УДК: 004.946

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ МОДЕЛИРОВАНИЯ ДИНАМИЧЕСКИХ VPN-СЕТЕЙ

А.И. Жирохов, А.В. Ануфренко, И.В. Ковальский, М.А. Снятков (Санкт-Петербург)

Современные телекоммуникационные сети характеризуется высоким ростом виртуальных сетевых ресурсов, которые логически разделены, но используют единую физическую инфраструктуру. И хотя само это явление не ново [1, 2] и именуется как логические, оверлейные, наложенные или *VPN*-сети (далее – *VPN*-сети), однако растущая интенсивность их развития и применения, а также разнообразие технологических подходов к построению затрудняют планирование их использования на ограниченном физическом сетевом ресурсе с учетом выполнения предъявляемых требований к передачи данных.

VPN-сети организуются поверх существующей физической инфраструктуры, являются надстройкой над стандартными сетевыми протоколами и обладают рядом преимуществ [3].

Основной проблемой эффективного применения *VPN*-сетей является несогласованность между операторами, предоставляющими физический сетевой ресурс и динамически меняющимися требованиями, предъявляемыми распределенными потребителями (программно-техническими средствами) *VPN*-сетей к данному ресурсу.

Проблема оптимизации *VPN*-сетей неоднократно исследовалась отечественными и зарубежными учеными [1], однако особенности применения динамических виртуальных сетей (*Dynamic Virtual Private Network, DVPN*) изучены недостаточно и представляют интерес планируемой работы (рис. 1).

