УДК 681.3: 330.131

Акинина Людмила Николаевна, старший преподаватель КФУ имени В.И. Вернадского

e-mail: akininal18@mail.ru

Попов Виталий Борисович, кандидат физико-математических наук, доцент КФУ имени В.И. Вернадского

e-mail: pvb55@mail.ru

Перехрест Роман Дмитриевич, магистрант КФУ имени В.И. Вернадского

e-mail: romaperehrest2012@mail.ru

ПРОГРАММНО–АППАРАТНЫЕ КОМПЛЕКСЫ VIPNET И ИХ ИСПОЛЬЗОВАНИЕ В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация: в работе проводится анализ программного обеспечения и программно-аппаратного комплекса ViPNet Coordinator. Описываются их основные функции и возможность применения на государственных предприятиях.

Ключевые слова: программно-аппаратные комплексы, защищенный электронный документооборота органов Пенсионного Фонда России (ПФР), корпоративные информационные системы, технология построения виртуальных защищенных сетей.

Akinina Lyudmila, V.I. Vernadsky Crimean Federal University, Simferopol, Crimea, Russia

e-mail: akininal18@mail.ru

Popov Vitali, V.I. Vernadsky Crimean Federal University, Simferopol, Crimea, Russia

e-mail: pvb55@mail.ru

Perehrest Roman, master student, V.I. Vernadsky Crimean Federal University, Simferopol, Crimea, Russia

e-mail: romaperehrest2012@mail.ru

HARDWARE-SOFTWARE COMPLEX VIPNET AND THEIR USE IN CORPORATE NETWORKS

Annotation: the paper analyzes the software and the hardware and software ViPNet Coordinator. Describes their main functions and the possibility of state-owned enterprises.

Keywords: hardware and software systems. The system of secure electronic document of the Pension Fund of Russia (PFR). Technology VipNet. The technology of building virtual private networks ViPNet.

На сегодняшний день, учитывая уровень развития информационных технологий, защита информации любой компании, а тем более государственного учреждения, имеет одно из первостепенных значений.

В данной статье рассмотрены эффективные средства создания защищенной и отказоустойчивой виртуальной корпоративной компьютерной сети любого масштаба. Гибкое сочетание компонентов виртуальных защищенных компьютерных сетей (ViPNet) и их функциональных возможностей позволяет удовлетворить любые потребности как небольших компаний, так и крупных коммерческих и государственных организаций, имеющих территориально распределенные сети.

Цель данной работы заключается в анализе документооборота Пенсионного фонда Республики Крым и его программной защите. Для

достижения поставленной цели предусматривается решение следующих задач, определивших логику научного исследования и его структуру:

– провести анализ технологических процессов Пенсионного фонда,

– описать общее представление технологии виртуальных защищенных компьютерных сетей,

– оптимизировать поток документооборота в организации,

– реализовать защиту данных с использованием технологии ViPNet,

– разработать методические рекомендации по совершенствованию механизма защиты информации и функционирования Пенсионного фонда Российской Федерации для эффективного использования финансовых ресурсов и повышения уровня пенсионного обеспечения в условиях реформирования пенсионной системы,

– рассмотреть основные функции системы электронного документооборота при использовании в организации, возможные варианты внедрения ViPNet в зависимости от конфигурации виртуальных приватных сетей в корпоративных сетях Пенсионного фонда Республики Крым.

Исследуемая тема рассматривалась в работах некоторых авторов. Стоит отметить издания В. В. Гусева [1, 2] «Администрирование системы защиты информации ViPNet», «Программно-аппаратные комплексы ViPNet, «Официальный курс по организации виртуальных защищенных сетей ViPNet», в которых дано исчерпывающее представлении о технологии ViPNet и рассмотрены основы администрирования программно-аппаратных комплексов ViPNet. Данные издания полезны для специалистов в области информационной безопасности, занимающихся практическими вопросами построения комплексных систем защиты информации и применения средств защиты в автоматизированных системах.

Исследуемая тема также затрагивается в монографии Н. В. Кабакова, А. О. Чефранова, Ю.Ф. Алабина [3] «Система защиты информации ViPNet».

Монография представляет собой краткий обзор продуктов торговой марки ViPNet, разработанных компанией ОАО "ИнфоТеКС" для решения задач по 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.

