

УДК 78.07:004.056

Панкова А.А., Зайченко Е.А.
МУЗЫКАЛЬНЫЕ КОНКУРСЫ В КИБЕРПРОСТРАНСТВЕ:
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ

Панкова Анастасия Андреевна, обучающаяся Белорусско-Российского университета; 212000, Республика Беларусь, г. Могилев, проспект Мира, 43; e-mail: rankko089@gmail.com.

Зайченко Елена Аркадьевна, старший преподаватель Белорусско-Российского университета; 212000, Республика Беларусь, г. Могилев, проспект Мира, 43; e-mail: helena.zai@mail.ru.

***Аннотация:** В статье рассматривается важность музыкальных конкурсов как платформы для открытия и поддержки новых талантов, а также как инструмента для продвижения музыкальной культуры и искусства. Акцент делается на предоставлении безопасности пользователей системы и их данных. Оговариваются технологии, с помощью которых можно защитить пользовательские данные. Предлагается использовать ролевую модель доступа для разграничения возможности пользователей системы.*

***Ключевые слова:** музыкальные конкурсы, безопасность данных, ролевое управление доступом, личные данные, ASP.NET Core MVC, Identity Framework, веб-приложения.*

Pankova A. A., Zaichenko E.A.

MUSIC COMPETITIONS IN CYBERSPACE: DATA SECURITY AND INFORMATION SECURITY

***Abstract:** The article examines the importance of music competitions as a platform for discovering and supporting new talents, as well as as a tool for promoting musical culture and art. The emphasis is on providing security to system users and their data. The technologies that can be used to protect user data are discussed. It is proposed to use a role-based access model to differentiate the capabilities of users of the system.*

***Keywords:** music contests, data security, personal data, ASP.NET Core MVC, Identity Framework, web applications.*

Музыкальные конкурсы представляют собой уникальную платформу для выявления и поддержки талантливых музыкантов независимо от их местонахождения и социального статуса [1]. Они служат мощным катализатором развития музыкальной индустрии, поощряют разнообразие и инновации. Участие в музыкальных конкурсах дает артистам возможность продемонстрировать свой талант перед широкой аудиторией и получить признание профессионалов индустрии. Организаторы музыкальных конкурсов заинтересованы в создании увлекательной атмосферы и обстановки для конкурсантов. Они тщательно планируют и структурируют мероприятие, предлагая разнообразные категории и жанры, чтобы предоставить участникам выбор и возможность продемонстрировать свою уникальность. На них лежит ответственность за то, чтобы конкурс был честным и прозрачным, должна быть обеспечена гарантия объективной оценки и справедливые условия для всех участников. Участники музыкальных конкурсов не только соревнуются за призы и звание победителя, но и способствуют развитию музыкальной культуры в целом. Молодые и перспективные музыканты могут учиться у опытных коллег и получать обратную связь от экспертов. Такие мероприятия стимулируют музыкантов постоянно совершенствовать свое мастерство и открывать новые музыкальные направления.

На данный момент конкурсы становятся всё более доступными благодаря развивающимся технологиям и разработке различных платформ, позволяющих большей аудитории наблюдать и участвовать в подобного рода мероприятиях. Таким образом, создается глобальное сообщество поклонников музыки, объединяющее людей разных культур и национальностей, объединенных общей страстью к музыке. В целом музыкальные конкурсы – это значимые события, которые способствуют развитию талантов, продвижению музыкальной культуры и созданию связей в музыкальном сообществе. Они вдохновляют людей, объединяют их и служат платформой для творческого самовыражения и взаимного обучения.

По мере роста популярности и доступности музыкальных онлайн-конкурсов все большее значение приобретают вопросы безопасности и защиты данных. В наш цифровой век, когда личные данные и аудиозаписи могут быть легко скопированы и использованы без разрешения, крайне важно защитить данные участников и их конфиденциальную информацию. Музыкальные конкурсы часто требуют от участников предоставления личных данных, таких как контактная информация, адреса электронной почты и даже музыкальные записи. Такие данные могут быть подвержены различным угрозам, таким как несанкционированный доступ, кража данных и фишинг. Поэтому безопасность данных – важный аспект организации музыкального конкурса. Кроме того, в контексте музыкальных конкурсов значительную роль играют вопросы безопасности идентификации и аутентификации пользователей. Участники, жюри и администраторы конкурсов должны иметь возможность безопасно входить в систему и получать доступ к функциям приложения. В разрабатываемой системе планируются следующие категории пользователей:

1) Администратор. Осуществляет управление системой, имеет возможность выполнять множество операций по конфигурированию и настройке веб-приложения;

2) член жюри. Имеет возможность просматривать загруженные участниками медиа-материалы, выставять оценки. Для него организован личный кабинет, имеется возможность обсуждений в чате с другими участниками жюри;

3) участник конкурса. Имеет возможность зарегистрироваться, создать личный кабинет, загружать видео- и аудиофайлы, задавать вопросы и получать рекомендации как от членов жюри, так и от других участников конкурса.