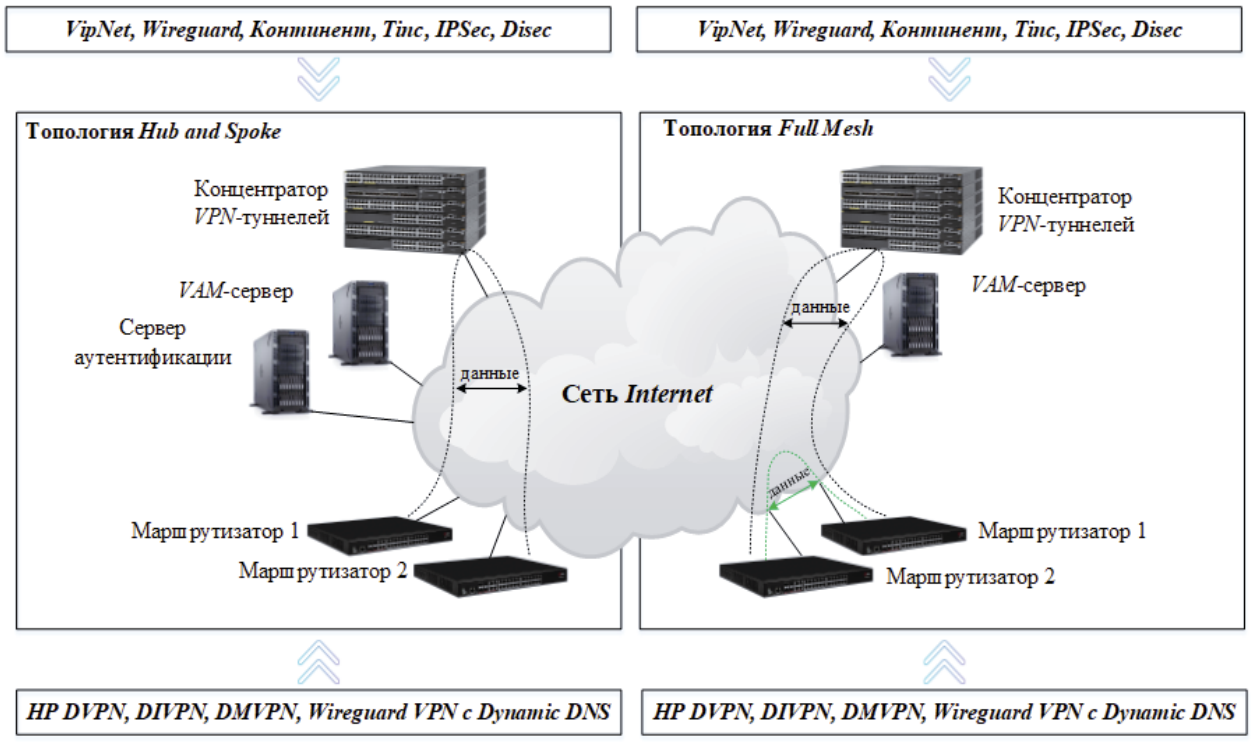

Рис. 1. Топологии виртуальных сетей с применением технологии динамического *VPN*

Динамическая виртуальная сеть – это логическое объединение сетевых устройств или пользователей, которые автоматически определяют своё расположение в

виртуальной сети [4]. *DVPN*-сети могут иметь различную топологию построения (*Hub and Spoke, Full Mesh*) и принципы аутентификации (через сервер аутентификации, через *VAM*-сервер). При построении *DVPN*-сети, можно использовать два основных подхода:

– построение сети с применением классических протоколов *DVPN,* таких как *HP DVPN*, *DIVPN*, *DMVPN* и т.д.;

– построение сети с применением «цифровых двойников» *VPN-серверов,* использующих классические протоколы *VPN* (*OpenVPN, WireGuard, IPSec*, *DiSec*, Континент, *VipNet* и т.д).

Таким образом, *DVPN*-сеть является сложным объектом исследования. Для реализации ее преимуществ требуется решения ряда научно-прикладных задач, связанных с разработкой модели функционирования *DVPN*-сети и методики по оценке ее характеристик, что и определило актуальность настоящей работы.

Анализ программных продуктов по разработке имитационных моделей сетей связи показал, что условно их можно разделить на две группы: симуляторы и эмуляторы (рис.2).

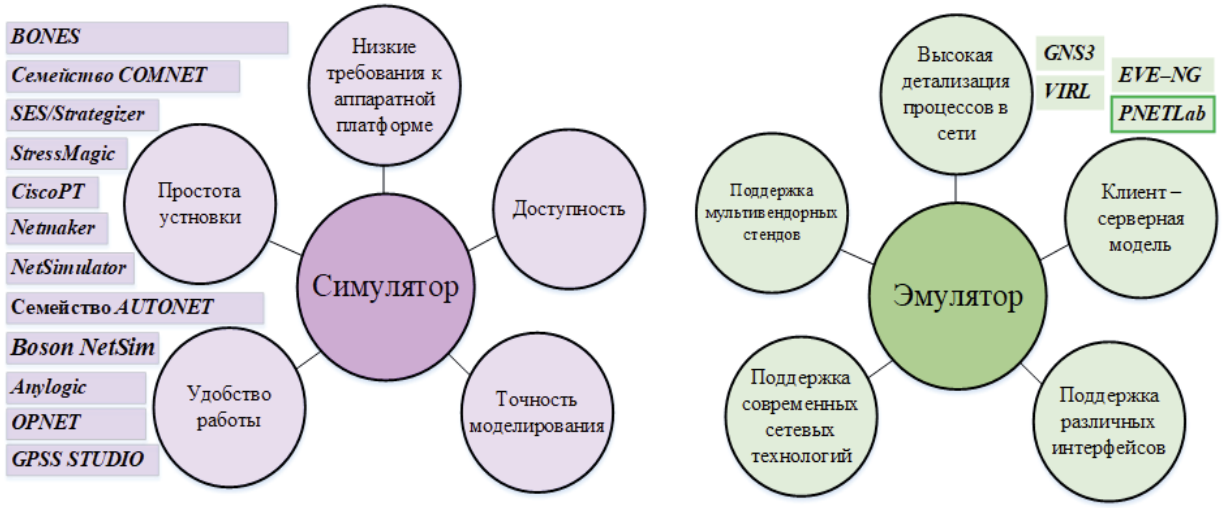

Рис. 2. Программные продукты для моделирования сетей связи

Программные симуляторы и эмуляторы представляют широкий функционал для исследования, планирования, проектирования и внедрения сетевых решений.

