УДК 004.056

МОДЕРНИЗАЦИЯ АЛГОРИТМА ПРОЕКТИРОВАНИЯ РАСПРЕДЕЛЁННОЙ СЕТИ ПРЕДПРИЯТИЯ

Калужин Е.А., Чижевский В.В.

ФГОУ ВО «Дальневосточный Федеральный Университет»

E-mail:workout24@mail.ru

В настоящее время большое число предприятий имеют территориально распределенную структуру. При этом удаленно расположенные филиалы поддерживают связь по средствам сетевых технологий. Кроме того, сетевые технологии используются в локальных вычислительных сетях и позволяют пользоваться общими ресурсами: файловыми, почтовыми серверами, серверами обновлений, приложений и т.д. В существующих алгоритмах проектирования сети основное внимание уделяется высокой пропускной способности и отказоустойчивости. В данной работе предлагается модернизированный алгоритм проектирования защищенной сети предприятия, основанный на принципах полноты защищаемой информации, обоснованности и законности. Также данный алгоритм реализует принцип превентивности и включает этап анализа возможной реорганизации сетевой структуры.

Ключевые слова: сетевые угрозы, защита информации, распределенная сеть, техническая модель.

IMPROVING OF THE ALGORITHM OF DESIGNING A DISTRIBUTED ENTERPRISE NETWORK

Kaluzhin E.A., Chizhevskiy V.V.

Currently, a large number of enterprises have a territorially distributed structure. At the same time, remotely located branches maintain communication by means of network technologies. In addition, network technologies are used in local computer networks and allow using common resources: file, mail servers, update servers, applications, etc. The existing algorithms of network design focus on high bandwidth and fault tolerance. In this paper, we propose a modernized algorithm for designing a secure enterprise network, based on the principles of the completeness of the protected information, validity and legality. Also, this algorithm implements the principle of prevention and includes a stage of analysis of the possible reorganization of the network structure.

Keywords: network threats, information security, distributed network

Вся информация, передающаяся по сетевым каналам, может быть скомпрометирована, что ведёт к нарушению её конфиденциальности, целостности и доступности. Угроза информационной

безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности [1]. Сетевые угрозы возникают вследствие уязвимостей программного или аппаратного обеспечения, неграмотного проектировании сети или некомпетентных действий пользователей. Сетевые атаки становятся всё более изощрёнными, что требует современных подходов при проектировании защищенной сети предприятия.

Целью данной научной работы является модернизация тривиального алгоритма проектирования сети предприятия. Для достижения цели был проанализирован процесс проектирования корпоративной сети предприятия, изучены его основные этапы, выделены недостатки.

Проектирования корпоративной сети предприятия является сложной, требующей комплексного подхода задачей. Процесс проектирования можно представить в виде структурной схемы (Рисунок 1).

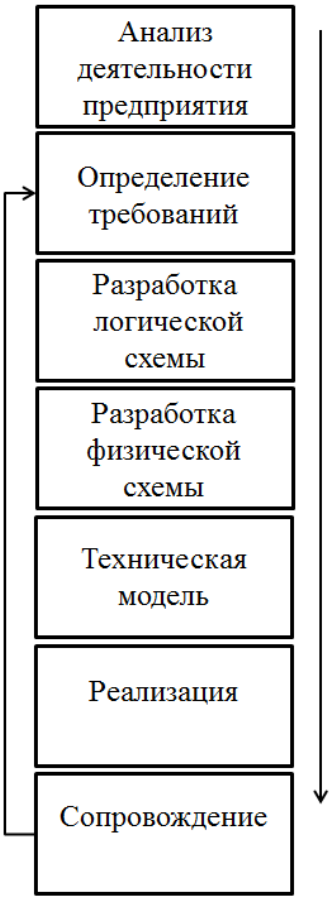

Рисунок 1 – Структурная схема создания корпоративной сети

При определении требований к проектируемой сетевой инфраструктуре проводится комплексный анализ предприятия, который включает в себя определение масштабов предприятия, задач сети, а также её сложности. В результате данного этапа специалист должен владеть

информацией о точном количестве филиалов, пользователей в каждом из них, примерном объеме циркулирующей информации, необходимых серверах и сервисах.

Под логической схемой сети понимается её организация на третьем (сетевом) и выше уровнях модели OSI [2]. Поэтому на этапе создания логической схемы продумывается ip-адресация, происходит разделение сети на виртуальные сети (VLAN), определяются места стыков внутренних сетей и каналов передачи данных. Пример логической схемы сетевой инфраструктуры изображен на Рисунке 2.

