СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Во время развития сетевых технологий прошлых поколений в основном решались проблемы технического характера. В следствие чего проектируемые системы на основе сетевых протоколов и стандартов прошлого всегда имеют уязвимости, которые могут быть обнаружены и использованы злоумышленником впоследствии. Из этого следует возможность взлома, компрометации, изменения и несанкционированного доступа к информации.

Проблема хранения конфиденциальных данных возникает в любой организации, работающей с информацией, потеря, утечка или искажение которой может привести к значительным последствиям. Диапазон принимаемых мер, варьируется от установки систем противодействия утечкам до принятия концепции нулевого доверия.

В настоящее время передовые методы защиты данных подразумевают возможность компрометации любого участка защищенной системы. Несмотря на технический прогресс в области защиты информации и сетевых технологий, даже новейшая инфраструктура нуждается в регулярных обновлениях программно-технического комплекса и отслеживания новых методик противодействия атакам. При этом подобный комплекс мер не ограничивает возможность злоумышленнику, внедренному в организацию, распространить данные за пределы внутренней сети.

Изоляция сети – наиболее эффективный метод борьбы с утечками. Даже в случае полной компрометации внутренней сети, злоумышленник не сможет передать конфиденциальные данные за пределы локальной сети. К сожалению, даже полностью изолированная система нуждается в доступе во внешний мир для выполнения своих функций. Данную проблему можно решить посредством физических накопителей, однако подобное решение не дает гарантий того, что данный накопитель не станет хранилищем конфиденциальной информации из внутренней сети, создавая возможность потери данных.

Для решения проблемы невозможности работы полностью изолированной сети используют методы однонаправленной передачи данных. Термин «Диод данных[1]» означает систему, в которой данные могут передаваться только в одном направлении, полностью блокируя любые возможности обратной передачи данных. Таким образом, даже в случае полной компрометации внутренней сети, передать данные во внешний мир не представляется возможным, предотвращая возможную утечку данных.

Диоды данных могут быть выполнены в программном или аппаратном варианте. В случае аппаратной реализации, корпус содержит интерфейсы для

подключения принимающей и передающей сети, а также разъём питания. Недостатком подобных устройств является невысокая скорость их работы, а также необходимость использования специальных протоколов передачи данных, не нуждающихся в обратном канале связи.

Программный диод данных – это сетевое устройство, в котором ограничение на передачу информации определяется логикой работы прошивки или конфигурации. Данный фактор позволяет реализовывать однонаправленную сеть на уже существующей инфраструктуре. Недостатком подобной системы, является теоретическая возможность утечки информации через обратный канал.

Так как большинство современных протоколов передачи данных общего назначения требует наличие двунаправленной связи, диод данных не может работать напрямую с распространёнными протоколами TCP, FTP, HTTP и нуждается в программно-аппаратном комплексе.

Реализуется подобный комплекс на базе прокси серверов, которые эмулируют работу TCP, SMB и других стандартов передачи данных. Дополнительным достоинством данной системы является возможности контроля входных данных, их мониторинга и фильтрации.

Диоды данных могут использоваться не только для защиты конфиденциальных данных, но и для защиты устройств от несанкционированного доступа. В случае работы с производственной инфраструктурой, возникает задача защиты устройств от возможности изменения их конфигурации удалённо. Для этой цели диод данных передаёт данные от датчика или системы отслеживания во внешнюю сеть, однако предотвращает возможность получения доступа к конфигурации устройства.

Цель дипломной работы – исследование принципов работы однонаправленных сетей и реализация программного комплекса для работы однонаправленной ведомственной сети.

Задачи дипломной работы:

– сравнительный анализ существующих систем однонаправленной передачи данных.

– разработка системы однонаправленной передачи данных по техническому заданию

– проведение технико-экономических обоснований исследования и разработки системы однонаправленной передачи данных.

1 СРАВНИТЕЛЬНЫЙ АНАЛИЗ АНАЛОГИЧНЫХ СИСТЕМ (УСТРОЙСТВ)

1.1 Анализ существующих систем защиты данных

Однонаправленная передача данных в закрытую сеть является частным случаем системы разграничения доступа. Подобными свойствами обладают межсетевые экраны и системы контроля трафика внутри локальной вычислительной сети. Таким образом, корректно сравнение разрабатываемой системы с межсетевыми экранами и другими методиками разграничения доступа к данным по сети.

В патенте «RU2712815 Защита сетевых устройств посредством межсетевого экрана» [2] приведена система, в которой посредством внедрения между внешней сетью и защищаемой сетью специального узла «Модуль Администрирования» происходит контроль трафика. Пример предлагаемой в патенте системы представлен на рисунке 1.1.

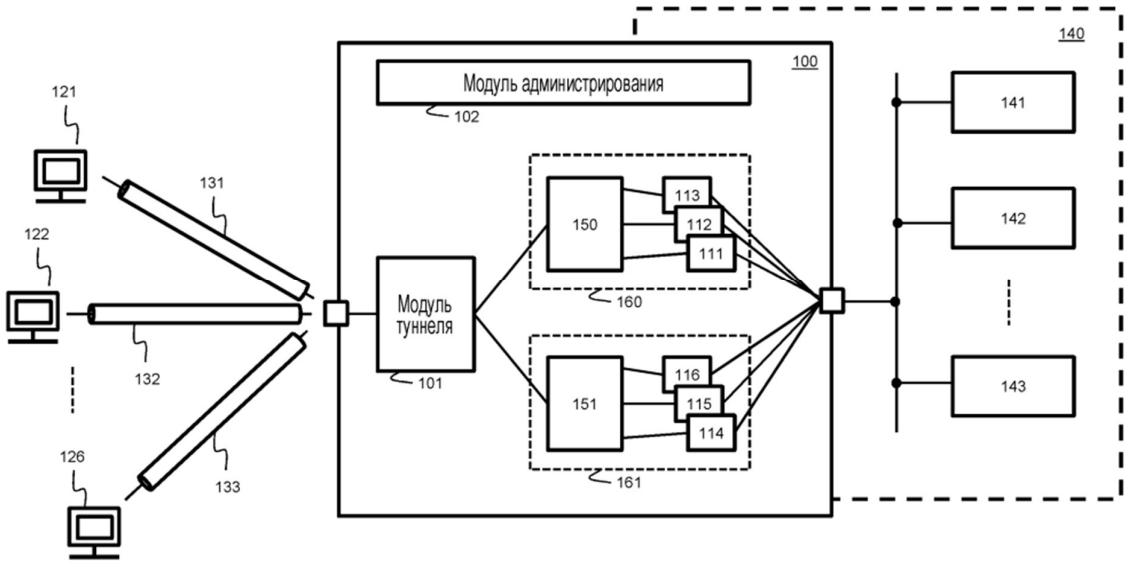

Рисунок 1.1 – Пример системы для защиты сетевых устройств от нежелательного сетевого доступа

В данном примере, три сетевых устройства (серверы 141, 142 и 143 приложений) являются частью частной сети 140. Доступ к серверам 141-143 получается изнутри частной сети 140 через частный сетевой адрес. Другими словами, адресация серверов 141-143 приложений не может быть осуществлена посредством их частных сетевых адресов извне частной сети 140. Частная сеть 140 отделена от внешней сети шлюзом 100, тем самым

обеспечивая прохождение трафика между внешней сетью и сетью 140 управляемым образом.

Предложенная система может идентифицировать клиентов 121-126 в качестве «доверенных клиентов» с правами доступа к одному или более из серверов 141-143 приложений внутри частной сети 140 для того, чтобы использовать функционирующие на них службы.

Для того чтобы управлять доступом клиентов 121-126 к серверам 141-143 приложений, сетевые туннели 131-133 создаются между клиентами 121-126 и шлюзом 100. Таким образом, частная сеть 140 расширяется для клиентов 121-126. Вследствие этого, клиенту 121-126, несмотря на то, что физически он не находится в частной сети 140, предоставляется адрес частной сети в диапазоне частной сети 140, и может, следовательно, потенциально осуществлять доступ к всем серверам 141-143 приложений посредством их соответствующего адреса частной сети.

Процесс создания сетевого туннеля между сетями представлен на рисунке 1.2.

