Приложение 1
к приказу ГБУ ДПО РЦОКИО
от 25.05.2017 № 817-08

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по обеспечению информационной безопасности с использованием средств криптографической защиты информации в образовательных организациях

1. Общие положения

1.1. Настоящий документ определяет состав и содержание организационных и технических мер по обеспечению безопасности конфиденциальной информации при её обработке в информационных системах с использованием средств криптографической защиты информации (далее - СКЗИ).

1.2. Настоящий документ разработан во исполнение следующих нормативных правовых актов Российской Федерации:

- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. N 66 г. Москва «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.3. Настоящий документ рекомендуем к исполнению в образовательных организациях и органах местного самоуправления, осуществляющих управление в сфере образования, использующих СКЗИ для обеспечения безопасности персональных данных при их обработке в информационных системах.

1.4. Эксплуатация СКЗИ должна осуществляться в соответствии с документацией на СКЗИ, требованиями, установленными в нормативных правовых актах Российской Федерации, регулирующими отношения в соответствующей области, и настоящими методическими рекомендациями.

2. Термины и определения

2.1. Информация - сведения (сообщения, данные) независимо от формы их представления;

2.2. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

2.3. Доступ к информации - возможность получения информации и её использования;

2.4. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

2.5. Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

2.6. Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

2.7. Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

2.8. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

2.9. Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

2.10. Средства криптографической защиты информации (СКЗИ) – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

3. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

3.1. Оператор информационной системы при работе с конфиденциальной информацией обязан использовать средства криптографической защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

3.2. К работе с СКЗИ допускаются только работники согласно перечню пользователей СКЗИ, утвержденному соответствующим обладателем конфиденциальной информации.

Пользователи СКЗИ допускаются к работе только после проведения соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют организации, имеющие лицензию ФСБ России на право осуществлять деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение об уровне подготовки пользователя СКЗИ, составленное сотрудником компании, обладающей лицензией ФСБ России.

3.3. Пользователи СКЗИ обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены, рубежи её защиты, в том числе сведения о криптоключах;
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать ответственному за обеспечение безопасности информации о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять ответственного за обеспечение безопасности информации о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

3.4. Оператор информационной системы при работе с конфиденциальной информацией обязан разработать и утвердить инструкцию пользователя СКЗИ, а так же ознакомить пользователей СКЗИ с настоящей инструкцией. Подтверждением ознакомления пользователей с инструкцией пользователя СКЗИ является лист ознакомления.

4. Порядок обращения с СКЗИ и криптоключами к ним. Мероприятия при компрометации криптоключей.

4.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в журнале учета средств криптографической защиты информации, эксплуатационной и технической документация к ним.

4.2. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования (CD/DVD диск, USB-носитель и т.д.).

4.3. Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

4.4. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующих журналах поэкземплярного учета.

4.5. Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

4.6. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования)

СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

4.7. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или пользователем СКЗИ, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

4.8. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

4.9. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от органа криптографической защиты или изготовителя.

4.10. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению издателю или по его указанию должны быть уничтожены на месте.

4.11. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (CD/DVD диск, USB-носитель и т.д.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к

соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

4.12. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают в соответствующий орган криптографической защиты.

4.13. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать в соответствующий орган криптографической защиты. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

4.14. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации.

5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.

5.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов.

5.2. Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ.

Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время.

Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

5.3. Размещение, специальное оборудование, охрана и организация режима в спецпомещениях органов криптографической защиты должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

5.4. Двери спецпомещений органов криптографической защиты должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам органов криптографической защиты под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких спецпомещений следует хранить в сейфе руководителя организации обладателя конфиденциальной информации. Хранение дубликатов ключей вне помещений организации обладателя конфиденциальной информации не допускается.

5.5. Для предотвращения просмотра извне спецпомещений органов криптографической защиты их окна должны быть защищены.

5.6. Каждый орган криптографической защиты для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должен иметь необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе руководителя организации обладателя конфиденциальной информации.

5.7. Дубликат ключа от хранилища руководителя организации обладателя конфиденциальной информации в опечатанной упаковке должен быть передан на хранение должностному лицу, под расписку в соответствующем журнале.

5.8. При утрате ключа от хранилища или от входной двери в спецпомещение организации обладателя конфиденциальной информации замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает руководитель организации обладателя конфиденциальной информации.

5.9. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

5.10. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено

от линии связи и убрано в опечатываемые хранилища. В противном случае пользователи СКЗИ по согласованию с органом криптографической защиты обязаны предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

5.11. Режим охраны спецпомещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации.

Приложение №1
к методической рекомендации
по обеспечению информационной безопасности с использованием средств криптографической защиты информации в образовательных организациях

Инструкция по использованию ViPNet Client 4.x

1. О программе

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

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

1.3. 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.

1.4. ViPNet-драйвер — 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.

1.5. Основной функцией программы ViPNet Монитор является настройка различных параметров ViPNet-драйвера и запись событий, возникающих в процессе обработки трафика драйвером, в журнал регистрации IP-пакетов. 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.

На компьютере программа ViPNet Монитор:

– Позволяет настраивать параметры встроенного сетевого экрана.
– Позволяет управлять параметрами обработки прикладных протоколов.
– Предоставляет встроенные функции для защищенного обмена сообщениями, проведения конференций, файлового обмена и так далее.

1.6. На клиентском узле транспортный модуль ViPNet MFTP обеспечивает обмен управляющими конвертами, конвертами программы ViPNet Деловая почта и файлами с другими сетевыми узлами ViPNet.

1.7. 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.

1.8. 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).

1.9. 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.

1.10. 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.

1.11. 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.

2. Системные требования

2.1. 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.

3. Запуск программы ViPNet Монитор

3.1. 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.

3.2. Перед окончанием загрузки Windows появится окно входа в программу ViPNet Монитор. Для запуска программы введите пароль (см. Рисунок 1).

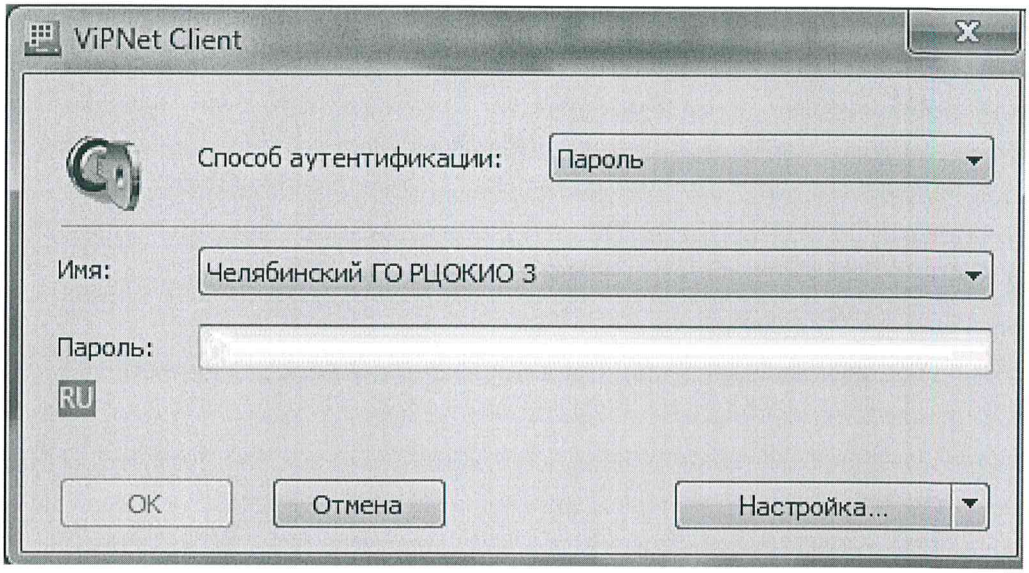

Рисунок 1. Окно входа в программу

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

3.4. Если вы вышли из программы или отказались от аутентификации при загрузке Windows, то для запуска программы ViPNet Монитор:

– При использовании Windows 7 или более ранней версии, откройте Пуск > Все программы > ViPNet > ViPNet Client > Монитор

– Если вы используете ОС Windows 8 на начальном экране откройте список приложений и выберите ViPNet > Монитор

– Если на рабочем столе есть ярлык ViPNet Монитор, то необходимо дважды щелкнуть ярлык программы (см. Рисунок 2).

