- защита хэшированных паролей в БД от «радужных таблиц»;
- водяные знаки на графическом контенте.

Социальная сеть в сфере здравоохранения является оптимальным решением для обмена опытом между врачами, студентами и пациентами, в том числе и международного обмена опытом; для распространения медицинской информации для пациентов, профессионалов и широкой общественности; для облегчения доступа к новейшим и наиболее актуальным медицинским данным с помощью сети интернет.

УДК 339.138

Студ. В. А. Бельмач
Науч. рук. доц. Н. Н. Буснюк
(кафедра информационных систем и технологий, БГТУ)

ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ ОБМЕНА СООБЩЕНИЕ ДЛЯ ОБМЕНА С ИСПОЛЬЗОВАНИЕМ ХЕШ-СТЕГАНОГРАФИИ

Стеганография – способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи. Этот термин ввел в 1499 году в Шпонгейме Иоганн Тритемий в своем трактате «Стеганография», зашифрованном под магическую книгу.

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку [1].

Для реализации данного метода было создано приложение, для разработки которого, в качестве СУБД использовалось MS SQL Server 2014. Основной технологией приложения является ASP .NET MVC версии 5.2. Доступ к базе данных осуществляется с помощью Entity Framework. Для разработки клиентской части применялись технологии Bootstrap 4, HTML5, jQuery. В качестве системы авторизации и аутентификации используется стандартная ASP .NET Identity.

Обмен сообщениями реализовано с помощью SignalR– библиотека для ASP.NET, которая упрощает добавление в приложения компонентов, работающих в реальном времени (простые чаты, более сложные многопользовательские видеоконференции). Библиотека предоставляет простой API для создания функционала, который позволяет вызывать функции JavaScript на стороне клиента из серверного кода, написанного с помощью языков платформы .NET. SignalRобрабатывает все подключения и автоматически рассылает сообщения всем подключенным клиентам либо каким-нибудь специфическим клиентам.

Преимуществом SignalR является то, что при создании подключения библиотека выбирает, если доступно, технологию WebSocket, так как это наиболее оптимальная технология, наиболее эффективно использующая память сервера. В то же время WebSocket может использоваться только на серверах под управлением Windows Server 2012 или Windows 8 и при наличии установленного .NET Framework 4.5. При этом также должна поддерживаться и браузером клиента. И если WebSocket недоступна на сервере или клиенте, то выбирается другой транспорт.

Если WebSocket недоступен, то SignalR использует технологию Server Sent Events, при ее поддержке сервером и клиентом. При невозможности использования данной технологии применяются скрытые фреймы – Forever Frames. Но если Forever Frames также недоступны, то применяется Long Polling. Например, если на стороне клиента браузер IE 8 и ниже, то используется Long Polling [2].

Суть хеш-стеганографии довольно-таки проста. Берем большое количество картинок или, как вариант, их можно сгенерировать. После чего берем хеш-функцию, например, MD5 и прогоняем все картинки через нее и результаты заносим в базу данных в виде «картинка – хеш». Это основа алгоритма, которую будем использовать при отправке сообщения. Предположим, что мы хотим передать сообщение – «алгоритм». Сообщение разбивается на буквы, каждую букву переводим в шестнадцатеричный формат, после чего выбираем первые 2 полубайта и ищем в базе данных картинку, с которой совпадает хеш. После того как нашли картинку передаем ее в канал. Это делается до тех пор, пока на каждую букву в нашем сообщении не найдется соответствующая картинка.

К данному алгоритму будет проведет небольшой апгрейд – это удаление картинки из базы данных после её применения, чтобы повторно её не использовать [3].

Результатом выполнения данной работы является веб-приложение, с помощью которого можно обмениться сообщениями с использованием хеш-стеганографии.

ЛИТЕРАТУРА

1. Стеганография [Электронный ресурс] – https://ru.wikipedia.org/wiki/Стеганография

2. Введение в SignalR 2 [Электронный ресурс] – https://metanit.com/sharp/mvc5/16.1.php

3. Хеш-стеганография [Электронный ресурс] – https://habrahabr.ru/post/272935/