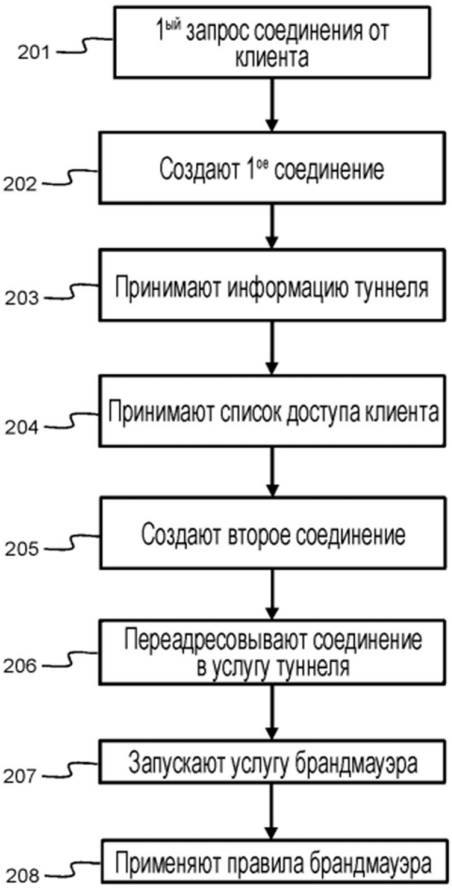

Рисунок 1.2 – Структурная схема создания сетевого туннеля между клиентским устройством и частной сетью

Посредством данного процесса, клиентское устройство 121-126 соединяется с частной сетью 140 через шлюз 100. На первом этапе 201, модуль 101 туннеля принимает первый запрос соединения от клиентского сетевого устройства 121, чтобы создать первое сетевое соединение со шлюзом 100. За этим, сетевое соединение создается на этапе 202. Данное первое сетевое соединение используется, чтобы осуществлять обмен информацией управления между клиентом 121 и шлюзом 100, и, в частности, с модулем 102 администрирования, реализованным в шлюзе 100. Для того, чтобы знать, что соединение служит для целей управления, модуль туннеля может инспектировать первый пакет данных, обмен которым осуществляется через каждое вновь созданное сетевое соединение. Если пакет данных является пакетом данных управления, модуль 101 туннеля идентифицирует сетевое соединение в качестве соединения управления и будет перенаправлять все дальнейшие пакеты, принимаемые через данное соединение, модулю 102 администрирования.

Представленная в патенте система позволяет гибко настраивать правила передачи данных в сети, а также проводить анализ передаваемого трафика. Данная особенность позволяет реализовать системы защиты от утечек, гибко разграничивать возможность получения данных используя систему авторизации, а также вести мониторинг получения доступа к данным, для своевременного обнаружения попытки произвести утечку данных.

Несмотря на расширенные возможности контроля трафика в сети, данная система имеет ряд уязвимостей, которые позволяют произвести атаку на защищаемые данные с целью уничтожения, модификации или хищения. Наличие слоя между защищаемой сетью и внешним миром, не способно предотвратить попытку передачи конфиденциальных данных во внешний мир со стороны защищаемой сети. Также данная система нуждается в регулярных обновлениях программно-технического комплекса, что, впрочем, не означает абсолютную защиту от взлома одного или нескольких устройств внутренней сети.

Таким образом, данная система лучше подходит для организации работы удаленных сотрудников, так как предоставляет удобный способ доступа во внутреннюю сеть. По этой же причине, данная система не может предоставить абсолютную защиту конфиденциальных данных, и не может использоваться в сетях, где отсутствие возможности утечки, важней удобства доступа к защищаемой информации.

В патенте «RU2607997C1 Система защиты компьютерных сетей от несанкционированного доступа» [3] приведено устройство которое представляет собой межсетевой фильтр, включаемый между двумя компьютерными сетями таким образом, что весь обмен информацией между

указанными сетями ограничивается с помощью правил фильтрации, при этом межсетевой фильтр содержит по меньшей мере два сетевых интерфейса для обмена данными между клиентами первой компьютерной сети и второй компьютерной сети из двух. Устройство дополнительно содержит узел обработки трафика, включающий устройство управления, обеспечивающее ввод правил фильтрации трафика и хранение информации о правилах фильтрации, устройство анализа трафика, обеспечивающее проверку соответствия поступающей информации правилам фильтрации, а также коммутирующее устройство, через которое указанные сетевые интерфейсы соединены между собой и которое обеспечивает прохождение разрешенной правилами фильтрации информации между сетевыми интерфейсами и блокировку неразрешенной правилами фильтрации информации, при этом правила фильтрации запрещают транзитную передачу любых пакетов между указанными сетевыми интерфейсами кроме тех, которые имеют разрешенные признаки и параметры адресации в своих заголовках, форму информационной части пакета, соответствующую шаблону, хранящемуся в памяти межсетевого фильтра, а также параметры запроса или ответа, соответствующие множеству разрешенных значений, хранящихся в памяти межсетевого фильтра.

Схема подключения компьютерной сети к представленному устройству представлено на рисунке 1.3.

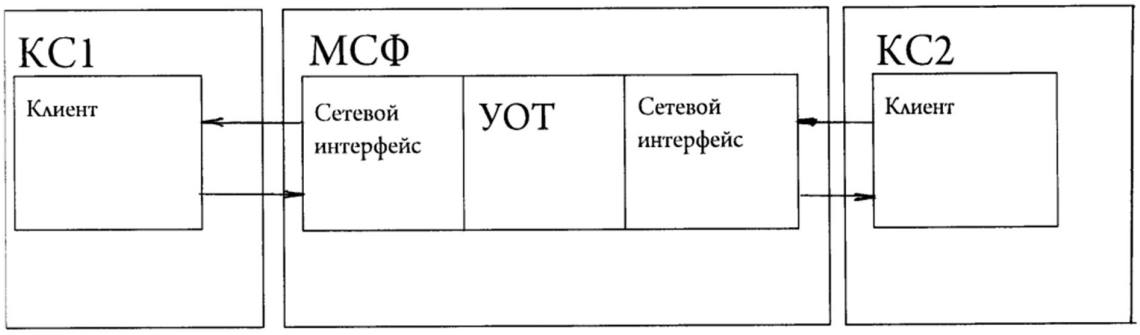

Рисунок 1.3 – Структурная схема подключения компьютерной сетей к устройству фильтрации трафика

Согласно разработке для управления процессами фильтрации трафика МСФ содержит специальный узел обработки трафика (УОТ), устройство управления которого информационно изолировано от сетевых интерфейсов, а взаимодействие с ним осуществляется через отдельный интерфейс управления. Все изменения программы фильтрации трафика, а также управление соединениями могут быть выполнены исключительно через интерфейс устройства управления УОТ, что полностью устраняет возможность несанкционированного доступа с МСФ со стороны сетей КС1 и КС2.

1.2 Принципы построения однонаправленных сетей

Документ «Unidirectional Networking»[4] от GIAC (Global Information Assurance Certification) описывает процесс разработки и возможные сложности в процессе реализации однонаправленной системы передачи данных. В данной работе предлагается рассматривать двунаправленное оптическое подключение, как пару отдельных однонаправленных каналов как показано на рисунке 1.4.

