

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут інформатики та радіоелектроніки
Факультет радіоелектроніки і телекомунікацій
(повне найменування інституту, назва факультету)

Кафедра захисту інформації
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

магістр

(ступінь вищої освіти (освітній ступінь))

на тему: Аналіз вразливостей системи захисту в об'єктах типу
«Розумний будинок»

Виконав: студент 6 курсу, групи РТ-713м
спеціальності (напряму підготовки)
125 Кібербезпека (Системи технічного
захисту інформації, автоматизація її
обробки)

(код і назва напряму підготовки, спеціальності)

Король З.З.

(прізвище та ініціали)

Керівник Лізунов С.І.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

Запоріжжя - 2018 рік

Запорізький національний технічний університет

(повне найменування вищого навчального закладу)

Інститут, факультет Інститут інформатики та радіoeлектроніки, Факультет радіoeлектроніки та телекомунікацій

Кафедра захисту інформації

Рівень вищої освіти (освітньо-кваліфікаційний рівень) магістр

Напрямок підготовки 125 Кібербезпека

(код і назва)

Спеціальність Системи технічного захисту інформації, автоматизація її обробки

(код і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри _____

Л.М. Карпуков

« _____ » 2018 р.

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Королію Зоряну Зоряновичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Аналіз вразливостей системи захисту в об'єктах типу «Розумний будинок»

керівник проекту (роботи) доц., к.т.н. Лізунов Сергій Іванович

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу

від “ 07 ” 11 2018 року № 329

2. Строк подання студентом проекту (роботи) 10 грудня 2018 р.

3. Вихідні дані до проекту (роботи) об'єкт типу «Розумний будинок», література по темі

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) аналіз системи «Розумний будинок»; аналіз загроз та вразливостей; розробка моделі вразливостей системи захисту в об'єктах типу «Розумний будинок»; методи боротьби з вразливостями

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) можливості «Розумного будинка»; інтелектуальні системи управління; вид теплопотоку системи «Розумний будинок»; двудольний граф вразливостей і засобів та механізмів захисту; схема роботи CUJO

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основна частина	доц., к.т.н. Лізунов С.І.		
Економічна частина	Левченко Н.М.		
Охорона праці	Коробко О.В.		
Нормоконтроль	ст. викл. Нікуліщев Г.І.		

7. Дата видачі завдання « 03 » вересня 2018 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Складання та затвердження ТЗ, підбір літератури	03.09-16.09.2018	
2	Аналіз системи «Розумний будинок»	17.09-23.09.2018	
3	Аналіз загроз і вразливостей	24.09-30.09.2018	
4	Модель дій зловмисника	01.10-07.10.2018	
5	Розробка моделі вразливостей системи захисту «Розумного будинка»	08.10-14.10.2018	
6	Оцінка ризику виділених загроз та вразливостей	15.10-21.10.2018	
7	Методи боротьби з вразливостями	22.10-28.10.2018	
8	Розробка економічної частини	29.10-04.11.2018	
9	Розробка заходів з охорони праці	05.11-11.11.2018	
10	Оформлення графічної частини	12.11-25.11.2018	

11	Оформлення пояснювальної записки	26.11-09.12.2018	
----	----------------------------------	------------------	--

Студент _____ Король З.З.
(підпис)

Керівник проекту (роботи) _____ Лізунов С.І.
(підпис)

РЕФЕРАТ

ПЗ: 85 стр., 6 рис., 15 табл., 15 источников.

Цель магистерской работы – анализ уязвимостей системы защиты в объектах типа «Умный дом».

Поставленная цель предполагает решение следующих взаимосвязанных задач:

- исследовать систему «Умный дом»;
- выделить основные угрозы и уязвимости системы;
- разработать модель уязвимостей системы защиты «Умного дома»;
- провести оценку уровней риска для выделенных угроз и уязвимостей;
- предложить методы и средства борьбы с уязвимостями.

СИСТЕМА «УМНЫЙ ДОМ», УГРОЗЫ И УЯЗВИМОСТИ, МОДЕЛЬ
УЯЗВИМОСТЕЙ СИСТЕМЫ ЗАЩИТЫ «УМНОГО ДОМА», ОЦЕНКА
УРОВНЕЙ РИСКА УГРОЗ И УЯЗВИМОСТЕЙ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ИК – инфракрасная

КПК – карманный персональный компьютер (планшет)

КС – кабельная система

КЦД – конфиденциальность, целостность, доступность информации

НСД – несанкционированный доступ

ОС – операционная система

ПК – персональный компьютер

ПО – программное обеспечение

ПЭМИ – побочные электромагнитные излучения

ПЭМИН – побочные электромагнитные излучения и наводки

СКС – структурированная кабельная система

СОДЕРЖАНИЕ

Введение.....	8
1. Система «Умный дом».....	9
1.1. Возможности системы «Умный дом».....	10
1.2. Назначение и характеристики подсистем «Умного дома».....	11
1.2.1. Подсистема охраны.....	12
1.2.2. Подсистема пожарной безопасности.....	14
1.2.3. Подсистема оповещения.....	15
1.2.4. Подсистема автоматических ворот и жалюзи.....	15
1.2.5. Автономные источники питания.....	16
1.2.6. Подсистема средств общения «Умного дома».....	17
1.2.7. Подсистема отопления.....	19
1.2.8. Подсистема водоснабжения.....	20
1.2.9. Подсистема газоснабжения.....	21
1.2.10. Подсистема освещения.....	21
1.2.11. Мультирум.....	22
1.2.12. Подсистема слаботочные системы.....	23
1.3. Проводная и беспроводная системы «Умный дом».....	25
1.4. Классификация систем по степени централизации и «открытости»....	27
2. Анализ угроз и уязвимостей.....	29
2.1. Система «Умный дом» глазами хакера.....	29
2.2. Уязвимости системы управления «Умный дом».....	31
2.3. Анализ угроз.....	32
3. Разработка модели уязвимостей системы защиты «Умного дома».....	36
3.1. Модель нарушителя.....	36
3.2. Модель уязвимостей.....	40
3.3. Оценка риска выделенных угроз и уязвимостей «Умного дома».....	42