Рисунок 2. Ярлык ViPNet Монитор

3.5. Откроется окно входа в программу (см. Рисунок 1.);

3.6. Если на вашем компьютере работает несколько пользователей ViPNet Client выберите нужного пользователя (см. Рисунок 3).

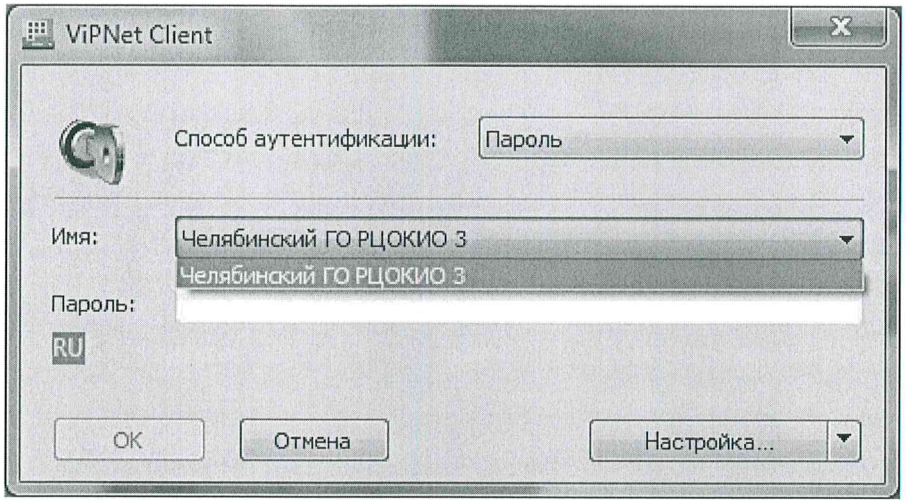

Рисунок 3. Окно выбора пользователя ViPNet Client

3.7. Выберите способ аутентификации – пароль (см. Рисунок 4).

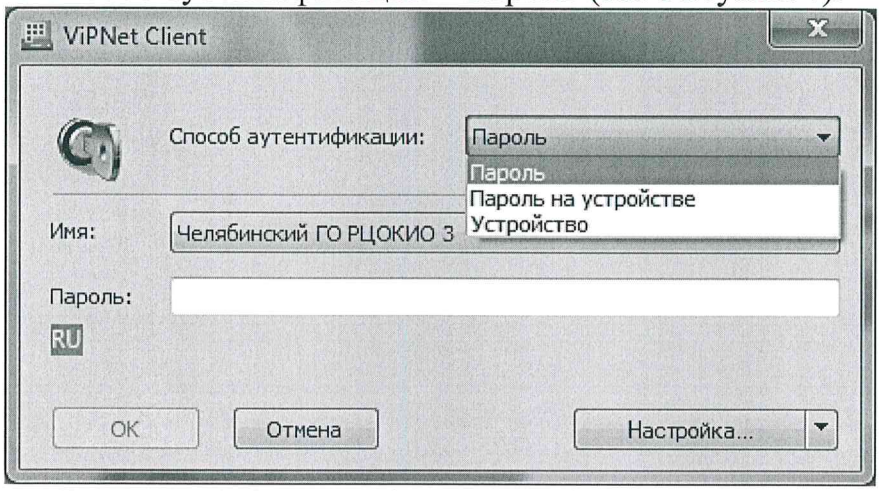

Рисунок 4. Окно выбора способа аутентификации

3.8. После удачного ввода пароля вас встретит окно программы ViPNet Монитор.

4. Интерфейс программы ViPNet Монитор

4.1. Окно программы ViPNet Монитор представлено на Рисунке 5.

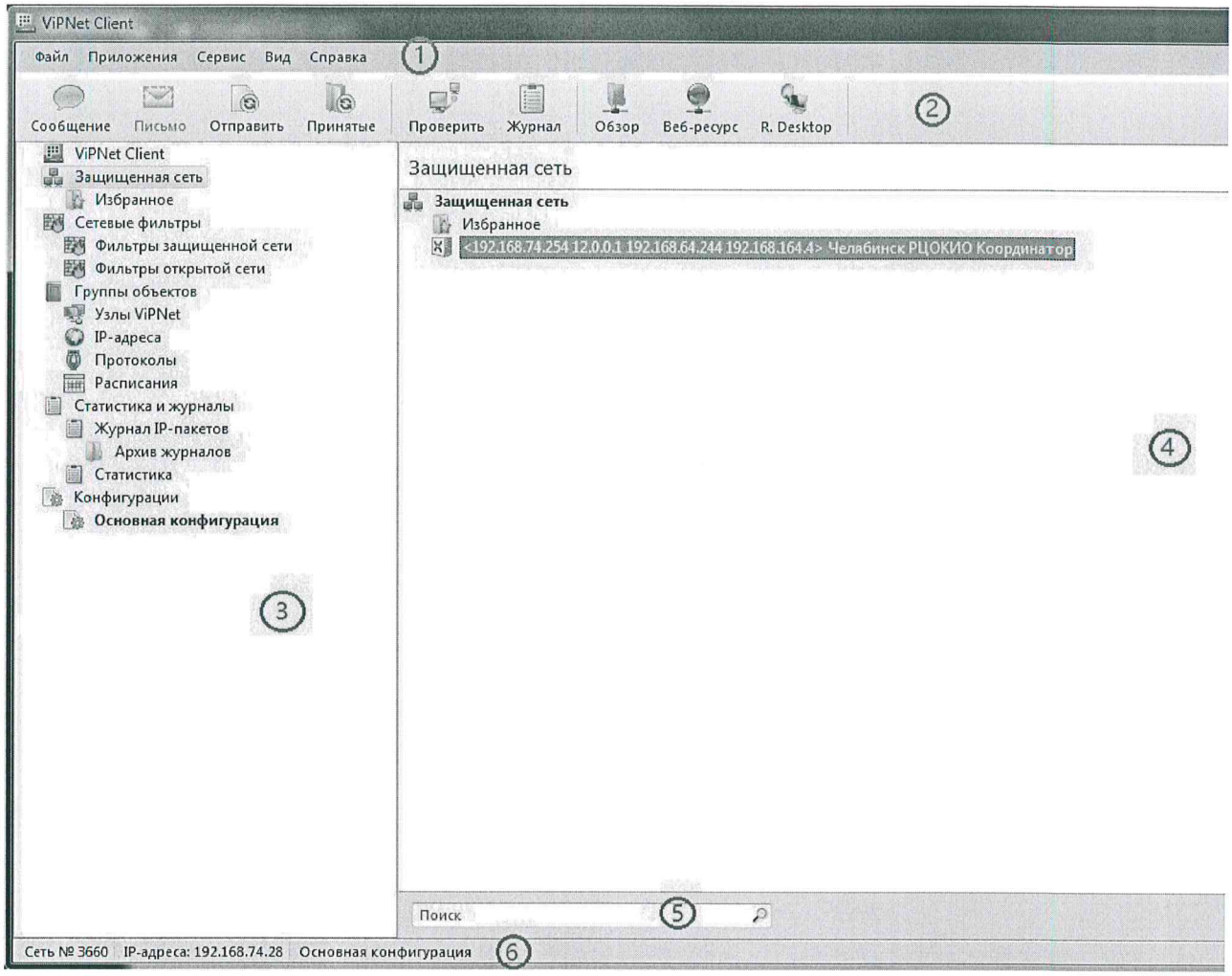

Рисунок 5. Окно программы ViPNet Монитор

4.2. Цифрами на Рисунке 5 обозначено:

