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.

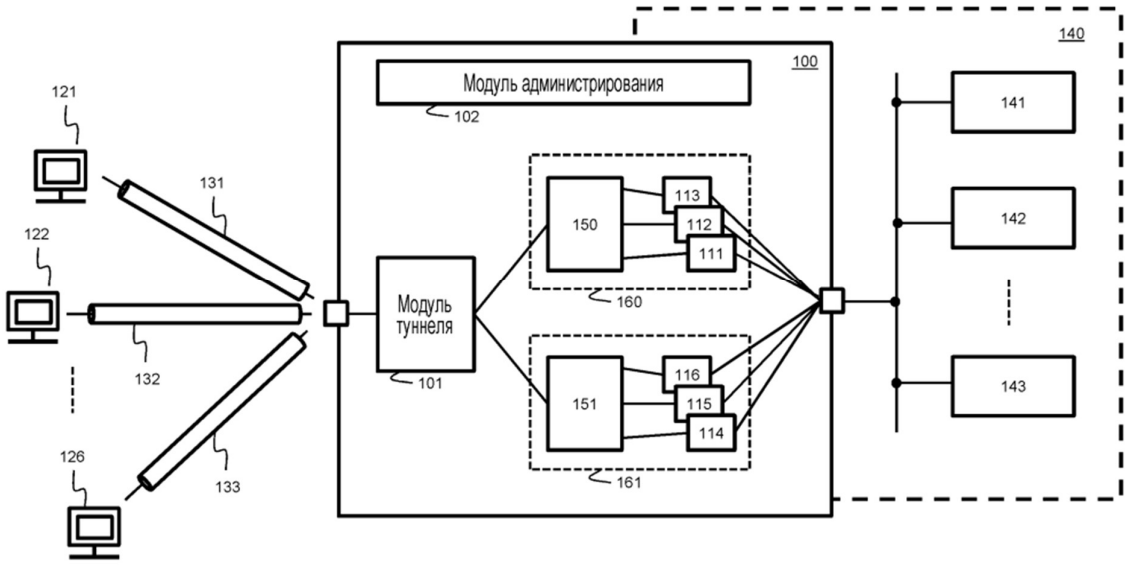

Рисунок 1.1 – Пример системы для защиты сетевых устройств от нежелательного сетевого доступа

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.

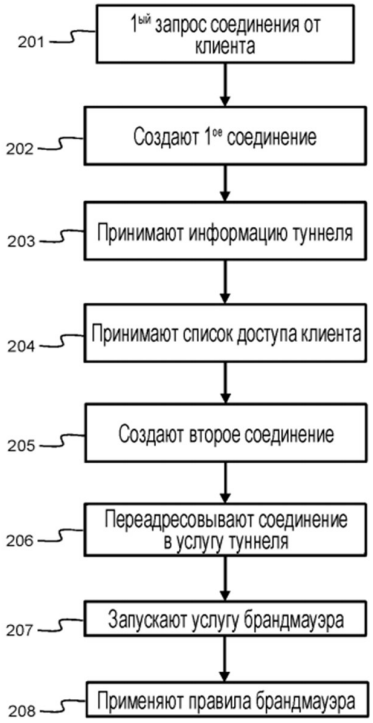

Рисунок 1.2 – Структурная схема создания сетевого туннеля между клиентским устройством и частной сетью

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.

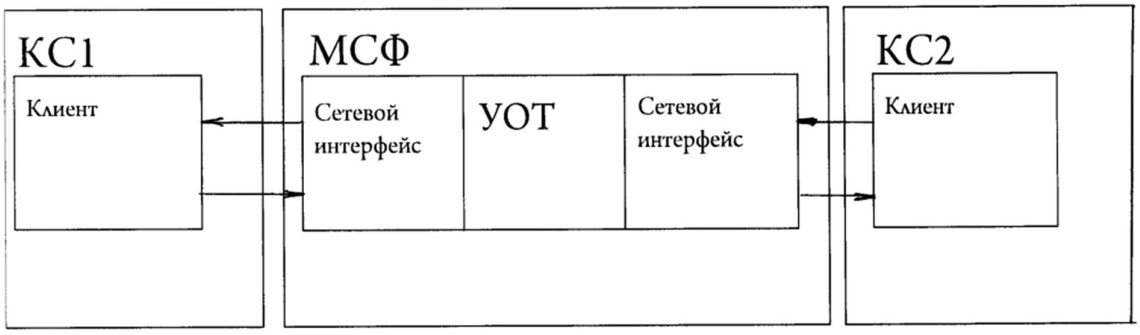

Рисунок 1.3 – Структурная схема подключения компьютерной сетей к устройству фильтрации трафика

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.

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.

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.

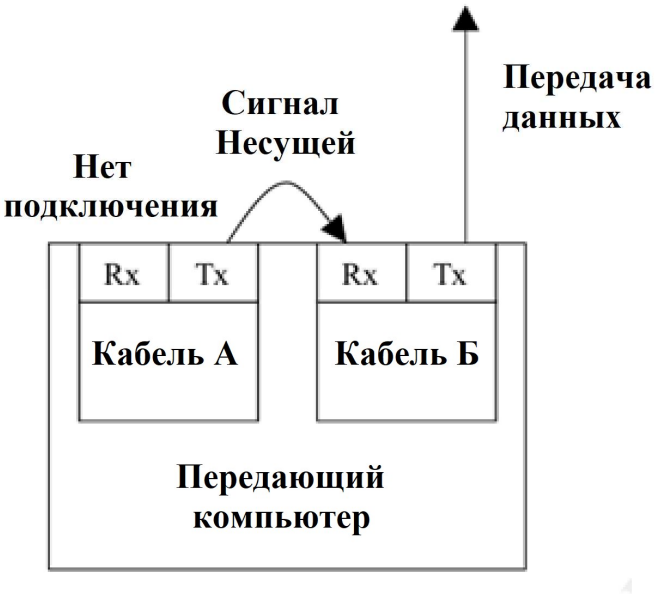

Рисунок 1.6 – Решение проблемы отсутствия, несущей на приемной стороне передатчика

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.

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» [7], 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+З

– 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.