НАЦІОНАЛЬНА БЕЗПЕКА

Кильдишев В.Й.
кандидат технических наук, доцент;
Стайкуца С.В.
кандидат философских наук, доцент;
Новицкий М.С., Леонтьев Е.А.
студенты,
Одесская национальная Академия связи имени А.С. Попова

АНАЛИЗ УГРОЗ И РИСКОВ ТЕХНОЛОГИИ SMART HOUSE

Процессы информатизации общества, экспоненциальный рост количества информации, развитие IT не может не сказываться на обустройстве и цифровизации локаций, в которых чаще всего находится человек – его дома. Объединение подсистем, которые обеспечивают безопасность и комфорт пользователей, позволяют эффективно использовать ресурсы и оптимизировать их потребление, настраивать алгоритмы и скрипты работы с получением синергетического эффекта – это возможно в интегрированных системах типа «Smart House» или «умный дом».

Как представлено в расчетах DISCOVERY Research Group [1] и YORK International [2], ежегодно увеличивается объем средств, которые затрачиваются на направление «умный дом» – построение, улучшение и оптимизацию параметров и характеристик. Так, только за последние 5 лет объем мирового рынка Smart House вырос более, чем в 3,5 раза с 7,2 до 26,2 млрд. долларов США. Налицо переход пользователей к «всеохватывающей» автоматизации. При этом вопросы безопасности и защиты от несанкционированного доступа и иных злоумышленных действий рассматриваются поверхностно

Как отмечается в [3], классификация выделяет три варианта построения системы «умный дом»:

– системы централизованного управления системы «умный дом»;

– системы децентрализованного управления системы «умный дом»;

– системы, принцип которых основан на использовании радиоканала в силовой проводке (X-10).

Каждый из вариантов имеет преимущества, но, в то же время, и недостатки, которые трансформируются в угрозы и риски.

Как отмечается в [3], важным моментом при создании СЗИ системы «умный дом» является формирование модели угроз. При этом возможен вариант составления угроз разными схемами, основываясь на нормативной базе – ГОСТ Р 51275, BS 7799, ISO 17799 и других.

Модель угроз – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [4]. Формой представления модели угроз является дерево угроз. Дерево угроз – это модель угроз, представленная в виде дерева. Для определения структуры дерева и возможных угроз в [3] предлагается выделять ключевые модули Smart House, к которым относятся:

- облачное управление системой «умный дом»;
- пульт дистанционного управления;
- сеть Wi-Fi;
- сеть электропитания;
- оптоволоконные и коаксиальные кабели;
- оборудование (датчики движения, видеокамеры и т.д.);
- программное обеспечение.

В данном случае для каждого модуля определяется набор угроз для того варианта, который использовался при построении системы. На рис. 1 представлено дерево угроз системы Smart House.