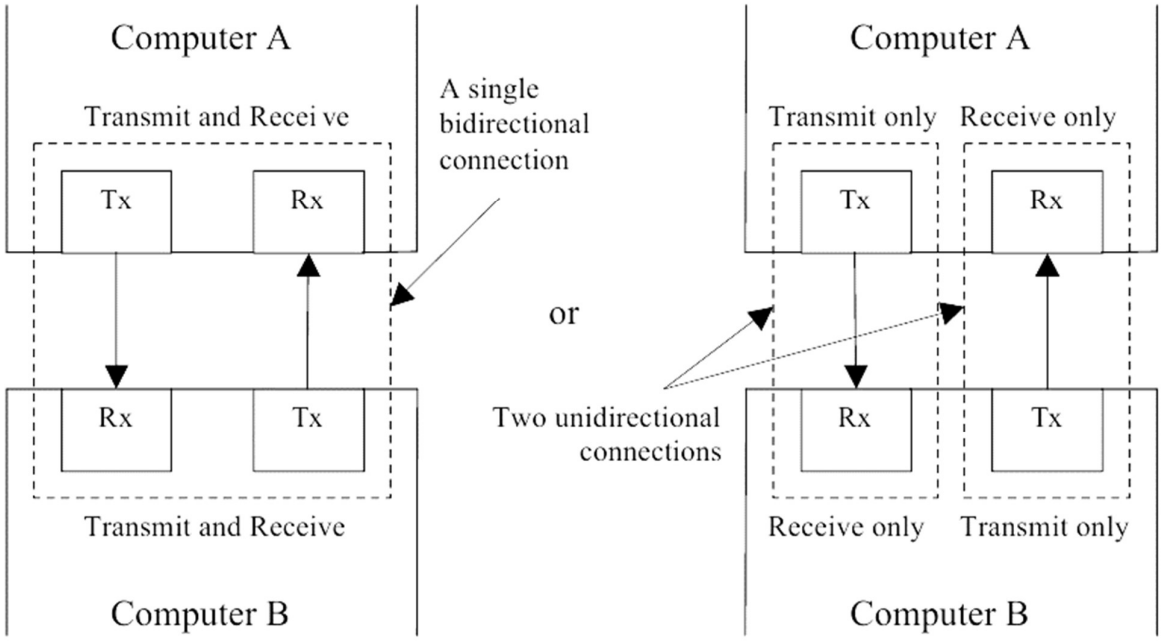

Рисунок 1.4 – Двунаправленное соединение как два однонаправленных соединения

Путем отключения одного из каналов, компьютеры будут соединены одним каналом, в который только один из компьютеров сможет передавать данные, а другой только принимать.

Для работы через однонаправленную сеть, нужно использовать протокол без активного подключения, а каждый передаваемый пакет воспринимать независимо. UDP не смотря на то, что является протоколом без необходимости наличия открытого соединения, однако, это вовсе не означает, что на реальных устройствах он реализован как полностью однонаправленный. В случае некоторых операционных систем, отсутствие ответа на отправку UDP приведет к внутренней ошибке.

В качестве метода обеспечения однонаправленной передачи данных, рекомендуется разместить аппаратный диод данных между устройствами, для

обеспечения гарантии, того, что данные не могут быть отправлены в обратном направлении. Подключение диода данных в систему показано на рисунке 1.5.

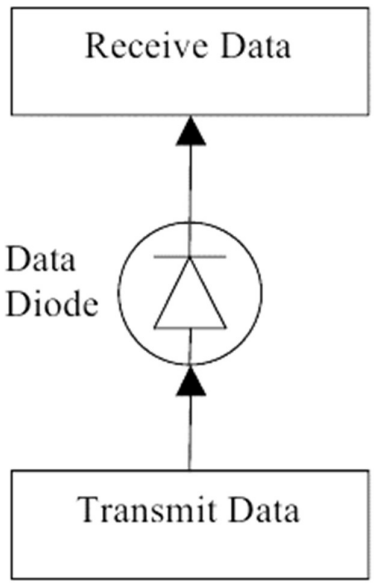

Рисунок 1.5 – Методика подключения диода данных в сеть

Если сетевое устройство не может принимать данные, то невозможно удаленно выполнять инструкции. С точки зрения удаленного устройства, нет способов изменить данные на передающем устройстве, без наличия физического доступа.

С точки зрения безопасности, компьютер, который может только принимать данные, может считаться конфиденциальным для внешнего пользователя. Если злоумышленник не может получить никакой информации о удаленном компьютере, то не сможет провести эффективную атаку на защищенный компьютер. Единственный способ просматривать информацию с защищенного таким образом компьютера – получение физического доступа. Теоретически возможна атака, в случае если злоумышленник обладает полным знанием о приемной стороне, но практически невозможна в случае, если злоумышленник с ней не знаком. Однако даже в данном случае, произвести утечку данных не получится. Таким образом, для внешнего пользователя, данный компьютер полностью конфиденциален.

Возникает множество практических проблем, когда сеть работает только в одном направлении. При использовании оптических сетевых карт, сигнал несущей предается по линии передачи. В случае отсутствия несущей на линии приема, сетевая карта не будет передавать данные. Для того, чтобы оптическая сетевая карта производила передачу, одним из решений предлагается

использование несущей из другой сетевой карты на стороне передачи. Схема подключения представлена на рисунке 1.6.

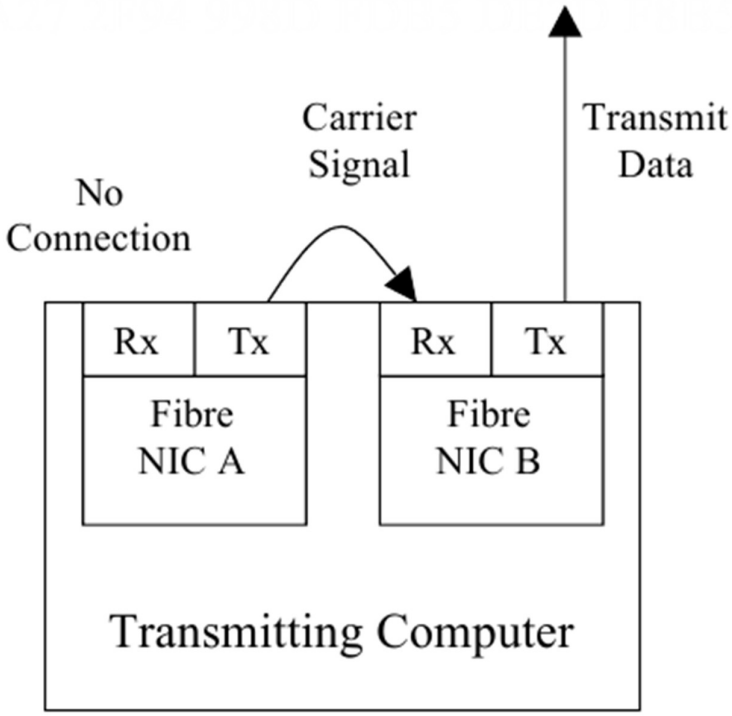

Рисунок 1.6 – Решение проблемы отсутствия, несущей на приемной стороне передатчика

Невозможно гарантировать отсутствие ошибок при передаче данных через однонаправленную сеть. Даже в случае, если принимающий компьютер может понять, какие данные повреждены или утеряны, нет способа, которым он мог бы об этом сообщить источнику.

Потеря данных может быть минимизирована использованием избыточности, через передачу данных больше, чем один раз, или с передачей дополнительной информации, такой как кода FEC (Forward Error Correction), для восстановления утерянных данных.

Для того, чтобы компьютер имел возможность принять пакет, он должен иметь MAC адрес на сетевой карте. MAC адрес это уникальный идентификатор выданный каждому сетевому устройству и используется для соединения данных на втором уровне OSI для идентификации каждой сетевой карты в сети.

Протокол определения адреса (ARP) используется устройствами для того, чтобы создать ассоциацию между MAC адресом и IP адресом устройства. Компьютер, который может производить обмен данными только в одном

направлении не может использовать ARP для определения MAC адреса принимающего компьютера, так как не способен получить ответ на ARP запрос.

Для того, чтобы обойти данное ограничение можно воспользоваться несколькими путями:

– Вручную настроить таблицу определения адреса на передающем узле

– Настроить сетевую карту так, что любая информация, полученная на нее, будет принята вне зависимости от адресата.

– Убедится, что передающая сторона и приемная сторона находятся в одной подсети и использовать широковещательный адрес.

Таким образом, используя однонаправленное соединение можно подключить незащищенную сеть к защищенной и гарантировать конфиденциальность защищаемой сети. Использование однонаправленной передачи данных значительно ограничивает число возможных сетевых уязвимостей.

1.3 Анализ существующего рынка аппаратных диодов данных (однонаправленных шлюзов)

Диод данных предназначен для гарантированной однонаправленной передачи информации между защищённым сегментом сети и внешними сетевыми устройствами.

Системы, содержащие в себе диод данных можно разделить на несколько типов:

– Для защиты от утечек данных

Для защиты конфигурации оборудования

– Для систем репликации

В первом случае данные могут только поступать в защищенную сеть, не позволяя произвести утечку. Во втором случае, данные с датчиков или системы трекинга свободно проходят диод данных, однако для изменения конфигурации оборудования потребуется наличие физического доступа к устройству. В случае систем репликации, использование диода данных не позволит злоумышленнику получить доступ к исходному серверу.

