ОГЛАВЛЕНИЕ

Глава 3

Глава 4

ИСПОЛЬЗУЕМЫЕ АББРЕВИАТУРЫ

AD – [Active Directory] – служба каталогов корпорации Microsoft.

DHCP – [Dynamic Host Configuration Protocol] – протокол динамической конфигурации узла.

DMZ – демилитаризованная зона.

DNS – [Domen Name System] – система доменных имен.

ERP – [Enterprise Resource Planning] – планирование ресурсов предприятия.

FTP – [File Transfer Protocol] – протокол передачи файлов.

IDS – [Intrusion Detection System] – система обнаружения вторжений.

NAT – [Network Address Translation] – преобразование сетевых адресов.

OSI – [open systems interconnection basic reference model] – базовая эталонная модель взаимодействия открытых систем, сетевая модель стека сетевых протоколов.

PKI – [Public Key Infrastructure] – инфраструктура открытых ключей.

RDP – [Remote Desktop Protocol] – протокол удаленного рабочего стола.

ViPNet-сеть – защищенная виртуальная сеть, построенная по ViPNet-технологии.

VPN – [Virtual Private Network или Virtual Protected Network] – виртуальная частная или защищенная сеть.

АКШ – асимметричный ключ шифрования.

dst-файл – дистрибутив ключей пользователя.

АП – абонентский пункт.

АРМ – автоматизированное рабочее место.

АС – автоматизированная система.

БД – база данных.

ДП – деловая почта.

ИСММК – индивидуальный симметричный межсетевой мастер-ключ.

ИСПДн – информационная система персональных данных.

КП – ключи пользователя.

КУ – ключи узла.

КЦ – ключевой центр.

МК – мастер-ключ.

ММК – межсетевой мастер-ключ.

НДВ – недекларированные возможности.

ОИ – открытый интернет (технология обработки информации в ПО ViPNet).

ОС – операционная система.

ОУД – оценочный уровень доверия.

П – пользователь.

ПАК – программно-аппаратный комплекс.

ПО – программное обеспечение.

ПЗ – прикладная задача.

ПСЭ – персональный сетевой экран.

РД – руководящий документ.

РНПК – резервный набор персональных ключей.

СГ – сетевая группа.

СКЗИ – средство криптографической защиты информации.

СМ – сервер-маршрутизатор.

СМЭВ – система межведомственного электронного взаимодействия.

СО – сетевой объект.

СОС – список отозванных сертификатов.

СП – сервис публикаций.

СУ – сетевой узел.

СЭД – система электронного документооборота.

ТК – тип коллектива.

УКЦ – удостоверяющий и ключевой центр.

УЛ – уполномоченное лицо.

УЦ – удостоверяющий центр.

УЦКУ – удостоверяющий центр корпоративного уровня.

ЦР – центр регистрации.

ЦУС – центр управления сетью.

ЭДО – электронный документооборот.

ЭК – элемент кластера.

ЭП – электронная подпись.

ВВЕДЕНИЕ

Пособие представляет собой краткий обзор продуктов торговой марки ViPNet, разработанных компанией ОАО «ИнфоТеКС» для решения задач организации защищенных виртуальных частных сетей (VPN), развертывания инфраструктуры открытых ключей (PKI), а также защиты персональных мобильных и домашних компьютеров. Рассмотрены практические сценарии использования технологий ViPNet.

Первая глава посвящена программным продуктам ViPNet, предназначенным для построения корпоративных виртуальных защищенных сетей на базе технологии VPN. Для этого созданы два комплексных решения, а именно продуктовая линейка ViPNet CUSTOM для организации защиты информации в крупных корпоративных сетях (до десятков тысяч сетевых узлов) и программное обеспечение ViPNet OFFICE для организации VPN-сетей типовых конфигураций в небольших локальных и распределенных IP-сетях. Подробно рассмотрены назначение и функциональные возможности двух модулей ПО ViPNet Administrator – базового программного комплекса для настройки и управления защищенной сетью, а именно программ ViPNet Administrator Центр управления сетью и ViPNet Administrator Удостоверяющий и ключевой центр. В этом же разделе уделено внимание ключевой структуре ViPNet, описан порядок формирования ключевой информации при построении защищенной сети, показаны различные варианты развертывания защищенной сети в зависимости от политики безопасности организации, применяющей технологию ViPNet. Приведен типовой порядок первичной конфигурации сети на основе технологии ViPNet.