1. Меню программы
2. Панель инструментов.
3. Панель навигации. Содержит перечень разделов, предназначенных для настройки различных параметров ViPNet Монитор:
   - Защищенная сеть - содержит список сетевых узлов ViPNet, которые связаны друг с другом посредством ViPNet Центр управления сетью
   - Сетевые фильтры:
     - Фильтр защищенной сети
     - Фильтр открытой сети
   - Группы объектов – содержит списки объектов, которые могут быть использованы при создании сетевых фильтров.
   - Статистика и журналы:
     - Журнал IP-пакетов предназначен для поиска записей в журнале IP-пакетов.
     - Статистика – предназначена для статистики IP – пакетов
   - Конфигурации – предназначен для управления конфигурации программы ViPNet Монитор

- Администратор – служит для настройки дополнительных параметров и отображается только после входа в режим администратора.

4. Панель просмотра.
5. Строка поиска. Поиск можно проводить по следующим параметрам:
   - Имя узла сети.
   - Имя компьютера.
   - Псевдоним.
   - Реальные и виртуальные IP-адреса.
   - DNS – имя.
   - Идентификатор узла.
6. Строка состояния. Содержит номер сети ViPNet, IP-адреса, назначенные узлу и текущую конфигурацию программы.

4.3. Для того чтобы посмотреть информацию о данном узле связи необходимо в панели навигации выбрать вкладку ViPNet Client (см. Рисунок 6).

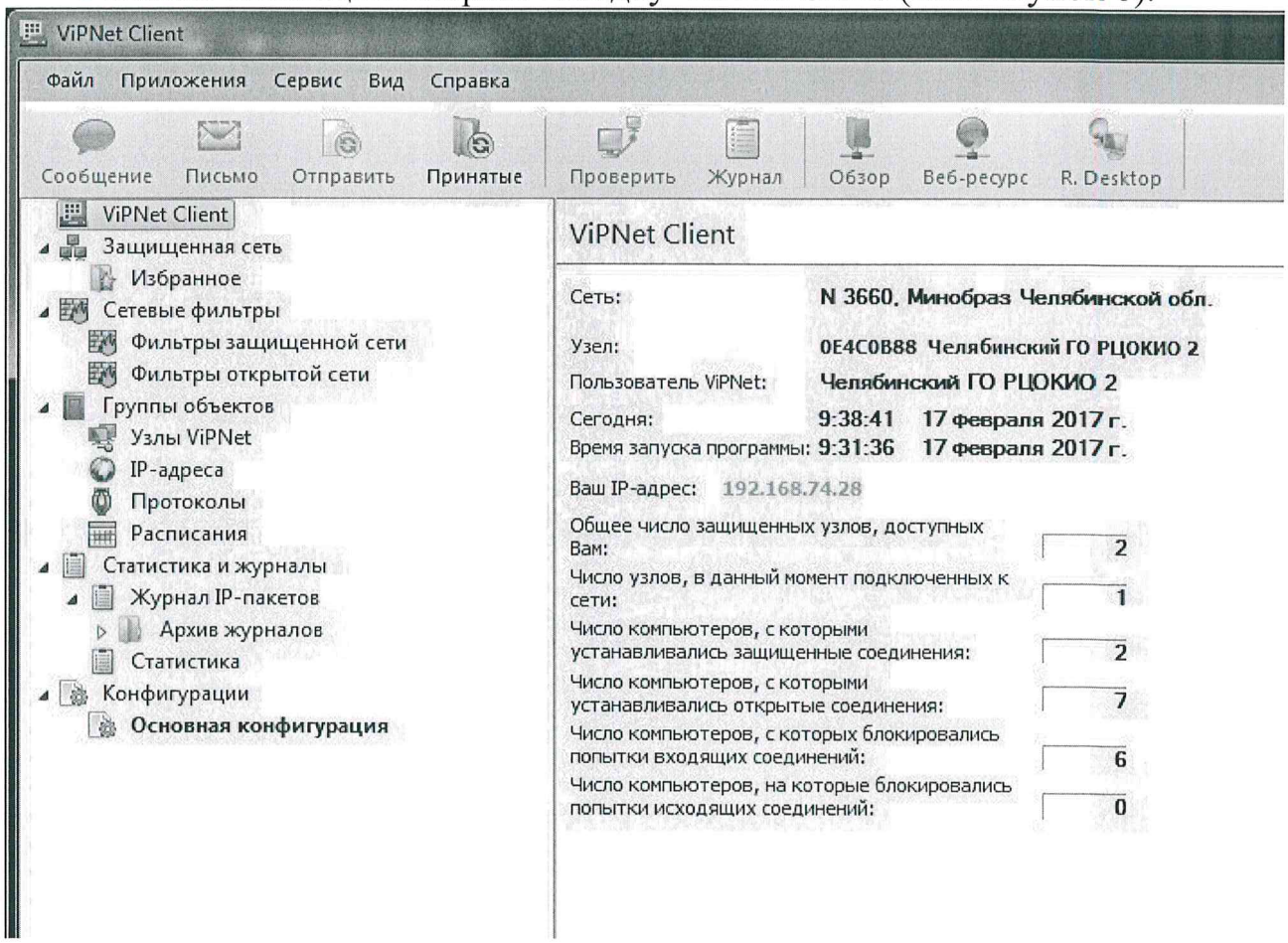

Рисунок 6. Информация о УС ViPNet Client.

4.4. Раздел Защищенная сеть содержит список защищенных узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью (см. Рисунок 7).

