А. В. Маршалов
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **Н. А. Аксенова**, ст. преподаватель

СРЕДСТВА РАЗРАБОТКИ AR ПРОЕКТА

Для разработки приложений дополненной реальности (AR) в Unity будет использоваться Unity AR Foundation. Это мощная среда, которая объединяет базовые функции ARKit, ARCore, Magic Leap и HoloLens, а также уникальные возможности Unity. С её помощью можно создавать надежные приложения, готовые к использованию сотрудниками компании или к выпуску в магазинах приложений.

Некоторые ключевые моменты о Unity AR Foundation:

1. Кроссплатформенность: Вы сможете разрабатывать приложения, которые работают на разных мобильных устройствах и гарнитурах дополненной реальности.

2. Единый рабочий процесс: AR Foundation объединяет функциональность разных платформ, позволяя вам использовать все их возможности в рамках одного проекта.

3. Расширяемость: Если какая-то функция доступна на одной платформе, но пока отсутствует на другой, AR Foundation позволяет добавить её в будущем без переписывания всего приложения.

Так же для тестирования будут использоваться устройства на операционной системе Android, на устройство будет установлено приложение AR Foundation. AR Foundation позволит запустить дополненную реальность на любом устройстве.

У. Д. Мешкова, Е. В. Рафалова
(ГГУ имени Ф. Скорины, Гомель)

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ИНТЕРНЕТА ВЕЩЕЙ

Разработка приложения для интернета вещей (IoT) включает важные этапы, связанные с организацией подключения устройств к сети, контролем этих устройств и обеспечением безопасности данных сети.

Для подключения устройств к сети используются различные технологии и протоколы связи, такие как Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, Ethernet и мобильные сети (например, 4G, 5G).

Каждое устройство должно иметь соответствующий модуль или интерфейс для подключения к выбранной технологии связи. Например, Wi-Fi-устройства должны иметь Wi-Fi-модуль, а Bluetooth-устройства - Bluetooth-модуль.

Важно учесть, что устройства могут использовать разные протоколы связи и иметь различные режимы работы (например, клиент-сервер, peer-to-peer), поэтому приложение должно быть способно взаимодействовать со всеми поддерживаемыми устройствами и протоколами.

Программное обеспечение для IoT предоставляет пользователю возможность контролировать устройства, связанные с системой. Это может включать в себя функции включения/выключения, регулировки параметров, изменения режимов работы и т. д.

Для контроля устройств через приложение используются команды и управляющие сообщения. Приложение отправляет соответствующие команды устройствам через выбранный протокол связи (например, MQTT или HTTP), и устройства выполняют соответствующие действия в ответ.

Пользовательский интерфейс приложения должен предоставлять интуитивно понятные элементы управления, такие как кнопки, ползунки или переключатели, чтобы пользователь мог легко взаимодействовать с устройствами.

Обеспечение безопасности при подключении устройств к интернету важно для защиты данных и предотвращения несанкционированного доступа к системе IoT.

Один из основных аспектов безопасности – защита сетевого соединения между устройствами и приложением. Это может быть достигнуто с помощью протоколов шифрования, таких как SSL/TLS, и использования безопасных протоколов связи, таких как MQTT с поддержкой аутентификации и авторизации.

Дополнительные меры безопасности включают в себя использование паролей, механизмов аутентификации и авторизации, ограничение доступа к функциональности через права доступа пользователей, ролевую модель, мониторинг и обнаружение вторжений, а также шифрование данных и резервное копирование.

Ролевая модель доступа определяет права доступа для различных пользователей или ролей в системе IoT. Например, администратор имеет полный доступ ко всем функциям и устройствам, в то время как обычные пользователи имеют ограниченные права на использование системы.

Мониторинг и обнаружение вторжений помогают обнаружить потенциальные угрозы и аномалии в системе IoT. Система может контролировать необычную активность, попытки несанкционированного доступа или взлома, и предпринимать соответствующие меры для предотвращения вторжений.

Шифрование данных является важным аспектом безопасности при передаче и хранении данных в системе IoT. Использование шифрования позволяет защищать конфиденциальность и целостность данных от чтения или изменения злоумышленниками.

Резервное копирование данных обеспечивает защиту от потери данных в случае сбоев или аварий. Регулярное создание резервных копий данных с помощью надежных методов и их хранение на отдельных устройствах или в облачных сервисах помогает обеспечить возможность восстановления данных в случае необходимости.

Перечисленные аспекты необходимо учитывать при проектировании системы интернета вещей для того, чтобы разработанное программное обеспечение соответствовало установленным критериям качества.

У. Д. Мешкова, Е. В. Рафалова
(ГГУ имени Ф. Скорины, Гомель)

СФЕРЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИНТЕРНЕТА ВЕЩЕЙ

Интернет вещей (IoT) представляет собой концепцию, в рамках которой различные физические объекты, такие как устройства, транспортные средства, домашние приборы и другие предметы, связываются и обмениваются данными через интернет. Эта технология открывает двери для новых возможностей автоматизации, мониторинга и улучшения эффективности в различных областях жизни.

Основные принципы работы IoT:

– подключенность. Устройства IoT обладают возможностью подключаться к интернету, что позволяет им обмениваться данными и коммуницировать друг с другом. Подключенность может быть осуществлена через беспроводные технологии, такие как Wi-Fi, Bluetooth, Zigbee или сотовые сети;

– сбор данных. Устройства IoT позволяют возможность собирать различные типы данных с помощью встроенных датчиков. Эти данные могут включать информацию о состоянии устройства, окружающей среде, расположении, поведении и другие параметры, которые могут быть полезны для анализа и принятия решений;

– обработка данных. Собранные данные могут быть обработаны прямо на устройстве IoT или переданы для обработки на удаленные серверы в облаке. Обработка данных позволяет анализировать информацию, выявлять тренды, прогнозировать события и принимать обоснованные решения на основе данных;