решениями, в том числе SNMP, Syslog, NTP, Active Directory. Заявленная пропускная способность диода данных – 1 Гбит/с.

Преимущества решений AMT InfoDiode:

– интеграция с Active Directory, Syslog, SIEM-системами; формирование файла метаинформации для его анализа средствами DLP;

– возможность передачи данных SCADA-систем и OPC-серверов, поддержка FTP / FTPS, CIFS, SMTP, SFTP и др., а также промышленных протоколов; приоритизация передачи данных и потоков;

– поддержка сценариев репликации баз данных Microsoft SQL, PostgreSQL, сценариев передачи обновлений WSUS, антивирусов KPSN от Kaspersky, сценариев трансляции рабочего стола оператора за границу защищаемого сегмента;

– помехоустойчивое кодирование, резервное копирование настроек.

Среди представленных на рынке устройств, доступны также диоды данных, получившие сертификацию Минобороны России, и может применяться в сетях, где обрабатывается информация составляющая государственную тайну

Комплект изделия «Рубикон-ОШ» [5], выпускаемого компанией «Эшелон», состоит изо двух полукомплектов (передатчик и приёмник), соединённых с использованием специализированных оптических плат. Таким образом обеспечивается полная гальваническая развязка передающего и принимающего полукомплектов, находящихся в сегментах разного уровня секретности, с невозможностью прохождения сетевых пакетов в обратном направлении на физическом уровне. «Рубикон-ОШ» может функционировать в следующих режимах:

– передача сетевых пакетов через однонаправленную связь посредством маршрутизации IP;

– односторонняя передача файлов с одного FTP-сервера, подключённого к передающему комплекту ОШ, на другой FTP-сервер, подключённый ко принимающему комплекту ОШ;

– может выполнять функции маршрутизатора (коммутатора уровня L3);

– объединять физические интерфейсы в сетевой мост (коммутатор уровня L2);

– работать как межсетевой экран и система обнаружения и предотвращения вторжений;

Преимущества однонаправленного шлюза «Рубикон»:

– производительность межсетевого экрана до 8,5 Гбит/с;

– производительность системы обнаружения вторжений до 2,5 Гбит/с;

– наличие накопителя информации объёмом 1 ТБ;

– широкий выбор сетевых интерфейсов (6 медных портов RJ-45, 2 оптических порта 10G SFP+3;

– устройство сертифицировано Минобороны России и может применяться в сетях, где обрабатывается информация составляющая государственную тайну.

Рассмотрим зарубежные решения в области диодов данных.

Компания Owl Cyber Defense [8] является одним из крупнейших производителей диодов данных. В данный момент вендор предлагает широкую линейку устройств для однонаправленной передачи трафика, оптимизированных для различных задач. Флагманом модельного ряда является OPDS-1000. Система «всё в одном» в формфакторе 1U обеспечивает передачу данных со скоростью от 26 Мбит/с до 1 Гбит/с в зависимости от конфигурации. Устройство сертифицировано по критериям безопасности EAL4+ и обладает встроенной поддержкой протоколов UDP, TCP/IP, SNMP, SMTP, NTP, SFTP и FTP. Данное устройство изображено на рисунке 1.9.

Помимо этого, разработчик предлагает комплексные решения для однонаправленной передачи данных, состоящие из пар прокси-серверов на оборудовании Dell. Система позволяет организовать полноценное движение данных с возможностями расширенного управления электропитанием, резервного копирования и самозащиты устройств. Система Owl PaciT рассчитана на передачу «сырого» трафика.

1.4 Вывод

В результате проведенного анализа современного состояния науки и техники в области защиты информации посредством однонаправленной передачи данных, сделан вывод, что системы, содержащие в себе диод данных являются наиболее надежными для обеспечения конфиденциальности данных.

Также приведены основные принципы построения систем однонаправленной придачи данных и обозначены ограничения и технические сложности в процессе разработки подобной системы.