Подробно описано ПО ViPNet Coordinator, предназначенное для защиты серверных частей защищенной сети и являющееся обязательным модулем в составе ViPNet CUSTOM. В данном разделе читатель может познакомиться с функциями ПО ViPNet Coordinator в защищенной сети, принципами осуществления соединений в сети ViPNet, технологией виртуальных IP-адресов, основными парамет-

рами, доступными в программе ViPNet Administrator ЦУС для настройки узлов с установленным ПО ViPNet Coordinator, принципами фильтрации трафика в ViPNet, практическими сценариями использования координатора.

Раздел 1.4 посвящен ПО ViPNet Client, играющему роль VPN-клиента в сети ViPNet и обеспечивающему защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях. Клиентское приложение на базе технологии ViPNet выполняет функции шифрования и расшифрования любого IP-трафика, проходящего через сетевую карту компьютера, – как входящего, так и исходящего, и предоставляет сервисы защищенных служб реального времени – для организации обмена сообщениями, проведения конференций, защищенных аудио- и видеопереговоров и защищенных почтовых услуг с возможностями аутентификации отправителя и получателя и контроля за прохождением и использованием документов.

В разделах 1.6–1.10 описаны программные продукты, позволяющие реализовать множество сценариев защиты информации в современных мультисервисных сетях связи. Раздел 1.7 посвящен кластерному решению в технологии ViPNet, реализующему в полном объеме функциональность координатора как одного из важнейших элементов защищенной сети, что особенно актуально для тех сетей и систем, к которым предъявляются повышенные требования к отказоустойчивости и доступности сервисов, обслуживаемых координаторами. Подробно описаны архитектура ViPNet-кластера и функциональное назначение его элементов, рассмотрена типовая схема организации кластера, принципы обработки туннелируемого трафика ViPNet-кластером.

В составе технологии ViPNet реализован программный комплекс ViPNet StateWatcher (Сервер мониторинга), предназначенный 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. В разделе 1.8 читатель может ознакомиться с архитектурой системы мониторинга на основе технологии ViPNet и механизмом работы ее компонентов.

Раздел 1.9 содержит информацию о программном обеспечении ViPNet Policy Manager (Центр управления политиками безопасности), реализующего централизованное управление политиками безопасности узлов виртуальной защищенной сети. Описаны принципы централизованного управления политиками безопасности на основе технологии ViPNet, состав шаблона политики безопасности,

параметры узлов, на основе которых формируются политики безопасности в ПО ViPNet Policy Manager, функции элементов, входящих в состав системы управления, правила формирования результирующих политик безопасности.

Дополнением к решениям ViPNet CUSTOM служит программа ViPNet SafeDisk-V, обеспечивающая организацию безопасного хранения конфиденциальной информации пользователей сетей ViPNet за счет создания виртуальных контейнеров большого объема. Строгое разграничение доступа пользователей к конфиденциальной информации осуществляется за счет интеграции в программный комплекс ViPNet CUSTOM и возможности регулирования доступа в зависимости от текущей конфигурации программы ViPNet Client Монитор. Функциональность программы и принципы защиты информации в ViPNet SafeDisk-V описаны в разделе 1.10.

В главу включена актуальная информация о сертификации данных продуктов по требованиям ФСБ РФ.

В последней части главы 1 рассмотрены функции программного модуля ViPNet Manager, предназначенного для создания структуры виртуальной защищенной сети и ключевых наборов пользователей, а также для периодического обслуживания небольших корпоративных сетей, построенных с использованием программного комплекса ViPNet OFFICE.

Глава 2 посвящена PKI-продуктам торговой марки ViPNet. Основное внимание уделено понятию инфраструктуры открытых ключей, функциям программно-аппаратного комплекса УЦКУ (Удостоверяющий центр корпоративного уровня) и отдельных его составляющих, а также моделям установления доверительных отношений при взаимодействии различных УЦ между собой. На основе нормативных документов, регламентирующих работу УЦКУ ViPNet, описан состав ПАК УЦКУ ViPNet и перечислены услуги, предоставляемые Удостоверяющим центром.

Глава 3 представляет собой обзор программно-аппаратных комплексов ViPNet. ПАК ViPNet – это интегрированные решения на базе нескольких аппаратных платформ и программного обеспечения производства ОАО «Инфотекс», предназначенные для организации сетевой защиты в VPN-сетях. Как правило, в качестве аппаратной платформы в комплексе может использоваться компактный компьютер или полноценный сервер, устанавливаемый в стандартные стойки. Рассмотрены принципы создания отказоустойчивого решения на базе ПО ViPNet Coordinator Linux – организация кластера горячего резервирования.