Первые диоды данных появились ещё в конце прошлого века, однако широкое распространение такие устройства получили с ростом числа целевых кибератак на объекты критической инфраструктуры. Возможно, именно поэтому мировой рынок инструментов для однонаправленной передачи данных в последние годы демонстрирует стабильный рост. Вместе с тем

объёмы продаж в сегменте диодов данных невелики по сравнению с другими сферами информационной безопасности.

Наибольшее число заказчиков диодов данных сконцентрировано в энергетическом секторе, нефтегазовых компаниях, государственных организациях и предприятиях, эксплуатирующих объекты критической инфраструктуры. Производственные и транспортные компании, использующие большое количество промышленных датчиков и программируемых контроллеров, вкладываются в защиту таких устройств от направленных проникновений и кражи данных. Вопросы информационной безопасности устройств автоматизации с каждым годом приобретают всё большее значение. Главным драйвером мирового рынка диодов данных специалисты называют возросшую активность киберпреступников, атакующих нефтегазовый сектор. Подключение предприятий отрасли к технологически сложным решениям, таким как IoT, призвано увеличить производительность и снизить затраты, но одновременно делает их более уязвимыми к кибератакам. Действия злоумышленников способны остановить деятельность компании, что может привести к огромным финансовым, репутационным и — в некоторых случаях — человеческим потерям, а также к экологическим катастрофам.[5]

Ключевыми вендорами, поставляющими диоды данных, являются компании: Advenica AB. BAE Systems. Belden. Deep Secure. Fibersystem. Forcepoint. Fox-IT. Garland Technology. Nexor. OPSWAT. Owl Cyber Defense. Siemens. ST Engineering. Waterfall.

В странах СНГ также существуют компании разрабатывающие и поставляющие диоды данных для внутреннего рынка. Большинство компаний работает в России.

Использование таких устройств в России предусматривается нормативными документами, регулирующими безопасность в государственных информационных системах и обработку персональных данных. Скорее всего, именно приказы ФСТЭК России № 17, 21 и 31 лучше всего стимулируют спрос на такие устройства на отечественном рынке. Для организации доступа к информации, содержащей государственную тайну, оборудование должно быть сертифицировано ФСТЭК России с указанием уровня контроля.

В России диоды данных выпускают как минимум пять производителей: «АйТи БАСТИОН». «АМТ-Груп». «Ореол Секьюрити». «Росэлектроника». «СиЭйЭн». «Эшелон». «Центр безопасности информации».

Компания «АМТ-Груп» предлагает линейку аппаратных и программно-аппаратных решений для однонаправленной передачи данных под брендом InfoDiode.[6] Они предназначены для организации обмена данными со

критически значимыми сегментами. Все системы сертифицированы ФСТЭК России по ТУ и уровню доверия 4. На рисунке 1.7 представлен диод данных AMT InfoDiode RACK single.

Рисунок 1.7 – AMT InfoDiode RACK single

Решения «АМТ-Груп» поддерживают передачу как стандартных транспортных протоколов (FTP / FTPS, CIFS, SMTP, SFTP, StartTls, IPsec, UDP), так и специализированных для SCADA-систем и OPC-серверов промышленных протоколов (OPC UA, Modbus, MQTT). Диоды могут быть «из коробки» интегрированы с различными прикладными сервисами и 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», выпускаемого компанией «Эшелон»[7], состоит из 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

Схема подключения устройства «Рубикон-ОШ» представлена на рисунке 1.8.

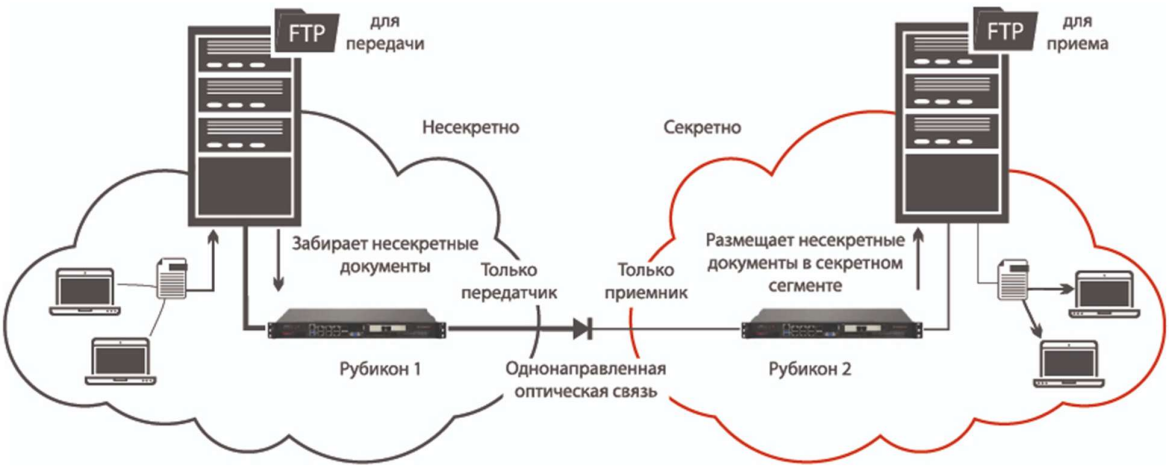

Рисунок 1.8 – Схема подключения устройства «Рубикон-ОШ»

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.

Рисунок 1.9 – Диод данных OPDS-1000 компании Owl Cyber Defense

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.

Преимущества устройств Owl Data Diode:

– Большое количество поддерживаемых протоколов.

– Сертификация EAL4+.

– Собственная защищённая операционная система Talon для безопасного администрирования устройств.

– Наличие широкого спектра приложений и коннекторов для расширения функциональных возможностей и интеграции с другими системами.

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 ВЕДОМСТВЕННОЙ СЕТИ

Исходя из предыдущего раздела, сделан вывод, о том, что на рынке широко представлены решения для однонаправленной передачи данных. Для создания независимой от производителя сети, был выбран вариант с использованием серверов: один открытый и один закрытый.

Структура сети представлена на рисунке 2.1

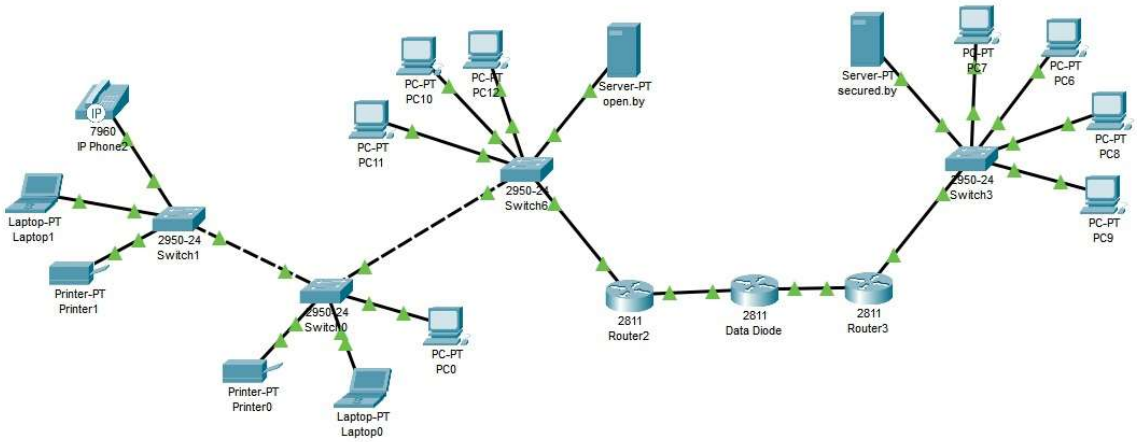

Рисунок 2.1 – Модель локальной вычислительной сети

2.1 Выбор маршрутизатора

Cisco C1111-4P[9] – 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. Маршрутизатор представлен на рисунке 2.1.1.

Рисунок 2.1.1 – Маршрутизатор CISCO C1111-4P

Технические характеристики маршрутизатора CISCO C1111-4 представлены в таблице 2.1.

