https://developer.nvidia.com/nvidia-video-codec-sdk [Дата обращения: 29 марта 2018].

3. Свободная энциклопедия «ВикипедиЯ» [Электронный ресурс] / Nvidia NVENC – Режим доступа: https://en.wikipedia.org/wiki/ Nvidia_NVENC [Дата обращения: 29 марта 2018].

Д.А. Симаков (ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **П.Л. Чечет**, канд. техн. наук, доцент

ОСНОВНЫЕ МЕХАНИЗМЫ РЕАЛИЗАЦИИ СИСТЕМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ПРОЕКТЕ ПО ЗАКАЗУ БИЛЕТОВ НА РАЗВЛЕКАТЕЛЬНЫЕ МЕРОПРИЯТИЯ

Так как не все пользователи в системе имеют доступ к базе данных или изменению данных других пользователей, необходимо использовать какие-то механизмы защиты и разделение прав пользователей.

Аутентификация служит для проверки принадлежности субъекта системы (пользователя) в соответствии с предоставленными им данными: паролю, цифровой подписи или цифровому ключу (токену).

Аутентификация, с которой часто путают авторизацию (предоставление прав) и идентификацию (распознавание субъекта по идентификатору), является средством защиты зарегистрированных пользователей от доступа к их личным данным.

Самые простой способ защиты пользователей от злоумышленников – это использование аутентификации по логину (идентификатору) и паролю пользователя. При передаче пароля между клиентом и сервером, он шифруется.

Однако даже в случаях шифрования пароль в таких случаях должен подчинятся политике безопасности, чтобы еще сильнее уменьшить вероятность взлома. При регистрации пароль пользователя должен соответствовать некоторым критериям, указанных либо в процессе регистрации, либо прописанных в документации политики безопасности. От степени надежности пароля зависит сколько времени потратит злоумышленник на получение доступа к конфиденциальным данным.

Для еще большей защищенности системы и её пользователей, был разработан протокол аутентификации Kerboros. Суть протокола заключается в том, что если предположительно среда передачи данных считается незащищенной, то вводится еще один посредник для взаимодействия между клиентом и сервером – сервер аутентификации. В таком случае клиент проходит аутентификацию сначала на сервере аутентификации,

получает ключ (токен) и с этим ключом пытается получить доступ уже на сервер где расположен веб-сайт или веб-приложение. При этом сервер приложения и сервер аутентификации знают, как этот ключ расшифровать и какие данных оттуда извлечь. Такой способ более эффективен чем простое использование пароля.

Используя такой подход при разработке проекта, регистрация пользователя занимает столько же времени, сколько при использовании простой незащищенной регистрации с помощью логина и пароля, при этом обеспечивая больший уровень защиты.

В роли сервера аутентификации в пределах данного проекта достаточно использовать веб-сервисы. Используя методологию Kerberos, для построения подобной системы использовались WebAPI, используемый для создания сервера аутентификации, и WCF (Windows Communication Foundation) как веб-сервисы доступа к данным (например, доступ к базе данных пользователей).

При авторизации со стороны клиента поступает запрос на сервис аутентификации WebAPI, где проверяется верны ли введенные данные (соответствует ли пароль логину пользователя), после чего клиенту возвращается токен, с помощью которого пользователь делает запрос к серверу, которые проверяет соответствует ли данный токен введенным данным пользователя (тоже с помощью сервиса аутентификации). Только после всех вышеперечисленных этапов происходит процесс аутентификации пользователя, т.е. предоставляются определенные права (или запреты) на различные операции.

Таким образом удалось создать веб-приложение, которое в достаточной мере защищено защищенное от злоумышленников и взломщиков.

Д.А. Симаков (ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **П.Л. Чечет,** канд. техн. наук, доцент

РАЗРАБОТКА АВТОМАТИЗИРОВАННЫХ ТЕСТОВ ДЛЯ ПРОЕКТА ПО ЗАКАЗУ БИЛЕТОВ НА РАЗВЛЕКАТЕЛЬНЫЕ МЕРОПРИЯТИЯ С ПОМОЩЬЮ МЕТОДА РАЗРАБОТКИ ЧЕРЕЗ ТЕСТИРОВАНИЕ

Тестирование программного обеспечения (или/и модульных частей приложения) – процесс проверки соответствия между действительным поведением программы и ее ожидаемым поведением с помощью конечного набора тестов.

Тестирование позволяет выявить наличие потенциальных ошибок, которые могут возникнут в процессе работы приложений, незначительных