Для обеспечения прав доступа планируется использовать ролевое управление доступом (role-based access control или RBAC). Между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права [2]. Роль – это набор полномочий, который необходим пользователю или группе пользователей для выполнения определённых рабочих задач. В модели, использующей контроль доступа на основе ролей, роли основаны на нескольких критериях, и могут включать в себя авторизацию, ответственность и профессиональную компетентность. Кроме того, доступ к ресурсам может быть ограничен конкретны-

ми задачами, такими как возможность просмотра, создания или изменения файлов. Принцип работы ролевой модели показан на рисунке 1.

Роль (ответ на вопрос «Что?») подразумевает те действия, которыми планируется наделить пользователя, т.е. что он должен иметь право делать.

Группа ролей («Кто?») определяет перечень пользователей системы, то есть кто именно может выполнять обозначенные в вопросе «Что?» действия.

Область (ответ на вопрос «Где?») определяет перечень объектов (файлы, папки), на которые планируется давать разрешения.

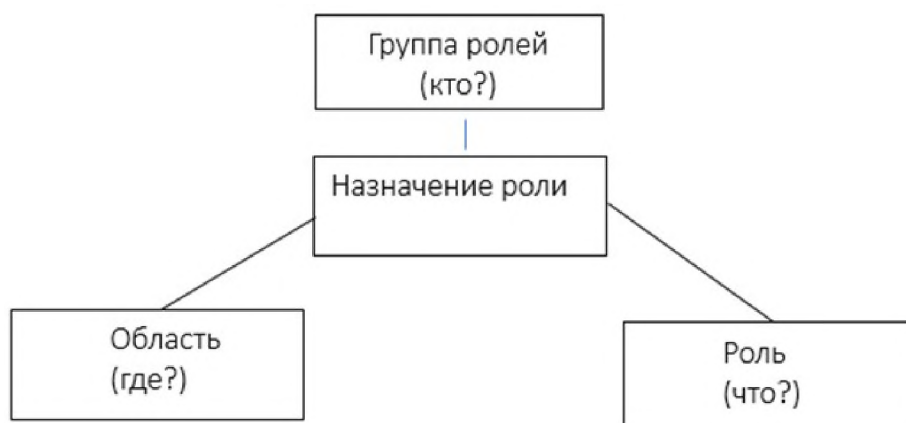


Рис. 1. Принцип работы ролевой модели доступа

Источник: составлено автором

Несомненным достоинством такой модели является простота назначения прав, потому что количество ролей существенно меньше, чем пользователей информационной системы. Кроме того, ролевая модель защищает от выдачи несовместимых полномочий. Учитывая эти проблемы, при разработке веб-приложения, направленного на создание платформы для участия в музыкальном конкурсе, необходимо знать о лучших практиках и технологиях, которые помогут обеспечить безопасность данных и информации.

ASP.NET Core MVC и Identity Framework предоставляют мощные инструменты для их решения, что делает их идеальным выбором для разработки, с обеспечением надежности и безопасности данных пользователей. Говоря о вышеупомянутых технологиях, следует более детально остановиться на каждой, чтобы наверняка понять какие удобства и возможности она предоставляет в разработке. Архитектурный паттерн Model-View-Controller (MVC) [3] делит приложение на три основные группы компонентов: модели, представления и контроллеры. Этот паттерн помогает обеспечить разделение обязанностей. В этой модели запросы пользователей направляются контроллеру, который манипулирует моделью, чтобы выполнить действия для пользователя или получить результаты запроса. Контроллер выбирает представления, которые будут показаны пользователю, и предоставляет данные модели, запрошенные пользователем. На диаграмме, представленной на рисунке 2, показаны компоненты и их взаимосвязи. ASP.NET Core – это кроссплатформенный фреймворк, разработанный компанией Microsoft для создания современных, высокопроизводительных и масштабируемых веб-приложений, мобильных

приложений и микросервисов на платформе .NET. Этот фреймворк позволяет создавать приложения, которые могут работать на различных операционных системах, таких как Windows, macOS и Linux, а также в контейнерных средах, таких как Docker.