Учебное пособие для инженеров и администраторов компьютерных сетей «Технология построения VPN ViPNet» А. О. Чефранова [4] представляет из себя курс лекций по технологии возведения виртуальных защищенных сетей ViPNet. Пособие приурочено к теоретическим вопросам применения технологии ViPNet. Рассмотрена терминология, концепции, формы, способы и средства, использующиеся в технологии возведения виртуальных защищенных сеток. Особое место отведено вопросам, связанным с отличительными чертами ключевой текстуры ViPNet-сети, технологию PKI, также вопросам обработки IP-трафика ViPNet-драйвером.

Защита информации с помощью технологии ViPNet организована, в частности, в органах Пенсионного фонда Российской Федерации (ПФ РФ). В том числе и в Крымском региональном управлении.

В современных электронных технологиях поддержка и защита информации является достаточно актуальной задачей. С этой точки зрения данная работа представляет определенный интерес.

Информационное взаимодействие по телекоммуникационным каналам связи между органом ПФР и Абонентом СЭД по обмену электронными документами с применением электронно-цифровой подписи, идущее по определенным правилам, называется *документооборотом*.

В ходе документооборота осуществляется взаимодействие между следующими *типами участников документооборота*:

– Абонент СЭД – организация, отправляющая сведения в орган ПФР (в ходе документооборота идентифицируется регистрационным номером организации в орган ПФР в формате «###-###-######», где «#» – это любая цифра);

– Орган ПФР – орган ПФР (в ходе документооборота идентифицируется строкой «###-###», где первая часть – код региона по классификатору ПФР, а вторая – код района по классификатору ПФР, если органом ПФР – Отделение, то устанавливается код района равный 000);

– Провайдер – Оператор связи, осуществляющий доставку шифрованного сообщения от одного абонента СЭД ПФР к другому по защищенным каналам передачи данных;

– НеопределенныйПровайдер ‾ оператор связи, осуществляющий доставку шифрованного сообщения от одного абонента СЭД ПФР к другому по каналам передачи данных.

Документооборот состоит из нескольких основных неделимых этапов передачи информации между субъектами. Эти этапы называются транзакциями. В рамках каждой транзакции формируется один транспортный пакет документов, представляющий из себя один архивированный файл. Транспортный пакет содержит информацию, позволяющую провести контроль его целостности. В случае повреждения пакета при пересылке, пакет не будет обработан принимающим субъектом, а будет сгенерировано сообщение об ошибке. Документы в транспортном пакете, в том числе и служебные документы, передаются подписанными ЭЦП в зашифрованном виде, а файл – описатель в открытом виде с ЭЦП, если в описании конкретного документооборота не оговорен иной вариант.

Документооборот при обработке, как правило, содержит четыре транзакции, однако в зависимости от типа передаваемой информации и

необходимости направления обязательного ответа на нее допустимы типы документооборота, содержащие сокращенное количество транзакций.

Типовому содержанию транзакций соответствуют:

– Отправитель передает по телекоммуникационным каналам связи пакет документов Получателю;

– Получатель, по результатам проверки сертификатов ключей ЭЦП, направляет Отправителю электронный документ фиксированного формата – квитанцию о получении пакета документов;

– Получатель направляет ответ на пакет документов Отправителю;

– Отправитель направляет Получателю электронный документ фиксированного формата – квитанцию о получении ответа.

Сокращенному содержанию транзакций соответствуют:

– Отправитель передает по телекоммуникационным каналам связи пакет документов Получателю;

– Получатель, по результатам проверки сертификатов ключей ЭЦП, направляет Отправителю электронный документ фиксированного формата – квитанцию о получении пакета документов.

В отдельных типах документооборота допустимы и другие варианты взаимодействия.

Каждый тип документооборота определяет:

– набор транзакций, которые осуществляются в рамках этого типа документооборота;

– типы документов, которые передаются в рамках этого типа документооборота;

– допустимые типы содержимого передаваемых документов.

Каждая транзакция определяет:

– участника документооборота, отправляющего документы;

– участника документооборота, принимающего документы;

– типы документов, которые должны быть переданы в рамках этой транзакции;

– набор подписей, которые должны стоять под передаваемыми документами.

