViPNet Монитор, а также изменение настроек параметров безопасности.
- В окне **Проверка соединения** отображаются только столбцы **Узел**, **Статус** и **Активность на компьютере**.
- Программа ViPNet MFTP запускается и работает в скрытом режиме. Открыть программу из меню **Приложения** нельзя, соответственно, ее настройка также невозможна.

## Параметры запуска программы

Чтобы изменить дополнительные параметры запуска программы ViPNet Монитор, в разделе **Администратор** (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220) выполните следующие действия:

- Если вы хотите отключить защиту трафика с помощью программного обеспечения ViPNet, установите флажок **Не активизировать защиту IP-трафика при загрузке операционной системы** и флажок **Не запускать монитор после входа в операционную систему**. В этом случае при загрузке Windows не будут выполняться аутентификация пользователя ViPNet, и будет невозможен доступ к домену, контроллер которого является защищенным или туннелируемым. Также будет невозможно автоматическое подключение к сетевым защищенным или туннелируемым ресурсам. Однако вы сможете восстановить подключение к защищенным ресурсам вручную после запуска программы ViPNet Монитор.

  **Внимание!** Не рекомендуется устанавливать флажок **Не активизировать защиту IP-трафика при загрузке операционной системы** на координаторах, а также на клиентах, которые имеют динамический IP-адрес или должны взаимодействовать с узлами, имеющими динамический IP-адрес. В противном случае может быть нарушено взаимодействие координаторов с защищенными узлами сети ViPNet.

- Если вы хотите запретить пользователям, имеющим учетные записи на данном компьютере, запускать программу ViPNet Монитор во время сеанса удаленной работы (например, с помощью Remote Desktop), снимите флажок **Разрешить запуск монитора в удаленной сессии**. По умолчанию этот флажок установлен.

  Эта функция доступна, только если на компьютере установлено программное обеспечение для удаленной работы.

  **Примечание.** На компьютере может быть запущен только один экземпляр программы ViPNet Монитор. Если программа запущена в сеансе работы другого пользователя, с помощью Диспетчера задач Windows завершите процесс `Monitor.exe`, затем запустите программу ViPNet Монитор.

- Если вы хотите, чтобы после загрузки Windows защита трафика была включена, но программа ViPNet Монитор не запускалась, установите флажок **Не запускать монитор после входа в операционную систему**. В этом случае после загрузки Windows будет загружен только ViPNet-драйвер, защита компьютера будет активна.
- Если вы хотите, чтобы при загрузке Windows пользователь не мог отказаться от запуска программы ViPNet Монитор, установите флажок **Обязательный ввод пароля при входе в операционную систему**. В этом случае в окне входа в программу кнопка **Отмена** будет недоступна.

**Примечание.** Если установлен флажок **Не активизировать защиту IP-трафика при загрузке операционной системы**, параметр **Обязательный ввод пароля при входе в операционную систему** не учитывается.

## Параметры блокировки компьютера

Если требуется, в разделе **Администратор** (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220) в группе **Блокировать компьютер** вы можете изменить параметры блокировки компьютера:

- По умолчанию в программе ViPNet Монитор включена автоматическая блокировка компьютера в случае бездействия пользователя. Если в течение заданного интервала времени не будут использоваться клавиатура и мышь, компьютер будет автоматически заблокирован.

  При необходимости в поле **При бездействии пользователя в течение** измените продолжительность интервала блокировки в минутах (по умолчанию задано значение 15 минут). Чтобы отключить автоматическую блокировку компьютера, укажите значение интервала блокировки, равное 0.

- По умолчанию в программе ViPNet Монитор включена автоматическая блокировка компьютера при отключении внешнего устройства, которое было использовано для аутентификации пользователя. Если вы хотите отключить блокировку компьютера при отключении внешнего устройства, снимите флажок **При отключении устройства аутентификации**.

  Блокировка компьютера при отключении устройства аутентификации действуют только в случае использования способов аутентификации «Пароль на устройстве» и «Устройство» (см. «Способы аутентификации пользователя» на стр. 70). Если используются внешние устройства iButton, Smartcard Athena, Аккорд-5MX (см. «Внешние устройства» на стр. 345), то функция автоматической блокировки не действует.

  Чтобы продолжить работу после автоматической блокировки, необходимо подключить внешнее устройство, ввести пароль пользователя Windows и, не изменяя способ аутентификации, ввести ПИН-код и пароль (если требуется).

**Внимание!** Для снятия блокировки требуется подключить именно то устройство, которое использовалось для входа в программу, и использовать тот же способ аутентификации. При подключении другого устройства или выборе другого способа аутентификации снять блокировку будет невозможно.

## Параметры защиты трафика

При необходимости в разделе **Администратор** (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220) вы можете изменить дополнительные параметры защиты IP-трафика:

- Программное обеспечение ViPNet автоматически блокирует входящие IP-пакеты, если разница между временем их отправки и временем приема больше заданного значения.

Действие данной функции распространяется на сетевые узлы ViPNet, с которыми у данного узла есть связь (эти узлы отображаются в разделе **Защищенная сеть**).

Если требуется, в поле **Допустимая разница между временами отправки и приема пакета** измените допустимый интервал времени между отправкой и приемом пакета в минутах (по умолчанию 120 минут).

**Внимание!** В результате действия данной функции могут быть заблокированы входящие IP-пакеты от сетевых узлов, на которых неправильно установлено системное время.

- При необходимости вы можете отменить на сетевом узле действие политик безопасности, полученных из программы ViPNet Policy Manager. Для этого в группе **Политики безопасности** снимите флажок **Применять политики безопасности**. Например, вы можете отменить действие политик безопасности, чтобы временно отключить ошибочно отправленные на узел сетевые фильтры.

  Если флажок **Применять политики безопасности** будет снят, действие уже принятых политик безопасности будет прекращено (сетевые фильтры, которые были получены в составе политик, будут скрыты и перестанут использоваться), на узел ViPNet Policy Manager будет отправлена информация о том, что на данном узле не будут приниматься новые политики безопасности.

  Если флажок **Применять политики безопасности** впоследствии будет повторно установлен, то действие уже принятых политик и получение новых политик из программы ViPNet Policy Manager будет возобновлено.

# Дополнительные настройки параметров безопасности

Помимо дополнительных параметров настройки в разделе **Администратор**, во время работы в режиме администратора сетевого узла (см. «Работа в программе в режиме администратора» на стр. 219) доступны следующие параметры на вкладке **Администратор** в окне **Настройка параметров безопасности**:

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

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

- **Автоматически входить в ViPNet** — позволяет выполнять вход в ПО ViPNet Монитор без необходимости подтверждения пароля пользователя ViPNet в окне входа в программу. Если флажок установлен, при запуске программы на текущем сетевом узле окно входа в программу не появляется и вход в ПО ViPNet Монитор выполняется автоматически. Это происходит в следующих случаях:
  - при использовании способа аутентификации **Пароль** — если пароль сохранен в реестре, то есть установлен флажок **Разрешить сохранение пароля в реестре**, а в окне входа в программу указан верный пароль и установлен флажок **Сохранить пароль**;
  - при использовании способов аутентификации **Пароль на устройстве** и **Устройство** — если внешнее устройство подключено к компьютеру и в окне входа в программу указан верный ПИН-код и установлен флажок **Сохранить ПИН-код**.
- **Разрешить использование внешних сертификатов** — позволяет использовать сертификаты не только из личного хранилища (хранилища программы), но также из хранилища операционной системы. Это может понадобиться в том случае, если в ПО ViPNet предполагается использовать криптопровайдер другого производителя (например, КриптоПро), а также сертификаты, изданные внешними Удостоверяющими центрами (вне сети ViPNet).
- **Доверять только сертификатам администраторов УЦ ViPNet** — если этот флажок снят, при проверке сертификата поиск корневого сертификата выполняется не только во внутреннем хранилище ПО ViPNet, но и в системных хранилищах **Доверенные корневые центры сертификации** и **Промежуточные центры сертификации**.
- **Игнорировать отсутствие списков аннулированных сертификатов** — этот флажок следует установить, если в системе используются сертификаты, изданные внешними удостоверяющими центрами, так как в таких сертификатах информация о списках аннулированных сертификатов может отсутствовать.

# Изменение способа аутентификации пользователя

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

1 Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 219).

2 В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите кнопку **Изменить**.

3 В окне **Способ аутентификации** выберите один из способов аутентификации. Описание возможных способов аутентификации пользователя приведено в разделе Способы аутентификации пользователя (на стр. 70).

---

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

---

При выборе способа аутентификации по сертификату подключите внешнее устройство и укажите нужный сертификат в списке сертификатов, обнаруженных на устройстве. При возникновении затруднений в выборе сертификата см. раздел Не удается выполнить аутентификацию с помощью сертификата (на стр. 283).

При выборе способа аутентификации по персональному ключу подключите внешнее устройство для сохранения на нем персонального ключа пользователя (см. «Симметричные ключи в ПО ViPNet» на стр. 323). При сохранении на устройство персонального ключа, который является ключом защиты (см. «Ключ защиты» на стр. 399), стоит учитывать следующую особенность. Если пользователь производит процедуры подписи и шифрования внутри сторонних приложений (например, в Microsoft Office), то в этом случае настоятельно рекомендуется его контейнер ключей (на стр. 399) сохранять также на этом устройстве. Иначе подписание и шифрование в сторонних приложениях будет невозможно из-за проблемы с доступом к ключу защиты. Контейнер ключей можно также перенести из текущей папки в другую папку на диске, но в этом случае каждый раз при подписании и шифровании в стороннем приложении вам потребуется вводить пароль.

---

**Внимание!** Если при использовании способа аутентификации **Устройство** внешнее устройство будет отключено, компьютер может быть автоматически заблокирован — в соответствии с настройками, заданными в режиме администратора (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220). Для продолжения работы необходимо вновь подключить это внешнее устройство. При необходимости параметры автоматической блокировки компьютера и IP-трафика могут быть изменены.

---

4 Нажмите кнопку **OK**.

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

В сетях ViPNet, управляемых с помощью ПО ViPNet Administrator, способ аутентификации также может изменить администратор сети в программе ViPNet Удостоверяющий и ключевой центр. Если администратор назначает пользователю способ аутентификации по сертификату, то пользователь в данном случае должен предоставить администратору внешнее устройство с сертификатом и закрытым ключом для регистрации. При этом должны быть соблюдены условия, описанные в примечании в разделе Устройство (на стр. 73). После назначения пользователю нового способа аутентификации администратор вышлет обновление ключей узла. Приняв данное обновление ключей, пользователь сможет выполнить аутентификацию на узле только выбранным способом.

# Просмотр журнала событий

В журнале событий регистрируются действия по изменению настроек программы ViPNet Client:

- Изменение сетевых фильтров.
- Вход пользователя в программу и его выход.
- Вход в режиме администратора.
- Смена конфигурации.
- Другие события.

Данная информация позволяет администратору контролировать соблюдение безопасности.

Для просмотра журнала событий:

1 Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 219).

2 В окне программы ViPNet Монитор на панели навигации выберите раздел **Администратор**.

3 В разделе **Администратор** нажмите кнопку **Журнал событий**.

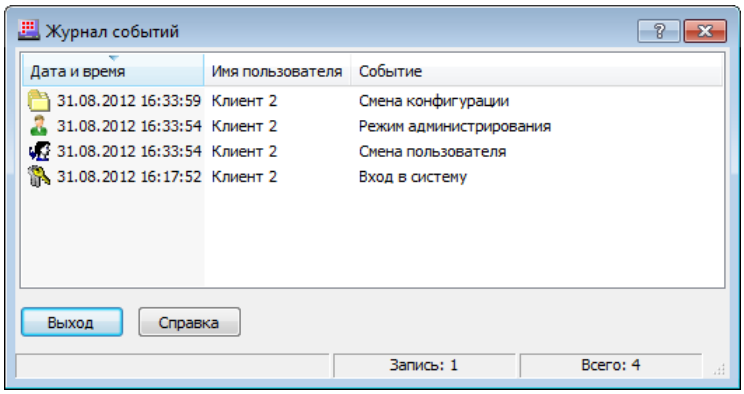



*Рисунок 104. Просмотр журнала событий*

4 Для просмотра журнала событий в формате HTML или XLS в окне **Журнал событий** щелкните любую строку правой кнопкой мыши и в контекстном меню выберите **Просмотр в HTML-**

**формате** или **Просмотр в XLS-формате** (для просмотра журнала в формате XLS на компьютере должна быть установлена программа Microsoft Excel).

Информация о фиксируемых в журнале событиях представлена в таблице ниже:

*Таблица 7. Фиксируемые в журнале события*

| Столбец | Описание |
|---|---|
| **Дата и время** | Когда произошло событие. |
| **Имя пользователя** | Кто являлся инициатором события. |
| **Событие** | Расшифровка событий:<br>•  Вход в систему.<br>•  Выход из системы.<br>•  Режим администратора — при входе в программу с паролем администратора.<br>•  Попытка входа в систему отвергнута (имя пользователя не установлено) — появляется в случае трехкратного неверного ввода пароля пользователя.<br>•  Попытка входа администратора в систему отвергнута (имя пользователя не установлено) — появляется в случае трехкратного неверного ввода пароля администратора.<br>•  Технологический перезапуск — перезагрузка программы после принятия файлов обновления.<br>•  Технологический перезапуск — перезагрузка программы после аварийного завершения.<br>•  Смена пользователя — вход в программу другого пользователя, зарегистрированного на данном сетевом узле.<br>•  Смена конфигурации — смена конфигурации программы в разделе **Конфигурации**.<br>•  Изменение фильтра — любые действия по созданию, редактированию или удалению фильтров.<br>•  Включение или выключение функции «Блокировать все протоколы кроме IP, ARP» — установка или снятие флажка **Блокировать все протоколы, кроме IP, ARP** в окне **Настройка** в разделе **Управление трафиком**.<br>•  Включение или выключение функции «Блокировать компьютер» — установка или снятие флажка **Блокировать компьютер** в окне **Настройка** в разделе **Общие** > **Запуск и аварийное завершение**. |

# Настройка параметров записи событий в журнал Windows

Если в вашей сети ViPNet развернут программный комплекс ViPNet StateWatcher (см. «ПК ViPNet StateWatcher» на стр. 401), вы можете разрешить ПК ViPNet StateWatcher собирать и анализировать дополнительную информацию о событиях на вашем защищенном сетевом узле. В этом случае необходимо включить запись событий, происходящих на сетевом узле ViPNet, в журнал Windows **Приложение**, так как ПК ViPNet StateWatcher при сборе информации о сетевом узле обращается к журналам событий Windows.

**Примечание.** Чтобы пользователи ПК ViPNet StateWatcher могли получать оповещения об этих событиях, администратор ПК ViPNet StateWatcher должен создать соответствующее правило анализа, указав в качестве источника события программное обеспечение ViPNet Client. Дополнительные сведения см. в документе «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher. Сервер мониторинга. Руководство администратора».

В программе ViPNet Монитор предусмотрена запись следующих типов событий в журнал Windows:

- блокирование IP-пакетов (см. «Блокированные IP-пакеты» на стр. 328);
- изменение пользователем защищенного узла настроек сетевых фильтров (см. «Создание сетевых фильтров» на стр. 144);
- несанкционированное изменение настроек сетевых фильтров.

Чтобы включить запись событий программой ViPNet Монитор в журнал Windows **Приложение**, выполните следующие действия:

1. Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 219).
2. В окне программы ViPNet Монитор на панели навигации выберите раздел **Администратор**.
3. В разделе **Администратор** в группе **Журнал событий Windows** установите один или несколько флажков, чтобы выполнялась запись соответствующих событий в журнал Windows:
   - блокирование IP-пакетов;
   - авторизированные изменения в настройках сетевых фильтров;
   - несанкционированные попытки изменить настройки сетевых фильтров.

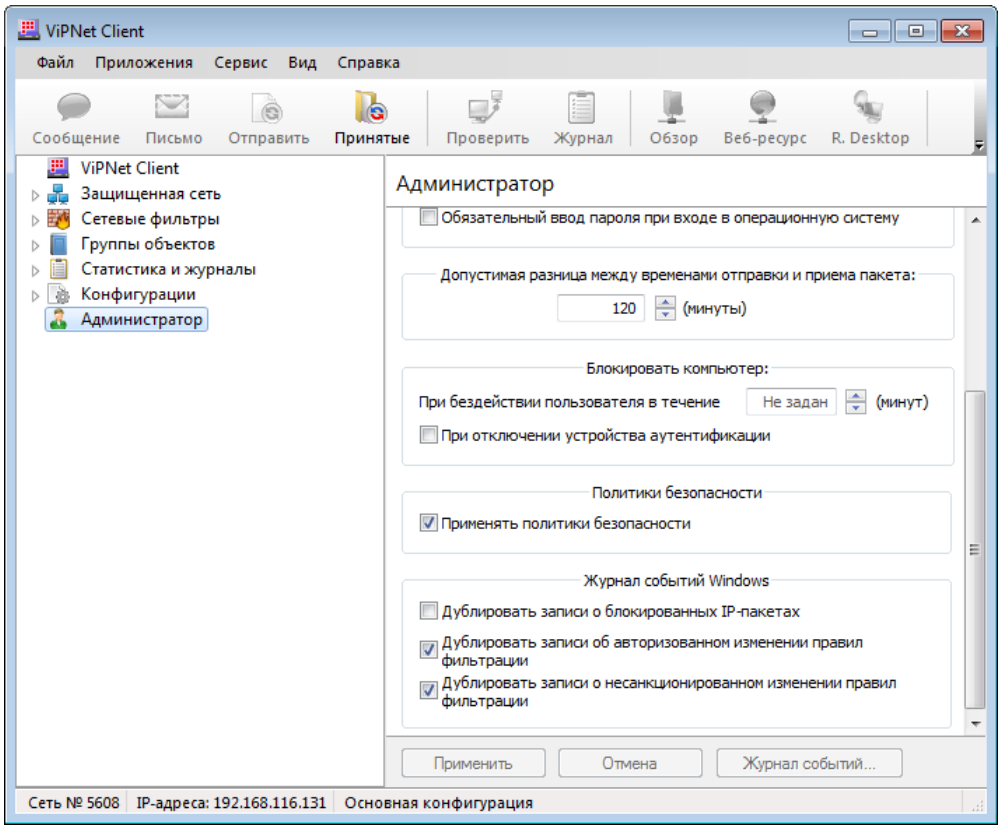



*Рисунок 105. Настройка записи событий в журнале Windows*

4 Нажмите кнопку **Применить**, чтобы начать запись событий в журнал Windows **Приложение**. При этом запись этих событий продолжится и в собственном журнале программы ViPNet Монитор.

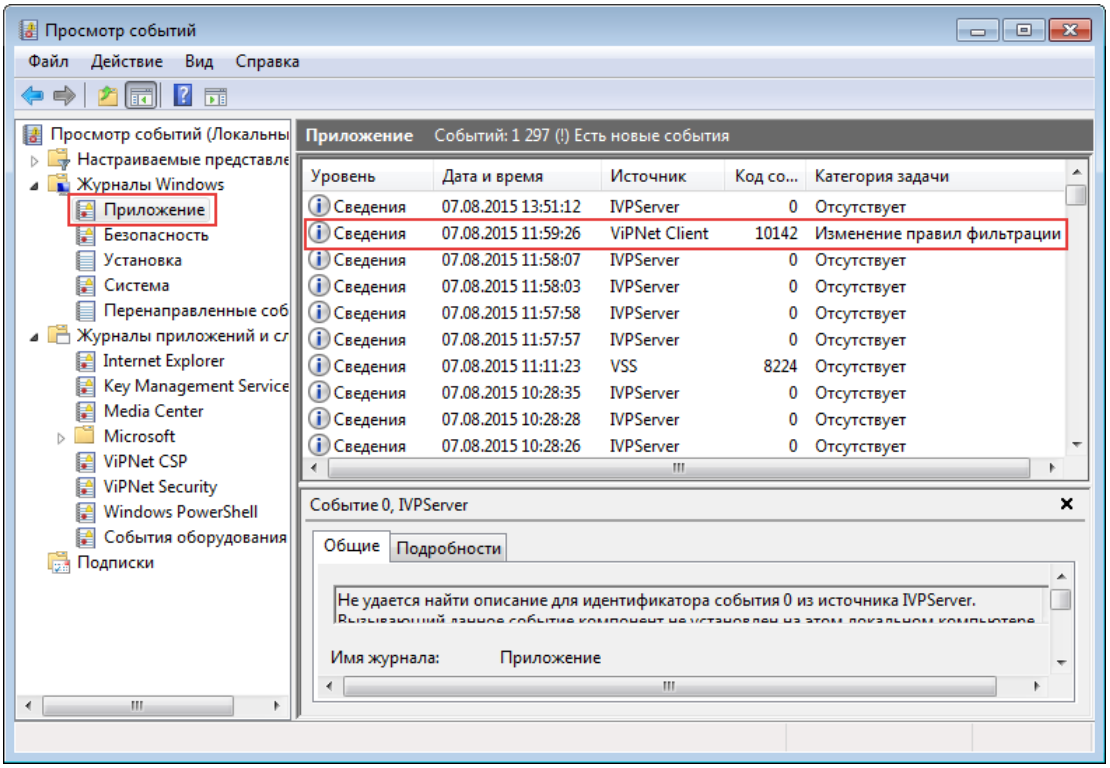



*Рисунок 106. Событие узла ViPNet, сохраненное в журнале Windows Приложение*

**Внимание!** В случае если количество записанных событий будет слишком большим, возникнет угроза переполнения журнала Windows: в зависимости от настроек журнала будут выполняться перезапись событий либо сохранение старых событий в архив. Чтобы избежать этого, проверьте настройки журнала и увеличьте его объем с помощью стандартных настроек журнала событий.

# Настройка параметров запуска и аварийного завершения программы ViPNet Монитор

Для настройки параметров запуска и экстренного завершения программы:

1 В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2 В окне **Настройка** на панели навигации выберите раздел **Общие** > **Запуск и аварийное завершение**.

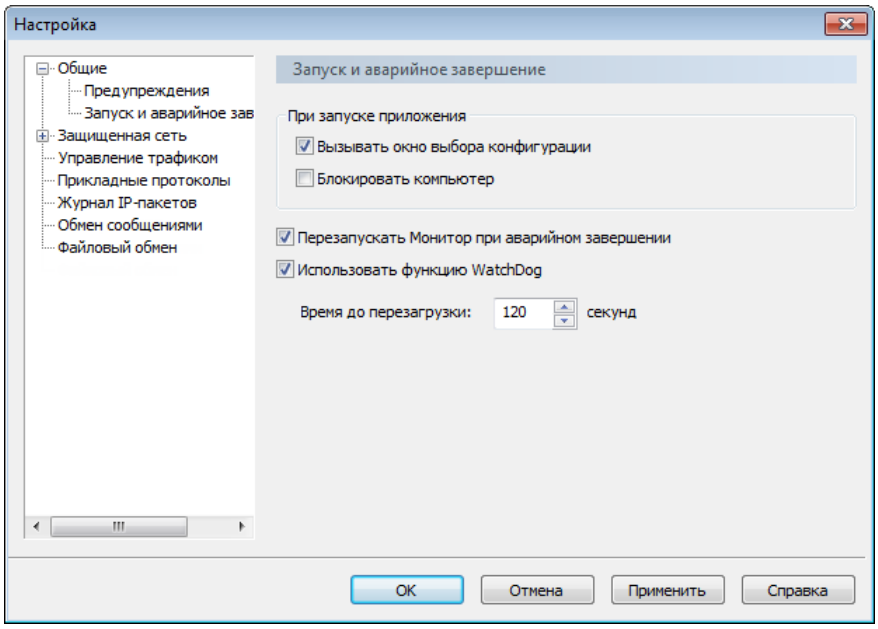



*Рисунок 107. Настройка параметров запуска и аварийного завершения работы программы*

3 Чтобы при запуске программы не производить выбор конфигурации (см. «Управление конфигурациями программы» на стр. 206), снимите флажок **Вызывать окно выбора конфигурации**. При этом запуск программы будет происходить в той конфигурации, которая использовалась в последнем сеансе работы.

Если в программе настроена только одна конфигурация, окно выбора появляться не будет независимо от установки флажка.

4 Чтобы при запуске программы блокировать доступ к рабочему столу компьютера, установите флажок **Блокировать компьютер**. Для разблокирования компьютера введите пароль пользователя Windows.

Данная функция полезна для предотвращения несанкционированной работы с компьютером после его перезагрузки, если настроен автоматический вход пользователя Windows в операционную систему. При этом программа ViPNet Монитор выполняет все функции по защите компьютера.

5 Чтобы отключить возможность перезапуска ViPNet Монитор после аварийного завершения работы программы, снимите флажок **Перезапускать Монитор при аварийном завершении**.

6 Для включения автоматической перезагрузки ОС при сбоях установите флажок **Использовать функцию WatchDog** и в поле **Время до перезагрузки** введите время (в секундах), по истечении которого будет происходить перезагрузка.

Функция WatchDog отслеживает работоспособность программы ViPNet Монитор. Если программа теряет работоспособность в результате какого-либо системного сбоя, WatchDog перезагружает ОС компьютера. Использование WatchDog особенно важно на удаленных компьютерах, доступ к которым проблематичен.

**Примечание.** В 64-разрядных операционных системах функция WatchDog не поддерживается.

# 12

# Настройка параметров безопасности


Смена пароля пользователя 235

Настройка параметров шифрования 239

Настройка параметров криптопровайдера ViPNet CSP 241

# Смена пароля пользователя

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

Смена текущего пароля пользователя требуется в следующих случаях:

- По истечении срока действия текущего пароля (в случае, если этот срок действия ограничен).
- При поступлении на сетевой узел обновления ключей из программы ViPNet Удостоверяющий и ключевой центр, содержащего новый пароль пользователя. В этом случае появится окно с сообщением «Рекомендуется сменить пароль пользователя», однако пароль не будет изменен автоматически, поэтому процедуру смены пароля необходимо выполнить вручную.
- Если контейнер ключей защищен с использованием не пароля, а персонального ключа пользователя, пароль к контейнеру ключей будет совпадать с паролем пользователя. Поэтому при необходимости смены пароля к контейнеру ключей (см. «Смена пароля к контейнеру» на стр. 272), следует сменить пароль пользователя.

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

Для того чтобы сменить пароль пользователя:

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

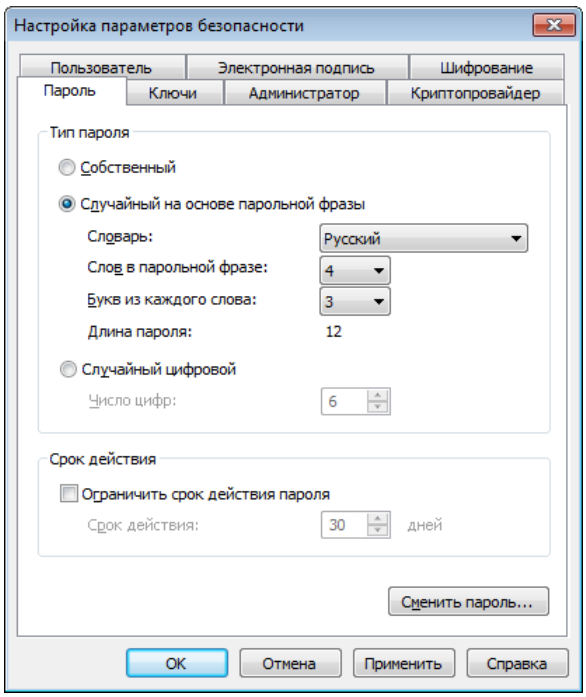



*Рисунок 108. Смена текущего пароля пользователя*

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

- **Собственный** — пароль, определяемый пользователем (см. «Выбор собственного пароля» на стр. 236);
- **Случайный на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы по заданным параметрам (см. «Выбор пароля на основе парольной фразы» на стр. 236);
- **Случайный цифровой** — пароль, формируемый автоматически из заданного числа цифр (см. «Выбор цифрового пароля» на стр. 238).

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

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

5 Нажмите кнопку **OK**.

# Выбор собственного пароля

Для того чтобы сменить текущий пароль пользователя на собственный:

1 На вкладке **Пароль** (см. Рисунок 98 на стр. 235) выберите **Собственный**.

2 Нажмите кнопку **Сменить пароль**.

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

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

4 Нажмите кнопку **OK**.

Теперь при запуске программы ViPNet Монитор 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 98 на стр. 235) выберите **Случайный на основе парольной фразы**, после чего задайте параметры нового пароля:

- В списке **Словарь** выберите язык парольной фразы.

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

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

---

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

---

2 Нажмите кнопку **Сменить пароль**.

3 Выполните действия, предлагаемые в окне **Электронная рулетка**.

---

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

---

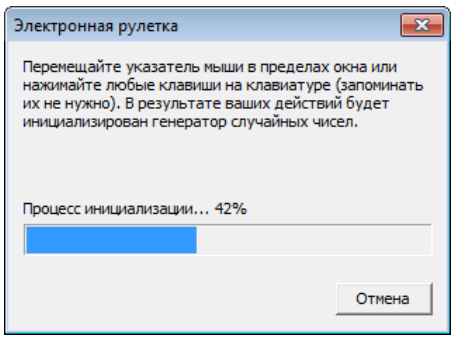



*Рисунок 109. Электронная рулетка*

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

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

Нажмите кнопку **OK**.

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

# Выбор цифрового пароля

Для того чтобы сменить текущий пароль пользователя на цифровой:

1 На вкладке **Пароль** (см. Рисунок 98 на стр. 235) выберите **Случайный цифровой**, после чего в поле **Число цифр** укажите длину пароля.

---

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

---

2 Нажмите кнопку **Сменить пароль**.

3 Выполните действия, предлагаемые в окне **Электронная рулетка** (см. Рисунок 99 на стр. 237).

---

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

---

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

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

Нажмите кнопку **ОК**.

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

# Настройка параметров шифрования

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

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

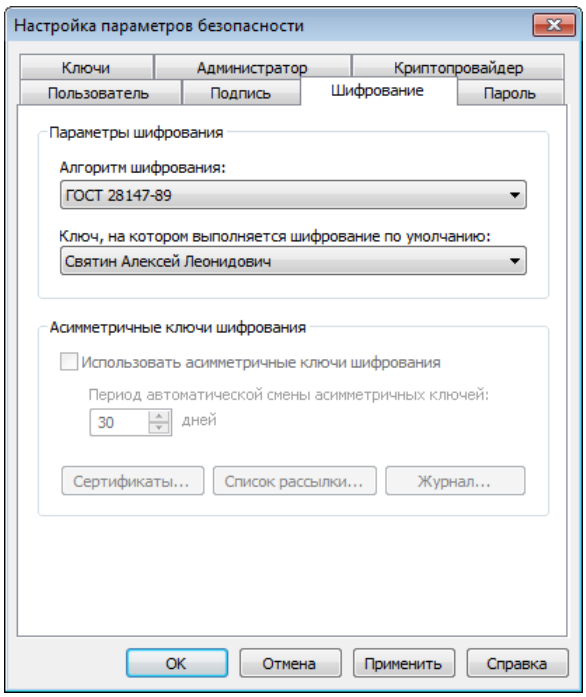



*Рисунок 110. Настройка параметров шифрования*

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

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

По умолчанию выбран алгоритм ГОСТ 28147-89. В соответствии с выбранным алгоритмом будет осуществляться как шифрование исходящего трафика, так и шифрование информации, передаваемой с помощью программы ViPNet Деловая почта (исходящих писем). Расшифрование входящего трафика и писем производится в соответствии с тем алгоритмом, который был задан при их зашифровании отправителем.

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

**Внимание!** В сертифицированной версии программы алгоритм AES не поддерживается. Вы не сможете выбрать этот алгоритм в списке. Кроме этого, входящая информация, зашифрованная на алгоритме AES, на вашем узле также не сможет быть расшифрована.

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

Выбор ключей шифрования позволяет разграничить доступ пользователей, работающих на одном сетевом узле, к зашифрованной переписке в программе ViPNet Деловая почта. То есть если исходящее письмо было зашифровано на ключах, доступных только вам, то другие пользователи, зарегистрированные на вашем узле, его прочитать не смогут.

4 Нажмите кнопку **OK**.

# Настройка параметров криптопровайдера ViPNet CSP

В состав программного обеспечения ViPNet Client включена программа ViPNet CSP. ViPNet CSP представляет собой криптопровайдер, который обеспечивает вызов криптографических функций, реализованных в соответствии с российскими стандартами, через интерфейс Microsoft CryptoAPI 2.0. Это позволяет использовать российские криптографические алгоритмы в различных приложениях Microsoft и других программах, использующих данный интерфейс. Кроме этого, программа ViPNet CSP обеспечивает работу с контейнерами ключей (см. «Контейнер ключей» на стр. 399) и поддержку различных внешних устройств хранения ключей (см. «Внешние устройства» на стр. 345).

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

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

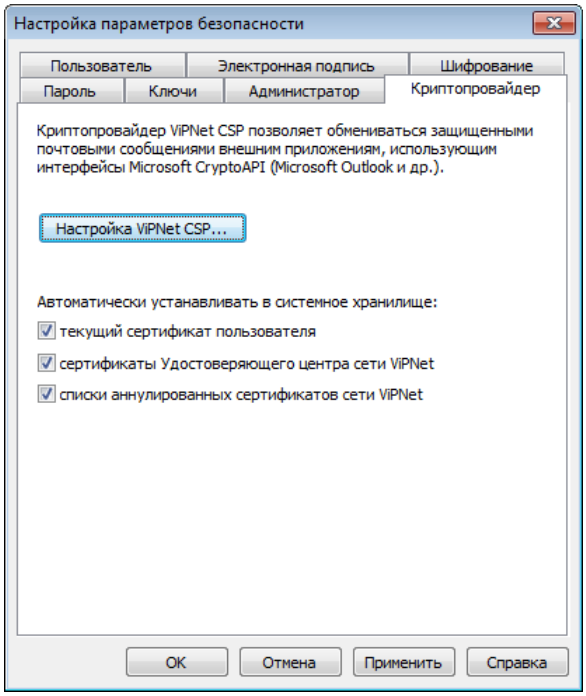



*Рисунок 111. Настройка параметров криптопровайдера ViPNet CSP*

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

- Задать необходимые параметры криптопровайдера ViPNet CSP.
- Выполнить операции с контейнерами ключей.

- Настроить параметры использования внешних устройств хранения данных — задать типы устройств, которые могут использоваться, выполнить инициализацию или изменить ПИН-код устройства.

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

3 При необходимости укажите, какие сертификаты и списки аннулированных сертификатов следует устанавливать в системное хранилище автоматически (см. «Установка в хранилище автоматически» на стр. 250), установив нужные флажки:

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

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

# 13

# Работа с сертификатами и ключами


Просмотр сертификатов 244

Управление сертификатами 249

Работа с контейнером ключей 270

# Просмотр сертификатов

Просмотр сертификата может потребоваться при необходимости получения более подробной информации о сертификате — о назначении сертификата, о его издателе, составе полей, причине недействительности сертификата и так далее. Подробная информация о сертификатах содержится в разделе Общие сведения о сертификатах ключей проверки электронной подписи (на стр. 309).

В программе ViPNet Client можно просматривать следующие типы сертификатов:

- текущий сертификат пользователя (см. «Просмотр текущего сертификата пользователя» на стр. 245),
- личные сертификаты пользователя (см. «Просмотр личных сертификатов пользователя» на стр. 245),
- доверенные корневые сертификаты (см. «Просмотр доверенных корневых сертификатов» на стр. 246),
- изданные сертификаты (см. «Просмотр изданных сертификатов» на стр. 246).

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

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

---

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

---

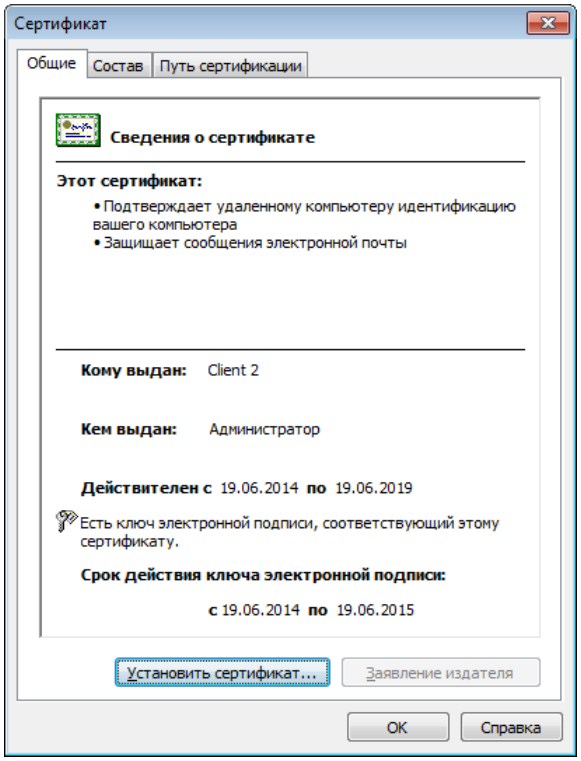



*Рисунок 112. Просмотр основной информации о сертификате*

# Просмотр текущего сертификата пользователя

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

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

# Просмотр личных сертификатов пользователя

Для просмотра личных сертификатов пользователя:

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

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

**Примечание.** Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование внешних сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 224).

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

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

# Просмотр доверенных корневых сертификатов

Для просмотра доверенных корневых сертификатов:

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

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

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

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

# Просмотр изданных сертификатов

Для просмотра изданных сертификатов:

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

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

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

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

# Просмотр цепочки сертификации

Для просмотра цепочки сертификации (см. «Цепочка сертификации» на стр. 404) определенного сертификата:

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

2 Откройте вкладку **Путь сертификации**.

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

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

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

# Просмотр полей сертификата и печать сертификата

Для просмотра полей определенного сертификата:

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

2 Откройте вкладку **Состав**.

По умолчанию на данной вкладке отображается перечень всех полей сертификата.

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

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

---

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

---

- **Только критические расширения** — только те расширения, которые признаны издателем критическими;

- **Только свойства** — параметры, которые не являются полями сертификата, но присваиваются сертификату при хранении его в системном хранилище используемой рабочей станции.

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

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

# Управление сертификатами

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

| Функциональная возможность | Ссылка |
|---|---|
| **Установка сертификатов в хранилище**. Возможна настройка параметров автоматической установки сертификатов в хранилище, а также установка сертификатов в хранилище вручную | Установка в хранилище автоматически (на стр. 250)<br>Установка в хранилище вручную (на стр. 252) |
| **Смена текущего сертификата**. Можно выбрать другой сертификат (из числа действительных личных сертификатов пользователя) в качестве текущего. | Смена текущего сертификата (на стр. 255) |
| **Обновление ключа электронной подписи и сертификата**. Можно настроить параметры автоматического оповещения об истечении срока действия текущего сертификата и соответствующего ему ключа электронной подписи, а также, при необходимости, сформировать запрос на обновление этого сертификата и ключа электронной подписи. | Настройка оповещения об истечении срока действия ключа электронной подписи и сертификата (на стр. 257)<br>Процедура обновления ключа электронной подписи и сертификата (на стр. 257) |
| **Ввод сертификата в действие**. Если требуется использовать сертификат, переданный на данный сетевой узел, необходимо ввести этот сертификат в действие. Можно настроить параметры автоматического ввода сертификатов в действие или выполнить ввод в действие вручную. | Ввод сертификата в действие (на стр. 263)<br>Ввод в действие автоматически (на стр. 264)<br>Ввод в действие вручную (на стр. 264) |
| **Просмотр и удаление запросов на сертификаты**. Можно просмотреть состояние запросов на сертификаты, сформированных текущим пользователем, а также удалить ненужные запросы. | Работа с запросами на сертификаты (на стр. 265)<br>Просмотр запроса на сертификат (на стр. 265)<br>Удаление запроса на сертификат (на стр. 266) |
| **Экспорт сертификата.** В зависимости от целей использования сертификата за пределами ПО ViPNet, сертификат может быть экспортирован в файлы различных форматов. | Экспорт сертификата (на стр. 266) |

# Установка сертификатов в хранилище операционной системы

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

**Внимание!** Для работы с защищенными документами, помимо сертификата пользователя, необходимо также установить в хранилище корневой сертификат (издателя) и список аннулированных сертификатов (см. «Список аннулированных сертификатов (CRL)» на стр. 403).

Установку можно выполнить автоматически или вручную.

**Внимание!** При необходимости установки сертификатов в хранилище ОС Windows Vista или Windows Server 2008 следует запускать программу ViPNet Client 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 аннулированных сертификатов) еще не были установлены в хранилище;
- в окне **Настройка параметров безопасности** на вкладке **Криптопровайдер** установлены флажки группы **Автоматически устанавливать в системное хранилище**.

**Примечание.** В автоматическом режиме выполняется установка сертификатов и списков аннулированных сертификатов в хранилище текущего пользователя.

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

Для установки корневого сертификата необходимо подтверждение этого действия пользователем в окне **Установка корневого сертификата**. Данное окно появляется тогда, когда корневой сертификат отсутствует в хранилище сертификатов Windows. Это может произойти в следующих случаях:

- При первичном запуске ПО ViPNet после развертывания сетевого узла.
- Если совместно с обновлением текущего сертификата пользователя получен новый корневой сертификат.

Для подтверждения автоматической установки корневого сертификата выполните следующие действия:

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

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

---

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

---

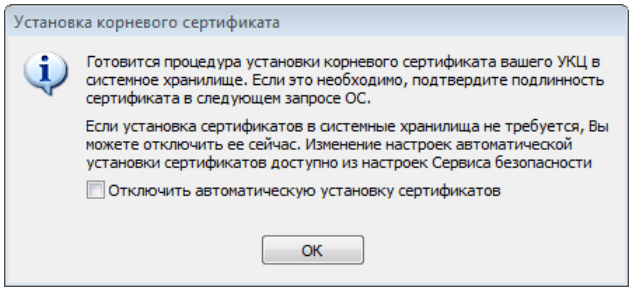



*Рисунок 113. Установка корневого сертификата*

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

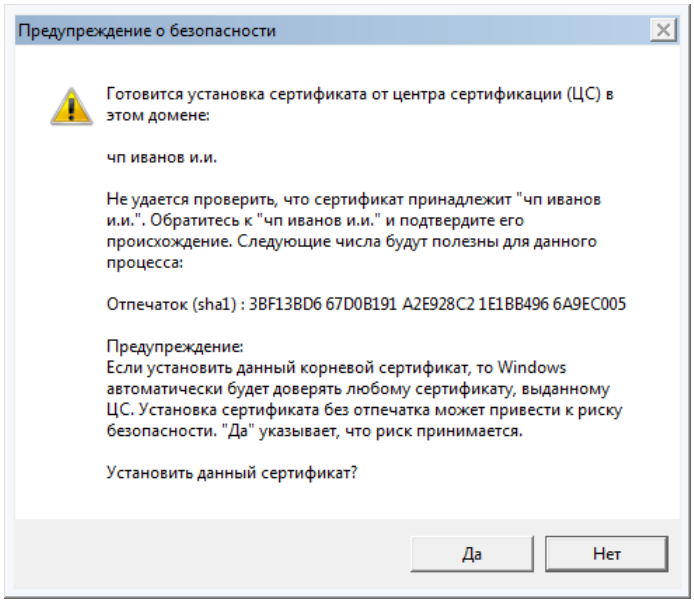



*Рисунок 114. Подтверждение подлинности корневого сертификата*

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

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

Корневой сертификат установлен в хранилище сертификатов текущего пользователя.

