ного механообрабатывающего производства на этапах подготовки производства и оперативной коррекции и его практическая реализация [6] позволяет снизить временные затраты на выпуск единицы продукции и увеличить ритмичность производства.

Литература

1. Соловьев В.К. Методология автоматизированного проектирования операционных технологических процессов изготовления объектов точного машиностроения [Текст] / В.К. Соловьев. // Технология машиностроения. – 2004. – № 4. – С.60 – 62.
2. Султан–Заде Н.М. Метод оптимизации структурной компоновки автоматических линий [Текст] / Н.М. Султан–Заде // Системы управления станками и автоматическими линиями: сб.науч.тр. – М.: ВЗМИ, 1982. – С. 9 – 13.
3. Белоусов А.П. Проектирование автоматических линий: Учебное пособие для маш.-строит. спец. вузов. [Текст] / А.П. Белоусов, А.И. Дащенко – М.: В. шк., 1983.– 328с.
4. Козлова Е.В. Модифицированный метод структурного распараллеливания В.А. Костенко для линейных и разветвляющихся участков схемы технологического процесса сборочного производства. [Текст] / Е.В. Козлова, В.А.Когутенко // Вестник СевГТУ: Автоматизация процессов и управление, Севастополь: Издательство СевНТУ, 2003, – С.107 – 112.
5. Скатков А.В. Информационная модель производственного процесса с элементами принятия об управлении технологическими маршрутами в механообработке [Текст] / А.В.Скатков, Е.В.Козлова //«Восточно-Европейский журнал передовых технологий» – Харьков: Изд. НПП «Тех. Ц.», 2005. – № 4, С.81–91.
6. Козлова Е.В. Интегрированная система поддержки принятия решений по управлению структурами производственных процессов [Текст] / Е.В.Козлова //«Восточно-Европейский журнал передовых технологий» – Харьков: Изд. НПП «Тех. Ц.», 2011. – № 3, С.45–50.

В статті розглядаються методи побудови і основні функції технології «Розумний будинок». Проаналізовані основні інформаційні загрози і проведена оцінка ризиків інформаційної безпеки "Розумного будинку"

Ключові слова: «Розумний дім», ризик інформаційної безпеки

В статье рассматриваются методы построения и основные функции технологии «Умный дом». Проанализированы основные информационные угрозы и проведена оценка рисков информационной безопасности «Умного дома»

Ключевые слова: «Умный дом», риск информационной безопасности

In article methods of creation and technology basic functions « Smart house» are considered. The basic information threats are analyzed and calculation and an information security risks assessment of "Smart house» is carried out

Keywords: «Smart house», a risk of information security

УДК 004.056.5

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ, ПОСТРОЕННЫХ ПО ТЕХНОЛОГИИ «УМНЫЙ ДОМ»

А.В. Снегуров
Кандидат технических наук, доцент*
Контактный тел.: (057) 702-10-67
Email: arksn@rambler.ru

Е.А. Ткаченко*
Контактный тел.: 063-569-54-77
Email: tkachenko_evgen@bigmir.net

А.Д. Кравченко*
Контактный тел.: 067-251-86-61
Email: kravchenko_ad@rambler.ru
*Кафедра телекоммуникационных систем
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14 г. Харьков, Украина, 61166

Постановка проблемы

Развитие технологии «Умный дом» привело к качественному изменению места и роли систем автоматизации и управления зданиями. Все больше людей задумываются о концепции взаимной увязки разнообразного инженерного оборудования зданий и организационно-технических решений по эксплуатации с

использованием систем автоматизации и управления. Целью использования данной технологии является создание системы, способной поддерживать безопасные и комфортные условия работы или проживания, а также обеспечивать упрощенную систему управления службами и подсистемами здания. Современная система, построенная по технологии «Умный дом» может включать в себя подсистемы управления климатом и освещением, охранной сигнализации и видеонаблюдения, водоснабжения, удаленного мониторинга и другие.

В настоящее время технология «Умный дом» считается одной из самых перспективных и динамически развивающихся. В США данная технология уже давно является широко применяемой в различных сферах автоматизации жилых зданий. В Европе, в том числе и в Украине, популяризация и развитие технологии «Умный дом» только набирает обороты. Наиболее популярными объектами для внедрения данной технологии является коммерческая недвижимость (торговые центры, офисные здания, банки, гостиницы), государственные здания (вокзалы, аэропорты, спортивные и культурные учреждения), а также объекты домашней автоматизации [1].