Таким образом, электронный документооборот между участниками системы осуществляется в несколько неделимых этапов передачи информации между субъектами. Электронные документы, передаваемые между Участниками СЭД ПФ РФ, в обязательном порядке подписываются, а также шифруются на автоматизированных рабочих местах Абонентов СЭД. Перемещение документов от одного участника СЭД ПФР к другому участнику осуществляется через транспортные маршрутизаторы только в зашифрованном виде. В рамках каждого этапа передачи информации формируется один транспортный пакет, представляющий из себя один архивированный файл. Транспортный пакет содержит информацию, позволяющую провести контроль его целостности. То есть, в случае повреждения пакета при пересылке пакет не будет обработан принимающим субъектом, а будет сгенерировано сообщение об ошибке. Все документы в транспортном пакете передаются в зашифрованном виде, а служебный файл и файл-описатель передаются в открытом виде с ЭЦП.

Технология обмена электронными документами в системе защищенного электронного документооборота ПФ РФ (СЭД ПФ РФ) по телекоммуникационным каналам связи предназначена для организации защищенного юридически значимого электронного документооборота между Абонентами СЭД ПФ РФ и органом ПФ РФ и осуществляется в соответствии со схемой (см. рис.).

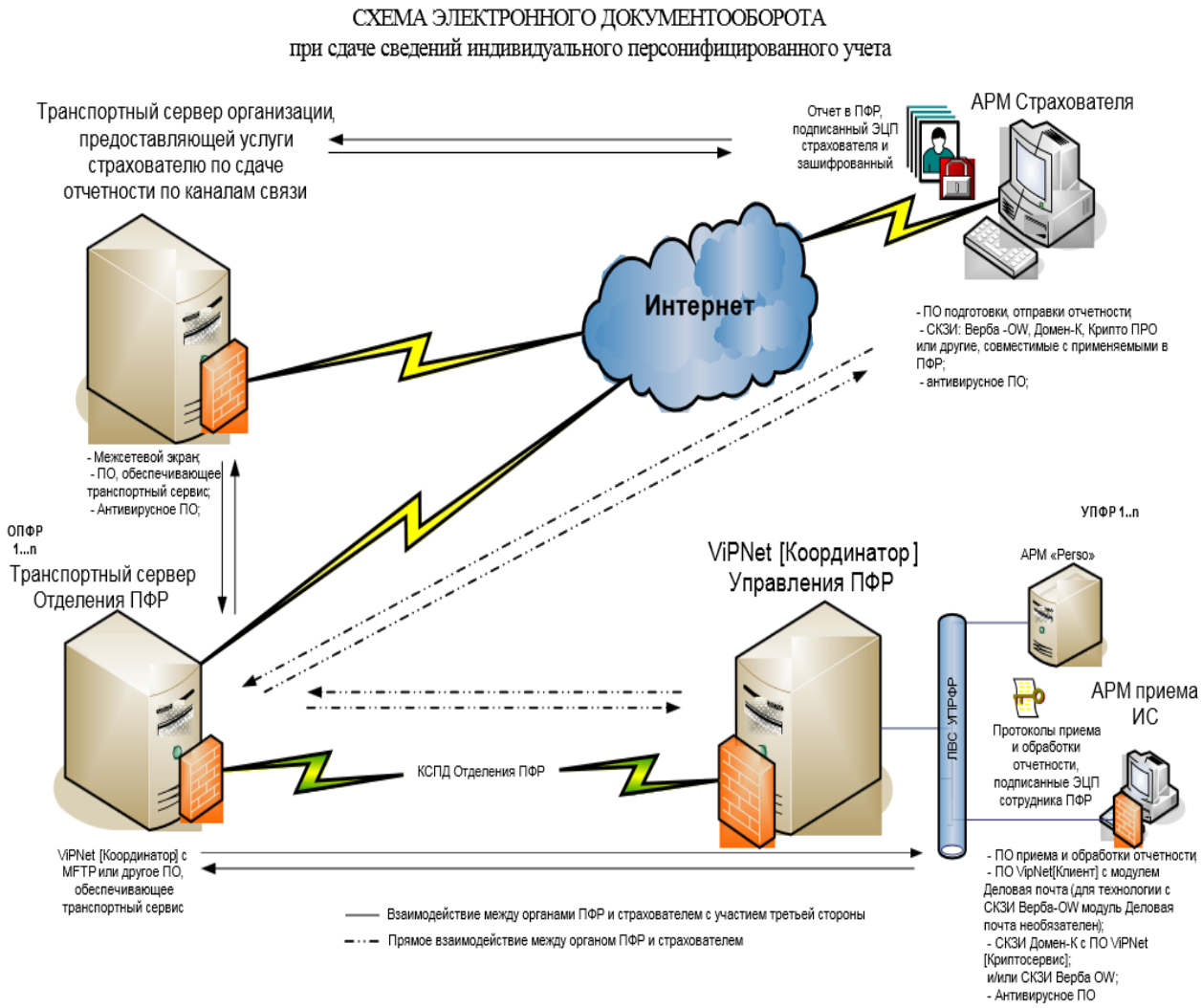

Рисунок – Схема электронного документооборота.

