ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД К МОДЕЛИРОВАНИЮ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕХНОЛОГИИ «УМНЫЙ ДОМ»

Абдрашитова В.И.
Хабибулина Н.Ю.
Томский политехнический университет
venera401@gmail.com

Введение

Годом рождения “умного дома” в том виде, каким мы его знаем сегодня, можно считать 1978 год[1]. В настоящее время существует большое количество различных систем “умный дом”, отличающихся по своему назначению, а значит и по сложности и составу системы. Целью внедрения подобных систем является тепло- и энергосбережение, повышение комфорта жизни и обеспечение безопасности жилища[2]. Система “умный дом” является совокупностью подсистем, которые в свою очередь могут состоять из своих подсистем. Рассматриваемый состав системы “умный дом” представлен на рисунке 1.

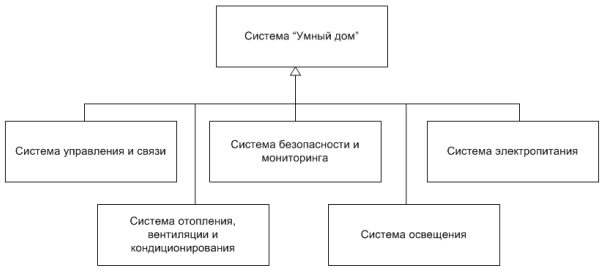

Рис. 1. Состав системы “умный дом”

Система “умный дом” представляет собой объект информатизации подверженный угрозам информационной безопасности[3]. Угрозы информационной безопасности системы зависят от методов построения системы, используемых технологий и обрабатываемых информационных потоков[4]. В силу того, что технология “умный дом” не имеет единой методологии для построения системы, оценка и обеспечение информационной безопасности являются сложно выполняемыми, так как требуется индивидуальный подход к каждой системе.

Объектно-ориентированный подход

Для осуществления единого метода оценки и обеспечения информационной безопасности предложено использовать объектно-ориентированный подход для описания системы “умный дом”. Полученная диаграмма классов представлена на рисунке 2.

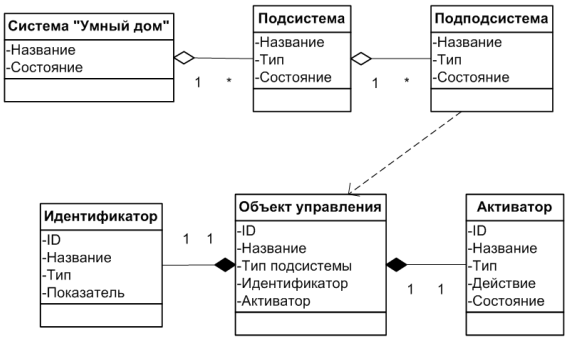

Рис. 2. Диаграмма классов

Предложенное решение позволяет описать систему “умный дом” любой сложности и состава функций. Предполагается, что всего в системе пять видов подсистем, которые были обозначены на рисунке 1. Каждая подсистема имеет свои подподсистемы, которые зависят от типа применяемой системы “умный дом”. Подподсистемы отвечают за работу с объектами управления, а у объекта обязательно указан тип подсистемы. Все объекты управления в “умном доме” имеют датчик для считывания необходимых данных (здесь он назван идентификатором) и исполнительный механизм (здесь он назван активатором), выполняющий какое-либо действие. Показатель идентификатора и действие активатора непосредственно влияют на состояние объекта и соответственно подсистем, а значит и на состояние информационной безопасности всей системы “умный дом”. Для определения угрозы безопасности и оценке уровня угрозы важно знать к какому типу подсистемы относится объект и не нужно знать тип подподсистемы. Это позволяет обойти проблему с различием состава и функций “умных домов”.

Угрозы информационной безопасности технологии “умный дом”

Виды угроз информационной безопасности технологии “умный дом”:

1) нарушение конфиденциальности информации;

Защищаемая информация становится известной лицам, не имеющим санкционированного доступа к этой информации.

2) нарушение целостности информации;

Защищаемая информация подверглась изменениям, потеряла достоверность и отличается от информации, которая была получена первоначально.

3) нарушение доступности информации;

Защищаемая информация становится недоступной для пользователей, которым она предназначена.

Наиболее вероятные угрозы информационной безопасности системы “умный дом”[5]:

1) Хакерские атаки на центральный сервер.
2) Влияние вирусных и троянских программ на работу системы.
3) Перехват информации, передаваемой по проводным и беспроводным каналам связи.
4) Доступ злоумышленника с правами администратора на центральный сервер с помощью хищения паролей и других реквизитов разграничения доступа.
5) Доступ к сети неавторизованных пользователей.
6) Наличие нарушителей в числе обслуживающего персонала.
7) Ошибки пользователя.
8) Кража (злоумышленный вывод из строя аппаратуры) системы «Умного дома».
9) Перебои в сети электропитания.
10) Стихийные бедствия.
11) Поломка аппаратуры системы.
12) Ошибки программного обеспечения.
13) Утечка информации через побочные электромагнитные излучения и наводки (ПЭМИН).
14) Утечка информации по акустоэлектрическому каналу.

Заключение

В результате проделанной работы была предложена методология представления системы “умный дом” на базе объектно-ориентированного подхода, которая позволяет описывать любые “умные дома” в независимости от их сложности и вида.

Наличие единого подхода к описанию системы “умный дом”, выявленные слабые места любого “умного дома” и список наиболее вероятных угроз информационной безопасности, которые могут в ней возникнуть, представляют возможным унифицированный подход для нахождения угроз информационной безопасности и оценки уровня данных угроз в зависимости от типа подсистем, к которым относятся управляемые объекты, подверженные угрозам.

Список использованных источников

1. История “умного дома”. [Электронный ресурс] / Портал автоматизации зданий.– URL: http://hosm.ru/info/history.html (Дата обращения 02.10.2015)
2. Гаврилов А.В. Искусственный домовой //Искусственный интеллект и принятие решений. 2012. – 02/2012. – С.77-89.
3. Защита информации. Объект информатизации. Факторы, воздействующие на информацию: ГОСТ Р 51275-2006. – Введ. 2008.02.01.– М.: Стандартинформ, 2007. – 8с.
4. Малыш В.Н., Букреев Д.С. Анализ угроз информационной безопасности системы «умный дом» //Труды международного симпозиума «Надежность и качество». 2012. – Т.1.
5. Снегуров А.В., Ткаченко Е.А., Кравченко А.Д. Риски информационной безопасности систем, построенных по технологии «умный дом» //Восточно-Европейский журнал передовых технологий. 2011. – №3(52) Т.4 2011 – С.30-34.