3.4.	CUJO – система защиты для «Умного дома».....	48
4.	Экономическое обоснование магистерской работы.....	51
4.1.	Планирование разработки модели уязвимостей системы защиты в объектах типа «Умный дом».....	51
4.2.	Построение сетевого графика.....	53
4.3.	Расчет параметров сетевого графика.....	54
4.4.	Определение затрат на разработку и проектирование.....	56
4.4.1.	Расчет основной заработной платы.....	56
4.4.2.	Отчисления на социальное страхование и другие фонды.....	56
4.4.3.	Определение затрат на материалы и комплектующие.....	56
4.4.4.	Затраты на специальное оборудование.....	57
4.4.5.	Накладные расходы.....	60
4.5.	Оценка экономической эффективности от реализации магистерской работы.....	60
5.	Охрана труда и безопасность в чрезвычайных ситуациях.....	64
5.1.	Анализ потенциальных опасностей.....	64
5.2.	Мероприятия по обеспечению безопасности.....	65
5.3.	Мероприятия по промышленной санитарии и гигиене труда.....	68
5.4.	Мероприятия по пожарной безопасности.....	74
5.5.	Мероприятия по обеспечению безопасности в чрезвычайных ситуациях.....	76
5.6.	Выводы по разделу «Охрана труда и безопасность в чрезвычайных ситуациях».....	80

Заключение.....	82
Список литературы.....	84

ВВЕДЕНИЕ

Системы автоматизированного управления зданиями или системы «Умного дома» получили большую популярность в последнее время. «Умный дом» – это автоматизированное строение современного типа, организованное для удобства людей при помощи высокотехнологичных устройств. Это может быть не только жилой дом, но также и государственное учреждение, стадион и даже аэропорт.

Большая часть современного оборудования, производимого для систем автоматизированного управления зданиями разными компаниями, может быть интегрирована в единые сети. Это становится возможным благодаря гибкости и структурированности автоматизированных сетей. В результате этого здание становится все более функциональным.

Однако в интеграции существуют свои недостатки. Дело в том, что сочетание разных технологий при построении одной автоматизированной системы увеличивает количество возможных недостатков решения с точки зрения безопасности. У каждой технологии, какой бы совершенной она ни была, существуют свои уязвимости. Увеличение числа устройств и технологий, используемых в системе, ведет к повышению уязвимости. Кроме того, процесс интеграции разных решений не исключает возможности допущения ошибки в проектировании. Это может привести к появлению дополнительных слабых мест в системе.

Мошенники могут воспользоваться уязвимостями современных систем автоматизированного контроля жизнеобеспечения «Умного дома» и предпринять попытку атаки.

1 СИСТЕМА «УМНЫЙ ДОМ»

«Умный дом» - жилой дом современного типа, организованный для проживания людей при помощи автоматизации и высокотехнологичных устройств. Само понятие «умный дом» было сформулировано Институтом интеллектуального здания в Вашингтоне (округ Колумбия) в 1970-х годах: здание, обеспечивающее продуктивное и эффективное использование рабочего пространства [1].

Под «Умным домом» следует понимать систему, которая обеспечивает комфорт (в том числе безопасность), и ресурсосбережение для всех пользователей. В простейшем случае она должна уметь распознавать конкретные ситуации, происходящие в доме, и соответствующим образом на них реагировать: одна из систем может управлять поведением других по заранее выработанным алгоритмам.

Основной особенностью интеллектуального здания является объединение отдельных подсистем в единый управляемый комплекс.

Принцип «Системы интеллектуального управления зданием» предполагает совершенно новый подход в организации жизнеобеспечения строения, в котором за счет комплекса программно-аппаратных средств значительно возрастает эффективность функционирования и надежность управления всех систем и исполнительных устройств здания.

Важным свойством «Умного дома», отличающим его от других способов организации жизненного пространства, является то, что это наиболее прогрессивная концепция взаимодействия человека с жилым пространством, когда человек одной командой задает желаемую обстановку, а уже автоматика в соответствии с внешними и внутренними условиями задает и отслеживает режимы работы всех инженерных систем и электроприборов.

1. Возможности системы «Умный дом»

«Умный дом» – это своего рода интеллектуальная электропроводка, которая работает на базе управляющей программы. Программа, в свою очередь, управляет домом и контролирует работу различных домашних приборов и инженерных систем. Она может управлять системами безопасности, кондиционирования и вентиляции, а также шторами, жалюзи, воротами или различными инженерными элементами, электроприборами.

Основными задачами системы «Умного дома» являются безопасность, автоматизация помещений, комфорт, бесперебойность, экономия электроэнергии.

Система «Умного дома» исключает необходимость использовать:

- пульты управления системами видеонаблюдения и охранно-пожарной сигнализации;
- блоки управления системами отопления и климатической техники;
- панели управления воротами, жалюзи и прочим;
- десятки выключателей света для управления освещением;
- несколько пультов при просмотре телевидения.



Рисунок 1.1 – Возможности «Умного дома»

В доме, оборудованном системой «Умный дом» достаточно одним

нажатием на настенной клавише (или пульте ДУ, сенсорной панели и т. д.) выбрать один из сценариев. При этом вы сможете дистанционно контролировать, включать и выключать работу различных приборов.

Возможности системы «Умный дом» поистине многогранны. Например, чтобы предотвратить вероятность ограбления, когда в доме никого нет, система имитирует присутствие хозяина путем раздвигания жалюзи, включения/выключения света и т.д. Если же злоумышленники все же проникают внутрь помещения или происходит другая экстраординарная ситуация, система молниеносно оповещает об этом хозяина.

2. Назначение и характеристики подсистем «Умного дома»

Под термином «Умный дом» обычно понимают интеграцию следующих подсистем в единую систему управления зданием [2]:

1. Система безопасности и мониторинга.
2. Системы управления и связи.
3. Система отопления, вентиляции и кондиционирования.
4. Система удалённого управления электроприборами, приводами механизмов и всеми системами автоматизации.
5. Система автоматической механизации здания (открытие/закрытие ворот, шлагбаумов, электроподогрев пола и т. п.)
6. Система управления с одного места аудио-, видеотехникой, домашним кинотеатром, подсистема «мультирум».
7. Система электропитания здания.
8. Система освещения.