В разделе 3.2 рассмотрен ПАК ViPNet Terminal, предназначенный для организации защищенного доступа к терминальным серверам Windows Server 2003/2008 по протоколу RDP. Кроме того, данное решение реализует шифрование сетевого трафика и функции персонального межсетевого экрана. ПО ViPNet Terminal обеспечивает работу по протоколу DHCP и прозрачную авторизацию по учетным записям пользователя в Active Directory. Представлены основные характеристики программно-аппаратных комплексов и сценарии их применения.

Глава 4 посвящена основным возможностям программных сетевых экранов ViPNet Office Firewall, ViPNet Personal Firewall, обеспечивающих надежную защиту локальной сети и отдельных компьютеров от несанкционированного доступа.

В главе 5 рассматриваются средства организации безопасного хранения конфиденциальной информации – программный комплекс ViPNet Safe Disk, реализующий создание виртуальных логических дисков и шифрование файлов при их сохранении в контейнере, и программа ViPNet CryptoFile, обеспечивающая шифрование и расшифрование файлов и подписание произвольных файлов электронной подписью (ЭП) и проверку подписи.

Криптопровайдеры торговой марки «ViPNet» описаны в главе 6. Это программа ViPNet CryptoService, предназначенная для защиты прикладной информации, передаваемой по незащищенным каналам связи, и предоставляющая пользователю возможность управлять своими криптографическими ключами: генерировать пары открытый–закрытый ключ, записывать ключи в защищенные контейнеры и на внешние электронные носители, а также считывать ключи из них, обновлять сертификаты. Программа ViPNet CSP – средство криптографической защиты информации, предназначенное для выполнения криптографических операций, доступ к которым обеспечивается встраиванием криптопровайдера в приложения через стандартизованные интерфейсы. Это позволяет вызывать криптографические функции из различных приложений Microsoft и другого ПО, использующего данный интерфейс. В результате использования этой программы пользователь может шифровать сообщения Microsoft Outlook и вложенные файлы, работать с документами MS Office, защищенными электронной подписью, с защищенными веб-соединениями и др.

В главе 7 приведен краткий обзор мобильных приложений ViPNet – ViPNet Client iOS и ViPNet Client Android – решений для защиты мобильных платформ от сетевых атак и организации удаленного доступа к защищенным корпоративным ресурсам. Описаны

базовые сценарии использования мобильных устройств с установленным приложением ViPNet: защищенная IP-телефония, терминальный доступ к корпоративным ресурсам и ресурсам сети Интернет, удаленный доступ к корпоративному серверу Microsoft Exchange.

Глава 8 посвящена использованию системы ViPNet Электронный документооборот (ЭДО) для защиты межведомственного электронного взаимодействия. В данном пособии рассматривается программное обеспечение, используемое при предоставлении в электронном виде государственных и муниципальных услуг: ViPNet ЭДО АРМ Госуслуг – клиентское программное обеспечение для обмена запросами на предоставление информации, ПАК ViPNet ЭДО Шлюз безопасности – специализированный сервер для обмена информацией между организациями по каналам СМЭВ, ViPNet ЭДО АРМ Контроль – программное обеспечение для администрирования ПАК ViPNet ЭДО Шлюз безопасности и мониторинга и сбора статистики по запросам, которые проходят через Шлюз безопасности. Приведены основные понятия и функции СМЭВ, а также типовые схемы взаимодействия компонентов системы ViPNet Электронный документооборот.

В глоссарии даны определения основных понятий и терминов, встречающихся в данном пособии.

Заранее выражаем признательность всем, кому предстоит работать с данным пособием, за предложения и замечания, которые можно направлять по адресу education@infotecs.ru.

История компании ОАО «ИнфоТеКС»

ОАО «ИнфоТеКС» (Информационные Технологии и Коммуникационные Системы) является компанией-разработчиком торговой марки ViPNet.

Компания была основана в 1989 г., в 1991 г. она была зарегистрирована как открытое акционерное общество. Деятельность компании осуществляется в двух направлениях: производство программного обеспечения для защиты информации и развитие и сопровождение проектов в области телефонной связи.

Краткие исторические вехи в развитии компании:

- 1990–1991 гг. Компания делает решительные шаги на рынке программного обеспечения для территориально распределенных защищенных от несанкционированного вмешательства банковских компьютерных сетей.