## Установка в хранилище вручную

Если изданный сертификат пользователя не был установлен в хранилище автоматически (см. «Установка в хранилище автоматически» на стр. 250), вы можете установить его в хранилище и сопоставить с ключом электронной подписи вручную. Также совместно с сертификатом пользователя вы можете установить в хранилище операционной системы сертификат издателя и список аннулированных сертификатов (CRL).

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

1. В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**.
2. Вызовите окно **Сертификаты** для того сертификата, который необходимо установить в хранилище (см. «Просмотр сертификатов» на стр. 244).
3. Нажмите кнопку **Установить сертификат**.
4. На странице приветствия мастера установки сертификатов нажмите кнопку **Далее**.
5. На странице **Выбор хранилища сертификатов** выполните следующие действия:
   - Укажите, в какое хранилище будет установлен ваш сертификат.
   - Если на сетевой узел кроме сертификата пользователя также поступили сертификаты издателей и CRL, для их установки установите соответствующие флажки.

   Нажмите кнопку **Далее**.

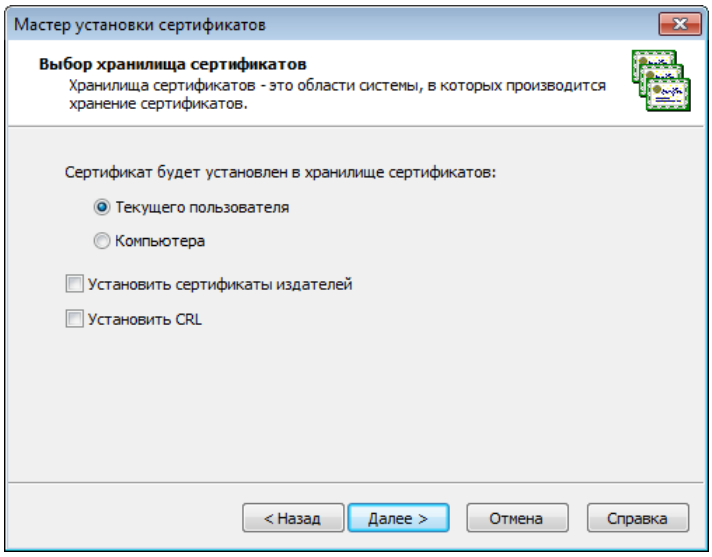



*Рисунок 115. Выбор хранилища сертификатов*

---

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

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

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

---

6 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.

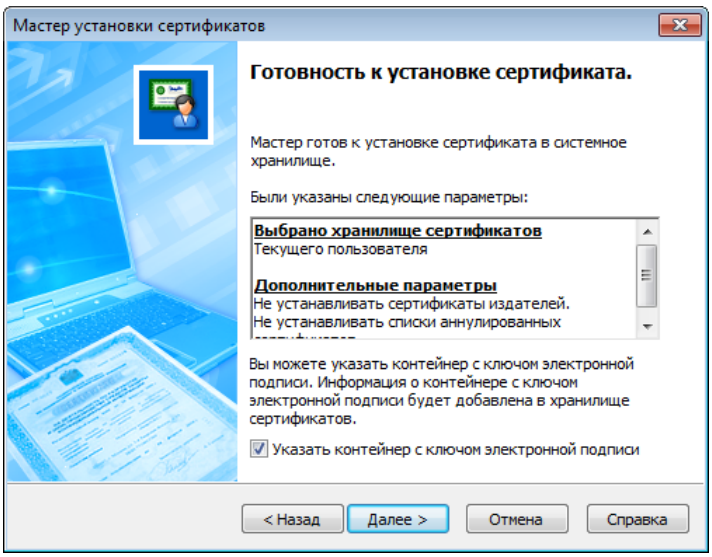



*Рисунок 116. Сертификат готов к установке*

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

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

- Нажмите кнопку **Далее**.

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

- папку на диске;
- устройство (с указанием его ПИН-кода).

> **Примечание.** Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 345).

После этого нажмите кнопку **OK**.

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

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

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

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

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

Сертификат установлен в выбранное хранилище сертификатов. Если в процессе установки сертификата ему не был сопоставлен ключ электронной подписи, необходимо вручную установить сертификат в контейнер ключей (см. «Установка сертификата в контейнер ключей» на стр. 277).

# Смена текущего сертификата

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

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

Для выбора действительного личного сертификата в качестве текущего:

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

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

**Примечание.** Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование внешних сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 224).

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

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

**Примечание.** В качестве текущего можно использовать только тот действительный личный сертификат, который введен в действие. Изданный, но не введенный в действие личный сертификат необходимо сначала ввести в действие (см. «Ввод сертификата в действие» на стр. 263), а затем назначить текущим.

При успешном выполнении описанных действий выбранный сертификат назначается текущим. При этом на вкладке **Ключи** (см. Рисунок 116 на стр. 271) в группе **Электронная подпись** меняется информация о контейнере ключей, в котором хранится выбранный сертификат.

# Обновление ключа электронной подписи и сертификата

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

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

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

Таким образом, требуется обновлять сертификат ключа проверки электронной подписи и ключ электронной подписи не реже, чем 1 раз в год.

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

---

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

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

В случае отсутствия ключа электронной подписи создать запрос на сертификат также невозможно.

---

## Настройка оповещения об истечении срока действия ключа электронной подписи и сертификата

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

Чтобы изменить настройки оповещения, выполните следующие действия:

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

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

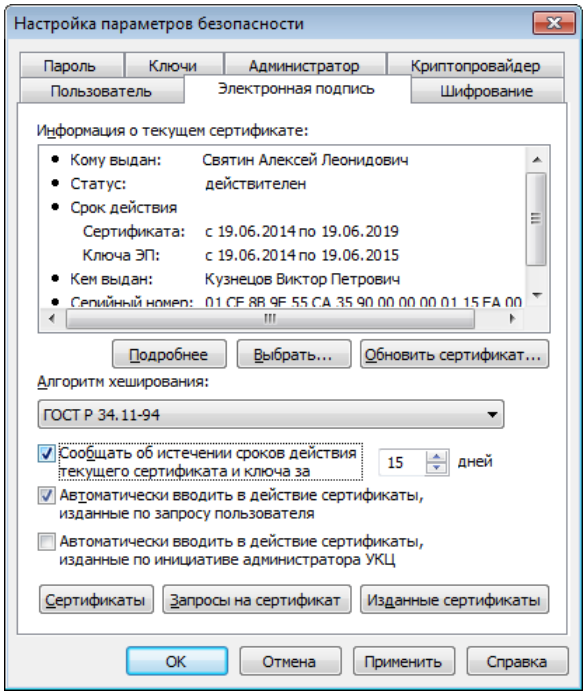



*Рисунок 117. Просмотр информации о текущем сертификате и настройка параметров оповещения об истечении сроков действия ключа электронной подписи и сертификата*

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

## Процедура обновления ключа электронной подписи и сертификата

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

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

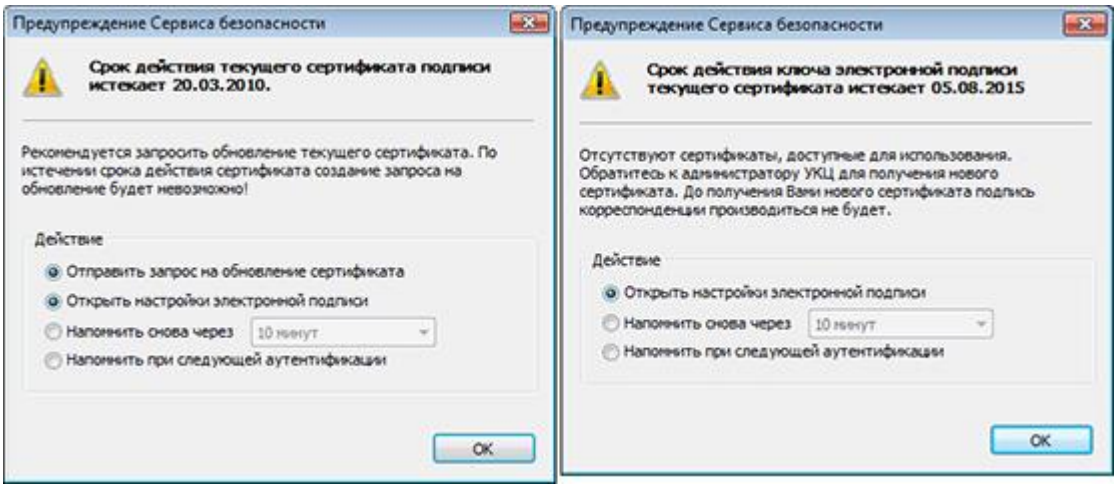



*Рисунок 118. Предупреждения о скором истечении срока действия сертификата и ключа электронной подписи*

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

---

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

---

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

- Если оповещение об истечении срока действия сертификата и ключа электронной подписи отключено:
  - В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**.
  - На вкладке **Электронная подпись** (см. Рисунок 107 на стр. 257) нажмите кнопку **Обновить сертификат**. Будет запущен **Мастер обновления сертификата**.

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

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

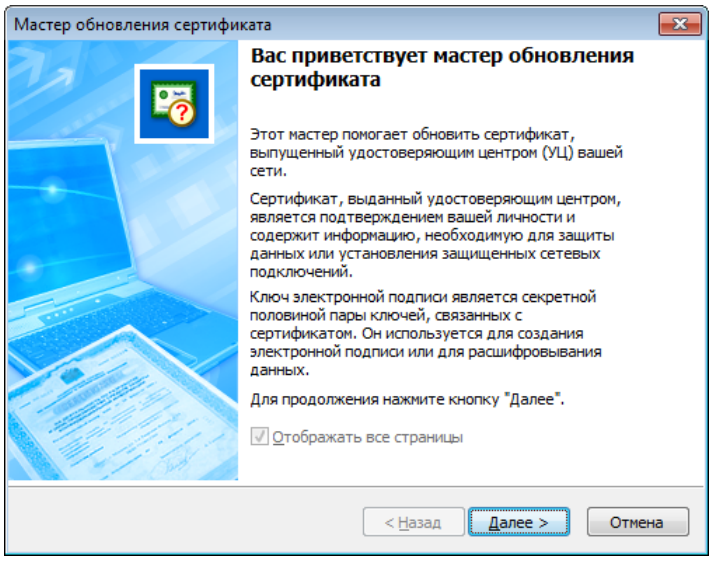



*Рисунок 119. Стартовая страница мастера обновления сертификата*

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

**2.1** Укажите назначение ключа и сертификата:

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

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

*Таблица 8. Характеристики алгоритмов*

| Алгоритм и его описание | Параметры алгоритма | Длина ключа проверки электронной подписи |
|---|---|---|
| ГОСТ Р 34.10-2001<br>См. RFC 4357 http://www.ietf.org/rfc/rfc4357.txt<br>Стандарт электронной подписи, основанный на арифметике эллиптических кривых<br>OID «1.2.643.2.2.19» | **Для подписи:**<br>ГОСТ Р 34.10 - 2001. Параметры по умолчанию (рекомендуется)<br>OID «1.2.643.2.2. 35.1»<br>ГОСТ Р 34.10 - 2001 Параметры подписи B<br>OID «1.2.643.2.2. 35.2»<br>ГОСТ Р 34.10 - 2001. Параметры подписи C<br>OID «1.2.643.2.2. 35.3»<br>**Для подписи и шифрования:**<br>ГОСТ Р 34.10 - 2001. EDH Параметры по умолчанию (рекомендуется)<br>OID «1.2.643.2.2. 36.0» | 512 |

| Алгоритм и его описание | Параметры алгоритма | Длина ключа проверки электронной подписи |
|---|---|---|
| | ГОСТ Р 34.10 - 2001. EDH Параметры обмена 2<br>OID «1.2.643.2.2. 36.1» | |
| ГОСТ Р 34.10-2012/512<br>Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 256 бит<br>OID «1.2.643.7.1.1.1.1» | ГОСТ Р 34.10 - 2001. Параметры по умолчанию (рекомендуется)<br>OID «1.2.643.2.2. 35.1»<br>ГОСТ Р 34.10 - 2001 Параметры подписи B<br>OID «1.2.643.2.2. 35.2»<br>ГОСТ Р 34.10 - 2001. Параметры подписи C<br>OID «1.2.643.2.2. 35.3» | 512 |
| ГОСТ Р 34.10-2012/1024<br>Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 512 бит<br>OID «1.2.643.7.1.1.1.2» | ГОСТ Р 34.10 - 2012/1024. Набор параметров A | 1024 |

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

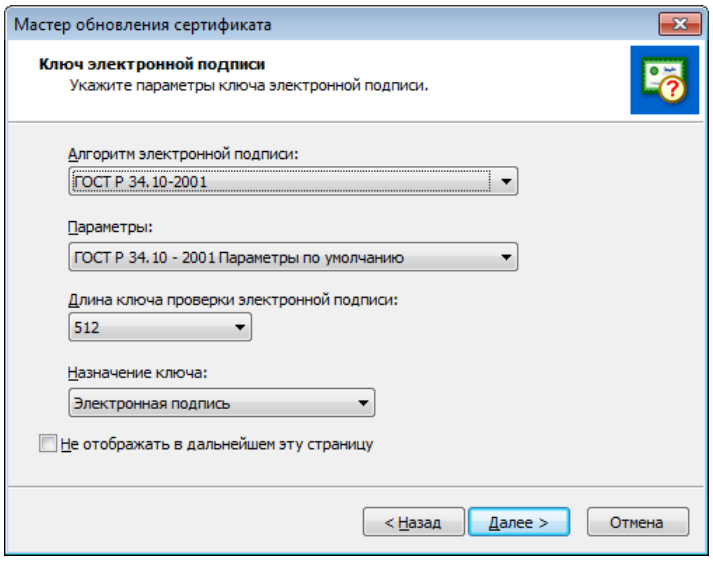



*Рисунок 120. Выбор алгоритма и его параметров*

**2.3** Нажмите кнопку **Далее**.

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

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

---

**Примечание.** Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 345).

---

После этого нажмите кнопку **Далее**.

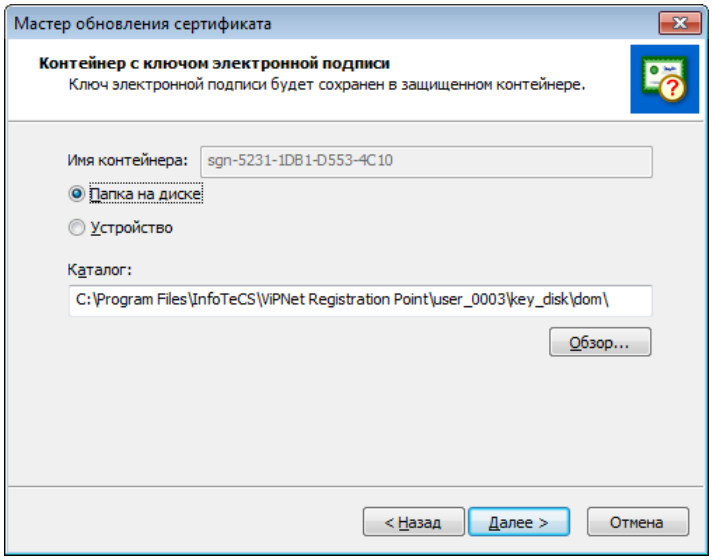



*Рисунок 121. Указание места хранения контейнера ключей*

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

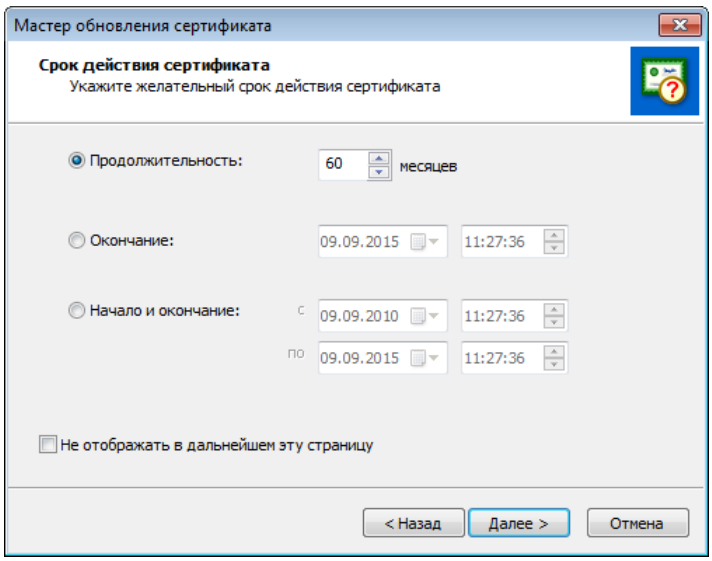



*Рисунок 122. Указание желаемого срока действия сертификата*

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

- Убедитесь в правильности параметров, заданных на предыдущих страницах мастера. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.
- При необходимости печати информации о запросе на принтере, используемом по умолчанию на данном сетевом узле, убедитесь в том, что установлен флажок **Печатать информацию о запросе**. В противном случае снимите флажок.

После этого нажмите кнопку **Далее**.

6 При появлении электронной рулетки следуйте указаниям окна.

---

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

---

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

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

---

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

---

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

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

**Внимание!** Если контейнер с ключом электронной подписи хранится в папке на диске, то он доступен всегда. Если контейнер хранится на внешнем устройстве, то он будет доступен только в том случае, если устройство подключено и сохранен ПИН-код к нему.

В окне **Менеджер сертификатов** для запроса, по которому был издан сертификат, будет отображаться статус **сертификат введен в действие** (см. «Просмотр запроса на сертификат» на стр. 265).

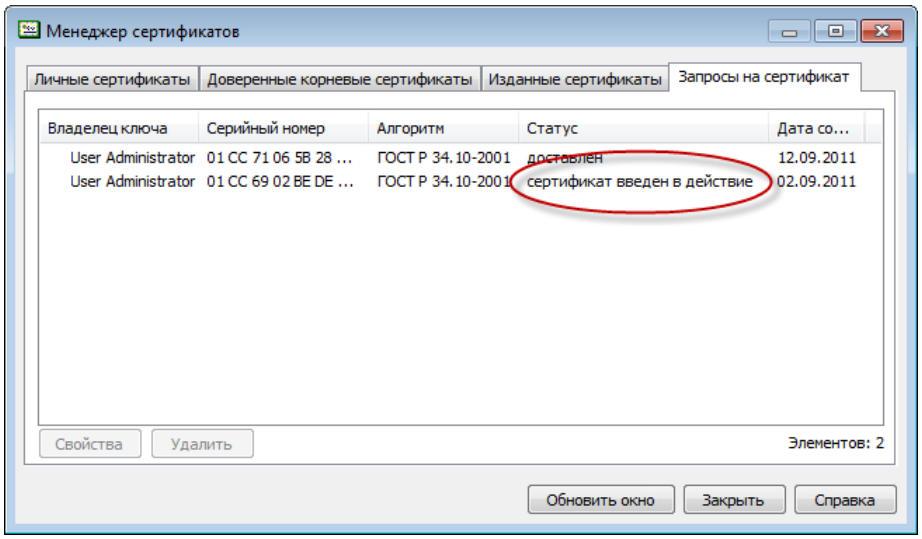



*Рисунок 123. Статус запроса в случае ввода сертификата в действие*

Если сертификат был получен, но не введен в действие автоматически, для запроса, по которому он был издан, будет отображаться статус **удовлетворен**. Выполните в данном случае ввод сертификата в действие вручную (см. «Ввод в действие вручную» на стр. 264).

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

# Ввод сертификата в действие

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

## Ввод в действие автоматически

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

При наличии данных флажков сертификаты будут вводиться в действие автоматически в течение часа с момента их получения. Сертификаты, изданные по вашим запросам, смогут вводиться в действие автоматически только в том случае, если доступны контейнеры с соответствующими ключами электронной подписи. В противном случае они могут быть введены в действие только вручную (см. «Ввод в действие вручную» на стр. 264).

**Внимание!** Если контейнер с ключом электронной подписи хранится в папке на диске, то он доступен всегда. Если контейнер хранится на внешнем устройстве, то он будет доступен только в том случае, если устройство подключено и сохранен ПИН-код к нему.

При вводе в действие сертификата, изданного по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр, появится окно **Предупреждение сервиса безопасности** с соответствующим сообщением (см. «Сертификат, изданный по инициативе администратора, введен в действие» на стр. 296).

## Ввод в действие вручную

Ввод сертификатов, полученных из программы ViPNet Удостоверяющий и ключевой центр, в действие вручную требуется выполнять в следующих случаях:

- Если не установлены флажки, позволяющие выполнять автоматический ввод сертификатов в действие.
- При автоматическом вводе сертификата в действие был недоступен контейнер с соответствующим ключом электронной подписи.

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

1. В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**, после чего нажмите кнопку **Изданные сертификаты**.
2. В окне **Менеджер сертификатов** на вкладке **Изданные сертификаты** выберите полученный сертификат, который необходимо ввести в действие, после чего нажмите кнопку **Ввести в действие**.

   В результате введенный в действие сертификат отобразится в окне **Менеджер сертификатов** на вкладке **Личные сертификаты**. Если необходимо использовать этот сертификат для подписания электронных документов, назначьте его текущим (см. «Смена текущего сертификата» на стр. 255).

# Работа с запросами на сертификаты

Работа с запросами на сертификаты (см. «Запрос на сертификат» на стр. 398) выполняется в окне **Менеджер сертификатов** на вкладке **Запросы на сертификат**.

Для вызова окна **Менеджер сертификатов**:

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

## Просмотр запроса на сертификат

Для просмотра подробной информации о запросе на сертификат:

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

   При необходимости запрос можно распечатать (на принтере, используемом по умолчанию на данном компьютере) с помощью кнопки **Печать**, а также сохранить в файл формата `*.txt` — с помощью кнопки **Копировать в файл**.

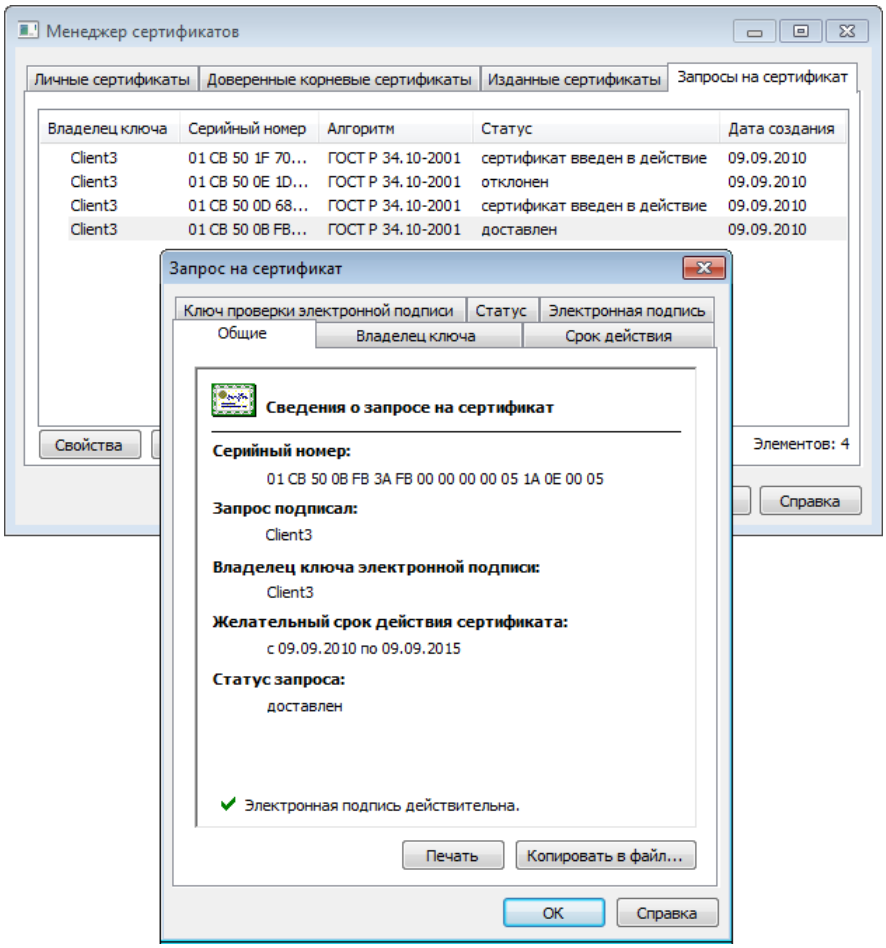



*Рисунок 124. Просмотр подробной информации о запросе на сертификат*

## Удаление запроса на сертификат

Для удаления запроса на сертификат:

1 В окне **Менеджер сертификатов** на вкладке **Запросы на сертификат** выберите нужный запрос (или несколько, удерживая клавишу **Ctrl**), после чего нажмите кнопку **Удалить**.

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

Информация о запросе будет удалена. Удаленный запрос не будет отображаться на вкладке **Запросы на сертификаты**.

# Экспорт сертификата

В программе ViPNet можно выполнить экспорт сертификата пользователя в различные форматы. Выбор формата экспорта зависит от целей, для которых проводится данный экспорт.

Экспорт сертификата может понадобиться для выполнения следующих задач:

- архивирование сертификата;

- копирование сертификата для использования на другом компьютере;
- отправка сертификата другому пользователю для организации обмена зашифрованными сообщениями;
- просмотр сертификата в удобной форме.

Для экспорта сертификата в файл определенного формата:

1 Вызовите окно **Сертификат** для того сертификата, который необходимо экспортировать (см. «Просмотр сертификатов» на стр. 244).

2 Откройте вкладку **Состав**, после чего нажмите кнопку **Копировать в файл**.

3 На начальной странице мастера экспорта сертификатов нажмите кнопку **Далее**.

---

**Совет.** Если при последующих запусках мастера желательно пропускать первую страницу, установите на ней флажок **Не отображать в дальнейшем эту страницу**.

---

4 На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов (см. «Форматы экспорта сертификатов» на стр. 268), после чего нажмите кнопку **Далее**.

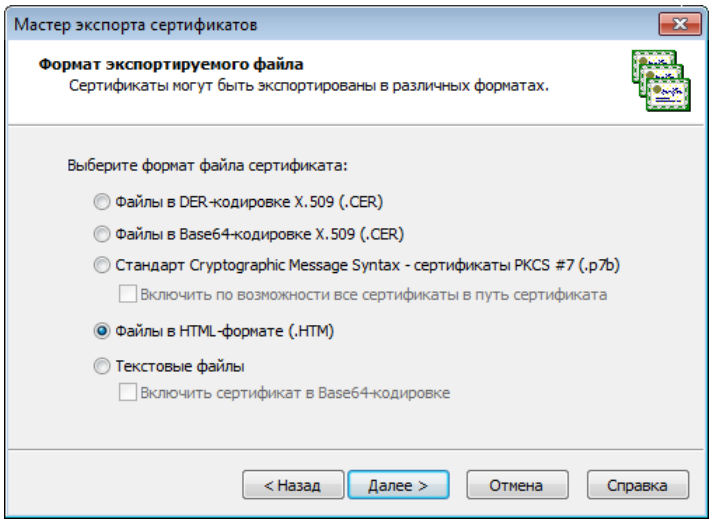



*Рисунок 125. Выбор формата файла*

5 На странице **Имя файла** укажите полный путь к создаваемому файлу, после чего нажмите кнопку **Далее**.

6 На странице **Завершение работы мастера экспорта сертификатов** убедитесь в правильности параметров экспорта, заданных на предыдущих страницах мастера, после чего нажмите кнопку **Готово**.

7 В окне с сообщением об успешном экспорте нажмите кнопку **OK**.

## Форматы экспорта сертификатов

При выборе формата экспорта сертификата следует руководствоваться перечисленными положениями.

- При экспорте сертификатов для импорта на компьютер с ОС Windows наиболее предпочтительный формат экспорта — PKCS #7, в первую очередь потому, что этот формат обеспечивает сохранение цепочки центров сертификации (пути сертификации) любого сертификата. Некоторые приложения требуют при импорте сертификата из файла представления в виде DER или Base64. Поэтому формат экспорта необходимо выбирать в соответствии с требованиями приложения или системы, в которую этот сертификат предполагается импортировать.
- Для просмотра сертификата и вывода его на печать используются текстовый и HTML-форматы.

Ниже приведена подробная информация о каждом из форматов экспорта сертификатов, поддерживаемых ПО ViPNet.

- **Стандарт Cryptographic Message Syntax (PKCS #7)**

  Формат PKCS #7 позволяет передавать сертификат и все сертификаты в цепочке сертификации с одного компьютера на другой или с компьютера на внешнее устройство. Файлы PKCS #7 обычно имеют расширение `.p7b` и совместимы со стандартом ITU-T X.509. Формат PKCS#7 разрешает такие атрибуты, как удостоверяющие подписи, связанные с обычными подписями. Для таких атрибутов, как метка времени, можно выполнить проверку подлинности вместе с содержимым сообщения. Дополнительные сведения о формате PKCS #7 см. на странице PKCS #7 веб-узла RSA Labs http://www.rsa.com/rsalabs/node.asp?id=2129.

- **Файлы в DER-кодировке X.509**

  DER (Distinguished Encoding Rules) для ASN.1, как определено в рекомендации ITU-T Recommendation X.509, — более ограниченный стандарт кодирования, чем альтернативный BER (Basic Encoding Rules) для ASN.1, определенный в рекомендации ITU-T Recommendation X.209, на котором основан DER. И BER, и DER обеспечивают независимый от платформы метод кодирования объектов, таких как сертификаты и сообщения, для передачи между устройствами и приложениями.

  При кодировании сертификата большинство приложений используют стандарт DER, так как сертификат (сведения о запросе на сертификат) должен быть закодирован с помощью DER и подписан. Файлы сертификатов DER имеют расширение `.cer`.

  Дополнительные сведения см. в документе «ITU-T Recommendation X.509, Information Technology — Open Systems Interconnection — The Directory: Authentication Framework» на веб-узле International Telecommunication Union (ITU) http://www.itu.int/ru/Pages/default.aspx.

- **Файлы в Base64-кодировке X.509**

  Этот метод кодирования создан для работы с протоколом S/MIME, который популярен при передаче бинарных файлов через Интернет. Base64 кодирует файлы в текстовый формат ASCII, при этом в процессе прохождения через шлюз файлы практически не повреждаются. Протокол S/MIME обеспечивает работу некоторых криптографических служб безопасности для приложений электронной почты, включая механизм неотрекаемости (с помощью электронных подписей), секретность и безопасность данных (с помощью кодирования,

процесса проверки подлинности и целостности сообщений). Файлы сертификатов Base64 имеют расширение `.cer`.

MIME (Multipurpose Internet Mail Extensions, спецификация RFC 1341 и последующие) определяет механизмы кодирования произвольных двоичных данных для передачи по электронной почте.

Дополнительные сведения см. в документе «RFC 2633 S/MIME Version 3 Message Specification, 1999» на веб-узле Internet Engineering Task Force (IETF) http://www.ietf.org/rfc/rfc2633.txt?number=2633.

- **Файлы в HTML-формате**

  Файлы для просмотра и печати в любом веб-браузере, а также в офисных и других программах, поддерживающих язык разметки гипертекста HTML.

- **Текстовые файлы**

  Файлы кодировки ANSI для просмотра в любом текстовом редакторе и вывода на печать.

# Работа с контейнером ключей

Контейнер ключей содержит ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи (на стр. 402).

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

- Установка (см. «Установка контейнера ключей» на стр. 275).

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

  Вы также можете установить контейнер ключей с помощью программы ViPNet CSP, входящей в состав ViPNet Client. Но при этом использовать ключ и сертификат из такого контейнера ключей вы сможете только в том случае, если вам разрешено использование внешних сертификатов (см. «Дополнительные настройки параметров безопасности» на стр. 224). В противном случае, они будут недоступны вам, даже если контейнер ключей будет установлен.

- Смена и удаление сохраненного пароля к контейнеру (см. «Смена пароля к контейнеру» на стр. 272).

  Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль. Удалять сохраненный пароль к контейнеру ключей может потребоваться в том случае, если изменились условия эксплуатации пароля или регламент вашей организации, вследствие чего хранение пароля на компьютере стало недопустимым.

- Изменение расположения контейнера (см. «Перенос контейнера ключей» на стр. 276).

  Перенос текущего контейнера ключей требуется в следующих случаях:

  - если расположение контейнера было изменено, например, вследствие того, что хранение контейнера по прежнему пути было признано небезопасным;
  - при переходе на способ аутентификации **Устройство** в случае, если используются процедуры электронной подписи и шифрования внутри сторонних приложений и при этом контейнер ключей изначально не хранился на внешнем устройстве, используемом для аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 226).

---

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

---

Для работы с контейнером ключей (см. «Контейнер ключей» на стр. 399):

1 Откройте вкладку **Ключи**.

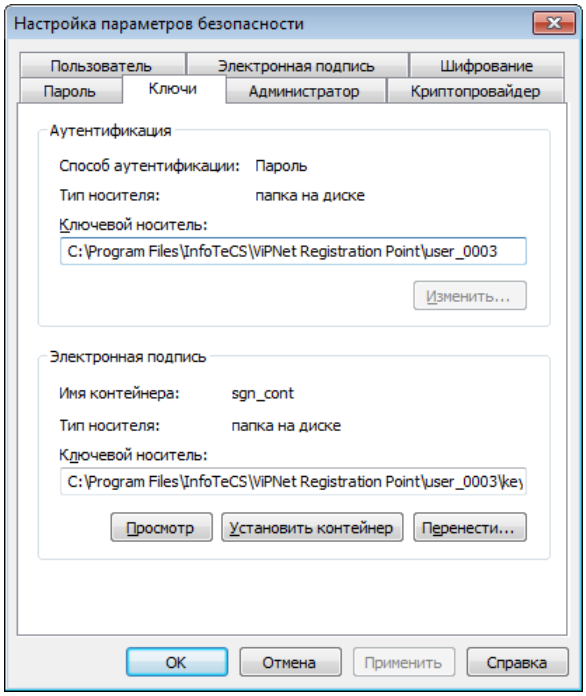



*Рисунок 126. Работа с контейнером ключей*

2 В группе **Электронная подпись** нажмите одну из следующих кнопок:

- **Просмотр** — для просмотра подробной информации об используемом контейнере ключей, а также для изменения свойств контейнера:
  - смены пароля (см. «Смена пароля к контейнеру» на стр. 272);
  - удаления пароля (см. «Удаление сохраненного на компьютере пароля к контейнеру ключей» на стр. 273);
  - проверки соответствия ключа электронной подписи сертификату (см. «Проверка контейнера ключей» на стр. 274);
  - удаления ключа электронной подписи.
- **Установить контейнер** — для установки нового контейнера ключей (см. «Установка контейнера ключей» на стр. 275).
- **Перенести** — для изменения расположения контейнера ключей (см. «Перенос контейнера ключей» на стр. 276).

---

**Примечание.** В группе **Электронная подпись** отображается информация о ключе электронной подписи, соответствующем текущему сертификату. При установке нового контейнера ключей (см. «Установка контейнера ключей» на стр. 275) информация о текущем сертификате, отображаемая на вкладке **Электронная подпись**, меняется автоматически.

---

# Смена пароля к контейнеру

Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль.

Для смены пароля к контейнеру ключей:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 116 на стр. 271) нажмите кнопку **Просмотр**.

2 В окне **Свойства контейнера ключей** нажмите кнопку **Сменить пароль**.

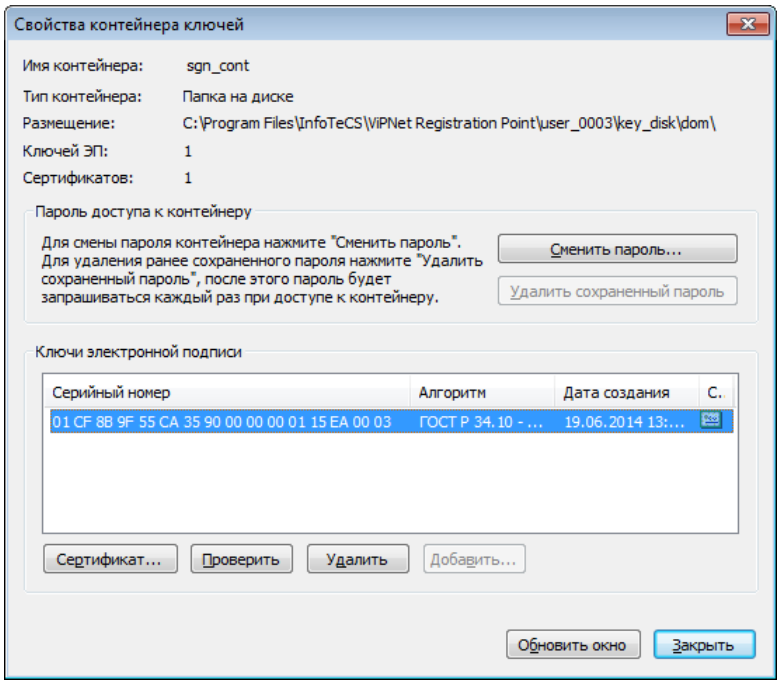



*Рисунок 127. Информация о контейнере ключей*

3 При появлении сообщения «Для данного контейнера смена пароля возможна только в настройке безопасности приложений ViPNet» нажмите кнопку **OK**, после чего завершите работу с окном **Свойства контейнера ключей** и измените пароль пользователя (см. «Смена пароля пользователя» на стр. 235).

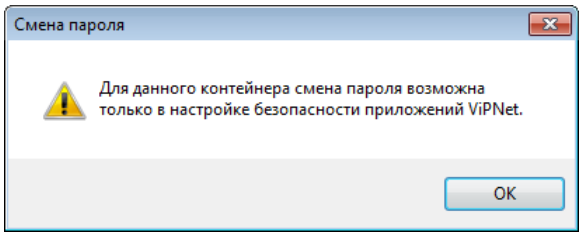



*Рисунок 128. Сообщение о невозможности смены пароля для доступа к контейнеру*

**Примечание.** Появление данного окна связано с тем, что контейнер ключей защищен с использованием не пароля, а персонального ключа пользователя. В этом случае пароль к контейнеру совпадает с паролем пользователя, поэтому изменение пароля к контейнеру возможно только вместе с изменением пароля пользователя.

4 Если контейнер ключей пользователя создан в программе ViPNet Registration Point либо был перенесен (см. «Перенос контейнера ключей» на стр. 276) из папки ключей пользователя (по умолчанию `C:\Program Files (x86)\InfoTeCS\ViPNet Client\user_<идентификатор пользователя>\key_disk\dom`) в другую папку, после нажатия на кнопку **Сменить пароль** появится окно **Пароль**. В окне **Пароль** введите текущий пароль доступа к контейнеру ключей и нажмите кнопку **OK**.

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

5 В окне **ViPNet CSP - пароль контейнера ключей** укажите и подтвердите новый пароль. Нажмите кнопку **OK**.

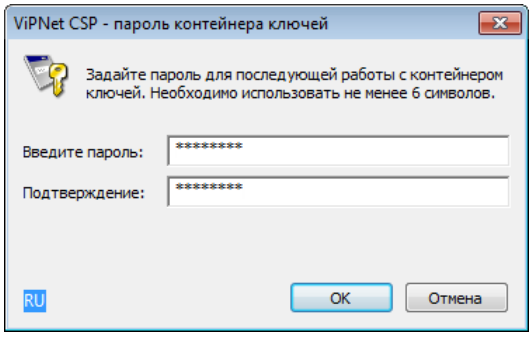



*Рисунок 129. Смена пароля доступа к контейнеру ключей*

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

Пароль доступа к контейнеру ключей изменен.

# Удаление сохраненного на компьютере пароля к контейнеру ключей

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

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

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 116 на стр. 271) нажмите кнопку **Просмотр**.

2 В окне **Свойства контейнера ключей** (см. Рисунок 117 на стр. 272) нажмите кнопку **Удалить сохраненный пароль**.

Сохраненный пароль удален. Теперь пароль необходимо вводить всякий раз при доступе к контейнеру ключей.

# Проверка контейнера ключей

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

Чтобы проверить контейнер ключей, выполните следующие действия:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 116 на стр. 271) нажмите кнопку **Просмотр**.

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

3 В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите кнопку **OK**.

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

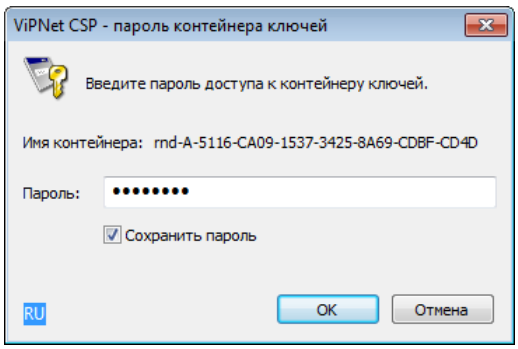



*Рисунок 130. Ввод пароля доступа к контейнеру ключей*

4 В результате будет сформирован фрагмент данных, который будет подписан с помощью ключа электронной подписи, после чего будет выполнена проверка электронной подписи с помощью ключа проверки электронной подписи. Таким образом, будет проверена пригодность ключа электронной подписи и его соответствие сертификату ключа проверки электронной подписи, хранящемуся в контейнере.

**Примечание.** Проверка возможна только в том случае, если в контейнере ключей есть сертификат, соответствующий ключу электронной подписи. Сертификат может отсутствовать в контейнере ключей, если он размещен отдельно. Сертификат размещается отдельно от контейнера ключей, если запрос на обновление сертификата сформирован в ПО ViPNet CSP. Если запрос сформирован в другой программе, сертификат автоматически помещается в контейнер ключей.

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

# Установка контейнера ключей

Если у вас есть контейнер ключей, ключи и сертификат из которого вы хотите использовать в ViPNet Client, то вы можете его установить в окне **Настройка параметров безопасности** на вкладке **Ключи**. Данная ситуация может возникнуть в следующих случаях:

- Вы переносите контейнер ключей с другого компьютера (см. «Перенос сетевого узла на другой компьютер» на стр. 47).
- Вы сформировали запрос на сертификат (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 257) и получили на него сертификат из программы ViPNet Удостоверяющий и ключевой центр не по сети, а в отдельном файле. В данном случае контейнер ключей, созданный при формировании запроса, не установлен автоматически и его требуется установить вручную.
- У вас есть контейнер ключей, сформированный с помощью ViPNet CSP (на стр. 17). О том, как сформировать контейнер ключей в ViPNet CSP, см. в документе «ViPNet CSP. Руководство пользователя».

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

Вы также можете установить контейнер ключей с помощью программы ViPNet CSP, входящей в состав ViPNet Client. Но при этом использовать ключ и сертификат из такого контейнера ключей вы сможете только в том случае, если вам разрешено использование внешних сертификатов (см. «Дополнительные настройки параметров безопасности» на стр. 224). В противном случае, они будут недоступны вам, даже если контейнер ключей будет установлен.

Для установки контейнера ключей выполните следующие действия:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 116 на стр. 271) нажмите кнопку **Установить контейнер**.

2 В окне **ViPNet CSP – инициализация контейнера ключа** укажите место хранения контейнера ключей:

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

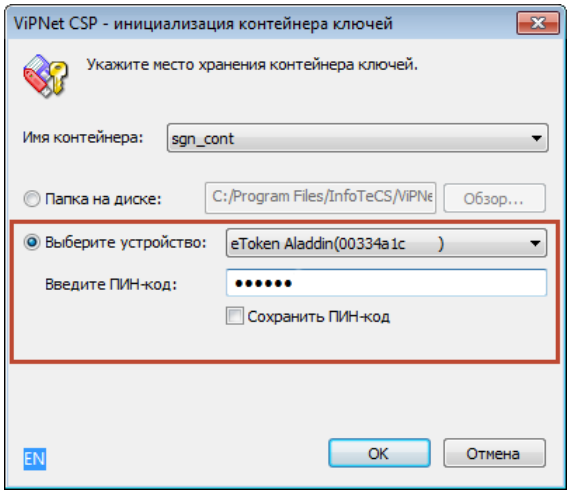



*Рисунок 131. Установка контейнера ключей с внешнего устройства*

Нажмите кнопку **OK**.