По данным экспертов компании YORK International [2], прогнозируется ежегодный рост рынка систем, использующих данную технологию на 20-25% в год. Этот рост обусловлен тем, что более развитая инженерная и информационная инфраструктура «Умного дома» позволяет реализовать качественно новый уровень предоставления услуг и существенно повысить его потребительскую ценность.

Однако наряду с очевидными достоинствами может возникнуть целый ряд проблем, связанных с обеспечением информационной безопасности организаций и лиц, использующих данную технологию.

Целью статьи является рассмотрение основных принципов построения технологии «Умный дом», выделение основных угроз информационной безопасности и оценка рисков информационной безопасности при эксплуатации систем, построенных с использованием данной технологии.

Основной материал исследования

При построении систем по технологии «Умный дом» можно выделить два различных подхода, которые имеют различную степень надежности.

- Централизованный;
- Децентрализованный;

Централизованный метод реализации технологии «Умный дом» по своей сути представляет собой объединение разнообразных датчиков и контролеров в единую сложную телекоммуникационную сеть с центральным контроллером [5]. В роли центрального контроллера может применяться сервер, в качестве которого используется любой современный компьютер, и программное обеспечение с поддержкой необходимого программного софта и протоколов. Данный контроллер являются "мозгом" системы автоматизации «Умного дома». В названии отражена главная суть подхода — к центральному котроллеру системы подключены все основные и вспомогательные блоки, при этом все компоненты оснащены собственными микроконтроллерами, но взаимодействуют они исключительно при помощи центрального контроллера.

Телекоммуникационная сеть является основным элементом, обеспечивающим функционирование системы жизнеобеспечения. Через сеть производится съем информации с различного рода датчиков и передача их главному серверу для обработки. Сервер после обработки информации осуществляет передачу сигналов управления на исполнительные элементы (датчики перекрытия воды, включения средств пожаротушения, блокировки дверей и т.д.). Через центральный сервер происходит настройка и управление «Умным домом» легальным пользователем, а также через него при необходимости осуществляется передача заданной информации хозяину квартиры (офиса) при его отсутствии (например, о несанкционированном проникновении, протечках, пожаре). Такая телекоммуникационная сеть может быть построена с использованием как проводных, так и беспроводных каналов связи, например с использованием Wi-Fi, Bluetooth, или 3G.

Использование данного подхода позволяет сочетать устройства разных производителей, что в свою очередь удешевляет развертывание всей системы. Основным минусом является большая зависимость от работы центрального контролера. Также пользователь может с целью управления и контроля подключить центральный контроллер к сети Интернет, тем самым подвергая всю систему различным угрозам и атакам.

Децентрализованный подход подразумевает развертывание системы с распределенной логикой. В отличие от централизованного подхода в децентрализованном подходе отсутствует центральный контроллер. В этом случае система состоит из датчиков, сенсоров и активаторов. Датчики обнаруживают изменение каких-либо характеристик в доме, движения или изменения заданных в программе параметров, и реагируют на эти изменения командой исполняющим устройствам, которые включаются активаторами. При децентрализованном подходе в случае отказа одного из компонентов нарушается только функциональная часть, за которую отвечал этот компонент. Поэтому такие системы являются более безопасными и надежными по сравнению с системами реализованные по централизованному методу. Значительным минусом данного подхода является то, что проектирование системы требует высокой квалификации и большого опыта, что в свою очередь сказывается и на стоимости развертывания системы.

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

Под конфиденциальностью информации 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», могут реализовывать разрешенные в системе

действия (открывать двери, включать кондиционирование или систему пожаротушения, мониторить ситуацию и т.д.). Нарушение доступности информации может привести к невозможности системы реагировать на различные ситуации, в том числе и аварийные.

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 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.

Значение риска информационной безопасности будем рассчитывать на основе вероятности (частоты) реализации угроз на уязвимые элементы системы, эффективности угроз в случае их реализации, а также возможного ущерба для активов системы. Для определения значения риска будем использовать качественную шкалу оценки, которая дает возможность выработать понимание о степени уязвимости систем, построенных по анализируемой технологии. Ниже приведены примеры качественных шкал оценки рисков информационной безопасности.

Под классом актива будем понимать роль той или иной подсистемы (элемента подсистемы) «Умного дома» в обеспечении качества функционирования системы (ущерба функционированию всей системы). Так, например, ложное срабатывание датчика утечки воды и датчика пожарной сигнализации, может привести к различным последствиям.