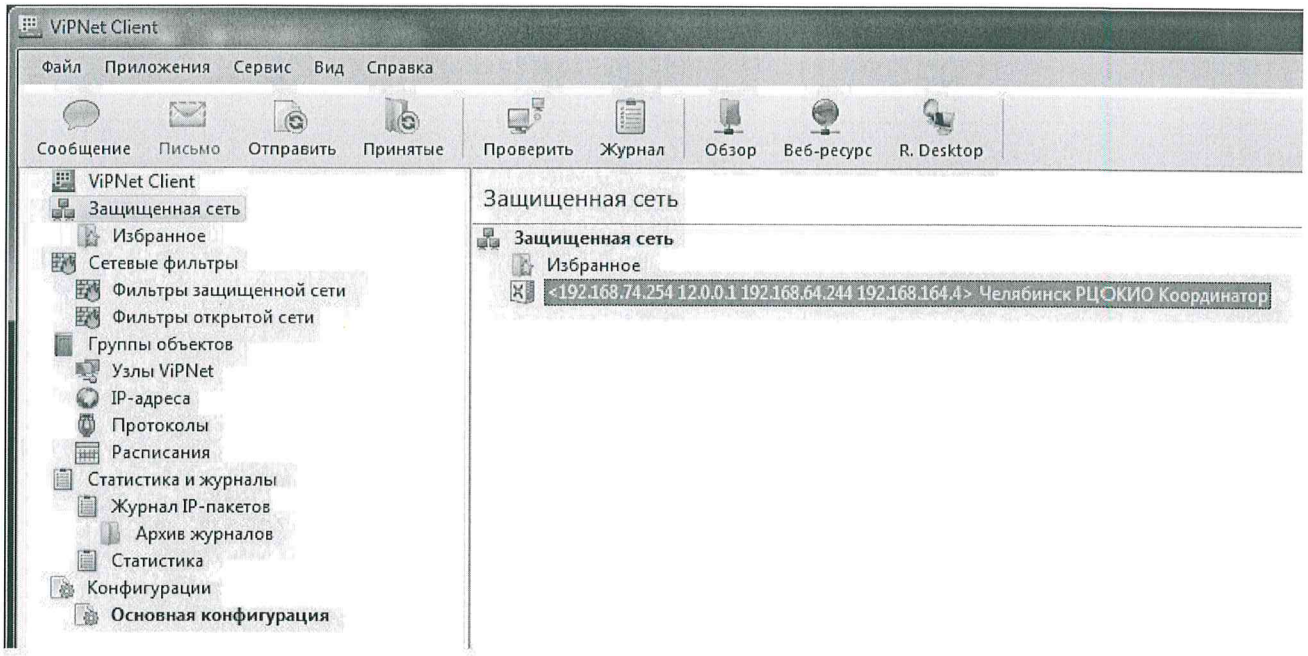

Рисунок 7. Проверка связи с координатором

4.5. Значок рядом с именем сетевого узла, а также цвет имени обозначают тип сетевого узла и его текущий статус (см. Рисунок 8).

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

Рисунок 8. Обозначение статуса сетевых узлов

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

1) 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.
2) Новая папка появится на панели навигации, а также в разделе Защищенная сеть.

3) Чтобы перенести сетевые узлы в какую-либо папку, в разделе Защищенная сеть выберите один или несколько сетевых узлов и перетащите их в нужную папку.
4) Чтобы переименовать папку, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт Переименовать.
5) 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.

4.7. Чтобы проверить соединение с другим узлом, начать сеанс обмена защищенными сообщениями, отправить файл или использовать другие встроенные функции программы ViPNet Монитор выполните одно из действий:

– выберите сетевой узел в списке и нажмите соответствующую кнопку на панели инструментов;
– выберите соответствующий пункт в контекстном меню сетевого узла.

4.8. Для проверки связи с координатором необходимо в панели навигации выбрать защищенную сеть, далее выбрать «Челябинск РЦОКИО Координатор» и в панели инструментов нажать «Проверить» (см. Рисунок 7).

4.9. После нажатия кнопки «Проверить» откроется новое окно «Проверка соединения». Столбец «Статус» может иметь одно из двух значений: «Доступен» или «Недоступен». Статус «Доступен» свидетельствует о функционировании защищенной сети (см. Рисунок 9).

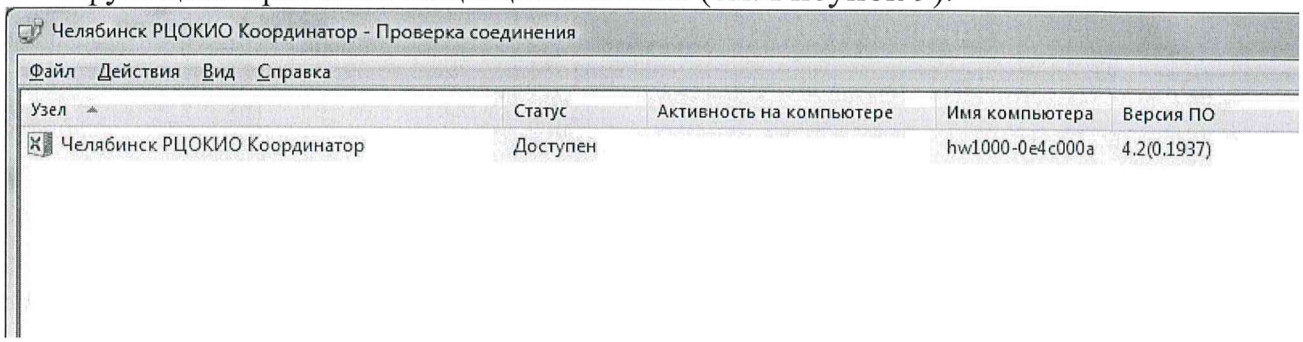

Рисунок 9. Проверка соединения

4.10. Если статус имеет значение «Недоступен» необходимо выполнить следующие действия:

– Проверить наличие подключение к сети Интернет.

– Проверить точное время и часовой пояс сети. Часовой пояс должен быть (UTC+05:00) Екатеринбург.
–

5. Завершение работы программы ViPNet Монитор.

5.1. 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.
2) Чтобы снова развернуть окно программы, щелкните значок программы ViPNet Монитор в области уведомлений на панели задач.
3) 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.

6. Возможные неполадки и способы их устранения

6.1. В случаи если при включении программы ViPNet Client на рабочей станции перестаёт корректно функционировать подключение к сети интернет необходимо:
– Добавить фильтр открытой сети (см. Рисунок 10)

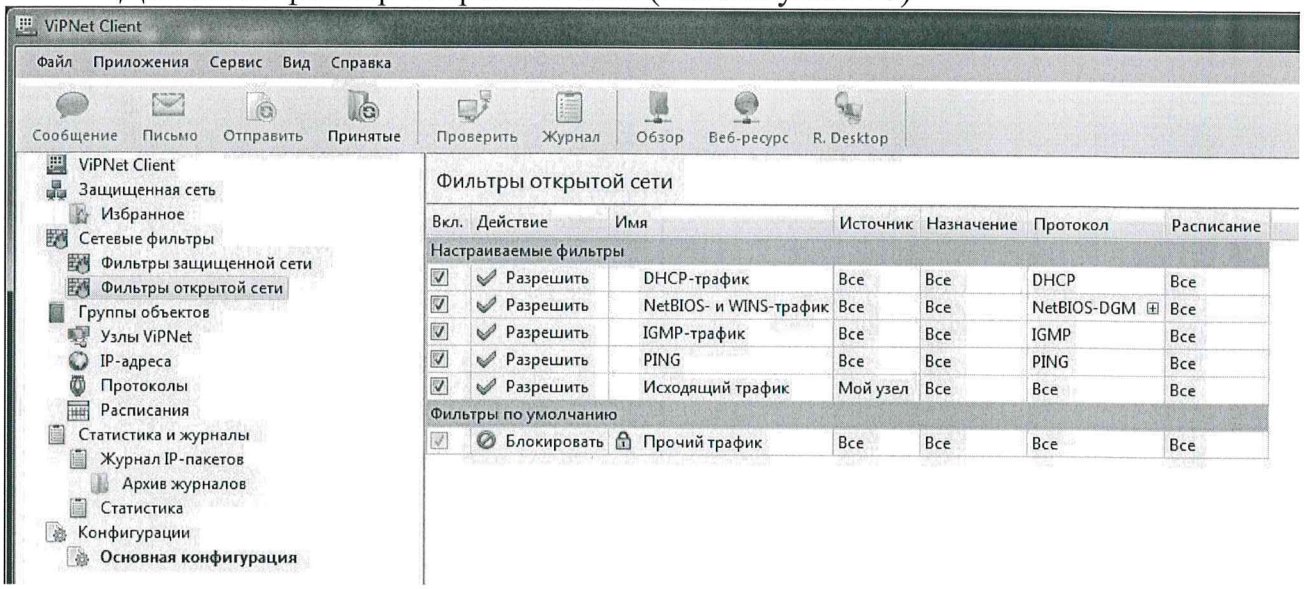

Рисунок 10. Фильтры открытой сети

– Для того чтобы добавить фильтр необходимо щелкнуть правой кнопкой мыши по любому существующему фильтру. В открывшемся контекстном меню выбрать пункт «Добавить».
– В открывшемся окне «Свойства фильтра» необходимо поменять наименование, а также установить в строке «Действие» значение