Таблица 2.1.1 – Технические характеристики маршрутизатора CISCO.

Параметр	Значение
Тип установки	Настольное
Универсальные порты Ethernet	1 x SFP combo
WAN порты Ethernet	1 x GE
LAN порты Ethernet	4 x GE
Память FLASH	4 Гб
Память FLASH максимум	4 Гб
Объем ОЗУ	4 Гб
Память ОЗУ максимум	4 Гб
Потребляемая мощность	12,5 Вт
Порты USB	1 x USB 3.0
Высота, мм	42
Размеры (В x Ш x Г), мм	42 x 323 x 230
Тип питания	AC 100-240В

2.2 Выбор коммутаторов

Cisco Catalyst 9200 (C9200L-24T-4G-A)[10] – это стекируемый сетевой коммутатор корпоративного класса, предоставляющий расширенные функции безопасности, которые защищают целостность аппаратного и программного обеспечения, а также всех данных, проходящих через коммутатор. Коммутатор представлен на рисунке 2.2.1.

Рисунок 2.2.1 – Коммутатор Cisco Catalyst 9200

Технические характеристики коммутатора Cisco Catalyst 9200 представлены в таблице 2.2.1.

Таблица 2.2.1 – Технические характеристики коммутатора CISCO.

Параметр	Значение
Тип установки	Стоечное
Универсальные порты Ethernet	24 x GE RJ-45
WAN порты Ethernet	4 x 1GE
LAN порты Ethernet	24 x Ethernet 10/100/1000
Память FLASH	4 Гб
Память FLASH максимум	4 Гб
Объем ОЗУ	2 Гб
Память ОЗУ максимум	2 Гб
Потребляемая мощность	12,5 Вт
Порты USB	2 x USB 3.0
Высота, мм	444
Размеры (В x Ш x Г), мм	444x44x288
Тип питания	AC 100-240В

2.3 Выбор сервера

ProLiant DL180 Gen10 P35519-B21[11] – безопасный современный сервер. Отличается масштабируемостью, производительностью и надежностью, что делает его идеальной платформой для компаний, готовых к использованию локальных и гибридных облачных приложений. Таким компаниям требуется оптимальное сочетание вычислительных ресурсов и систем хранения данных для достижения важнейших целей. Сервер изображен на рисунке 2.3.1

Рисунок 2.3.1 – Сервер HPE ProLiant DL180 Gen10 P35519-B21

Основные технические характеристики сервера занесены в таблицу 2.2.3

Таблица 2.3.1 – Технические характеристики сервера.

Параметры	Значение
Процессор	Intel Xeon Silver 4210R 2,4ГГц
Тактовая частота процессора	2400МГц
Количество разъемов	2x1Gb Ethernet
Объем оперативной памяти	16 Гб
Тип памяти	DDR4-2933 Registered
Мощность	500 Вт
Тип шасси	SFF Easy Install Rail Kit
Контроллер	2 x 1Gbe (HPE Ethernet 332i)
Размеры (В x Ш x Г), см	46×60×19

2.4 Выбор однонаправленного шлюза

Однонаправленный шлюз (диод данных) СТРОМ-100[12] предназначен 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. Устройство СТРОМ-100 изображено на рисунке 2.4.1.

Рисунок 2.4.1 – Однонаправленный шлюз СТРОМ-100

Технические характеристики СТРОМ-100 занесены в таблицу 2.4.1.

Таблица 2.3.1 – Технические характеристики сервера.

Параметры	Значение
Скорость передачи	до 100 Мбит/с
Время загрузки	менее 5 секунд.
Внешний интерфейс	Ethernet 100BASE-T
Внутренний интерфейс	Ethernet 100BASE-FX
Конфигурирование	Файл на карте памяти.
Мощность	12 Вт
Размеры (В х Ш х Г), мм	44x483x272

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.

3 РАЗРАБОТКА И ОБОСНОВАНИЕ СТРУКТУРНОЙ СХЕМЫ ПРОЕКТИРУЕМОЙ СЕТИ

Для выполнения требований технического задания необходимо разработать структурную схему ведомственной сети. На рисунке 3.1 представлена модель сети, реализованная с использованием Cisco Packet Tracer.

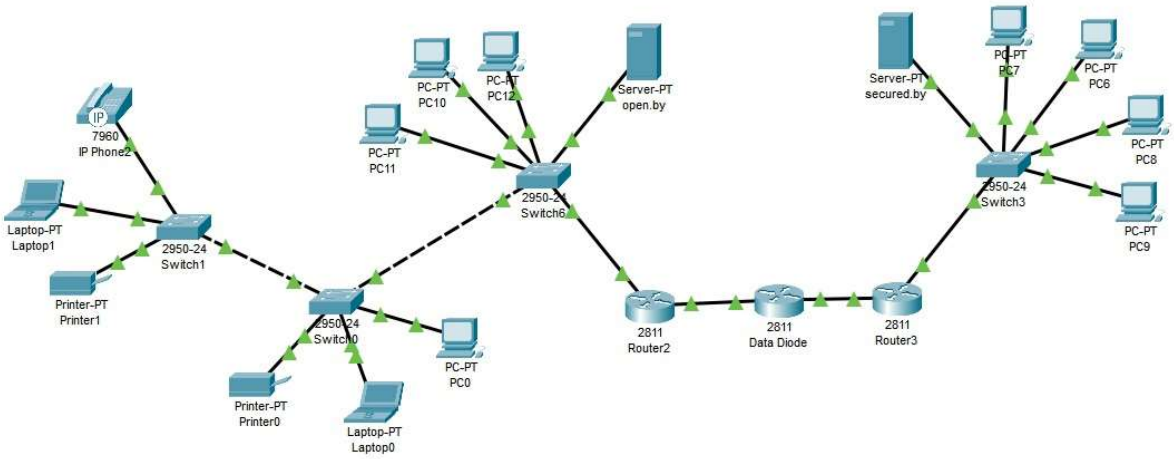

Рисунок 3.1 – Модель реализованная в Cisco Packet Tracer

В представленной модели однонаправленной ведомственной сети важную роль играет диод данных (однонаправленный шлюз), который позволяет осуществить фильтрацию трафика. В данном случае он реализован программно, посредством конфигурации маршрутизатора. Для корректной реализации однонаправленного шлюза на базе маршрутизатора в Cisco Packet Tracker использовался универсальный и мощный механизм фильтрации: список контроля доступом (Access Control List[13]).

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, которые предназначены для публикации данных из публичной подсети в закрытую.

Публичная подсеть, изображена на рисунке 3.2.

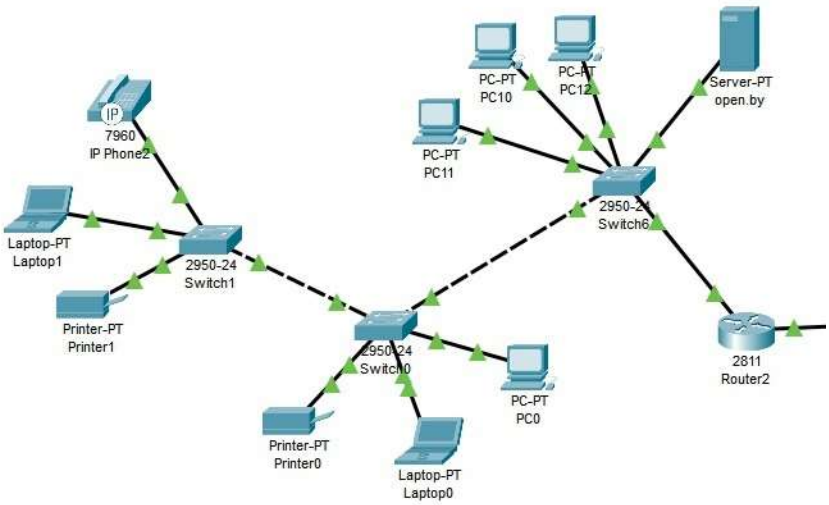

Рисунок 3.2 – Публичная подсеть

В открытой сети находится ftp-сервер open.by с 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.