Симуляторы потребляют небольшое количество ресурсов и просты в установке, однако являются либо неспециализированным ПО, либо поддерживают устройства ограниченного числа вендоров с неполным функционалом.

Эмуляторы виртуализируют реальные сетевые устройства, ввиду чего позволяют создавать наиболее точные виртуальные стенды, отражающие работу реальной сети. Однако, по причине виртуализации для их корректной работы необходимо больше вычислительной мощности, памяти и места для хранения данных.

Необходимо отметить, что симуляторов сетей связи на сегодняшний день гораздо больше, чем эмуляторов, в том числе есть и отечественные симуляторы (например, *GPSS STUDIO*), что весьма актуально в рамках особого внимания к развитию доверенного ПО.

Анализ программных продуктов привел к выводу о том, что универсального инструмента для проведения исследований в области телекоммуникаций не существует. Для эффективной работы необходимо выбирать оптимальный набор ПО, наиболее удовлетворяющий задачам исследования. В рамках настоящей работы с учетом изученных достоинств и недостатков [5] для моделирования *DVPN*-сети выбрана виртуальная лаборатория *PNetLab* (табл. 1).

Таблица 1. Сравнительный анализ телекоммуникационных симуляторов и эмуляторов

Особенности/ПО	*CPT*	*NetSim*	*EVE-NG*	*GNS3*	*VIRL*	*PnetLab*
Цена	5	3	4	5	2	4
Требования к производительности	5	4	3	3	3	3
Количечтво работающих устройств	3	4	5	5	4	5
Кол-во образов сетевых устройств	3	4	5	5	4	5
Поддержка сетевого интерфейсов	3	4	5	5	5	5
Доступность для изучения	5	4	3	2	3	4
Удобство работы с образами	5	5	3	2	4	4
Итог (баллы):	29	28	28	27	25	30

При этом значимым является возможность формирования в *PNetLab* виртуального стенда с образами сетевого оборудования, функционал которого аналогичен функционалу их оригиналов.

Большим преимуществом *PNetLab* является возможность работы непосредственно с файлами развернутых лабораторий, изменение которых является механизмом изменения топологии виртуального фрагмента сети – добавления/удаления узлов, изменения связей между ними, модификации их начальных конфигураций. Это позволяет моделировать следующие сценарии:

– автоматическое масштабирование инфраструктуры (добавление нового VPN-сервера при росте нагрузки);

– миграция сервисов между узлами;

– изменение сетевой топологии в ответ на события.

Такой механизм позволяет исследовать варианты построения *DVPN*-сети как с применением классического подхода, так и применение «цифровых двойников».

Также важными функциями в рамках исследования *DVPN*-сети является возможность подключать виртуальные сетевые элементы *PNetLab* к реальной сети связи и объединять виртуальные сетевые фрагменты *PNetLab*, созданные на разных аппаратных платформах, в единую сеть (рис. 3). Тестирование различных способов подключения элементов виртуальной лаборатории во внешнюю сеть определило степень их влияния на быстродействие работы программы (первый и третий способ наиболее производительные, рис. 3).