Качественная шкала оценки уровня класса актива может выглядеть в следующем виде.

Высокое влияние на систему (ВВ) - влияние на конфиденциальность, целостность и доступность элементов системы может причинить организации (владельцам) значительный или катастрофический ущерб.

Среднее влияние на систему (СВ) - влияние на конфиденциальность, целостность и доступность элементов системы может причинить организации (владельцам) средний ущерб. Средний ущерб не вызывает значительных или катастрофических изменений, однако нарушает нормальную работу организации (нормальную жизнедеятельность).

Низкое влияние на **систему (НВ)** – влияние на конфиденциальность, целостность и доступность элементов системы не причиняет организации (владельцам) какого – либо серьезного ущерба.

Оценку вероятности реализации угрозы на уязвимые элементы системы, построенной по технологии «Умный дом», будем оценивать через частоту реализации угрозы за определенный период.

1. **Высокая.** Вероятно реализация одного или нескольких угроз в пределах года.

2. **Средняя**. Угроза может возникнуть в пределах двух-трех лет.

3. **Низкая.** Возникновение угрозы в пределах трех лет маловероятно.

Оценку эффективности реализации угрозы на уязвимые элементы данной системы будем оценивать по следующей шкале:

1. **Высокая подверженность воздействию.** Значительный или полный ущерб для актива.

2. **Средняя подверженность воздействию.** Средний или ограниченный ущерб.

3. **Низкая подверженность воздействию.** Незначительный ущерб или отсутствие такового.

Так, например, такой канал утечки конфиденциальной информации, как съем злоумышленником побочных электромагнитных излучений сервера, имеет разную эффективность в различных условиях и может принимать значение от низкой до высокой подверженности воздействию.

Для вычисления уровня риска будем использовать подход, предложенный компанией Microsoft.

На первом этапе, на основании значения класса актива и оценки подверженности актива воздействию (эффективности реализации угрозы) определяется уровень влияния (таблица 1).

Таблица 1

Определение уровня влияния

Класс актива	Высокое влияние	Средний	Высокий	Высокий
	Среднее влияние	Низкий	Средний	Высокий
	Низкое влияние	Низкий	Низкий	Средний
		Низкая	Средняя	Высокая
		Уровень подверженности воздействию		

На втором этапе, на основании уровня влияния и вероятности реализации угрозы определяется итоговый риск информационной безопасности (таблица 2).

Таблица 2

Определение итогового риска

Влияние (из таблицы 1)	Высокий	Средний	Высокий	Высокий
	Средний	Низкий	Средний	Высокий
	Низкий	Низкий	Низкий	Средний
		Низкий	Средний	Высокий
		Уровень вероятности реализации угрозы		

Проведем оценку рисков информационной безопасности системы, построенной по технологии «Умный дом». В качестве примера возьмем помещение офиса, в котором циркулирует конфиденциальная информация, существуют требования по обеспечению доступности и целостности информации, а также требования по нормальной жизнедеятельности сотрудников. Все офисное оборудование подключено через единую сеть, которую контролирует центральный контролер.

Необходимо отметить, что точная оценка рисков информационной безопасности должна осуществляться для конкретных условий существования организации, к которым относятся степень важности информации, циркулирующей в организации, ее расположение, используемые механизмы управления информационной безопасностью и т.д. В данной статье производится только приближенная оценка рисков для выработки понимания о необходимости использования механизмов обеспечения информационной безопасности таких технологий.

Выделим наиболее вероятные угрозы, через которые может произойти нарушение информационной безопасности «Умного дома» при использовании централизованного подхода.

Таблица 3

Угрозы информационной безопасности «Умного дома»

