АНАЛИЗ IOT, КАК ОБЪЕКТА ОБЕСПЕЧЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

Сохибжон Рустамович Ботиров *(ассистент ТУИТ)*

Зоирова Муниса *(студент бакалавра ТУИТ)*

Базовая идея IoT состоит в обеспечении взаимодействия различных вещей в окружающем нас пространстве, предоставлении бесперебойной связи и передачи контекстной информации, которую эти вещи генерируют. Взаимодействие вещей происходит на основе существующих и развивающихся информационно-коммуникационных технологий. В пространстве IoT наряду с уже существующими требованиями к информационно-коммуникационным технологиям, такими как обеспечение связи "в любое время" и "в любом месте", появляется новое – "связь с любой вещью". Это требование предполагает взаимодействие, т.е. обмен информацией как между самими вещами, так и между человеком и вещью [1].

Концепция IoT предполагает, что каждая физическая вещь имеет устройство – элемент оборудования, который предоставляет возможность коммуникации (обязательное требование), а также ряд дополнительных возможностей. К ним относятся возможности производить измерения, срабатывать, а также возможность ввода, хранения и обработки данных. Все устройства можно разделить на категории: устройства переноса и сбора данных, сенсорные и исполнительные устройства, широкого/общего назначения.

К первой категории относятся устройства, позволяющие подключить физическую вещь к сети связи. Вторая категория – это считывающие или записывающие устройства. В третьей категории находятся сенсорные устройства, позволяющие обнаруживать и измерять информацию, а затем преобразовывать ее в цифровые электрические сигналы. Исполнительные

устройства производят обратную операцию, преобразуя цифровые электрические сигналы в различные действия. Четвертая категория включает устройства, относящиеся к различным областям применения IoT и обладающие встроенными возможностями обработки информации и связи.

Разработанная четырехуровневая эталонная модель дает представление об архитектуре и позволяет произвести оценку возможностей IoT. Для этих целей, наиболее интересны четвертый (верхний) и первый (нижний) уровни. На верхнем уровне модели расположены приложения IoT, производящие интерпретацию поступающей от устройств информации. Приложения зависят от данных, которые они обрабатывают, и их потребителей. Некоторые приложения сосредоточены на мониторинге данных, другие на управлении ими. Задачи мониторинга и управления порождают различные модели приложений и шаблоны программирования, а также затрагивают вопросы операционных систем, мобильности, серверов приложений и много-поточности. В общем виде индивидуальные пользователи могут применять приложения для домашней автоматизации, обеспечения безопасности, автоматического мониторинга устройств и управления повседневными задачами.

Потенциальные угрозы сетевой безопасности, возникающие в среде IoT, также можно рассматривать с точки зрения эталонной модели. На каждом уровне модели присутствуют угрозы безопасности, как специфичные только для этого уровня, так и общие для всей модели. Так, на всех уровнях модели присутствует угроза несанкционированного доступа к приложению или устройству. В случае исполнительных устройств несанкционированный доступ может привести к несанкционированным действиям самой вещи. На уровне приложения – это угрозы утечки информации, нарушения целостности данных и неприкосновенности частной жизни. На уровне сети – угрозы утечки данных об использовании сигнализации и нарушения их целостности. На уровне устройства – угрозы несанкционированного

вскрытия, несанкционированного контроля/управления, утечки данных, хранящихся в устройстве, повреждения их целостности[2].

Для нейтрализации описанных угроз безопасности применяются алгоритмы авторизации и идентификации, производится шифрование передаваемых и хранимых данных, проводится аудит систем и применяется антивирусное программное обеспечение. Но не все устройства и приложения обладают высокой производительностью, поэтому применение криптостойких алгоритмов не всегда является возможным.

Рассмотрим, например, такой показатель, как надёжность. Большинство протоколов работает поверх TCP, что обеспечивает простой уровень надёжности. Каждый байт, попадающий в коммуникационный канал, должен быть доставлен получателю, даже если понадобится выполнить множество попыток. Это реализуется просто и чаще всего без проблем, но не позволяет управлять синхронизацией. В случае медленного абонента одноканальный TCP-трафик дублируется.

По контролю качества сервиса заметно отличается от других протоколов протокол DDS, поскольку ориентирован на коммуникации между устройствами. Кроме надёжности, DDS обеспечивает также контроль так называемой «жизнеспособности» (при исследовании проблем), обнаружения и использования ресурсов, а также синхронизации.

Обеспечение сетевой безопасности IoT, возможно только при глубоком анализе архитектуры и протоколов используемых на уровне передачи информации. Но не стоит забывать об оценке сетевой безопасности, прежде чем принимать меры по обеспечению безопасности для экономической эффективности принимаемых мер.

1. П. Зернов. Интернет вещей (IoT): возможности и потенциальные угрозы безопасности / Технологии и средства связи, 2018 г.

2. Ганшин Д.Г., Сальников В.С., Цопа А.И. Архитектура безопасности распределенной системы IoT / Харьковский национальный университет радиоэлектроники