Технология обмена электронными документами в СЭД ПФ РФ описывает порядок подключения Абонентов и их взаимодействия с органами ПФ РФ, порядок обеспечения защиты информации и поддержания в актуальном состоянии ключевой документации, описывает компоненты СЭД ПФ РФ и их взаимосвязь.

Система защищенного электронного документооборота органов ПФ РФ с Абонентами СЭД по телекоммуникационным каналам связи включает следующие основные компоненты:

– автоматизированное рабочее место (АРМ) Абонента СЭД;

– АРМ специалиста органа ПФ РФ;

– удостоверяющие центры с установленными доверительными отношениями;

– удостоверяющий центр ПФ РФ;

– коммуникационная составляющая.

Программно-технические компоненты на стороне органа ПФ РФ и на стороне Абонента предназначены для формирования электронных документов, их подписания электронной цифровой подписью (ЭЦП) и шифрования перед осуществлением транспортировки от отправителя к получателю. Функции транспортного сервера Абонентов выполняет сервер организации, оказывающей им услуги Удостоверяющего центра, либо другая организация.

Для технологий, использующих сервисы системы ViPNet, на транспортном сервере Удостоверяющего центра или организации устанавливается программное обеспечение (ПО) ViPNet Клиент (Деловая почта) и ПО VipNet Координатор.

VipNet Клиент в территориальном органе ПФ РФ может быть установлен на том же рабочем месте, на котором установлен АРМ специалиста органа ПФ РФ, либо на другом рабочем месте. Важно, чтобы рабочее место, на котором установлен АРМ специалиста органа ПФР, и рабочее место, на котором установлен VipNet Клиент могли обмениваться файлами, например, с использованием общего сетевого ресурса (сетевого диска).

Вместо технологии VipNet для транспортировки электронных документов допустимо применять другие программы, разрешенные к использованию в ПФ РФ.

В рамках Системы исходящая информация шифруется либо на рабочем месте Абонента, либо на рабочем месте специалиста органа ПФР. Через транспортные серверы информация проходит только в зашифрованном виде.

Программно-аппаратный комплекс (ПАК) VipNet Coordinator HW предназначен для организации сетевой защиты в VPN сетях. ПАК реализован на базе программного обеспечения компании ОАО «Инфотекс» и нескольких аппаратных платформ сторонних производителей [1,2].

Задачей VPN-сети, развернутой с помощью технологии ViPNet, помимо типовой задачи VPN-сетей – защиты трафика в глобальных сетях, является задача обеспечить защиту трафика различных сетевых устройств в процессе информационного обмена между ними на всем пути от узла-источника к узлу-получателю независимо от расположения этих узлов. На этом пути может находиться разнородная сетевая инфраструктура, включающая Интернет, корпоративные, локальные сети и их сегменты.

Виртуальная сеть строится с использованием программных компонентов ViPNet, путем установки на компьютеры ПО ViPNet Client, ПО ViPNet Coordinator, ПО ViPNet Coordinator Linux, а также программно-аппаратных комплексов ViPNet серии HW100/1000/2000/VPNM. В виртуальную сеть могут включаться также мобильные устройства на платформах IOS, Android с установленным специальным ПО ViPNet Client под эти платформы [1].

Компьютеры и мобильные платформы с ПО ViPNetClient именуются Клиентами.

Компьютер с ПО ViPNetCoordinator, ПО ViPNetCoordinatorLinux, а также программно-аппаратные комплексы ViPNet серии HW100/1000/2000/VPNM именуется Координатором.

Координаторы обеспечивают сетевую защиту туннелируемых ими сетевых ресурсов, включение в VPN защищенных компьютеров независимо от места их расположения и оповещение Клиентов и координаторов о способах доступа к другим сетевых узлам, связанных с ними.

Координаторы, как правило, устанавливаются на границе сетей, и выполняют функции [1]:

– *Сервера IP-адресов* – функция, которая в автоматическом режиме с помощью специального защищенного протокола динамической маршрутизации VPN-трафика обеспечивает обмен между узлами ViPNet актуальной информацией о топологии сети как внутри данной виртуальной сети, так и при взаимодействии с узлами других виртуальных сетей ViPNet. Результатом работы данного протокола является возможность маршрутизации VPN-трафика между узлами сети ViPNet тем методом, который наиболее оптимален для используемого способа и места подключения узла к сети.

