ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Гарифьянов Данил Мине-Хаматович

магистрант, Казанский (Приволжский) Федеральный Университет, РФ, г. Казань

Вахитов Илдар Хатыбович

научный руководитель, док. биол. наук, профессор, Казанский (Приволжский) Федеральный Университет, РФ, г. Казаньдок. биол. наук, профессор, Казанский (Приволжский) Федеральный Университет, РФ, г. Казань

Аннотация. В статье рассмотрена разработка проекта по созданию сетевой инфраструктуры для филиала поликлиники находящейся на удаленной площадке. В проекте были учтены исходные данные по расположению инфраструктуры, требования по обеспечению непрерывности медицинских процессов, информационной безопасности. Был разработан проект модульной сети передачи данных, обеспечивающий следующие характеристики:

- высокую производительность за счет применения современного коммутационного оборудования, технологий агрегации каналов связи;

- отказоустойчивость за счет резервирования основного оборудования (стекирование, кластеризация), каналов связи (применение динамической маршрутизации), резервирование схем электропитания (применение централизованных ИБП, «горячего» резервирования блоков питания основного оборудования);

- управляемость за счет применения ограниченной номенклатуры оборудования, консолидации управления группами устройств (коммутаторов, межсетевых экранов, устройств криптографической защиты), а также за счет применения технологий внеполосного и внутриполостного управления;

- безопасной за счет применения современных комплексных средств защиты информации.

- В проекте учтены все современные требования информационной безопасности (предусмотрены средства межсетевого экранирования, предотвращения вторжений, фильтрации трафика), а также требования регуляторов (ФСБ, ФСТЭК) в области защиты персональных данных медицинских информационных систем. Для трафика, содержащего персональные данные, предусмотрена криптографическая защита, соответствующая ГОСТ 28147-89, ГОСТ ГОСТ Р 34.10-2012.

- особенности и тенденции в защите персональных данных в медицинских информационных системах. Проанализированы изменения законодательства в отношении защиты персональных данных в медицинских учреждениях и требования, предъявляемые к техническим средствам защиты информации. Выявлена необходимость использования комплексного подхода к вопросу защиты персональных данных, связанных с передачей информации по безопасным каналам связи между удаленной медицинской информационной системой и центром обработки данных.

Ключевые слова: защита персональных данных, медицинские информационные системы, защищенные частные сети (VPN), криптографическая защита.

Введение

Дизайн современных медицинских информационных систем обусловлен необходимостью сбора, хранения, передачи и предоставления данных медицинским работникам. Безопасный сбор, хранение и использование медицинских данных является актуальным требованием и проблемой для системы здравоохранения. Здравоохранение включает разнообразный набор систем сбора данных, таких как медицинская документация, результаты обследования здоровья пациента, административные отчеты и даже используемые устройства пациентов, которые отражают текущее местоположение пациента и состояние здоровья. Эти данные собираются и используются различными структурами, такими как больницы, медицинскими центрами, врачами, передаются в Единую государственную информационную систему здравоохранения.

Цель и задачи

Цель данной статьи заключается в разработке проекта защищенной и отказоустойчивой инфраструктуры филиала поликлиники, расположенного на удаленной площадке

Задачами являются разработка следующих документов:

· Структурная схема

· Логическая схема

· Пояснительная записка к эскизному техническому решению по разработке и созданию эскизного проекта защищенной и отказоустойчивой сетевой инфраструктуры поликлиники.

Разработка

Сетевая инфраструктура обеспечивает отказоустойчивое взаимодействие серверных и клиентских компонентов информационных систем поликлиники, функционирование почтовой системы и системы IP телефонии, отказоустойчивый и безопасный доступ к информационным ресурсам поликлиники, а также внешних организаций.

Сетевая инфраструктура мед. учреждения (МУ) состоит из следующих подсистем:

1. Сегмента внутренней локальной сети на площадке МУ.

2. Сегмента сети периметра, предназначенного для организации доступа к ресурсам поликлиники.

3. Подсистемы криптографической защиты, необходимой для защиты конфиденциальной информации от раскрытия, модификации и навязывания при ее передаче по сети интернет за пределами контролируемой зоны на участке между филиал поликлиники (ФП) и поликлиникой.

4. Подсистемы межсетевого экранирования, предназначенной для обеспечения уровня защищенности ресурсов информационных систем, адекватного современным и прогнозируемым угрозам информационной безопасности.

