Введение

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

Продуктовый комплекс СЗИ ViPNet (ПК ViPNet) – уникальное предложение на рынке средств защиты информации, представляющее интегрированный набор продуктов линеек ViPNet Network Security и ViPNet PKI, ориентированных на решение задач информационной безопасности для корпоративных и государственных информационных систем.

Компоненты ПК ViPNet используются для решения следующих основных задач обеспечения 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 производителей;
- создание централизованных комплексов управления, аудита и мониторинга средств защиты информации в распределенных сетях – Центров эксплуатации средств защиты ViPNet.

ПК ViPNet ориентирован на организацию одновременного защищенного взаимодействия узлов в любой схеме взаимодействия (клиент-клиент, сервер-сервер, клиент-сервер, клиент-группасерверов и т. д.), в то время как большинство VPN решений других производителей обеспечивают только соединения уровня сервер-сервер или сервер-клиент. Данная функциональность дает возможность реализовывать внедрение средств информационной безопасности в корпоративные сети сложной топологии, реализовывать политику разграничения доступа в рамках всей корпоративной сети, а также проектировать распределенную систему взаимодействий клиентских и серверных компонентов, балансируя нагрузку на последние, так как, в общем случае при взаимодействии клиент-

клиент VPN-сервер не задействован в операциях шифрования трафика. Большое внимание в ПК ViPNet уделено решению проблемы функционирования в условиях наличия разнообразного сетевого оборудования и программного обеспечения, реализующего динамическую или статическую трансляцию адресов/портов (NAT/PAT), что существенно облегчает процесс интеграции системы защиты в существующую инфраструктуру сети. В типовых топологиях ручной настройки клиентских компонент не требуется.

Глава 1 посвящена программным продуктам ViPNet, состоящим из продуктов линеек ViPNet Network Security и ViPNet PKI. Линейка ViPNet Network Security объединяет в своем составе компоненты сетевой безопасности, а так же средства мониторинга и обнаружения вторжений. Линейка ViPNet PKI может выступать как самостоятельный комплекс компонентов, реализующий полную PKI инфраструктуру, либо использоваться как дополнение к средствам сетевой безопасности ViPNet Network Security. В состав линеек ViPNet Network Security и ViPNet PKI входят программные, программно-аппаратные и аппаратные компоненты. В состав ПК ViPNet входит средство обнаружения вторжений – ViPNet IDS, позволяющее повысить уровень защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и телекоммуникационного оборудования посредством своевременного оповещения о фактах сетевых атак. Компоненты ПК ViPNet оптимизированы для масштабирования защищенных сетей от единиц объектов до десятков тысяч. Компоненты ПК ViPNet адаптированы к различным формам и средам функционирования: поддерживаются мобильные, настольные, серверные среды, среды виртуализации, а также специализированные и промышленные среды и условия функционирования. Средства защиты информации ПК ViPNet тестируются на совместимость со средствами защиты информации производства технологических партнеров компании ИнфоТеКС, ведущих российских и зарубежных разработчиков в рамках интеграционных производственных программ.

Глава 2 посвящена PKI-продуктам торговой марки ViPNet. Линейка ViPNet PKI представляет собой как самостоятельный комплекс компонентов, реализующий полную инфраструктуру продуктов открытого ключа, так и выступает в виде дополнения к средствам сетевой безопасности ViPNet Network Security. Основное внимание уделено понятию об инфраструктуре открытых ключей, функциям программного комплекса УЦ ViPNetи отдельных его составляющих, а также моделям установления доверительных отношений при взаимодействии различных УЦ между собой. На основе нормативных документов, регламентирующих работу УЦ ViPNet, описан состав ПК УЦ 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 3.3 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, обеспечивающей шифрование и расшифрование файлов и подписание произвольных файлов электронной подписью (ЭП) и проверку подписи.

В главе 6 описаны криптопровайдеры торговой марки «ViPNet». 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, защищёнными электронной подписью, с защищенными веб-соединениями, и д.р.

В главе 7 приведен краткий обзор мобильных приложений ViPNet – ViPNet Client for iOS и ViPNet Client for 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: защищённая 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» приведены 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

О компании ОАО «ИнфоТеКС»

Компания ИнфоТеКС (ОАО «Информационные Технологии и Коммуникационные Системы») – ведущий отечественный разработчик и производитель высокотехнологичных программных и программно-аппаратных средств защиты информации. Компания основана в 1989 г., а в 1991 г. ИнфоТеКС зарегистрирован среди первых акционерных обществ России.

Флагманской разработкой компании ИнфоТеКС является технология ViPNet – гибкое VPN-решение для безопасной передачи данных в защищенной сети. Сегодня технология ViPNet – это самое масштабируемое и надежное решение на российском рынке информационной безопасности.

Торговая марка ViPNet объединяет целый ряд продуктов и сетевых решений для крупного, среднего и малого бизнеса и включает:

- программные и программно-аппаратные средства организации виртуальных частных сетей (VPN) и инфраструктуры открытых ключей (PKI);
- средства межсетевого экранирования и персональные сетевые экраны;
- средства шифрования данных, которые хранятся и обрабатываются на компьютерах и в сети;
- средства шифрования данных, которые хранятся и обрабатываются на компьютерах и в сети;
- системы централизованного управления и мониторинга СЗИ;
- средства криптографической защиты информации для встраивания в прикладные системы сторонних разработчиков (системы юридически значимого документооборота, порталы и т.п.);
- программно-аппаратные комплексы (или самостоятельные сетевые устройства) обнаружения компьютерных атак ViPNet IDS.

В числе заказчиков компании ИнфоТеКС: предприятия госсектора, банки, ведущие телекоммуникационные компании, крупнейшие организации нефтегазодобывающей, перерабатывающей и металлургической отрасли.

В ГК ИнфоТеКС входит три дочерние компании: «ИнфоТеКС Интернет Траст» (услуги защиты информации, в том числе в области систем электронного документооборота); «Перспективный мониторинг» и НОЧУ ДПО «Учебный центр ИнфоТеКС», который сотрудничает с ведущими ВУЗами страны, среди которых МГУ им. Ломоносова, МГТУ им. Баумана, Томский государственный университет систем управления и радиоэлектроники (ТУСУР), Дальневосточный федеральный университет (ДВФУ), Санкт-Петербургский государственный морской технический университет (СПбГМТУ), Астраханский государственный технический университет (АГТУ) и многие другие.

Система менеджмента качества ИнфоТеКС сертифицирована по международному стандарту ISO 9001:2008.

Продукты ИнфоТеКС регулярно проходят сертификацию в ФСБ России и ФСТЭК России, а также в отраслевых системах сертификации.