– *Маршрутизатора VPN-пакетов* функция, обеспечивающая маршрутизацию транзитного VPN-трафика, проходящего через координатор на другие VPN-узлы. *Маршрутизация* осуществляется на основании идентификаторов защищенных узлов, находящихся в открытой части VPN-пакетов, которая защищена от подделки, и на основании данных, полученных в результате работы протокола динамической маршрутизации VPN-трафика. Одновременно выполняется функция трансляции адресов для VPN-трафика, и все пакеты, поступающие на координатор, отправляются на другие узлы с использованием IP-адреса координатора.

– *VPN шлюза* – стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) между локальными открытыми и удаленными защищенными или туннелируемыми узлами. Координатор такой канал может создавать через каскад других координаторов, выполняющих функцию маршрутизации VPN-пакетов.

– *Транспортного Сервера* – функция, которая обеспечивает доставку обновлений ключевой, справочной информации, политики ПО из программ управления сетью ViPNet на защищенные узлы.

– *Межсетевого экрана* – функция фильтрации открытых, защищенных и туннелируемых транзитных и локальных сетевых соединений, трансляции адресов для открытых и туннелируемых соединений.

Узлы сети ViPNet могут быть подключены к сети произвольным образом и в любом ее месте. При появлении любого трафика в адрес других узлов он немедленно, без каких-либо протоколов предварительного установления соединений с узлом- получателем инкапсулируется в ViPNet-пакеты и передается через VPN-сеть на узел- получатель [3].

Основным условием успешного соединения клиента с любым конечным узлом является наличие при включении доступа к своему Координатору, который выполняет для него функцию Сервера IP-адресов и передает ему всю необходимую информацию о способе доступа к узлам, с которыми связан.

При внедрении технологии ViPNet в корпоративную сеть, мы получаем гарантированно надежные результаты, отвечающие всем запросам сегодняшнего дня, а именно [4]:

Комплексный подход к обеспечению ИБ:

- многоуровневая защита от сетевых атак;
- конфиденциальность, целостность и доступность информационных ресурсов при использовании любых каналов связи;
- централизованное управление средствами защиты;

Уникальные механизмы сетевой безопасности:

- виртуализация адресного пространства в рамках VPN;
- полное сокрытие структуры защищаемой сети и передаваемой информации;
- низкоуровневый драйвер защиты приложений и операционной системы;

Прозрачная работа в современных сетях связи:

- поддержка всех доступных технологий связи: xDSL, Ethernet, WiFi, WiMAX, GPRS/EDGE/3G;
- полная совместимость с протоколами TCP/IP;
- прозрачная работа через NAT/PAT, поддержка DHCP, DNS;

– корректная обработка мультимедийного трафика и IP-телефонии;

Неограниченная масштабируемость и высокая надежность:

– до десятков тысяч сетевых узлов в одной защищенной сети;

– возможность произвольного связывания защищенных сетей;

– доступные конфигурации серверных продуктов с режимами горячего резервирования и кластеризации;

Развитые прикладные сервисы:

– все необходимые компоненты для развертывания инфраструктуры Удостоверяющих центров;

– элементы документооборота и механизмы электронной цифровой подписи;

– защищенные чат и конференция;

– поддержка стандартных интерфейсов для встраивания в прикладное программное обеспечение заказчика;

Соответствие требованиям законодательства и регуляторов рынка (регулярная сертификация продуктов Компании на соответствие требованиям ФСБ и ФСТЭК России к средствам защиты конфиденциальной информации, включая персональные данные).

Список литературы:

1. Гусев В.В. Программно-аппаратные комплексы ViPNet / В.В. Гусев. // Москва. – Горячая линия – Телеком. – 2014. 354с.

2. Гусев В.В. Администрирование системы защиты информации ViPNet / В.В. Гусев // Москва. – Горячая линия – Телеком. – 2013. 379с.

3. Кабакова Н. В., Чефранова А.О., Алабина Ю.Ф. Система защиты информации ViPNet. Курс лекций / Н.В. Кабакова, А.О. Чефранова, Ю.Ф. Алабина // М. – ДМК-Пресс. – 2015. – 456с.

4. Чефранова А.О. Технология построения VPN ViPNet / А.О. Чефранова // М. – Горячая линия – Телеком. – 2009. – 289с.