УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ, ПОСТРОЕННЫХ ПО ТЕХНОЛОГИИ «УМНЫЙ ДОМ»

Снегуров А.В., Ткаченко Е.А., Кравченко А.Д.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-13-06,
E-mail: arksn@rambler.ru ; факс (057) 702-11-13

The report considered the problem of information security systems based on technology of "smart house", discussed the threats of information security for such systems.

Постановка проблемы. Технология «Умный дом» является одной из наиболее перспективных для управления сервисом офисных и производственных помещений, жилых зданий. Автоматизация управления всеми процессами жизнеобеспечения является настолько привлекательной, что приводит к огромному предложению на рынке данных услуг различными компаниями. По данным экспертов компании YORK International [1], прогнозируется ежегодный рост рынка систем, использующих данную технологию, на 20-25% в год. Автоматизированное управление электро-, водо-, газо-, теплоснабжением, кондиционированием, мониторинг различных процессов позволяют не только уменьшить эксплуатационные затраты, но и повысить безопасность персонала (жильцов).

Однако внедрение данной технологии влечет за собой появление новых проблем, связанных информационной безопасностью. Так уже в мире произошло ряд атак на информационные системы энергогенерирующих, промышленных компаний, управления транспортом, системы управления водоснабжением [2-4]. Следует ожидать увеличение подобных атак в будущем.

Учитывая экономическую подоплеку большинства атак на информационные ресурсы организаций можно отменить, что подобные атаки на систему «Умный дом» могут иметь целью шантаж с дальнейшим вымоганием денег, дезорганизация работы конкурирующей организации, получение конфиденциальной информации о деятельности конкурирующей организации (VIP-жильцов) и т.д.

Целью доклада является рассмотрение проблемы обеспечения информационной безопасности интеллектуальных систем, построенных по технологии «Умный дом», выделение основных угроз информационной безопасности, возникающих при эксплуатации систем, построенных с использованием данной технологии.

Рассмотрим угрозы информационной безопасности систем, построенных по технологии «Умный дом». Считаем, что базовыми классическими угрозами информационной безопасности являются нарушение конфиденциальности, целостности и доступности (КЦД) информации.

Под конфиденциальностью информации в данном исследовании мы понимаем невозможность утечки конфиденциальной информации организаций (лиц), эксплуатирующих «Умный дом», через его подсистемы (например, через телекоммуникационную сеть).

Под доступностью информации мы понимаем такое состояние системы, при котором легальные пользователи (и сама система), используя элементы «Умного дома», имеют доступ к информации о состоянии системы и могут реализовывать разрешенные в системе действия (открывать двери, включать кондиционирование или систему пожаротушения, отключать газ или воду в случае утечки, мониторить ситуацию и т.д.). Нарушение доступности информации может привести к невозможности системы реагировать на различные ситуации, в том числе и аварийные. Примером может быть ситуация утечки газа при которой система не может провести необходимые отключения, запустить вентиляцию вследствие нарушения доступности информации.

Под целостностью информации мы понимаем такое состояние системы, при котором легальные пользователи (и сама система) получают достоверную информацию о состоянии подсистем «Умного дома». Получение системой недостоверной информации о температуре в помещениях, наличии пожара, утечки газа и воды, физическом проникно-

вении нарушителя в здание и т.п. приведет к неадекватным ее действиям (например, к включению системы пожаротушения, перекрытию воды и т.д.).

Из примеров видно, что нарушение конфиденциальности, целостности и доступности информации в системе, построенной по технологии «Умный дом», может привести как к дезорганизации работы организаций (лиц), ее эксплуатирующих, так и к катастрофическим последствиям.

Выделим наиболее вероятные угрозы, через которые может произойти нарушение информационной безопасности анализируемой системы. При этом будем учитывать, что данная система построена по централизованной схеме, где управление осуществляется через центральный сервер.

