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.

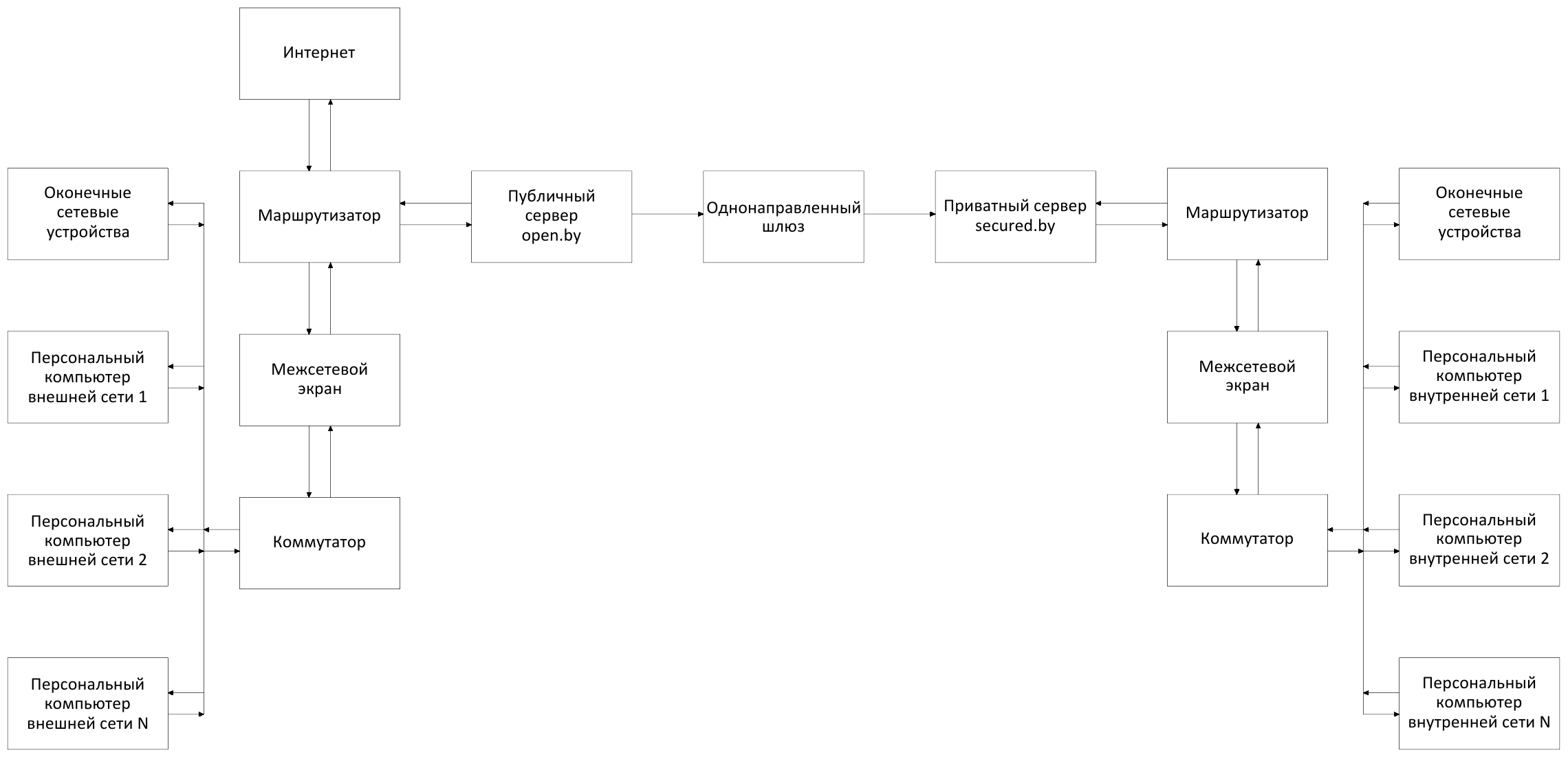


Рисунок 3.1 – Структурная схема сети

В представленной модели однонаправленной ведомственной сети важную роль играет диод данных (однонаправленный шлюз), 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.

Между публичной и закрытой сетью расположен программный однонаправленный шлюз, пропускающий данные только в направлении закрытой сети, предотвращая возможные утечки данных. В подсетях расположены два сервера. Сервер в публичной сети предназначен для передачи данных на сервер в закрытой сети. Публичная подсеть, изображена на рисунке 3.2.