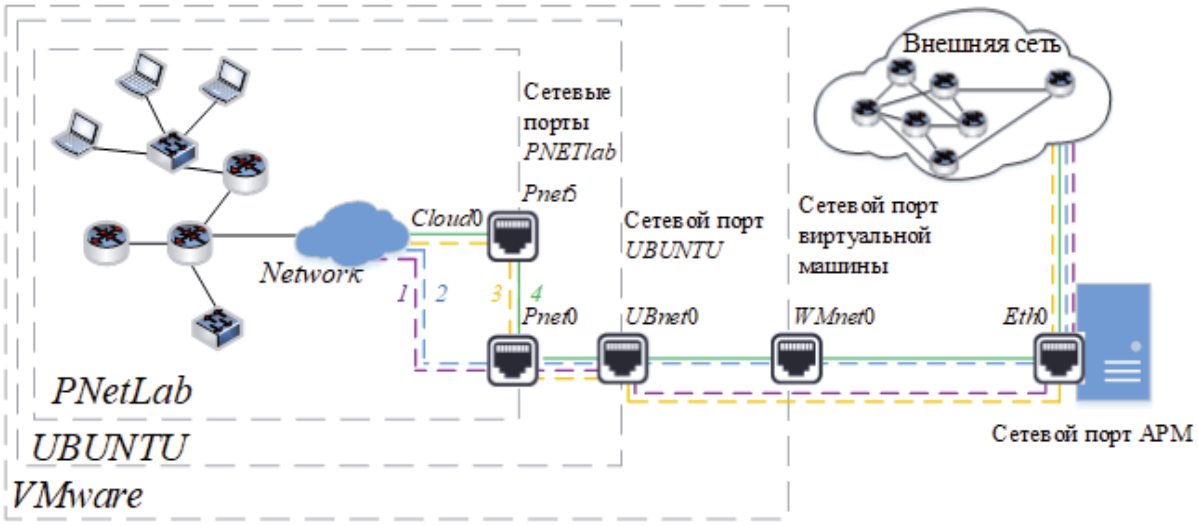

Рис. 3. Варианты подключения элементов *PNetLab* к внешней сети

В рамках подготовки стенда для моделирования *DVPN*-сети в *PNetLab* был протестирован следующий функционал:

– создание требуемой сетевой архитектуры – протестированы сетевые элементы трехуровневой структура сети, представляющей интерес исследования;

– реализация функций сетевого мониторинга – протестирована работа интересующего ПО: *Zabbix* и *Algorius*;

– имитация работы нарушителя – протестирован набор программ операционной системы *Kali Linux*;

– реализация функций сетевого тестирования – протестировано интересующее ПО: *ixchatiot* и *nfsen*;

– имитация среды передачи данных – протестирована работа ПО *Wanulator*.

Добавление образов оборудования и компьютеров с необходимым ПО производилось согласно блок-схемы, представленной на рис. 5. Тестирование представленного выше функционала виртуальной лаборатории не вызвало затруднений за исключением имитации среды передачи данных (ПО *Wanulator*).

Необходимо отметить, что ПО *Wanulator* распространяется в виде готового *iso*-образа загрузочного носителя и базируется на *Debian*-подобных операционных системах, загружаемых как *Live-CD*. Подобный подход позволяет добиться универсальности в использовании на различном оборудовании.

Механизм использования *iso*-образа *Wanulator*-подобных программ на «виртуальной машине» имеет специфику использования *iso*-образа *Live-CD*, размещенного на физическом носителе компьютера вне «виртуальной машины». При создании образа для «виртуальной лаборатории» *PNetLab* с использованием *VMWare* необходимо, чтобы все данные, используемые в образе, хранились в памяти эмулируемого компьютера, на базе которого будет сформирован образ для *PNetLab*.