- Начало 1992 г. Выход на рынок DOS-версии продукта «Корпоративная наложенная сеть „ИнфоТеКС“». Продукт позволял развертывать корпоративную защищенную почтовую систему с интегрированными механизмами шифрования и электронной подписи (ЭП).
- 1992–1993 гг. Работа над проектом создания выделенной корпоративной сети Сбербанка РФ на каналах связи ОАО «Ростелеком» для ряда областных банков СБ РФ, реализация проектов выделенной телефонной связи для нефтегазодобывающей и перерабатывающей отраслей.
- 1994 г. Создание пилотной корпоративной защищенной сети для ЦБ РФ на базе системы спутниковой связи «Сокол – Банкир», которая впоследствии охватила около 40 ГУ ЦБ РФ по территории России.
- 1994 г. Компания выходит на рынок услуг местной связи и создает свое подразделение в Элисте, которое по итогам 1996–1997 гг. охватывает примерно 50% местного рынка услуг радиотелефонной связи.
- 1995–1996 гг. Открывается новое направление деятельности компании – телекоммуникационное. Компания управляет проектом создания транкинговой радиотелефонной сети связи в Республике Калмыкия. В 1999–2000 гг. под управлением ОАО «ИнфоТеКС» была проведена модернизация существующей сети и построена новая сеть цифровой междугородней телефонной связи.
- 1997–1998 гг. Управление строительством цифровой телефонной сети общего пользования на юге России (Ростов-на-Дону, Таганрог). На услуги построенной сети получен международный сертификат качества ISO 9001.
- 1997–1998 гг. На рынок вышла Windows-версия «Корпоративной наложенной сети „ИнфоТеКС“», что позволило в посткризисный период сохранить объем продаж и увеличить долю на зарождающемся российском рынке средств защиты информации (СЗИ). Определено основное направление компании – разработка новых сетевых продуктов по защите информации, ориентированных на TCP/IP и использующих основные принципы организации VPN.
- 1999–2000 гг. Создание целого ряда продуктов и сетевых решений, объединенных торговой маркой ViPNet. Ряд продуктов, среди которых ViPNet Corporate, ViPNet CUSTOM, получили значительное признание на рынке. Осуществлено

внедрение продуктов ViPNet в сегменте сети Министерства иностранных дел, нескольких подразделениях региональных железных дорог. Также продукты ViPNet используются рейдерами в металлургической отрасли, брокерскими фирмами, операторами телефонной связи и интернет-провайдерами.

- 2001–2002 гг. Продвигаемая компанией технология ViPNet становится масштабируемым отечественным программным решением для построения защищенных VPN-сетей. Продукты торговой марки ViPNet проходят сертификацию в Гостехкомиссии по требованиям к межсетевым экранам и автоматизированным системам, защищающим и обрабатывающим конфиденциальную информацию. Организация собственных учебных курсов в компании.
- 2003 г. Выпуск релизов программных модулей ViPNet практически для всех широко используемых на рынке операционных систем – Windows, Linux, Sun Solaris 8. В декабре 2003 г. продуктовая линейка компании пополнилась новым решением – программно-аппаратным комплексом ViPNet Удостоверяющий центр корпоративного уровня, тем самым компания делает уверенный шаг в область инфраструктуры открытых ключей PKI (Public Key Infrastructure).
- 2004 г. Работа по расширению функциональности продуктовой линейки ViPNet и ее дифференциации для разноуровневых бизнес-процессов: разработаны новые программные решения для среднего и малого бизнеса – ViPNet OFFICE и ViPNet Tunnel. С выпуском и сертификацией в ФАПСИ СКЗИ «Домен-К 2.0», поддерживающего новый ГОСТ Р 34.10–2001 и сертификаты ЭП в формате X.509, заложены основы для дальнейшего развития ViPNet в области PKI. Большим интересом у заказчиков стал пользоваться программный комплекс ViPNet Координатор Linux – кластер горячего резервирования, позволяющий решать задачи резервирования и доступности высоконагруженных узлов защищенных сетей ViPNet. Наиболее крупным проектом 2004 г. для компании стал проект по сетевой защите системы продажи железнодорожных билетов АСУ «Экспресс-3».
- 2005 г. Выпуск криптопровайдера ViPNet на базе СКЗИ «Домен-К 2.0». Этот криптопровайдер поддерживает работу через Microsoft Crypto API, входит в состав ПО ViPNet CryptoService. ПО «Удостоверяющий центр ViPNet 3.0» сертифицировано в ФСБ (ФАПСИ). В 2005 г. компания

реализовала целый ряд успешных проектов с новыми клиентами: Фондом обязательного медицинского страхования, Министерством финансов РФ, Федеральной службой по финансовому мониторингу, ОАО «ЦентрТелеком», Администрацией Президента и Правительством Республики Бурятия и др.

