РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСТРОЙСТВ «УМНОГО» ДОМА

В.Ф. Кулиш

Системы «умного» дома устанавливаются во все большем количестве квартир и домов. Это создает более комфортные условия для жизни и позволяет накапливать информацию о пользовательских привычках. Пользователи могут создавать и изменять сценарии управления домом использую накопленные данные, что ведет к экономии потребляемых ресурсов. Системы такого вида, как правило, включают в себя большое количество датчиков, а также контролирующие устройства для включения или выключения приборов в доме на основании данных, поступающих от датчиков. Данные о работе приборов в доме накапливаются концентратором, который управляет всеми устройствами, а затем отправляет накопленную информацию на сервер. Сервер, помимо хранения накопленной информации, позволяет удаленно управлять устройствами в квартире или доме. Таким образом архитектура системы «умного» дома состоит из трех слоев: сенсорный слой (собирает информацию о состоянии жилого помещения), слой контроля (управляет устройствами на основе данных от сенсорного слоя), слой хранения (хранит исторические данные о работе приборов). Основными рисками информационной безопасности таких систем являются утечка информации о текущих и о предыдущих состояниях устройств в доме, удаленный контроль над приборами в доме, а также заражение устройств вредоносным программным обеспечением. Данные риски могут быть реализованы с помощью следующих атак.

1. Сбор и анализ метаданных сетевого трафика устройств.
2. Получение доступа к серверу сбора данных.
3. Получение удаленного доступа к одному из устройств системы или всей системе «умного» дома.
4. Создание виртуальной копии устройства для получения статистики работы реального устройства в системе.