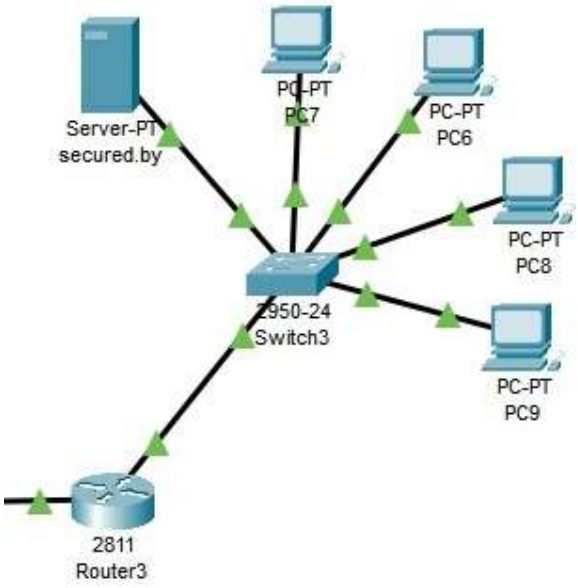

Рисунок 3.3 – Защищенная подсеть

В защищенной подсети расположен ftp-сервер secured.by с 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 PC0, расположенного в публичной сети, требуется передать данные на PC9, расположенный в закрытой сети.

Для этого, на первом шаге, пользователь PC0, подключается к серверу open.by и открывает каталог для отправки данных в защищенную сеть. Далее происходит загрузка данных на публичный сервер, пользователь PC0 по завершению загрузки, может отключиться от сервера. Передача данных в публичной сети изображена на рисунке 3.4

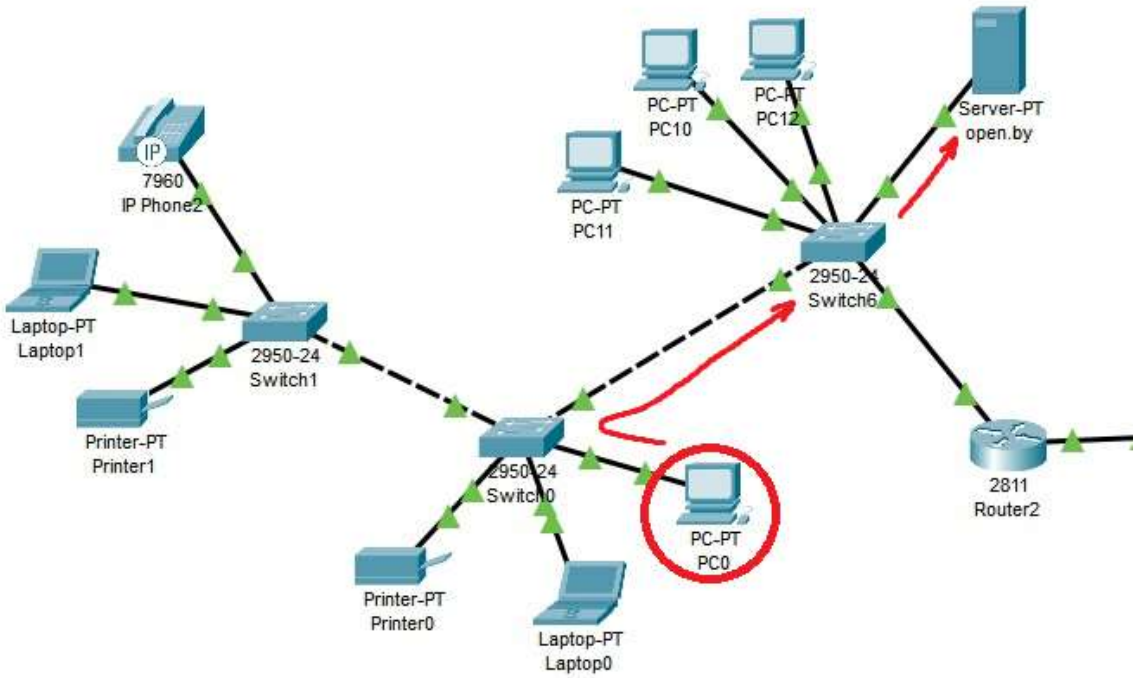

Рисунок 3.4 – Передача данных в публичной подсети

После загрузки информации на сервер open.by, начинается процесс однонаправленной передачи данных посредством пакетов UDP через диод данных на защищенный сервер secured.by. Движение трафика изображено на рисунке 3.5. С сервера open.by, трафик поступает на Router2, тот в свою очередь перенаправляет трафик через диод данных на Router3. После чего, данные поступают на сервер secured.by, находящийся в защищенной сети.

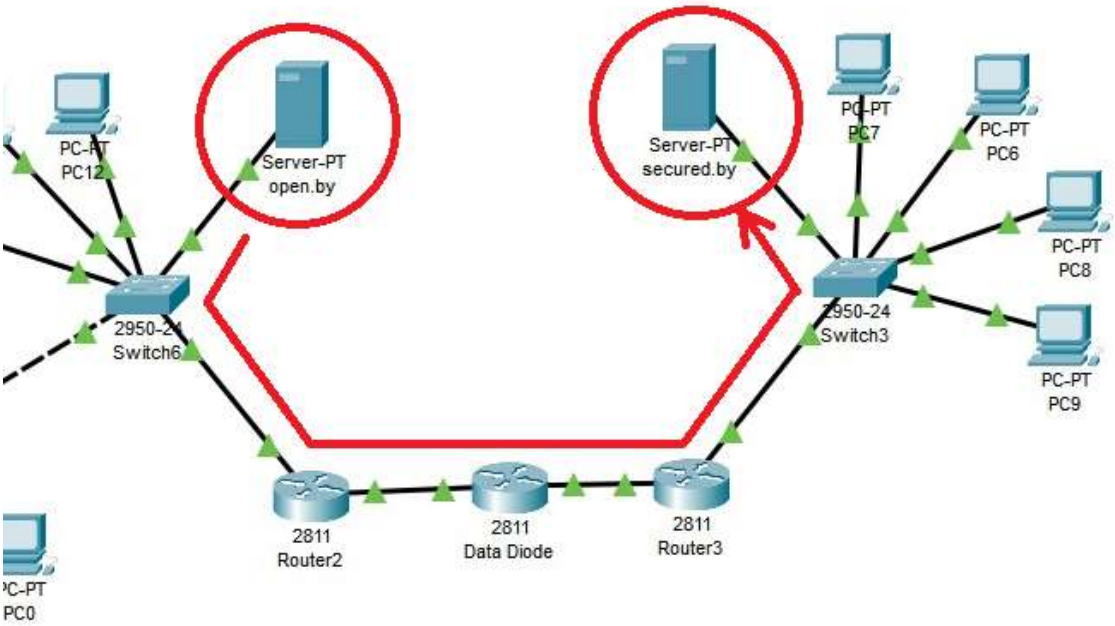

Рисунок 3.5 – Передача данных в публичной подсети

После передачи данных на сервер secured.by, они становятся доступны для пользователей внутренней сети. Пользователь PC9 подключается к серверу и может скачать данные с защищенного сервера на свой ПК в случае необходимости. Схема передачи данных изображена на рисунке 3.6.

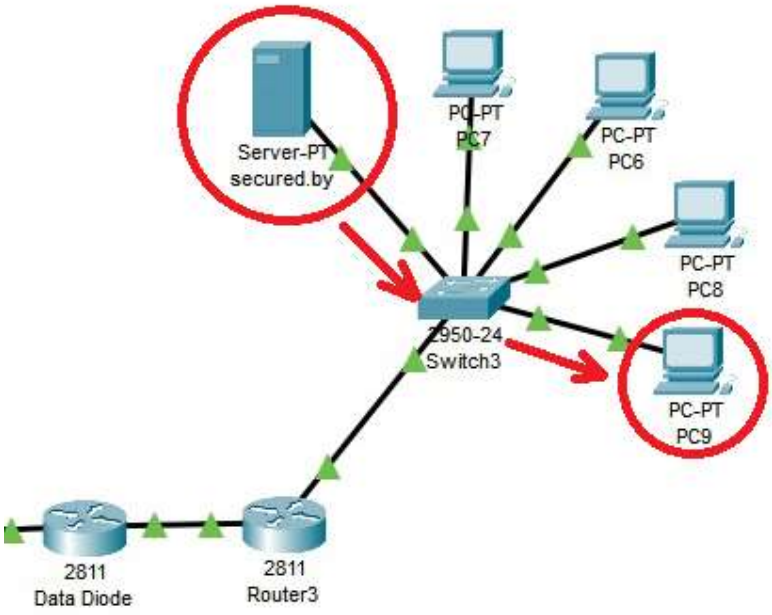

Рисунок 3.6 – Передача данных в закрытой подсети

4 РАЗРАБОТКА И ОБОСНОВАНИЕ СТРУКТУРНОЙ СХЕМЫ АЛГОРИТМА ПЕРЕДАЧИ ДАННЫХ ПО СЕТИ

Для выполнения требований технического задания необходимо разработать алгоритм передачи данных из открытой сети в закрытую. Алгоритм работы программы состоит из двух блоков: приемного и передающего.