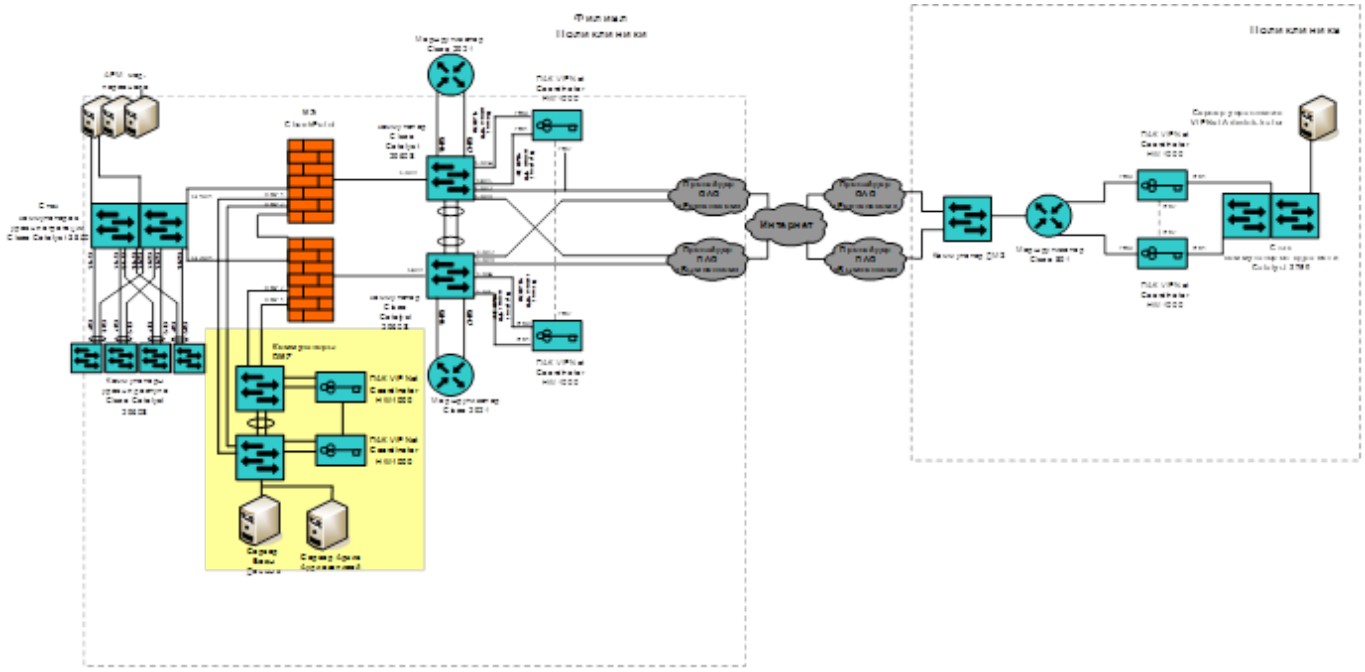

Рисунок 1Структурная схема

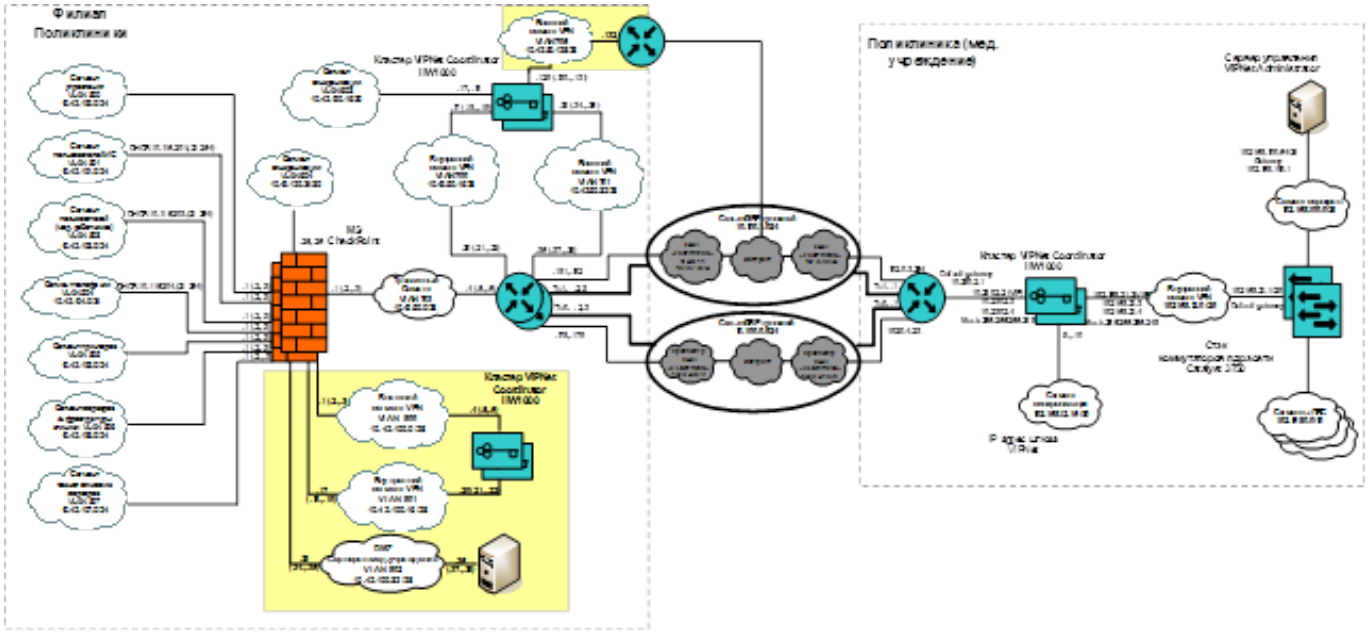

Рисунок 2 Логическая схема

Сегмент внутренней локальной сети в МУ имеет иерархическую инфраструктуру, включающую в себя:

- уровень агрегации;

- уровень доступа.

Уровень агрегации предназначен для подключения коммутаторов уровня доступа, системы межсетевого экранирования (МСЭ).

Уровень агрегации обеспечивает резервирование каналов связи и балансировку нагрузки до коммутаторов доступа и обеспечивает отказоустойчивость входящих в него компонентов таким образом, что выход из строя единичного компонента (блок питания, кабель, коммутатор) не приводит к отказу работоспособности внутренней локальной сети.

Отказоустойчивость обеспечивается объединением коммутаторов агрегации в стек.

В качестве коммутаторов уровня агрегации используются коммутаторы Cisco Catalyst 3850-48T-S.

Уровень доступа предназначен для подключения пользовательских АРМ, IP телефонов и сетевых принтеров. Он строится на базе четырёх коммутаторов Cisco Catalyst 2960S–48FPD-L, подключаемых к коммутаторам уровня агрегации по каналам Gigabit Ethernet.

Каждый коммутатор уровня доступа подключается к каждому коммутатору уровня агрегации по одному каналу GE. Так как коммутаторы уровня агрегации объединены в один логический коммутатор по технологии стекирования, то оба канала GE от коммутатора уровня доступа к коммутаторам уровня агрегации объединяются в единый логический интерфейс по технологии EtherChannel с совокупной скоростью передачи данных до 2 Гбит/с.