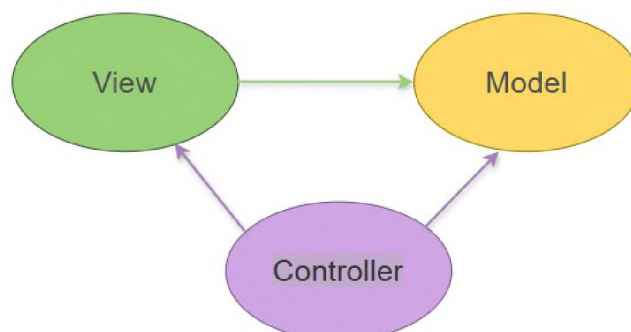


Рис. 2. Основные компоненты паттерна MVC

Источник: составлено автором

К его основным преимуществам можно отнести способность создавать высокопроизводительные веб-приложения за счет оптимизации и использования новых технологий. Помимо этого, ASP.NET Core поддерживает микросервисную архитектуру, которая позволяет проще масштабировать и обновлять компоненты приложения, независимо друг от друга. А также, его можно легко интегрировать с Identity Framework [4]. В свою очередь Identity Framework является компонентом в экосистеме ASP.NET, который предлагает множество сервисов для работы с учетными записями пользователей. С его помощью можно сохранять учетные записи пользователей в своем приложении, обрабатывать информацию о пользователях, обеспечивать дополнительную безопасность с помощью двухфакторной аутентификации и даже подключать к учетным записям пользователей другие параметры входа, например, вход в социальные сети. В общем виде схема данной технологии представлена на рисунке 3.

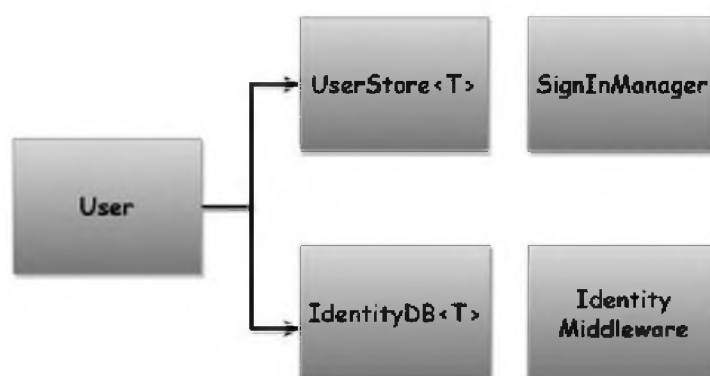


Рис. 3. Схема средств Identity Framework [5]

Компоненты и классы из вышеуказанной схемы предоставляют функционал для обработки, управления и хранения информации о пользователях,

ролях, имеющихся в приложении, и другой информации, необходимой для корректной работы входа в систему и дальнейшего взаимодействия с ней. Identity предоставляет ряд функций для обеспечения безопасности пользователей, включая защиту от несанкционированного доступа и кражи данных. Она дает возможность управлять правами доступа пользователей к различным ресурсам и функциям приложения. Это достигается с помощью системы ролей и политик, которые позволяют легко определять разрешенные действия для каждого пользователя. Для повышения уровня безопасности Identity Framework поддерживает двухфакторную аутентификацию, а для защиты персональных данных пользователей в Identity Framework используется усовершенствованный алгоритм хеширования паролей, который делает невозможным прямое считывание паролей в случае утечки данных.

Таким образом, рассматривая данную технологию, которая поддерживается и получает регулярные обновления, можно с уверенностью сказать, что она является достойным инструментом, позволяющим обеспечивать безопасность и защиту данных пользователей разрабатываемого веб-приложения для музыкального конкурса.

Список использованных источников:

1. Нужны ли музыкальные конкурсы? [Электронный ресурс]. – Режим доступа: <https://art.sovfarfor.com/muzyka/nuzhny-li-muzykalnye-konkursy>
2. Галатенко, В.А. Основы информационной безопасности : Курс лекций / В.А. Галатенко. – Москва : Интуит НОУ, 2016. – 266 с.
3. Общие сведения ASP.NET Core MVC [Электронный ресурс]. – Режим доступа: Overview of ASP.NET Core MVC | Microsoft Learn
4. ASP.NET 8. Что нового в аутентификации и авторизации [Электронный ресурс]. – Режим доступа: ASP.NET 8: What's New About Authentication and Authorization | ABP Community
5. Asp Net Core Identity Overview Tutorials Technology [Электронный ресурс]. – Режим доступа: Identity Framework Core (mavink.com)