«Пропускать трафик» (см. Рисунок 11). Сохранить изменения нажав кнопку «Ок».

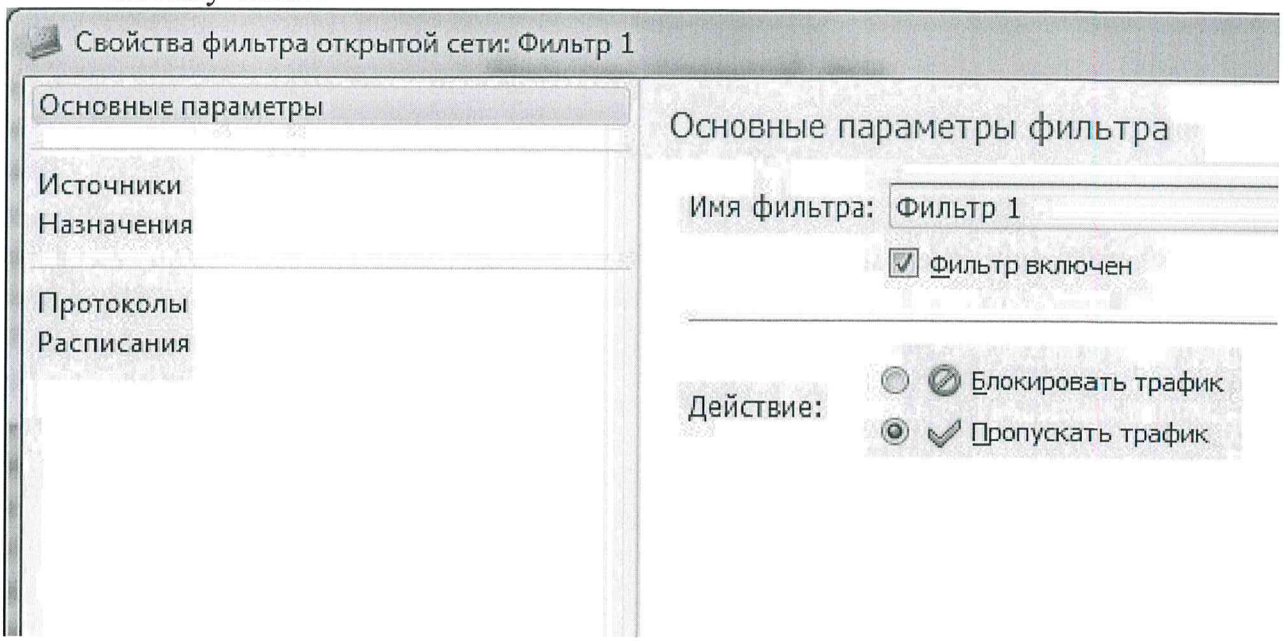

Рисунок 11. Создание нового фильтра открытой сети

– После добавления фильтра необходимо его применить. Чтобы применить фильтр необходимо в правом нижнем углу нажать кнопку «Применить».

6.2. В случаи если при запуске программы ViPNet Монитор появляется сообщение «Истек срок действия аннулированных сертификатов» необходимо:

– В меню программы ViPNet Монитор выбрать Сервис > Настройка параметров безопасности (см. Рисунок 12).

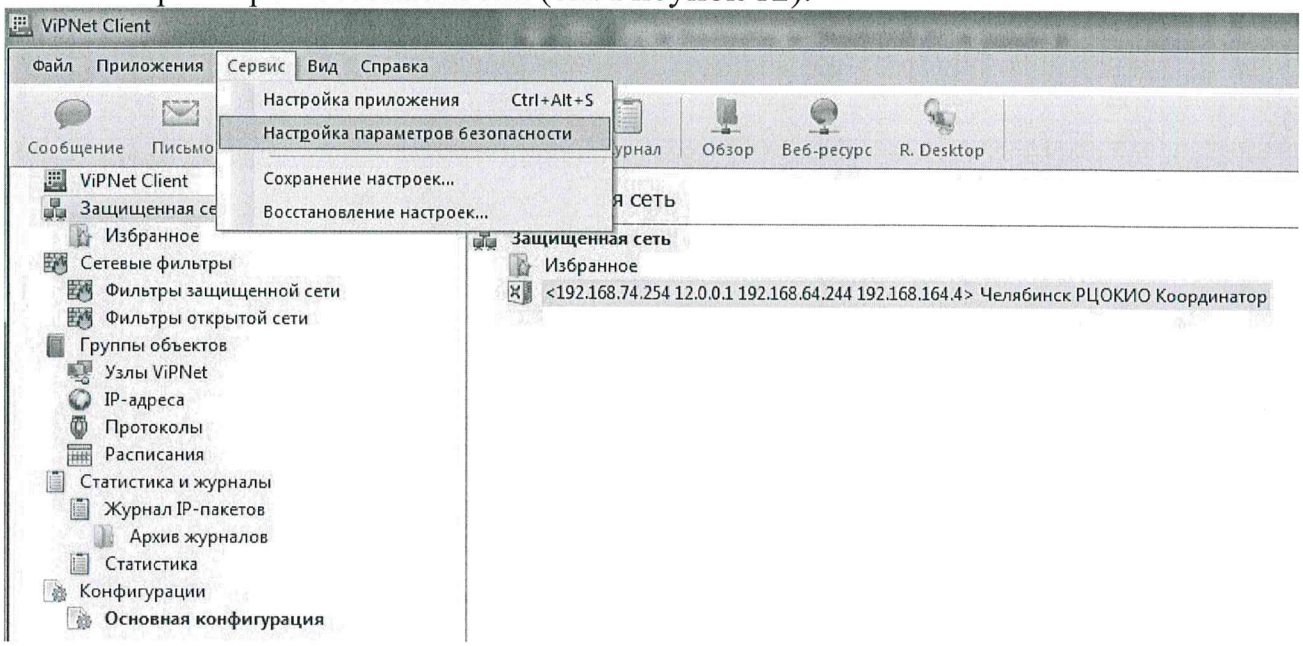

Рисунок 12. Настройка параметров безопасности

– В открывшемся окне «Настройка параметров безопасности» выбрать вкладку Электронная подпись. Статус должен иметь значение «действителен» (см. Рисунок 13).

