ИНФОРМАЦИОННАЯ СИСТЕМА ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «УМНОГО ДОМА»

Степурко М.Н.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Дуйнова Ю.А. – старший преподаватель БГАС

Информационная система оценки угроз информационной безопасности «умного дома» позволяет на основе показаний датчиков и исполнительных механизмов оценить возможные угрозы информационной безопасности системы «умный дом».

Проектируемая информационная системы оценки угроз информационной безопасности основана на модели средства информационной безопасности, выделенной в процессе анализа литературных источников. Модель проектируемой системы:

– описание модели системы «умный дом»;
– описание модели угроз информационной безопасности;
– разработка методов оценки угроз;

Описание «умного дома» осуществляется путем разделения системы на подсистемы. Выделены следующие подсистемы [1]: управления и связи, безопасности и мониторинга, освещения, климат-контроля, кухонного оборудования, мультимедиа.

Далее подсистема разбивается на компоненты, объекты управления и элементы: датчик и исполнительный механизм. Все объекты управления в «умном доме» имеют датчик для считывания необходимых данных и исполнительный механизм, выполняющий какое-либо действие. Показания датчика и действие исполнительного механизма непосредственно оказывают влияние на состояние

объекта и состояние информационной безопасности всей системы, поэтому для них определяются ограничения.

Метод оценки состояния «умного дома» основывается на следующих этапах:

– описание системы «умный дом» пользователя;

– сбор данных с системы, определение ограничений;

– анализ данных, сравнение с установленными ограничениями;

– определение подсистемы и объекта, в котором возникла угроза;

– оценка угрозы по определенному экспертами списку угроз и информационных активов;

Список угроз [2] представлен в таблице 1.

Таблица 1 – Угрозы информационной безопасности «умного дома»

Тип атаки	Уязвимость	Возможные последствия
Хакерские атаки на центральный сервер	Подключение сети «умного дома» к Интернет. Отсутствие (неэффективность) механизмов защиты периметра сети	Нарушение работы, либо выход из строя центрального сервера, а следовательно и всей системы. Нарушение конфиденциальности, целостности и доступности информации (КЦД)
Влияние вирусных и троянских программ на работу системы	Подключение сети «умного дома» к Интернет. Отсутствие (неэффективность) механизмов защиты периметра сети	Сбои в ПО системы, а следовательно нарушение работы либо вывод из строя аппаратуры системы. Нарушение КЦД информации, находящейся внутри сети
Перехват информации, передаваемой по проводным и беспроводным каналам связи	Возможность доступа злоумышленника к проводным каналам или к зоне устойчивого перехвата радиосигналов сети. Отсутствие (неэффективность) механизмов защиты трафика	Нарушение конфиденциальности информации передаваемой по каналу. Возможен захват управления системой
Ошибки пользователя.	Отсутствие (неэффективность) механизмов защиты системы от неправильных действий пользователей	Нарушение КЦД информации. Возможны сбои в системе из-за неправильного использования оборудования
Утечка информации по акустоэлектрическому каналу	Наличие акустоэлектрических преобразователей (датчики охранной, пожарной сигнализации и т.д.), подключенных к проводным линиям	Нарушение конфиденциальности информации

Информационная система также способна проводить анализ угроз перехвата данных, собранных с датчиков IoT-устройств с использованием вредоносного ПО [3], таких как: перехват нажатий клавиш на клавиатуре (Keystroke Inference Attack), перехват данных о текущем состоянии IoT-устройств (Task Inference Attack), определение местоположения (Location Inference Attack), прослушивание (Eavesdropping). Возможные последствия реализации угроз: кража ID и пароля через датчик движения, утечка данных о местоположении пользователя и внутренней структуре дома, утечка конфиденциальной информации через IP-камеру, утечка информации о местоположении пользователя внутри дома через магнитный датчик.

Информационная система на основе выявленных угроз даёт следующие рекомендации [4] пользователю: отслеживание поведения системы с целью выявления любой подозрительной активности, частое резервное копирование данных, внедрение многофакторной аутентификации, использование оборудования и программного обеспечения для сбора и анализа сетевого трафика.

Список использованных источников:

1. Малыш, В.Н. Анализ угроз информационной безопасности системы «Умный дом» / В.Н. Малыш, Д.С. Букреев // Труды международного симпозиума «Надежность и качество». – 2012. – Т.1.

2. Снегуров, А.В. Риски информационной безопасности систем, построенных по технологии «Умный дом» / А.В. Снегуров, Е.А. Ткаченко, А.Д. Кравченко // Восточно-Европейский журнал передовых технологий. – 2011. – Т.4, №3(52). – С.30-34.

3. Park, M. Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective / M. Park, H. Oh, K. Lee // Sensors. – 2019. – Vol.19, iss.9. – DOI: 10.3390/s19092148.

4. Ali, B. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes / B. Ali, A. I. Awad // Sensors. – 2018. – Vol.18, iss.3. – DOI: 10.3390/s18030817.