Рисунок 3.2 – Публичная подсеть

В открытой сети находится ftp-сервер open.by c ipv4-адресом 192.168.100.10/28, позволяющий хранить, обрабатывать и передавать информацию. Устройства, находящиеся в одной сети с сервером, могут беспрепятственно публиковать данные в специальный каталог, размещенный на сервере. Защищенная сеть, изображена на рисунке 3.3.

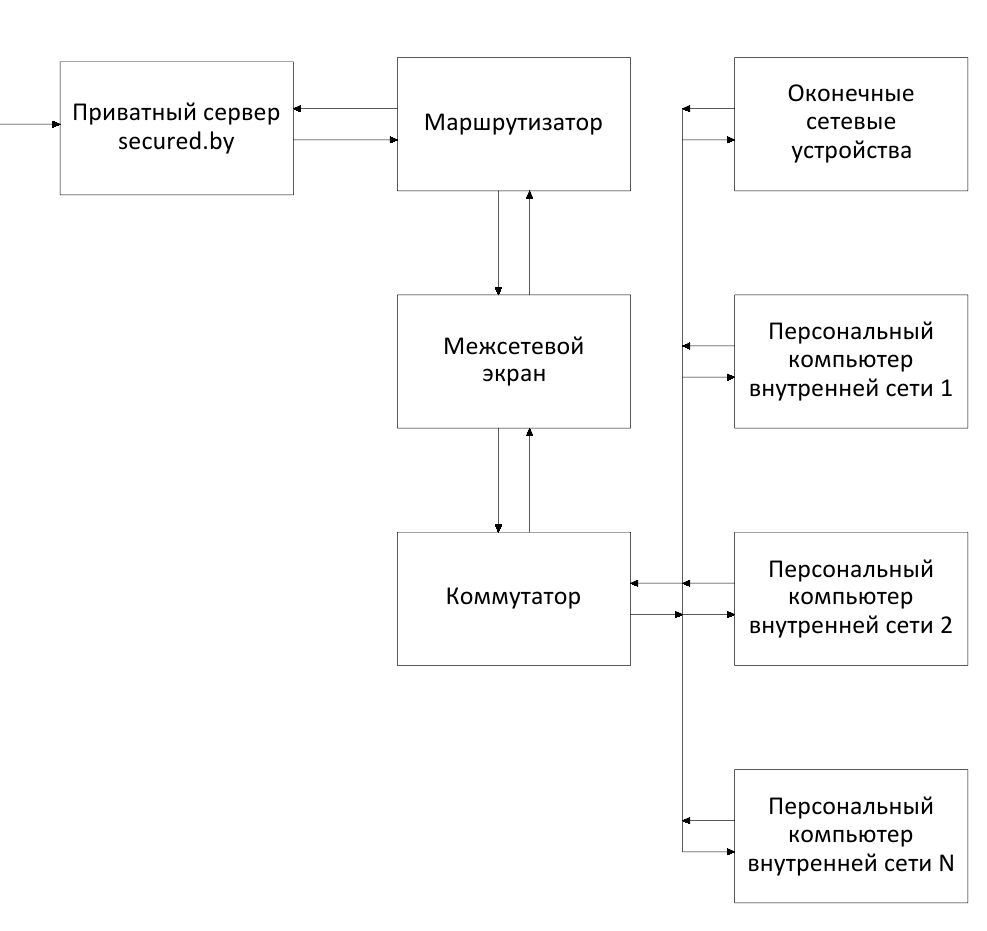


Рисунок 3.3 – Защищенная подсеть

В защищенной подсети расположен ftp-сервер secured.by c ipv4-адресом 192.168.50.10/28, который позволяет хранить информацию и передавать ее только в пределах своей сети.

Для демонстрации принципа работы сети, рассмотрим ситуацию, когда пользователю персонального компьютера внешней сети, расположенного в публичной сети, требуется передать данные на персональный компьютер внутренней сети, расположенный в приватной сети.

Для этого, на первом шаге, пользователь публичной сети, подключается к серверу open.by посредством протокола FTP и открывает каталог для отправки данных в защищенную сеть. Далее пользователь загружает необходимые данные на публичный сервер.

