Федеральное государственное бюджетное образовательное учреждение высшего образования

Саратовский государственный технический университет

имени Гагарина Ю. А.

Система банковских платежей

СОГЛАСОВАНО  
Руководитель работы  
\_\_\_\_\_\_\_.\_\_.2022г.

Разработчики:

Студент с1-ИБС-42  
\_\_\_\_\_ ***Солодилов В.В.***  
\_\_.\_\_.2022г.

**Введение**

Веб-приложение «Система банковских платежей» предназначена для проведения платежей между коммерческими организациями, а также для осуществления оплат различных услуг в пользу юридической организации со стороны пользователя. Банк осуществляет хранение денежных средств, а также обработку и проверку осуществления проведенных платежей.

1. **Постановка задачи**

Коммерческий банк заключает договора с различными юридическими лицами для приема платежей населения за оказываемые услуги. Каждое юридическое лицо может иметь несколько расчетных счетов, на которые должны поступить принятые денежные средства, и несколько назначений платежей. На один счет могут поступать платежи по нескольким назначениям, при этом каждому назначению соответствует не более одного счета. Банк имеет несколько филиалов, в каждом из которых осуществляется прием платежей. Необходимо разработать информационную систему, позволяющую хранить информацию о принятых банком платежей с полным набором реквизитов в течение календарного года, а также реализовать возможность проведения платежей как физическим лицом, так и между коммерческими лицами.

Дополнительно предусмотреть возможность изменения реквизитов организации-получателя платежей, при этом реквизиты уже принятых платежей должны быть доступны для просмотра, как с учетом изменения реквизитов, так и с изначальными реквизитами.

1. **Назначение разработки**

Разработка веб-приложения ведётся в рамках курсовой проекта по дисциплине «Безопасность систем баз данных». Приложение предназначено для хранения и просмотра проведенных платежей в пользу организаций со стороны пользователя или других организаций. Для каждого лица хранения информации о проведенных платежах происходит отдельно. Предусмотрено разграничения ролей на «Пользователь», «Юридическое лицо», «Менеджер», «Администратор».

1. **Функциональная часть**

Для выполнения поставленной задачи необходимо реализовать следующий функционал:

* Регистрация юридического и физического лиц
* Изменение расчётных данных юридического лица
* Удаление данных юридического или физического лиц
* Проведение платежей в сторону юридического лица пользователей или между юридическими лицами
* Хранение и просмотр информации о проведенных платежах
  1. **Требования к приложению**

Данные о физических и юридических лицах, расчётных счетах, а также проведенных платежей хранятся в базе данных. Обеспечивается разграничение прав доступ к данным:

1. Пользователь или организация имеют право на чтение информации о проведенных платежах, со своей стороны.
2. Менеджер имеет право на чтение информации о всех проведенных платежах.
3. Администратор имеет права на чтение и запись информации о всех проведенных платежах.
   1. **Порядок контроля и приёмки**

Контроль и приёмка программы производятся комиссией в составе преподавателя по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем» и студента, выполнившего работу.

1. **Нефункциональная часть**
   1. **Требования к безопасности**

Для обеспечения безопасности пользователей при работе с сайтом используются такие методы, как хеширование паролей при создании учётной записи, а также экранирования каждого SQL-запроса с целью минимизации атаки SQL-инъекции.

Для хеширования паролей применяется алгоритм хеширования MD5, который, на данный момент, позволяет добиться максимальной защищенности исходных данных.

Для обеспечения работы пользователя с сайтом применяются различные методы аутентификации, а также разделения ролей.

* + 1. **Поддерживаемые типы аутентификации**

*Аутентификация по постоянному паролю.*

Для успешной аутентификации пользователь должен предоставить username и password. Пара username/password задается пользователем при его регистрации на сайте, при этом в качестве username может выступать придуманное пользователем имя или адрес электронной почты в случае, если первое не было указано.

При аутентификации пользователь вводит свои данные в HTML-форму, которая отправляется на сервер. В случае успеха веб-приложение создает session token, который помещается в куки браузера. При дальнейшем заходе на сайт это позволит пользователю не вводит постоянно свои данные.

Для сессии установлено ограничение в 15 минут, т.е. при бездействии происходит автоматический выход пользователя из системы, а токен удаляется. В результате этого пользователь должен заново ввести данные для продолжения работы на сайте.

*Аутентификация по одноразовым паролям.*

Реализуется в дополнение к аутентификации по постоянному паролю. Представляет собой случайно сгенерированный код, приходящий на указанную пользователем почту при каждой аутентификации на сайте.

* + 1. **Защищаемый и открытый контент**

В веб-приложении предусмотрено разделение ролей пользователей, поэтому пользователю доступен только тот контент, который находится на его или ниже уровне в иерархии ролей.

Весь контент, который отображается конкретному пользователю при работе с сайтом, является открытым. Защищаемым является контент, который не может быть доступен пользователю из-за несоответствия его роли с требуемой, и конфиденциальная информация о каждом конкретном пользователе, такая как электронная почта, пароль, истории платежей, а также некоторые мелкие операции.

* 1. **Максимальное время отклика**

Для максимального время отклика установлено пороговое значение в 30 секунд, после чего приложение прекратит отвечать на запросы.

* 1. **Пиковая нагрузка**

Для оценки значения пиковой нагрузки на сайт используется следующая формула:

*Количество одновременных пользователей* = (количество пользователей за 2 часа) \* среднее время, проведенное на странице (в секундах) / 3600 секунд / 2 часа.

Выполнив вычисления, получаем:

* Всего сессий за 2 часа = 20 000 сессий
* Среднее время, проведенное на странице = 300 секунд
* Одновременных пользователей = 833 пользователя
  1. **Используемые технологии**

Для обеспечения функционирования веб-приложения необходимо используется следующее программное обеспечение:

1. Операционная система Windows 10
2. СУБД Microsoft SQL Server 2019
3. Язык программирования Java
4. Spring Framework
   1. **Ответственность**

Ответственность за работу приложения лежит на разработчике. В случае выявления неполадки или обнаружения уязвимости необходимо в максимально короткое время устранить выявленные недостатки для обеспечения максимальной работоспособности сайта.