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

В результате ключ электронной подписи и сертификат, которые хранятся в выбранном контейнере, будут назначены текущими. Информация о сертификате, который хранится в установленном контейнере, отобразится на вкладке **Электронная подпись**.

# Перенос контейнера ключей

Перенос текущего контейнера ключей может потребоваться для изменения расположения контейнера, например, если хранение контейнера по прежнему пути было признано небезопасным.

**Примечание.** Перенести можно только контейнер с ключами, сформированными в ПО ViPNet версии не ниже 3.2.x.

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

Для того чтобы поменять расположение контейнера ключей:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 116 на стр. 271) нажмите кнопку **Перенести**.

2 В окне **ViPNet CSP – инициализация контейнера ключей** укажите новое место хранения контейнера ключей:

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

**Примечание.** Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 345).

Контейнер ключей будет перенесен по указанному пути.

# Установка сертификата в контейнер ключей

Если по каким-то причинам ваш сертификат не находится в контейнере ключей (например, вы не сопоставили сертификат с ключом электронной подписи в процессе установки сертификата в хранилище (см. «Установка сертификатов в хранилище» на стр. 250)), то его требуется установить в контейнер ключей вручную. Установить сертификат в контейнер можно как в программе ViPNet CSP, так и в окне **Настройка параметров безопасности**. При этом в обоих случаях контейнер ключей должен быть установлен в программу.

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

1. Перейдите на вкладку **Ключи** (см. Рисунок 116 на стр. 271).
2. Установите контейнер ключей, если он не установлен (см. «Установка контейнера ключей» на стр. 275).
3. Перейдите в свойства контейнера с помощью кнопки **Просмотр**.
4. В окне **Свойства контейнера ключей** нажмите кнопку **Добавить**.
5. В появившемся окне укажите файл сертификата, который соответствует ключу электронной подписи, находящемуся в контейнере. Если будет установлено, что указанный сертификат соответствует ключу электронной подписи, он будет добавлен в контейнер. В противном случае, появится соответствующее сообщение.

# A

# Возможные неполадки и способы их устранения

# Сбор диагностической информации при возникновении неполадок

При обращении в службу технического сопровождения компании «ИнфоТеКС» в случае возникновения каких-либо неполадок в работе ПО ViPNet вам, как правило, потребуется предоставить информацию о компьютере, на котором данное ПО установлено. На основе этой информации сотрудники отдела сопровождения смогут выявить причины возникновения неполадок и определить способы их устранения.

Информацию о компьютере вы можете получить с помощью утилиты lumpdiag, встроенной в ПО ViPNet Client. Для работы с утилитой вы должны обладать правами администратора операционной системы.

Утилита собирает информацию о компьютере (например, информацию о системе, криптографическом окружении и так далее) независимо от работоспособности ПО ViPNet Client.

**Примечание.** В процессе работы утилиты сбор вашей конфиденциальной информации не производится. ОАО «ИнфоТеКС» ответственно подходит к защите вашей личной информации и принимает все меры для предотвращения несанкционированного доступа или разглашения информации, которую вы нам предоставляете.

С помощью утилиты вы можете собрать необходимую информацию либо в архив, либо в папку `\SysEnv`, которая автоматически создается в папке установки ПО ViPNet Client.

Для получения справочной информации по использованию утилиты в командной строке введите: `lumpdiag -h`, где `h` — ключ, который вызывает справку. Если утилита вызвана без указания каких-либо ключей, считается, что она вызвана с данной опцией.

Для сбора информации в командной строке введите:

`lumpdiag -a [<archive file>]`, где:

- `-a` — ключ, который запускает процесс сбора информации на компьютере;
- `<archive file>` — путь к архиву, в который будут упакованы файлы, собранные в результате работы утилиты.

  Если при сборе информации параметр `<archive file>` не был указан, то собранная информация будет сохранена в папке `\SysEnv` папки установки ПО ViPNet Client (по умолчанию: `c:\Program Files (Program Files (x86))\InfoTeCS\ViPNet Client`). Если папка `\SysEnv` уже существует, то утилита запросит у вас разрешение на перезапись содержимого папки.

# Возможные неполадки

## Невозможно проверить сертификат, которым подписан файл установки программы

На компьютере с операционной системой Windows Vista при установке программы может появиться предупреждение системы безопасности о невозможности проверить сертификат, которым подписан данный файл установки.

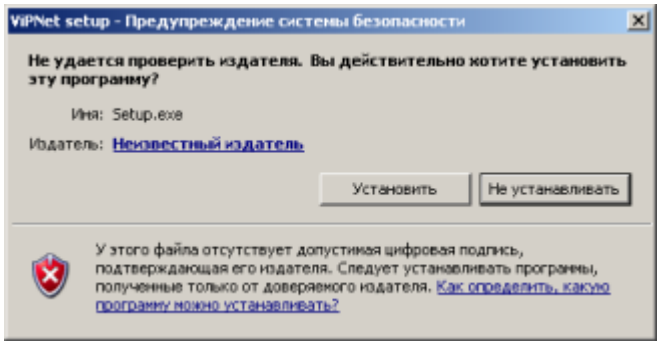



*Рисунок 132. Невозможно проверить сертификат*

Это может произойти, если отсутствует или недействителен корневой сертификат или какой-либо сертификат из цепочки сертификации.

Возможные варианты решения проблемы:

- С помощью кнопки **Не устанавливать** прервите установку программы, затем установите обновление операционной системы KB931125 (либо просто установите все обновления текущей версии вашей операционной системы). В результате цепочка сертификации будет обновлена, и сертификат, которым подписан файл установки, можно будет проверить.

  После обновления заново начните установку ViPNet Client.

- При необходимости вы можете установить программу без обновления операционной системы. В этом случае в окне предупреждения системы безопасности нажмите кнопку **Установить**.

## Невозможно установить или обновить программу

Если у вас установлен антивирус Касперского, установка или обновление ViPNet Client может быть заблокировано самозащитой антивируса. Для установки программы отключите самозащиту антивируса.

**Внимание!** Если вы приостановите антивирусную защиту или выйдете из программы Kaspersky Anti-Virus, проблема не будет решена. Необходимо отключить самозащиту антивируса описанным ниже способом.

Для решения проблемы выполните следующие действия:

1. В окне программы Kaspersky Anti-Virus на нижней панели нажмите ссылку **Настройка**.
2. На странице **Настройка** выберите раздел **Дополнительно** и нажмите ссылку **Самозащита**.
3. На странице **Параметры самозащиты** снимите флажок **Включить самозащиту**.
4. В окне подтверждения нажмите кнопку **Продолжить**.

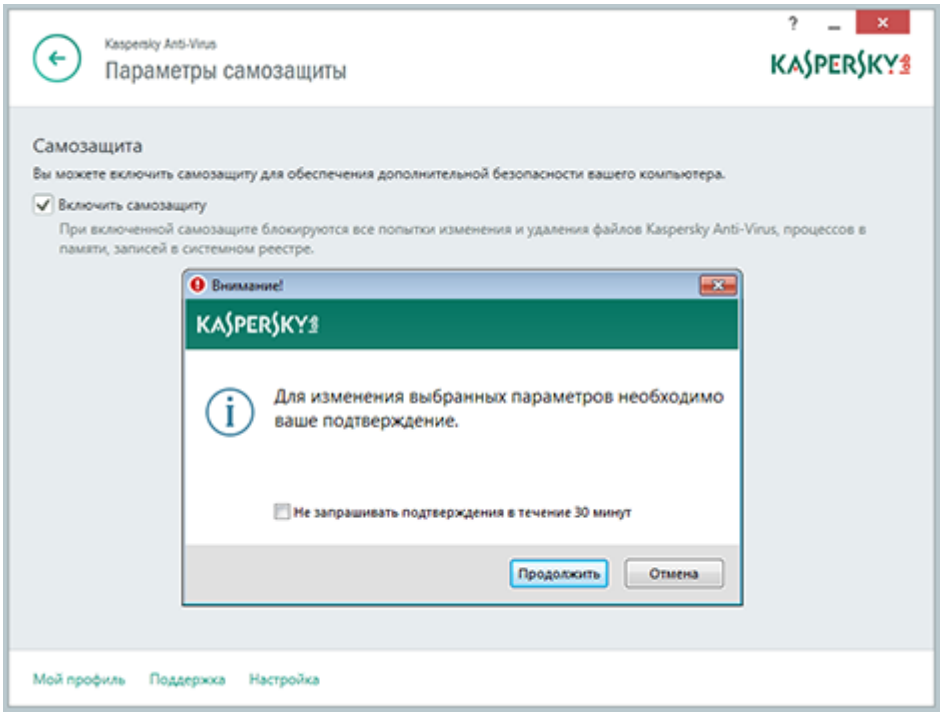



*Рисунок 133. Отключение самозащиты в антивирусе Касперского*

После отключения самозащиты антивируса Касперского заново начните установку ViPNet Client. Отключение самозащиты требуется только на время установки.

# Установка программы не выполняется в неинтерактивном режиме

Если вы устанавливаете программу в неинтерактивном режиме на компьютер с операционной системой Windows Vista, вы можете обнаружить, что установка не выполняется: через несколько минут после запуска установки не проявляются признаки установки программы (например, возникновение ярлыка программы на рабочем столе). Это может быть связано с невозможностью проверить сертификат, которым подписан файл установки программы, из-за того что отсутствует или недействителен корневой сертификат или какой-либо сертификат из цепочки сертификации.

Для решения проблемы установите обновление операционной системы KB931125 (либо просто установите все обновления текущей версии вашей операционной системы). В результате цепочка сертификации будет обновлена, и сертификат, которым подписан файл установки, можно будет проверить. После обновления заново начните установку ViPNet Client.

# Невозможно запустить программу

Вероятно, программа ViPNet Монитор была удалена с компьютера либо были удалены файлы, необходимые для ее работы. Убедитесь в том, что программа ViPNet Монитор установлена, и в случае необходимости переустановите ее либо обратитесь за помощью к администратору сети ViPNet.

# Не найдены ключи пользователя или неверный пароль

В этом случае программа выдает следующее сообщение:

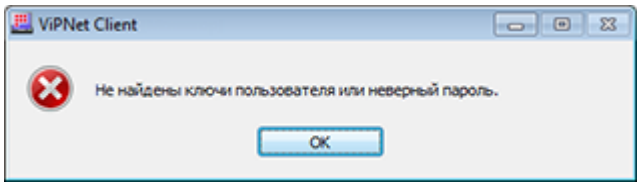



*Рисунок 134. Сообщение о неверном пароле*

Возможные варианты решения проблемы:

- Проверьте состояние клавиши **Caps Lock**.
- Проверьте раскладку клавиатуры, используя соответствующий индикатор в окне ввода пароля. Если используется случайный пароль, его следует набирать в английской раскладке клавиатуры.
- Проверьте правильность пароля и еще раз внимательно наберите пароль.
- Возможно, ключи пользователя установлены в папку, которая отличается от папки ключей пользователя по умолчанию.

  В этом случае в окне ввода пароля щелкните значок справа от кнопки **Настройка**, в меню выберите пункт **Папка ключей пользователя** и укажите путь к папке ключей пользователя.

  Если операционная система еще не загружена, в окне ввода пароля ViPNet нажмите кнопку **Отмена**. После загрузки операционной системы запустите ViPNet Монитор и укажите путь к папке ключей пользователя.

# Не удается выполнить аутентификацию с помощью сертификата

Если вам не удается войти в программу ViPNet Client, используя для аутентификации сертификат и соответствующий ему ключ электронной подписи, которые хранятся на внешнем устройстве, это может быть вызвано одной из следующих причин:

- Сертификат не соответствует стандарту RSA и ГОСТ.
- Внешнее устройство хранения данных не поддерживает стандарт PKCS#11. Проверить, поддерживает ли ваше устройство этот стандарт, можно по разделу Внешние устройства (на стр. 345).
- Срок действия выбранного сертификата истек. При выборе недействительного сертификата появится соответствующее сообщение. В этом случае следует передать сертификат администратору вашего удостоверяющего центра для обновления.
- Выбранный сертификат присутствует в списке аннулированных сертификатов, который установлен в хранилище данного узла. При выборе аннулированного сертификата появится соответствующее сообщение. В этом случае следует обратиться к администратору вашего удостоверяющего центра.
- Выбранный сертификат не имеет назначения «Шифрование ключей». Это расширение должно отображаться в окне **Сертификат**, на вкладке **Состав**, в поле **Использование ключа**. В этом случае следует обратиться к администратору вашего удостоверяющего центра для переиздания сертификата.
- Сертификат издателя не установлен в системное хранилище **Доверенные корневые сертификаты**. В этом случае следует получить сертификат издателя у администратора вашего удостоверяющего центра и установить его в указанное системное хранилище. Для этого дважды щелкните по сертификату и следуйте указаниям мастера установки сертификатов.

# Невозможно сохранить пароль

Чтобы предоставить возможность сохранения пароля, войдите в программу ViPNet Монитор в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 219).

# Невозможно подключиться к ресурсам в Интернете

Возможные причины:

- Соединение с ресурсами Интернета заблокировано фильтрами открытой сети или заблокирован IP-трафик компьютера. Убедитесь, что настроены сетевые фильтры,

разрешающие соединение с требуемыми адресами (см. «Создание фильтров для открытой сети» на стр. 147), а также в том, что IP-трафик компьютера не заблокирован (об этом свидетельствует, например, наличие в меню **Файл** > **Конфигурации** команды **Блокировать IP-трафик**).

- На компьютере установлена версия антивируса Avast, конфликтующая с ПО ViPNet. Чтобы обеспечить нормальное совместное функционирование антивируса Avast и программного обеспечения ViPNet, обновите программу Avast до версии 10.3.223 или более новой.

# Невозможно установить соединение с защищенным узлом

Возможные причины:

- Сетевой узел выключен или на нем не запущена программа ViPNet Монитор.
- Нет ключей, необходимых для связи с сетевым узлом. Обратитесь к администратору сети ViPNet.
- Ваш компьютер физически не подключен к сети или не имеет выхода в Интернет.

# Невозможно обратиться к узлам домена по DNS-имени

Если в сети ViPNet вашей организации используется служба Active Directory и при этом контроллеры домена с DNS-серверами, которые в рамках домена синхронизируются между собой, находятся на разных узлах ViPNet или туннелируются разными координаторами, то могут возникнуть проблемы разрешения IP-адресов при обращении к ним с других защищенных узлов. В этом случае выполните указания раздела Использование DNS-серверов на контроллерах домена (на стр. 125).

# Невозможно получить удаленный доступ к защищенным узлам по DNS-имени

Если вам не удалось получить удаленный доступ к защищенному узлу по DNS-имени, выполните следующие действия:

1 В командной строке введите `ipconfig /all`.

2 Если в полученной информации в списке DNS-серверов первым указан IP-адрес версии IPv6 (например, `2001::11a3:09d7:1f34:8a2e:07a0:765d`), в окне программы ViPNet Монитор

в меню **Сервис** выберите пункт **Настройка приложения** и перейдите в раздел **Управление трафиком**.

3 Убедитесь, что установлен флажок **Блокировать все протоколы, кроме IP, ARP**.

# Невозможно установить соединение с открытым узлом в локальной сети

Возможные причины:

- IP-адрес открытого узла присутствует в списке защищенных узлов. В этом случае ViPNet-драйвер пытается послать зашифрованный пакет на открытый компьютер, установить соединение не удается. Для устранения данной проблемы необходимо удалить адрес открытого узла из списка адресов защищенных узлов.
- Неправильно настроены фильтры для работы с открытой сетью. Для нормальной работы в сетях Microsoft убедитесь, что включены и настроены нужные фильтры открытой сети (см. «Общие сведения о сетевых фильтрах» на стр. 129).

# Невозможно установить соединение по протоколу SSL

Возможно, причиной неполадки является сбой одного из компонентов программы ViPNet Client. Для решения данной проблемы выполните действия, описанные в разделе Невозможно запустить службу MSSQLSERVER (на стр. 287).

# Невозможно установить соединение по протоколу PPPoE

Соединение по протоколу PPPoE может быть заблокировано программой ViPNet Монитор. Для решения данной проблемы выполните следующие действия:

1 В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2 В окне **Настройка** откройте раздел **Управление трафиком**.

3 Снимите флажок **Блокировать все протоколы, кроме IP, ARP**.

4 Нажмите кнопку **OK**.

# В сети зарегистрирован узел с таким же идентификатором, как у вашего узла

В этом случае:

- В журнале событий регистрируется событие с номером 95 (см. «Блокированные IP-пакеты» на стр. 328).
- Полностью блокируется весь IP-трафик.
- В программе ViPNet Монитор появляется следующее сообщение:

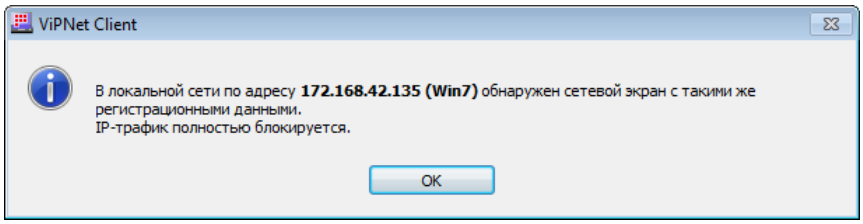



*Рисунок 135. Сообщение о том, что в сети обнаружен узел с таким же идентификатором*

Для устранения данной проблемы требуется удалить дубликат вашего узла из сети ViPNet (удалить на нем текущие ключи или установить новые ключи). После этого требуется перезагрузить ваш компьютер.

# Обнаружен конфликт IP-адресов или DNS-имен

При добавлении IP-адреса или DNS-имени в процессе настройки доступа к защищенному или туннелируемому узлу может оказаться, что он совпадает с IP-адресом или DNS-именем, заданным ранее для другого узла. Тогда появится следующее сообщение:

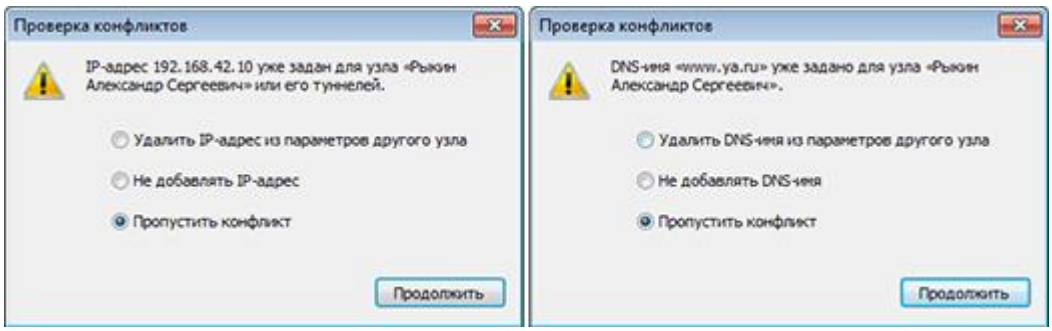



*Рисунок 136. Действия при обнаружении пересечения IP-адресов или DNS-имен*

Конфликт IP-адресов и DNS-имен также может быть обнаружен в ходе их проверки с помощью кнопки **Проверить конфликты**  . В этом случае появится такое сообщение:

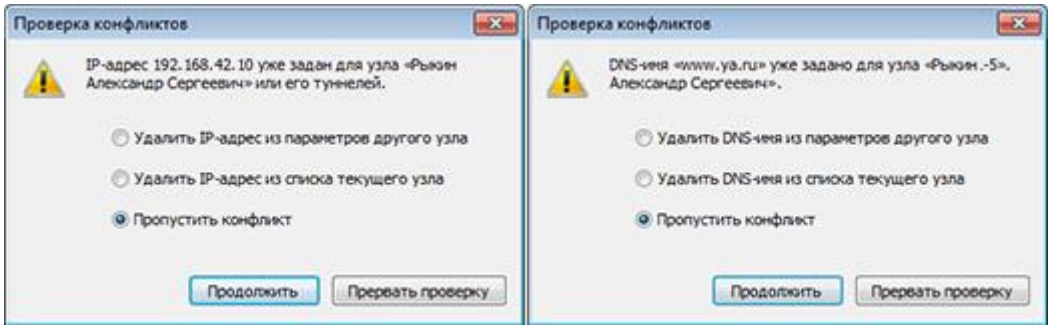



*Рисунок 137. Действия при обнаружении пересечения IP-адресов или DNS-имен*

Для устранения конфликта IP-адресов или DNS-имен вы можете:

- удалить повторяющийся IP-адрес или DNS-имя из параметров другого узла;
- не добавлять IP-адрес или DNS-имя в первом случае, удалить IP-адрес или DNS-имя из списка текущего узла — во втором.

Кроме этого, вы можете не учитывать возникший конфликт (в первом случае будет добавлен указанный IP-адрес или DNS-имя), а также во втором случае прервать проверку.

# Невозможно запустить службу MSSQLSERVER

Возможно, причиной неполадки является сбой одного из компонентов программы ViPNet Client. Для решения данной проблемы выполните следующие действия:

1. В командной строке Windows выполните команду: `regsvr32 /u C:\Windows\System32\itcssp.dll`.
2. Измените имя файла `itcssp.dll`, находящегося в папке `C:\Windows\System32`, на любое другое.

   Если на компьютере была установлена программа ViPNet CSP с поддержкой 64-разрядных операционных систем, в папке `C:\Windows\SysWOW64` также существует файл `itcssp.dll`, который требуется переименовать.
3. Перезагрузите компьютер.

# Невозможно изменить настройки в программе ViPNet Монитор

Изменение настроек программы ViPNet Монитор может быть невозможно по одной из следующих причин:

- На сетевом узле ограничены полномочия пользователя. Изменить настройки программы ViPNet Монитор может только пользователь с максимальным уровнем полномочий.

Обратитесь к администратору сети ViPNet с просьбой повысить уровень полномочий в программе ViPNet Центр управления сетью.

**Примечание.** В сетях ViPNet VPN на клиентских узлах по умолчанию ограничен интерфейс программы ViPNet Client. Настройки программы можно выполнить только в режиме администратора сетевого узла.

- Установлены ограничения интерфейса в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 219). Обратитесь к администратору сети ViPNet с просьбой снять ограничение.

# Не удается использовать аппаратный датчик случайных чисел

Если требуется использовать в программном обеспечении ViPNet аппаратный датчик случайных чисел, выполните следующие действия:

1. На компьютере, на котором требуется использовать аппаратный датчик случайных чисел, в зависимости от используемой операционной системы выполните одно из следующих действий:
   - В Windows Vista и более поздних — создайте папку `C:\ProgramData\InfoTeCS\ViPNet CSP`.
   - В Windows XP и Windows Server 2003 — создайте папку `C:\Documents and Settings\All Users\Application Data\InfoTeCS\ViPNet CSP`.
2. В указанной папке создайте текстовый файл следующего содержания:

   ```
   [Common]
   EnableCspSupport=Yes
   [Devices]
   RandomNumberGeneratorType=<тип датчика>
   ```

3. В качестве значения параметра `RandomNumberGeneratorType` укажите тип датчика случайных чисел, который требуется использовать. Этот параметр может иметь следующие значения:
   - `accord` — Аккорд-АМДЗ.
   - `sobol` — электронный замок «Соболь».
   - `bio` — электронная рулетка (используется в программном обеспечении ViPNet по умолчанию).
   - `tokenJava` — eToken PRO (Java).
   - `ruToken` — Rutoken ЭЦП.
4. Сохраните созданный файл, затем измените его имя и расширение на `csp_config.ini`.

При следующем вызове датчика случайных чисел будет использоваться указанный датчик.

# Нарушение работоспособности сторонних приложений

Из-за специфики работы программного обеспечения ViPNet может быть нарушена работа сторонних приложений.

Для устранения конфликта ПО ViPNet со сторонними приложениями внесите изменения в системный реестр Windows, для этого выполните следующие действия:

1 В меню **Пуск** выберите пункт **Выполнить**.

2 В окне **Выполнить** в поле **Открыть** введите `regedit` и нажмите кнопку **OK**. Откроется окно **Редактор реестра**.

**Внимание!** Неправильное редактирование реестра может привести к возникновению неполадок в работе операционной системы, поэтому обязательно создайте резервную копию реестра. Это позволит восстановить реестр при возникновении неполадок.

3 В разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Infotecs\PatchEngine` присвойте параметру `Flags` значение 0.

4 Перезагрузите компьютер.

Если после выполнения указанных действий проблема не будет решена, обратитесь в службу технической поддержки компании «ИнфоТеКС» (см. «Обратная связь» на стр. 24).

# Не проходит обновление ПО, отправленное из Центра управления сетью

Одна из возможных причин неудачного обновления ПО в том, что программе установки не удалось завершить работу всех компонентов ПО ViPNet (например, какие-то компоненты ПО ViPNet были запущены в сессии другого пользователя). В этом случае для решения проблемы выполните следующие действия:

1 Перезагрузите компьютер, на котором не удалось обновить ПО ViPNet.

2 Повторно отправьте обновление из программы ViPNet Центр управления сетью или ViPNet Network Manager и примите его на узле (см. «Обновление, отправленное из ЦУСа или ViPNet Network Manager» на стр. 41).

# Предупреждения сервиса безопасности

Предупреждения сервиса безопасности предназначены для своевременного информирования пользователя о таких событиях, как истечение сроков действия пароля, текущего сертификата, ключа электронной подписи и списка аннулированных сертификатов, а также ввод в действие сертификата, изданного по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр.

Проверка статуса пароля, текущего сертификата и ключа электронной подписи выполняется каждые 5 минут.

## Срок действия пароля истек

Окно с сообщением об истечении срока действия пароля пользователя появляется в следующих случаях:

- Если в окне **Настройка параметров безопасности** на вкладке **Пароль** (см. Рисунок 98 на стр. 235) установлен флажок **Ограничить срок действия пароля** и задан срок действия пароля.

  Появление окна свидетельствует о том, что указанный срок подошел к концу.

- Если от программы ViPNet Удостоверяющий и ключевой центр получены ключи пользователя с новым паролем пользователя.

  При этом автоматической смены пароля не происходит, поэтому пароль необходимо сменить вручную (см. «Смена пароля пользователя» на стр. 235).

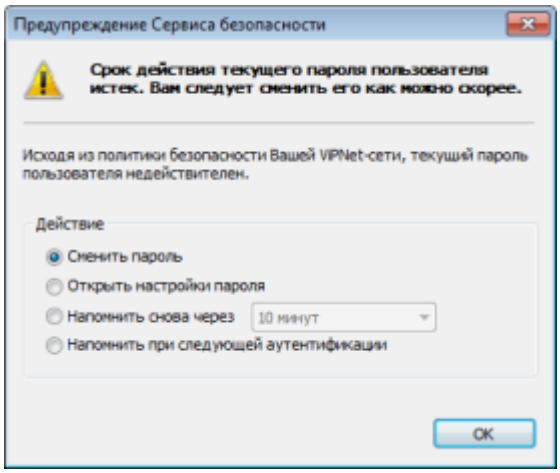



*Рисунок 138. Предупреждение об истечении срока действия пароля пользователя*

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий:

   - **Сменить пароль** — для указания нового пароля в соответствии с настройками, заданными в окне **Настройка параметров безопасности** на вкладке **Пароль** (см. Рисунок 98 на стр. 235);
   - **Открыть настройки пароля** — для вызова окна **Настройка параметров безопасности** на вкладке **Пароль** (см. Рисунок 98 на стр. 235), с помощью которой можно сначала задать параметры пароля, а затем сменить его;
   - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя);
   - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Client.

2 Нажмите кнопку **ОК**.

# Текущий сертификат не найден или недействителен

Окно с сообщением о том, что текущий сертификат не найден либо недействителен, появляется в следующих случаях:

- Если текущий сертификат не найден либо недействителен, однако найдены другие действительные личные сертификаты.

  В этом случае вы можете назначить один из них текущим, выбрав **Выбрать другой сертификат в качестве текущего**.

- Если не найден ни один действительный личный сертификат.

  В этом случае обратитесь к администратору вашей сети ViPNet для получения нового сертификата.

---

**Внимание!** Пока не получен и не введен в действие новый сертификат, подписание электронных документов невозможно.

---

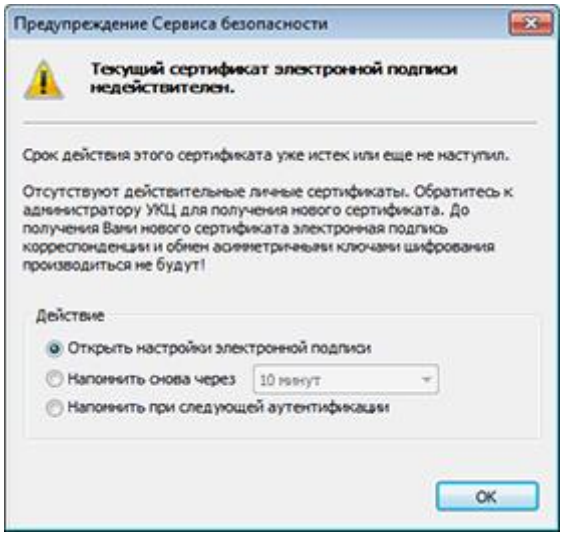



*Рисунок 139. Предупреждение о том, что текущий сертификат недействителен*

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий:

- **Выбрать другой сертификат в качестве текущего** — для назначения другого действительного личного сертификата текущим с помощью окна **Назначение сертификата текущим**.

---

**Примечание.** Данное положение переключателя отображается в окне предупреждения в случае, если в хранилище пользователя найдены другие действительные личные сертификаты.

---

- **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись**, с помощью которой можно управлять сертификатами.
- **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
- **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Client.

2 Нажмите кнопку **OK**.

# Срок действия текущего ключа электронной подписи или соответствующего сертификата близок к концу

Предупреждение о скором истечении срока действия ключа электронной подписи или соответствующего ему сертификата появляется в следующих случаях:

- Если срок действия ключа электронной подписи или сертификата близок к концу, при этом не найдено запросов на обновление текущего сертификата (или последний запрос на обновление удовлетворен, однако соответствующий сертификат не может быть назначен текущим).

  В этом случае Вы можете сформировать запрос на обновление сертификата (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 257). Для этого:

  - если истекает срок действия сертификата, выберите **Отправить запрос на обновление сертификата**;
  - если истекает срок действия ключа электронной подписи, выберите **Открыть настройки подписи**, затем в окне **Настройка параметров безопасности** на вкладке **Электронная подпись** нажмите кнопку **Обновить сертификат**.

- Если срок действия ключа электронной подписи или сертификата близок к концу, при этом последний запрос на обновление текущего сертификата либо отклонен, либо находится в состоянии обработки в программе ViPNet Удостоверяющий и ключевой центр.

  В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте еще один запрос на обновление текущего сертификата.

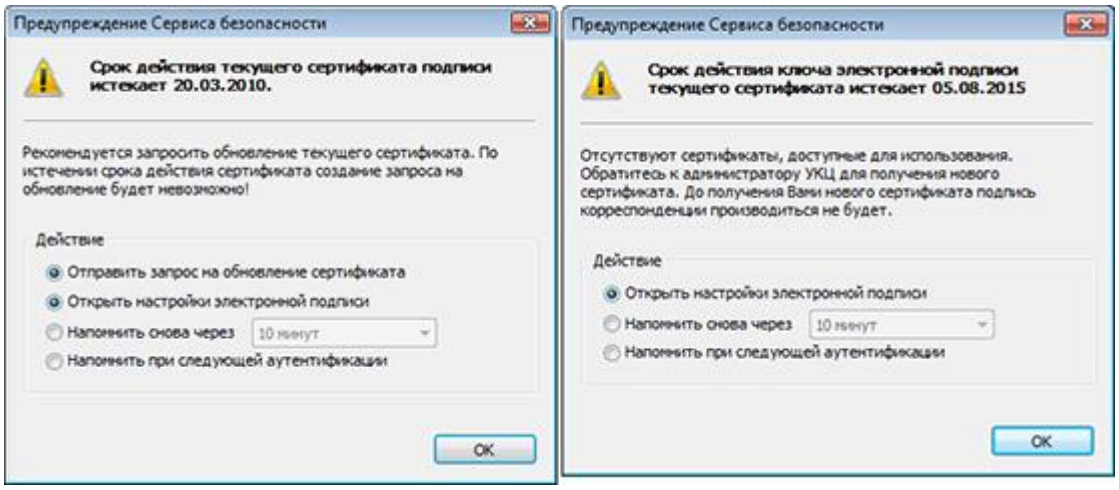



*Рисунок 140. Предупреждения о скором истечении срока действия сертификата и ключа электронной подписи*

При появлении окна с таким предупреждением:

1 В зависимости от вида предупреждения выберите одно из предложенных действий:

- **Выбрать другой сертификат в качестве текущего** — для назначения другого действительного личного сертификата текущим с помощью окна **Назначение сертификата текущим**.
- **Отправить запрос на обновление сертификата** — для формирования запроса на обновление текущего сертификата с помощью мастера обновления сертификатов (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 257).
- **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись**, с помощью которой можно управлять сертификатами.
- **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
- **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Client.

2 Нажмите кнопку **OK**.

# Срок действия текущего ключа электронной подписи уже истек

Предупреждение об истечении срока действия ключа электронной подписи появляется в следующих случаях:

- Если срок действия ключа электронной подписи подошел к концу, при этом не найдено запросов на обновление текущего сертификата (или последний запрос на обновление удовлетворен, однако соответствующий сертификат не может быть назначен текущим).

  В этом случае вы можете открыть вкладку **Электронная подпись** окна **Настройка параметров безопасности**, выбрав **Открыть настройки подписи**. С помощью соответствующей кнопки на вкладке **Электронная подпись** вы можете обновить текущий сертификат (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 257). Однако в программе ViPNet Удостоверяющий и ключевой центр такой запрос не будет обработан автоматически, а будет ожидать решения администратора.

  ---

  **Внимание!** Созданный запрос подписывается с использованием ключа электронной подписи, соответствующего текущему сертификату. Однако эта подпись используется не для подтверждения авторства, а только для проверки целостности запроса. Такие запросы имеют статус **Не подписан** (см. «Просмотр запроса на сертификат» на стр. 265).

  ---

- Если срок действия ключа электронной подписи подошел к концу, при этом последний запрос на обновление текущего сертификата либо отклонен, либо находится в состоянии обработки в программе ViPNet Удостоверяющий и ключевой центр.

В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте еще один запрос на обновление текущего сертификата.

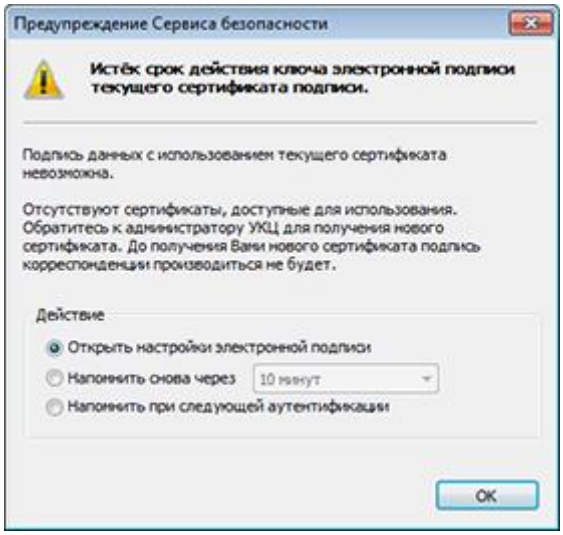



*Рисунок 141. Предупреждение о том, что истек срок действия ключа электронной подписи*

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий:

- **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись**, с помощью которой можно управлять сертификатами.
- **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
- **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Client.

2 Нажмите кнопку **OK**.

# Действительный список аннулированных сертификатов не найден

Предупреждение о том, что действительный список аннулированных сертификатов не найден, появляется при выполнении следующих условий:

- если список аннулированных сертификатов не обнаружен в хранилище пользователя или срок его действия истек;
- если список аннулированных сертификатов, соответствующий текущему сертификату для аутентификации, не обнаружен в хранилище пользователя или срок его действия истек;

- если в окне **Настройка параметров безопасности** на вкладке **Администратор** снят флажок **Игнорировать отсутствие списков аннулированных сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 224).

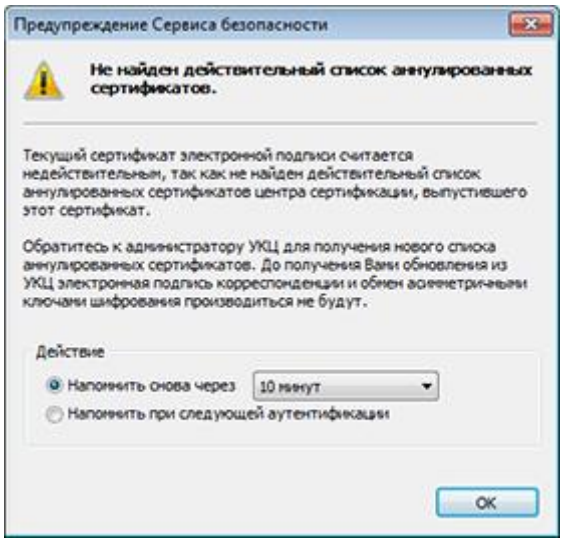



*Рисунок 142. Предупреждение о том, что действительный список аннулированных сертификатов не найден*

При появлении окна с таким предупреждением:

- Обратитесь к администратору вашей сети ViPNet для получения нового списка аннулированных сертификатов.
- Выберите одно из предложенных действий:
  - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
  - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Client.

  После этого нажмите кнопку **OK**.

# Сертификат, изданный по инициативе администратора, введен в действие

Предупреждение о том, что введен в действие сертификат, изданный по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр, появляется при выполнении следующих условий:

- В окне **Настройка параметров безопасности** на вкладке **Электронная подпись** (см. Рисунок 107 на стр. 257) установлен флажок **Автоматически вводить в действие сертификаты, изданные по инициативе администратора УКЦ**.

- В составе обновления получены ключи, сформированные администратором программы ViPNet Удостоверяющий и ключевой центр без запроса со стороны пользователя и содержащие новый сертификат пользователя и ключ электронной подписи.

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий:

   - **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись** (см. Рисунок 107 на стр. 257), с помощью которой можно просмотреть сведения о текущем сертификате, а также управлять сертификатами.
   - **Отправить запрос на обновление сертификата** — для формирования запроса на обновление текущего сертификата с помощью мастера обновления сертификатов (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 257).

     Отправлять запрос на обновление сертификата следует в том случае, если политика безопасности вашей организации запрещает использовать ключ электронной подписи, сформированный не вами лично, а на сетевом узле администратора. В результате обновления вам будет доставлен сертификат, который будет соответствовать ключу электронной подписи, сформированному на вашем компьютере.

2 Нажмите кнопку **OK**.

# Срок действия сертификата, используемого при аутентификации, подходит к концу

Если пользователь выбрал способ аутентификации в ПО ViPNet Client при помощи сертификата на устройстве, за 45 дней до истечения срока действия этого сертификата появится соответствующее предупреждение сервиса безопасности. Вид предупреждения зависит от того, хранятся ли на внешнем устройстве другие сертификаты, подходящие для аутентификации.

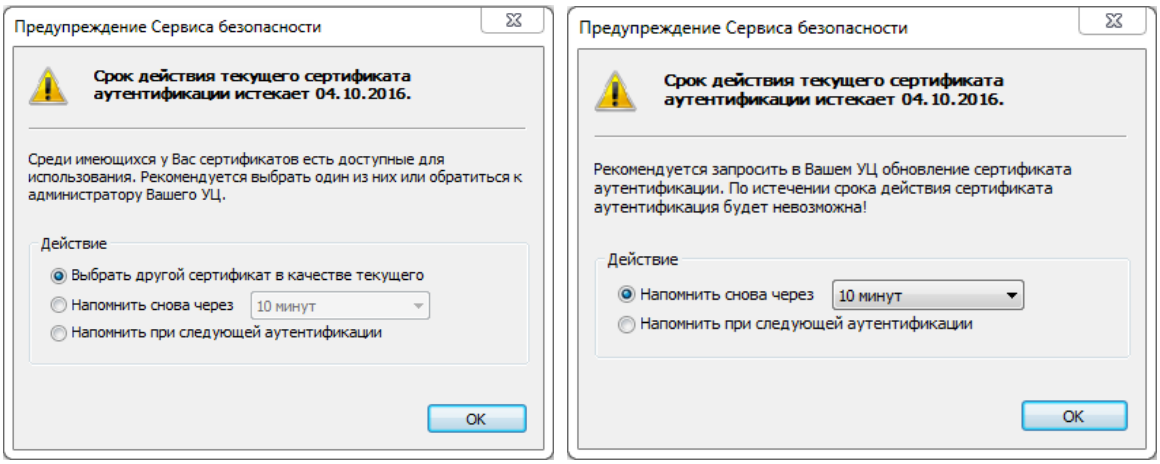



*Рисунок 143. Предупреждения о скором истечении срока действия сертификата, используемого при аутентификации*

Выполните следующие действия:

- Если на внешнем устройстве найдены другие сертификаты, подходящие для аутентификации, и соответствующие им списки аннулированных сертификатов установлены в хранилище и являются действительными, выберите одно из предложенных действий:
    - **Выбрать другой сертификат в качестве текущего** — для назначения другого сертификата для аутентификации с помощью окна **Выбор сертификата**.
    - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
    - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске ПО ViPNet Client.
- Если на внешнем устройстве нет других подходящих для аутентификации сертификатов, выберите одно из двух действий, чтобы настроить напоминание, и затем получите новый сертификат для аутентификации (см. «Особенности аутентификации с помощью сертификата на устройстве» на стр. 74).
- Если на внешнем устройстве есть другие подходящие для аутентификации сертификаты, но соответствующие им CRL просрочены либо не установлены, выберите одно из двух действий, чтобы настроить напоминание, и затем обратитесь к администратору вашей сети ViPNet для получения соответствующего списка аннулированных сертификатов. После обновления CRL или установки его в хранилище при следующей проверке появится окно предупреждения о скором истечении срока действия сертификата, в котором вы сможете выбрать действие **Выбрать другой сертификат в качестве текущего**.

# Срок сертификата, используемого при аутентификации, истек

Если срок действия сертификата, используемого при аутентификации, истек, появится соответствующее предупреждение сервиса безопасности.

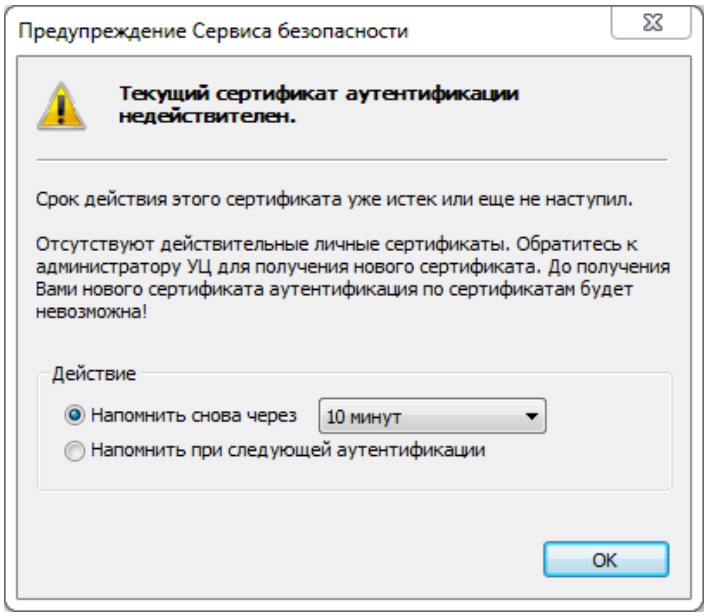



*Рисунок 144. Предупреждения об истечении срока действия сертификата, используемого при аутентификации*

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий, чтобы настроить напоминание.
2. Получите новый сертификат для аутентификации (см. «Особенности аутентификации с помощью сертификата на устройстве» на стр. 74).