- 2006 г. Деятельность компании можно охарактеризовать как «расширение и углубление». Активно развивается направление обучения технических специалистов – клиентов и партнеров компании на учебных курсах: появились новые учебные программы и учебно-методические материалы. Отдел учебных программ компании проводит не только типовое обучение по заявленным программам, но и обучение по специальным программам, адаптированным по требованиям таких клиентов, как ПФР, ФОМС, ОАО «РЖД». Получены сертификаты на СКЗИ «ViPNet Клиент» и «ViPNet Координатор», а также проведена сертификация по требованиям ФСБ к межсетевым и персональным сетевым экранам. Впервые в этом году компания провела партнерский семинар, ставший впоследствии для компании и ее партнеров ежегодным традиционным мероприятием.
- 2007–2008 гг. Работы по расширению спектра поддерживаемых аппаратных платформ. Концепция защищенного мобильного пользователя получает поддержку в виде версий ПО ViPNet Client и ViPNet SafeDisk для ОС Windows Mobile 2003/5. Взят курс на создание линейки программно-аппаратных комплексов, выполняющих функции межсетевых экранов и криптошлюзов: выпущены ПАК NME-RVPN ViPNet (на базе аппаратного модуля расширения для маршрутизаторов Cisco) и ПАК ViPNet Coordinator HW100. Начиная с 2008 г. продукция компании проходит сертификацию в системе добровольной сертификации ГАЗПРОМСЕРТ. В свете выхода закона о защите персональных данных и соответствующих рекомендаций регулирующих органов компания начинает предлагать свои услуги по проектированию и организации защиты персональных данных коммерческим и государственным заказчикам. Совместно с партнерами компания работает над большими проектами по криптографической защите информации в ФОМСе и Роструде. В конце 2007 г. компания получает статус секретарской компании Технического комитета № 26, курирующего

вопросы развития и стандартизации направления криптографической защиты информации.

- 2009 г. Выпуск новой версии всей продуктовой линейки – версии 3.0. Выпущена первая версия системы централизованного мониторинга ViPNet StateWatcher. Выход на рынок программного обеспечения ViPNet Cluster, реализующего принципы балансировки нагрузки в режиме реального времени. Выпущены ПАК ViPNet Coordinator HW1000 и ПАК ViPNet Coordinator HW-VPNM. Специалисты Компании – эксперты ТК № 26 – активно работают над приведением отечественных стандартов (ГОСТ 28147–89 и ГОСТ Р34.10–2001) в соответствие международной системе стандартизации ISO. Подавляющая часть проектов компании выполняется партнерами компании в регионах России для государственных заказчиков федерального и муниципального уровней.
- 2010 г. Дальнейшее развитие технологии ViPNet в сторону поддержки PKI.
- 2011 г. Выход на рынок ViPNet Client под ОС Android и iOS.
- 2012 г. Выпуск новой версии бесплатного криптопровайдера ViPNet CSP, получение положительного заключения ФСБ России, которое подтверждает соответствие ViPNet CSP требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для СКЗИ классов КС1/КС2. Получены сертификаты ФСБ России на «Удостоверяющий центр корпоративного уровня» по классам КС2 и КС3. Создан и сертифицирован ViPNet SOAP-шлюз, построенный на платформе ПАКа ViPNet Coordinator HW1000 и предназначенный для осуществления обмена информацией между организациями в рамках оказания государственных и муниципальных услуг в электронном виде по каналам СМЭВ с применением электронной подписи.

Компания продолжает активно развиваться и создавать новые продукты и решения, а также писать свою историю...

ГЛАВА 1

Продукты ViPNet для построения виртуальных защищенных сетей

Компания ОАО «ИнфоТеКС» выпускает более 25 различных продуктов (программных и программно-аппаратных комплексов), каждый из которых может содержать в себе несколько функциональных модулей. Все это многообразие продуктов призвано удовлетворить самые широкие запросы, связанные с задачами организации защищенных виртуальных частных сетей (VPN) и инфраструктуры открытых ключей (PKI).

Компанией «ИнфоТеКС» разработаны два комплексных программных решения, предназначенных для построения корпоративных виртуальных защищенных сетей: продуктовая линейка ViPNet CUSTOM и программный комплекс ViPNet OFFICE.