Программное обеспечение, размещенное на публичном сервере, в ходе запланированного сканирования каталога на предмет изменений или в ходе перехвата системного события записи файла в каталог, начинает отправку файла на удаленный сервер secured.by посредством пакетов UDP через диод данных. Движение трафика изображено на рисунке 3.4

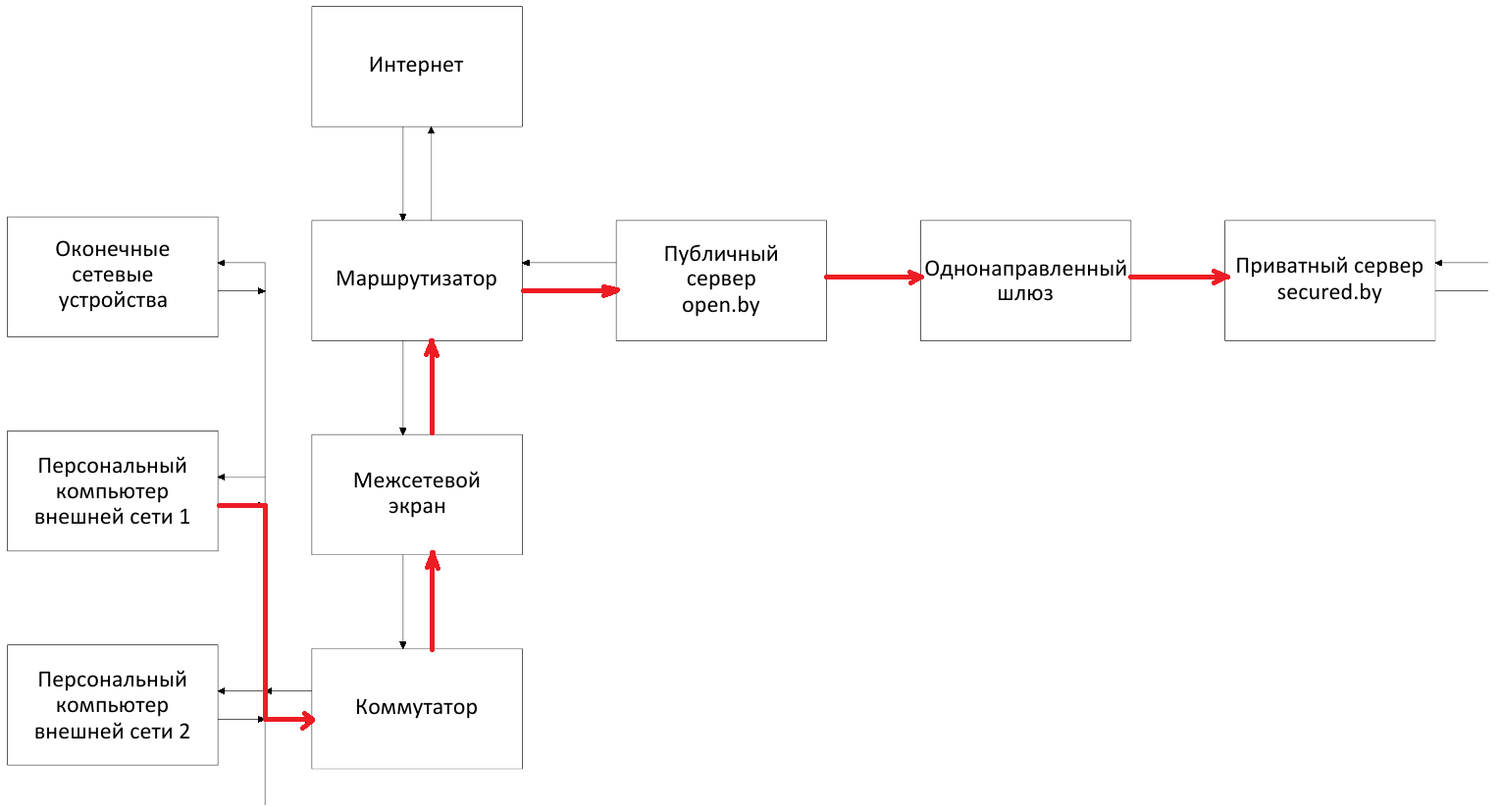


Рисунок 3.4 – Передача данных на сервер secured.by

В процессе передачи данных на сервере secured.by, создается, заполняется приходящими данными и проверяется на целостность приходящий файл. По завершению передачи пакетов, происходит копирование итогового файла из каталога «Downloading» в рабочий каталог.

После копирования, компьютер внутренней сети может получить доступ к каталогу на сервере secured.by. Схема передачи данных во внутренней сети описана на рисунке 3.5.