№	Тип атаки	Уязвимость	Возможные последствия
1	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)
2	Влияние вирусных и троянских программ на работу системы	Подключение сети «Умного дома» к Интернет. Отсутствие (неэффективность) механизмов защиты периметра сети	Сбой в ПО системы, а следовательно нарушение работы либо вывод из строя аппаратуры системы. Нарушение КЦД информации, находящейся внутри сети
3	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
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	Ошибки пользователя.	Отсутствие (неэффективность) механизмов защиты системы от неправильных действий пользователей	Нарушение КЦД информации. Возможны сбои в системе из-за неправильного использования оборудования
8	Кража (злоумышленный вывод из строя аппаратуры) системы «Умного дома»	Отсутствие (неэффективность) – физической охраны объекта	Нарушение КЦД информации
9	Перебои в сети электропитания	Отсутствие системы автономного электропитания	Дезорганизация работы системы
10	Стихийные бедствия (пожар и др.)	Отсутствие (неэффективность) механизмов защиты	Дезорганизация работы системы
11	Поломка аппаратуры системы	Низкая надежность оборудования, низкая квалификация персонала	Нарушение КЦД информации
12	Ошибки программного обеспечения	Использование нелицензионного ПО, низкая квалификация персонала, отсутствие (неэффективность) тестирования закупаемого ПО	Нарушение КЦД информации
13	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
14	Утечка информации по акустоэлектрическому каналу	Наличие акустоэлектрических преобразователей (датчики охранной, пожарной сигнализации и т.д.), подключенных к проводным линиям	Нарушение конфиденциальности информации

Уровень риска для выделеных угроз ”Умного дома” представлен в таблице 4

Таблица 4

Уровень риска для выделеных угроз ”Умного дома”

№	Тип атаки	Вероятность атаки	Уровень подверженности воздействию	Класс актива	Уровень риска
1	Хакерские атаки на центральный сервер	Высокая	Высокий	Высокое влияние	Высокий
2	Влияние вирусных и троянских программ на работу системы	Высокая	Высокий	Высокое влияние	Высокий
3	Перехват информации, передаваемой по проводным и беспроводным каналам связи	Средняя	Средний	Среднее влияние	Средний
4	Доступ злоумышленника с правами администратора на центральный сервер с помощью хищения паролей и других реквизитов разграничения доступа	Низкая - средняя	Высокий	Высокое влияние	Высокий
5	Доступ к сети неавторизованных пользователей	Высокий	Среднее	Среднее – низкое	Высокий - средний
6	Наличие нарушителей в числе обслуживающего персонала (охранники, наладчики, уборщики и др.)	Средняя	Высокий	Высокое – среднее влияние	Высокий
7	Ошибки пользователя	Высокая	Средний	Низкое влияние	Средний
8	Кража (злоумышленный вывод из строя аппаратуры) системы «Умного дома»	Средняя	Высокий	Среднее – низкое влияние	Высокий - средний
9	Перебои в сети электропитания	Низкая (если есть автономный источник электропитания) Высокая (если автономного электропитания нет)	Высокий	Высокое влияние	Средний - высокий
10	Стихийные бедствия (пожар и др.)	Средняя	Высокий	Высокое влияние	Высокий
11	Поломка аппаратуры системы	Средняя	Средний	Среднее влияние	Средний
12	Ошибки программного обеспечения	Средняя - высокая	Высокий	Высокое влияние	Высокий
13	Утечка информации через побочные электромагнитные излучения и наводки (ПЭМИН)	Средняя	Средняя	Среднее влияние	Средний
14	Утечка информации по акустоэлектрическому каналу	Средняя	Средняя	Среднее влияние	Средний

Выводы

Исходя из результатов оценки, самыми опасными являются те угрозы, при которых злоумышленник может брать под контроль всю систему, построенную по анализируемой технологии. Поэтому крайне необходимым является проведение мероприятий по защите телекоммуникационной сети, разграничение прав доступа пользователей, защита от инсайдеров. Опасными являются риски 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. Поэтому важной задачей при проектировании подобных систем является детальная оценка риска для конкретных условий с анализом всех потенциальных угроз и уязвимостей. В дальнейших исследованиях будут разработаны методики оценки результатов воздействия различных угроз на уязвимые элементы систем, построенных по технологии «Умный дом».

Литература

1. «Умный дом» [Электронный ресурс] — Режим доступа: \www/ URL: http://umnydom.kiev.ua/index.php?nma=catalog&fla=stat&cat_id=3&page=1&nums=24/ — 05.03.2011 г. — Загл. С экрана.
2. 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.
3. Гирак П. «Интелектуальное здание»: зачем тратить деньги? [Текст]/ П. Гирак// Журн. S.M.A.R.T. — 2008. – № 2.- С. 8-12.
4. Кузьмич А. Неутомимый труженик. Системы «Умного дома» [Текст]/ А. Кузьмич// Журн. S.M.A.R.T. — 2009. – № 2.- С. 10-13.
5. Категории «Умных домов» [Электронный ресурс] / Дом Бизнес Строй. — Режим доступа: \www/ URL: http://ruswires.net/post_1267720042.html/ — 04.03.2011 г. — Загл. С экрана.