---

**Внимание!** Если вы используете программу ViPNet Деловая почта, необходимо заменить сертификат, используемый для аутентификации, до истечения его срока действия, чтобы не выполнять повторную установку ключей. В противном случае после повторной установки ключей будет потерян доступ к зашифрованным письмам программы ViPNet Деловая почта (в том числе в архивах).

---

# Сертификат, используемый при аутентификации, недействителен

Предупреждение сервиса безопасности о недействительном сертификате, используемом при аутентификации, появляется в случае, когда сертификат издателя не установлен в системное хранилище **Доверенные корневые сертификаты**.

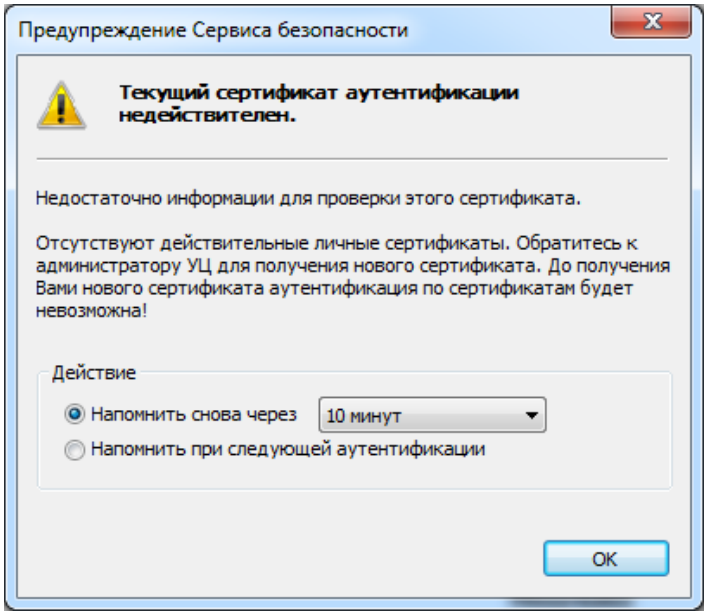



*Рисунок 145. Предупреждение о недействительном сертификате, используемом при аутентификации*

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий, чтобы настроить напоминание.

2 Обратитесь к администратору вашей сети ViPNet, чтобы получить сертификат издателя и затем установите его в системное хранилище **Доверенные корневые сертификаты**. Для этого дважды щелкните по сертификату и следуйте указаниям мастера установки сертификатов (см. Установка в хранилище вручную на стр. 252).

# Сертификат, используемый при аутентификации, не найден

Если устройство, используемое для аутентификации с помощью сертификата, не подключено, появится соответствующее предупреждение.

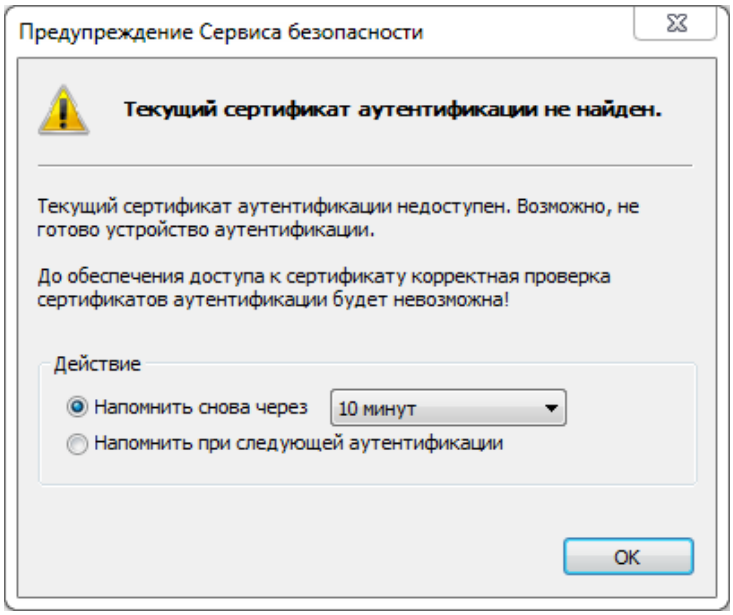



*Рисунок 146. Предупреждение о ненайденном сертификате, используемом при аутентификации*

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий, чтобы настроить напоминание.
2. Подключите внешнее устройство с сертификатом, который используется для аутентификации.

# B

# Общие сведения о сертификатах и ключах

# Основы криптографии

Криптография используется для решения трех основных задач:

- обеспечение конфиденциальности данных;
- контроль целостности данных;
- обеспечение подлинности авторства данных.

Первая задача решается с помощью симметричных алгоритмов шифрования. Для решения второй и третьей задач требуется использование асимметричных алгоритмов и электронной подписи.

В данном разделе содержится упрощенное описание алгоритмов с симметричным ключом, с асимметричным ключом, электронной подписи, а также приводятся примеры использования этих алгоритмов в информационных системах (приведенные примеры не относятся к технологии ViPNet).

## Симметричное шифрование

В симметричных алгоритмах для зашифрования и расшифрования применяется один и тот же криптографический ключ. Для того чтобы и отправитель, и получатель могли прочитать исходный текст (или другие данные, не обязательно текстовые), обе стороны должны знать ключ алгоритма.

На схеме ниже изображен процесс симметричного зашифрования и расшифрования.

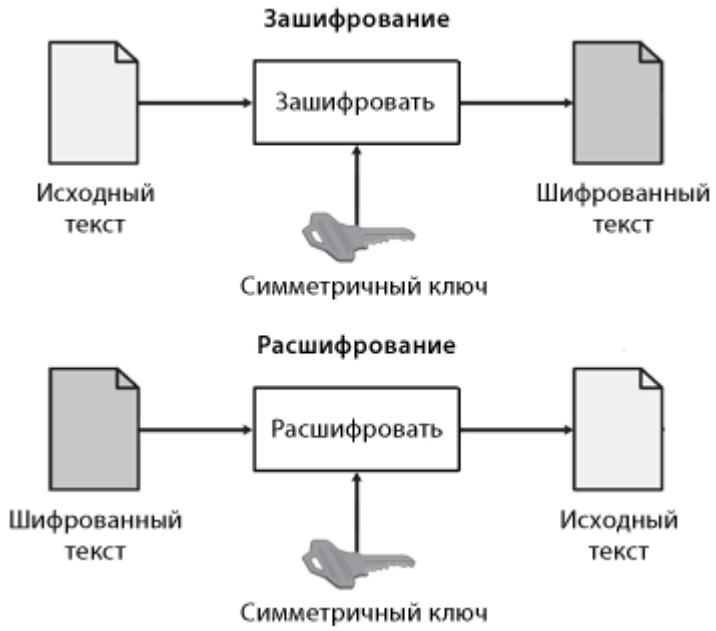



*Рисунок 147. Зашифрование и расшифрование на симметричном ключе*

Симметричные алгоритмы шифрования способны обрабатывать большое количество данных за короткое время благодаря использованию для зашифрования и расшифрования одного и того же

ключа, а также благодаря простоте симметричных алгоритмов по сравнению с асимметричными. Поэтому симметричные алгоритмы часто используют для шифрования больших массивов данных.

Для шифрования данных с помощью симметричного алгоритма криптографическая система использует симметричный ключ. Длина ключа (обычно выражаемая в битах) зависит от алгоритма шифрования и программы, которая использует этот алгоритм.

С помощью симметричного ключа исходный (открытый) текст преобразуется в шифрованный (закрытый) текст. Затем шифрованный текст отправляется получателю. Если получателю известен симметричный ключ, на котором зашифрован текст, получатель может преобразовать шифрованный текст в исходный вид.

**Примечание.** На практике симметричный ключ нужно передать получателю каким-либо надежным способом. Обычно создается симметричный ключ парной связи, который передается получателю лично. Затем для шифрования используются случайные (сессионные) симметричные ключи, которые зашифровываются на ключе парной связи и в таком виде предаются по различным каналам вместе с шифрованным текстом.

Наибольшую угрозу безопасности информации при симметричном шифровании представляет перехват симметричного ключа парной связи. Если он будет перехвачен, злоумышленники смогут расшифровать все данные, зашифрованные на этом ключе.

# Асимметричное шифрование

Асимметричные алгоритмы шифрования используют два математически связанных ключа: открытый ключ и закрытый ключ. Для зашифрования применяется открытый ключ, для расшифрования — закрытый ключ.

Открытый ключ распространяется свободно. Закрытым ключом владеет только пользователь, который создает пару асимметричных ключей. Закрытый ключ следует хранить в секрете, чтобы исключить возможность его перехвата.

Использование двух различных ключей для зашифрования и расшифрования, а также более сложный алгоритм делают процесс шифрования с помощью асимметричных ключей гораздо более медленным, чем шифрование с помощью симметричных ключей.

Открытый ключ может быть использован любыми лицами для отправки зашифрованных данных владельцу закрытого ключа. При этом парой ключей владеет только получатель зашифрованных данных. Таким образом, только получатель может расшифровать эти данные с помощью имеющегося у него закрытого ключа.

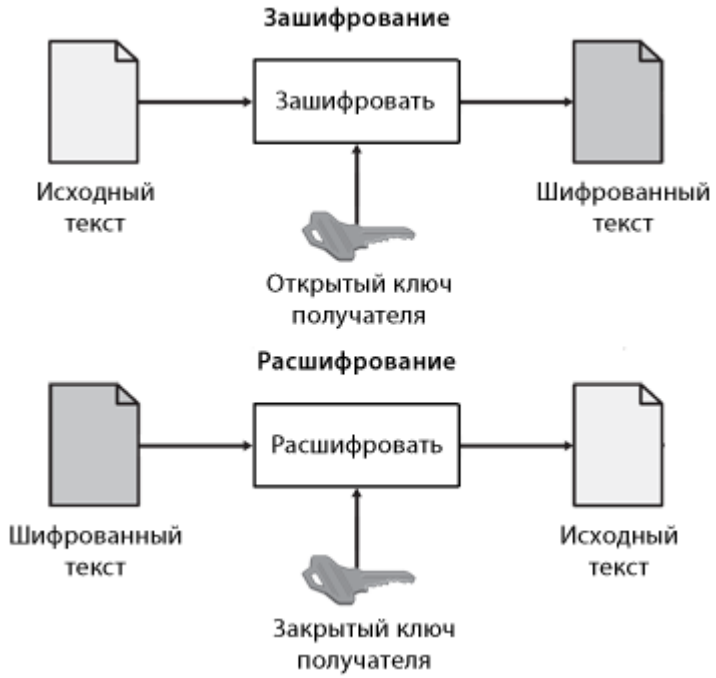



*Рисунок 148. Зашифрование и расшифрование на асимметричном ключе*

**Примечание.** На практике асимметричные алгоритмы в чистом виде используются очень редко. Обычно данные зашифровываются с помощью симметричного алгоритма, а затем с помощью асимметричного алгоритма зашифровывается только симметричный ключ. Комбинированные (гибридные) криптографические алгоритмы рассматриваются ниже (см. «Сочетание симметричного и асимметричного шифрования» на стр. 305).

# Сочетание симметричного и асимметричного шифрования

В большинстве приложений симметричные и асимметричные алгоритмы применяются совместно, что позволяет использовать преимущества обоих алгоритмов.

В случае совместного использования симметричного и асимметричного алгоритмов:

- Исходный текст преобразуется в шифрованный с помощью симметричного алгоритма шифрования. Преимущество этого алгоритма заключается в высокой скорости шифрования.
- Для передачи получателю симметричный ключ, на котором был зашифрован текст, зашифровывается с помощью асимметричного алгоритма. Преимущество асимметричного алгоритма заключается в том, что только владелец закрытого ключа сможет расшифровать симметричный ключ.

На следующем рисунке изображен процесс шифрования с помощью комбинированного алгоритма.

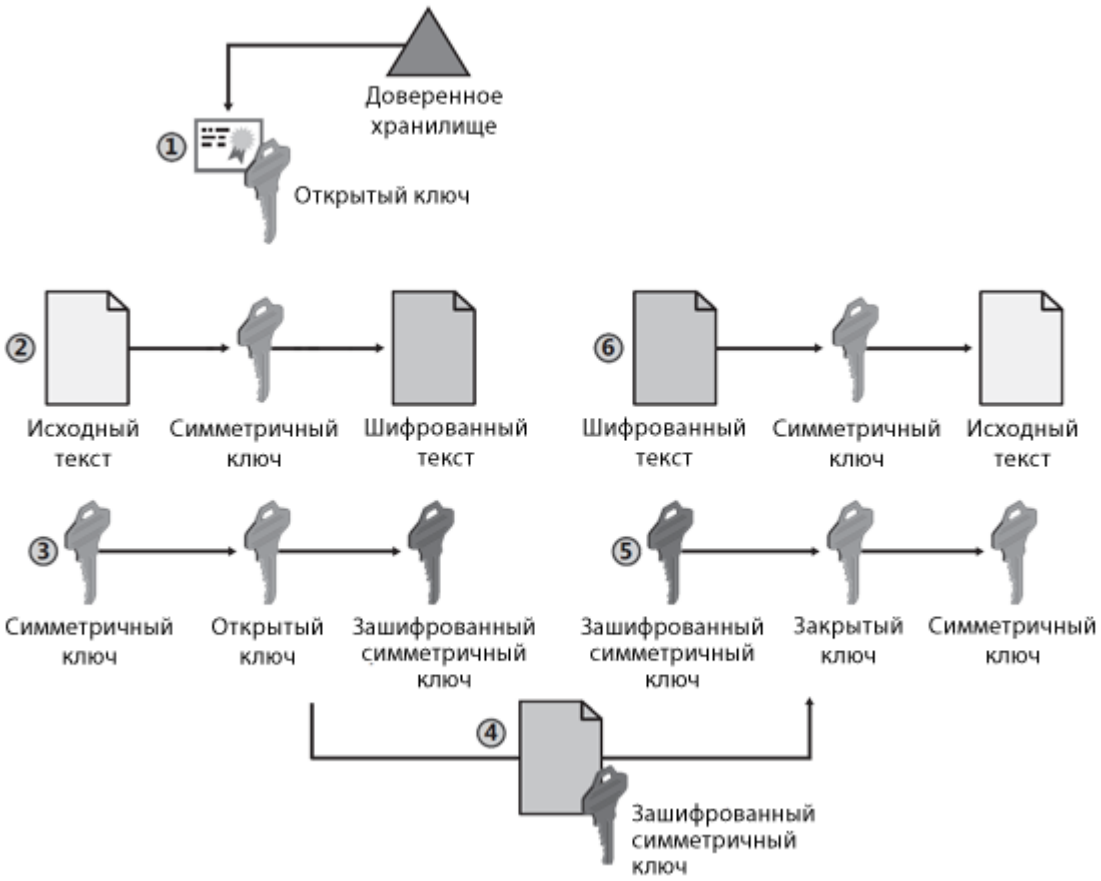



*Рисунок 149. Шифрование с помощью комбинированного алгоритма*

1. Отправитель запрашивает открытый ключ получателя из доверенного хранилища.
2. Отправитель создает симметричный ключ и зашифровывает с его помощью исходный текст.
3. Симметричный ключ зашифровывается на открытом ключе получателя, чтобы предотвратить перехват ключа во время передачи.
4. Зашифрованный симметричный ключ и шифрованный текст передаются получателю.
5. С помощью своего закрытого ключа получатель расшифровывает симметричный ключ.
6. С помощью симметричного ключа получатель расшифровывает шифрованный текст, в результате он получает исходный текст.

# Сочетание хэш-функции и асимметричного алгоритма электронной подписи

Электронная подпись защищает данные следующим образом:

- Для подписания данных используется хэш-функция, с помощью которой определяется хэш-сумма исходных данных. По хэш-сумме можно определить, имеют ли место какие-либо изменения в этих данных.

- Полученная хэш-сумма подписывается электронной подписью, позволяя подтвердить личность подписавшего. Кроме того, электронная подпись не позволяет подписавшему лицу отказаться от авторства, так как только оно владеет ключом электронной подписи, использованным для подписания. Невозможность отказаться от авторства называется неотрекаемостью.

Большинство приложений, осуществляющих электронную подпись, используют сочетание хэш-функции и асимметричного алгоритма подписи. Хэш-функция позволяет проверить целостность исходного сообщения, а электронная подпись защищает полученную хэш-функцию от изменения и позволяет определить личность автора сообщения.

Приведенная ниже схема иллюстрирует применение хэш-функции и асимметричного алгоритма в электронной подписи.

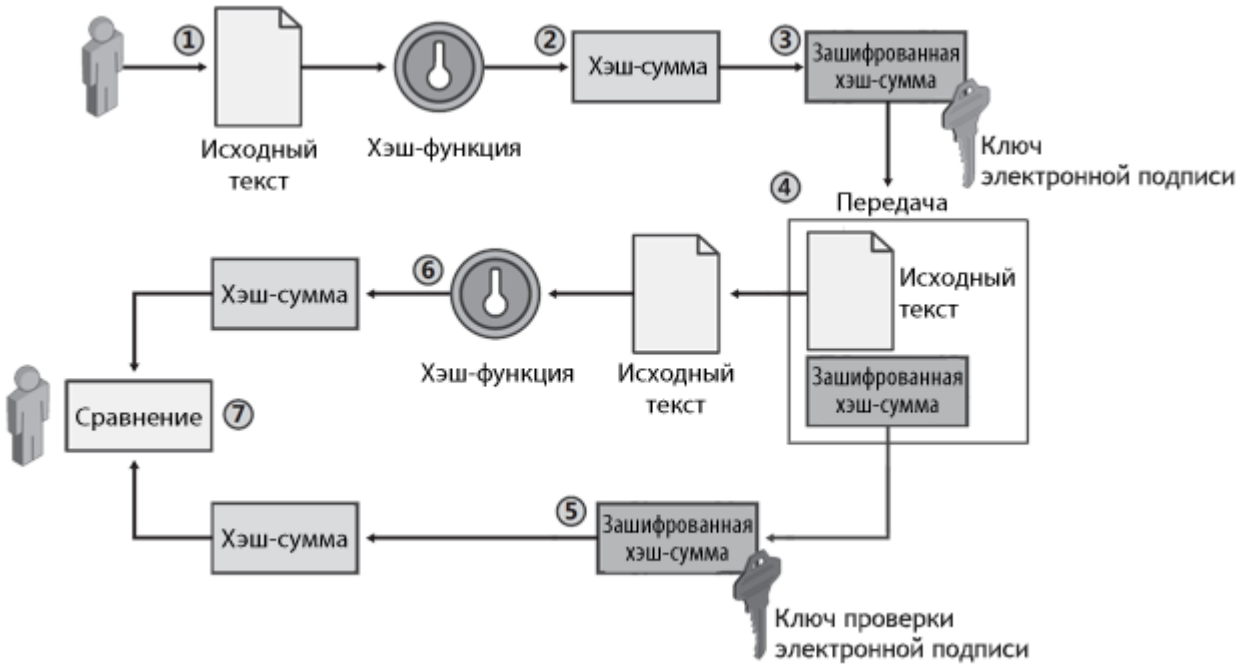



*Рисунок 150. Применение хэш-функции и асимметричного алгоритма в электронной подписи*

1 Отправитель создает файл с исходным сообщением.

2 Программное обеспечение отправителя вычисляет хэш-сумму исходного сообщения.

3 Полученная хэш-сумма зашифровывается с помощью ключа электронной подписи отправителя.

4 Исходное сообщение и зашифрованная хэш-функция передаются получателю.

---

**Примечание.** При использовании электронной подписи исходное сообщение не зашифровывается. Само сообщение может быть изменено, но любые изменения сделают хэш-сумму, передаваемую вместе с сообщением, недействительной.

---

5 Получатель расшифровывает хэш-сумму сообщения с помощью ключа проверки электронной подписи отправителя. Ключ проверки электронной подписи может быть передан вместе с сообщением или получен из доверенного хранилища.

6 Получатель использует ту же хэш-функцию, что и отправитель, чтобы вычислить хэш-сумму полученного сообщения.

7 Вычисленная хэш-сумма сравнивается с хэш-суммой, полученной от отправителя. Если эти хэш-суммы различаются между собой, то сообщение или хэш-сумма были изменены при передаче.

# Общие сведения о сертификатах ключей проверки электронной подписи

## Определение и назначение

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

- Ключ электронной подписи — для формирования электронной подписи (см. «Электронная подпись» на стр. 404) и расшифрования сообщения. Ключ электронной подписи хранится в тайне и не подлежит распространению.
- Ключ проверки электронной подписи — для проверки электронной подписи и зашифрования сообщения. Ключ проверки электронной подписи известен всем участникам информационного обмена и может передаваться по незащищенным каналам связи.

Таким образом, криптография с ключом проверки электронной подписи позволяет выполнять следующие операции:

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

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

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

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

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

Сертификат включает ключ проверки электронной подписи и список дополнительных атрибутов, принадлежащих пользователю (владельцу сертификата). К таким атрибутам относятся: имена владельца и издателя сертификата, номер сертификата, время действия сертификата, предназначение ключа проверки электронной подписи (электронная подпись, шифрование) и так далее. Структура и протоколы использования сертификатов определяются международными стандартами (см. «Структура» на стр. 312).

Различаются следующие виды сертификатов:

- Сертификат пользователя — для зашифрования исходящих сообщений и для проверки электронной подписи на стороне получателя.
- Сертификат издателя — сертификат, с помощью которого был издан текущий сертификат пользователя. Помимо основных возможностей, которые предоставляет сертификат пользователя, сертификат издателя позволяет также проверить все сертификаты, подписанные с помощью ключа электронной подписи, соответствующего этому сертификату.
- Корневой сертификат — самоподписанный сертификат издателя, являющийся главным из вышестоящих сертификатов. Корневой сертификат не может быть проверен с помощью другого сертификата, поэтому пользователь должен безусловно доверять источнику, из которого получен данный сертификат.
- Кросс-сертификат — это сертификат администратора удостоверяющего центра, изданный администратором другого удостоверяющего центра. Таким образом, для кросс-сертификата значения полей «Издатель» и «Субъект» различны и определяют разные удостоверяющие центры. С помощью кросс-сертификатов устанавливаются доверительные отношения между различными удостоверяющими центрами. В зависимости от модели доверительных отношений, установленной между удостоверяющими центрами (см. «PKI и асимметричная криптография» на стр. 314), может использоваться либо как сертификат издателя (в иерархической модели), либо для проверки сертификатов пользователей другой сети (в распределенной модели).


*Рисунок 151. Типы сертификатов*

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

Таким образом, криптография с ключом проверки электронной подписи и инфраструктура обмена сертификатами ключей проверки электронной подписи (см. «PKI и асимметричная криптография» на стр. 314) позволяют выполнять шифрование сообщений, а также предоставляют возможность подписывать сообщения с помощью электронной подписи.

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

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

# Структура

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

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

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

К обязательным полям относятся:

- номер версии стандарта X.509,
- серийный номер сертификата,
- идентификатор алгоритма подписи издателя,
- идентификатор алгоритма подписи владельца,
- имя издателя,
- период действия,
- ключ проверки электронной подписи владельца,
- имя владельца сертификата.

---

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

---

К необязательным полям относятся:

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

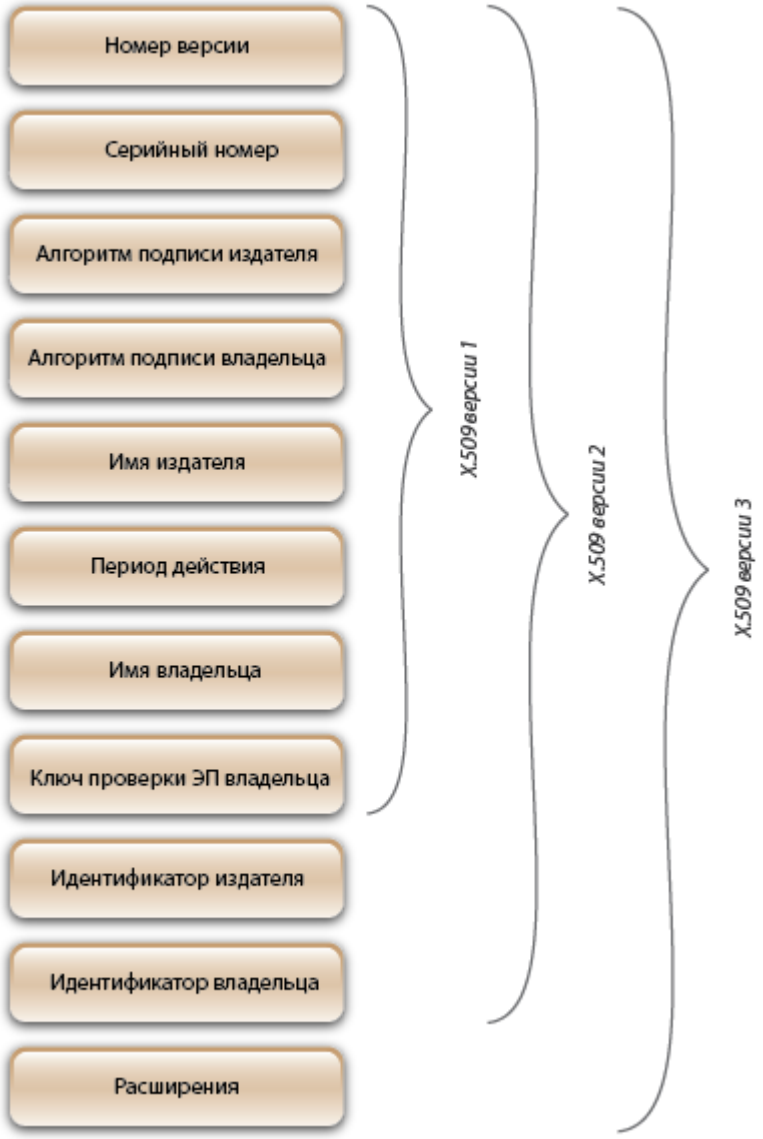
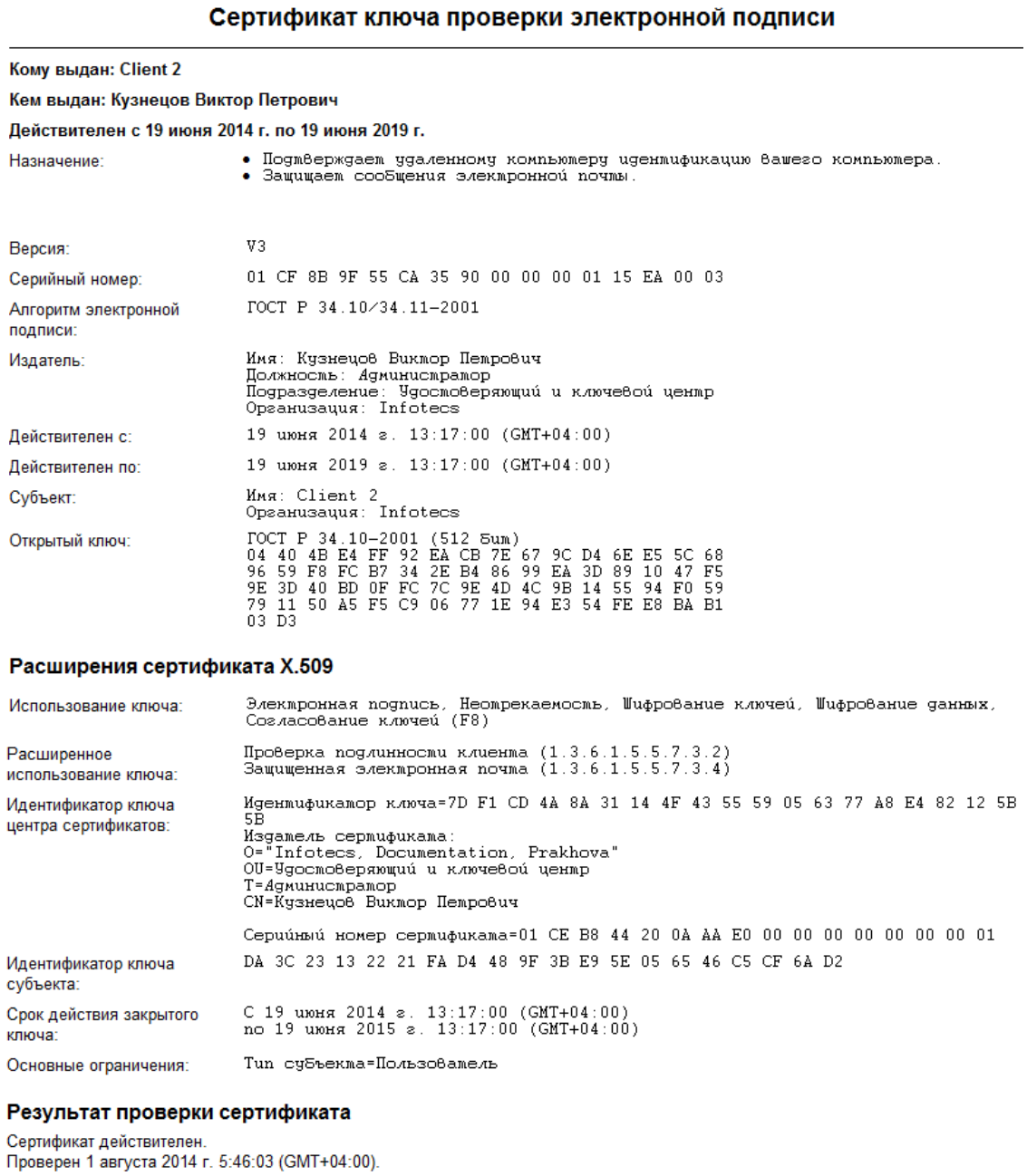



*Рисунок 152. Структура сертификата, соответствующего стандарту X.509 версий 1, 2 и 3*



**Сертификат ключа проверки электронной подписи**

**Кому выдан: Client 2**

**Кем выдан: Кузнецов Виктор Петрович**

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

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

**Расширения сертификата X.509**

| | |
|---|---|
| Использование ключа: | Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8) |
| Расширенное использование ключа: | Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)<br>Защищенная электронная почта (1.3.6.1.5.5.7.3.4) |
| Идентификатор ключа центра сертификатов: | Идентификатор ключа=7D F1 CD 4A 8A 31 14 4F 43 55 59 05 63 77 A8 E4 82 12 5B 5B<br>Издатель сертификата:<br>O="Infotecs, Documentation, Prakhova"<br>OU=Удостоверяющий и ключевой центр<br>T=Администратор<br>CN=Кузнецов Виктор Петрович<br><br>Серийный номер сертификата=01 CE B8 44 20 0A AA E0 00 00 00 00 00 00 00 01 |
| Идентификатор ключа субъекта: | DA 3C 23 13 22 21 FA D4 48 9F 3B E9 5E 05 65 46 C5 CF 6A D2 |
| Срок действия закрытого ключа: | С 19 июня 2014 г. 13:17:00 (GMT+04:00)<br>по 19 июня 2015 г. 13:17:00 (GMT+04:00) |
| Основные ограничения: | Тип субъекта=Пользователь |

**Результат проверки сертификата**

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

*Рисунок 153. Пример сертификата ViPNet, соответствующего стандарту X.509 версии 3*

# PKI и асимметричная криптография

Одной из реализаций инфраструктуры, позволяющей управлять сертификатами ключа проверки электронной подписи, является технология PKI (инфраструктура открытых ключей) (на стр. 396). PKI обслуживает жизненный цикл сертификата: издание сертификатов, хранение, резервное копирование, печать, взаимную сертификацию, ведение списков аннулированных сертификатов (CRL), автоматическое обновление сертификатов после истечения срока их действия.

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

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

- В иерархической модели доверительных отношений удостоверяющие центры объединяются в древовидную структуру, в основании которой находится головной удостоверяющий центр. Головной удостоверяющий центр выдает кросс-сертификаты подчиненным ему центрам, тем самым обеспечивая доверие к ключам проверки электронной подписи этих центров. Каждый удостоверяющий центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие к сертификату каждого удостоверяющего центра основано на заверении его ключом вышестоящего центра. Сертификат головного удостоверяющего центра (корневой сертификат (на стр. 400)) является самоподписанным. В остальных удостоверяющих центрах администраторы не имеют собственных корневых сертификатов и для установления доверительных отношений формируют запросы на кросс-сертификат к своим вышестоящим удостоверяющим центрам.

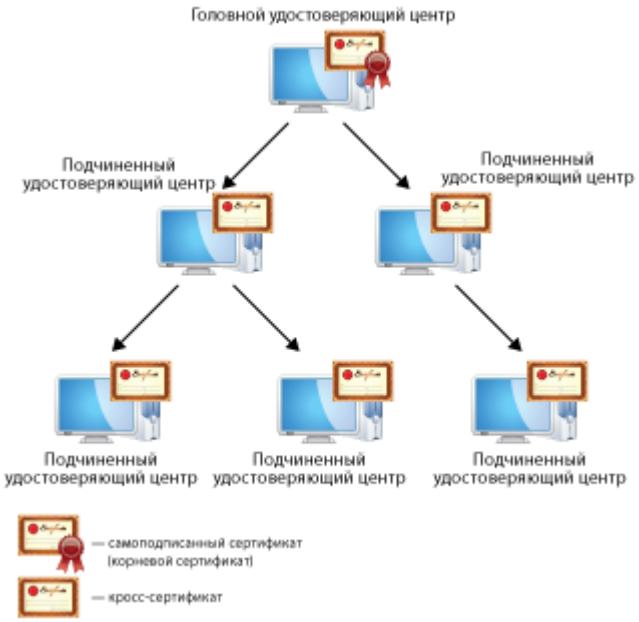



*Рисунок 154. Иерархическая модель доверительных отношений*

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

каждом удостоверяющем центре в дополнение к корневому сертификату имеются кросс-сертификаты, изданные для администраторов в других удостоверяющих центрах.

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

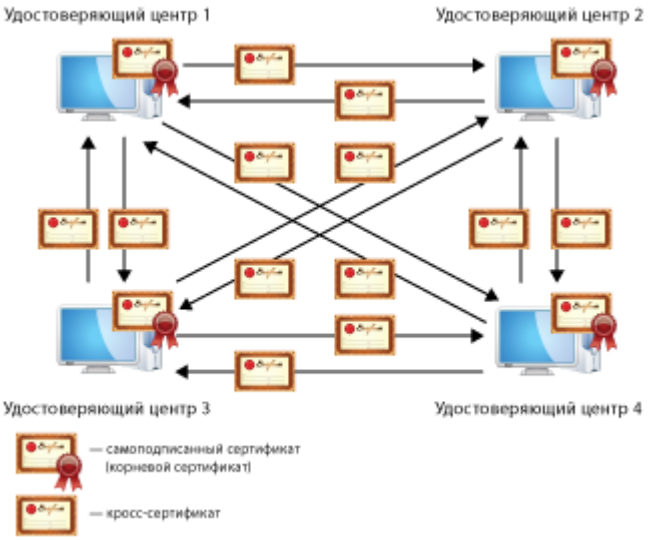



*Рисунок 155. Распределенная модель доверительных отношений*

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

# Использование сертификатов для шифрования электронных документов

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

## Зашифрование

1. Пользователь создает электронный документ.
2. Открытый ключ получателя извлекается из сертификата.

3 Формируется симметричный сеансовый ключ, для однократного использования в рамках данного сеанса.

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

5 Сеансовый ключ зашифровывается на ключе, который вырабатывается по протоколу Диффи — Хеллмана с использованием открытого ключа получателя.

6 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

7 Документ отправляется.


*Рисунок 156. Процесс зашифрования электронных документов*

## Расшифрование

1 Пользователь получает электронный документ.

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

3 Закрытый ключ получателя документа извлекается из контейнера ключей.

4 Сеансовый ключ расшифровывается с использованием закрытого ключа получателя.

5 Документ расшифровывается с использованием расшифрованного сеансового ключа.

6 Расшифрованный документ доступен получателю.


*Рисунок 157. Процесс расшифрования электронных документов*

# Использование сертификатов для подписания электронных документов

Когда отправитель подписывает документ, он использует ключ электронной подписи, соответствующий ключу проверки электронной подписи, который хранится в сертификате. Когда получатель проверяет электронную подпись (см. «Электронная подпись» на стр. 404) сообщения, он извлекает ключ проверки электронной подписи из сертификата отправителя.

## Подписание

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

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


*Рисунок 158. Процесс подписания электронного документа*

## Проверка подписи

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

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


*Рисунок 159. Процесс проверки электронной подписи*

# Использование сертификатов для подписания и шифрования электронных документов

## Подписание и зашифрование

1 Пользователь создает электронный документ.

2 Вычисляется значение хэш-функции документа.

3 Ключ электронной подписи отправителя извлекается из контейнера ключей.

4 Открытый ключ получателя извлекается из сертификата получателя.

5 С использованием ключа электронной подписи отправителя на основе значения хэш-функции формируется электронная подпись.

6 Электронная подпись прикрепляется к документу.

7 Формируется симметричный сеансовый ключ, для однократного использования в рамках данного сеанса.

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

9 Сеансовый ключ зашифровывается на ключе, который вырабатывается по протоколу Диффи — Хеллмана с открытого ключа получателя.

10 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

11 Документ отправляется.


*Рисунок 160. Процесс подписания и зашифрования электронных документов*

## Расшифрование и проверка

1 Пользователь получает электронный документ.

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

3 Закрытый ключ получателя документа извлекается из контейнера ключей.

4 Сеансовый ключ расшифровывается с помощью закрытого ключа получателя.

5 Документ расшифровывается с использованием расшифрованного сеансового ключа.

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

7 Вычисляется значение хэш-функции документа.

8 Ключ проверки электронной подписи отправителя извлекается из сертификата отправителя.

9 Электронная подпись расшифровывается с использованием ключа проверки электронной подписи отправителя.

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

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

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

12 Расшифрованный документ доступен получателю.

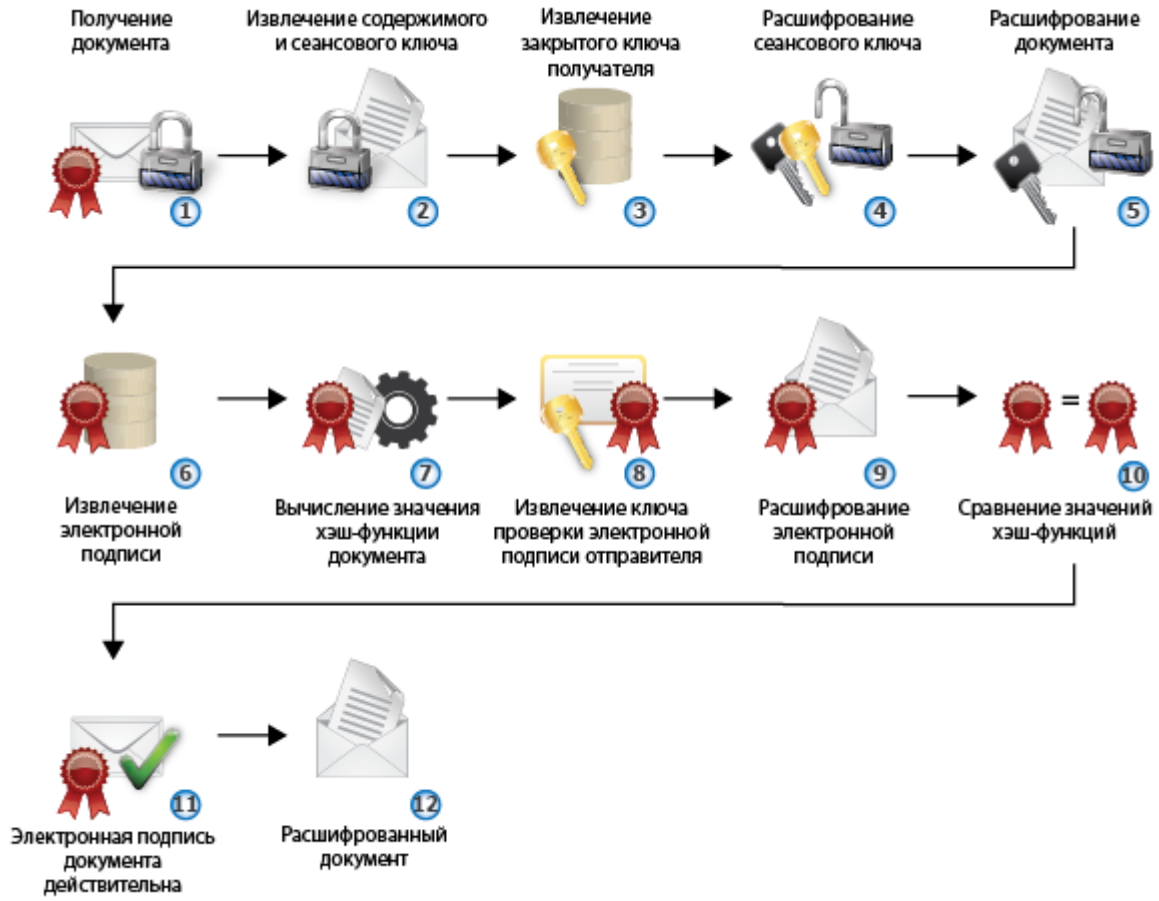



*Рисунок 161. Процесс расшифрования и проверки электронного документа*

# Ключевая система ViPNet

В технологии ViPNet для шифрования применяется комбинация криптографических алгоритмов с симметричными и асимметричными ключами.

*Таблица 9. Применение криптографических алгоритмов в ПО ViPNet*

| Криптографические алгоритмы | |
|---|---|
| **С симметричными ключами** | **С асимметричными ключами** |
| • шифрование IP-трафика<br>• шифрование сообщений программы ViPNet Деловая почта<br>• шифрование прикладных и служебных конвертов | • создание и проверка электронной подписи<br>• шифрование в сторонних приложениях с помощью криптопровайдера ViPNet CSP |

# Симметричные ключи в ПО ViPNet

Симметричные алгоритмы используются для шифрования информации и контроля ее целостности. Для каждой пары сетевых узлов ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager создается симметричный ключ обмена, предназначенный для шифрования обмена данными между этими сетевыми узлами. Таким образом, формируется матрица симметричных ключей, содержащая данные обо всех созданных для сетевых узлов симметричных ключах обмена. Эта матрица зашифрована, поэтому доступ к ней имеет только программа ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager. Симметричные ключи обмена следует передавать по защищенным каналам (дистрибутивы для первой установки справочников и ключей передаются лично). Если злоумышленники завладеют симметричными ключами, вся система защиты сетевого узла будет скомпрометирована.

Симметричные ключи обмена используются для шифрования IP-трафика, почтовых сообщений, прикладных и транспортных конвертов.


*Рисунок 162. Применение ключей обмена*

Для защиты ключей обмена применяется три уровня шифрования:

- ключи обмена зашифрованы на ключах защиты;
- ключи защиты зашифрованы на персональных ключах;
- в свою очередь, персональные ключи зашифрованы на парольных ключах.

