**Исследование различных проблем сетевой безопасности в Интернете вещей (IoT)**

 **защита сети умного дома**

На рисунке 1 показан пример сети умного дома, которые были смоделированы с помощью инструмента пакета Cisco для трейсера. В этой сети Домашний шлюз подключен к нескольким интеллектуальным устройствам IoT, таким как интеллектуальная солнечная панель, интеллектуальная батарея, интеллектуальный вентилятор, планшетный ПК, измеритель температуры, детектор дыма, интеллектуальная дверь, интеллектуальная лампа, интеллектуальная кофеварка и умная гаражная дверь. Домашний шлюз подключен к модему, с помощью которого пользователи могут получить доступ в интернет. Пользователь может использовать планшетный компьютер для управления всеми интеллектуальными устройствами в сети. Интеллектуальные сети имеют неотъемлемые проблемы с точки зрения безопасности. Нарушитель может нарушить сеть двумя способами. Во-первых, путем компрометации безопасности сети путем вмешательства в узлы, а во-вторых, путем запуска атак на сеть удаленно через Интернет.

Чтобы преступникам было труднее получить доступ к сети, необходимо принять меры безопасности. Для защиты сети могут быть использованы физические и сетевые меры безопасности. Сеть может быть защищена физически путем развертывания систем безопасности, которые предупреждают жильцов дома и громко сигнализируют. Стандартизированные методы защиты сети могут быть использованы для предотвращения удаленных атак на сеть.

На рис.2 показана та же самая умная домашняя сеть, изображенная на Рис. 1, которая была защищена с помощью физической и сетевой безопасности. Сеть на Рис. 2 состоит из домашнего шлюза, подключенного к нескольким интеллектуальным устройствам IoT, таким как умная солнечная панель, умная батарея, умный вентилятор, планшетный ПК, измеритель температуры, детектор дыма, умная дверь, Умная лампа, умная кофеварка и умная гаражная дверь. Сеть была защищена с помощью физических и сетевых методов безопасности. Физическая защита сети включает в себя развертывание растяжек, сирен/сигнализаций и камер безопасности. Эти устройства управляются с помощью микроконтроллерного блока (MCU). Микроконтроллер подключен к ноутбуку, который используется для хранения данных с растяжек, сирен/сигнализаций и камер безопасности. Ноутбук подключен к сети, чтобы сделать данные, связанные с безопасностью, доступными по сети. Вся сеть разделилась на две части. Одна часть состоит из конечных устройств Интернета вещей, а другая-из компьютеров, устройств хранения данных и реализаций физической безопасности. Если бы все устройства находились на том же сетевом уровне, что и сеть, показанная на Рис.1, компрометация даже одного из конечных устройств разрушила бы безопасность всей сети. Таким образом, наличие многоуровневой сети гарантирует, что если одна часть сети была скомпрометирована, другая часть сети будет в безопасности, потому что злоумышленникам придется пройти через дополнительные уровни безопасности, чтобы получить доступ к устройствам в другой части сети. Кроме того, в Сети был использован физический брандмауэр для обеспечения дополнительной сетевой безопасности.

В сети, показанной на Рис.1, хакеры должны пройти только через один уровень безопасности, чтобы получить доступ к сети. С другой стороны, преступники должны были бы пройти через 2 уровня сетевой безопасности, чтобы получить доступ к сети, изображенной на Рис.2. Этот метод защиты сети не только затруднит злоумышленникам взлом