Сегмент сети периметра

Сегмент сети периметра предназначен для организации доступа к ресурсам ФП и ресурсам поликлиники.

Для обеспечения логической транспортной инфраструктуры при организации связи ФП с поликлиникой, а также при подключении внешнего сегмента МСЭ и подсистемы криптографической защиты, используются маршрутизаторы периметра сети.

В качестве маршрутизаторов периметра сети используются маршрутизаторы Cisco 2921.

Для обеспечения связности маршрутизаторов периметра, внешних сегментов МСЭ и подсистемы криптографической защиты, используются коммутаторы Cisco Catalyst 2960S-24TS-L.

Для организации связи между ФП и поликлиникой через каналы передачи данных, арендуемых у провайдеров, используется технология mGRE, которая позволяет создать виртуальную частную сеть с возможностью динамического создания туннелей между узлами. Между сетью ФП и сетью его поликлиники создаются динамические туннели mGRE. Криптографическая защита передаваемых данных осуществляется при помощи туннелей VPN, создаваемых проектируемыми шлюзами VIPNet Coordinator в ФП и существующими шлюзами VIPNet Coordinator в поликлинике.

Для реализации решения используются маршрутизаторы Cisco 2921 со стороны ФП и маршрутизатор Cisco 891 со стороны поликлиники.

