БЕЗОПАСНОСТЬ ЭКОСИСТЕМЫ УМНОГО ДОМА

Е.А. Шитик, П.И. Цыркунович

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

С развитием технологий Интернета вещей (IoT, Internet of Things) интеллектуальные устройства умного дома стали все более распространенными и доступными для использования. В свою очередь, это приводит к возрастанию интереса со стороны киберпреступников, которые ищут способы атаковать такие устройства. В результате этого, защита устройств умного дома стала важной задачей для разработчиков и производителей. Кроме этого, во всем мире растерт обеспокоенность безопасностью личных данных пользователей и обеспечением их защиты. В этом плане экосистема умного дома, которая зачастую строится на основе интеграции смарт-устройств различных производителей, конфигурируется и эксплуатируется пользователями без достаточной квалификации в области безопасности, является весьма уязвимой.

Для того, чтобы обеспечить должный уровень защиты, надо знать потенциальные слабые места и уязвимости проекта. Мы рассматриваем слабые звенья экосистемы умного дома в реализации информационных потоков проекта. Пусть общая схема системы умного дома такова: (Пользователь) – (Управляющая система) –

(Устройство автоматизации). Первый поток находится между пользователем и управляющей системой – в нем передаются команды пользователя программной платформе, на которой реализован умный дом. Второй - между управляющей системой и конечными устройствами автоматизации. К слабому звену можно так же отнести: открытость для внешнего доступа («торчание в интернет», передачу данных во внешние облачные хранилища), беспроводное общение между устройствами.

Чтобы обезопасить экосистему умного дома, необходимо в первую очередь повысить защищенность всех описанных выше слабых звеньев. К числу таких методов можно отнести: выбор безопасного протокола передачи данных – Zig-Bee, Z-Wave; реагирование на физическое вмешательство, которое может создать аномальное состояние; аутентификацию на стороне конечного устройства.

К особенностям нашего подхода к защите умного дома нужно отнести и использование специализированных устройств, называемых «защищенные шлюзы». Они обеспечивают контроль доступа, маршрутизацию трафика, аутентификацию пользователей, мониторинг и обнаружение взломов. Также защищенные шлюзы могут иметь функцию бэкапа и восстановления системы.

В заключение можно сказать, что защита устройств умного дома от киберугроз является важной задачей, которой необходимо уделить должное внимание. Пользователи должны соблюдать базовые меры по обеспечению безопасности, а производители должны уделять внимание безопасности на всех этапах разработки и выпуска смарт-устройств. По-нашему мнению, в сфере IoT, безопасность – основной сдерживающий фактор [1].

Список литературы

1. Kanev A.N., Nasteka A.V., Bessonova C.E. Automation Device Authentication at «Smart Home» // Vestnik policii. 2016. Vol. 7, iss. 1.