

ных при повторном тестировании). Ухудшение результатов при увеличении числа поколений также объясняется вероятностной природой алгоритма.

Результат

Использование генетического алгоритма для формирования баз решающих правил позволяет за сравнительно короткое время сформировать достаточно точную систему правил, описывающую заданные виды атак. Сгенерировав с помощью «сплоитов» и «фоновых» трафика обучающий массив, с помощью генетического алгоритма можно быстро построить систему правил, нейтрализующую данные атаки с минимальной долей ложных тревог и при этом уменьшить работу экспертов.

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО ОБМЕНА ДАННЫМИ МЕЖДУ МИС И НЕЗАВИСИМОЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ ПО ПРОТОКОЛУ MEDML

А. М. Воробьев

(Тюмень, ТюмГУ, artandvor@gmail.com)

Важной социально значимой задачей является повышение доступности и качества медицинских услуг. Одним из направлений решения задачи является сокращение очередей в регистратурах, упрощение процесса записи на прием. Этому способствует применение медицинских информационных систем и организация возможности самозаписи пациентов через Интернет.

В медицинских учреждениях России используется множество медицинских информационных систем (МИС), разработанных различными компаниями, написанных на разных языках и имеющих разные структуры. Большинство медицинских систем не предусматривают возможность самозаписи через веб-сайт. Поэтому учреждения при предоставлении возможности организации записи через Ин-

тернет вынуждены либо создавать собственный сайт, либо интегрировать в МИС уже готовые решения для такой записи.

Целью работы является разработка механизма по организации безопасного обмена данными между МИС и независимой информационной системой по протоколу MedML [3]. Для достижения цели были сформулированы следующие задачи:

- 1) проработать общую концепцию обмена данными, обозначить подходы к реализации всех требуемых методов;
- 2) реализовать модуль для организации обмена данными между МИС и информационной системой по данному протоколу;
- 3) разработать веб-сервис и модифицировать базу данных (далее БД) и программное обеспечение (ПО) МИС для работы с веб-сервисом;
- 4) обеспечить защищенный обмен данными между МИС и информационной системой.

Разрабатываемая концепция компонентов систем позволит обмениваться информацией между МИС и независимой информационной системой по протоколу MedML (рис. 1).

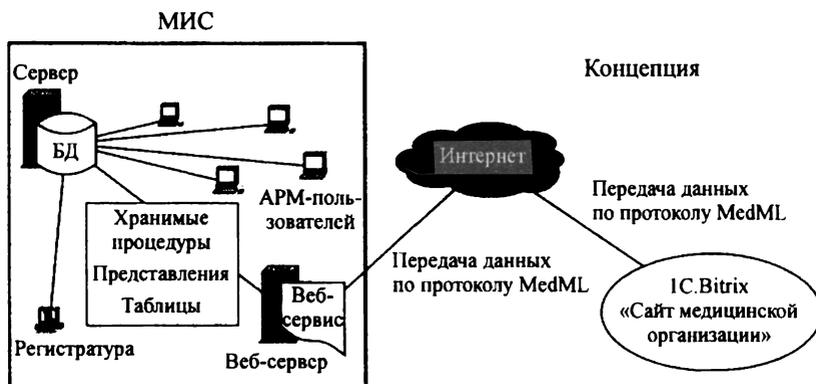


Рис. 1. Концепция работы системы

С одной стороны, имеется МИС, в которой существует возможность ведения справочной информации по работе учреждения, оказываемым услугам, специалистам, имеются функции составления расписания, организации записи на прием через регистратуру.

С другой стороны, система 1С.Bitrix «Сайт медицинской организации» содержит тот же набор функций, что и МИС, только запись на прием осуществляется через онлайн-регистратуру. Для поддержания справочников в актуальном состоянии необходимо обеспечить взаимодействие двух систем.

Главной системой при организации обмена данными является МИС, в которой происходит модификация списков врачей, услуг, расписания, которые выгружаются на сайт.