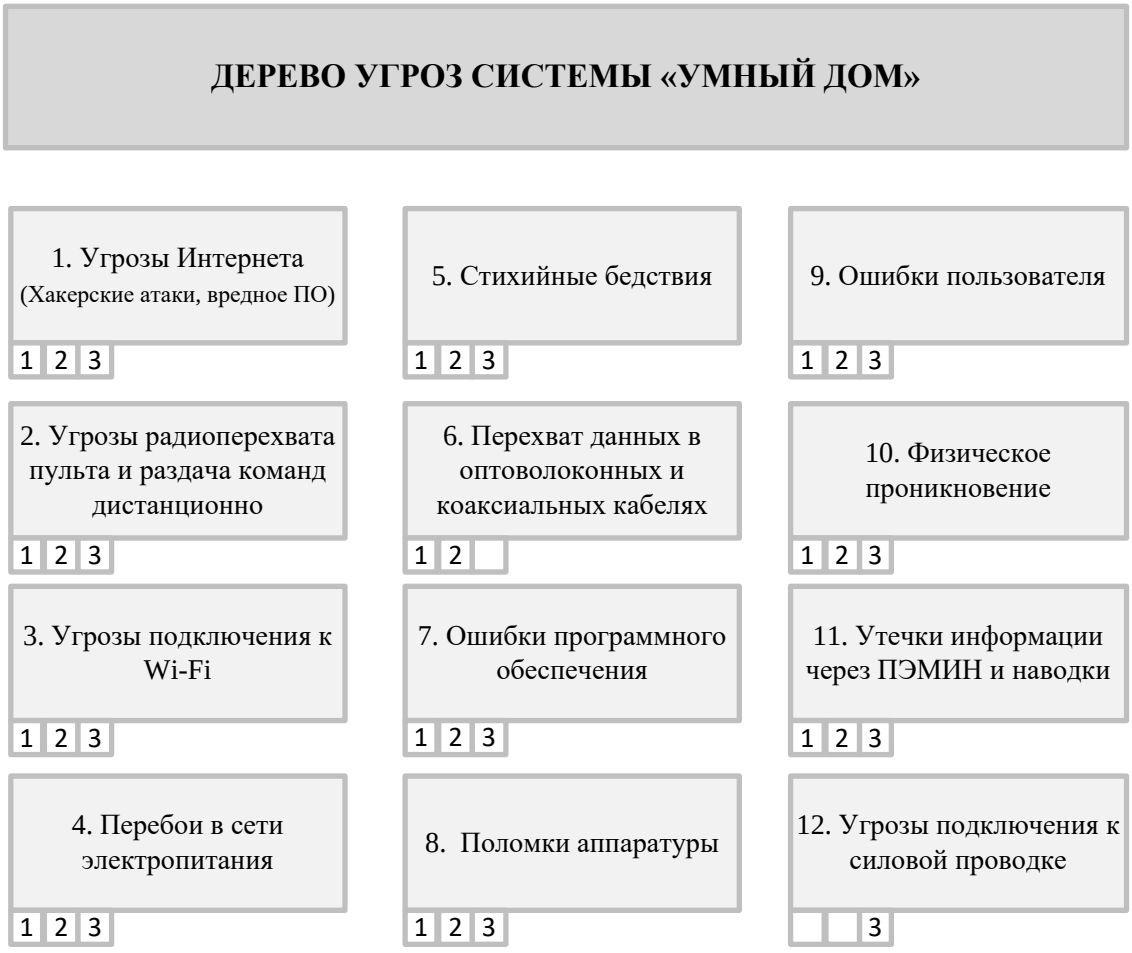

Рис. 1. Дерево угроз системы «Умный дом»,

где 1 – схема централизованной системы,
2 – схема децентрализованной системы, 3 – схема X-10

Угроза каждого типа приводит к появлению ряда уязвимостей. Например, при распространении вредоносного программного обеспечения основными каналами являются Bluetooth, HTTP-канал, GSM-канал, локальная сеть и «логические» бомбы. Существует несколько вирусных программ, которые классифицируются исходя из их целей – осуществления управления системой и осуществления перехвата информации. При возникновении такого типа угрозы к уязвимостям програмного обеспечения систем умного дома относятся:

– отсутствие контроля над широковещательной рассылкой датаграмм в сети Smart House;

– отсутствие возможности блокирования подключений неавторизированных пользователей;

– отсутствие проверки аутентичности управляющей программы.

Оценку вероятности реализации угрозы на уязвимые элементы Smart House проводят через частоту реализации угрозы за период, как показано в [5]. Предлагается рассматривать 3 уровня угрозы (высокая, средняя и низкая). При оценке эффективности реализации угрозы также используется 3 градации. Для вычисления уровня риска используется подход, предложенный компанией Microsoft. Как итог – выделение вероятных угроз, через которые может произойти нарушение ИБ Smart House в формате тип атаки – уязвимость – возможные последствия. В дополнение к угрозам, представленным на рис. 1, добавлены такие типы атак, как утечки информации через электроакустический канал и ПЭМИН.

Технология Smart House развивается и становится доступнее для пользователей на фоне удобства и снижения стоимости программно-аппаратных решений. Новые тренды информационной цивилизации, такие как IoT и Smart City, только подчеркивают актуальность технологии. Дальнейшая интеграция и полнота взаимодействия системы «Умный дом» с киберпространством подчеркивает важность понимания угроз, составления модели (дерева) рисков и выбора действенных контрмер.

Список использованных источников:

1. Темпы роста мирового рынка систем «умный дом» (млрд евро) [Электронный ресурс]. – Режим доступу: www.drgroup.ru.

2. Перспективы рынка систем «Умный дом» [Электронный ресурс] / Центр инженерных технологий CENTEC. – Режим доступа: www.centecgroup.ru

3. Овчинников Н. А. Разработка модели угроз системы защиты информации «Умный дом» / Н. А. Овчинников, Е. А. Максимова // Информационные системы и технологии. – 2015. – С. 141-146.

4. Модели угроз. Практическая защита персональных данных [Електронний ресурс]. – Режим доступу: URL:pdsec.ru/model_ugroz

5. Снегуров А. В. Риски информационной безопасности, построенной по технологии «Умный дом» / А. В. Снегуров, Е. А. Ткаченко, А. Д. Кравченко. // Восточно-Европейский журнал передовых технологий. – 2001. – С. 30-34.