Программа передачи данных занимается отслеживанием рабочей папки на случай появления новых файлов или изменения существующих. При обнаружении изменений, происходит отправка изменений на защищенный сервер. Структурная схема передающей программы представлена на рисунке 4.1.

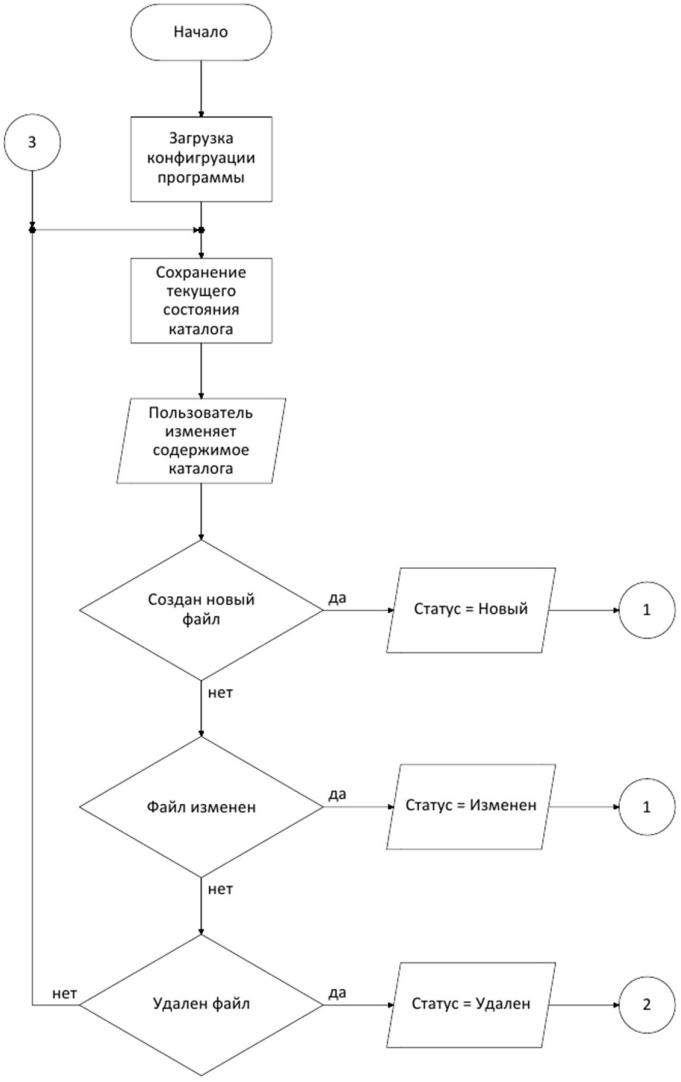

Рисунок 4.1 – Алгоритм работы передающей программы

Для корректного отслеживания изменений перед началом работы, необходимо записать во внутренний буфер список файлов и их hash значения.

Пользователь изменяет содержимое отслеживаемого каталога и приложению нужно каким-либо путем получить информацию об этом. Современные операционные системы позволяют настраивать отслеживание изменения в каталоге и способны отправлять уведомление об этом в приложение, можно практически мгновенно приступить к отправке данных на удаленный сервер. В случае, если данная функция не поддерживается, можно через равные интервалы времени проводить сканирование каталога на предмет изменений и самостоятельно обнаруживать изменения.

После обнаружения изменения, оно категорируется по статусу и происходит переход в блок отправки, представленный на рисунке 4.2.

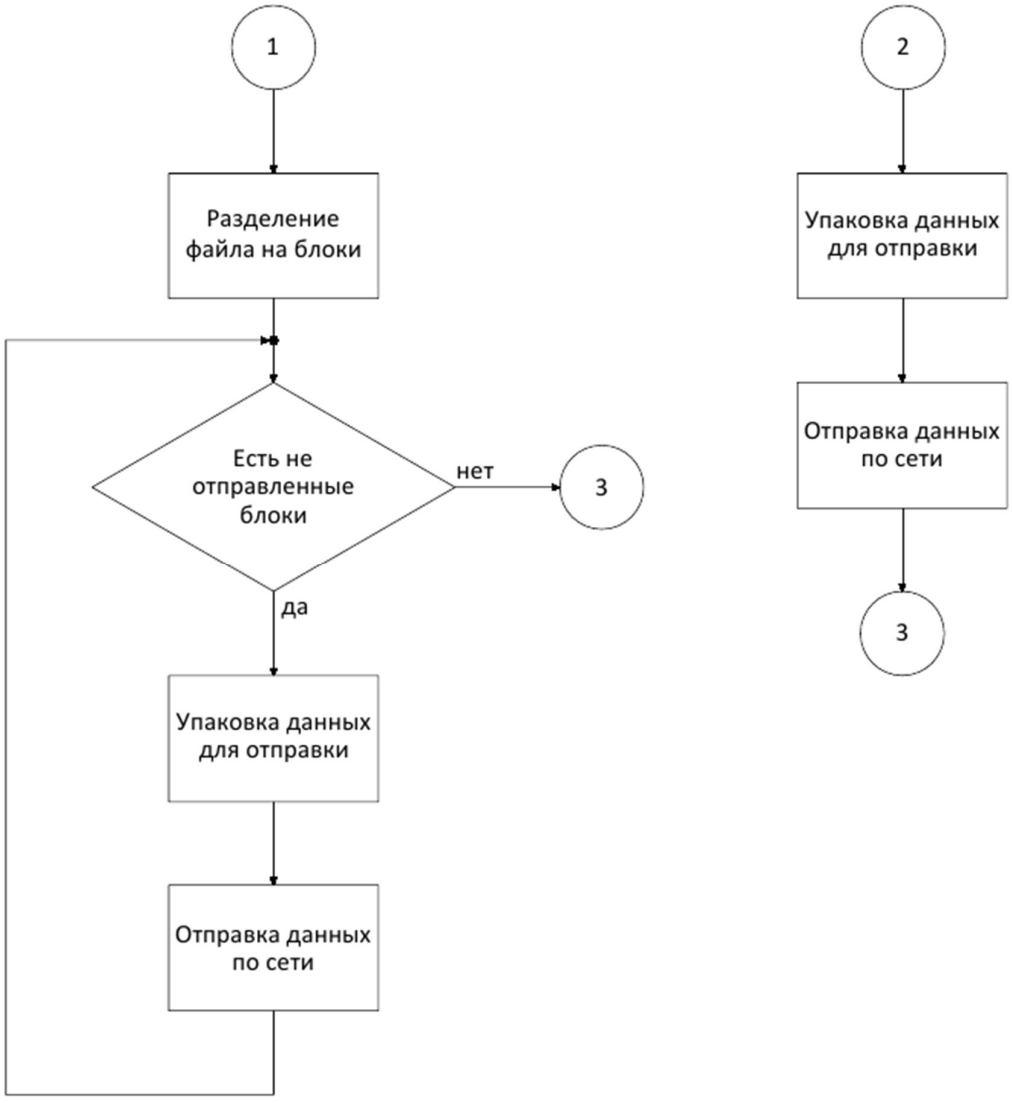

Рисунок 4.2 – Алгоритм работы блока отправки данных

В блоке отправки данных, происходит разбиение файла на блоки, которые последовательно отправляются по сети. В случае удаления файла, отправляется только 1 пакет с инструкцией об удалении файла.