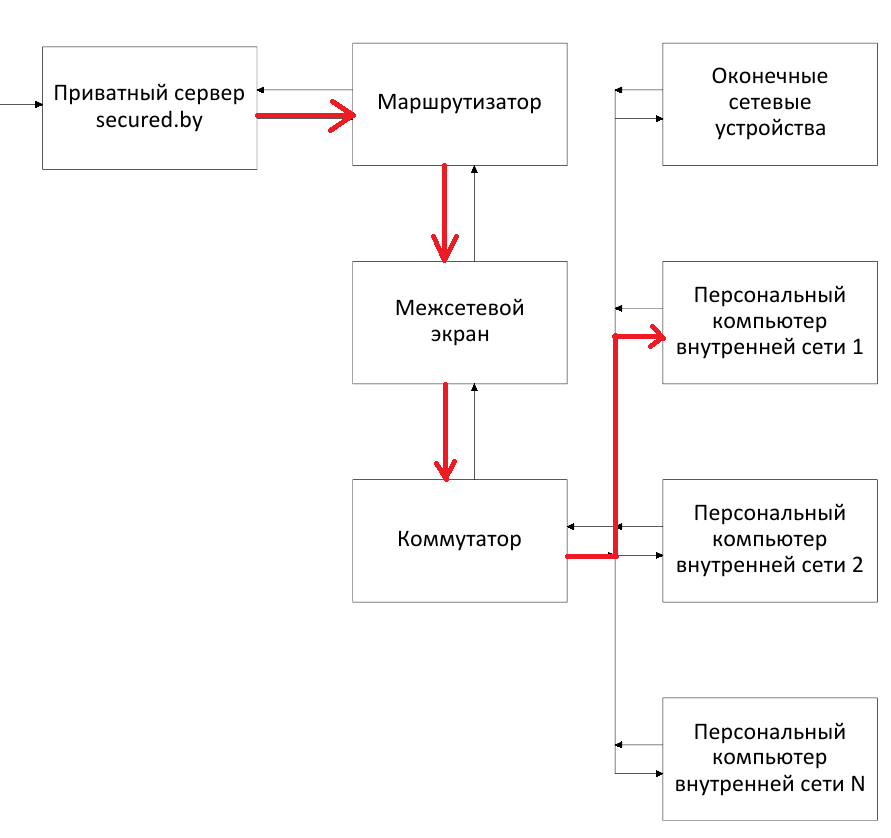


Рисунок 3.5 – Передача данных в приватной сети

3.2 Выбор оборудования

В качестве маршрутизатора используется Cisco C1111-4P – это современный высокопроизводительный беспроводной роутер, который входит в линейку оборудования Cisco 1100 Series Integrated Services Routers, которая ориентирована на филиалы, а также компании малого и среднего размера. Устройство имеет широкие функциональные возможности, и обеспечивает высокий уровень надёжности и сетевой безопасности.

Данный маршрутизатор обладает одним WAN портом Gigabit Ethernet и четырьмя портами LAN Gigabit Ethernet.

Коммутатор Cisco Catalyst 9200 (C9200L-24T-4G-A) – это стекируемый сетевой коммутатор корпоративного класса, предоставляющий расширенные функции безопасности, которые защищают целостность аппаратного и программного обеспечения, а также всех данных, проходящих через коммутатор.

Обладает 24 Ethernet портами с поддерживаемой скоростью до 1 Гигабит\с каждый. Таким образом, используя один коммутатор можно подключить большое число устройств к сети.

Сервер ProLiant DL180 Gen10 P35519-B21 – безопасный современный сервер. Отличается масштабируемостью, производительностью и надежностью, что делает его идеальной платформой для компаний, готовых к использованию локальных и гибридных облачных приложений.

В качестве однонаправленного шлюза используется СТРОМ-100, предназначенный для гарантированной однонаправленной передачи информации из открытых сетей в сети, в которых циркулирует информация ограниченного доступа. Помимо этого, возможно использовать диод данных для защиты сети при передаче из нее информации в открытые сети, в том числе подключенные к сети Интернет. При соединении сетей через однонаправленный шлюз в первом случае гарантируется отсутствие утечек из конфиденциальной сети, во втором - невозможность воздействия из открытых сетей на защищаемую сеть.

Внешний интерфейс устройства Ethernet 100BASE-TX.

Внутренний интерфейс Ethernet 100BASE-FX.

3.3 Вывод

Благодаря выбранному оборудованию можно организовать высокоскоростную передачу данных внутри защищенной и открытой сетей. Скорость работы диода данных ограничивает передачу информации между сетями 100 Мбит\с, что достаточно по техническому заданию. Для передачи данных из открытой сети в закрытую, необходимо использовать специальное программное обеспечение, которое позволит синхронизировать каталог закрытой сети с каталогом открытой сети.