Что касается записи на прием, то при самозаписи через Интернет, веб-сайт должен запрашивать у МИС разрешение на указанное время и исполнять запись только после подтверждения.

Так как выбранный веб-сайт на платформе 1С.Bitrix способен осуществлять обмен данными только по протоколу MedML, стандартизированному формату взаимодействия медицинских систем, а также использовать для передачи технологию SOAP, то синхронизирующим объектом между МИС и веб-сайтом будет выступать веб-сервис.

Взаимодействие МИС и веб-сервиса представляется следующим образом: в БД МИС создаются хранимые процедуры и представления, что делает веб-сервис универсальным, так как при изменении структуры МИС не придется менять сервис, достаточно будет организовать формирование представлений в надлежащем виде. Более того, данный веб-сервис можно использовать для интеграции в другие МИС, единственной задачей модификации структуры будет создание необходимых представлений и таблиц в БД МИС.

Для экономии трафика реализован механизм выгрузки только изменений с момента последнего обновления БД веб-сайта.

Система 1С.Bitrix периодически (временной интервал настраивается на стороне сайта) отправляет запрос серверу о выгрузке на сайт обновившихся данных. Если на сайте происходит запись на услугу, то запрос сразу же отправляется веб-сервису, где с помощью процедуры осуществляется проверка по двум параметрам: не записан ли пациент на данное время к другому врачу или не занято ли время у этой услуги. При отрицательных ответах на сайт возвращается сообщение о подтверждении записи, в ином случае пользователь получает отказ с объяснением причины.

Веб-сервис имеет всего две функции: «ОбработатьДокумент» и «ПолучитьДанные».

Первая операция – «ОбработатьДокумент» – предназначена для заказа или отмены услуг. Операция имеет один двунаправленный параметр (входной и выходной), который имеет тип <Документ>, описанный в стандарте MedML. Свойство <Операция> параметра <Документ> должно иметь значение «Заказ услуг» или «Отмена услуг», в зависимости от необходимой функции.

Вторая операция – «ПолучитьДанные» – предназначена для получения данных об организации в целом, расписании ее работы, оказываемых в ней услугах. Кроме этого, операция может передавать документы, отменяющие по каким-либо причинам услуги, ранее заказанные с сайта. Операция имеет один двунаправленный параметр (входной и выходной) с именем <Параметры>, который может иметь вложенные теги-параметры:

- «ВыгрузкаОрганизаций» – выгружаемый пакет содержит информацию об организации, включающую в себя структурные подразделения организации, медицинские кабинеты, врачей.

- «ВыгрузкаУслуг» – выгружаемый пакет – это список медицинских услуг, доступных для заказа в рамках соглашения, указанного в узле плана обмена.

- «ВыгрузкаРасписания» – выгружаемый пакет состоит из расписания работы медицинских кабинетов с указанием врача и доступных в этом кабинете услуг. Если при этом wsdl-серверу передан параметр «ВыгружатьТолькоИзменения», то выгружаются только изменения в расписании с момента последнего обновления.

- «ВыгрузкаПакетаПредложений» – выгружаемый пакет содержит пакет предложений, содержащий цены на медицинские услуги. Цены формируются на основе соглашения, указанного в узле плана обмена.

При описании концепции, в процессе разработки сервиса встал вопрос о передаче обновленных данных из МИС на сайт, так как при изменении одной позиции расписания нецелесообразно опять передавать все расписание целиком.

Поэтому для оптимизации работы и устранения данной проблемы были созданы дополнительные таблицы по каждому выгружаемым данным (рис. 2).