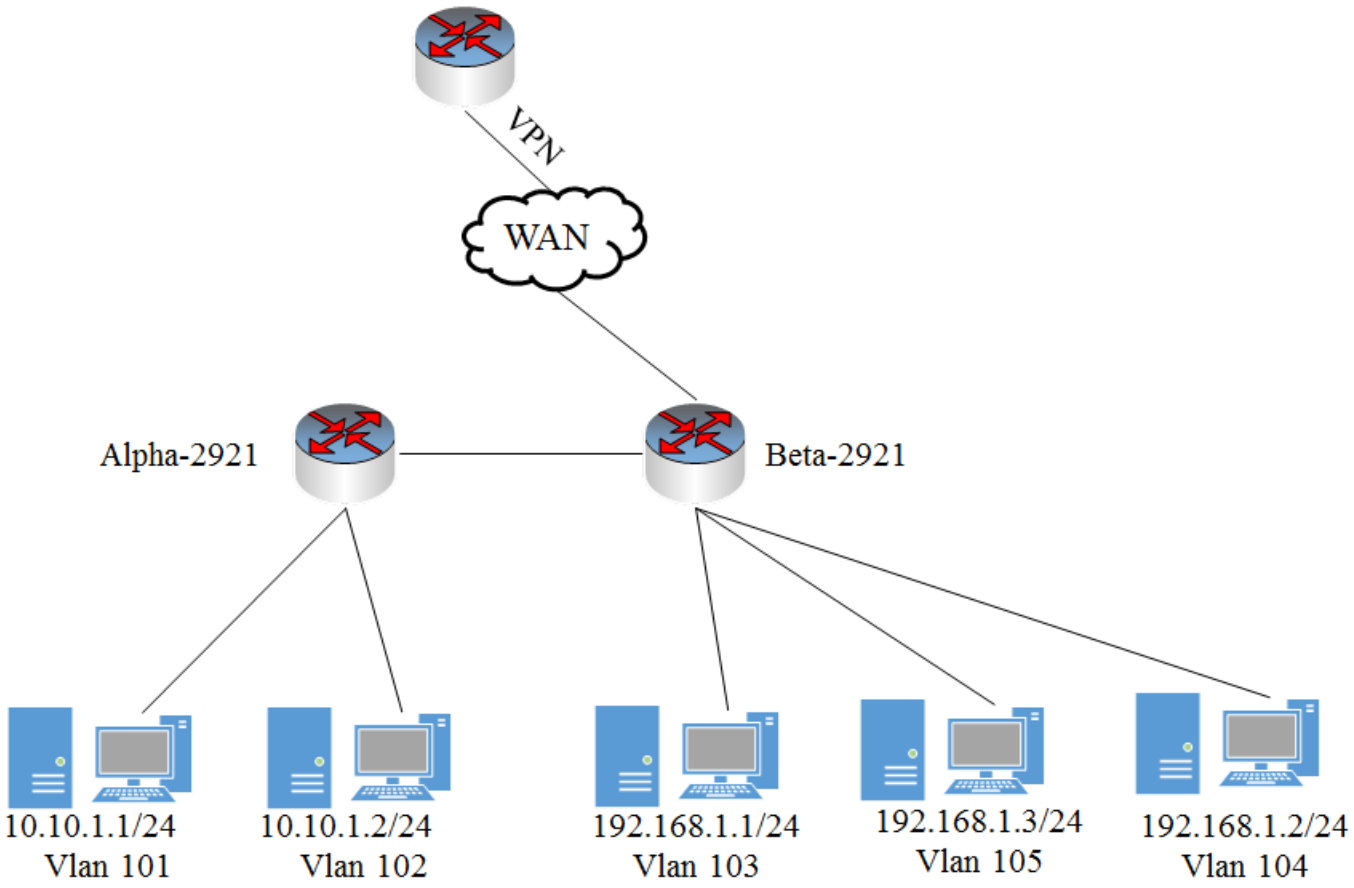

Рисунок 2 – Пример логической схемы сети

Такая схема демонстрирует разделение сети на подсети (VLAN), ip-адресацию этих подсетей, а также логическую связь сетевых шлюзов, работающих на третьем и выше уровнях модели OSI.

Физическая топология сети определяет схему соединения элементов кабелями. Она демонстрирует организацию на канальном и физическом уровне модели OSI [3]. При разработке физической топологии происходит планирование физического распределения сетевого оборудования, назначение физических портов. Пример физической схемы сетевой инфраструктуры изображен на Рисунке 3.