Все подсистемы, которые контролируются «Умным домом», можно поделить на такие группы:

1. Безопасность (проводится контроль работы систем доступа, видеонаблюдения, следит за атмосферой в доме – загазованность, задымленностью, сигнализирует о попытках злоумышленников

проникнуть в дом, о пожаре, контролирует доступ к информации и техническим системам).

2. Инженерная (управления вентиляционной системой, системами кондиционирования, водо-, тепло-, электроснабжения, телекоммуникаций и освещения).

3. Развлечения (мультирум, домашнее кино, эфирное и спутниковое ТВ).

Рассмотрим основные подсистемы «Умного дома».

2.1. Подсистема охраны

Контроль проникновения в помещение позволяет контролировать внутренние помещения в доме или квартире. Получив сигнал о проникновении, система проинформирует о возникшей аварии, позвонившись по телефонной линии и голосом сообщив о причине вызова, а также отправит тревожное SMS-сообщение, включит сирену и внешний световой сигнал, чтобы отпугнуть воров.

Датчики движения, которые включают аварийную сигнализацию в случае взлома могут также установить внешний контроль проникновения, оставаясь внутри дома, заблокировав при этом участок (или двери и окна).

Имитация присутствия: при длительном отсутствии система по заданному графику будет включать свет, музыку, раздвигать шторы, создавая иллюзию вашего присутствия.

Имитация присутствия животных. Данная функция отпугнет случайного воришку, при нажатии на кнопку звонка в квартире раздастся грозный лай собаки.

Ограничение доступа. В системе предусмотрен 3-х уровневый доступ к управлению системой (условно хозяин, член семьи и гость), ограничивая круг лиц, полностью управляющих системой.

Система видеонаблюдения. Беспроводная система видеонаблюдения может работать 24 часа в сутки, не упуская из виду ни один уголок дома. По желанию, можно настроить систему в режим ожидания. Цифровое видеонаблюдение превосходно интегрируется в «Умный дом» и слаженно работает в команде с охранными системами. Как только тревожный видеосигнал поступит в систему охраны, «Умный дом» среагирует сигнальным оповещением, сообщит о происшествии вам и оперативному отряду.

Дом постоянно ведет непрерывное ip видеонаблюдение не только внутри помещения, но и за периметром. Видеокамеры мгновенно реагируют на движение объектов. И в том случае, когда кто-то появится на придомовой территории камеры, моментально запишут это событие и сообщат на компьютер, телевизор или панель. При этом нет необходимости разбираться и пролистывать архив с какой видеокамеры поступил сигнал. Система сама покажет нужный фрагмент.

Видеоархив пишется в ночное время. Благодаря световым датчикам не один нарушитель не сможет быть незамеченным. Внезапный свет от камеры - и вор в центре внимания. Вы сможете увидеть видеозапись с момента реагирования камеры или датчиков.

Также система видеонаблюдения умеет распознавать объекты движения. Встроенный интеллект определит – злоумышленник или это домашнее животное гуляет по дому. В случае опасности система незамедлительно среагирует.

Управлять системой видеонаблюдения можно как находясь дома, так и будучи в отъезде. Видеосигналы с камер обрабатываются и сохраняются в многодневный видеоархив. После чего возможно управлять этими записями с любого монитора или телевизора. Видеокамеры могут менять режимы запись/не запись в зависимости от установленных условий – таймер, реакция на движение, включена охранная система, определенное время суток.

Особой функцией системы является видеоаналитика – домашний оператор осуществляет анализ видеосигналов. В зависимости от выявленных факторов дом сам принимает решение каким образом реагировать на ту или иную ситуацию и какие меры безопасности предпринимать.

2.2. Подсистема пожарной безопасности

Контроль возгорания. Система мгновенно приведёт в действие существующую противопожарную систему, отключит вентиляцию, чтобы поток воздуха не способствовал возгоранию, электричество и газ. А если вас нет дома, голосом сообщит о случившемся, дозвонившись по телефону, а также отправит тревожное SMS-сообщение. Система также включит сирену и внешний световой сигнал, чтобы предупредить соседей о случившемся и уберечь от опасности.

Последовательность действий системы при возникновении возгорания [3]:

1.Информация о возгорании и о времени его возникновения заносится в протокол сообщений.

2.Информация о датчике, зафиксировавшем возгорание, заносится в протокол сообщений.

3.Выключается электроэнергия и электророзетки.

4.Перекрывается подача газа.

5.Выключается вентиляция.

6.Включается система дымоудаления.

7.Включается внешний сигнал «ПОЖАР».

8.Производится звонок по определенным пользователем номерам при возгорании.

9.Выключается режим контроля возгорания.

2.3. Подсистема оповещения

Голосовое сообщение. Система голосом оповестит обо всех событиях в доме и вовремя обо всём напомним. При возникновении аварийных ситуаций она голосом сообщит о причине вызова, дозвонившись по телефону.

Автодозвон по телефонным номерам. В случаях возгорания, проникновения, утечки газа, протечки воды, нажатия тревожной кнопки и при аварии системы осуществляется дозвон по телефонной линии и голосом сообщается о причине дозвона. Номера телефонов и голосовые сообщения вводятся пользователем с пульта и монитора компьютера.

Об аварии система может оповестить хозяина и по сотовой связи, послав SMS-сообщение 5-ти абонентам.

С помощью добавочного модуля программы контролировать состояние дома можно находясь далеко за его пределами через всемирную сеть Интернет. Стоит только послать запрос, и система пришлёт информацию о текущем состоянии дома.

2.4. Подсистема автоматических ворот и жалюзи

Дистанционное управление воротами - позволяет полностью автоматизировать процесс открывания и закрывания ворот, шлагбаумов. Автоматика для ворот состоит из блока управления и датчиков с фотоэлементами. Также прилагается пульт, с помощью которого осуществляется дистанционное управление воротами.