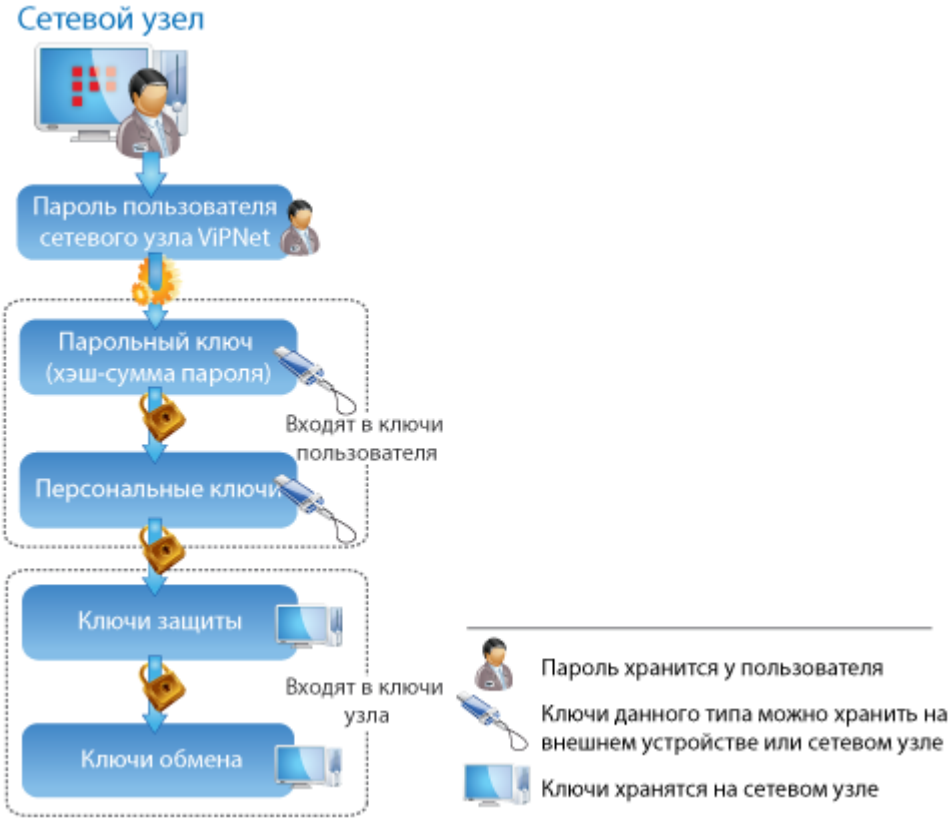



*Рисунок 163. Иерархия защиты ключей обмена на сетевом узле*

При создании структуры сети ViPNet администратор создает в программе ViPNet Administrator или ViPNet Network Manager файл дистрибутива ключей (`*.dst`) для каждого пользователя сетевого узла ViPNet. Файлы дистрибутивов необходимы для установки справочников и ключей на сетевых узлах. Они содержат ключи пользователя (персональный ключ и ключи электронной подписи), набор ключей обмена с другими сетевыми узлами, справочники, необходимые для связи с другими сетевыми узлами, и регистрационный файл `infotecs.re`. Обновление ключей для сетевых узлов производится по инициативе администратора сети ViPNet.

**Примечание.** По собственной инициативе пользователь может сделать запрос на обновление сертификата электронной подписи. Для этого в окне **Настройка параметров безопасности** на вкладке **Подпись** нужно нажать кнопку **Обновить сертификат**.

В ПО ViPNet для шифрования используются следующие симметричные алгоритмы:

- ГОСТ 28147-89 (длина ключа 256 бит) — российский стандарт симметричного шифрования.

- AES (256 бит) — принятый в США стандарт симметричного шифрования на основе алгоритма Rijndael.

По умолчанию используется алгоритм ГОСТ 28147-89. При необходимости можно выбрать алгоритм AES. В сертифицированных версиях ПО ViPNet алгоритм шифрования AES не поддерживается, возможность его выбора отсутствует.

# Асимметричные ключи в ПО ViPNet

При использовании симметричного алгоритма зашифрование и расшифрование выполняются с помощью одного и того же ключа. При использовании асимметричного алгоритма ключ, с помощью которого шифруется сообщение, является открытым (известен всем отправителям), а ключ, с помощью которого это сообщение расшифровывается, является закрытым (известен только получателю зашифрованного сообщения).

Каждый пользователь имеет пару ключей шифрования — открытый ключ и закрытый ключ. Закрытый ключ необходимо держать в тайне, а открытый ключ можно свободно распространять. Между этими ключами существует математическая связь, однако на практике невозможно за конечное время получить закрытый ключ из открытого.

Асимметричные ключи используются в технологии ViPNet для издания сертификатов и создания электронных подписей (см. «Сочетание хэш-функции и асимметричного алгоритма электронной подписи» на стр. 306). Если на компьютере установлено ПО ViPNet, в состав которого входит криптопровайдер ViPNet CSP, асимметричные ключи можно использовать для шифрования (см. «Асимметричное шифрование» на стр. 304). Одна и та же пара асимметричных ключей может использоваться как для шифрования, так и для подписи. Однако, в отличие от шифрования, для подписи используется закрытый ключ (ключ электронной подписи), а для проверки подписи — сертификат ключа проверки электронной подписи. Сертификат содержит открытый ключ (ключ проверки электронной подписи), удостоверенный (в том числе подписанный) уполномоченным лицом (администратором УКЦ), информацию о владельце сертификата, сроке его действия и прочее.

Пару асимметричных ключей можно независимо создать на сетевом узле ViPNet. Для этого в окне **Настройка параметров безопасности** на вкладке **Подпись** нужно сделать запрос на обновление сертификата, выбрав в качестве назначения ключа **Подпись и шифрование**.

**Примечание.** Обновление сертификата требуется в том случае, если истекает срок действия текущего сертификата или закрытого ключа, а также если текущий сертификат не предназначен для шифрования.

Ключ электронной подписи хранится в зашифрованном виде в файле, который называется контейнером ключей. Его следует хранить в тайне от других пользователей: рекомендуется использовать съемные носители или внешние устройства (на стр. 345). Схема защиты ключа электронной подписи в зависимости от места его хранения изображена на следующем рисунке.


*Рисунок 164. Схема защиты ключа электронной подписи*

Если ключ электронной подписи хранится на внешнем устройстве, ключом защиты (см. «Ключ защиты» на стр. 399) для него является парольный ключ. Если ключ электронной подписи хранится на жестком диске или в дистрибутиве ключей, ключом защиты для него является персональный ключ.

Ключи проверки электронной подписи в сетях ViPNet передаются в составе подписанного сообщения программы ViPNet Деловая почта. Также ключи проверки электронной подписи могут храниться в составе сертификатов в общем хранилище сертификатов, например в службе каталогов Active Directory.

Асимметричное шифрование подразумевает отправку зашифрованного сообщения владельцу выбранного при зашифровании сертификата. Зашифрование сообщений можно выполнять в таких приложениях, как Microsoft Outlook, Outlook Express и так далее. Для этого сертификат получателя должен содержать в соответствующем поле адрес электронной почты.

---

**Примечание.** При издании сертификата в программе ViPNet Network Manager адрес электронной почты указать невозможно.

---

Следует понимать, что технология асимметричного шифрования основана на стандартном использовании интерфейса Microsoft CryptoAPI. Следовательно, при использовании данной технологии пользователи ViPNet могут быть не связаны между собой в смысле топологии сети ViPNet (их сети могут не являться доверенными). Для расшифрования сообщения получателю достаточно закрытого ключа, сертификата и установленного на компьютере программного обеспечения, в состав которого входит криптопровайдер ViPNet CSP.

# C

# События, отслеживаемые ПО ViPNet

Все события разделены на группы и подгруппы. Иерархическая схема этих групп изображена на следующем рисунке:


*Рисунок 165. Классификация событий в журнале IP-пакетов*

# Блокированные IP-пакеты

*Таблица 10. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные фильтрами защищенной сети***

| № события | Название события | Описание события |
|---|---|---|
| 1 | **Не найден ключ для сетевого узла** | Не найден ключ для связи с пользователем, идентификатор которого указан в пакете |
| 2 | **Неверное значение имито** | Защищаемые данные или открытая информация криптосистемы были изменены |
| 3 | **IP-пакет блокирован фильтром защищенной сети** | Согласно настройкам фильтров входящий зашифрованный пакет или исходящий предназначенный для шифрования открытый пакет был заблокирован |
| 4 | **Слишком большая разница во времени** | Время отправки пакета отличается от времени приема на величину большую, чем указано в настройке допустимого времени отправки принятых пакетов |
| 7 | **Неизвестный метод шифрования** | Не поддерживается метод шифрования, код которого указан во входящем пакете |
| 8 | **Искаженный IPLIR заголовок** | Недопустимые параметры в расшифрованном пакете |
| 9 | **Неизвестный идентификатор сетевого узла** | Идентификатор отправителя в пакете неизвестен |
| 13 | **Превышено время жизни IP-пакета** | Пакет уничтожен из-за превышения лимита его нахождения в сети |
| 14 | **Получен IP-пакет для другого сетевого узла** | Принят пакет для другого адресата |
| 15 | **Слишком много фрагментов для IP-пакета** | Превышено допустимое количество одновременно обрабатываемых фрагментированных пакетов |
| 16 | **Исчерпана лицензия на количество туннелируемых адресов** | Это событие регистрируется только на координаторе, осуществляющем туннелирование. На координатор одновременно поступили пакеты от большего количества узлов, чем разрешено лицензией |
| 17 | **Неверный IP-адрес** | Поступил пакет с некорректным или неизвестным IP-адресом. Чаще всего событие возникает на координаторе в следующем случае: на координатор поступил зашифрованный пакет, предназначенный для туннелируемого узла данного координатора, но IP-адрес этого узла отсутствует в списке туннелируемых адресов координатора |

| | | |
|---|---|---|
| **18** | **Неизвестный IP-адрес получателя** | В пакете отсутствует или указан неизвестный IP-адрес получателя |
| **19** | **Попытка отправителя послать сообщение от имени чужого узла** | Поступил пакет от узла, который не является его отправителем |
| **70** | **Пакет заблокирован транзитным фильтром для защищенного узла** | Это событие регистрируется только на координаторе с операционной системой Linux. Пакет заблокирован фильтрами для транзитного зашифрованного трафика |

*Таблица 11. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные фильтрами открытой сети***

| № события | Название события | Описание события |
|---|---|---|
| **22** | **Незашифрованный IP-пакет от сетевого узла** | От защищённого адресата пришел открытый пакет |
| **23** | **Незашифрованный широковещательный IP-пакет от сетевого узла** | От защищённого адресата пришел открытый широковещательный пакет |
| **24** | **Открытый IP-пакет для служб ViPNet** | Служебный трафик ViPNet поступил в открытом виде |
| **30** | **Локальный IP-пакет блокирован фильтром открытой сети** | Пакет блокируется локальным фильтром открытой сети или для пакета не удалось найти подходящий фильтр |
| **31** | **Транзитный IP-пакет блокирован фильтром открытой сети** | Это событие регистрируется только на координаторе. Пакет блокируется транзитным фильтром открытой сети или для пакета не удалось найти подходящий фильтр |
| **32** | **Широковещательный IP-пакет блокирован фильтром открытой сети** | Пакет блокируется фильтром открытого широковещательного трафика или для пакета не удалось найти подходящий фильтр |
| **33** | **IP-пакет блокирован фильтром антиспуфинга** | Это событие регистрируется только на координаторе. Найден соответствующий фильтр в таблице антиспуфинга |
| **37** | **Пакет блокирован фильтром для туннелируемых узлов** | Это событие регистрируется только на координаторе. Пакет блокируется фильтром трафика туннелируемых узлов или для пакета не удалось найти подходящий фильтр |
| **39** | **IP-пакет блокирован фильтрами по умолчанию при загрузке компьютера** | Пакет заблокирован фильтрами по умолчанию при загрузке компьютера |

*Таблица 12. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные по другим причинам***

| № события | Название события | Описание события |
|---|---|---|
| 80 | **Размер IP-пакета меньше допустимого** | Размер IP-пакета меньше минимально возможного |
| 81 | **Недопустимая версия протокола IP** | В данной версии поддерживается только протокол IP версии 4 |
| 82 | **Недопустимая длина заголовка IP** | Длина заголовка протокола IP меньше минимально возможного |
| 83 | **Недопустимая длина IP-пакета** | Длина пакета меньше, чем указано в заголовке протокола IP |
| 84 | **Несовпадение контрольной суммы IP** | Подсчитанное значение контрольной суммы IP-пакета не совпадает со значением, указанным в пакете |
| 85 | **Размер заголовка TCP меньше минимально допустимого** | Недопустимо короткий заголовок протокола TCP |
| 86 | **Размер заголовка UDP меньше минимально допустимого** | Недопустимо короткий заголовок протокола UDP |
| 87 | **Процедура дефрагментации завершилась с ошибкой** | Ошибка при попытке дефрагментации входящего IP-пакета. |
| 88 | **Широковещательный адрес отправителя IP-пакета** | Адрес отправителя в пакете указан широковещательный |
| 89 | **Процедура дефрагментации завершилась с ошибкой** | Ошибка при попытке дефрагментации входящего IP-пакета. |
| 90 | **Недостаточно ресурсов для криптообработки** | Невозможно создать ключ для зашифрования или расшифрования пакета из-за недостаточности свободных ресурсов криптодрайвера.<br>Если эта ошибка стабильно проявляется, обратитесь в службу поддержки компании «ИнфоТеКС». Возможно, потребуется обновление версии драйвера, использующего больше машинных ресурсов, или более совершенная модель компьютера. |
| 91 | **IP-пакет получен во время инициализации драйвера** | Блокировка всех пакетов во время инициализации драйвера |
| 92 | **Слишком большой размер IP-пакета** | Размер пакета ограничен параметром 48 Кбайт |

| | | |
|---|---|---|
| **93** | **Превышено время сборки фрагментов IP-пакета** | За допустимое время получены не все фрагменты фрагментированного пакета |
| **95** | **Обнаружен сетевой узел с таким же идентификатором** | В сети появился узел с таким же идентификатором, но другим IP-адресом |
| **97** | **IP-пакет блокирован фильтром SQL** | Соединение заблокировано фильтром Microsoft SQL |
| **101** | **Не найден маршрут для транзитного IP-пакета** | Это событие регистрируется только на координаторе. Не найдено правило для транзитного пакета в таблице маршрутов |
| **103** | **Превышено максимальное количество соединений** | Количество уже установленных соединений превышает максимально допустимое ПО ViPNet (не лицензией) |
| **104** | **Соединение уже существует** | Если параметры исходящих пакетов для создаваемого соединения совпадают с уже существующими, то такое соединение блокируется |
| **105** | **Не удалось выделить динамический порт для правила трансляции адресов** | Это событие регистрируется только на координаторе. Координатор не смог выделить порт для динамического правила трансляции адресов (например, все порты в пуле закончились) |
| **111** | **Не найден ключ обмена** | Не найден ключ для связи с сетевым узлом получателя |
| **112** | **Нарушена имитовставка открытой части зашифрованного пакета 4.2** | Неверное значение имито для транзитного зашифрованного трафика |
| **113** | **Неизвестный ID источника** | Неизвестный идентификатор сетевого узла–источника транзитного зашифрованного пакета |
| **115** | **Не удалось найти маршрут для IP-пакета** | По каким-либо причинам не найден маршрут в таблице маршрутизации |
| **116** | **Сетевой интерфейс не найден** | IP-пакет не может быть отправлен, так как не найден сетевой интерфейс |
| **117** | **Не удалось разрешить MAC-адрес по IP-адресу** | Не удалось определить MAC-адрес получателя пакета по его IP-адресу |
| **118** | **Не удалось произвести шифрование IP-пакета** | Ошибка при шифровании исходящего IP-пакета для защищенного узла |
| **119** | **Неизвестный формат IPLIR заголовка** | Получен зашифрованный IP-пакет неизвестного формата |
| **120** | **Несогласованная информация о способе доступа до сетевого узла** | Ошибка при отправке IP-пакета для защищенного узла |

| | | |
|---|---|---|
| 121 | **Ошибка в работе кластера** | Это событие регистрируется только на кластере ViPNet. Внутренняя ошибка кластера |
| 122 | **Неизвестный протокол канального уровня** | Получен IP-пакет неизвестного протокола |

**Примечание.** Если вы используете Windows Server 2003 или более позднюю версию Windows, события 82 и 89 не фиксируются в журнале IP-пакетов, так как операционная система автоматически блокирует соответствующие IP-пакеты.

# Пропущенные IP-пакеты и служебные события

*Таблица 13. Группа **Все IP-пакеты\Все пропущенные IP-пакеты\Пропущенные зашифрованные IP-пакеты***

| № события | Название события | Описание события |
|---|---|---|
| 40 | **Пропущен зашифрованный IP-пакет** | Пропущен зашифрованный пакет |
| 41 | **Пропущен пакет, зашифрованный на широковещательном ключе** | Пропущен IP-пакет, зашифрованный на ключе для широковещательных пакетов |
| 44 | **Осуществлена маршрутизация зашифрованного транзитного IP-пакета с изменением его адреса** | Это событие регистрируется только на координаторе. Пакет направлен на другой узел путём подмены в нём адреса получателя |
| 45 | **Зашифрован (расшифрован) пакет туннелируемого узла** | Это событие регистрируется только на координаторе. Зашифрован или расшифрован пакет для туннелируемого узла |

*Таблица 14. Группа **Все IP-пакеты\Все пропущенные IP-пакеты\Пропущенные незашифрованные IP-пакеты***

| № события | Название события | Описание события |
|---|---|---|
| 60 | **Пропущен незашифрованный локальный IP-пакет** | Найден разрешающий фильтр открытой сети для локальных IP-пакетов |
| 61 | **Пропущен незашифрованный широковещательный IP-пакет** | Найден разрешающий фильтр открытой сети для широковещательных IP-пакетов |
| 62 | **Пропущен незашифрованный транзитный IP-пакет** | Это событие регистрируется только на координаторе. Найден разрешающий фильтр открытой сети для транзитных IP-пакетов |
| 63 | **Пакет пропущен фильтром для туннелируемых узлов** | Это событие регистрируется только на координаторе. Найден разрешающий фильтр для IP-пакетов от туннелируемых узлов |
| 64 | **IP-пакет пропущен фильтрами по умолчанию при загрузке компьютера** | Пакет пропущен фильтрами, которые действуют при загрузке компьютера |

*Таблица 15. Группа **Все IP-пакеты\Служебные события** (дополнительная информация, формируемая для IP-пакетов, уже зарегистрированных в журнале)*

| № события | Название события | Описание события |
|---|---|---|
| **42** | **Изменился IP-адрес узла** | Драйвер обнаружил, что IP-адрес узла или параметры доступа к нему через внешнюю сеть изменились, и соответствующим образом скорректировал свои таблицы. При изменении параметров доступа событие регистрируется только для сетевых узлов, не работающих через межсетевой экран с динамической или статической трансляцией адресов. |
| **46** | **Изменились параметры доступа к сетевому узлу** | Драйвер обнаружил, что параметры доступа к сетевому узлу через внешнюю сеть изменились, и соответствующим образом скорректировал свои таблицы. Событие регистрируется для сетевых узлов, работающих через межсетевой экран с динамической или статической трансляцией адресов. В качестве IP-адресов и портов регистрируются данные из IP-пакета, поступившего из сети, до его преобразования драйвером. |
| **48** | **Адрес сетевого узла зарегистрирован из широковещательного пакета** | Зарегистрировано событие, что от узла поступают широковещательные пакеты |
| **49** | **Изменились параметры доступа к своему узлу из внешней сети** | Поступила информация об изменении параметров доступа через внешнюю сеть к своему сетевому узлу. В качестве IP-адресов и портов регистрируются данные по доступу к своему узлу (**Получатель**) и к узлу, от которого получена информация (**Отправитель**) |
| **110** | **На DNS-сервере зарегистрирован новый IP-адрес узла** | Поступило сообщение от DNS-сервера, что для узла с именем, указанным в поле **Отправитель**, зарегистрирован IP-адрес, указанный в поле **IP-адрес отправителя** |
| **114** | **Имя на DNS (WINS)-сервере не зарегистрировано** | Поступило сообщение от DNS-сервера, что запрошенное DNS-имя защищенного узла не зарегистрировано на данном DNS-сервере |

D

# Региональные настройки

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

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

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

# Региональные настройки в ОС Server 2003

Для установки поддержки кириллицы на ОС Server 2003 выполните следующие действия:

1 Откройте **Панель управления** (**Control Panel**).

2 Щелкните **Язык и региональные стандарты** (**Regional and Language Options**).

3 В окне **Язык и региональные стандарты** (**Regional and Language Options**) перейдите на вкладку **Дополнительно** (**Advanced**).

4 Далее в списке выберите **Русский** (**Russian**).

5 Установите флажок **Применить эти параметры для текущей учетной записи и для стандартного профиля пользователя** (**Apply all settings to the current user account and to the default user profile**).

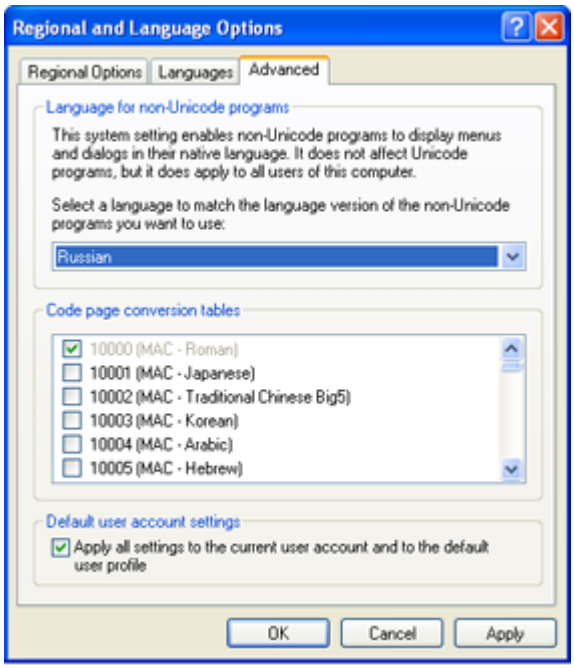



*Рисунок 166. Выбор языка для программ, не поддерживающих Юникод*

6 Нажмите кнопку **OK**. Возможно, потребуется перезагрузка.

# Региональные настройки в ОС Windows Vista, Server 2008, Windows 7, Server 2008 R2

Для установки поддержки кириллицы на ОС Windows Vista, Server 2008, Windows 7, Server 2008 R2 выполните следующие действия:

1 Откройте **Панель управления** (**Control Panel**) > **Часы, язык и регион** (**Clock, Language, and Region**) > **Язык и региональные стандарты** (**Region and Language**).

2 В окне **Язык и региональные стандарты** (**Region and Language**) перейдите на вкладку **Дополнительно** (**Administrative**).

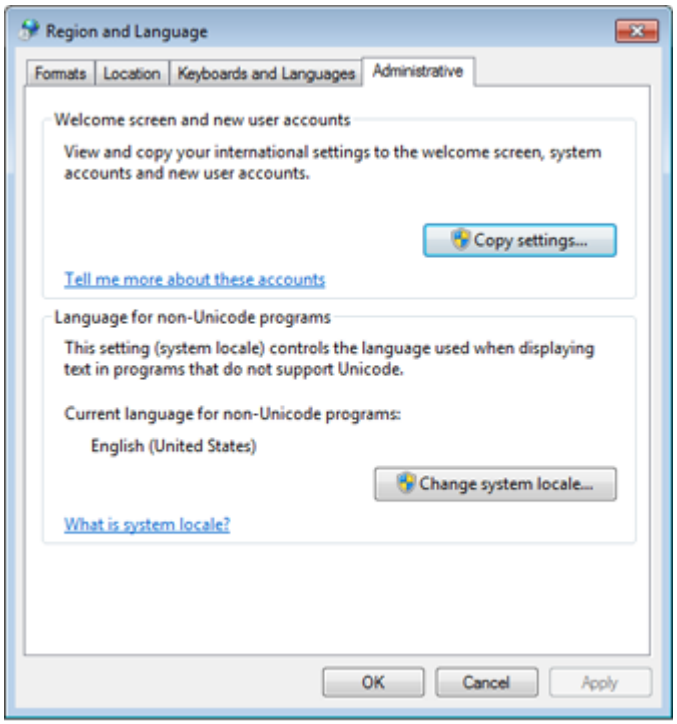



*Рисунок 167. Дополнительные языковые параметры*

3 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

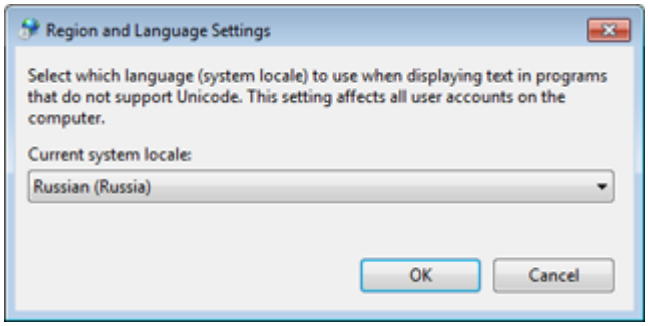



*Рисунок 168. Выбор языка системы*

5 Нажмите кнопку **OK**. Потребуется перезагрузка.

6 После перезагрузки откройте **Панель управления** (**Control Panel**) > **Часы, язык и регион** (**Clock, Language, and Region**) > **Язык и региональные стандарты** (**Region and Language**).

7 В окне **Язык и региональные стандарты** (**Region and Language**) перейдите на вкладку **Дополнительно** (**Administrative**).

8 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

9 В открывшемся окне установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

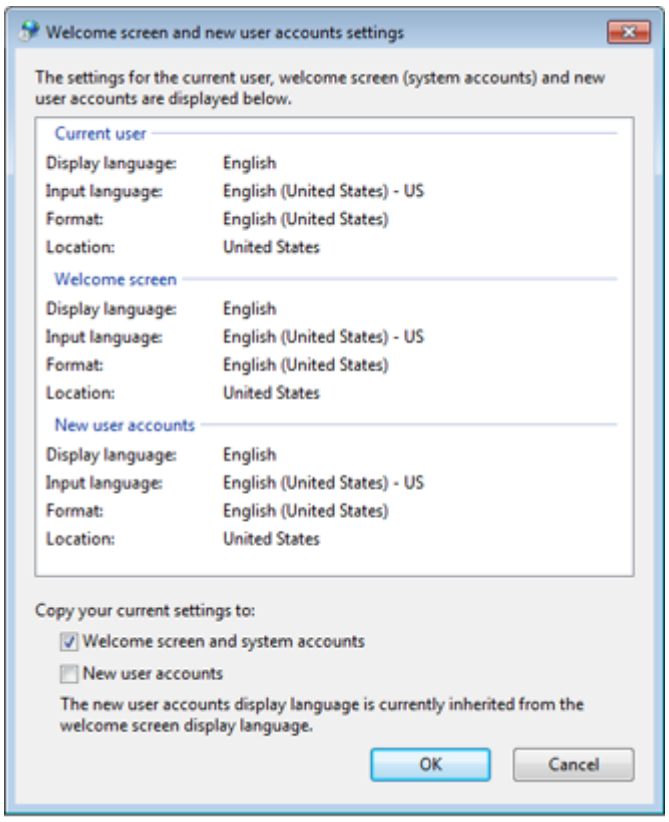



*Рисунок 169. Копирование параметров*

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

1 В окне **Язык и региональные стандарты** (**Region and Language**) на вкладке **Форматы** (**Formats**) в списке **Формат** (**Format**) выберите **Русский (Россия)** (**Russian (Russia)**).

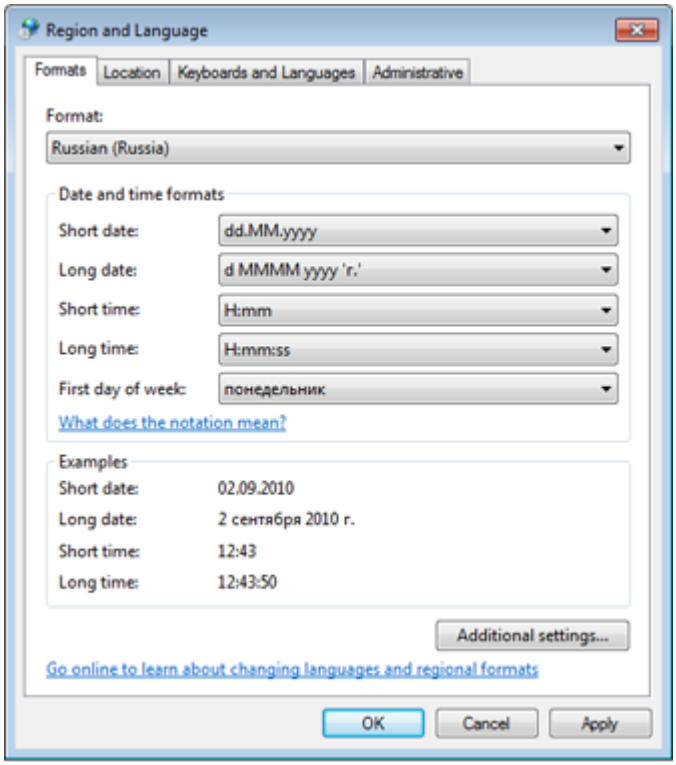



*Рисунок 170. Настройка форматов*

2 В окне **Язык и региональные стандарты** (**Region and Language**) на вкладке **Расположение** (**Location**) в списке **Текущее расположение** (**Current location**) выберите **Россия**.

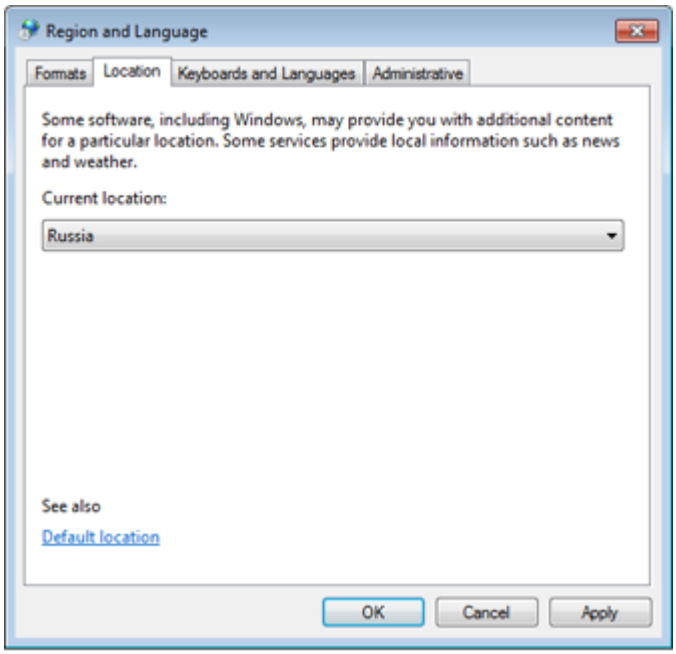



*Рисунок 171. Выбор текущего расположения*

# Региональные настройки в ОС Windows 8.1, Server 2012

Для установки поддержки кириллицы на ОС Windows 8.1, Server 2012 выполните следующие действия:

1 Откройте **Панель управления** (**Control Panel**) > **Региональные стандарты** (**Region**).

2 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

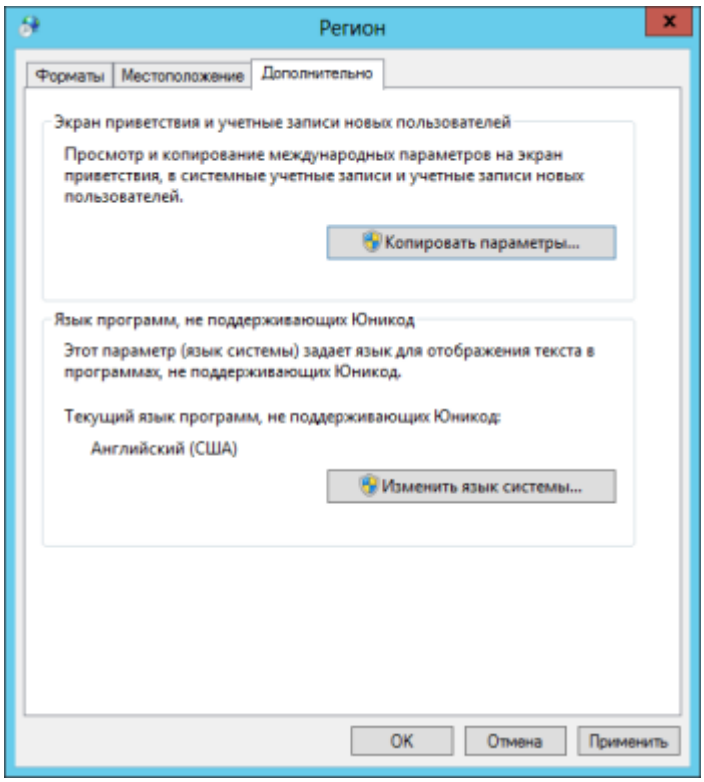



*Рисунок 172. Дополнительные языковые параметры*

3 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

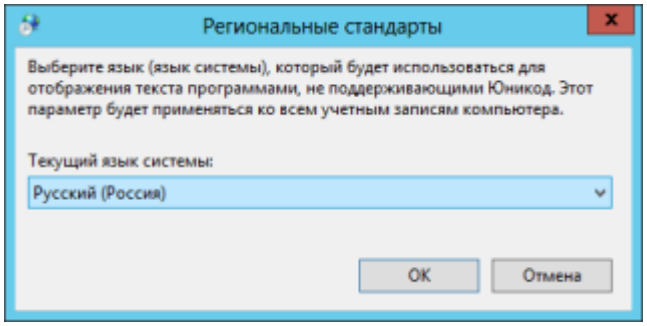



*Рисунок 173. Выбор языка системы*

5 Нажмите кнопку **OK**. Потребуется перезагрузка.

6 После перезагрузки откройте **Панель управления** (**Control Panel**) > **Региональные стандарты** (**Region**).

7 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

8 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

9 В открывшемся окне установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

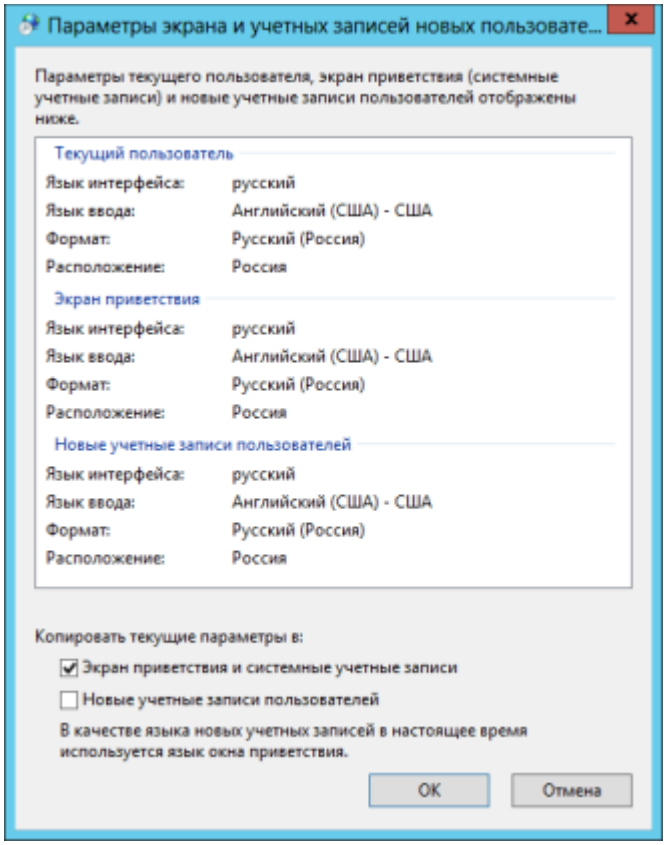



*Рисунок 174. Копирование параметров*

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

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

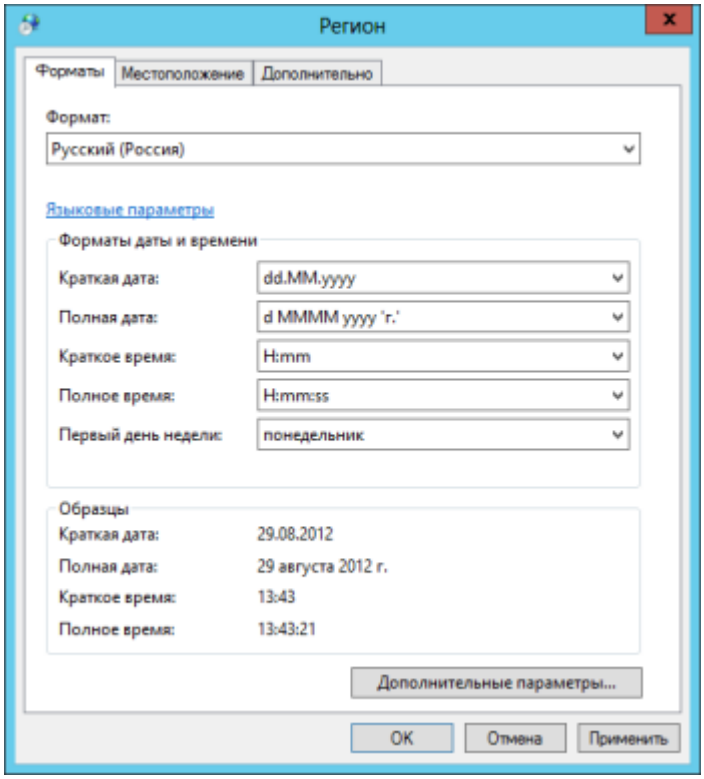



*Рисунок 175. Настройка форматов*

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

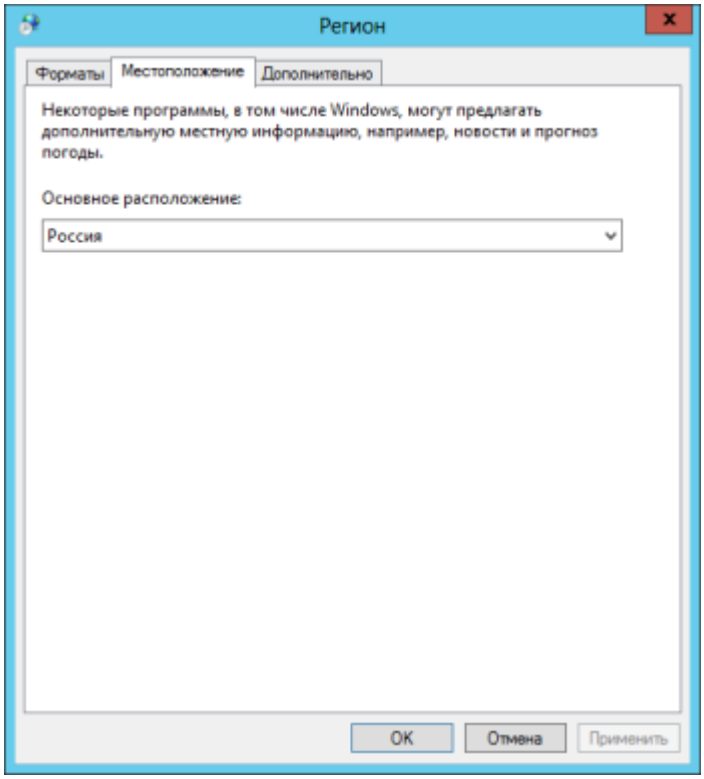



*Рисунок 176. Выбор текущего расположения*

E

# Внешние устройства

## Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей (см. «Контейнер ключей» на стр. 399), которые вы можете использовать для аутентификации, формирования электронной подписи (см. «Электронная подпись» на стр. 404) или для других целей.

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

Программное обеспечение ViPNet Монитор поддерживает два способа аутентификации с помощью внешнего устройства (см. «Способы аутентификации пользователя» на стр. 70):

- По персональному ключу пользователя ViPNet, который хранится на устройстве. Этот способ аутентификации имеет следующие ограничения:
  - Одно внешнее устройство невозможно использовать для аутентификации нескольких пользователей ViPNet.
  - Одно внешнее устройство невозможно использовать для аутентификации одного пользователя на нескольких узлах ViPNet.
  - Если используется этот способ аутентификации, тогда ключи электронной подписи пользователя, изданные в удостоверяющем центре на базе ПО ViPNet, должны храниться на одном устройстве с персональным ключом.
- По сертификату, который хранится на устройстве вместе с соответствующим закрытым ключом. Требования к сертификату см. в разделе Особенности аутентификации с помощью сертификата (на стр. 74).

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP (см. «Настройка параметров криптопровайдера ViPNet CSP» на стр. 241). Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

# Список поддерживаемых внешних устройств

В следующей таблице перечислены внешние устройства, которые могут быть использованы в программном обеспечении ViPNet. Для каждого семейства устройств в таблице приведено описание, указаны условия и особенности работы с устройствами.