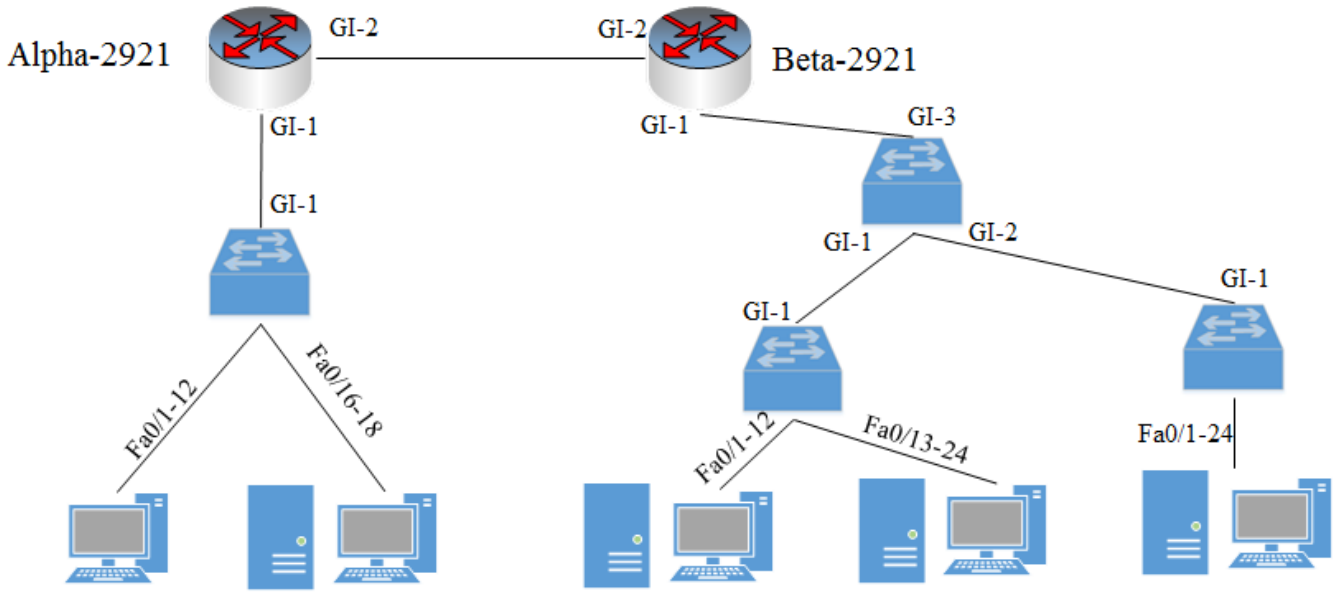

Рисунок 3 – Пример физической схемы сети

На такой схеме изображена структура соединения оборудования проводами, определены используемые и резервированные порты.

Техническая модель объединяет физическую и логическую схему. На данном этапе происходит выбор наиболее подходящего оборудования и написание технического задания. По завершении данного этапа у специалистов должен уже быть четкий план сети, перечень необходимых программных и аппаратных средств, а также техническое задание.

После этапа реализации, во время сопровождения может возникнуть необходимость в изменении структуры сети ввиду различных факторов, например, из-за интеграции новой информационной системы. Поэтому алгоритм является циклическим и имеет возврат к стадии определения требований.

Итак, данный алгоритм является универсальным и чаще всего используется при проектировании сетевой инфраструктуры предприятия. Безусловно, каждый объект является индивидуальным, поэтому возможно смещение вышеуказанных этапов, однако концепция остается неизменной. Основными недостатками подобного алгоритма проектирования сетевой инфраструктуры являются:

1. Отсутствие стадии разработки системы защиты информации. Как правило, при проектировании сетевой инфраструктуры предприятия малое внимание уделяется обеспечению информационной безопасности. Это вызвано необходимостью покупки дополнительных средств защиты и дополнительными затратами. Однако стоит отметить, что установка средств защиты в уже спроектированную систему требует её реорганизацию и влечет больше затрат.

2. Отсутствие стадии планирования расширения предприятия. Зачастую, многие компании присоединяют новые фирмы, открывают дополнительные филиалы, или же закрывают неприбыльные. Как правило, подобные варианты развития событий не учитываются на стадии разработки технической модели, поэтому после реализации и сдачи сети в эксплуатацию возникают проблемы с добавление новых компонентов и реорганизацией системы.