При нажатии на определенную кнопку на пульте, автоматика ворот принимает сигнал, после чего выполняет соответствующую команду. Главной задачей фурнитуры для ворот является предотвращение возможности контакта створок с въезжающим или выезжающим автотранспортом. Датчики устанавливаются на расстоянии 30 - 90 см от поверхности земли и

срабатывают в тот момент, когда на пути закрывающихся ворот находится какое-либо препятствие – автомобиль, люди, животные и т.д. При этом, процесс закрытия/открытия ворот, шлагбаума автоматически прекращается до тех пор, пока препятствие не будет убрано.

Управление жалюзи. Работа автоматики базируется на датчиках, встроенных в карнизы. Исполнительные команды передаются через панель управления и система распоряжается работой модуля согласно указанным условиям.

Система способна автоматически контролировать доступ солнечного света в помещение в зависимости от времени суток и погодных условий, закрывать все жалюзи в доме при постановке его на сигнализацию, обеспечивать оптимальные условия для нахождения в помещении.

2.5. Автономные источники питания

Собственная система автономного источника питания будет обеспечивать гарантированную и бесперебойную работу всего электрического и инженерного оборудования дома. В случае сбоя, поломки или отказа электросети резервное электроснабжение предоставит выделенную мощность, необходимую для работы оборудования дома.

Источниками бесперебойного электропитания для дома могут быть [3]:

1.Стабилизатор напряжения – устройство защиты от перепадов напряжения и помех сети, которое при нестабильном входном напряжении поддерживает на выходе номинальное напряжение (220В/50Гц).

2.Источник резервного электропитания – работает от внутренних аккумуляторных или внешних подключаемых батарей различной емкости.

Резервное электроснабжение активируется в случае сбоев или отсутствия напряжения в общей электросети. Электрогенератор автоматически приводится в действие с помощью автомата ввода резерва.

Бывают дизельные, газовые или бензиновые электростанции, которые могут формировать как постоянный, так и переменный ток.

Такие типы электрогенераторов могут служить как резервным источником питания – предназначены для кратковременного использования (на несколько часов), так и постоянным источником – для круглосуточного электроснабжения объекта на длительный срок (для строящихся объектов).

Источником бесперебойного электропитания дома могут быть инверторы различной мощности, вырабатываемая электроэнергия которыми зависит от аккумуляторных батарей. За время стабильной работы основной системы электропитания инвертор бесперебойного питания (ИБП) аккумулирует заряд в батареях.

ИБП защищают электросеть от кратковременного отключения и падения напряжения, от искажения формы сигнала, частоты, шумов, выбросов и перегрузок.

2.6. Подсистема средств общения «Умного дома»

Управление через Internet. Для управления и настройки дома из офиса, машины и т.д. программа позволяет с помощью электронной почты передавать необходимые команды. Для этого основная программа разделяется на два независимых модуля, один из которых находится в доме и ждет команд. Другой же находится вместе с вами на вашем рабочем компьютере.

Дистанционное управление. Для удобства управления бытовыми устройствами в доме, был создан пульт дистанционного управления, позволяющий совмещать в себе управление телевизором, видеомagniтофоном, музыкальным центром, спутниковым ресивером.

Он так же позволяет включать и отключать: осветительные приборы, управляемые электрические розетки, различные сценарии освещения. При помощи комбинаций нескольких кнопок – открыть ворота, поставить дом на

охрану и совершить много других различных действий.

Контроль и управление всем домом посредством пульта системы «Умный дом»:

Настенный пульт – основной пульт системы, позволяющий вам полноценно работать со всеми функциональными возможностями системы. Предназначен для ввода информации в систему и её отображения.

При входе в дом вы с помощью него снимаете систему с охраны, а уходя из дома – устанавливаете систему на охрану. Вы можете просмотреть протокол сообщений о событиях, произошедших за ваше отсутствие, ввести номера телефонов, по которым будет производиться звонок в аварийных ситуациях и т.д.

Управление с компьютера. Дружественная для пользователя программа, работающая в среде операционной системы Windows, позволяет включать и выключать определённые режимы системы «Умный дом», а также производить настройки её работы, читать и выводить на печать протокол сообщений.

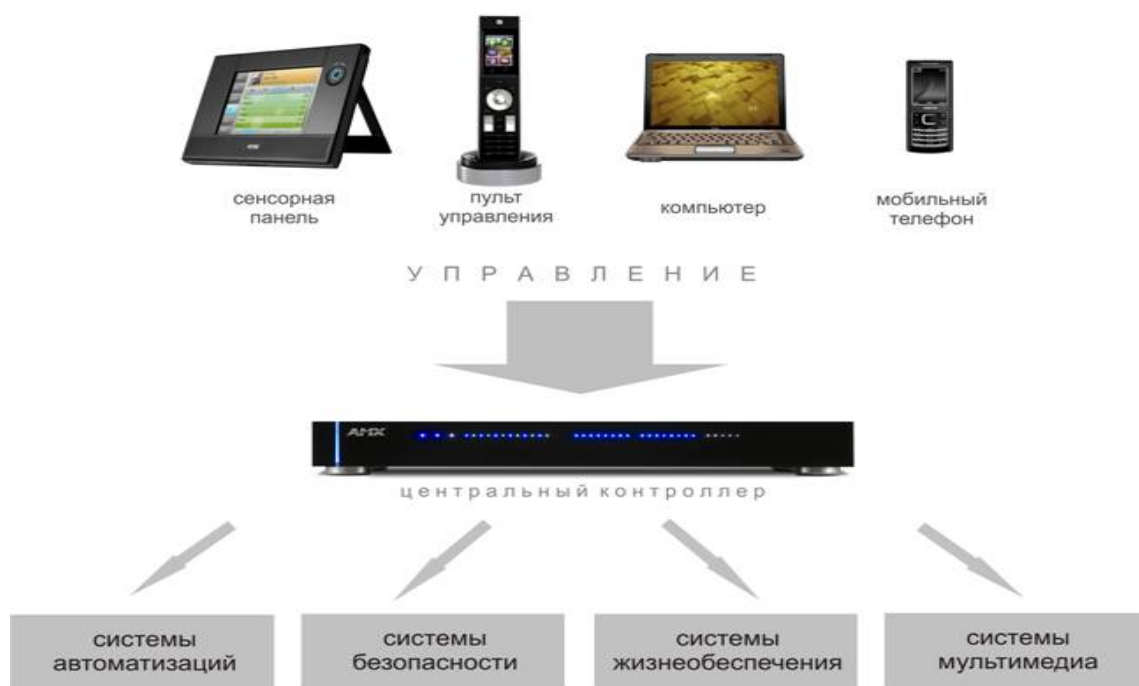


Рисунок 1.2 – Интеллектуальные системы управления

2.7. Подсистема отопления

Система позволяет управлять отоплением нескольких помещений (до 512). Температурный диапазон измерения и регулировки заданных температур от 0 до 125°C (сауна) [3].

