

БЕЗОПАСНОСТЬ В ИНТЕГРИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ОРГАНИЗАЦИЙ

Акиншева И.В., Еромов В.В.

**Могилевский государственный университет имени А.А. Кулешова
г. Могилев, Республика Беларусь**

В настоящее время вопросам безопасности и конфиденциальности данных в интегрированных информационных системах различных организаций уделяется значительное внимание

Информационные системы, работающие с конфиденциальными данными (денежные проводки, клиентские базы и пр.), подразумевают контроль и разграничение прав доступа между сотрудниками организации. Для предотвращения несанкционированного доступа к базам данных различных приложений система безопасности организации должна быть тесно интегрирована с системой безопасности системы управления базами данных.

Целью работы является разработка универсального разделения прав доступа и ролей пользователей в информационной системе с использованием механизмов аутентификации.

Практическая значимость работы заключается в автоматизированном разграничении ролей пользователей в информационной системе, устраняющем трудозатратный процесс учета выдачи логинов и паролей, а также разделения уровней управления информационной системой и доступа к данным в общей базе данных системы.

Актуальность представленной работы обусловлена необходимостью для любой организации соблюдать конфиденциальность данных, предназначенных как для внутренних, так и для внешних пользователей информационной системы

Методы защиты объектов в информационных системах должны легко поддаваться абстрагированию. Поэтому логично выделять часть приложения, предоставляющую требуемый уровень абстракции, для последующего многократного использования. Это позволит разработчикам сосредоточиться на реализации основных функций системы в целом, не отвлекаясь на решение проблем, связанных с безопасностью.

В идеале каждый пользователь, имеющий отношение к организации и работающий с данными, являющимися собственностью этой организации, должен получить одну учетную запись. Эта запись станет ключом пользователя ко всем приложениям организации, а доступ ключа к тому или иному приложению интегрированной информационной системы будет регулироваться правами в общей системе безопасности.

Обязанности по регистрации пользователей в приложениях, как правило, возлагаются на администраторов баз данных или на системных администраторов.

Системные администраторы не должны вникать в тонкости физической организации безопасности того или иного приложения (например, какому пользователю какую роль назначить или, в какие таблицы прописывать информацию о нём). Принципы разграничения ролей, присвоения прав пользователям и создания учётных записей должны быть едиными и не зависящими от приложения в общей информационной системе.

Поэтому глобальные настройки разрабатываемого приложения хранятся в отдельных файлах и отвечают за параметры, необходимые для подключения к базе данных: наименование драйвера, адрес базы данных, имена пользователей и пароли.

Представленная функциональность глобальных настроек должна быть доступна только через административную утилиту.

Для автоматизации аутентификации пользователей в разрабатываемом приложении используется аннотация «@Controller», определяющая такой класс как Контроллер в классической модели взаимодействия частей приложения. Части данной аннотации указывают, что все методы в Контроллере относятся к указанным в свойствах аннотации URL-адресам.

В разрабатываемой приложении необходимо использовать шесть контроллеров, четыре из которых являются справочными данными, а два оставшиеся относятся к сущностям «Orders» и «User».

Чтобы получить функционал приложения, доступный для пользователя, необходимо авторизоваться. Для этого надо нажать на кнопку «Войти» на заголовочном меню представления приложения. После нажатия на данную кнопку, будет открыта специальная форма для ввода данных пользователя (рисунок 1). Если данные пользователя не верны, то форма откроется снова и в ней появится уведомление о неверно введенных данных. Такие же действия предельно администратор для доступа к функционалу приложения, находящемуся в его компетенции.

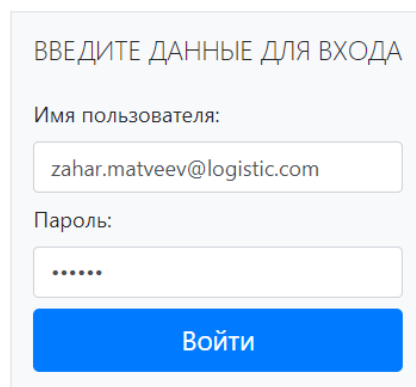


Рисунок 1 – Форма авторизации

Приложения, входящие в интегрированную информационную систему организации, взаимодействуют с базой системы безопасности посредством собственной базы данных, а не через клиентские части. Это избавляет администратора от проблем, связанных с модификацией системы безопасности в будущем.

Выполненная универсальная часть приложения может найти практическое применение при дальнейших разработках всего комплекса приложений, входящих в интегрированную информационную систему организации для автоматизации процесса аутентификации групп пользователей.

Список использованных источников

1 Гарнаев, А. WEB-программирование на Java и JavaScript / А. Гарнаев, С. Гарнаев. – Москва: СПб. : Питер, 2017. – 718 с.

2 СТБ ISO/IEC 27001-2016 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»