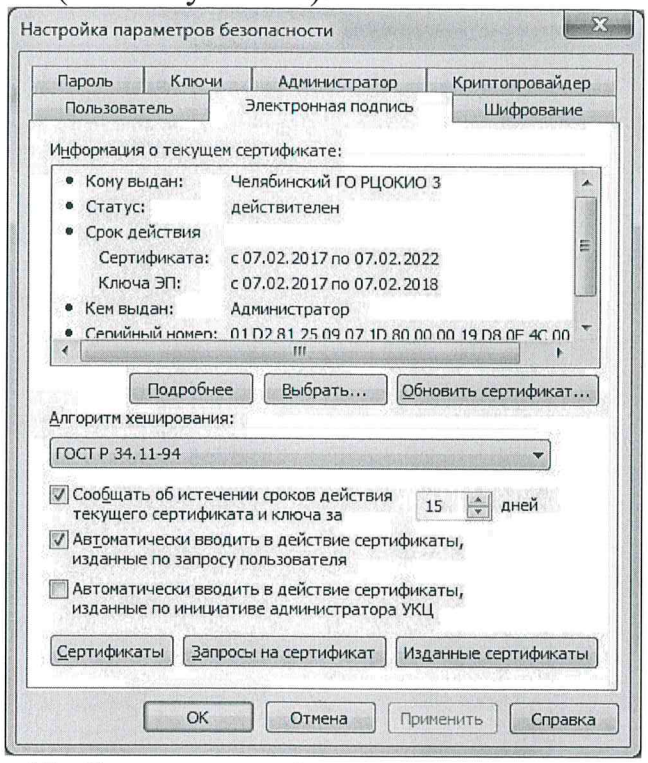

Рисунок 13. Статус сертификата электронной подписи.

– Если статус имеет значение «недействителен» необходимо проверить выбран ли действующий сертификат электронной подписи нажав на кнопку «Выбрать». Далее необходимо выбрать последний изданный сертификат электронной подписи. После выбора актуального сертификата необходимо сохранить изменения нажав кнопку «Ок» (см. Рисунок 14).

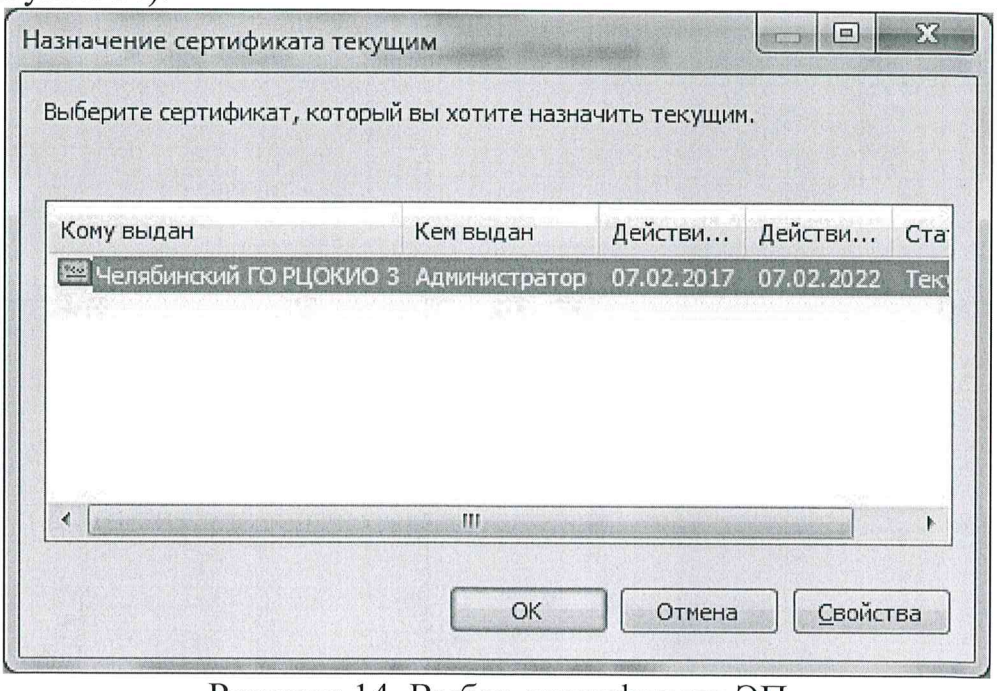

Рисунок 14. Выбор сертификата ЭП

– Если все вышеупомянутые действия не помогли, нужно принудительно получить обновления сети ViPNet. Для этого необходимо:
  1) В меню программы выбрать вкладку Приложения > Транспортный модуль (см. Рисунок 15).

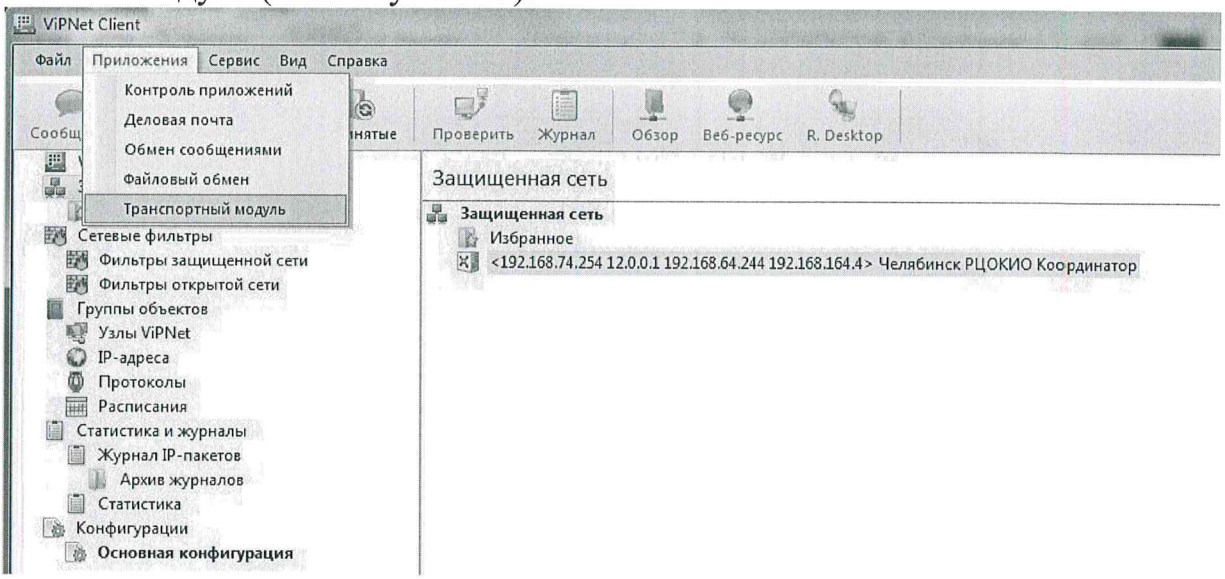

Рисунок 15. Транспортный модуль

  2) В появившемся окне необходимо нажать кнопку «Опросить». После того как обновления придут, программа автоматически перезапуститься и обновления вступят в силу.