В каждом помещении задана недельная программа со своими температурными и временными установками. Это позволяет добиться оптимального управления отоплением дома и дает экономию электроэнергии. Задание режима и температуры может осуществляться с пульта или экрана компьютера. Производя управление с компьютера, можно установить любую программу отопления.

Принцип действия: система обрабатывает сигналы от подключённых датчиков и включает (выключает) подключённые источники тепла (электрические тёплые полы, ИК-панели, электрические конвекторы), в зависимости от значения текущей температуры, доводя тем самым температуру в помещении к заданной.

Во главе стоит главный блок (MAIN), обмен информацией его с портом и с пультом осуществляется через общую шину SST-BUS. Датчики температуры и источники тепла подключаются к порту, который ведёт с ними обмен информацией (принимает сигналы от датчиков и включает или выключает источники тепла).

Сохранение в памяти заданных параметров неограниченно долго даже при выключенном сетевом напряжении.

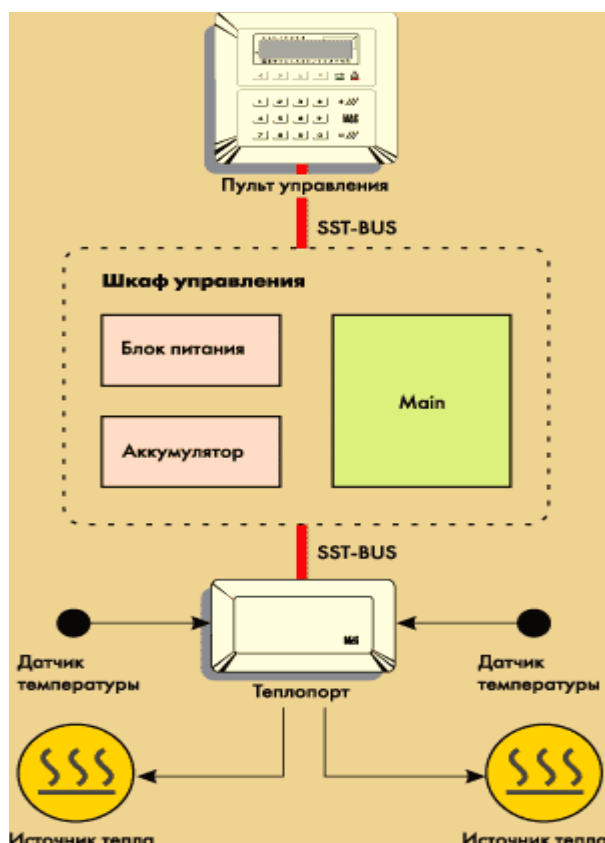


Рисунок 1.3 – Вид теплопорта системы «Умный дом»

2.8. Подсистема водоснабжения

Система может быть, как проводной, так и работать на радиоканале - это позволяет провести установку до и после ремонта.

Предотвращение протечки воды, контроль протечек воды. Расположенные в местах возможной протечки воды (на полу под раковиной, ванной, стиральной машиной и т.д.) датчики вовремя «обнаружат» протечку воды в системе водоснабжения или отопления.

Получив сигнал от подключённых датчиков протечки воды системы водоснабжения, система заблокирует подачу воды до устранения причин протечки и проинформирует вас о возникшей аварии, дозвонившись по телефонной линии и голосом сообщив о причине вызова, а также отправит тревожное SMS-сообщение. В случае протечки система управления

водоснабжением заблокирует подачу воды электромагнитными клапанами либо отключит работу насоса. В системе предусмотрены 2 контура контроля (например, разные этажи), работающие независимо.

2.9. Подсистема газоснабжения

Контроль утечки газа предназначен для своевременного отключения подачи газа и информирования при возникновении данной аварийной ситуации, что позволяет снизить ущерб от возможного взрыва и возгорания помещения (дома) и как следствие – спасти вашу жизнь.

Расположенные в местах возможной утечки газа датчики подадут сигнал системе, которая включит сигнализацию, вентиляцию, и выключит электроэнергию, оставив только аварийное освещение. При возникновении аварии система проинформирует о возникшей аварии, дозвонившись к вам по телефонной линии и голосом сообщив о причине вызова, а также отправит тревожное SMS-сообщение.

Принцип работы системы контроля утечки газа: при срабатывании датчика утечки газа или датчика пожара – поступает сигнал на порт системы «McS». Порт формирует сигнал на главный блок системы. Главный блок выдает команду на клапаны перекрытия газа и на автодозвониватель. Клапан перекрывает газ. Автодозвониватель в это время производит дозвон по обозначенным телефонам и голосом или SMS сообщает о случившейся аварии.

2.10. Подсистема освещения

Системы управления освещением делят на локальные и глобальные. Первые управляют освещением в одной комнате, вторые – комплексно с помощью единой панели, в том числе и на улице. Обычно дневное и искусственное освещение объединяют в единую систему, компоненты

интегрируют в единый комплекс. Например, в вечернее время автоматически закрываются шторы или жалюзи, включается свет в комнате. Такая система может выполнять [3]:

- голосовое и автоматическое управление освещением на территории вне дома, в каждой комнате отдельно и во всем доме из любой из них;
- создавать эффект присутствия, решения реализуются программно;
- регулировать освещение в соответствии с ситуацией и временем суток;
- включать и выключать освещение в коридоре и других «проходных» зонах;
- переключать энергозависимое оборудование и освещение в режим экономии;
- отключать определенные зоны при перегрузке в сети;
- обеспечивать световое сопровождение, наращивая постепенно интенсивность света до нужного значения при передвижении по дому ночью.