Таблица1 – Вероятные угрозы информационной безопасности систем, построенных по технологии «Умный дом»

№ п/п	Тип атаки	Уязвимость	Возможные последствия
1	Хакерские атаки на центральный сервер, влияние вредоносного программного обеспечения (ПО) на функционирование системы	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 КЦД информации
2	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
3.	Радиоэлектронное подавление беспроводных каналов передачи информации	Возможность доступа злоумышленника к зоне, где возможно радиоэлектронное подавление беспроводных каналов передачи информации	Нарушение доступности и целостности информации
4	Доступ злоумышленника с правами администратора на центральный сервер с помощью хищения паролей и других реквизитов разграничения доступа	Отсутствие (неэффективность) механизмов аутентификации и идентификации	Нарушение КЦД информации, находящейся внутри сети
5	Доступ к сети неавторизованных пользователей.	Отсутствие (неэффективность) механизмов аутентификации и идентификации	Нарушение КЦД информации, находящейся внутри сети
6	Наличие нарушителей в числе обслуживающего персонала (охранники, наладчики, уборщики и др.)	Отсутствие (неэффективность) организационных мероприятий по отбору и контролю за персоналом	Нарушение КЦД информации. Возможны сбои в системе из-за неправильного обслуживания оборудования. Уровень опасности зависит от степени доступа инсайдера к системе

7	Кража (злоумышленный вывод из строя аппаратуры) системы «Умного дома»	Отсутствие (неэффективность) – физической охраны объекта	Нарушение КЦД информации
8	Перебои в сети электропитания	Отсутствие системы автономного электропитания	Дезорганизация работы системы
9	Стихийные бедствия (пожар и др.)	Отсутствие (неэффективность) механизмов защиты	Дезорганизация работы системы
10	Поломка аппаратуры системы	Низкая надежность оборудования, низкая квалификация персонала	Нарушение КЦД информации
11	Ошибки программного обеспечения	Использование нелицензионного ПО, низкая квалификация персонала, отсутствие (неэффективность) тестирования закупаемого ПО	Нарушение КЦД информации
12	Утечка информации через побочные электромагнитные излучения и наводки (ПЭМИН)	Наличие ПЭМИ компьютерной техники. Выход проводников, в которых могут быть наводки излучений, за пределы контролируемой зоны	Нарушение конфиденциальности информации, обрабатываемой на ЭВМ
13	Утечка информации по акусто-электрическому каналу	Наличие акустоэлектрических преобразователей (датчики охранной, пожарной сигнализации и т.д.), подключенных к проводным линиям	Нарушение конфиденциальности информации

Исходя из результатов оценки самыми опасными являются те угрозы, при которых злоумышленник может брать под контроль всю систему. Поэтому крайне необходимым является проведение мероприятий по защите телекоммуникационной сети, разграничение прав доступа пользователей, защита от инсайдеров. Опасными являются угрозы потери электропитания, пожар в серверной, поломки оборудования и отказ программного обеспечения, отвечающего за централизованное управление системой. Реализация данных угроз может привести к катастрофическим последствиям для всей системы.

В настоящее время на кафедре телекоммуникационных систем ХНУРЭ проводятся исследования, посвященные анализу всех потенциальных угроз и уязвимостей систем, построенных по технологии «Умный дом», разрабатываются методики оценки результатов воздействия различных угроз на уязвимые элементы данных систем, разрабатываются предложения по повышению их информационной безопасности.

Литература:

6.Перспективы рынка систем "Умный дом" [Электронный ресурс] / Центр инженерных технологий CENTEC. — Режим доступа: \www/ URL: http://www.centecgroup.ru/press/articles/18/ — 02.03.2011 г. — Загл. с экрана.

2. Хакеры оставили без электричества 3 млн бразильцев [Электронный ресурс] / Securitylab. - Режим доступа: \www/ URL: http://www.securitylab.ru/news/387521.php: - 10.11.2009 г. — Загл. с экрана.

3. Энергосистема Австралии спасена благодаря Linux [Электронный ресурс] / Securitylab. - Режим доступа: \www/ URL: http://www.securitylab.ru/news/386273.php: 06.11. 2009 г. — Загл. с экрана.

4. McAfee сообщила о росте числа ИТ-атак на промышленные объекты [Электронный ресурс] / Securitylab. - Режим доступа: \www/ URL: http://www.securitylab.ru/news/405455.php: 10.11.2009г. — Загл. с экрана.