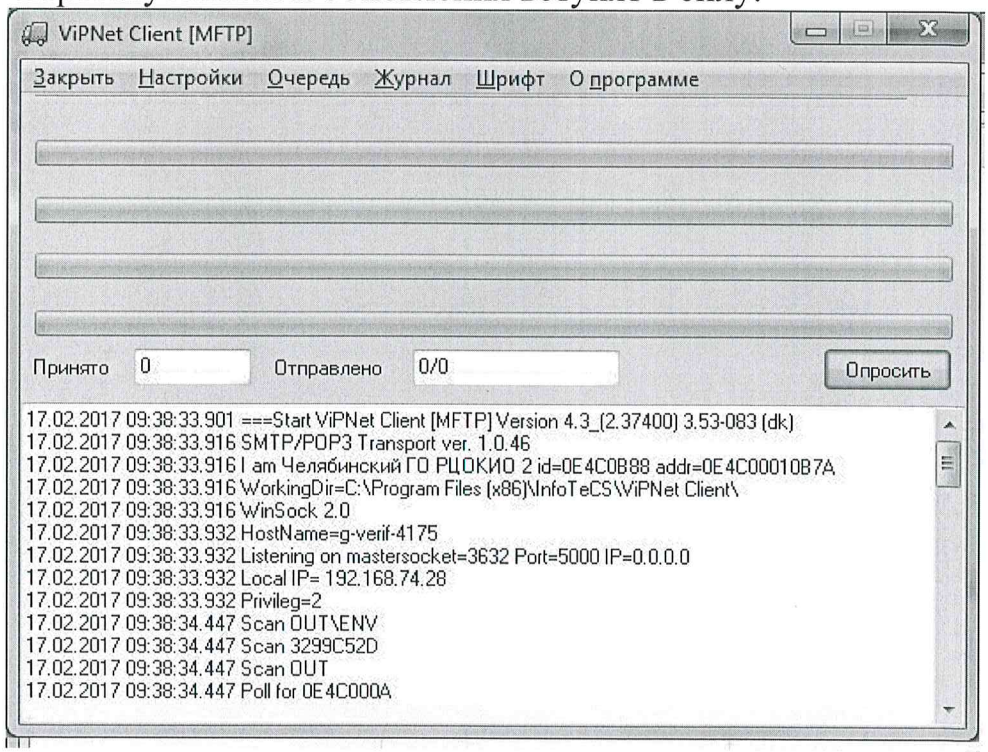

Рисунок 16. Получение обновлений сети ViPNet.

– Если указанные выше действия не устранили проблему сос списком аннулированных сертификатов необходимо связаться с Администратором сети.

Приложение №1
к методической рекомендации
по обеспечению информационной безопасности с использованием средств криптографической защиты информации в образовательных организациях

Инструкция по использованию программного обеспечения «Деловая почта»

1. О программе

1.1. Программа ViPNet Деловая почта предназначена для обмена электронными письмами в защищенной сети. Этой возможностью могут воспользоваться только те пользователи сети ViPNet, у которых есть связь друг с другом.
Программа ViPNet Деловая почта входит в состав программного обеспечения ViPNet Client и может быть установлена на компьютер вместе с другими компонентами данного программного обеспечения или отдельно.

1.2. Программа ViPNet Деловая почта обладает стандартными функциями почтового клиента:
- Отправка и прием писем.
- Отправка и прием вложенных в письма файлов.
- Подписание писем и вложений электронной подписью.
- Шифрование файлов вложений.

1.3. Программа ViPNet Деловая почта также имеет ряд особенностей:
- Доступ к программе на сетевом узле ViPNet имеет только пользователь этого сетевого узла.
- Письма программы ViPNet Деловая почта передаются по защищенным каналам в сети ViPNet с помощью транспортного модуля MFTP.
- Письма программы ViPNet Деловая почта зашифрованы на ключах адресата и не могут быть прочитаны кем-либо другим.
- Программа ViPNet Деловая почта имеет мощную систему автоматической обработки входящих писем и исходящих файлов.

2. Системные требования

2.1. Требования к компьютеру для установки программы ViPNet Деловая почта:
- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.

- Объем оперативной памяти — не менее 512 Мбайт.
- Свободное место на жестком диске — не менее 150 Мбайт (рекомендуется 250 Мбайт).
- Сетевой адаптер или модем.
- Операционная система — Windows Vista (32/64-разрядная), Windows Server 2008 (32/64- разрядная), Windows Server 2008 R2 (64-разрядная), Windows Small Business Server 2008 SP2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Windows 8.1 (32/64-разрядная), Windows Small Business Server 2011 (64-разрядная), Windows Server 2012 (64- разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная). Для операционной системы должен быть установлен самый последний пакет обновлений.
- При использовании Internet Explorer — версия 6.0 или выше.

3. Запуск и завершение работы с программой

3.1. Чтобы запустить программу ViPNet Деловая почта, выполните следующие действия:

- Для запуска программы ViPNet Деловая почта используйте один из следующих способов:

1) Если запущена программа ViPNet Монитор, в окне программы в меню Приложения выберите пункт Деловая почта. Немедленно будет открыто окно программы ViPNet Деловая почта. Аутентификация пользователя в этом случае не требуется.
2) Если через транспортный модуль MFTP будут получены новые письма, программа ViPNet Деловая почта будет запущена автоматически. При этом откроется окно входа в программу ViPNet Деловая почта. Если же до этого уже была выполнена аутентификация в программе ViPNet Монитор, то откроется главное окно программы ViPNet Деловая почта.
3) Чтобы запустить программу ViPNet Деловая почта с помощью ярлыка, 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 > Деловая почта.
   - Если вы используете операционную систему Windows 8 или Windows Server 2012, на начальном экране откройте список приложений и выберите ViPNet > Деловая почта.
   - Дважды щелкните ярлык, откроется окно входа в программу (см. Рисунок 1).

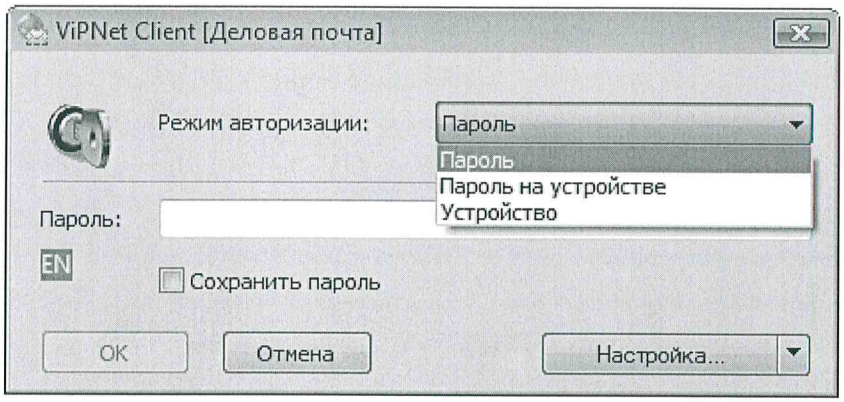

Рисунок 1. Окно входа в программу.

4) Введите пароль и нажмите кнопку «Ок». Пароль для аутентификации в программе Деловая почта аналогичен паролю программы Монитор.

3.2. Чтобы завершить работу с программой, выполните одно из действий:

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

4. Интерфейс программы

4.1. Внешний вид окна программы ViPNet Деловая почта представлен на Рисунке 2.