2.11. Мультирум

Мультирум – это система распределения видео- и аудиосигналов по нескольким комнатам-зонам. Он реализует передачу изображения и звука от разных источников в разные помещения дома. В общем случае система мультирум состоит из источников сигнала (DVD-плеер, видеомаягнитофон, спутниковый ТВ-тюнер), нескольких устройств коммутации, кабельной сети передачи, акустических систем, телевизоров.

Состав может варьироваться, но суть одна: мультирум – это централизованно управляемые изображения и звук, передаваемые по всей квартире.

Функционирование системы мультирум обеспечивают [3]:

- приемник/передатчик, в роли которого выступает специальный матричный коммутатор;
- интерфейс дистанционного управления, выполненный в виде пульта;
- звуковые усилители;
- настенные панели управления сенсорного типа, с помощью которых удобно работать с центральным хранилищем данных.

Система мультимедиа решает такие задачи:

1. Организация потока аудио и видео с индивидуальным источником и уровнем звука в любую из комнат, подключенных к системе.
2. Создание и поддержка централизованного хранилища данных, используемого на различных устройствах.
3. Обеспечение оповещения и связи между различными помещениями, подключенными к системе.
4. Создание звуковых эффектов при переходе между комнатами и озвучивание бани, сауны, бассейна – любых помещений и даже прилегающей территории.

2.12. Подсистема слаботочные системы

Структурированная кабельная система – это совокупность кабелей, разъемов, панелей и распределительных устройств, объединяющие здание или группу зданий в единое информационное пространство [3]. Такая система включает в себя компьютерные, телефонные, телевизионные сети, а также кабели охранной и пожарной сигнализации, систем контроля доступа и других систем безопасности.

Основное отличие СКС от простого комплекса сетей заключается в том, что СКС проектируется и монтируется на этапе строительства, и в нее изначально заложена огромная мощность и пропускная способность. Это является одновременно и основным достоинством структурированных

кабельных систем (каналы СКС способны выдержать очень большую нагрузку) и их основным недостатком (в отличие от проектирования и монтажа простых телефонных или компьютерных сетей проектирование СКС требует привлечения специалистов высочайшей квалификации).

Центральным элементом структурированных кабельных систем является главный коммутационный узел здания, который представляет собой аппаратный комплекс, объединяющей все входящие и исходящие кабели этажных коммуникационных узлов с каналами, ведущими из здания. Этажные КС в свою очередь объединяют все кабели, идущие от входных точек этажа, и являются, таким образом, коммуникационными узлами второго порядка.

Входные точки или точки входа представляют собой не что иное, как разъемы для подключения различных устройств к системе кабелей. Примерами таких устройств могут быть:

- датчики и контрольные панели систем безопасности;
- персональные компьютеры;
- серверы;
- телефонные аппараты, факсимильные аппараты.

Система ЛВС (локальная вычислительная сеть) выполняет ряд функций:

- обеспечивает обмен данными между основными узлами системы «Умного дома» (Центральным контроллером, панелями и пультами управления);
- обеспечивает обмен медиаданными между медиасервером и клиентами, а также их связь с центральным контроллером;
- обеспечивает связь системы «Умного дома», а также любых устройств пользователя (ноутбук, компьютер, КПК, мобильный телефон и проч.), с сетью Интернет;
- обеспечивает обмен данными между устройствами пользователя (ноутбук, компьютер, КПК и проч.) и подсистемами «Умного

дома» (Центральный контроллер, видеонаблюдение, медиасервер).

Система ЛВС обеспечивает как проводной, так и беспроводной (радио канал Wi-fi) способы подключения и обмена данными.

Система телефонной связи предназначена для:

- обеспечения проводной и/или беспроводной (стандарта DECT) телефонии;
- обеспечения проводной и/или беспроводной IP телефонии;
- обеспечения связи с домофоном и открывания электрического замка входной двери;
- распределения и переадресации входящих вызовов (в т.ч. и домофона);
- осуществления связи между абонентами внутренней телефонной сети.

3. Проводная и беспроводная системы «Умный дом»

Схема «Умного дома» базируется на трех элементах: кнопка управления, центральный элемент, управляемое оборудование [4].

Роль «кнопок» могут выполнять такие домашние устройства, как выключатели, Touch-панели, клавиатуры, пульты, iPad или iPhone. И даже собственный голос или хлопок ладони могут давать команды системе. За пределами дома можно управлять системой с помощью Интернет, мобильным телефоном, SMS и звонками на голосовое меню.

Центральный элемент (или контроллер «Умного дома») руководит компонентами и осуществляет контроль над всей системой. Он может быть подключен к компьютеру, получать приказы удаленно, по Интернет или посредством GSM порта (SMS сообщения). Для системы «Умный дом» контроллер – это сердце и мозг, самый главный элемент, основа интеллектуального электроснабжения.

В качестве исполнительного устройства может выступать любая домашняя техника, начиная от лампочки и заканчивая сложной охранной системой.

Программно-аппаратный комплекс интеллектуализации жилья имеет модульное строение. Взаимодействие модулей друг с другом, включая и связь с локальным концентратором – «мозгом» системы, осуществляется посредством определённых протоколов передачи данных. Одни протоколы приспособлены для проводных устройств, другие – для беспроводных, т.е. для передачи информации посредством радиосигналов. Соответственно классифицируются на беспроводные и проводные системы «Умный дом».

Некоторыми производителями разработаны и универсальные протоколы, позволяющие интегрировать в одну систему оба типа устройств. Это делает управление бытовыми функциями максимально пластичным. Например, беспроводными могут быть компоненты отдельных модулей (освещения, контроля климата и др.).

