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;

– взаимодействие и управление. IoT позволяет объектам взаимодействовать между собой и с людьми. Устройства могут обмениваться данными, передавать команды и получать инструкции, что открывает двери для создания новых сервисов и бизнес-моделей. От простых умных домов и автономных автомобилей до сложных систем умных городов и промышленных сетей, IoT предоставляет возможности для автоматизации и оптимизации различных процессов;

– безопасность и приватность. С увеличением количества подключенных устройств IoT становится важным обеспечение защиты данных и приватности. Устройства должны быть защищены от несанкционированного доступа и взлома. Технологии шифрования, аутентификации и механизмы контроля доступа играют важную роль в обеспечении безопасности IoT.

IoT стал неотъемлемой частью умного дома. Эта концепция позволяет автоматизировать и управлять различными устройствами в доме, такими как освещение, отопление, системы безопасности и домашние электроприборы. Это создает комфортные условия для жильцов и помогает экономить энергию.

Также IoT используется для управления и мониторинга различных аспектов городской инфраструктуры, включая уличное освещение, системы управления транспортом, учет ресурсов и сбор отходов. Применение IoT технологий повышает качество жизни жителей, улучшает эффективность использования ресурсов и обеспечивает устойчивое развитие. Такой подход называется умным городом.

IoT технологии могут быть использованы для мониторинга здоровья пациентов, управления медицинским оборудованием, автоматизации процессов врачебной диагностики и лечения. Это повышает эффективность здравоохранения, снижает затраты и улучшает результаты лечения.

Технологии интернета вещей (IoT) представляют собой мощный инструмент, способный упростить рутинные действия и привнести новые возможности в различные сферы жизни. IoT позволяет объектам собирать и обмениваться данными, анализировать информацию и принимать обоснованные решения. Однако, с развитием IoT возникают вопросы безопасности и приватности, которые требуют серьезного внимания. С учетом правильного применения и защиты, IoT может стать ключевым фактором в улучшении качества жизни, оптимизации ресурсов и создании новых возможностей для инноваций и развития.

Д. В. Мирош
(БелГУТ, Гомель)
Науч. рук. **В. Н. Галушко**, канд. техн. наук, доцент

ДИАГНОСТИКА ИЗОЛЯЦИИ МАШИН ПЕРЕМЕННОГО ТОКА

Переход к стратегии обслуживания по фактическому техническому состоянию наиболее актуален для широко распространенного оборудования, срок службы которого зависит от многих факторов: характер, условия, режим и длительность выполняемых работ, конструктивные особенности и качество изготовления.

Мониторинг фактического состояния позволяет снизить вероятность внезапных отказов и своевременно оценивать остаточный ресурс объекта исследования. Диагностика неисправностей трехфазных асинхронных двигателей позволит решить различные проблемы на производстве, связанные с внезапностью выхода из строя и сопутствующими рисками, оптимизацией затрат при планировании обслуживания и ремонтных работ.

К текущему моменту имеется множество статей и других литературных источников, описывающих испытания и оценку состояния изоляции обмоток в электрических машинах, в том числе и для асинхронных двигателей (далее – АЭД). Важность этих исследований трудно переоценить, поскольку о реальном состоянии электрической