На каждом из физических маршрутизаторов выделяются несколько экземпляров виртуальных маршрутизаторов VRF:

- VRF_0 – создается на маршрутизаторе для подключения к внешнему каналу арендуемому у операторов связи ПАО «ВымпелКом» ассоциирован только с одним внешним суб-интерфейсом, подключенным к внешнему каналу, используется для создания транспортной сети и маршрутизации по сети оператора связи. В данном экземпляре виртуального маршрутизатора работает протокол динамической маршрутизации EIGRP для обеспечения переключения каналов связи провайдеров и балансировки нагрузки;

- VRF_1 – создается на маршрутизаторе для подключения к внешнему каналу арендуемому у операторов связи ОАО «Ростелеком», ассоциирован только с одним внешним суб-интерфейсом, подключенным к внешнему каналу, используется для создания транспортной сети и маршрутизации по сети оператора связи. В данном экземпляре виртуального

маршрутизатора работает протокол динамической маршрутизации EIGRP для обеспечения переключения каналов связи провайдеров и балансировки нагрузки;

- VRF_Global – имеется на маршрутизаторе по умолчанию, ассоциирован с внутренними интерфейсами и суб-интерфейсами, используется для подключения всех маршрутизируемых интерфейсов, не входящих в VRF_1 и VRF_2.

Решение предусматривает возможность использования нескольких внешних каналов связи между ФП и Поликлиникой с использованием отказоустойчивости и балансировки нагрузки. Отказоустойчивость и балансировка нагрузки обеспечиваются использованием протокола динамической маршрутизации EIGRP. Протокол EIGRP запускается в экземплярах виртуальных маршрутизаторов VRF_1 и VRF_2. Маршрутизаторы ФП и Поликлиникой устанавливают друг с другом смежность через виртуальные интерфейсы Tunnel.

Для предотвращения несанкционированного подключения оборудования к транспортной сети, и инъекции ложных маршрутов в протоколе EIGRP, используется аутентификация по алгоритму MD5.

Для организации отказоустойчивого подключения маршрутизаторов периметра сети к внешнему сегменту МСЭ и подсистеме криптографической защиты, на маршрутизаторах периметра сети используется протокол HSRP. Группа интерфейсов маршрутизаторов объединяется под общим IP-адресом. Один из маршрутизаторов выбирается основным для передачи трафика, другой резервным. Выбор основного и резервного маршрутизатора основан на значении установленного приоритета.

Подсистема криптографической защиты

Подсистема криптографической защиты каналов связи выполняет следующие функции:

- создание защищенного соединения (построение VPN);

- шифрование передаваемой информации по алгоритму ГОСТ 28147-89;

- управление компонентами системы и справочно-ключевой информацией.

Подсистема криптографической защиты каналов реализуется на основе технологии защищенной частной сети на основе решений семейства ViPNet производства компании ОАО «ИнфоТеКС».

В состав системы входят следующие компоненты:

- VPN-шлюзы;

- сервер управления.

VPN-шлюзы

В качестве VPN-шлюзов используются программно-аппаратные комплексы ViPNet Coordinator HW1000.

ПАК ViPNet Coordinator HW1000 развертываются на площадках Поликлиники и ФП.

ПАК ViPNet Coordinator HW1000 выполняют следующие функции:

- устанавливает между собой защищенное соединение;

- обеспечивает шифрование и передачу информации между защищаемыми ресурсами ЛВС по алгоритму ГОСТ 28147-89 через установленное защищенное соединение.

Логическая схема подключения ПАК представлена на рисунке ниже.