Следует отметить, что традиционно проводные (кабельные) системы считались наиболее надёжными. Однако «загрязнённость» силовых сетей рядового дома XXI века настолько высока, что требует применения «помехозащищённых» алгоритмов передачи информации по проводам. «Зашумлённость» радиодиапазона тоже существенна, но современные протоколы радиопередачи данных обеспечивают отличную стабильность функционирования беспроводных систем «Умный дом». А главное – внедрение проводной системы возможно только на этапе строительства здания и требует внесения её элементов в соответствующие проекты сетей. При завершённом же ремонте идеально подойдут беспроводные устройства.

4. Классификация систем по степени централизации и «открытости»

Респектабельные американские гиганты Crestron и AMX производят централизованные (сосредоточенные) системы домашней автоматизации, в которых все процессы контролируются одним центральным процессором [4]. С одной стороны, процессор испытывает значительные нагрузки, и выход его из строя приведет к глобальным последствиям (однако надёжность оборудования этих производителей превосходная). С другой стороны, степень интеграции всех функций максимально высока, что позволяет реализовывать сложнейшие сценарии функционирования бытового оборудования. Централизованные системы класса «люкс» славятся респектабельными интерфейсами и непревзойдёнными возможностями построения сложных мультимедийных взаимодействий.

Указанные американские производители оборудования «Умный дом» используют протоколы передачи данных с фирменной кодировкой, абсолютно помехоустойчивые, но не всегда позволяющие интегрировать в единую систему чужое оборудование, т.е. их протоколы/системы являются закрытыми. Стоит отметить, что под брендом AMX в последние годы выпускаются и системы с общедоступными, универсальными алгоритмами кодировки – открытыми протоколами. Открытые протоколы (KNX, C-Bus, LanDrive, LON, ZigBee, Wi-Fi и др.) хороши тем, что позволяют легко расширять системы за счёт разнородных элементов, вплоть до обычной бытовой техники, производители которой всё чаще предусматривают возможность её внедрения в систему «Умный дом». Однако проектировать и монтировать такие комплексы бывает нелегко из-за уникального набора компонентов, характер взаимодействия которых и помехозащищённость всей системы не всегда предсказуемы.

Использование производителем уникального (закрытого) протокола отнюдь не всегда означает, что в систему априори нельзя внедрить оборудование другой фирмы, просто нужно исключить вероятность конфликта при передаче данных. Некоторые производители предусматривают

возможность совмещения их оборудования с другими брендами посредством специфических шлюзов.

Децентрализованные (распределённые) системы «Умный дом» управляются посредством нескольких отдельно программируемых периферийных контроллеров, а не центрального процессора (хотя таковой иногда в систему включается) [4]. Распределение контроллеров может отличаться у разных линеек оборудования «Умный дом»: у одних оно зональное (все сети и оборудование одной комнаты или рабочей области контролируются одним локальным процессором), у других – функциональное (на каждый периферийный контроллер «завязана» отдельная инженерная сеть или функциональная группа приборов без соблюдения территориального принципа). В распределённых системах чуть ли не каждый элемент оснащён собственным микропроцессором, что позволяет им общаться друг с другом непосредственно, а не через центральный «мозг». Иерархичность систем варьирует, локальные контроллеры часто объединяются в сети более высокого уровня со своим концентратором. Но в любом случае, выход из строя части системы не приводит к коллапсу всех процессов в здании.

Выделяют три крупных международных платформы автоматизации, обеспечивающих функционирование распределённых систем по открытым протоколам: LonWorks, BacNe и KNX.

Особенно интересными и функциональными считаются решения, сочетающие оба типа систем – централизованную и распределённую – в единой инсталляции, поскольку каждая из них имеет свою специализацию и достоинства.

2 АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ

2.1. Система «Умный дом» глазами хакера

«Умный дом» защищен полностью только тогда, когда функционирует система управления. А ведь она, как и любая другая компьютерная программа, может быть подвержена опасности взлома или заражения вирусами. Особенно при удаленном управлении системой [5].

С точки зрения хакера система управления «Умным домом» - это просто несколько специфичная компьютерная программа, которую также можно взломать.

Автоматизированных домов становится все больше. Следовательно, можно ожидать и увеличения числа посягательств на них. Способы взлома и проникновения совершенствуются вслед за развитием систем защиты.

Предположим, что хакер получает доступ к системе управления автоматизированным домом. После того, как это сделано, у него есть несколько вариантов действий в зависимости от того, что является целью проникновения.

Он может взломать систему контроля доступа, отключить выборочно прибор или датчик, открыть электронные замки, отключить камеры, разбить окно и проникнуть в дом. Кроме того, хакер может отключить различные системы – например, пожарную сигнализацию и систему пожаротушения, сбить настройку системы отопления и т.д. И, наконец, хакер может просто стереть программу управления, после чего дом будет парализован. При большом желании злоумышленник может даже подделать или отключить уведомления о событиях в умном здании, если система предполагает удаленный мониторинг.

Для того чтобы взломать систему управления «Умного дома», нужно доподлинно знать: тип оборудования, выбор которого сегодня достаточно велик, способ управления и контроля за состоянием системы, программное

обеспечение, установленное в доме.

Ослабить или усилить защиту системы управления могут несколько факторов. Например, распространенность оборудования. Наиболее уязвимы системы, где в качестве контроллера выступает обычный компьютер. Современные контроллеры для управления зданием не используют обычный ПК. Все это осложняет задачу злоумышленников.

Нельзя также забывать об уязвимости программного обеспечения. Наиболее подвержены хакерским атакам программы в среде Windows. Операционные системы и утилиты, используемые в системах «Умный дом», как правило, имеют узкую специализацию и менее подвержены взлому. Более уязвима также система, которая имеет постоянную возможность удалённого управления через интернет в отличие от систем, где эта функция является временной/отключаемой [6].

Утечка информации может привести к более серьезным последствиям, нежели отсутствие защиты. Эта проблема имеет место, если доступ в дом имеет множество людей. Данная проблема успешно решается путем предоставления каждому пользователю своего уровня доступа. Лучше всего, когда управление системой безопасности доступно одному человеку, а остальные пользователи имеют допуск только к простым функциям «Умного дома».