Таким образом, одной физической организации односторонней передачи данных недостаточно, нужен программно-аппаратный комплекс способный решать задачи по маршрутизации данных в сети, поддержанию современных протоколов передачи данных. Существующие аналоги поддерживают также распространенные протоколы TCP, FTP, HTTP, которые требуют наличие двунаправленной связи.

2 ОБОСНОВАНИЕ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ К ВЕДОМСТВЕННОЙ СЕТИ

Согласно техническому заданию, для маршрутизации пактов используется модель TCP/IP (Transmission Control Protocol/Internet Protocol).

Стек протоколов TCP/IP — сетевая модель, которая описывает процесс передачи цифровых данных. Регламентирует и описывает всю уровневую архитектуру и протоколы, входящие в стек, документ RFC 1122 [7]. В данной модели стандарт выделяет четыре уровня: канальный, межсетевой, транспортный и прикладной.

На канальном уровне модели TCP/IP на уровне сетевых устройств происходит обмен информацией, определяется как данные будут передаваться от одного устройства к другому. На данном уровне используется протокол Ethernet определенный в стандарте IEEE группы 802.3 [8]. Отправляющее и принимающее устройство в сети имеют определенные уникальные идентификаторы – MAC-адреса. Такие идентификаторы вместе с типом передаваемых данных и самими данными инкапсулируются в Ethernet. В следствие чего составляется фрагмент данных, который называется фреймом или кадром.

Межсетевой уровень позволяет устройствам из разных сетей взаимодействовать между собой, объединить локальные сети. Взаимодействие между сетями осуществляют пограничные и магистральные маршрутизаторы. Маршрутизатор отправляет пакет напрямую при условии, что устройство назначения находится в той же подсети, что и отправляющее устройство. Для того, чтобы определить к какой подсети принадлежит устройство назначения, маршрутизатор использует протокол интернета IP (Internet Protocol), описанный в документе RFC 791 [9]. Каждое сетевое устройство в глобальной сети имеет свой уникальный идентификатор – IP-адрес. Этот протокол необходим для определения и доставки данных к устройству назначения.

На транспортном уровне происходит передача пакетов между сетевыми устройствами с использованием протокола UDP (User Datagram Protocol). – очень быстрый протокол, поскольку в нем определен самый минимальный механизм, необходимый для передачи данных. UDP не требует открывать соединение, и данные могут быть отправлены сразу же, как только они подготовлены. UDP не отправляет подтверждающие сообщения. Этот протокол определен в RFC 768 [10].

На прикладном уровне модели TCP/IP происходит предоставление услуг пользователю или обмен данными по уже установленным соединениям.

File Transfer Protocol (FTP) – протокол передачи файлов по сети, описанный в спецификации RFC 959[11]. Протокол построен на архитектуре «клиент-сервер» и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером.

В качестве протокола динамической маршрутизации стека TCP/IP используется протокол OSPF (Open Shortest Path First) – основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути Алгоритм Дейкстры. Открытый протокол маршрутизации не устанавливает отдельных требований к расчету метрики и оценки маршрутов. Его стандарт определяет стоимость каждого пути. В случае прохождения маршрута через несколько соединений их стоимость суммируется. Оптимальным признается маршрут с наименьшей стоимостью. Протокол OSPF определен в RFC 2328 [12].

Данные через диод данных передаются с использованием технологии Fast Ethernet которая обеспечивает скорость передачи 100 Мбит/с. Данный стандарт описывается в IEEE 802.3 который содержит описание различных стандартов передачи данных посредством кабелей Ethernet. Для работы однонаправленного шлюза используются стандарты 100BASE-TX и 100BASE-FX описанные в стандарте IEEE 802.3u [13].

В качестве среды передачи 100BASE-TX применяются две витые пары. Одна линия используется для передачи данных, а вторая — для их приема. Спецификация содержит описания как экранированных, так и неэкранированных витых пар.

В сетях стандарта 100Base-FX используется волоконно-оптический, длиной сегмента до 412 метров. Стандарт определяет, что в кабеле имеются две жилы многомодового волокна – одна для передачи, а другая для приема данных.

