УДК 004.4

ИСПОЛЬЗОВАНИЕ SSL В ИНФОРМАЦИОННОЙ СИСТЕМЕ УНИВЕРСИТЕТА

Казаков В.Е., к.т.н., доц., Деркаченко П.Г., ст. преп., Бизюк А.Н., ст. преп.

Витебский государственный технологический университет,
г. Витебск, Республика Беларусь

Реферат. *В статье рассматривается круг вопросов, связанных с интеграцией SSL в информационную систему университета.*

Ключевые слова: информационная система, Spring Boot, SSL, HTTPS.

При использовании информационной системы университета [1] возникла необходимость защитить персональные данные абитуриентов, регистрирующихся в клиентском приложении «Личный кабинет абитуриента». Это клиентское приложение использует внутренние сервисы информационной системы университета, в частности авторизационный сервис. Однако данный клиент функционирует не в закрытой локальной сети университета, а в публичном доступе Интернет. В этом случае персональные данные, которые вводит в систему абитуриент, должны передаваться по защищённому каналу, чтобы сторонний пользователь Интернета не смог получить к ним доступ во время их передачи.

Для организации защищённого соединения было принято решение использовать технологию SSL.

SSL (Secure Sockets Layer — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь между узлами публичной сети. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений [2].

При использовании SSL-протокола информация передается в закодированном виде по HTTPS и расшифровать ее можно только с помощью специального ключа в отличие от привычного протокола HTTP. Для работы SSL-протокола требуется, чтобы на сервере был установлен SSL-сертификат. SSL-сертификат – это своего рода уникальная цифровая подпись сайта, доменного имени, на котором размещён сайт.

Компании, предоставляющие хостинговые услуги, зачастую предоставляют за дополнительную плату или без сертификаты для сайтов, размещаемых клиентом на их площадке. В этом случае, может возникнуть ряд ограничений при использовании данного сертификата вне площадки хостера, а, поскольку информационная система университета размещается на собственных серверах, то в нашем случае такой способ получения сертификата неудобен.

Сертификат можно приобрести в соответствующей организации (например, Let's Encrypt). В интересах развития безопасного Интернета такие организации могут выдавать сертификаты бесплатно, на определённое время с возможностью повторного получения нового.

Сертификат можно сгенерировать (подписать) самостоятельно с помощью различных утилит, встроенных в системы разработки программного обеспечения и операционные системы [3]. Самоподписанные сертификаты используются, в частности, в процессе разработки и тестирования программного обеспечения.

Для генерации самоподписанного сертификата в операционной системе Windows имеется встроенная программа keytool. Данную программу нужно запустить из командной строки при помощи команды keytool -genkeypair с некоторыми параметрами.

УО «ВГТУ» был закуплен постоянно действующий сертификат на домен vstu.by, который также используется для основного портала университета.

Следующим этапом работы по обеспечению защиты персональных данных стала интеграция технологии SSL в информационную систему университета. Как видно из рисунка 1, все внешние подключения к системе из сети Интернет проходят через один сервис (API Gateway). Остальные взаимодействия между сервисами системы происходят внутри локальной сети университета. Следовательно, взаимодействие по защищённому протоколу необходимо обеспечить между внешними клиентами и шлюзовым сервисом.

Для клиента изменения будет касаться только URL-адресов, по которым клиент обращается к сервисам. Адреса останутся теми же, измениться только протокол, по

которому клиент будет обращаться к системе. Эти изменения будут касаться не только внешних клиентов, таких как «Личный кабинет абитуриента», но и внутренних клиентов, поскольку и для тех, и для других используется один и тот же шлюзовой сервис.

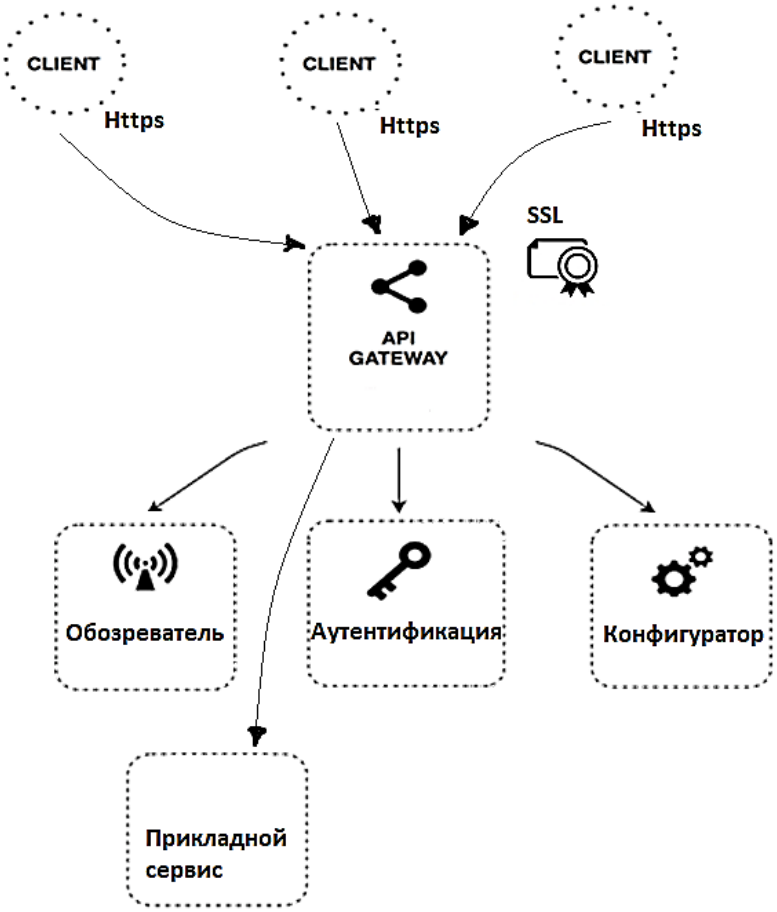

Рисунок 1 – Интеграция SSL в информационную систему университета

Информационная система университета, в том числе и сервис API Gateway, разработана на основе фреймворка Spring Boot. Spring Boot – это стандартное расширение фреймворка Spring для конфигурирования программных продуктов корпоративного уровня, позволяющее создавать автономные приложения, которые можно «просто запустить» [4].

