ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ СИСТЕМЫ PACS, ИНТЕГРИРОВАННОЙ С ВИРТУАЛЬНОЙ ЛАБОРАТОРИЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Нгуен Х. К.

Иванов Н. Н. − к. ф-м. н., доцент

Расширение системы архивации и передачи изображений PACS на основе сервис-ориентированной архитектуры СОА позволяет существенно расширить возможности постановки диагноза пациента путем привлечения к анализу данных внешних экспертов, а также дополнить возможности системы путем реализации виртуальной лаборатории (ВЛ). При внедрении СОА-подхода для расширения системы PACS безопасность становится одной из проблем, с которой сталкиваются пользователи. В сообщении предлагается модель организации безопасности для расширенной системы PACS.

В 1983 году на основе запросов медицинских работников и новых возможностей компьютерных систем были сформулированы основные положения архитектуры системы PACS (Picture Archiving Communication System), предназначенной для хранения и использования медицинских изображений [1]. В настоящее время она широко применяется в большинстве медицинских учреждениях. Экономическая составляющая использования PACS состоит в сокращении затрат, связанных с хранением и обработкой носителей данных, ускоренным поиском информации, удобным форматом для просмотра изображений на экране компьютера, возможностью коллективного доступа к базам данных. В системе для изображений применяется формат DICOM [2]. В нем наряду с изображением хранятся персональные данные пациента и история его болезни.

С целью увеличения возможностей PACS для постановки диагноза пациента нами была реализована ее расширение на основе СОА. Были добавлены такие компоненты, как Сервисная шина и две компоненты, соответствующие двум новым функциям телемедицины: Консультант и Консилиум, которые формализуют обращение к консультанту и организуют консилиум для обсуждения диагноза пациента [3]. Новая система получила название APACS. Применение СОА, с его слабо-связанными сервисами легко позволило APACS подключиться к другим системам [4]. Это увеличило возможности PACS как инструмента образования, улучшающего качество инженерного обучения и научного исследования. Была реализована учебная ВЛ удаленного доступа исследования биомедицинских изображений, интегрированная с системой APACS на основе СОА подхода. Учебная ВЛ обеспечивает виртуальное пространство для практических экспериментов с целью ознакомления и освоения этапов процесса обработки медицинских изображений, задач и технологий, используемых в обработке медицинских изображений [5]. Интеграция учебной ВЛ с системой APACS на основе СОА, схема которой показана на рисунке 1, обостряет проблемы безопасности, с которой могут столкнуться пользователи.

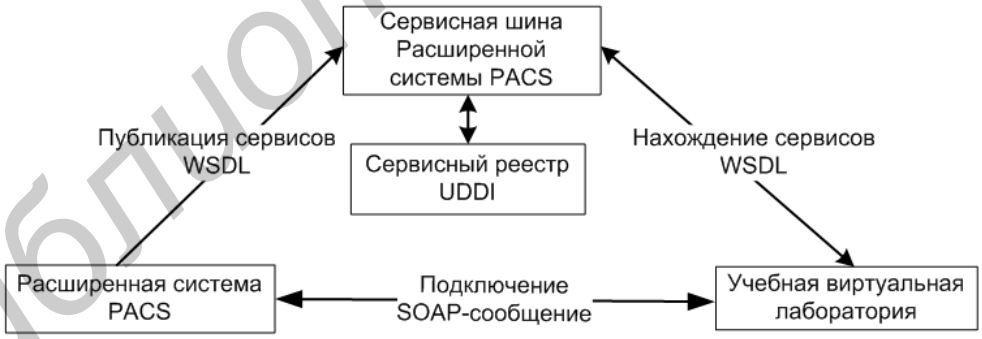

Рис. 1 – Схема интеграции ВЛ с APACS на основе СОА

В СОА идентификация пользователя и авторизация его прав доступ, являются разнородными, для APACS и для учебной ВЛ они различны по своей сути. Возникают новые усложненные задачи организации безопасности, так как мероприятия по сохранению секретности данных и предотвращению утечки информации значительно усложняются.

Кроме этого, должен быть защищен и процесс обмена информацией между этими двумя системами. Схема этого процесса обмена показана на рисунке 1. Согласно схемы, после получения ответа от системы APACS о возможности доступа к сервису, учебная ВЛ подключает к ним через обмены SOAP-сообщениями (Simple Object Access Protocol Message), которые описаны на языке веб-сервисов WSDL (Web Services Description Language). Описание сервисов хранится в специальном реестре системы APACS. SOAP-сообщение является XML-документом, содержащим адреса отправителя и получателя, имя сервиса, и само сообщение. Система безопасности должна защитить эти SOAP-сообщения и обеспечить их целостность в процессе передачи. Подход к организации безопасности для системы APACS с интегрированной с ней учебной ВЛ должен удовлетворять трем требованиям [6]:

1. Возможность интеграции систем безопасности для APACS и для учебной ВЛ.

2. Обеспечить конфиденциальность целостность сообщений в процессе их передачи по сети.
3. Система безопасности должна быть организована в виде сервисов безопасности.

