УДК 004.056

Исследование устройств умного дома на предмет угроз информационной безопасности

К. Ю. Борисов, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург
Руководитель А. Н. Югансон, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург

В условиях масштабной и быстрой цифровизации всех сфер жизнедеятельности и бизнеса неизбежно появляются тенденции к использованию автоматизированных систем, управляющих определёнными процессами без участия человека. Такие системы составляются из устройств Интернета вещей, которые объединяются в сети и взаимодействуют друг с другом.

Целью работы является обеспечение безопасности использования устройств умного дома как одного из проявлений Интернета вещей.

Для достижения данной цели необходимо изучить основную концепцию построения умного дома, провести базовый анализ возможных угроз безопасности и построить модель злоумышленника для данной работы. Затем необходимо провести анализ отдельных устройств умного дома на предмет возможных уязвимостей, эксплуатация которых злоумышленником может представлять угрозу для устройств, находящихся в зоне, в которой работает система умного дома. В результате работы необходимо составить рекомендации по обеспечению информационной безопасности при использовании устройств умного дома.

В ходе исследования была изучена современная концепция построения системы умного дома, основанная на центральном узле, контролирующем работу подключаемых к нему устройств. Также возможно использование отдельных устройств без подключения их к центральному узлу. Уязвимости могут содержать как центральный узел, так и подключаемые устройства. Подключаемые устройства могут быть уязвимы независимо от того, подключены они к центральному узлу или нет. Дополнительным источником уязвимостей могут выступать мобильные приложения, созданные для управления устройствами умного дома. Поддержка устройством умного дома функционала удалённого управления через сеть Интернет, как правило, значительно увеличивает количество угроз безопасности.

В качестве исследуемых устройств были взяты как центральный узел, так и подключаемые устройства различных категорий: умная розетка (TP-Link HS110), умная лампа (TP-Link LB110), датчик открывания двери. Для каждого из устройств проведено исследование функционала и механизма работы протоколов взаимодействия устройств с сетью, друг с другом и с управляющими приложениями. На основе этих данных был составлен список потенциальных угроз безопасности.

Устройства умного дома подвержены атакам различного вида, в зависимости от атакуемого устройства: центральный узел, периферийное устройство, мобильное приложение для управления. Успешная атака злоумышленника на устройства умного дома может привести к нарушению различных аспектов безопасности. При атаке на любое устройство может быть нарушена конфиденциальность системы путём получения злоумышленником данных о сетевых устройствах или ключей аутентификации беспроводной сети. Может быть нарушена целостность системы при атаке на центральный узел путём нарушения функционирования системы умного дома как единого целого. Атака на устройства умного дома, обеспечивающие физическую безопасность, такие как датчики открывания дверей, может привести к нарушению доступности вследствие нарушения функционирования извещений о несанкционированном доступе на объект.

В ходе поиска уязвимостей были проанализированы угрозы безопасности системам умного дома. Был составлен список рекомендаций по обеспечению информационной безопасности при использовании устройств умного дома: установка сложных паролей, отключение дистанционного управления, отключение небезопасного функционала, перенос устройств умного дома в отдельную подсеть. Впоследствии планируется разрабатывать

методику обеспечения информационной безопасности для повышения защищённости объекта с системой умного дома.

Автор	«__» _____ 2019	_____	К. Ю. Борисов
Научный руководитель	«__» _____ 2019	_____	А. Н. Юганссон