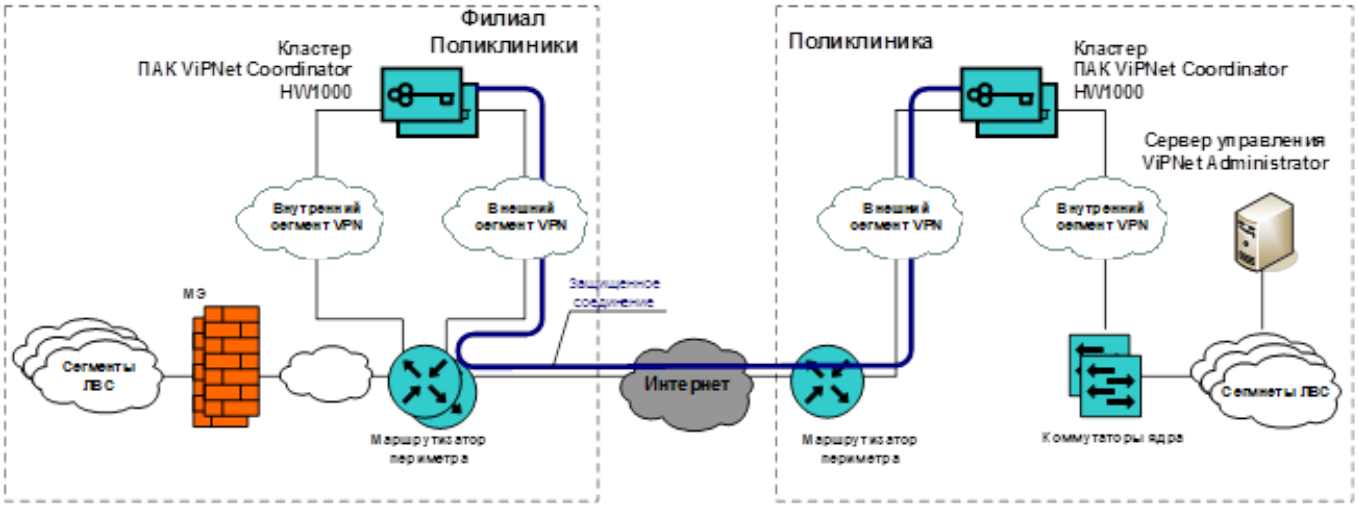

Рисунок 3 - Логическая схема подключения ПАК ViPNet Coordinator HW1000

ПАК ViPNet Coordinator HW1000 развертываются на границах ЛВС Поликлиники и ФП, до точки подключения ЛВС к сетям связи общего пользования, проходящим за пределами контролируемой зоны.

Для подключения кластеров ПАК ViPNet Coordinator HW1000 к ЛВС создаются два сегмента сегмента:

- внешний сегмент VPN;

- внутренний сегмент VPN.

Внешний сегмент VPN используется для построения защищенного соединения передачи зашифрованного трафика. Внутренний сегмент VPN используется для передачи открытого трафика между ПАК и ЛВС.

Трафик, передаваемый из ЛВС ФП в ЛВС Поликлиники, маршрутизируется через внутренний интерфейс ПАК ViPNet Coordinator HW1000. ПАК ViPNet Coordinator HW1000 ФП осуществляет шифрование полученного трафика и его передачу через защищенное соединение на ПАК ViPNet Coordinator HW1000 в Поликлинику. ПАК ViPNet Coordinator HW1000 в Поликлинике расшифровывает полученный трафик и передает его (через внутренний сегмент VPN) получателям в ЛВС Поликлиники. Обратный трафик из ЛВС Поликлиники в ЛВС Филиала передается аналогичным образом.

В Поликлинике и в ФП развертываются по 2 шт. ПАК ViPNet Coordinator HW1000. 2 ПАК, развернутые на каждой площадке, объединяются в отказоустойчивый кластер. В кластере один ПАК является активным и производит обработку трафика, а второй – резервным. При отказе активного ПАК, резервный ПАК становится активным и переключает сетевые потоки на себя.

ПАК ViPNet Coordinator HW 1000 имеет сертификат соответствия ФСБ России № СФ/124-2606 по требованиям к СКЗИ класса КС3. Сертификат действителен до 23 июля 2018 года.

Список литературы:

1. Учебник. В.Олифер «Компьютерные сети Принципы, технологии, протоколы 4-е издание». – [Электронный ресурс] – Режим доступа. –URL:

http://elib.sbras.ru:8080/jspui/bitstream/SBRAS/9349/1/olifer_ru.pdf (Дата обращения 20.04.2018).

2. «Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-издание, исправленное». – [Электронный ресурс] – Режим доступа. –URL: http://www.williamspublishing.com/Books/978-5-8459-0842-1.html (Дата обращения 7.05.2018).

3. Дансмор Б. Скандьер Т. «Справочник по телекоммуникационным технологиям Cisco» – [Электронный ресурс] – Режим доступа. –URL: http://www.studmed.ru/dansmor-b-skander-t-spravochnik-po-telekommunikacionnym-tehnologiyam_b5e4ed2b762.html (Дата обращения 15.05.2018).

4. Комплект документации на продукты ViPNet – [Электронный ресурс] – Режим доступа. –URL: https://infotecs.ru/downloads/documentacii/ (Дата обращения 23.05.2018).