*Таблица 16. Поддерживаемые внешние устройства*

| Название семейства устройств в программе ViPNet CSP | Полные названия и типы устройств | Необходимые и рекомендуемые условия работы с семейством устройств |
|---|---|---|
| **ESMART Token** | Смарт-карты и токены семейства **ESMART Token**, **ESMART Token ГОСТ**, **ESMART Token USB 64K** | На компьютере должно быть установлено ПО ESMART PKI Client (рекомендуемая версия — 1.1.3).<br>**Примечание.** При использовании устройства ESMART Token ГОСТ возможна аутентификация только по персональному ключу на устройстве. |
| **Infotecs Software Token** | **Infotecs Software Token** — программная реализация стандарта PKCS#11 | Аутентификация по этому токену возможна только после входа в ОС Windows при запуске программы ViPNet Монитор или ViPNet Деловая почта.<br>Необходимое ПО входит в поставку ViPNet CSP. С помощью программы token_manager.exe на компьютере должен быть создан виртуальный токен. |
| **A-Key** | Смарт-карты **aKey S1000**, **aKey S1003**, **aKey S1004** производства компании Ak Kamal Security | На компьютере должна быть установлена библиотека akpkcs11.dll, предоставленная компанией Ak Kamal Security.<br>Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — `12345678`.<br>Перенос ключей подписи на данный тип устройств невозможен.<br>**Примечание.** При использовании этих устройств возможна аутентификация только по персональному ключу на устройстве. |

| Название семейства устройств в программе ViPNet CSP | Полные названия и типы устройств | Необходимые и рекомендуемые условия работы с семейством устройств |
|---|---|---|
| **ViPNet HSM** | Виртуальный токен **ViPNet HSM** производства ОАО «ИнфоТеКС» | Аутентификация по этому токену возможна только после входа в ОС Windows при запуске программы ViPNet Монитор или ViPNet Деловая почта.<br>Необходимо установить клиентское приложение ViPNet HSM и проинициализировать виртуальный токен. |
| **JaCarta** | Персональные электронные ключи и смарт-карты **JaCarta PKI**, **JaCarta Laser** производства компании «Аладдин Р.Д.» | На компьютере должно быть установлено ПО JC-Client компании «Аладдин Р.Д.» (рекомендуемая версия — 6.30.06). |
| **JCDS** | Смарт-карты **Gemalto Optelio Contactless D72**, **KONA 131 72K** и **JaCarta LT** с апплетом от компании «Аладдин Р.Д.» | На карту должен быть загружен апплет Datastore, позволяющий модулю jcpkcs11ds.dll компании «Аладдин Р.Д.» работать с картой.<br>Для администрирования смарт-карт JaCarta LT на компьютере должно быть установлено ПО JC-PROClient версии 1.5.0.199, рекомендуется использовать модуль сопряжения jcpkcs11ds.dll версии 1.1.3.20.<br>**Примечание.** При использовании JaCarta LT возможна аутентификация только по персональному ключу на устройстве. |
| **Siemens CardOS** | Смарт-карты **CardOS/M4.01a**, **CardOS V4.3B**, **CardOS V4.2B**, **CardOS V4.2B DI**, **CardOS V4.2C**, **CardOS V4.4** производства компании Atos (Siemens) | На компьютере должно быть установлено ПО Siemens CardOS API V5.0. |
| **eToken GOST** | Персональные электронные ключи **eToken ГОСТ** и **JaCarta ГОСТ** производства компании «Аладдин Р.Д.» | Для работы с указанными устройствами на компьютере должно быть установлено ПО JC-GOST Client (рекомендуемая версия —1.5.3.446).<br>Перенос ключей подписи на данный тип устройств невозможен. |

| Название семейства устройств в программе ViPNet CSP | Полные названия и типы устройств | Необходимые и рекомендуемые условия работы с семейством устройств |
|---|---|---|
| **Rutoken ECP/**<br>**Rutoken Lite** | Электронные идентификаторы **Рутокен ЭЦП** и **Рутокен Lite** производства компании «Актив» | На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 2.100.00.0542).<br>Перенос ключей подписи на идентификаторы Рутокен ЭЦП невозможен.<br>**Примечание.** При использовании Rutoken Lite возможна аутентификация только по персональному ключу на устройстве. |
| **Rutoken/**<br>**Rutoken S** | Электронные идентификаторы **Рутокен** и **Рутокен S** производства компании «Актив» | На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 2.100.00.0542). |
| **eToken Aladdin** | Персональные электронные ключи **eToken PRO (Java)**, **eToken PRO**,<br>смарт-карты **eToken PRO (Java)**, **eToken PRO**,<br>**JaCarta PRO**, **eToken NG-Flash** производства компании «Аладдин Р.Д.» | На компьютере должно быть установлено ПО PKI Client версии 5.1 SP1.<br>Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт.<br>Для работы смарт-карты JaCarta PRO на компьютере должно быть установлено ПО JC-PROClient версии 1.0.6 и должен быть включен режим совместимости с eToken. |

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

# Алгоритмы и функции, поддерживаемые внешними устройствами

В следующей таблице перечислены криптографические алгоритмы, поддерживаемые внешними устройствами, приведена информация о возможности использования устройств в качестве датчиков случайных чисел, а также информация о поддержке стандарта PKCS#11.

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

*Таблица 17. Алгоритмы и функции, поддерживаемые внешними устройствами*

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

| Название семейства устройств в программе ViPNet CSP | Поддержка российских криптографических алгоритмов, реализованных аппаратно (на устройстве) | Поддержка российских криптографических алгоритмов, реализованных программно (ViPNet CSP) | Функции ДСЧ | Поддержка PKCS#11 |
|---|---|---|---|---|
| **Rutoken/ Rutoken S** | отсутствует | ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 | Нет | Да |
| **eToken Aladdin** | отсутствует | ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 | Да | Да |

F

# Рекомендации по обеспечению совместной работы ПО ViPNet Client с другими приложениями

# Совместное использование программы ViPNet Монитор и технологии Hyper-V

Hyper-V — это система виртуализации, реализованная в 64-разрядной версии операционной системы Microsoft Windows Server 2008.

Особенностью Hyper-V является то, что для обеспечения доступа виртуальных машин к внешней сети требуется выделить один из физических сетевых интерфейсов компьютера. Этот интерфейс будет подключен к виртуальному коммутатору Hyper-V, а вместо него в хостовой операционной системе будет создан виртуальный интерфейс с такими же настройками.

Для правильного подключения виртуальных сетевых интерфейсов (в том числе в хостовой операционной системе) к внешней сети на физическом интерфейсе, который используется для этого подключения, должны быть отключены все службы и протоколы, кроме протокола коммутации виртуальных сетей (Virtual Network Switching Protocol).

При установке программы ViPNet Монитор на компьютер с 64-разрядной операционной системой на всех сетевых интерфейсах компьютера включается служба Iplir lightweight Filter (x64 edition), то есть сетевой ViPNet-драйвер (на стр. 15). Этот драйвер осуществляет шифрование, расшифрование и фильтрацию IP-пакетов, проходящих через сетевой интерфейс, и может нарушить работоспособность виртуальной сети Hyper-V.

Чтобы обеспечить нормальное функционирование виртуальной сети и программного обеспечения ViPNet в хостовой операционной системе, в настройках физического сетевого интерфейса, подключенного к виртуальной сети Hyper-V, требуется отключить службу Iplir lightweight Filter (x64 edition).

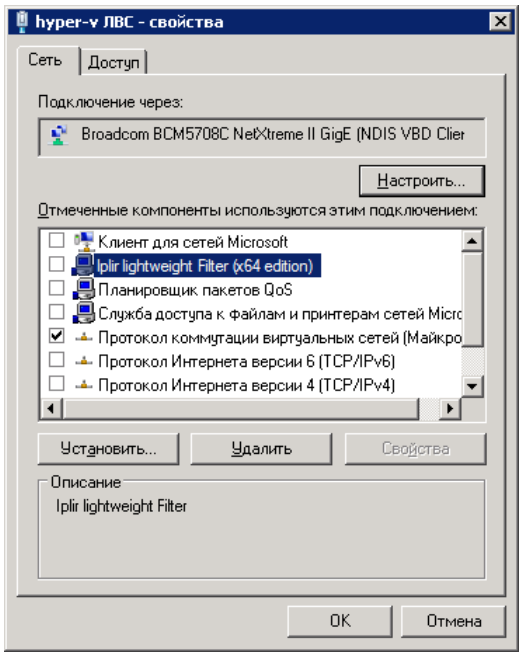



*Рисунок 177. Настройки физического интерфейса, подключенного к виртуальной сети Hyper-V*

# Совместное использование ПО ViPNet Client и Secret Net

При совместной установке на компьютер ПО ViPNet Client и Secret Net возможны проблемы при обновлении справочников и ключей сетевого узла ViPNet. Это связано с наличием в ПО Secret Net ограничения доступа пользователей к конфиденциальным данным, в том числе к папкам, в которых ПО ViPNet Client хранит справочники и ключи. Чтобы справочники и ключи обновлялись при любом уровне доступа пользователей ПО Secret Net, необходимо снять конфиденциальность с соответствующих папок. Для этого создайте файл в формате XML, текст которого приведен в разделе Настройка доступа к папкам справочников и ключей (на стр. 355), и выполните приведенные ниже действия. Созданный файл используйте при настройке ПО Secret Net.

**Внимание!** Рекомендации, приведенные в данном разделе, относятся к программному обеспечению Secret Net версий 6.5 и 7.0.

Чтобы обеспечить совместную работу ПО ViPNet Client и Secret Net, выполните следующие действия в указанном порядке:

1. Установите на компьютер ПО Secret Net.
2. Установите на компьютер ПО ViPNet Client. После установки не перезагружайте компьютер.

**Внимание!** Если после установки ПО ViPNet Client вы перезагрузите компьютер, то все последующие настройки, производимые в ПО Secret Net, не будут применены.

3. Запустите программу «Настройка подсистемы полномочного управления доступом», входящую в состав ПО Secret Net (далее — «программа настройки»). Для этого в меню **Пуск** выберите **Все программы** > **Код безопасности** > **Secret Net** > **Настройка подсистемы полномочного управления доступом**.
4. В окне программы настройки на панели навигации в разделе **Вручную** выберите подраздел **Программы**.

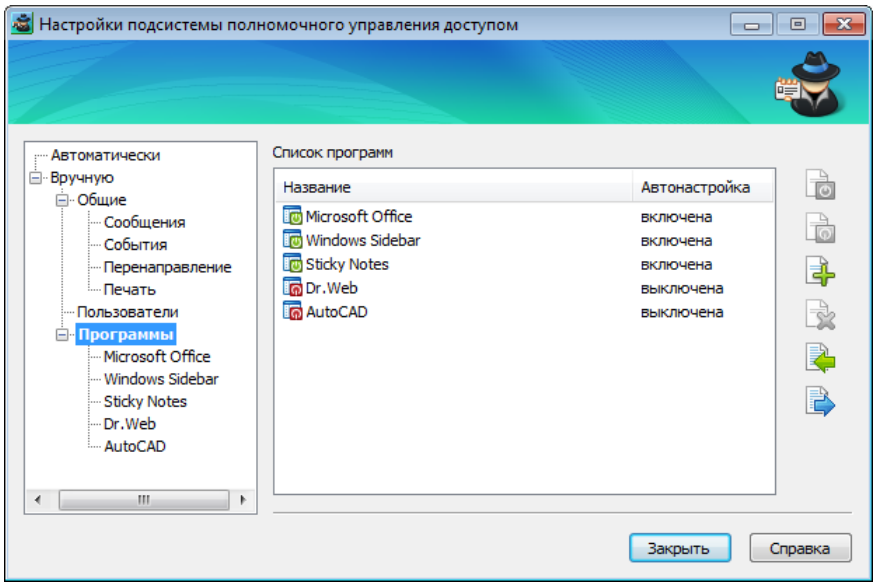



*Рисунок 178. Настройка подсистемы полномочного управления доступом*

5 На панели просмотра нажмите кнопку **Добавить программы** и в открывшемся окне выберите файл в формате XML, содержащий настройки доступа к папкам справочников и ключей. В списке программ на панели навигации появится программа ViPNet Client.

6 На панели просмотра в списке программ выберите **ViPNet Client** и нажмите кнопку **Настроить**. Начнется процесс настройки параметров, по окончании которого появится соответствующее сообщение.

В результате в ПО Secret Net будет установлена категория «неконфиденциально» для тех папок, которые ПО ViPNet Client использует при обновлении справочников и ключей. По завершении настройки перезагрузите компьютер и установите справочники и ключи сетевого узла ViPNet.

# Настройка доступа к папкам справочников и ключей

Приведенный ниже текст XML-файла предназначен для установки категории «неконфиденциально» для папок, используемых ПО ViPNet Client при обновлении справочников и ключей.

```
<?xml version="1.0" encoding="windows-1251"?>
<ProgramList>
  <Default>
    <Program Name="ViPNet Client" Turn="On" OSVersion="Vista;2008;2008R2;7;">
      <Action Name="SetMandatAttr">
        <Rule Level="0" Flags="4" Recursion="2"
        AddMBSDir="yes">%allusersprofile%\InfoTeCS\</Rule>
        <Rule Level="0" Flags="4" Recursion="2"
        AddMBSDir="yes">%ProgramFiles%\InfoTeCS\ViPNet Client</Rule>
      </Action>
```

```
    </Program>
    <Program Name="ViPNet Client" Turn="On" OSVersion="2003R2;XP;">
      <Action Name="SetMandatAttr">
        <Rule Level="0" Flags="4" Recursion="2"
        AddMBSDir="yes">%ProgramFiles%\InfoTeCS\ViPNet Client</Rule>
        <Rule Level="0" Flags="4" Recursion="2"
        AddMBSDir="yes">%allusersprofile%\Application Data\InfoTeCS</Rule>
      </Action>
    </Program>
  </Default>
  <Program Name="ViPNet Client" Turn="On" OSVersion="Vista;2008;2008R2;7;">
    <Action Name="SetMandatAttr">
      <Rule Level="0" Flags="4" Recursion="2"
      AddMBSDir="yes">%allusersprofile%\InfoTeCS\</Rule>
      <Rule Level="0" Flags="4" Recursion="2"
      AddMBSDir="yes">%ProgramFiles%\InfoTeCS\ViPNet Client</Rule>
    </Action>
  </Program>
  <Program Name="ViPNet Client" Turn="On" OSVersion="2003R2;XP;">
    <Action Name="SetMandatAttr">
      <Rule Level="0" Flags="4" Recursion="2"
      AddMBSDir="yes">%ProgramFiles%\InfoTeCS\ViPNet Client</Rule>
      <Rule Level="0" Flags="4" Recursion="2"
      AddMBSDir="yes">%allusersprofile%\Application Data\InfoTeCS</Rule>
    </Action>
  </Program>
</ProgramList>
```

# Совместное использование ПО ViPNet Client и Cisco Agent Desktop

Если регламент работы контакт-центра требует прослушивания и записи разговоров операторов супервизором и для данных операций используются приложения Cisco Agent Desktop (на узлах операторов) и Cisco Supervisor Desktop (на узле супервизора), то на компьютерах операторов не следует устанавливать ПО ViPNet Client. Защиту трафика, передаваемого между узлами операторов и супервизора, в этом случае можно организовать с помощью туннелированных соединений.

При совместном использовании Cisco Agent Desktop и ViPNet Client передача голосового трафика на узел супервизора производится некорректно по следующим причинам. Голосовой трафик операторов зеркалируется драйвером Cisco Agent Desktop на узел супервизора, где прослушивается и записывается супервизором с помощью Cisco Supervisor Desktop. Если на узле оператора установлен ViPNet Client, то весь исходящий трафик передается в обработанном виде (IP-пакеты имеют преобразованный заголовок). Но зеркалируемый голосовой трафик не проходит обработку в ViPNet Client из-за того, что передается приложением Cisco Agent Desktop сразу на узел супервизора. При этом в необработанном виде голосовой трафик не может быть принят на его узле.

Данная проблема возникает из-за того, что Intermediate Ndis-драйвер приложения Cisco Agent Desktop, отвечающий за зеркалирование трафика на узел супервизора, и сетевой ViPNet-драйвер, осуществляющий обработку трафика, находятся на разных уровнях стека протокола TCP/IP. ViPNet-драйвер в стеке TCP/IP располагается на сетевом уровне. Драйвер Cisco встраивается в стек ниже — на канальном уровне — и зеркалирует голосовой трафик на узел супервизора напрямую, не передавая его ViPNet-драйверу. Поэтому IP-пакеты отправляются супервизору в необработанном виде.

Если на узлах операторов не будет установлено ПО ViPNet, то весь IP-трафик (в том числе голосовой) будет передаваться в открытом виде и сможет быть принят на узле супервизора при наличии соответствующих фильтров открытого трафика. Чтобы IP-трафик через внешние сети передавался в зашифрованном виде, между узлами операторов и супервизора следует организовать туннелируемые соединения.

Если функции прослушивания и записи разговоров операторов не осуществляются в контакт-центре, то тогда на узлах операторов вместе с приложением Cisco Agent Desktop можно установить ПО ViPNet Client.

# Совместное использование ПО ViPNet Монитор и ESET NOD32 Smart Security

При совместной установке на компьютер ПО ViPNet Client и ESET NOD32 Smart Security возможны проблемы с установлением соединения между защищенными узлами и доступом к ресурсам Интернета. Чтобы обеспечить на компьютере совместное функционирование программ ViPNet Монитор и ESET NOD32 Smart Security, в программе ESET NOD32 Smart Security создайте правила, разрешающие обмен данными по протоколу 241 (см. «Протоколы соединений в защищенной сети» на стр. 91) и использование компонента `Itcsnatproxy.exe`.

Выполните следующие действия:

1. Откройте главное окно программы ESET NOD32 Smart Security и выберите вкладку **Настройка**.
2. В правой части окна щелкните ссылку **Сеть** и в открывшемся окне щелкните ссылку **Настроить правила и зоны**.
3. В окне **Настройка зон и правил** нажмите кнопку **Создать**.
4. В окне **Новое правило** выберите вкладку **Общие** и в группе **Общая информация об этом правиле** укажите название разрешающего правила для протокола 241.

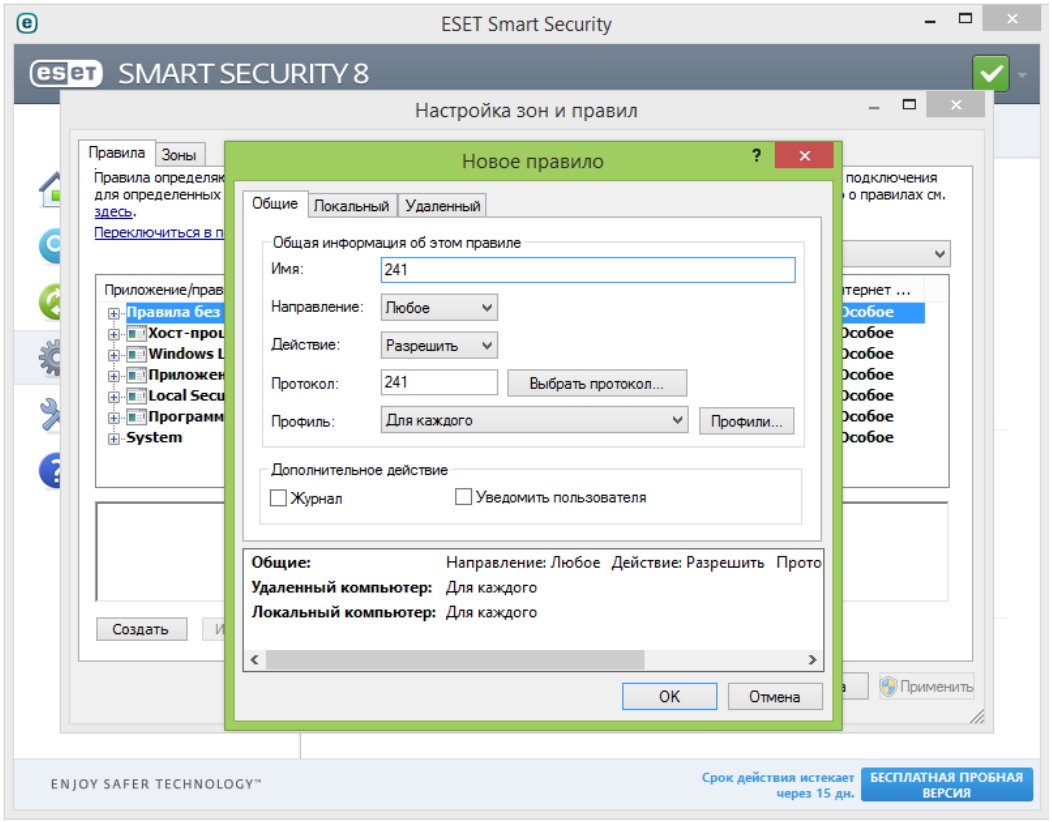



*Рисунок 179. Создание правила в ESET NOD32 Smart Security для протокола 241*

5 Нажмите кнопку **Выбрать протокол** и выберите протокол 241.

6 Нажмите кнопку **OK**, чтобы сохранить правило.

7 В окне **Настройка зон и правил** нажмите кнопку **Создать**, чтобы создать правило для компоненты `Itcsnatproxy.exe`.

8 В окне **Новое правило** на вкладке **Общие** в группе **Общая информация об этом правиле** укажите название разрешающего правила.

9 Перейдите на вкладку **Локальный** и в группе **Приложение** укажите путь к файлу `Itcsnatproxy.exe`. Например,

```
C:\Program Files (x86)\InfoTeCS\ViPNet Client\Itcsnatproxy.exe
```

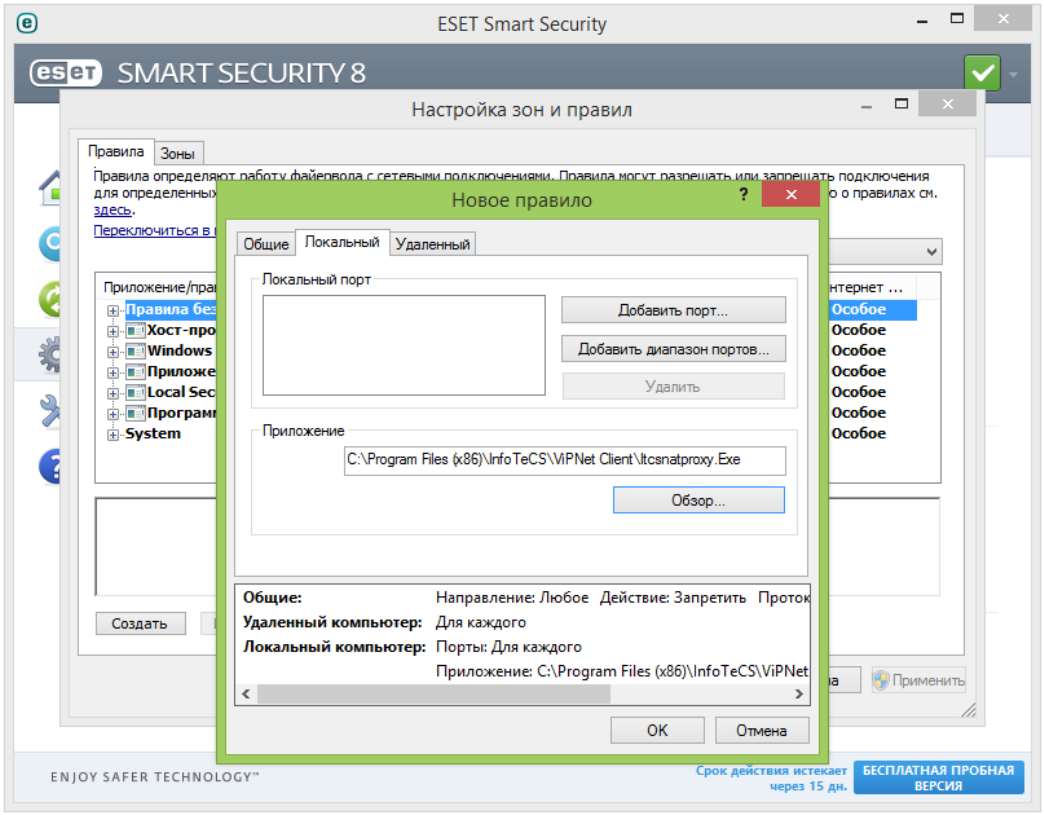



*Рисунок 180. Создание правила в ESET NOD32 Smart Security для компоненты Itcsnatproxy.exe*

10 Нажмите кнопку **OK**, чтобы сохранить правило.

11 В окне **Настройка зон и правил** нажмите кнопку **Применить**. Соединение между защищенными узлами и доступ к ресурсам Интернет будут восстановлены.

# Совместное использование ПО ViPNet Монитор и Avast

Если на сетевом узле ViPNet включен межсетевой экран Avast, могут возникнуть проблемы с соединением между сетевыми узлами ViPNet. Чтобы обеспечить совместное функционирование программ ViPNet Монитор и Avast, добавьте три правила для межсетевого экрана, разрешающие обмен данными по протоколу 241, а также прохождение входящего и исходящего UDP-трафика через порт 55777 (см. «Протоколы соединений в защищенной сети» на стр. 91). Для этого выполните следующие действия:

1 В главном окне программы выберите раздел **Настройки**.

2 В открывшемся окне выберите пункт **Активная защита** и рядом с пунктом **Брандмауэр** щелкните ссылку **Настройки**.

3 В открывшемся окне выберите пункт **Политики** и в группе **Предпочтения** установите флажок **Режим общего доступа к подключению Интернета (ICS)**.

4 Нажмите кнопку **Правила работы с пакетами**, откроется окно **Правила для пакетов**.

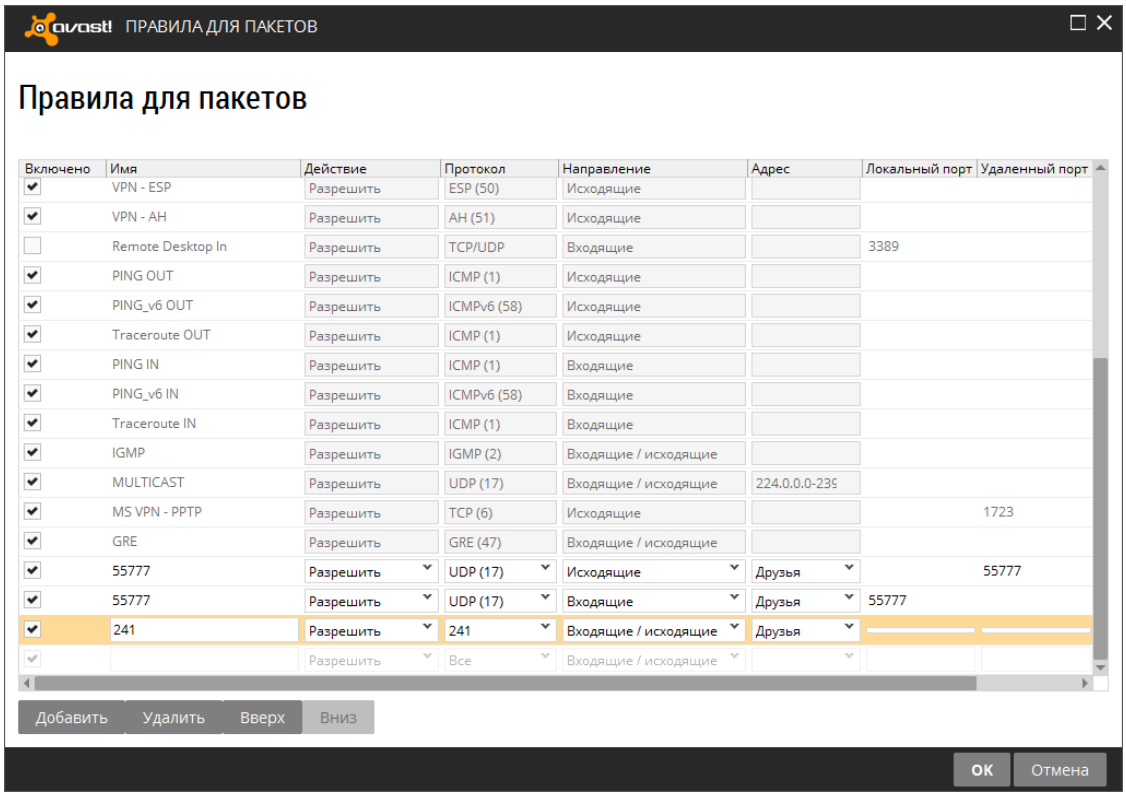



*Рисунок 181. Создание правила в программе Avast*

5 Нажмите кнопку **Добавить**, чтобы создать правило **Исходящий UDP-трафик**, и настройте его в соответствии со значениями параметров, которые представлены в следующей таблице:

*Таблица 18. Параметры правил для межсетевого экрана Avast*

| Правило | Действие | Про-токол | Направление | Адрес | Локальный порт | Удаленный порт |
|---|---|---|---|---|---|---|
| **Исходящий UDP-трафик** | Разрешить | UDP | Исходящие | Друзья | | 55777 |
| **Входящий UDP-трафик** | Разрешить | UDP | Входящие | Друзья | 55777 | |
| **Протокол 241** | Разрешить | 241 | Входящие/ исходящие | Друзья | | |

6 Создайте еще два правила в соответствии со значениями из таблицы и нажмите кнопку **OK**.

7 Вернитесь в главное окно Avast и выберите раздел **Инструменты** > **Брандмауэр**.

8 В нижней части открывшегося окна щелкните ссылку **Правила для приложений** и в открывшемся окне **Правила для приложений** прокрутите список приложений вниз, чтобы найти группу **InfoTeCS**.

9 Чтобы разрешить все соединения для программы ViPNet, выберите программу, щелкните ссылку **Указать порты** и в списке **Для всех остальных соединений** выберите пункт **Определять автоматически**.

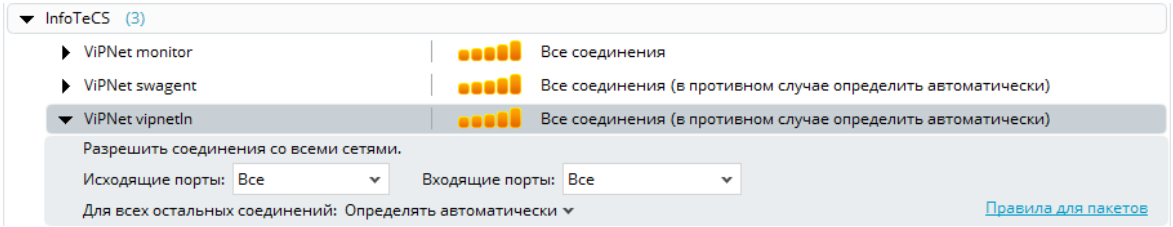



*Рисунок 182. Настройка разрешения соединения с сетями в программе Avast*

10 Повторите шаг 9 для каждой программы в группе **InfoTeCS** и затем нажмите кнопку **Закрыть**, чтобы завершить настройку межсетевого экрана Avast для совместной работы с ПО ViPNet Монитор.

# Совместное использование ПО ViPNet Монитор и AVG Internet Security

Если на сетевом узле ViPNet включен межсетевой экран AVG Internet Security, могут возникнуть проблемы с соединением между сетевыми узлами ViPNet. Чтобы обеспечить совместное функционирование программ ViPNet Монитор и AVG Internet Security, вы можете:

- отключить межсетевой экран AVG Internet Security;
- добавить три правила для межсетевого экрана AVG Internet Security, разрешающие обмен данными по протоколу 241, а также прохождение входящего и исходящего UDP-трафика через порт 55777 (см. «Протоколы соединений в защищенной сети» на стр. 91).

Чтобы добавить правила, выполните следующие действия:

1 В главном окне AVG Internet Security выберите **Firewall** и в открывшемся окне нажмите  .

2 В открывшемся окне нажмите кнопку **Режим для опытных пользователей**.

3 В разделе **Системные службы** нажмите кнопку **Управление системными правилами пользователя**.

4 Нажмите кнопку **Добавить**, чтобы создать правило **Входящий UDP-трафик**, и настройте его в соответствии со значениями параметров, которые представлены в следующей таблице:

*Таблица 19. Параметры правил для межсетевого экрана AVG Internet Security*

| Правило | Прото-кол | Направление | Локальный порт | Удаленный порт | Удален-ный адрес | Действие |
|---|---|---|---|---|---|---|
| **Входящий UDP-трафик** | UDP | Входящее | 55777 | Все порты | Все сети | Разрешить |
| **Исходящий UDP-трафик** | UDP | Исходящее | Все порты | 55777 | Все сети | Разрешить |
| **Протокол 241** | 241 | В обоих направлениях | | | Все сети | Разрешить |

5 Создайте еще два правила в соответствии со значениями из таблицы и нажмите кнопку **OK**, чтобы завершить настройку межсетевого экрана AVG Internet Security.

G

# История версий

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

## Что нового в версии 4.3.1

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.1 по сравнению с версией 4.3.0.

- **Поддержка Windows 10**

  Начиная с версии 4.3.1, ПО ViPNet Client поддерживает операционную систему Windows 10.

- **Отключение поддержки TLS/SSL в программе ViPNet CSP по умолчанию**

  Теперь, если установка программы ViPNet CSP в составе ПО ViPNet Client выполняется впервые, поддержка протокола TLS/SSL отключена. При необходимости вы можете включить поддержку, запустив установочный файл программы ViPNet CSP и добавив соответствующий компонент.

- **Изменение в требованиях к обновлению ПО ViPNet Client**

  Теперь перед обновлением операционной системы до Windows 10 на узле с установленным ПО ViPNet Client либо при обновлении ПО ViPNet Client на узле с установленной ОС Windows 10 необходимо вручную отключать поддержку TLS/SSL (см. Обновление ПО ViPNet Client на стр. 40).

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

# Что нового в версии 4.3.0

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.0 по сравнению с версией 4.2. Более подробная информация приведена в документе «Новые возможности ViPNet Client и ViPNet Coordinator версии 4.x. Приложение к документации ViPNet».

- **Восстановление предустановленных фильтров и групп объектов**

  В версии 4.3 появилась возможность восстановить предустановленные сетевые фильтры. Это позволяет отказаться от произведенных изменений в настраиваемых фильтрах и вернуться к исходному состоянию. Вместе с фильтрами также будут восстановлены предустановленные группы объектов.

- **Поддержка централизованного управления алгоритмом шифрования и сохранением пароля в реестре**

  На сетевых узлах версии 4.3 автоматически изменяются алгоритм шифрования и разрешение на сохранение пароля в реестре в соответствии со значениями, которые передает администратор сети ViPNet в составе обновления справочников и ключей. Централизованное управление этими параметрами возможно в ПО ViPNet Administrator версии 4.4.1 и выше. Пользователь или администратор сетевого узла по-прежнему может изменить указанные параметры, однако изменение будет действительно до следующего обновления справочников и ключей.

- **Поддержка централизованного управления состоянием сетевого экрана Windows**

  На клиентах версии 4.3 автоматически устанавливается состояние сетевого экрана Windows, заданное администратором сети ViPNet в программе ViPNet Центр управления сетью. Централизованное управление состоянием сетевого экрана Windows поддерживается в ПО ViPNet Administrator версии 4.4.1 и выше. Если для управления сетью используется более ранняя версия ViPNet Administrator, действует правило по умолчанию: при первом запуске программы ViPNet Монитор сетевой экран Windows автоматически отключается.

- **Дополнительные параметры установки с помощью групповых политик**

  Появилась возможность задать дополнительные параметры при установке ПО ViPNet Client с помощью групповых политик. Теперь, используя готовые файлы настроек в формате MST, вы можете выбрать, нужно ли устанавливать программу ViPNet Деловая почта и дополнительные компоненты ViPNet CSP.

# Что нового в версии 4.2

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.2.

- **Оптимизация маршрутизации защищенного IP-трафика между клиентами**

  Узлы с программным обеспечением ViPNet Client версии 4.2 в отличие от предыдущих версий, как в локальной сети, так и во внешней, устанавливают соединения с другими узлами по прямым доступным маршрутам, по возможности минуя координаторы. Даже если два клиента стоят за разными устройствами с динамической трансляцией адресов, они смогут соединиться

напрямую. Единственное условие, при котором прямое соединение между клиентами будет невозможно, — если устройства NAT обоих клиентов при отправке IP-пакетов от них по разным адресам каждый раз выделяют случайный порт. Так работает симметричный NAT. В этом случае соединение между двумя такими клиентами установится через один из их серверов соединений.


*Рисунок 183. Организация соединений между сетевыми узлами ViPNet*

- **Настройка подключения клиентов к сети ViPNet**

  Клиенты версии 4.2 автоматически определяют тип подключения к внешней сети. Взаимодействие с узлами внешней сети они устанавливают с помощью серверов соединений (см. «Сервер соединений» на стр. 402). В связи с этим теперь в настройках клиентских узлов отсутствует настройка типа межсетевого экрана, но имеется возможность выбора сервера соединений.

  Как правило, изменять сервер соединений не требуется. Единственный случай, когда может потребоваться выбор иного сервера соединений, — это подключение клиента к другой локальной сети, в которой нет доступа к вашему серверу соединений, но есть другой координатор, имеющий связь с клиентом. В настройках клиентского узла присутствуют и другие настройки, но они скрыты как дополнительные, и их не следует изменять без необходимости.

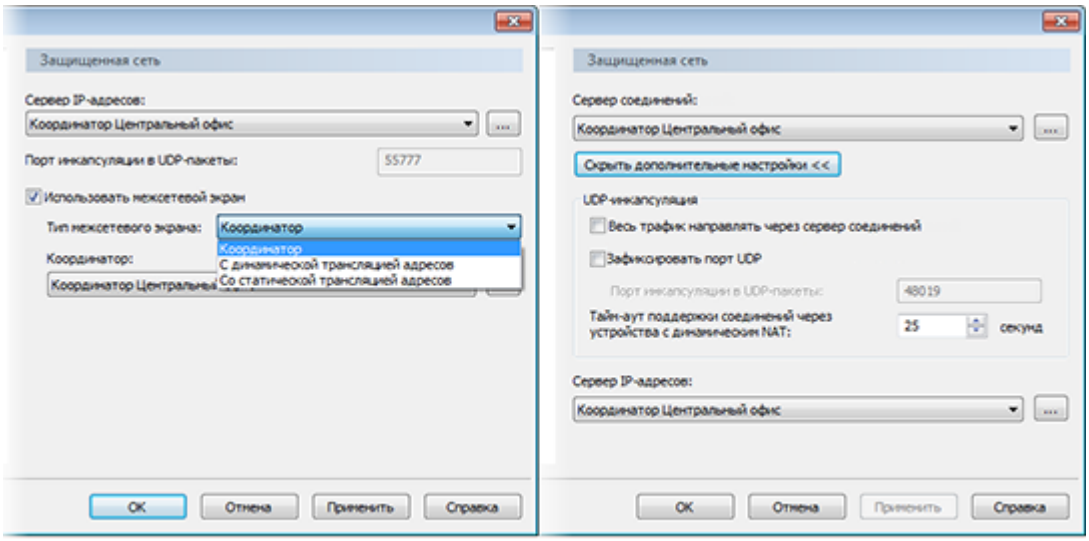



*Рисунок 184. Изменение настроек подключения к сети ViPNet в ViPNet Client*

- **Возможность подключения к сети ViPNet через TCP-туннель**

  При удаленном подключении клиентов к сетям ViPNet может возникать проблема с передачей IP-пакетов по протоколу UDP из-за того, что данный протокол блокируется некоторыми интернет-провайдерами. Теперь клиент может устанавливать соединения с другими узлами сети ViPNet через TCP-туннель, настроенный на его сервере соединений, в том случае, если передача IP-пакетов по протоколу UDP невозможна.

  При настройке TCP-туннеля на координаторе задается порт, на который должны поступать переданные TCP-пакеты. Информация о номере порта TCP-туннеля автоматически рассылается на все клиенты, для которых координатор является сервером соединений. На клиенте номер порта доступа к координатору через TCP-туннель отображается в свойствах данного координатора. Если в свойствах координатора порт не указан, но при этом известно, что на этом координаторе развернут TCP-туннель, порт может быть задан вручную.

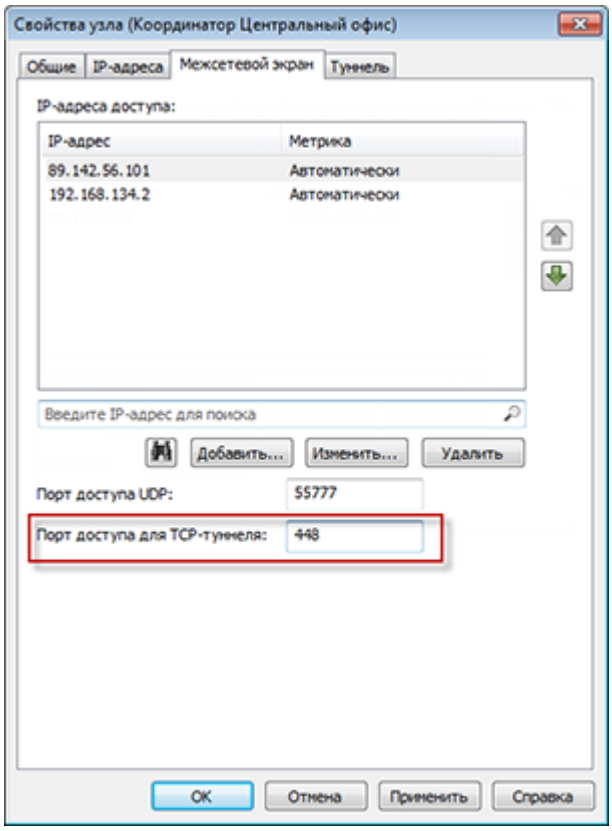



*Рисунок 185. Возможность задания порта TCP-туннеля*

- **Изменения в мастере обновления сертификата**

  В мастере обновления сертификата была удалена настройка способа передачи запроса в связи с тем, что способ передачи запроса через файл стал невостребованным. В программе ViPNet Удостоверяющий и ключевой центр (УКЦ) версии 4.x обработка файлов с расширением `*.sok`, полученных напрямую от пользователя, невозможна. Теперь созданные запросы на обновление сертификатов могут быть переданы в УКЦ только через транспортный модуль ViPNet MFTP.

  Кроме этого, в мастере была исключена возможность выбора режима ожидания сертификата из УКЦ в реальном времени и параметра ввода сертификата в действие сразу после получения. Использование указанных настроек в некоторых случаях приводило к сбою процесса ввода в действие полученного из УКЦ сертификата. Теперь возможность сбоя при вводе в действие полученного сертификата исключена. Он автоматически вводится в действие при получении, если в окне настроек параметров безопасности на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по инициативе пользователя**.

- **Изменение логики оповещений системы обновления ViPNet**

  В версии 4.2, если настроена автоматическая установка обновлений, то все операции система обновления ViPNet производит в «тихом» режиме без выдачи сообщений на экран. Если настроена установка обновлений вручную, то при поступлении файлов обновления в области уведомлений отображается соответствующая информация.

В предыдущих версиях программы значок системы обновлений в области уведомлений присутствовал всегда. В текущей версии значок присутствует только тогда, когда требуется выполнить дополнительные действия, например, перезагрузить компьютер после установки обновления или принять обновления, если настроена установка обновлений вручную. Также в текущей версии окно системы обновления ViPNet можно открыть из меню **Пуск**.

- **Изменения в совместном использовании программ ViPNet Client и ViPNet SafeDisk-V**

  Для повышения уровня защиты конфиденциальной информации изменены условия запуска программы ViPNet SafeDisk-V, интегрированной с ViPNet Client. Теперь, если в программе ViPNet Монитор отключена защита IP-трафика, программа ViPNet SafeDisk-V не запускается, а при запущенной программе ViPNet SafeDisk-V нельзя отключить защиту IP-трафика.

- **Запись событий, происходящих на защищенном узле ViPNet, в журнал Windows**

  Реализована возможность сбора и удаленного анализа программным комплексом ViPNet StateWatcher информации о блокированных IP-пакетах и изменениях в настройках сетевых фильтров защищенного узла. Теперь в программе ViPNet Монитор администратор узла ViPNet может включить запись этих событий в журнал Windows, к которому ПК ViPNet StateWatcher обращается при сборе информации о сетевом узле ViPNet.

- **Новые возможности при обмене защищенными сообщениями**

  В программе обмена защищенными сообщениями версии 4.2 появились дополнительные возможности. Теперь вы можете:

  - осуществлять поиск слов в сообщениях открытых сеансов;
  - осуществлять переход между сеансами обмена;
  - узнать дату и время последнего обмена сообщениями с участником сеанса;
  - отправлять письма или файлы во время сеанса обмена сообщениями;
  - проверять соединение с получателем.

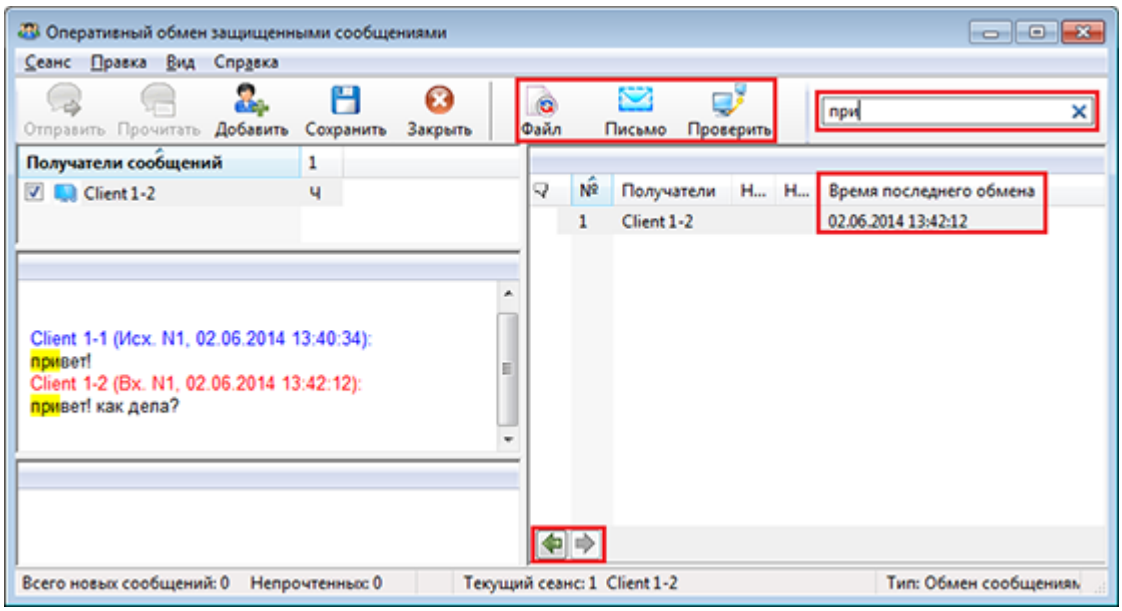



*Рисунок 186. Новые возможности при обмене защищенными сообщениями*

Кроме этого, теперь при закрытии программы обмена защищенными сообщениями все начатые сеансы сохраняются, и когда вы в следующий раз запускаете программу, они восстанавливаются. В предыдущих версиях при закрытии программы закрывались все текущие сеансы обмена сообщениями.