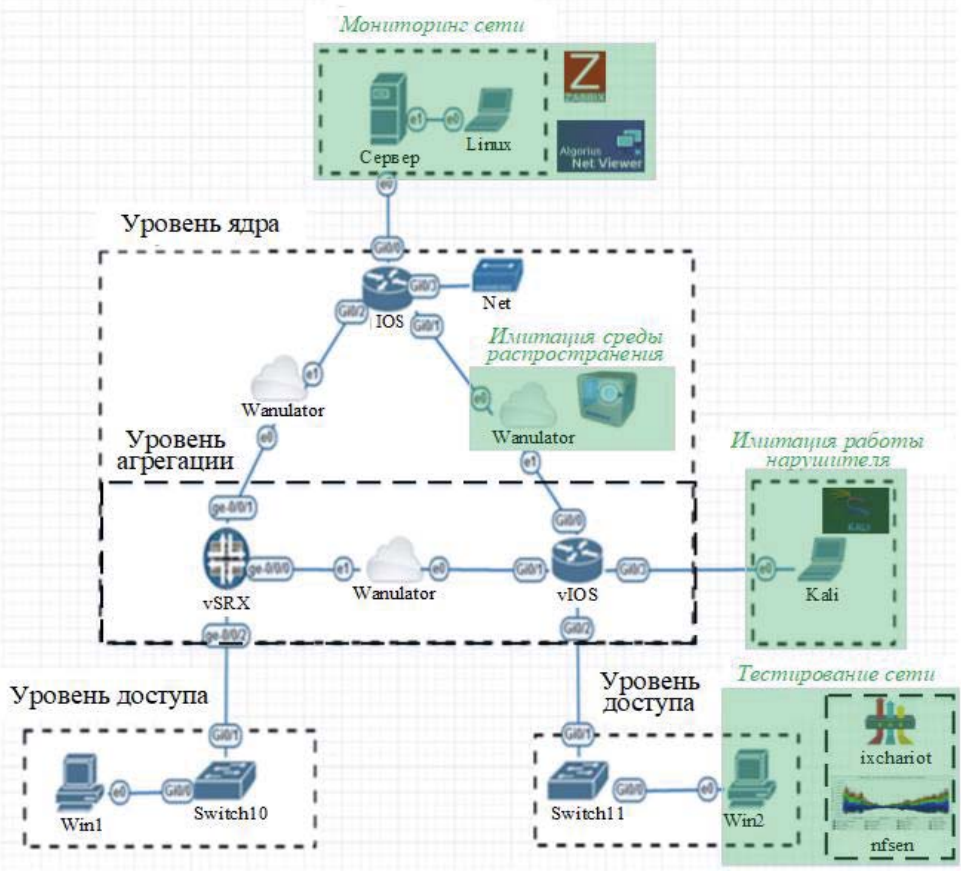

Рис. 4. Тестовый стенд для моделирования *DVPN*-сети

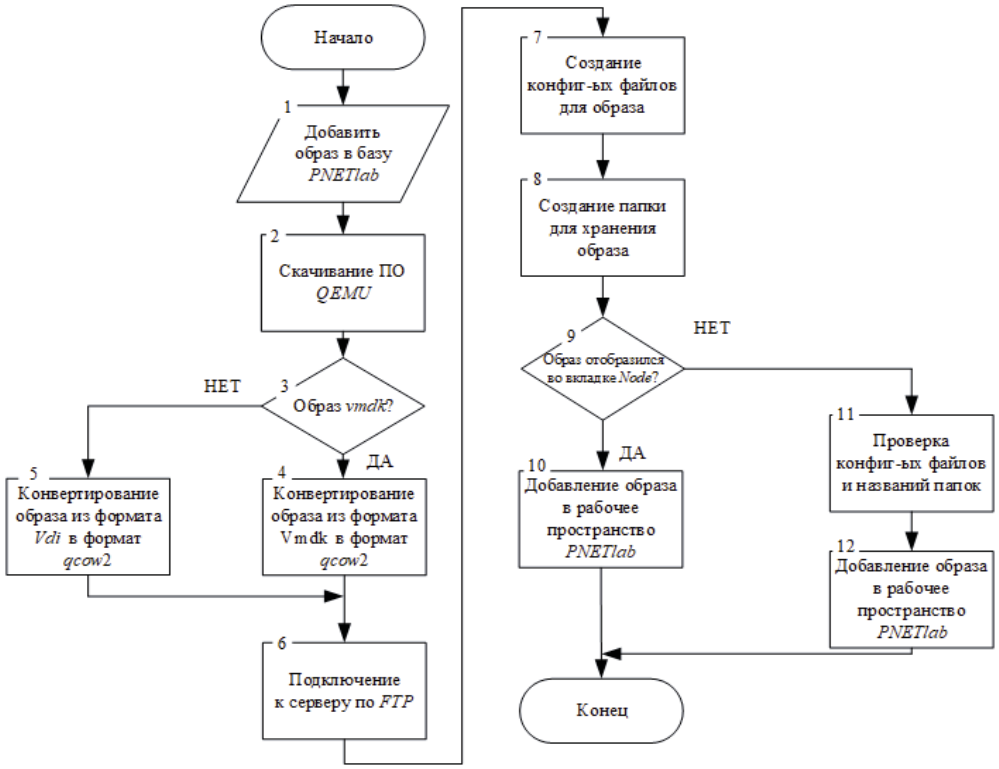

Рис. 5. Блок-схема добавления образов оборудования в виртуальную лабораторию

Результаты тестирования функциональных возможностей виртуальной лаборатории *PnetLab* подтвердили целесообразность использования этого программного продукта для исследования вопросов функционирования *DVPN*-сетей.

Вывод

Виртуальная лаборатория *PnetLab* позволяет разработать имитационную модель функционирования *DVPN*-сети, учитывающую нагрузочные, функциональные и структурные параметры реальной телекоммуникационной инфраструктуры, а также внешние деструктивные воздействия.

На следующем этапах работы предстоит решить вопросы, связанные с анализом особенностей (рис.6):

– технологий динамического *VPN*;
– информационного обмена в *DVPN*-сетях;
– построения логической и физической архитектуры сети.

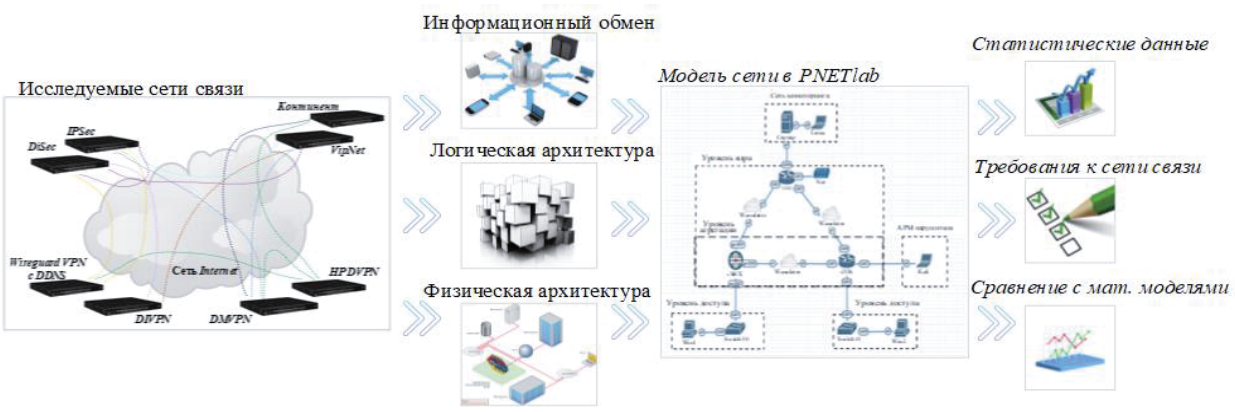

Рис. 6. Этапы разработки модели *DVPN*-сети

Дальнейшим этапом исследования является разработка модели функционирования *DVPN*-сети, на основе которой будет возможно:

– собирать статистические данные о функционировании сети;

– формировать требования к применению DVPN-сетей;

– сравнивать результаты математических моделей с результатами разработанного виртуального стенда.

Модель функционирования *DVPN*-сети позволит продвинуться в решении проблем оптимизации ограниченного физического сетевого ресурса, выделяемого для функционирования *VPN*-сетей.

Литература

1. **Росляков А.В., Лысиков А.А., Халиуллина Ю.Т.** Задачи планирования и оптимизации наложенных сервисных сетей // T-Comm: Телекоммуникации и транспорт. 2015. Том 9. №6. С. 15-20.
2. **Дорт-Гольц А. А.** Анализ функционирования наложенных сетей в сетях операторов // Электросвязь. 2014. № 3, С. 22-26.
3. https://blog.greencloudvps.com/overlay-network-why-would-you-need-it.php.
4. https://studfile.net/preview/7715206/page:11/.
5. https://kevindarian.com/featured-post/pnetlab-setup-and-configuration-guide-2025-master-network-simulations/.