На рисунке 2 дана схема безопасности для APACS с интегрированной с ней ВЛ.

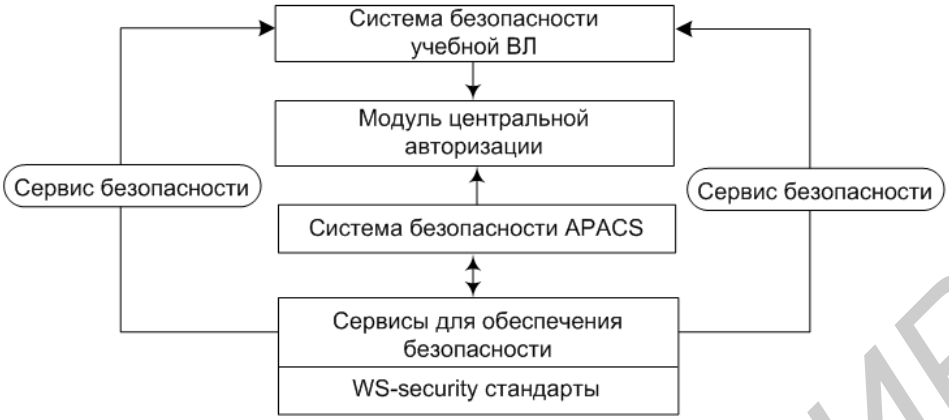

Рис. 2 – Схема организации безопасности для системы APACS с интегрированной ВЛ

Модули аутентификации и авторизации являются частями системы APACS, которая поставляет все сервисы. В данной архитектуре учебная ВЛ играет роль потребителя сервисов. Система безопасности учебной ВЛ и систему безопасности системы APACS могут быть разработаны независимо и затем интегрированы подходом СОА. Информация о пользователях учебной ВЛ и их права могут дублироваться в главном модуле авторизации и они могут быть дополнены правами доступа к сервисам системы APACS. Централизованная политика доступа более удобна: она создается и управляется из единой точки администрирования.

Для обеспечения безопасности в процессе передачи SOAP-сообщения удовлетворяют стандартам безопасности веб-сервисов WS-Security, WS-Policy, WS-Trust, WS-Privacy и WS-SecureConversation [7] и шифруются. WS-Security определяет базовые механизмы и форматы использования security-token в составе SOAP-запросов. WS-Security не определяет никаких новых технологий, она опирается на уже существующие стандарты, к примеру, XML Encryption, XML Signature, или на криптографические алгоритмы. WS-Policy определяет шаблоны и правила описания политики безопасности для веб-сервисов. WS-Trust описывает правила организации доверительных отношений между участниками веб-взаимодействия. WS-Privacy определяет форматы политики конфиденциальности при обмене SOAP-сообщениями. WS-SecureConversation регламентирует правила безопасного обмена сообщениями в СОА-архитектуре.

Сервисы для обеспечения безопасности были построены в системе APACS для обеспечения безопасности при работе сервисов, а также других функций системы APACS. Эти сервисы находятся в сервисном реестре и комбинируются для создания системы безопасности системы APACS. Ниже представлен список служебных сервисов, которые используются в системе безопасности системы APACS [8]:

сервис аутентификации;
сервис авторизации для управления доступом;
сервис обеспечения конфиденциальности;
сервис конверсии полномочий доступа;

Список использованных источников:

1. Fred, W. P. Information management and distribution in a medical picture archive and communication system / W. P. Fred. – Chicago: Illinois, 1992. – 240 p.
2. National Electrical Manufacturers Association / Digital Imaging. – Washington: ACR-Nema Standards Publication, 1985.– 128 p.
3. Нгуен, К. Х. Расширение PACS дополнительными сервисами / К. Х. Нгуен. Материал международной научно-технической конференции МЕДЭЛЕКТРОНИКА, Минск, 2012. – С. 88–90.
4. Erl, T. Service-Oriented Architecture: Concepts, Technology, and Design / T. Erl. – Boston: Prentice Hall, 2005. – 792 p.
5. Нгуен, К. Х. Учебная виртуальная лаборатория удаленного доступа исследования биомедицинских изображений, интегрированная с расширенной системой PACS [Электронный ресурс] / К. Х. Нгуен // Режим доступа: http://www.fan-nauka.narod.ru/2013.html.
6. Шепелявый, Д. А. Обеспечение безопасности Web-сервисов / Д. А. Шепелявый // Информационная безопасность.– 2008. – № 1. С. 1–3.
7. Mark N. Web Services Security / N. Mark, H.B. Phillip, M.C. Sean, S. Mike, A.W. Paul. – Berkeley: McGraw-Hill, 2012. – 312 p.
8. Нгуен, К. Х. Модель обеспечения безопасности для расширенной системы архивации и передачи изображений на основе СОА / К. Х. Нгуен. Материал международной научно-технической конференции МЕДЭЛЕКТРОНИКА, Минск, 2012. – С. 113–116.