- **Оповещение об изменении групп объектов или сетевых фильтров**

  В новой версии при добавлении или изменении групп объектов и сетевых фильтров в строке состояния главного окна программы появляется сообщение о том, что группы объектов или фильтры были изменены, но изменения не применены. Сообщение в строке состояния будет отображаться до тех пор, пока не будет нажата кнопка **Применить** и в течение 30 секунд не будет подтверждено сохранение изменений.

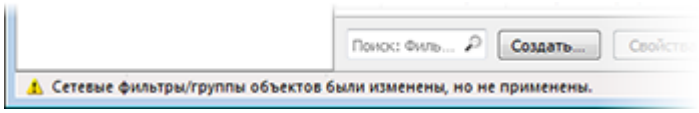



*Рисунок 187. Оповещение об изменении групп объектов и сетевых фильтров*

- **Изменения в программе ViPNet Деловая почта**

  В новой версии программы ViPNet Деловая почта при создании письма вы можете оформить его, изменив тип, размер, начертание шрифта, вставив в текст изображение, список и так далее.

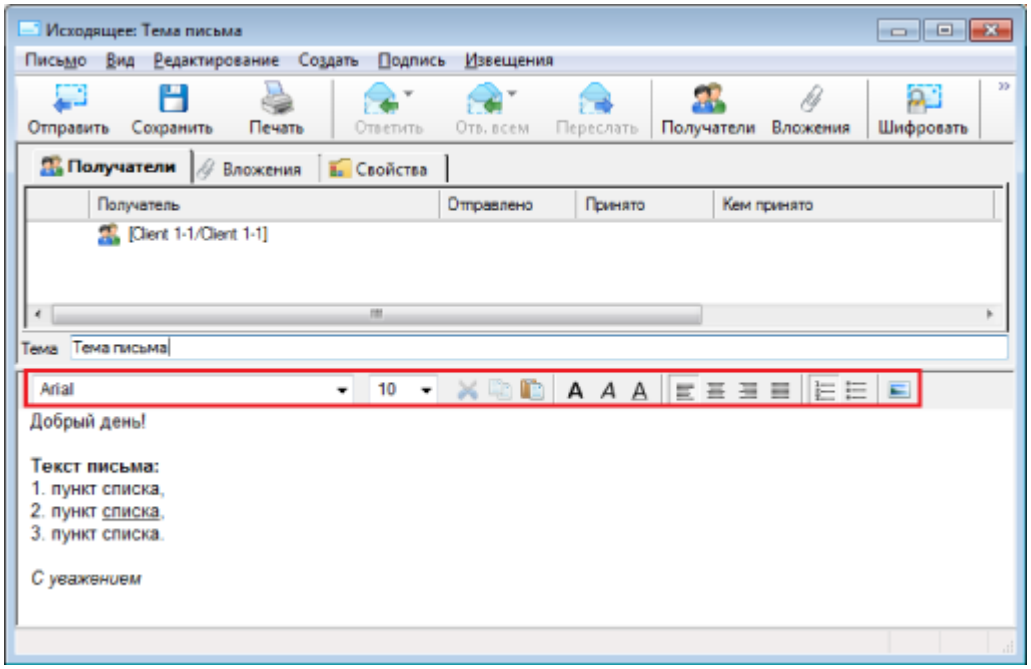



*Рисунок 188. Панель форматирования в окне создания писем*

Также в версии 4.2 реализована возможность создания новых правил автопроцессинга для файлов во внутреннем формате программы ViPNet Деловая почта (`*.bml`).

Кроме того, теперь вы можете настроить правила обработки входящих писем для конкретных пользователей сетевого узла в случае, когда пользователей несколько.

# Что нового в версии 4.1

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.1.

- **Отключение сетевого экрана Windows при первом запуске программы**

  При установке программы ViPNet Client версии 4.1 стандартный сетевой экран Windows остается включенным и выключается автоматически только при первом запуске программы. Такая логика позволяет обеспечить непрерывную защиту вашего компьютера при развертывании сети. Сообщение об отключении сетевого экрана не выводится. В версиях 3.2.x сетевой экран выключается при установке программного обеспечения.

- **Новые алгоритмы подписи**

  В программе ViPNet Монитор версии 4.1 реализована поддержка ключей электронной подписи, созданных по алгоритму ГОСТ 34.10.2012.

- **Возможность использования экранной клавиатуры для аутентификации**

  В версии 4.1 во время загрузки Windows для аутентификации в программе ViPNet Монитор вы можете использовать экранную клавиатуру. Для этого нажмите кнопку  и в меню выберите пункт **Экранная клавиатура**.

- **Изменения в программе ViPNet Деловая почта**

  В версии 4.1 реализована возможность сохранения вложений в базе данных для размещения в архиве вместе с письмами. В этом случае архив представляет собой один файл. Размещение архива писем и вложений в одном файле позволяет упростить копирование или перенос архива на внешний носитель, например, с целью резервирования.

  В ViPNet Деловая почта используются новые значки, а также добавлена колонка **Статус**, в которой атрибуты письма представлены графически.

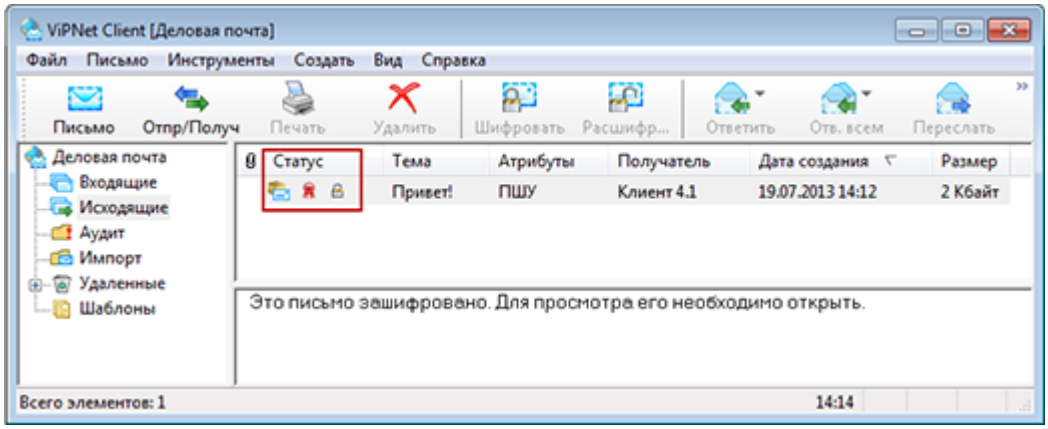



*Рисунок 189. Новая колонка для отображения статуса письма*

# Что нового в версии 4.0

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.0.

- **Поддержка централизованного управления политиками безопасности**

  В программе ViPNet Монитор реализована возможность применять сетевые фильтры и правила трансляции IP-адресов, созданные в программе ViPNet Policy Manager.

- **Новый формат сетевых фильтров и правил трансляции IP-адресов**

  В версии 4.0 используется новый формат сетевых фильтров и правил трансляции IP-адресов (см. «Интегрированный сетевой экран» на стр. 126), который позволяет применять политики безопасности, созданные в программе ViPNet Policy Manager. При переходе на новую версию фильтры и правила конвертируются без каких-либо потерь. Таким образом, никаких действий со стороны пользователя не требуется.

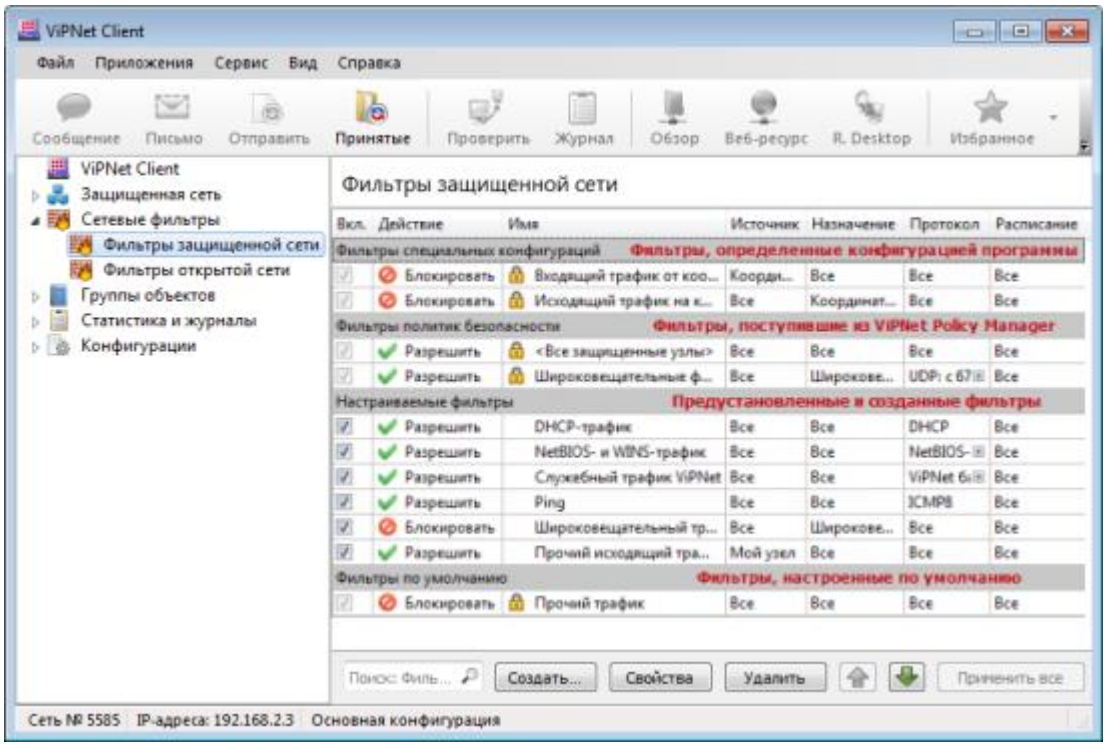



*Рисунок 190. Отображение сетевых фильтров в программе ViPNet Монитор*

- **Отказ от режимов безопасности**

  В версии 4.0 режимы безопасности не используются. Необходимый уровень безопасности можно настроить, создав сетевые фильтры или назначив соответствующий уровень полномочий пользователя.

- **Использование технологии MSI для установки ПО ViPNet**

  Для программы ViPNet Монитор версии 4.0 разработан установочный пакет MSI, который позволяет устанавливать программу с использованием Microsoft System Center, а также с помощью программ, обращающихся к командной строке Windows для запуска

автоматической установки ViPNet Монитор (см. «Установка в неинтерактивном режиме» на стр. 29).

- **Установка и настройка ViPNet CSP**

  Программа ViPNet CSP может быть установлена как из отдельного установочного файла, так и вместе с программами ViPNet Client и ViPNet Coordinator версии 4.0. При любом из способов установки ViPNet CSP устанавливается как отдельная программа, что обеспечивает удобство обновления ViPNet CSP независимо от программ ViPNet Client и ViPNet Coordinator.

  Настройка криптопровайдера теперь выполняется только в программе ViPNet CSP. На вкладке **Криптопровайдер** программы ViPNet Монитор можно осуществить только переход к окну настройки.

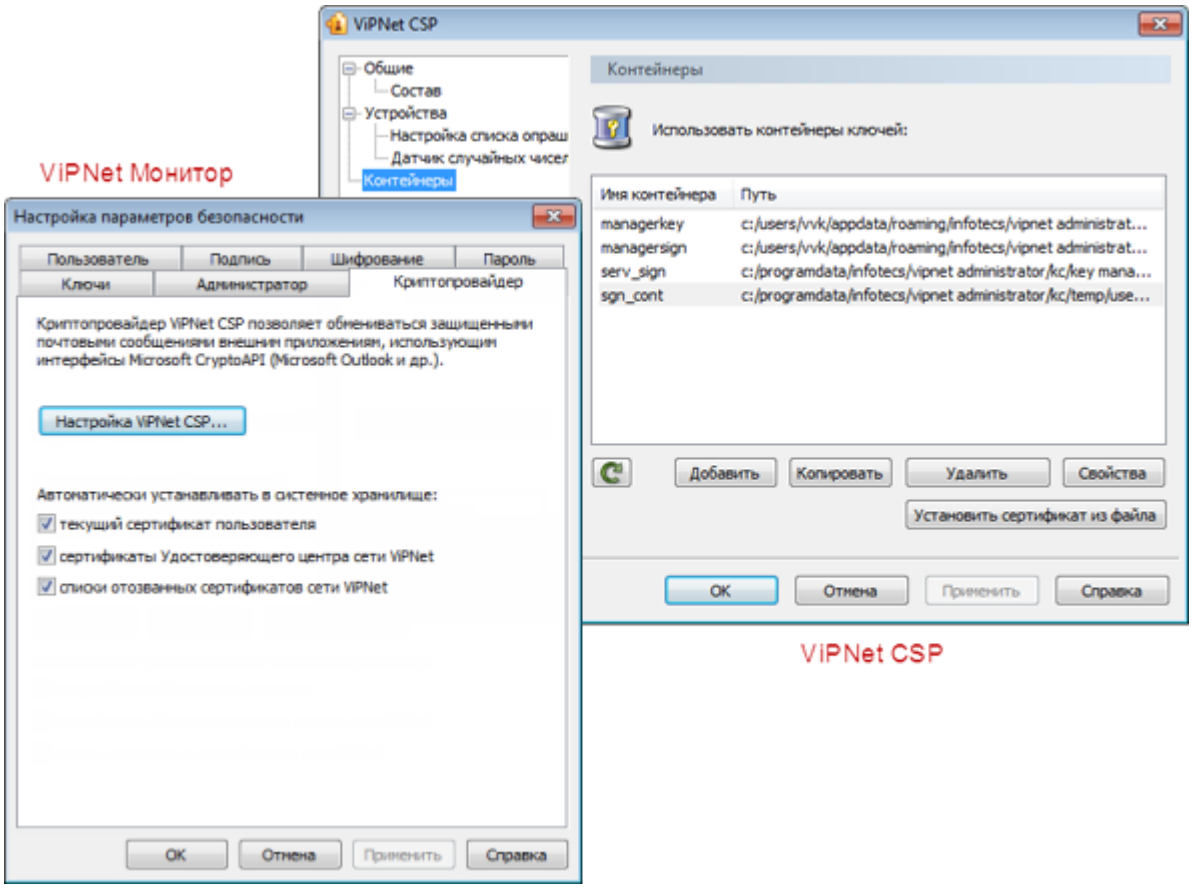



*Рисунок 191. Настройка параметров криптопровайдера*

- **Мастер установки ключей ViPNet**

  В версии 4.0 мастер первичной инициализации больше не используется. Мастер установки ключей ViPNet позволяет выполнять все сценарии, связанные с установкой и обновлением ключей на сетевом узле ViPNet (см. «Установка справочников и ключей» на стр. 51).

- **Способы аутентификации пользователя**

  В программе ViPNet Монитор версии 4.0 при использовании устройства аутентификации (способ **Устройство**) для входа в программу реализована возможность выполнять аутентификацию пользователя не только с помощью персонального ключа (как в версии 3.2.x), но и с помощью сертификата (см. «Способы аутентификации пользователя» на стр. 70).

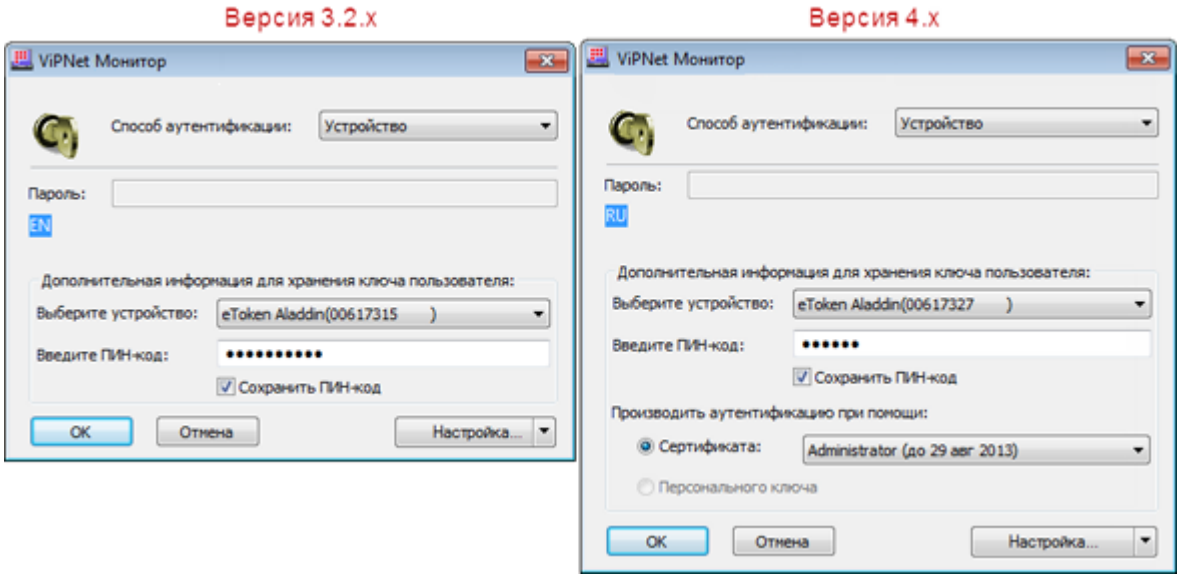



*Рисунок 192. Использование устройства для аутентификации пользователя*

Способ аутентификации **Пароль на устройстве** в дальнейшем поддерживаться не будет, поэтому в версии 4.0 рекомендуется перейти на другие способы аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 226).

Если для входа в программу используется пароль, то при смене пользователя достаточно выбрать в соответствующем списке учетную запись. При этом не требуется указывать папку ключей пользователя.

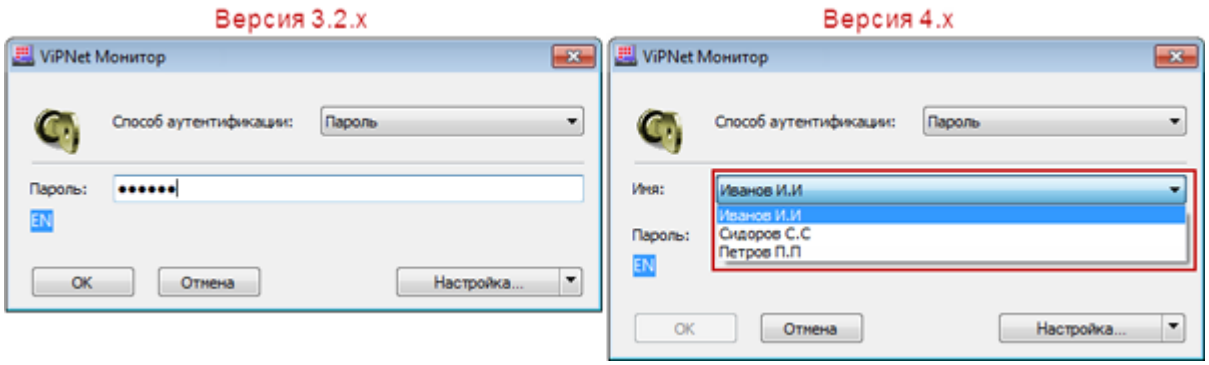



*Рисунок 193. Аутентификация пользователя с помощью пароля*

- **Система обновления ViPNet**

  В ViPNet Монитор версии 4.0 реализована новая система обновления, позволяющая принимать и устанавливать обновления программного обеспечения, справочников и ключей, а также политик безопасности, созданных в ViPNet Policy Manager. Система обновления продуктов ViPNet предоставляет удобный графический интерфейс для работы с поступившими файлами обновления.

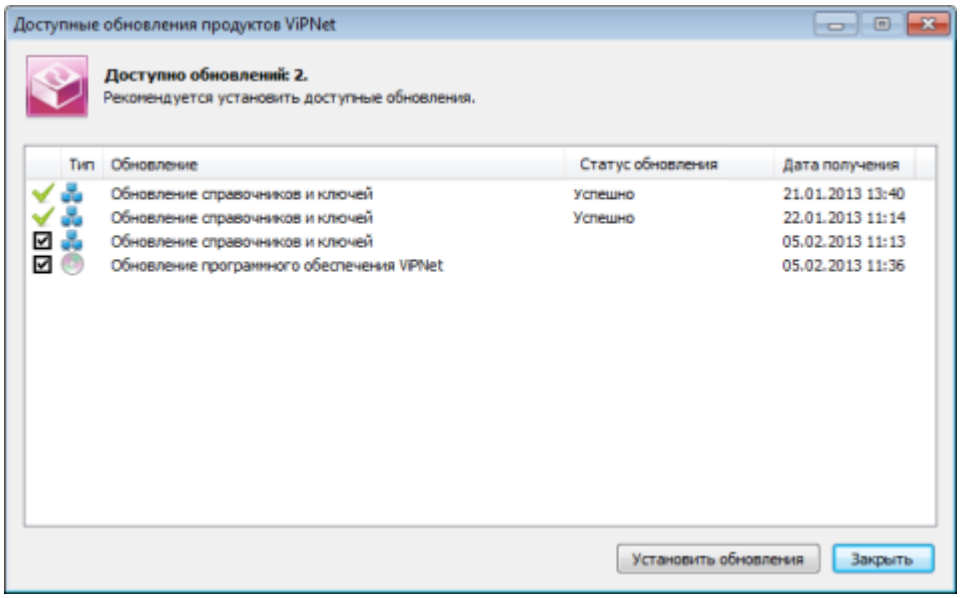



*Рисунок 194. Список полученных обновлений*

При поступлении файлов обновления вы получите уведомление.

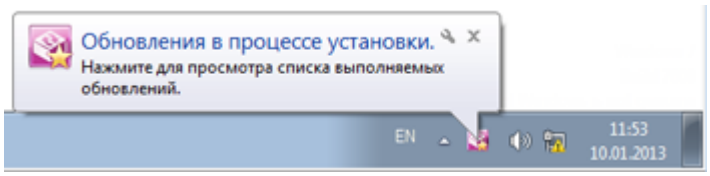



*Рисунок 195. Уведомление о получении и установке файлов обновления*

- **Создание фильтров для IP-пакетов**

  В программе ViPNet Монитор версии 4.0 реализована возможность использовать журнал IP-пакетов для создания фильтров (как разрешающих, так и блокирующих). В связи с этим удален раздел **Блокированные IP-пакеты** и все действия над IP-пакетами выполняются в разделе **Журнал IP-пакетов**.

- **Смена конфигураций программы**

  В программе ViPNet Монитор версии 4.x реализована возможность автоматической смены конфигураций. Если вы работаете с несколькими конфигурациями программы, каждую из которых нужно устанавливать в определенное время, вы можете настроить расписание смены этих конфигураций.

- **Ограниченный интерфейс пользователя**

  В версии 4.0 возможность ограничивать интерфейс пользователя (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 220) приравнена к назначению уровня полномочий 3. Таким образом, если узлу назначен уровень полномочий 3, то флажок ограничения интерфейса пользователя будет недоступен.

- **Блокировка компьютера и IP-трафика**

  В программе ViPNet Монитор версии 4.0 блокировка компьютера осуществляется стандартными средствами операционной системы. Реализована возможность блокировки всего IP-трафика (любые соединения с защищенными и открытыми узлами будут запрещены)

и отключения защиты трафика (прекращение обработки трафика и ведения журнала регистрации IP-пакетов, отключение системы обнаружения атак).

- **Интеграция с программой ViPNet SafeDisk-V**

  В версии 4.0 при работе с программой ViPNet SafeDisk-V больше не используются защищенные и незащищенные конфигурации. Параметры защиты трафика задаются в специальном окне. При запуске ViPNet SafeDisk-V программа ViPNet Монитор перезапускается, и большинство настроек становятся недоступными для редактирования, в том числе в целях безопасности невозможно сменить пользователя или выйти из программы ViPNet Монитор.

- **Новая база данных в программе ViPNet Деловая почта**

  В программе ViPNet Деловая почта версии 4.0 используется встроенная база данных SQLite, которая позволяет снять ограничение на количество писем в архиве базы данных, а также обеспечивает возможность одновременной обработки входящих и исходящих писем при автопроцессинге.

- **Изменения в интерфейсе и терминологии**

  *Таблица 20. Основные изменения в терминологии и интерфейсе*

| Что изменено | Версия 3.2.x | Версия 4.0 |
|---|---|---|
| Термины | Абонентский пункт | Клиент |
| | Прикладная задача | Роль |
| | Правила фильтрация трафика | Сетевые фильтры |
| | Экспорт настроек | Сохранение настроек |
| | Импорт настроек | Восстановление настроек |
| Главное меню | | Полностью переработано |
| Запуск компонентов Деловая почта, Контроль приложений, Файловый обмен, MFTP | Запускаются по нажатию соответствующих кнопок в главном окне программы ViPNet Монитор | Запускаются из меню **Приложения** |
| Сетевые фильтры | | Представление фильтров в программах ViPNet Монитор и ViPNet Policy Manager было приведено к единому виду |
| Настройка управления трафиком | Окно **Настройка** разделы **Общие** и **Обнаружение атак** | Настройка вынесена в новый раздел, а именно окно **Настройка** раздел **Управление трафиком** |
| Блокировка компьютера | Кнопка в главном окне программы | Кнопка блокировки удалена |

- **Обновление документации и справки**

Документация и справка, поставляемые вместе с ПО ViPNet Client, были существенно обновлены, для того чтобы отразить произошедшие изменения в функциональности программы.

# Что нового в версии 3.2.11

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.11.

- **Исправление ошибок в программе ViPNet Client**

  В программе ViPNet Client исправлены следующие ошибки:

  - Блокировка DHCP-трафика при запущенной программе ViPNet Client в случае, когда из одного сегмента сети по широковещательной рассылке передается большое количество запросов к DHCP-серверу.
  - Невозможность регистрировать DNS-серверы в файле `DNS.TXT` на компьютере, имя которого содержит русские символы.
  - Невозможность удаленного подключения с помощью программы Remote Desktop Connection.

- **Исправление ошибок в программе ViPNet Деловая почта**

  Исправлена ошибка архивации, которая проявлялась в предыдущих версиях программы.

# Что нового в версии 3.2.10

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.10.

- **Предупреждение о блокировании IP-пакетов**

  В программе ViPNet Монитор появилась возможность уведомления о блокировании IP-пакетов встроенным сетевым экраном. Чтобы включить уведомление, в окне **Настройка** в разделе **Общие** > **Предупреждения** установите флажок **Выдавать предупреждение о блокированных IP-пакетах**.

- **Исправление ошибок в ПО ViPNet Client:**

  - Исправлена ошибка, вызывавшая критический системный сбой в операционной системе Windows XP SP3.
  - Исправлена ошибка при проверке соединения с узлами, на которых установлено ПО ViPNet более ранних версий.

- **Изменения, касающиеся работы с сертификатами открытого ключа:**

  - Прекращена поддержка алгоритма формирования и проверки электронной подписи ГОСТ Р 34.10-94.
  - Исправлены ошибки при опросе точек распространения списков отозванных сертификатов (СОС).

- Исправлены ошибки при формировании запроса на квалифицированный сертификат.

- **Исправление ошибок в программе ViPNet Деловая почта**

  Исправлена ошибка при проверке электронной подписи сообщений, в которых отсутствует текст письма.

# Что нового в версии 3.2.9

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.9. Более подробная информация приведена в документе «Новые возможности ViPNet Client и ViPNet Coordinator версии 3.2. Приложение к документации ViPNet».

- **Совместимость с программным обеспечением других производителей**

  Обеспечена совместимость программного обеспечения ViPNet с приложениями Lumension Device Control, Cisco Security Agent, Kaspersky Administration Kit, MSDE 2000.

- **Улучшенная поддержка многоядерных процессоров**

  Оптимизирована параллельная обработка IP-пакетов в многопроцессорных системах. Благодаря своевременной обработке IP-пакетов и отправке полученных данных в нужной последовательности повышается скорость и качество передачи мультимедиа информации.

- **Увеличение количества обрабатываемых программой прикладных протоколов**

  Расширен список прикладных протоколов, для которых в программе ViPNet Монитор реализована специальная обработка IP-пакетов.

- **Интеграция ПО ViPNet Client с ПО ViPNet SafeDisk-V**

  Благодаря интеграции обеспечена дополнительная защита конфиденциальной информации, хранящейся в контейнерах ViPNet SafeDisk-V (на стр. 397). Теперь доступ к контейнерам в программе ViPNet SafeDisk-V определяется текущей конфигурацией ViPNet Монитор — защищенной или незащищенной.

- **Новый способ представления информации о блокированных IP-пакетах**

  В разделе **Блокированные IP-пакеты** главного окна представлены IP-пакеты, заблокированные с момента запуска программы ViPNet Монитор или с момента последней очистки списка.

- **Изменение отображения фильтров защищенной сети и задания правил фильтрации защищенного трафика**

  Информация обо всех фильтрах объединена в разделе **Сетевые фильтры** главного окна.

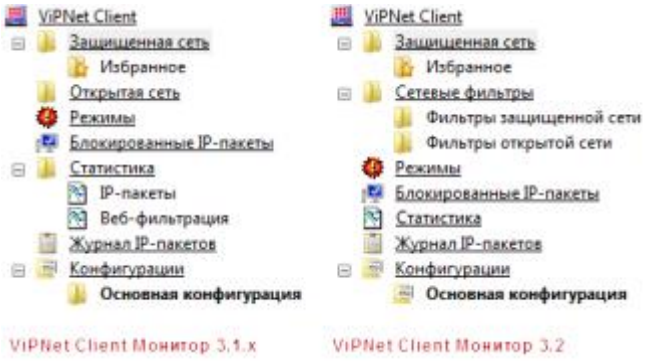



*Рисунок 196. Отображение фильтров на панели навигации главного окна в ПО ViPNet Client Монитор версий 3.1.x и 3.2*

Приведена к единому виду структура фильтров защищенной и открытой сети, а также набор возможных действий с фильтрами.

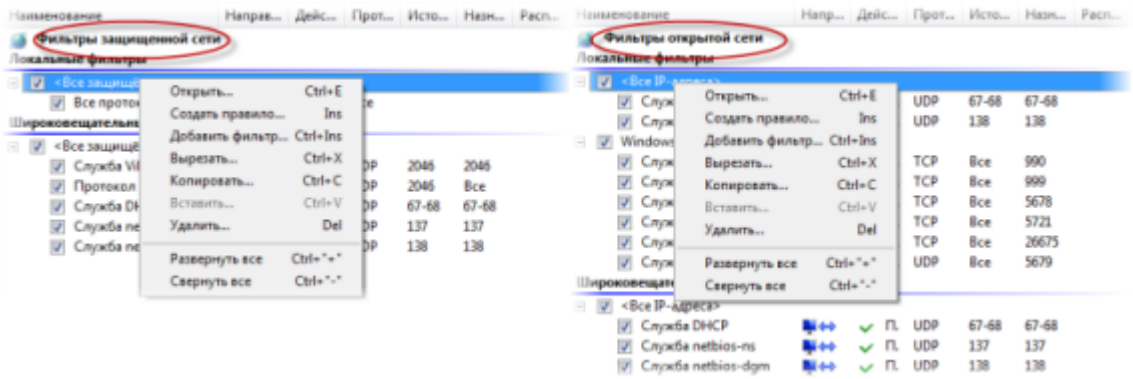



*Рисунок 197. Отображение фильтров защищенной и открытой сетей в ПО ViPNet Монитор 3.2 и возможные действия с этими фильтрами*

- **Автоматический вход в ПО ViPNet Client**

  Реализована возможность входа в программу без необходимости подтверждения пароля пользователя ViPNet в окне входа в программу. Управление данной функцией возможно только в режиме администратора в окне **Настройка параметров безопасности** на вкладке **Администратор**. Если флажок **Автоматически входить в ViPNet** установлен, при запуске программы на текущем сетевом узле окно входа в программу не появляется и вход в ПО ViPNet Client выполняется автоматически.

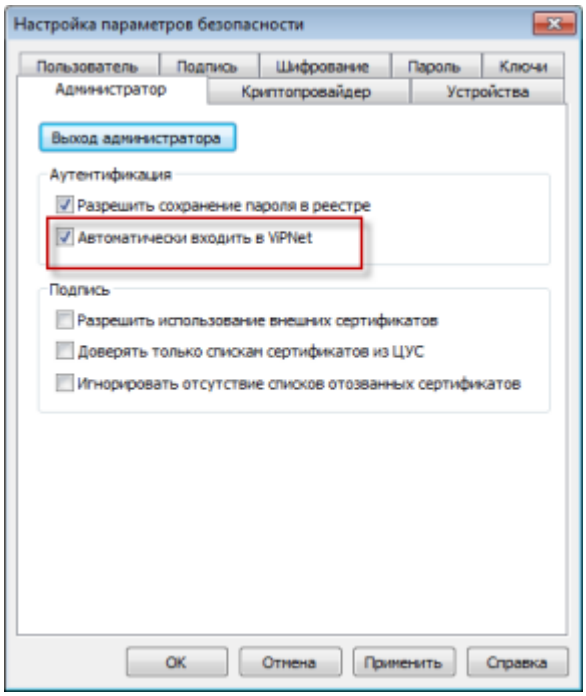



*Рисунок 198. Настройка автоматического входа в ПО ViPNet Client*

- **Автоматическое получение и ввод в действие сертификатов, изданных по инициативе администратора без запроса со стороны пользователя**

  Реализована возможность автоматически получать и вводить в действие сертификаты, изданные администратором в программе ViPNet Удостоверяющий и ключевой центр по собственной инициативе. Если функция включена, получение таких сертификатов и ввод их в действие не требуют никаких дополнительных действий со стороны пользователя. После того как сертификат будет введен в действие, появится окно **Предупреждение сервиса безопасности** с соответствующим сообщением (см. «Сертификат, изданный по инициативе администратора, введен в действие» на стр. 296).

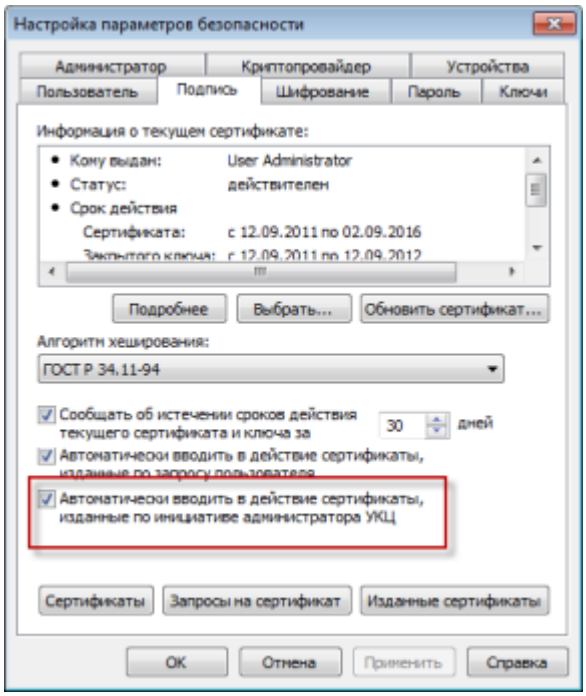



*Рисунок 199. Новый элемент вкладки «Подпись» окна «Настройка параметров безопасности»*

- **Разработан новый мастер установки ключей ViPNet**

  Новый мастер установки ключей поддерживает работу с дистрибутивами ключей, созданными в программе ViPNet Удостоверяющий и ключевой центр версий 2.8 и 3.x и в программе ViPNet Network Manager версий 2.x и 3.0. Кроме того, новый мастер обладает более богатыми функциональными возможностями и удобным пользовательским интерфейсом.

**Внимание!** В сетях ViPNet, управляемых с помощью ПО ViPNet Administrator, не рекомендуется использовать мастер **Установка ключей сети ViPNet** на сетевых узлах, на которых зарегистрировано несколько пользователей ViPNet или установлено несколько программ, использующих ключи ViPNet.

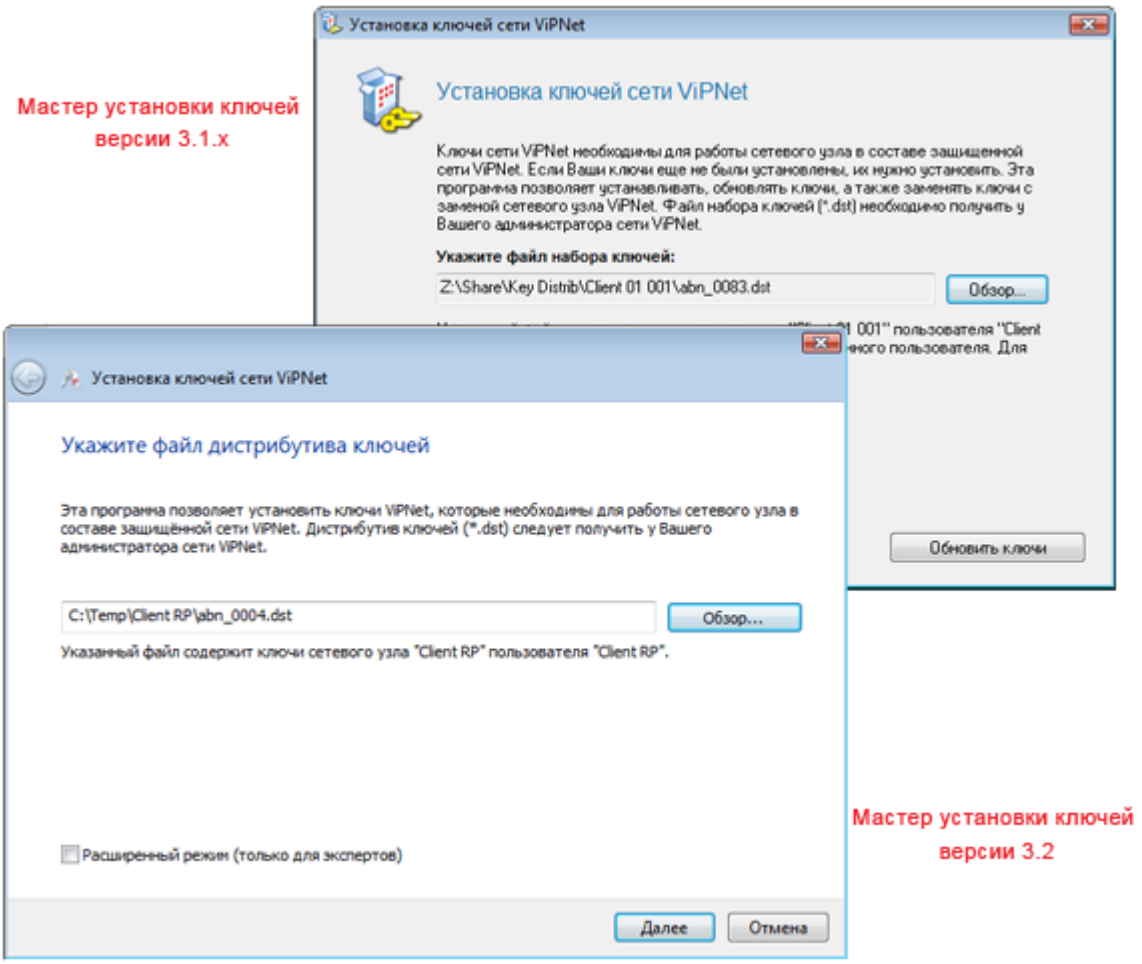



*Рисунок 200. Новый мастер установки ключей ViPNet*

- **Доработка Криптопровайдера ViPNet**

  Реализована следующая функциональность для компонента Криптопровайдер ViPNet:

  - поддержка TLS-протокола в ОС Windows 7;
  - совместимость с 64-разрядными операционными системами;
  - шифрование и электронная подпись в Microsoft Office 2010.

  Появилась возможность установки сертификата в контейнер ключей.

- **Доработка программы ViPNet Контроль приложений**

  Реализована следующая функциональность для программы ViPNet Контроль приложений:

  - совместимость с 64-разрядными операционными системами;
  - работа в нескольких сессиях.

- **Расширен список поддерживаемых устройств аутентификации**

Реализована поддержка следующих устройств аутентификации: Mifare, Mifare Standard 4K, eToken ГОСТ, JaCarta, устройства компании Gemalto с апплетом «Аладдин Р.Д.», устройство Kaztoken с поддержкой казахстанского стандарта электронной подписи. Теперь эти устройства можно применять для записи и считывания персональной информации.

- **Ограничено использование устаревших алгоритмов шифрования**

  В соответствии с требованиями контролирующих органов в приложениях ViPNet введен запрет на шифрование файлов размером более 4 Мбайт с использованием ключей, созданных в программе ViPNet Удостоверяющий и ключевой центр версии 2.8. В связи с этим программе ViPNet Деловая почта будет невозможна отправка вложенных файлов размером более 4 Мбайт в доверенные сети, для связи с которыми используются ключи версии 2.8.

  Администратору сети ViPNet рекомендуется обновить межсетевые мастер-ключи, если программное обеспечение ViPNet Administrator было обновлено с версии 2.8 до версии 3.x и после этого не выполнялась смена межсетевых мастер-ключей. Подробнее об обновлении межсетевых мастер-ключей см. документ «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора».

- **Изменены некоторые термины и названия элементов интерфейса, содержащие эти термины**

  Для соответствия Федеральному закону 06.04.2011 N 63-ФЗ «Об электронной подписи» (текст закона http://www.rg.ru/2011/04/08/podpis-dok.html) термин «электронная цифровая подпись» («цифровая подпись») в интерфейсе программы изменен на термин «электронная подпись».