После завершения цикла отправки файла, алгоритм сохраняет новое состояние каталога и ожидает следующих изменений.

Для получения данных на принимающей стороне находится другая часть программы, ответственная за корректный прием и конструирование файлов из сетевых пакетов. Алгоритм представлен на рисунке 4.3.

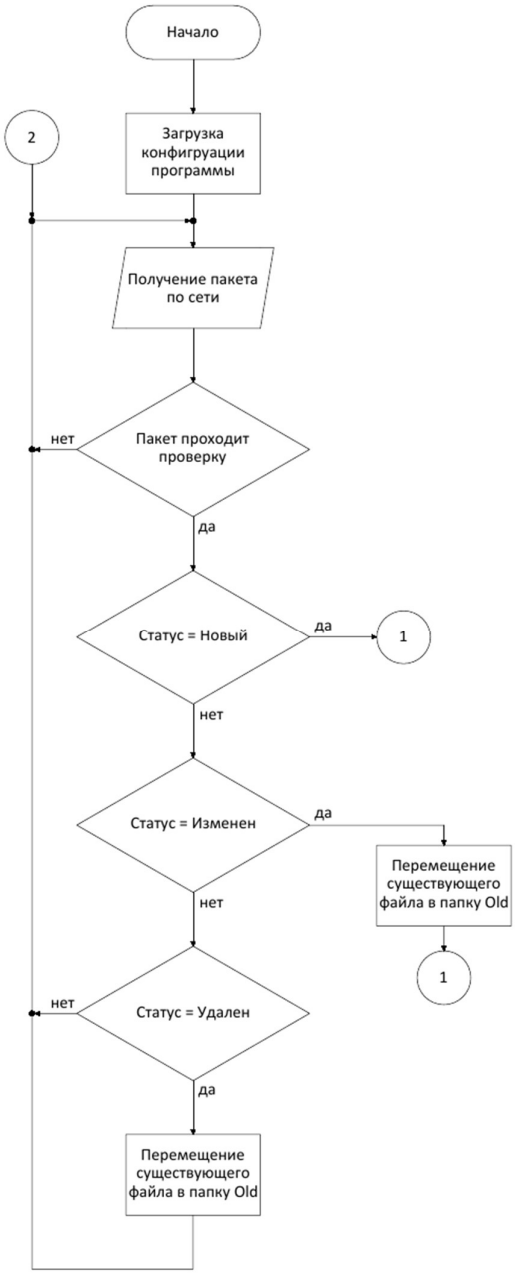

Рисунок 4.3 – Алгоритм работы принимающей стороны

Для корректной работы, на приемной стороне присутствует 3 каталога:

– Old, для хранения удаленных и измененных копий файлов;

– Download, для хранения файлов в процессе загрузки;

– Work, с готовыми к работе файлами.

После конфигурации программы, она ожидает новый сетевой пакет. При получении пакета, он проходит проверку, на случай его повторного получения для предотвращения множественных обработок одного пакета. Если проверка не пройдена, то пакет сбрасывается.

После прохождения проверки, пакет в зависимости от своего статуса, обрабатывается:

– Если пакет в статусе Удален, то, файл из рабочего каталога, переносится в папку Old.

– Если пакет в статусе Изменен, то происходит перенос предыдущей версии файла из папки Work в папку Old, и начинается процесс конструирования файла.

– Если пакет в статусе Новый, то происходит процесс конструирования файла.

Процесс конструирования представлен на рисунке 4.4.

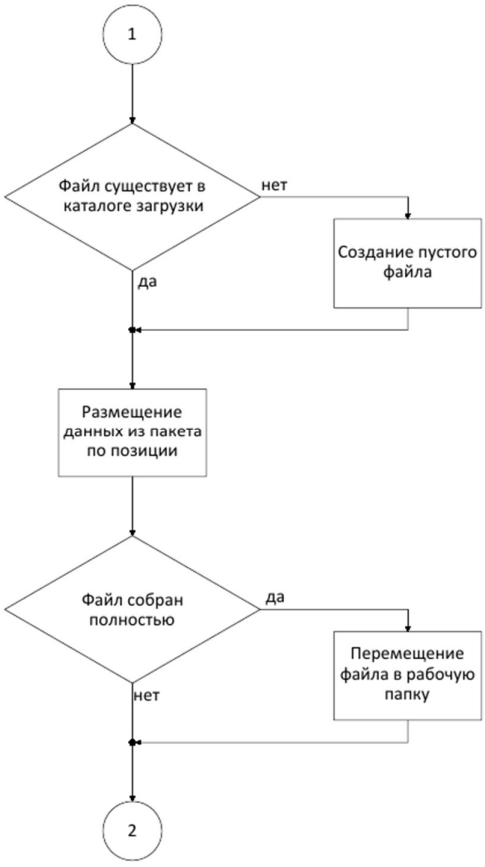

Рисунок 4.3 – Алгоритм работы принимающей стороны

При приеме файла, происходит проверка на наличие создаваемого файла в каталоге Download. В случае отсутствия, создается файл заполненный нулями необходимого объема. Далее происходит замена части файла, полученными данными по сети. Таким образом, происходит постепенное заполнение файла оригинальными данными.

В случае, если полученный пакет был последним необходимым для полного восстановления файла, данный файл переносится из каталога Download в каталог Work.

После обработки пакета, происходит возврат в ожидание следующего пакета.

Таким образом обобщенная схема алгоритма позволяет передавать различные файлы по сети, защищена от дупликации пакетов, позволяет обновлять и переносить неиспользуемые данные на защищенном сервере.

ЗАКЛЮЧЕНИЕ

В ходе преддипломной практики, получены практические навыки патентного поиска, анализа аналогичных решений. В результате первого раздела, сделан вывод, о наличии общемировой практики использования однонаправленных шлюзов в вопросах защиты данных. Приведена инструкция по внедрению подобных систем и возможные проблемы, с которыми можно столкнутся при реализации работы с однонаправленными сетями на практике. Проведен анализ рынка аппаратных диодов данных.

Во втором разделе, выбрано оборудование для реализации однонаправленной ведомственной сети.

В третьем разделе приведена модель проектируемой сети, приведен пример работы построенной модели. Разработана логическая топология ведомственной сети

В четвертом разделе, разработана структурная схема алгоритма синхронизации. Приведен принцип работы, указаны детали реализации отдельных блоков. Разработаны алгоритмы работы приемной и передающей части программы.

По результатам преддипломной практики, можно судить, о целесообразности продолжения разработки однонаправленной ведомственной сети.

Список использованных источников

[1] Диод данных [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/

[2] RU2712815C1 [Электронный ресурс]: RU2712815C1 Защита сетевых устройств посредством межсетевого экрана. – Режим доступа: RU2712815C1.pdf.

[3] RU2607997C1 [Электронный ресурс]: RU2607997C1 Система защиты компьютерных сетей от несанкционированного доступа. – Режим доступа: RU2607997C1.pdf.

[4] Unidirectional Networking [Электронный ресурс]: GIAC Security Essential Certification Practical Assignment Version 1.4b – Режим доступа: unidirectional-networking_2848.pdf

[5] Обзор рынка диодов данных [Электронный ресурс] – Режим доступа: https://www.anti-malware.ru/

[6] AMT InfoDiode [Электронный ресурс] – Режим доступа: https://infodiode.ru/

[7] РУБИКОН-ОШ [Электронный ресурс] – Режим доступа: https://npo-echelon.ru/

[8] Owl Cyber Defense [Электронный ресурс] – Режим доступа: https://owlcyberdefense.com/

[9] Маршрутизатор CISCO C1111-4P [Электронный ресурс] – Режим доступа: https://www.unibelus.by/

[10] Коммутатор Cisco Catalyst 9200 (C9200L-24T-4G-A) [Электронный ресурс] – Режим доступа: https://www.unibelus.by

[11] Сервер HPE ProLiant DL180 Gen10 P35519-B21 [Электронный ресурс] – Режим доступа: https://hpserver.by/

[12] СТРОМ-100 [Электронный ресурс]. – Режим доступа: https://www.cryptoex.ru/

[13] Access Control List (ACL) [Электронный ресурс]. – Режим доступа: https://www.imperva.com/