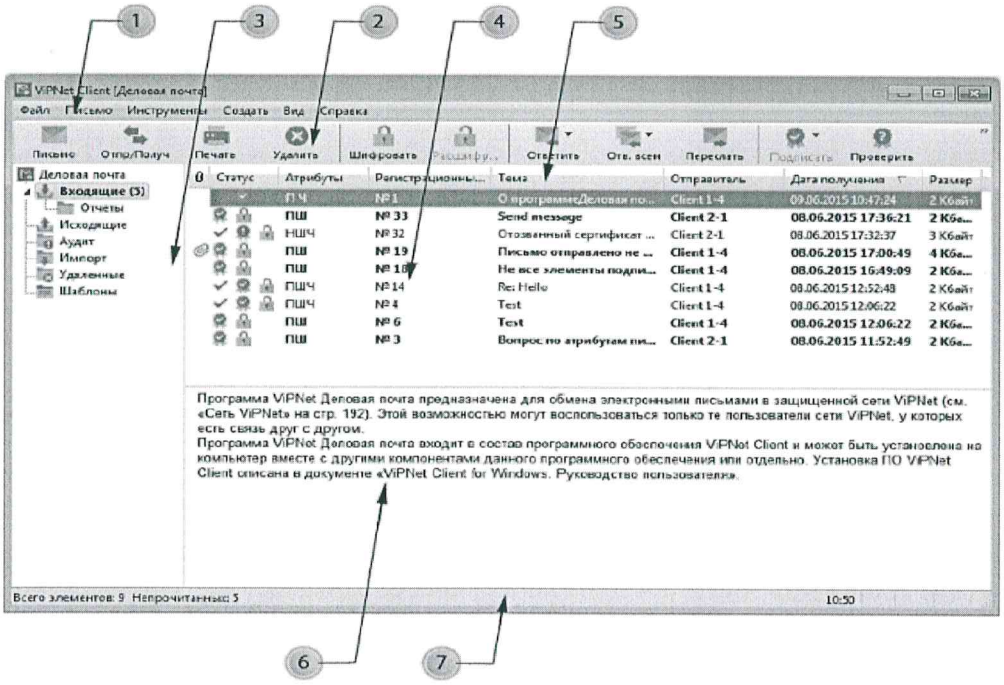

Рисунок 2. Интерфейс программы ViPNet Деловая почта

4.2. Цифрами на рисунке обозначены:

1) Главное меню программы.

2) Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню Вид выберите пункт Панель инструментов, затем щелкните Настройка.
3) Панель папок. На этой панели отображается иерархическая структура папок программы ViPNet Деловая почта. Если в папке есть непрочитанные письма, имя папки выделено полужирным шрифтом, а количество непрочитанных писем указано после имени папки в скобках. Если папка содержит вложенные папки, в которых есть непрочитанные письма, в скобках указаны два числа: количество непрочитанных писем в папке и суммарное количество непрочитанных писем во вложенных папках.
4) Панель писем. На этой панели отображается список писем, находящихся в выбранной на панели (3) папке. Чтобы просмотреть список находящихся в папке писем в формате HTML, на панели писем щелкните правой кнопкой мыши заголовок какого-либо столбца и в контекстном меню выберите пункт Просмотр в HTML-формате.
5) Столбцы панели писем (4). Чтобы отсортировать список писем по одному из столбцов, щелкните заголовок столбца. С помощью контекстного меню можно удалить или добавить столбцы. В столбце Статус отображаются значки, которые обозначают статус письма. В столбце Атрибут отображаются коды статуса письма. Описание значков и кодов статуса представлено на Рисунке 3.

Значок	Атрибут	Статус
	Ш	Письмо и все вложения зашифрованы
	П	Все элементы письма (текст и вложения) подписаны и все подписи верны
	п	Не все элементы письма подписаны, но все имеющиеся подписи верны
	Н	Все элементы письма подписаны и хотя бы одна подпись неверна
	н	Не все элементы письма подписаны и хотя бы одна подпись неверна
	У	Письмо упаковано для всех выбранных получателей, но еще не отправлено
	у	Письмо упаковано для некоторых получателей (не для всех), но еще не отправлено
	О	Письмо отправлено всем получателям, но еще не доставлено
	о	Письмо отправлено некоторым (не всем) получателям, но еще не доставлено
	Д	Письмо доставлено всем получателям, но еще не прочитано
	д	Письмо доставлено некоторым получателям, но еще не всем
	Ч	В папке **Исходящие**: письмо прочитано всеми получателями. В папке **Входящие**: текст письма и все вложения прочитаны.
	ч	В папке **Исходящие**: письмо прочитано некоторыми получателями, но еще не всеми. В папке **Входящие**: текст письма прочитан, но не все вложения прочитаны.
	!	Письмо не может быть отправлено получателю. Такая ситуация может возникнуть в случае, если клиент, на который отправлено письмо, отключен от координатора или удален из сети.

Рисунок 3. Статусы писем

6) Панель чтения. На этой панели отображается текст письма, выбранного на панели (4).
7) Строка состояния. В строке состояния указано общее количество писем в выбранной папке и ее подпапках, а также количество непрочитанных (в папке Входящие) или недоставленных (в папке Исходящие) писем. Количество писем определенного типа отображается в виде суммы двух чисел: количество писем данного типа в выбранной папке и суммарное количество писем данного типа во вложенных папках.

5. Основные операции с программой

5.1. Создание писем. Чтобы написать письмо, выполните следующие действия:

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

5.2. Подписание писем электронной подписью. Чтобы подписать письмо электронной подписью, выполните следующие действия:

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

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

Чтобы прочитать письмо:

- В окне программы ViPNet Деловая почта на левой панели выберите папку, в которой находится письмо.
- Выберите письмо в списке. Если письмо не зашифровано, его текст отобразится в поле под списком писем. Если письмо зашифровано, для его просмотра выполните одно из действий:
  1) Нажмите кнопку **Расшифровать**  на панели инструментов.
  2) Откройте письмо в отдельном окне двойным щелчком.

5.4. Ответ на письмо. Чтобы ответить на письмо, выполните следующие действия:

- Выберите письмо в списке или откройте в отдельном окне двойным щелчком.
- В окне программы ViPNet Деловая почта или в окне просмотра письма на панели инструментов нажмите кнопку **Ответить**  или **Ответить всем**  . Откроется окно создания письма.
- Напишите и отправьте письмо.

5.5. Удаление писем. Чтобы удалить письмо, выполните следующие действия:

- В окне программы ViPNet Деловая почта на левой панели выберите папку с письмом, которое нужно удалить.
- В списке выберите письмо и нажмите кнопку **Удалить**  на панели инструментов или нажмите клавишу **Delete**.
  Письмо будут перемещено в папку **Удаленные**, в подпапку с именем, которое совпадает с именем исходной папки письма.

6. Возможные неполадки и способы их устранения

6.1. Письмо упаковано, но не отправлено. В случае если отправленное письмо имеет атрибут  , на клиенте в программе ViPNet Монитор выполните следующие действия:

- Проверьте соединение с координатором клиента.

6.2. Письмо отправлено, но не доставлено. В случае если письмо имеет атрибут  :

- Убедитесь в том, что сетевой узел получателя включен и на нем запущены программы ViPNet Монитор и ViPNet MFTP.
- Обратитесь к администратору вашей сети ViPNet для проведения аналогичной проверки на всех компьютерах, составляющих маршрут передачи данных от вашего клиента до узла получателя.

6.3. Входящее письмо перемещено в папку **Проблемные** или **Поврежденные**. Если при обработке входящего письма программой ViPNet Деловая почта произошла ошибка, в зависимости от типа ошибки входящее письмо будет автоматически помещено в одну из двух основных подпапок в папке **Аудит**, а на экране появится соответствующее предупреждение. Если выбрать такое письмо, вместо текста письма на панели чтения будет отображаться информация о номере, теме, отправителе письма и коде ошибки.