Очевидно, что для устранения вышеуказанных недостатков необходимо переработать алгоритм проектирование сетевой инфраструктуры, добавив дополнительные этапы. Таким образом, модернизированный алгоритм можно представить в виде структурной схемы (Рисунок 4)

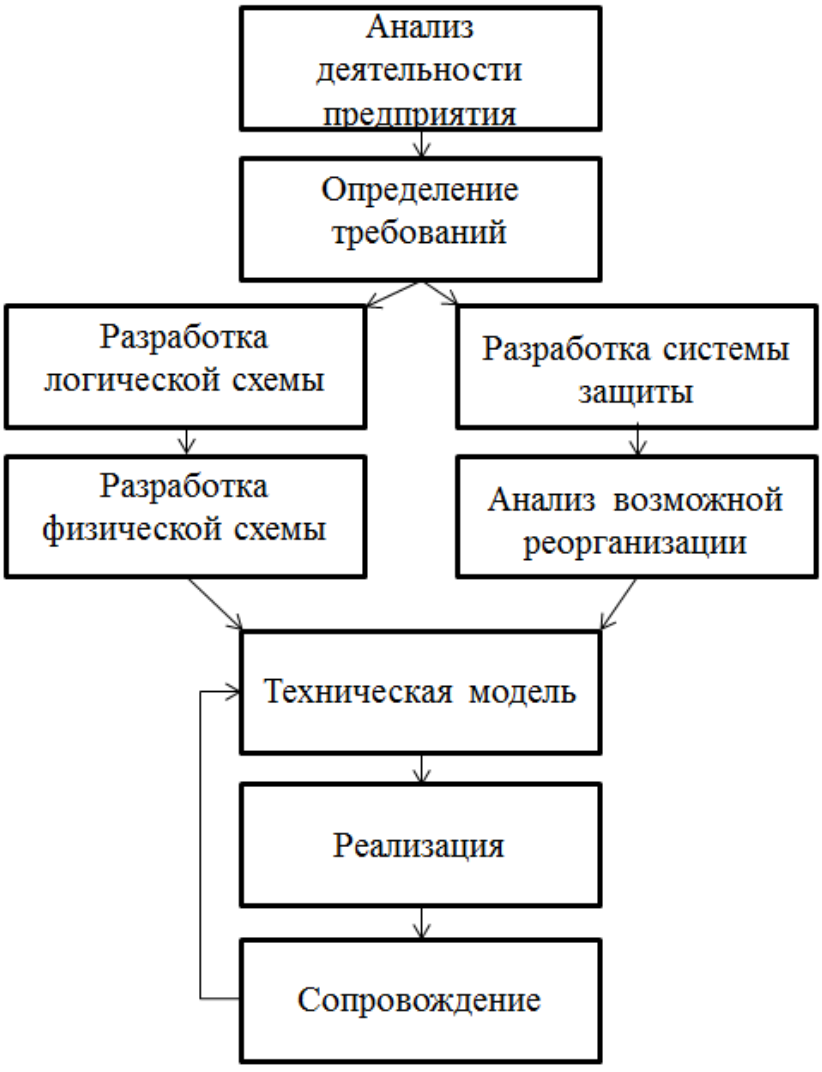

Рисунок 4 - Структурная схема создания защищенной сети

Согласно представленной схеме, процесс проектирования системы защиты информации и разработки топологии сети выполняются параллельно и вместе представляют собой техническую модель. Система защиты информации должна удовлетворять принципу полноты защищаемой информации, принципу обоснованности и принципу законности [4]. Принцип полноты защищаемой

информации заключается в том, что защищенность системы оценивается по защищенности самого уязвимого элемента. Принцип обоснованности несет следующий посыл: проектируемая система защиты должна соответствовать возможным угрозам и нарушителям. Поэтому необходимо провести анализ возможных нарушителей и актуальных угроз, в результате чего должны быть разработаны внутриорганизационные документы – модель нарушителя и угроз. Модель нарушителя позволяет ответить на вопросы «кто» и «с какой целью» может попытаться скомпрометировать информацию. Модель угроз позволяет получить картину актуальных угроз [5]. Кроме того, система защиты должна соответствовать принципу законности, т.е. должна соответствовать нормативно-правовым актам.

Анализ возможной реорганизации реализует принцип превентивности и позволяет быстро разработать новую техническую модель, при этом поддерживая уровень информационной безопасности на прежнем уровне.

Таким образом, предлагаемый алгоритм проектирования распределенной сети позволяет создать мобильную защищенную сеть, которую можно реорганизовать, подстроить под изменившуюся структуру предприятия оперативно и без дополнительных затрат.

Список литературы

1. Государственный стандарт Российской Федерации: «Защита информации». ГОСТР 50922-96 .

2. Э.Таненбаум, Д.Уэзеролл. Компьютерные сети. – СПб.: Питер, 2016. – 960 с.

3. Куроуз, Д. Компьютерные сети. Нисходящий подход / Д. Куроуз, К. Росс. - М.: Эксмо, 2016. - 912 с.

4. Гришина,М.В. Организация комплексной системы защиты информации: Учебное пособие.- Гелиос АРВ.-2007.-340 с.

5. Шаханова М.В. Современные технологии информационной безопасности: Учебно-методический комплекс.- ДВФУ.-2013.- 180 с.