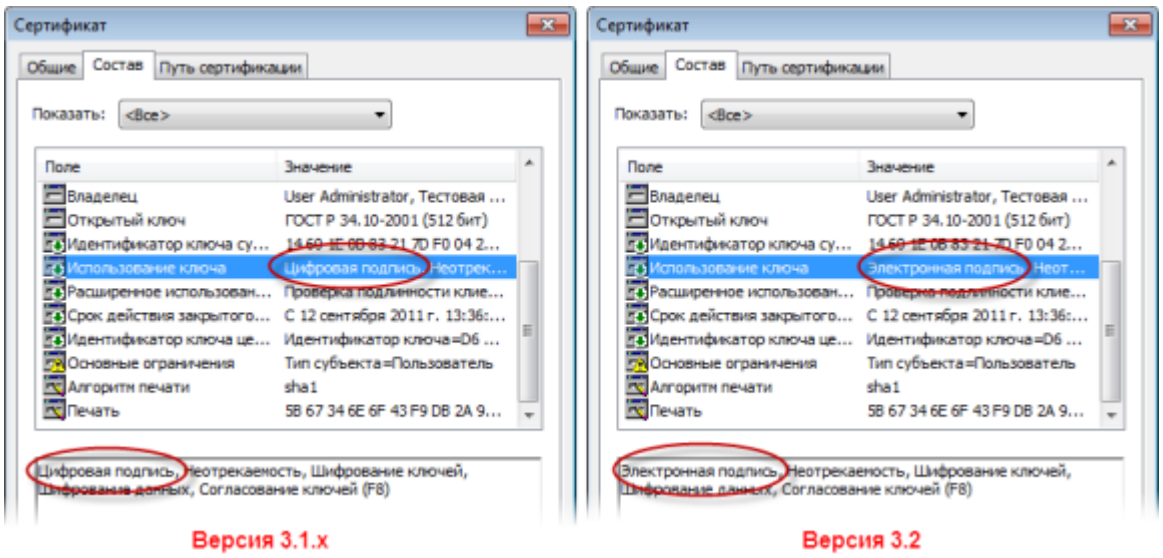



*Рисунок 201. Изменение термина «цифровая подпись» на примере окна «Сертификат»*

Прочие изменения терминологии приведены в таблице ниже:

| Что изменено | До изменения, в версиях 3.1.x | В результате изменения, в версии 3.2 |
|---|---|---|
| Название окна | **Правило доступа** (окно, вызываемое из раздела **Защищенная сеть**) | **Свойства узла** |
| Термины | **Правило доступа** | **Правило** |
| | **Фильтр протоколов** | **Фильтр** |
| Пункт меню **Сервис** | **Настройка прикладных протоколов** | Пункт отсутствует |
| Раздел окна **Настройка** | **Блокированные IP-пакеты** | Раздел отсутствует |
| Интерфейс для настройки параметров работы прикладных протоколов | Окно **Настройка прикладных протоколов** | Раздел **Настройка прикладных протоколов** в окне **Настройка** |
| Контекстное меню элементов раздела **Блокированные IP-пакеты** главного окна | Совпадает с контекстным меню элементов разделов **Открытая сеть** и **Защищенная сеть** | Индивидуальное контекстное меню |

- **Обновление документации и справки**

  Документация и справка, поставляемые вместе с ПО ViPNet Client, были существенно обновлены, для того чтобы отразить изменения в функционале программы.

# Что нового в версии 3.1.5

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.1.5.

- **Контроль работоспособности приложений, установленных на ViPNet-кластере**

  Реализована возможность организовать постоянное слежение за работоспособностью приложений, установленных на ViPNet-кластере и специально адаптированных для работы на нем. Это позволяет обеспечить высокий уровень отказоустойчивости и доступности данных приложений в процессе их работы. Настройка параметров контроля работоспособности приложений и мониторинг их состояния осуществляется с помощью программы ViPNet Cluster Монитор. Подробную информацию см. в документе «ViPNet Cluster. Руководство администратора».

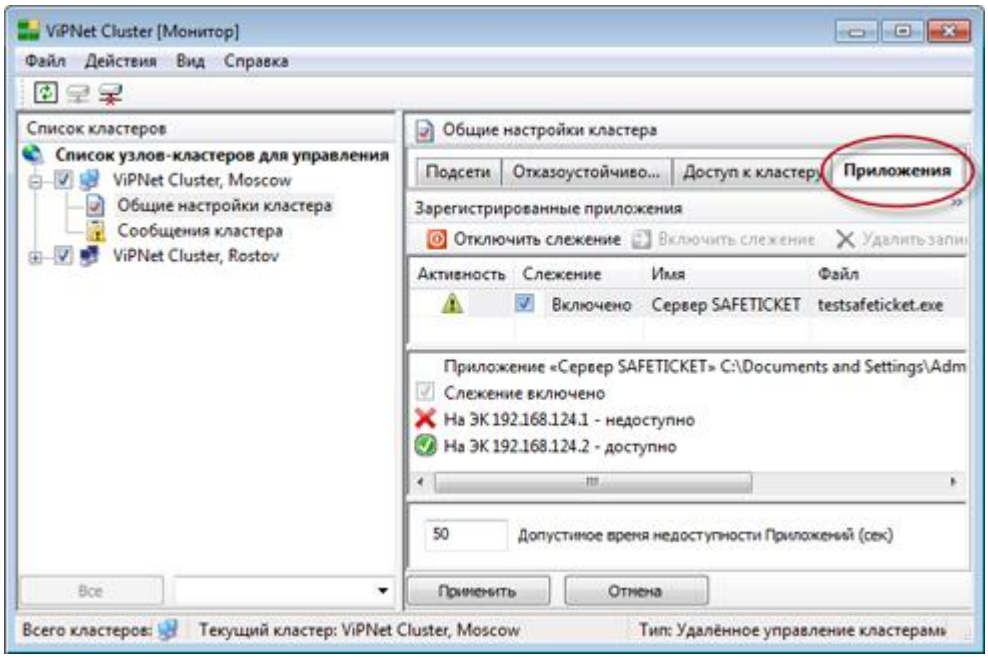



*Рисунок 202. Настройка параметров контроля приложений в ViPNet Cluster Монитор*

- **Изменены некоторые термины и названия элементов интерфейса, содержащие эти термины**

| Старый термин | Новый термин |
|---|---|
| Режим авторизации | Способ аутентификации |
| Контейнер ключей подписи, ключевой контейнер, контейнер закрытого ключа, контейнер с закрытым ключом, контейнер с открытым ключом | Контейнер ключей |
| Дистрибутив справочно-ключевой информации | Дистрибутив ключей |
| Ключевой диск (КД) | Ключи пользователя ViPNet |
| Ключевой набор (КН) | Ключи узла ViPNet |

В связи с изменениями переработан интерфейс программ ViPNet Client и ViPNet Coordinator.

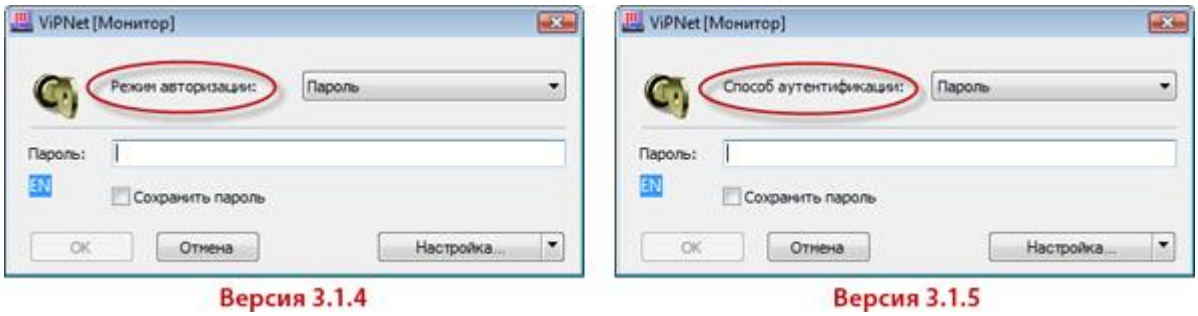



*Рисунок 203. Измененный интерфейс окна ввода пароля*

В соответствии с заменой терминов обновлена документация и справка по всем продуктам.

- **Документация и справка других локализаций**

  Проведена проверка актуальности документации и справки к продуктам ViPNet на других языках (немецком, испанском и французском) в соответствии с текущей русской версией. Также выполнено обновление английской документации и справки.

# Что нового в версии 3.1.4

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.1.4.

- **Модернизированный механизм блокировки компьютера**

  Изменен механизм блокировки компьютера: теперь для блокировки используется встроенная функциональность ОС Windows.

- **Автоматическая защита узла при отключении устройства аутентификации пользователя**

  Добавлен контроль отключения аппаратных средств аутентификации пользователя. Теперь при отключении устройства аутентификации автоматически блокируется компьютер и IP-трафик. Режим блокировки можно изменить с помощью настроек: задать блокировку только компьютера, только IP-трафика либо не использовать блокировку.

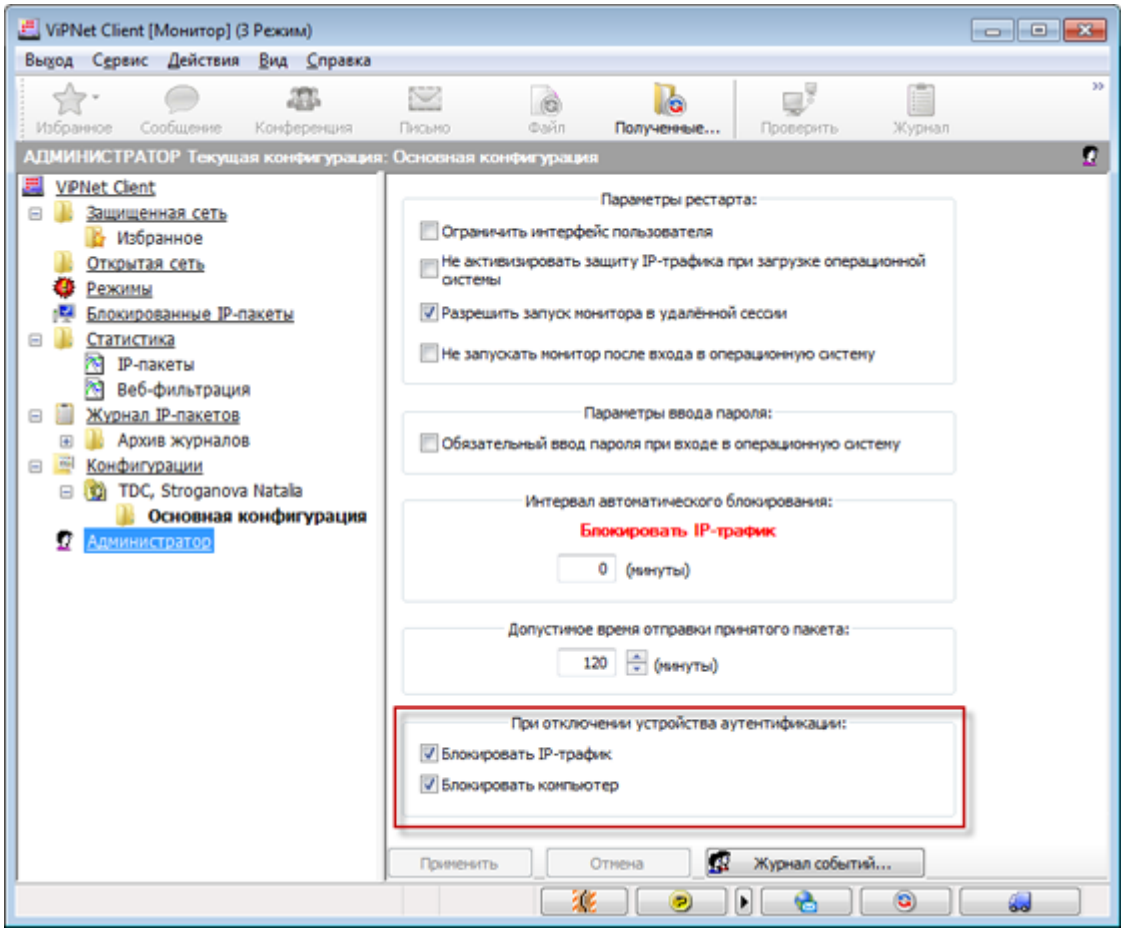



*Рисунок 204. Настройка блокировки при отключении устройства аутентификации*

- **Ограничение количества записей в разделе блокированных IP-пакетов**

  Реализован контроль числа отображаемых блокированных IP-пакетов. Теперь отображается не более 300 IP-адресов и для каждого адреса не более 30 записей по каждому порту. Информация в разделе блокированных IP-пакетов обновляется при каждом открытии или обновлении раздела. Если при этом указанные ограничения окажутся превышены, то будут удалены самые старые записи и добавлены новые.

- **Более информативный экспортированный журнал IP-пакетов**

  Расширен список параметров IP-пакетов, включаемых в экспортированную версию журнала IP-пакетов. Теперь при просмотре журнала в веб-браузере или в Microsoft Excel отображается полная информация о пакетах.

- **Более информативные сведения о числе элементов в папках программы ViPNet Деловая почта**

  Изменен принцип отображения числа элементов в папках программы ViPNet Деловая почта. Теперь при перемещении по дереву папок отображается общее число элементов, содержащихся в текущей папке и всех ее подпапках. Для папки «Входящие» дополнительно отображается число непрочитанных писем, а для папки «Исходящие» — число недоставленных писем.

- **Корректное отображение последней выделенной позиции в папке при переходе между папками программы ViPNet Деловая почта**

  Реализовано сохранение позиции последнего выбранного элемента при переходе между папками программы ViPNet Деловая почта. Теперь при переходе из одной папки в другую запоминается позиция выбранного элемента, и при возврате в папку этот элемент остается выбранным и находится в той же позиции экрана.

- **Доработка поиска в программе ViPNet Деловая почта**

  Изменена логика при открытии окна поиска в программе ViPNet Деловая почта. Теперь в качестве папки поиска (поле **Искать в**) подставляется текущая папка, а также не перемещается фокус (текущим всегда является поле **Архив**).

- **Более прозрачная логика обработки входящих писем правилами автопроцессинга**

  Изменена логика обработки входящих писем правилами автопроцессинга программы ViPNet Деловая почта. В новой версии:

  - если в правиле задан список отправителей, то под это правило подпадают входящие письма, отправитель которых входит в заданный список;
  - если в правиле задан список пользователей для проверки подписи, то под это правило подпадают входящие письма, вложения которых подписаны одним из заданных пользователей (при условии действительности подписи);
  - входящие письма с отсутствующим текстом (телом письма) не копируются на диск в виде файла blank.txt.

- **Более понятное управление включением и отключением криптопровайдера ViPNet CSP**

  Изменен способ включения и отключения криптопровайдера ViPNet CSP в настройках параметров безопасности (на вкладке Криптопровайдер). Теперь вместо флажка используется кнопка, а также отображается понятное сообщение в случае отсутствия прав на изменение этого параметра.

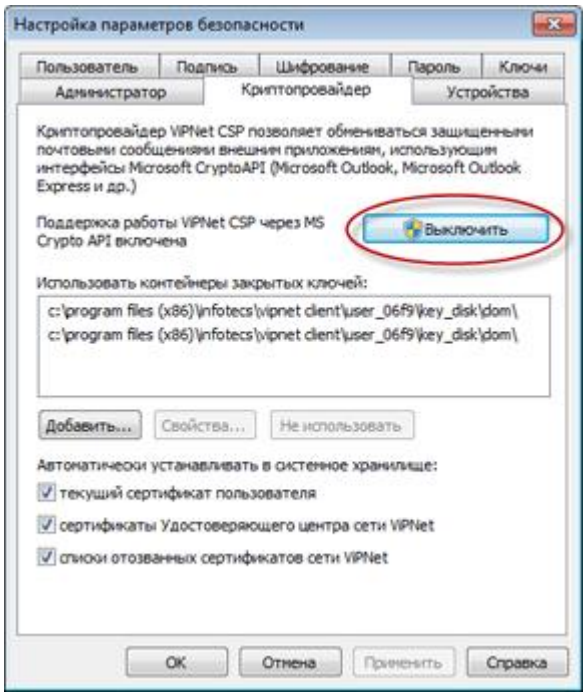



*Рисунок 205. Кнопка включения и отключения криптопровайдера*

- **Устранена проблема входа в программу ViPNet Монитор при использовании Network Logon 5.1**

  Обеспечена совместимость программы ViPNet Монитор с eToken Network Logon 5.1. Теперь вход в ViPNet Монитор происходит одинаково как при использовании Network Logon 5.1, так и без него.

- **Улучшенная справка**

  Изменен внешний вид справки, улучшена наглядность предоставляемой справочной информации.

- **Документация и справка других локализаций**

  Выпущена документация и справка к продуктам ViPNet на испанском языке. Документация и справка на немецком и французском языках обновлены в соответствии с русской версией. Также выполнено обновление английской документации и справки.

# Что нового в версии 3.1.3

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.1.3.

- **Сняты ограничения на удаленный запуск ПО ViPNet**

  Изменено значение параметра «Разрешить запуск монитора в удаленной сессии», используемое по умолчанию. Теперь удаленным пользователям запуск ViPNet Монитор по умолчанию разрешен.

- **Оптимизирована межузловая рассылка**

Существенно сокращено число служебных рассылок между сетевыми узлами. Теперь информация о состоянии и параметрах узлов отправляется только тем узлам сети, которым эта информация действительно необходима. Для снижения числа рассылок дополнительно используется агрегирование сообщений в течение определенного периода времени.

- **Поддержка DHCP-протокола при работе в конфигурации «Открытый Интернет»**

  Изменена технология выхода защищенных узлов в открытый Интернет. Теперь при работе в конфигурации «Открытый Интернет» узлы могут получать IP-адреса от защищенного DHCP-сервера.

- **Поддержка кластера на 64-разрядных ОС**

  Реализована поддержка функционирования ПО ViPNet Cluster на координаторах, работающих под управлением 64-разрядных операционных систем.

- **Расширенная поддержка системы централизованного мониторинга ViPNet StateWatcher**

  Реализован агент мониторинга, расширяющий сбор информации о состоянии узлов сети ViPNet. Теперь можно анализировать работоспособность транспортного модуля MFTP и программы ViPNet Деловая почта, количество конвертов в очереди и их суммарный размер, список туннелируемых координатором адресов, суммарный трафик на каждом сетевом интерфейсе (отдельно исходящий и входящий), загрузку процессора, использование памяти и дискового пространства, записи о событиях из системного журнала и журнала приложений ОС Windows.

- **Усилена защита от некорректной установки или обновления ключей на сетевых узлах**

  Реализован контроль соответствия дистрибутива ключей (файла *.dst) типу сетевого узла (клиент или координатор). Теперь установка или обновление выполняются, только если дистрибутив создан для того же приложения (ViPNet Client или ViPNet Coordinator), которое установлено на узле.

- **Документация и справка других локализаций**

  Появилась документация и справка к продуктам ViPNet на немецком и французском языках.

# Что нового в версии 3.1.2

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.1.2.

- **Более понятные названия способов аутентификации.**

  Названия режимов, используемых для авторизации пользователей, переименованы следующим образом:

  - **Пароль**.
  - **Пароль на устройстве**.
  - **Устройство**.

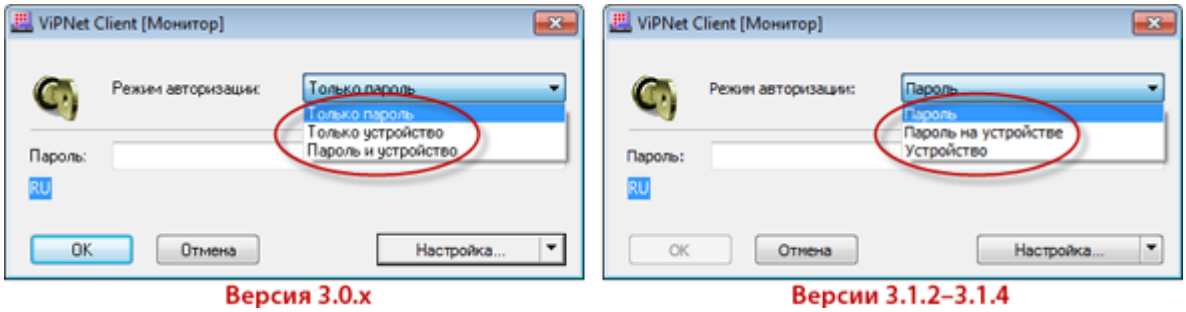



*Рисунок 206. Изменение типов авторизации*

- **Оптимальное расположение различных настроек**

  Настройки, находившиеся на панели навигации, удалены с неё и объединены с другими настройками.

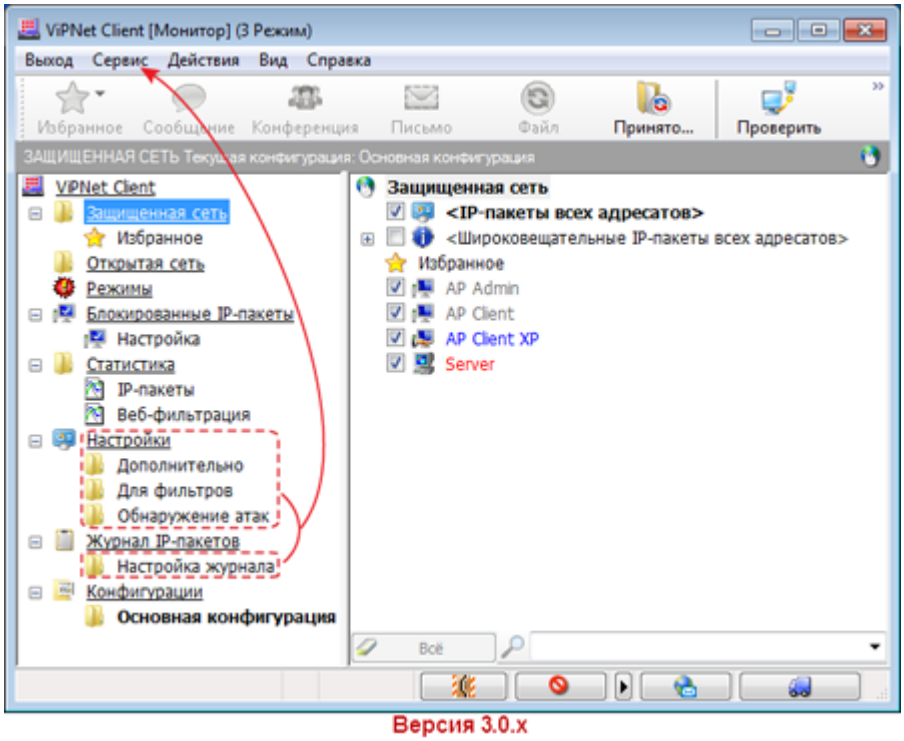



*Рисунок 207. Изменение местоположения настроек защищенной сети*

Теперь все настройки содержатся в одном окне, которое вызывается по команде **Сервис** > **Настройки**.

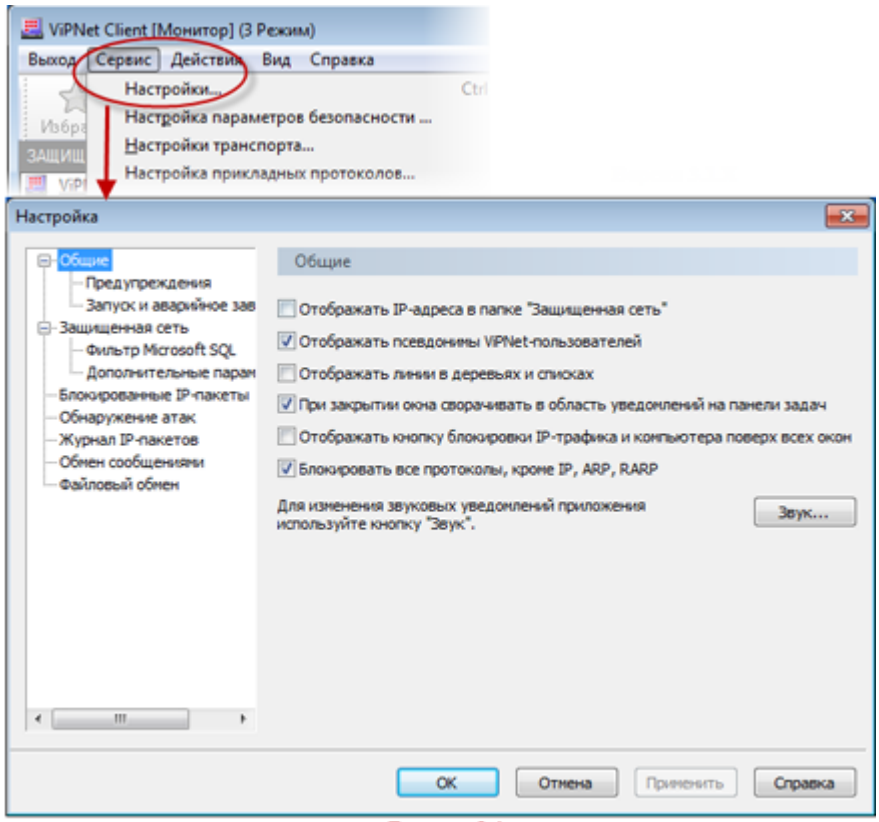



*Рисунок 208. Настройки защищенной сети в новой версии*

- **Дополнительный способ проверки соединения с узлом**

  Появилась возможность проверить соединение с узлом в течение сеанса обмена защищенными сообщениями с этим узлом. Для этого достаточно щелкнуть узел правой кнопкой мыши и в контекстном меню выбрать команду **Проверить соединение**.

- **Более удобный способ просмотра информации о статусе нескольких узлов**

  При проверке соединения сразу с несколькими сетевыми узлами информация о статусе этих узлов отображается не в отдельных окнах, а в одном окне.

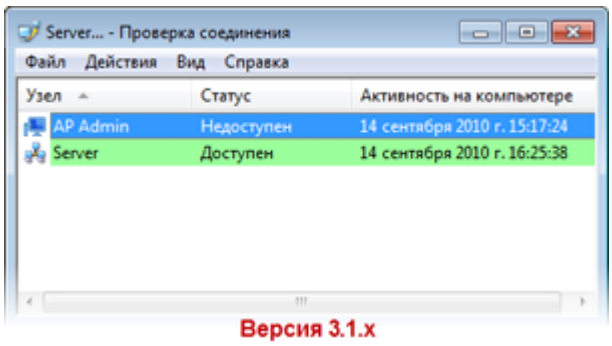



*Рисунок 209. Проверка соединения с несколькими узлами сети*

- **Детализация информации о доступности узла**

  К сообщениям, выводимым при проверке соединения с узлом, добавлено специальное сообщение для ситуации, когда узел доступен по сети, но ПО ViPNet на нем неактивно.

- **Более простая процедура отправки файлов**

  Сократилось количество действий, необходимых для отправки файлов получателям.

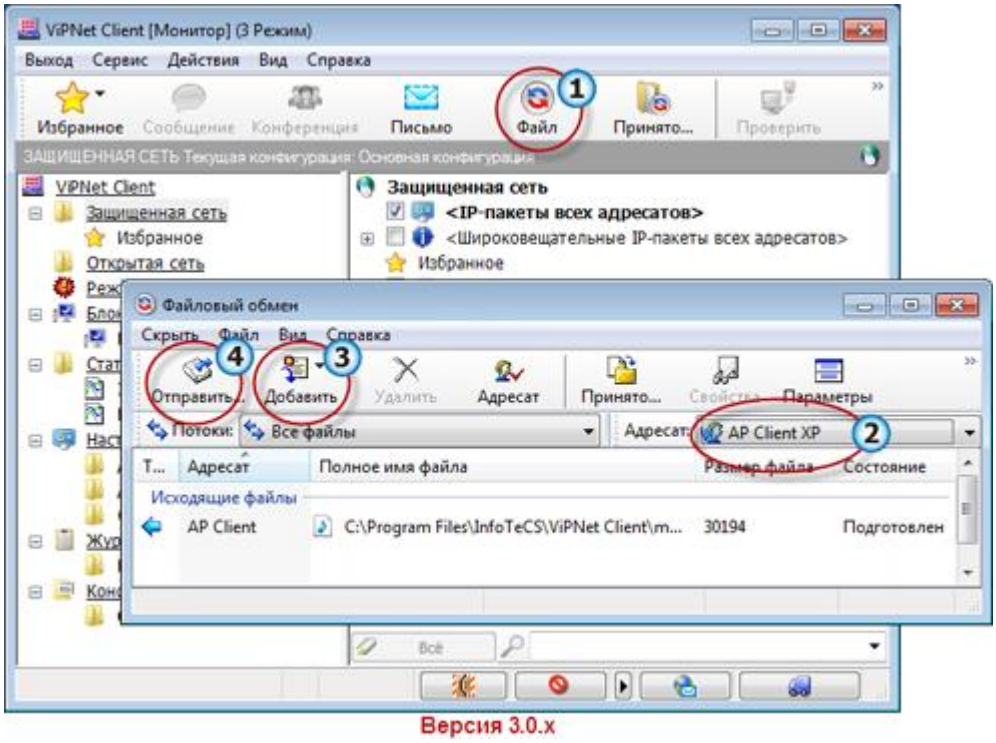



*Рисунок 210. Процесс файлового обмена*

Теперь отправка файлов осуществляется сразу после выбора получателя (сетевого узла).

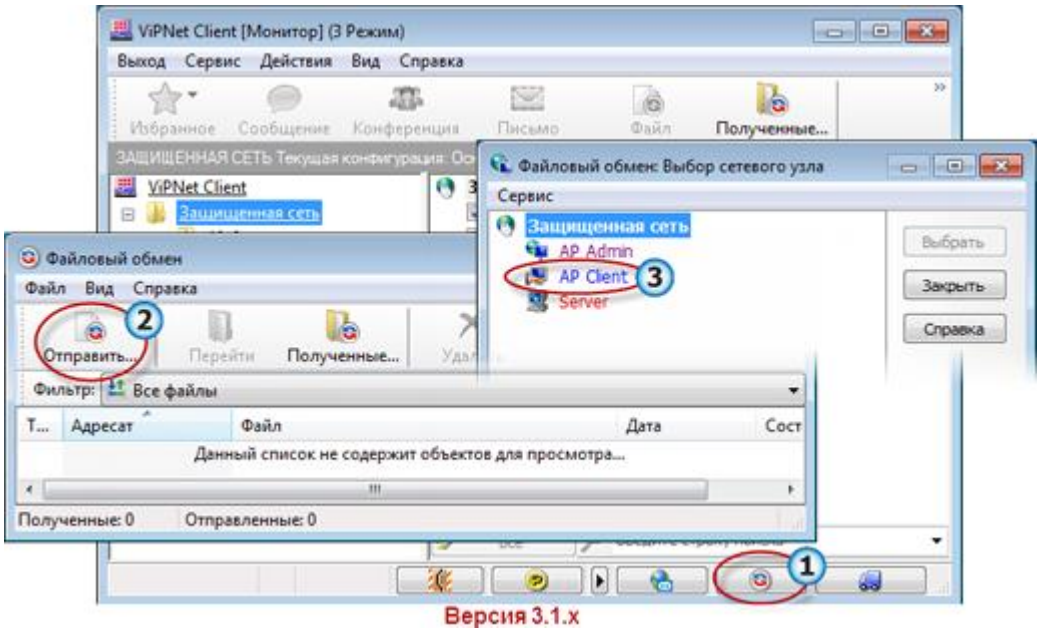



*Рисунок 211. Измененный процесс файлового обмена*

- **Возможность добавления правил фильтрации при просмотре блокированных IP-пакетов**

  Появилась возможность добавлять правила фильтрации для открытой сети и туннелируемых узлов из окна блокированных IP-пакетов.

- **Расширенные возможности поиска**

  Расширен список параметров, по которым выполняется поиск сетевых узлов. Теперь узлы можно искать по имени или идентификатору узла, имени компьютера, псевдониму, DNS-имени, по виртуальным и реальным IP-адресам.

- **Дополнительные способы входа в режим администратора**

  Появилась возможность быстро войти в режим администратора одним из следующих способов: из области уведомлений Windows или по команде **Сервис** > **Вход администратора**.

- **Унификация логики доступа к журналу IP-пакетов**

  Переход к просмотру журнала IP-пакетов, выполняемый из разных точек интерфейса, теперь происходит одинаковым образом: сначала открывается окно поиска для задания параметров отбора записей из журнала, затем — окно просмотра отобранных записей.

- **Возможность настройки некоторых параметров при входе в программу**

  Появилась возможность указать транспортный каталог и каталог ключей пользователя при входе в программу.

- **Новый механизм включения антиспуфинга на координаторе**

  Изменен механизм включения антиспуфинга на координаторе: теперь антиспуфинг включается отдельно для каждого сетевого интерфейса.

- **Дополнительные полномочия пользователей**

  Добавлена поддержка новых полномочий «h» для прикладной задачи «Защита трафика». При этом уровне полномочий на узле всегда присутствуют две фиксированные конфигурации «Внутренняя сеть» и «Интернет». В конфигурации «Внутренняя сеть» разрешена работа с ресурсами защищенной сети и запрещен доступ в Интернет, в конфигурации «Интернет» разрешена работа в Интернете и запрещен доступ в защищенную сеть.

- **Независимость установки ПО ViPNet от текущей локализации**

  Убраны отличия в регистрации ПО ViPNet различных локализаций. Теперь при обновлении ПО ViPNet можно установить поверх используемой версии версию другой локализации.

- **Расширенная поддержка протокола SIP**

  Реализована поддержка протокола SIP в случае, когда на компьютере установлено несколько сетевых интерфейсов. Теперь в этом случае есть возможность пользоваться IP-телефонией, защищенной технологиями ViPNet.

- **Автоматическая настройка доступа к корпоративным защищенным DNS- и WINS-серверам**

  Реализована регистрация защищенных DNS- и WINS-серверов средствами ПО ViPNet (см. «Создание списка DNS (WINS) серверов вручную» на стр. 121). Теперь достаточно внести информацию о серверах в специальный файл, и их IP-адреса автоматически будут добавлены в настройки сетевых интерфейсов. Автоматическая настройка удобна для мобильных пользователей, а также в случае, если DNS- и WINS-серверы доступны по виртуальным адресам.

- **Усовершенствованная документация и справка**

Полностью переработаны документация и справка, улучшено их качество. При переработке документации акцент сделан на сценарный подход.

# Глоссарий

## DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса серверов DNS, IP-адреса серверов WINS.

## PKI (инфраструктура открытых ключей)

От англ. Public Key Infrastructure — инфраструктура открытых ключей. Комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

## TCP-туннель

Способ соединения клиентов, находящихся во внешних сетях, с другими узлами сети ViPNet. Используется в том случае, если соединение по UDP-протоколу блокируется провайдерами услуг Интернета.

TCP-туннель разворачивается на координаторе, который является для клиента сервером соединений. Основной принцип соединения через TCP-туннель заключается в следующем: от клиента до координатора передача IP-пакетов осуществляется по протоколу TCP, на координаторе полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по протоколу UDP.

## ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

## ViPNet Network Manager

Программа, которая входит в состав программного комплекса ViPNet VPN. Предназначена для создания, конфигурирования и управления малыми и средними сетями ViPNet.

## ViPNet SafeDisk-V

Программное обеспечение, предназначенное для защиты конфиденциальной информации. Входит в состав программных комплексов ViPNet и ViPNet VPN. Для хранения конфиденциальной информации в программе ViPNet SafeDisk-V создается контейнер, который представляет собой зашифрованный файл на жестком диске или на съемном носителе.

## ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

## ViPNet Центр управления сетью (ЦУС)

В сети, которая администрируется при помощи ПО ViPNet Administrator, ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

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

В сети, которая администрируется при помощи ПО ViPNet Network Manager, Центр управления сетью — это рабочее место администратора сети ViPNet. В ЦУСе создается структура сети ViPNet, формируются и отправляются на сетевые узлы обновления наборов ключей и программного обеспечения ViPNet.

## Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является

тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

## Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet Б назначаются непосредственно на узле А. На других узлах узлу ViPNet Б могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

## Внешние IP-адреса

Адреса внешней сети.

## Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

## Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

## Закрытый ключ

Закрытая (секретная) часть пары асимметричных ключей. Может использоваться для создания электронных подписей, которые можно проверять с помощью парного ему открытого ключа, или для расшифрования сообщений, которые были зашифрованы парным ему открытым ключом.

Ключ электронной подписи является закрытым ключом.

## Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

### Защищенное соединение

Соединение между узлами, зашифрованное с помощью программного обеспечения ViPNet.

### Защищенные прикладные серверы

Прикладные серверы (веб-сервер, почтовый сервер, FTP-сервер и так далее), размещенные на защищенных узлах.

### Защищенный DNS или WINS сервер

Сервер DNS или WINS, размещенный на защищенном узле.

### Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

### Клиент (ViPNet-клиент)

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

### Ключ защиты

Ключ, на котором шифруется другой ключ.

### Ключи пользователя ViPNet

Совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей, и к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

### Контейнер ключей

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

## Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator или ViPNet Coordinator Linux) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

## Корневой сертификат

Самоподписанный сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

## Лицензия на сеть

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet. В частности, лицензия на сеть ViPNet определяет следующее: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов, на которые можно добавить ту или иную роль, максимальную разрешенную версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

## Обновление справочников и ключей

Файлы, формируемые администратором сети ViPNet в управляющем приложении (ViPNet Центр управления сетью, ViPNet Удостоверяющий и ключевой центр, ViPNet Network Manager) при изменении справочников и ключей для сетевых узлов ViPNet, то есть, в случае добавления, удаления сетевого узла ViPNet, добавления пользователя, издания нового сертификата и так далее. Администратор сети ViPNet централизованно высылает на сетевой узел сформированные новые ключи и справочники из ЦУСа или ViPNet Network Manager.

## Открытый Интернет

Технология, реализованная в программном обеспечении ViPNet. При подключении к Интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от Интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

## Открытый ключ

Открытая (не секретная) часть пары асимметричных ключей. Открытый ключ доступен любым пользователям информационной системы и может использоваться для шифрования и подтверждения подлинности электронной подписи.

Ключ проверки электронной подписи является открытым ключом.

### Открытый сервер DNS или WINS

Сервер DNS или WINS на открытом узле.

### Открытый узел

Узел, с которым обмен информацией происходит в незашифрованном виде.

### Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

### Папка ключей сетевого узла

Папка, в которой находятся ключи сетевого узла ViPNet и справочники.

### Пароль администратора сетевого узла ViPNet

Пароль для входа на сетевом узле ViPNet в режим администратора, в рамках которого становятся доступны дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр (в сетях, которые администрируются при помощи ПО ViPNet Administrator) или ViPNet Network Manager (в сетях, которые администрируются при помощи ПО ViPNet Network Manager).

### Пароль пользователя на основе парольной фразы

Пароль пользователя необходим для входа в любую программу ViPNet. Случайный пароль создается на основе парольной фразы, которую можно использовать для запоминания пароля. Парольные фразы могут быть созданы на нескольких языках. Фразы представляют собой грамматически корректные конструкции, однако слова, составляющие фразу, выбираются случайным образом из большого по объему словаря. Парольная фраза может содержать 3 или 4 слова, при желании пароль может быть создан из двух парольных фраз.

Чтобы получить пароль из парольной фразы, достаточно набрать без пробелов в раскладке латиницей первые X букв из каждого слова парольной фразы, содержащей Y слов. Пользователь сам задает параметры X и Y, а также язык парольной фразы.

Например, при использовании трех первых букв из каждого слова парольной фразы «Затейливый ювелир утащил сдобу» получим пароль «pfn.dtenfclj».

### ПК ViPNet StateWatcher

Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher, который предназначен для наблюдения за состоянием узлов сетей ViPNet, мониторинга событий безопасности, происходящих на сетевых узлах, своевременного выявления неполадок в работе узлов и оперативного оповещения пользователей о возникающих проблемах.

### Политика безопасности

Набор параметров, регулирующих безопасность сетевого узла. В технологии ViPNet безопасность сетевых узлов обеспечивается с помощью сетевых фильтров и правил трансляции IP-адресов.

### Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

### Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ или ViPNet Network Manager создает для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

### Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

### Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервером соединений для клиента назначен сервер IP-адресов.

### Сертификат ключа проверки электронной подписи

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

### Сетевой узел ViPNet

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

### Сеть ViPNet

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

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

### Список аннулированных сертификатов (CRL)

Список сертификатов, которые были аннулированы или приостановлены администратором удостоверяющего центра и недействительны на момент, указанный в данном списке аннулированных сертификатов.

### Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в управляющих приложениях ViPNet, предназначенных для создания структуры и конфигурирования сети ViPNet (ViPNet Центр управления сетью, ViPNet Network Manager).

### Структура сети ViPNet

Упорядоченная совокупность связей между компонентами сети ViPNet, такими как:

- рабочее место администратора сети ViPNet;
- координаторы;
- клиенты.

Каждый клиент должен быть зарегистрирован на координаторе. Связи между координаторами и рабочим местом администратора, а также между координатором и его клиентами обязательны. Остальные связи создаются в соответствии с корпоративной политикой безопасности.

### Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

### Туннелирование

Технология, позволяющая защитить соединение с участием открытых узлов при передаче данных через Интернет и другие публичные сети. Туннелирование заключается в шифровании трафика открытых узлов координаторами.

### Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

### Файл контейнера

Специальный файл, в котором хранится защищенная информация. Этот файл подключается в качестве нового логического диска в вашей операционной системе. Вы можете работать с этим диском, как с обычным диском Windows: перетаскивать, копировать, вставлять, удалять файлы и так далее.

Файл контейнера имеет расширение `*.sdc` и по умолчанию является скрытым. Чтобы увидеть этот файл, на **Панели управления** откройте **Свойства папки**, на вкладке **Вид** включите опцию **Показывать скрытые файлы и папки**.

### Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

### Частный адрес

Для сетей на базе протокола IP, не требующих непосредственного подключения к Интернету, выделено три диапазона IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255, которые никогда не используются в Интернете. Чтобы выйти в Интернет с адресом из такого диапазона, необходимо использовать межсетевой экран с функцией NAT или технологию прокси.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

### Электронная подпись

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

# Указатель


## D

DNS - 101, 107, 111, 115, 116, 118, 120

## E

eToken Aladdin - 345

## I

iButton - 345

## R

ruToken - 345

## S

Shipka - 345
Smartcard - 345

## V

ViPNet-драйвер - 15, 16, 18, 96, 129, 333, 351

## W

WINS - 111, 115, 116, 118, 120

## А

Администратор сети ViPNet - 41, 65
Администратор узла ViPNet - 78, 219, 220, 224, 226, 227, 283, 287
Асимметричный ключ - 304, 325

## В

Виртуальный адрес - 78, 96, 107, 111

## Д

Дистрибутив ключей - 58, 65, 323, 398

## Ж

Журнал IP-пакетов - 16, 78, 193, 198, 200, 333
Журнал событий - 227

## З

Защищенная сеть - 78, 129
Защищенный трафик - 127, 129, 193

## К

Клиент - 47, 107, 208, 399
Компрометация ключей - 58, 65
Конференция - 174
Конфигурация программы - 78, 206, 208, 228
КриптоПро - 351

## О

Обмен защищенными сообщениями - 171
Обновление ПО ViPNet - 40, 41, 42
Обновление сертификата - 61, 293, 294, 399
Обновление справочников и ключей - 58, 61, 96, 228, 323, 325
Открытая сеть - 78, 129
Открытый Интернет - 208, 400
Открытый трафик - 127, 129, 193

## П

Папка ключей - 47
Прикладной протокол - 156, 157

## С

Сетевой узел ViPNet - 78, 96, 109
Сетевой фильтр - 129, 144, 151
Сетевой экран (Firewall) - 126
Симметричный ключ - 239, 303, 323
Способ аутентификации - 70, 226
Справочники и ключи - 47, 51, 58, 61, 64, 76, 226, 302, 403
Статистика IP-пакетов - 78, 204
Статус сетевого узла - 78, 188

## Т

Терминальный сервер - 213
Трансляция адресов - 328, 403
Туннелирование - 96, 123, 403
Туннелируемый адрес - 96, 107, 123, 328
Туннелируемый узел - 96, 107, 115, 121, 123, 333, 403

## У

Удаленное управление сетевым узлом ViPNet - 185, 211

## Ф

Файловый обмен - 78, 179
Фильтр протокола - 129