1.1. Продуктовая линейка ViPNet CUSTOM

ViPNet CUSTOM – самая обширная продуктовая линейка корпоративного уровня – конструктор защищенных сетей, предлагающий решение всего спектра задач по организации VPN и PKI. Продукты, входящие в состав ViPNet CUSTOM, на регулярной основе проходят сертификацию по требованиям ФСБ и ФСТЭК России к средствам защиты информации ограниченного доступа (конфиденциальной информации), включая персональные данные. Это позволяет использовать данные продукты как в коммерческих, так и в государственных компаниях и организациях.

ViPNet CUSTOM позволяет организовывать защиту информации в крупных сетях (от нескольких десятков до десятков тысяч сетевых узлов – рабочих станций, серверов и мобильных компьютеров) и нацелен на решение двух важных задач информационной безопасности:

- создание защищенной, доверенной среды передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи (Интернет, телефонные и беспроводные линии связи) путем организации виртуальной частной сети (VPN) с одним или несколькими центрами управления;
- развертывание инфраструктуры открытых ключей (PKI) с организацией удостоверяющего центра с целью использования механизмов электронной подписи в прикладном программном обеспечении заказчика (системах документооборота и делопроизводства, электронной почте, банковском программном обеспечении, электронных торговых площадках и витринах), с поддержкой возможности взаимодействия с PKI-продуктами других отечественных производителей.

С использованием ViPNet CUSTOM могут разрабатываться решения по защите информации, требующие разработки (доработки) функционала компонентов комплекса по требованиям заказчика.

Продукты ViPNet CUSTOM рассчитаны на применение в самых разнообразных условиях современных мультисервисных сетей связи – от локальных сетей с несколькими десятками компьютеров до глобальных, географически распределенных сетей передачи данных, включающих в себя десятки тысяч сетевых узлов с применением Интернета в качестве транспортной среды. Все продукты ViPNet CUSTOM предназначены для работы в составе единого комплекса средств защиты информации ViPNet. Автономное применение данных продуктов не предусматривается.

Все продукты можно разделить на:

- ПО, предназначенное для реализации функций управления защищенной сетью. Это программы:
  - ViPNet Administrator,
  - ViPNet StateWatcher,
  - ViPNet PolicyManager,
  - ViPNet Publication Service,
  - ViPNet Registration Point;

- серверные продукты:
  - ViPNet Coordinator (Windows),
  - ViPNet Cluster (Windows),
  - ViPNet Coordinator (Linux),
  - ViPNet Failover (Linux)
  - ПАК ViPNet Coordinator HW100,
  - ПАК ViPNet Coordinator HW1000,
  - ПАК ViPNet Coordinator HW2000,
  - ПАК ViPNet Coordinator HW-VPNM,
  - ПАК NME-RVPN ViPNet;
- клиентское ПО:
  - ViPNet Client,
  - ViPNet Terminal,
  - ViPNet SafeDisk-V,
  - ViPNet Client Android,
  - ViPNet Client iOS,
  - ViPNet CryptoService.

Ниже схематично представлена совместимость программного обеспечения с операционными системами:

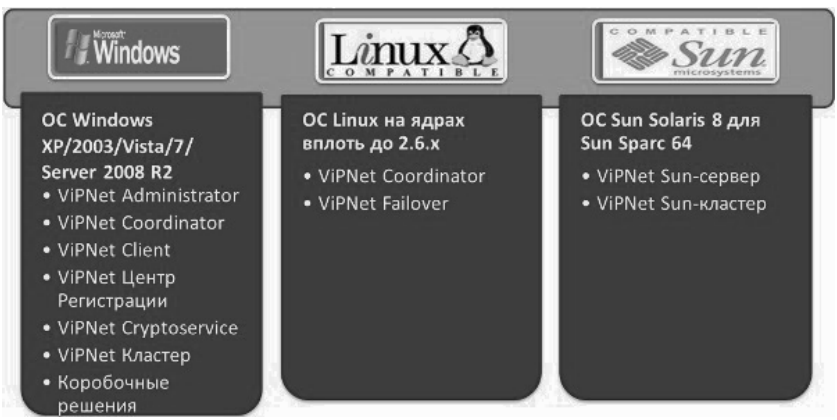

Рис. 1. *Совместимость ПО ViPNet и ряда операционных систем*

Для решения задачи обеспечения защищенного взаимодействия непосредственно между компьютерами в большой распределенной сети в системе должны присутствовать как минимум **3 обязательных элемента**: ПО ViPNet Administrator, ПО ViPNet Coordinator, ПО ViPNet Client.