Для добавления сертификата в Spring Boot приложение следует скопировать этот сертификат в папку src/main/resources данного приложения.

Spring Boot предоставляет набор декларативных свойств, позволяющий без дополнительного кодирования внедрить в приложение и настроить различные инструменты, в том числе и SSL (security.require-ssl, server.ssl). Для этого достаточно в конфигурационном файле spring boot приложения инициализировать их соответствующими значениями.

Далее можно добавить в конфигурационный класс переопределение внутренней фабрики контейнеров сервлетов EmbeddedServletContainerFactory, чтобы создаваемый контейнер мог перенаправлять все http запросы на защищённый канал https [5].

В итоге информационная система университета повысила уровень защиты данных от несанкционированного доступа как при их передаче в сети Интернет, так и в пределах локальной сети университета.

Список использованных источников

1. Казаков, В. Е. Микросервисная среда для организации информационной системы университета / В. Е. Казаков, К. Н. Ринейский, М. В. Глушнев, С. С. Ланин // Материалы докладов 51 Международной научно-технической конференции преподавателей и студентов / УО «ВГТУ». – Витебск, 2018. – С. 5–8.
2. Материалы сайта ssl.com [Электронный ресурс]. – Режим доступа:

https://www.ssl.com/faqs/faq-what-is-ssl/. – Дата доступа: 03.05.2020.
3. Материалы сайта Справка–Google Domains [Электронный ресурс]. – Режим доступа: https://support.google.com/domains/answer/7630973?hl=ru. – Дата доступа: 03.05.2020.
4. Материалы сайта spring.io [Электронный ресурс]. – Режим доступа: https://spring.io/projects/spring-boot. – Дата доступа: 13.04.2020.
5. Как настроить HTTPS в Spring Boot материалы сайта java-master.com [Электронный ресурс]. – Режим доступа: https://java-master.com/%D0%BA%D0%B0%D0%BA-%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B8%D1%82%D1%8C-https-%D0%B2-spring-boot. – Дата доступа: 13.04.2020.

УДК 535.375.51

ПРИЧИНЫ СВЕРХПОГЛОЩЕНИЯ В ЛЮТЕЦИЙ АЛЮМИНИЕВОМ ГРАНАТЕ, АКТИВИРОВАННОМ ИОНАМИ ТУЛИЯ

Корниенко А.А.[1], проф., Фомичева Л.А.[2], доц., Дунина Е.Б.[1], доц.

[1]Витебский государственный технологический университет, г. Витебск, Республика Беларусь

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

Реферат. *Для устранения противоречия между наблюдаемой интенсивностью полосы поглощения $^3H_6 \rightarrow {}^3F_4$ иона тулия в монокристалле $Lu_3Al_5O_{12}$ и измеренным временем жизни уровня $^3F_4$ выдвинута гипотеза о дополнительном или сверх поглощении, вызванном двухфотонными процессами. Установлено, что мультиплеты $^3H_6$, $^3F_4$, $^3H_4$ образуют трехуровневую систему приблизительно с эквидистантным расположением, для которой может реализоваться резонансное двухфотонное поглощение. Анализ экспериментальных данных показал, если предполагаемые двухфотонные процессы исключить, то радиационное время жизни уровня $^3F_4$ хорошо согласуется с экспериментальным значением и противоречие между данными по поглощению и излучению устраняется. Возможность реализации предполагаемых двухфотонных процессов подтверждена теоретическими расчетами.*

Ключевые слова: ион тулия, $Lu_3Al_5O_{12}$, аномально сильное поглощение.

Интенсивность излучения на некоторой длине волны взаимосвязана с интенсивностью поглощения на этой же длине волны. При определенных условиях, нет промежуточных уровней между возбужденным уровнем и основным, или коэффициент ветвления люминесценции с возбужденного уровня на основной значительно больше коэффициентов ветвления на промежуточные уровни, эта взаимосвязь будет однозначной – чем больше интенсивность поглощения, тем больше интенсивность излучения и меньше время жизни возбужденного уровня. У иона тулия первый возбужденный уровень $^3F_4$, средняя энергия 5831 см$^{-1}$. Для перехода $^3H_6 \rightarrow {}^3F_4$ измерена интенсиность поглощения, она характеризуется силой осциллятора $f_{\text{expt}} = 1.45 \times 10^{-6}$ и измерено время жизни $\tau_{\text{expt}}(^3F_4) \approx 10000$ мкс. Эти экспериментальные данные противоречат друг другу. Противоречие состоит в том, что согласно измеренной силе осциллятора абсорбционного перехода $^3H_6 \rightarrow {}^3F_4$, излучательное время жизни должно быть $\tau_{rad}(^3F_4) = 6650$ мкс, что в 1.5 раза меньше наблюдаемого или флюоросцентного времени. Так как из-за различных процессов в реальном кристалле (столкновения, перенос энергии, тепловое движение) флюоросцентное время всегда меньше или, в крайнем случае, равно излучательному, то выявленное противоречие требует принципиально нового объяснения. Для объяснения этого противоречия в данной работе сделано предположение, что на длине волны перехода $^3H_6 \rightarrow {}^3F_4$ есть дополнительное или сверх поглощение. У иона тулия основной мультиплет $^3H_6$ и