Маршрутизация данных внутри каждой сети, реализуется на стандарте Gigabit Ethernet, который описан в документе IEEE 802.3ab [14]. Данный стандарт обеспечивает скорость передачи данных 1 Гбит/с.

Для реализации программы передачи и приема данных в сети используется язык программирования C++20, описанный в стандарте ISO/IEC 14882:2020 [15].

3 РАЗРАБОТКА И ОБОСНОВАНИЕ СТРУКТУРНОЙ СХЕМЫ ПРОЕКТИРУЕМОЙ СЕТИ

3.1 Разработка схемы сети

Для выполнения требований технического задания необходимо разработать структурную схему проектируемой сети. На рисунке 3.1 представлена разработанная схема сети.

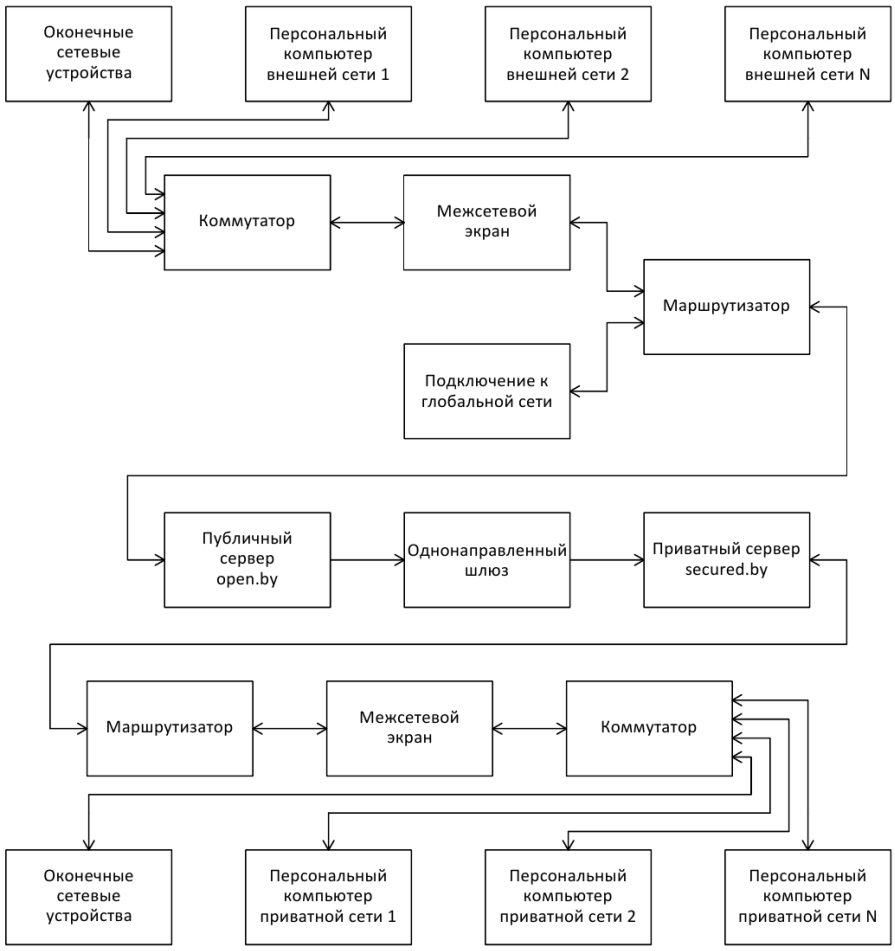

Рисунок 3.1 – Структурная схема сети

В представленной модели однонаправленной ведомственной сети важную роль играет диод данных, который позволяет осуществить фильтрацию трафика.

Согласно техническому заданию, в сети происходит односторонняя передача данных из публичной подсети в закрытую подсеть. Для передачи данных между подсетями в представленной модели ведомственной сети, используется FastEthernet, со скоростью работы до 100 Мбит/с, что соответствует техническому заданию.