ЗАЩИТА ИНФОРМАЦИИ В УСТРОЙСТВАХ ИНТЕРНЕТА ВЕЩЕЙ, МАТРИЦА РИСКОВ

Н.Ю. Дашко, С.П. Способ

Информационные технологии являются неотъемлемой частью жизни человека на сегодняшний день. Данные технологии работают на базе использования множества средств и методов сбора, обработки, а также передачи данных с целью получения информации необходимого качества и состоянии какого-либо объекта, процесса или явления. С стремлением за улучшением качества жизни человека, повышением ее безопасности и автоматизации бытовых и иных задач сформировался «Интернет вещей». Это сеть, состоящая из взаимосвязанных физических объектов (вещей) или устройств, которые имеют встроенные датчики, а также программного обеспечения, позволяющего осуществлять передачу и обмен данными между физическим миром и компьютерными системами, с помощью использования стандартных протоколов связи. Основная проблема использования сетей IoT заключается в том, что они не имеют защиты от воздействий со стороны злоумышленника. Это может привести, в лучшем случае, к причинению вреда имуществу пользователя, а в худшем – его здоровью и жизни. Например, устройства контроля и управления электрической сетью могут быть захвачены злоумышленником с помощью любого устройства, имеющего доступ к сети Интернет, и соответствующего программного обеспечения. Получив полный или частичный контроль над устройством, злоумышленник может осуществить отключение или порчу электрических приборов, в том числе критически необходимых приборов (систем жизнеобеспечения в больницах, систем мониторинга на производстве, охранных систем и т.д.), создать короткие замыкания в сети и даже вызвать пожар или аварию, если речь идет о производстве.

Универсальным и удобным способ выявления наиболее уязвимых и рискованных мест в сети, например, умного дома является матрица рисков. Матрица представляет из себя таблицу столбцы которой называются «Активы» и строки «Уязвимости». Под активами понимается ресурсы, допустим. Для умного дома – личная жизнь, финансы, личные данные. Оценивая уязвимости можно выявить риск, в том случае, если злоумышленник воспользуется ей и какие это принесет потери активов. Наиболее важные и слабые места выделяются красным, менее желтым или зеленым.

В объемах современного мира трудно на глаз определить риски от взлома того, или иного сетевого узла Вашего дома. Требуется метод, позволяющий комплексно анализировать сеть умного дома и эффективно выявлять наиболее рискованные объекты сети, которые нуждаются в проработки вопросов безопасности

Литература

1. Попов В.Г., Галиаскаров Д.Ф, Гвоздев Л.Б. Актуальность обеспечения информационной безопасности в сетях IoT // StudNet. 2021. № 4.

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб: Питер, 2012. 960 с.