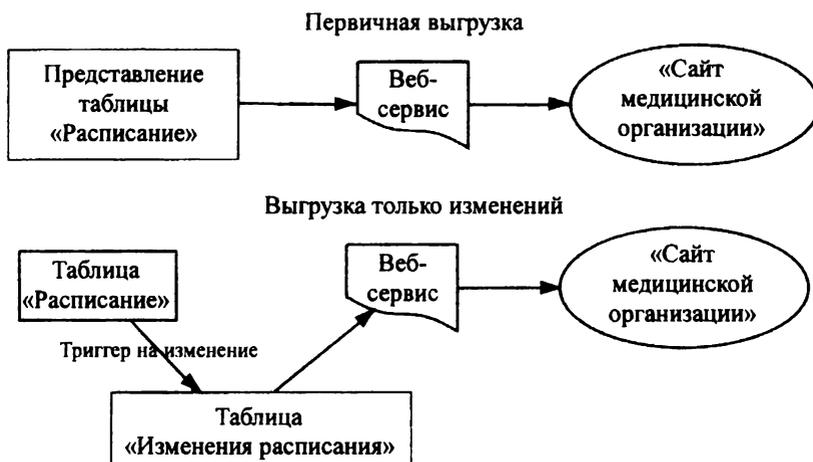


Рис. 2. Схема выгрузки данных

Передаваемые по сети данные являются обезличенными и не несут в себе интересной информации для перехвата с целью кражи информации [2]. Нарушение целостности данных при передаче также является неактуальной угрозой, так как нет оправданных мотивов для подмены. Ввиду того, что веб-сервер, на котором располагается веб-сервис, находится в пределах контролируемой зоны, угроза нарушения его работоспособности также является неактуальной.

Наиболее актуальной угрозой является DDoS-атака, что может быть выгодно организациям-конкурентам для подрыва репутации медицинского учреждения. Как таковых универсальных мер защиты от DDoS-атак нет, поэтому минимизировать риск от такой атаки можно несколькими способами [1]:

- аппаратное решение проблемы: решения от ведущих фирм производителей типа Cisco, Zcom, portel и т. п.;
- программное решение проблемы: система анализа трафика, которая позволит своевременно узнать о начинающейся атаке и вовремя принять меры по ее предотвращению;

- работа веб-сервера: простая и быстрая перезагрузка, а также организация второго административного сетевого интерфейса, через который можно получить доступ к серверу в случае загрузки основного канала.

Актуальной угрозой является возможность доступа в локальную сеть ЛПУ через сеть Интернет через веб-сервис. Оптимальным вариантом минимизации рисков от этой угрозы является установка firewall на границе веб-сервиса и общественной сети, закрытие всех портов, кроме 80, для доступа к веб-сервису. Кроме того, целесообразно выделить БД МИС и веб-сервис в изолированную сеть и для веб-сервиса создать отдельного пользователя в БД МИС с ограниченными возможностями на чтение представлений, таблиц и запуск хранимых процедур.

Таким образом, разработанный веб-сервис обеспечивает взаимодействие МИС и 1С.Bitrix «Сайт медицинской организации» и предоставляет возможность подачи, обработки записи через веб-сайт и синхронизацию справочников услуг, специалистов и расписания. Сервис осуществляет возможность выгрузки только изменившихся данных из МИС на сайт, что позволяет существенно снизить трафик передаваемой информации.

Библиографические ссылки

1. *Захаров А. А., Оленников Е. А., Широких Е. А., Воробьев А. М.* О некоторых подходах к информационной защите электронной очереди ЛПУ // Вестн. УрФО. 2012. № 1 (3). С. 78–84. (Безопасность в информационной сфере).

2. *Воробьев А. М.* Использование интернет-технологий с целью за-
владения персональными данными пользователя // Безопасность инфор-
мационного пространства : сб. ст. Тюмень : Изд-во Тюм. гос. ун-та, 2012.
С. 120–123.

3. Стандарт MedML // Справочно-информационный интернет-портал medml.ru, 2011 [Электронный ресурс]. Режим доступа: <http://medml.ru/>, свободный (дата обращения: 20.05.2013).