При проникновении хакера в неподготовленную систему к вирусным атакам, он может стереть всю программу управления, и все системы «Умного дома» перестанут функционировать.

Взломать систему, которая отличается уникальной аппаратурой и программным обеспечением можно, получив информацию о взламываемой системе. Отсюда можно сделать вывод, что главная угроза вторжения – это получение информации о системе установки и проектирования.

Использование распространенных операционных систем и обычных ПК в системе управления зданием влечет за собой риск заразить компьютер. Но чем более специфичное оборудование и программное обеспечение

используется, тем сложнее это сделать, тем более что многие современные контролеры управления зданием – это весьма специализированные устройства со своей ОС и уникальной программой. Возможность создания вирусов для них очень мала.

На отсутствие вирусов для систем «Умного дома» влияют их малая распространенность, закрытость протоколов, а также незначительное число специалистов по оборудованию данных систем.

Наибольшей опасностью для вторжения в систему является пока человеческий фактор. То есть обычная халатность жильцов или недобросовестность проектировщиков. В техническом плане наиболее уязвимы системы под управлением Windows, но как уже говорилось, большинство современных систем автоматизированных зданий используют специфичное программное обеспечение и оборудование. Создание системы, которая будет обладать большими параметрами защиты, возможна. Все это будет определяться только потребностями конкретного проекта.

2.2 Уязвимости системы управления «Умный дом»

Вся система «Умного дома» состоит из множества составляющих, некоторые из них наиболее сильно нуждаются в защите. Одним из уязвимых элементов является обмен информацией между компьютером (сервером) и контроллером. Для того чтобы информация не попала в чужие руки, она осуществляется путем передачи по интернет-каналам в зашифрованном виде. Теоретически этого должно быть достаточно, чтобы исключить возможность утечки информации, однако большинство производителей оборудования для систем распределенной автоматики не предпринимают мер для защиты от сетевого компрометирующего воздействия. Ставка делается на «закрытость» протокола обмена, т.е. всего лишь на то, что язык протокола обмена знает исключительно узкий круг специалистов [7]. Следует отметить, что проблема необходимости контроля целостности измерительных и исполнительных

цепей точно так же актуальна и для децентрализованных систем тоже. Однако компрометация путем посылки ложной информации по сети передачи данных децентрализованной системы во много раз опаснее. Такая угроза называется «сетевым компрометирующим воздействием». Единственным методом борьбы с сетевым компрометирующим воздействием является аутентификация отправителя сообщения. Поддержка аутентификации может быть реализована либо на сеансовом уровне модели OSI/ISO, либо на уровне приложения. Так, например, когда один контроллер сети автоматике высылает другому пакет информации, суть содержания которого должна привести к некоторому критическому действию, второй контроллер «желает» удостовериться в «личности» отправителя. В качестве доказательства полномочий отправителя (аутентичности) используется либо цифровая подпись, либо механизм «запрос–ответ», где в запросе высылается некое случайное число (фраза), а в качестве ответа используется число (фраза), зашифрованная на ключе, известном только этим двум контроллерам.

2.3 Анализ угроз

Угроза – это потенциально возможно событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза. Под угрозой автоматизированной системе понимается возможность реализации воздействия на информацию, обрабатываемую в автоматизированной системе, приводящего к нарушению конфиденциальности, целостности или доступности этой информации [8].

Под конфиденциальностью информации понимается невозможность утечки конфиденциальной информации организаций (лиц), эксплуатирующих «Умный дом», через его подсистемы (например, через телекоммуникационную сеть).

Под доступностью информации понимается такое состояние системы, при котором легальные пользователи (и сама система), используя элементы «Умного дома», могут реализовывать разрешенные в системе действия (включать кондиционирование или систему пожаротушения, открывать двери, 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 понимается 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.).

Анализ угроз приведенный в таблице 2.1 поможет определить какие угрозы на систему являются самыми опасными.

Таблица 2.1 – Анализ угроз и уязвимостей

№	Угрозы	Уязвимости	Возможные последствия
1	2	3	4
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	Нарушение конфиденциальности, целостности и доступности информации (КИД)
2	Влияние вирусных и троянских программ на	Подключение сети «Умного дома» к Интернет	Сбои в ПО системы, а следовательно

Продолжение таблицы 2.1 – Анализ угроз и уязвимостей

1	2	3	4
	работу системы		нарушение работы либо вывод из строя аппаратуры системы. Нарушение КИД информации, находящейся внутри сети
3	Перехват информации, передаваемой по проводным и беспроводным каналам связи	Возможность доступа злоумышленника к проводным каналам сети. Отсутствие (неэффективность) механизмов защиты трафика	Нарушение конфиденциальности информации, передаваемой по каналу. Возможен захват управления системой
4	Ошибки пользователя	Отсутствие (неэффективность) механизмов защиты системы от неправильных действий пользователей	Нарушение КИД информации. Возможны сбои в системе из-за неправильного использования оборудования
5	Кража (злоумышленный вывод из строя аппаратуры) системы «Умного дома»	Отсутствие (неэффективность) физической охраны объекта	Нарушение КИД информации

6	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 КЦД информации, обрабатываемой на компьютере
7	Утечка информации по	Наличие акустоэлектрических	Нарушение

Продолжение таблицы 2.1 – Анализ угроз и уязвимостей

1	2	3	4
	акустоэлектрическому каналу	преобразователей (датчики охранной, пожарной сигнализации и т.д.), подключенных к проводным линиям	целостности и конфиденциальности информации
8	Сетевое компрометирующее воздействие	Недостаточная защита протоколов, а также слабая процедура авторизации и идентификации пользователей	Нарушение целостности и конфиденциальности информации
9	Перебои в сети электропитания	Отсутствие системы автономного электропитания	Дезорганизация работы системы
10	Ошибки программного обеспечения	Использование нелегального ПО, низкая квалификация персонала, отсутствие (неэффективность) тестирования закупаемого ПО	Нарушение КИД информации

Данные таблицы 2.1, позволяют наглядно видеть наиболее распространенные угрозы и уязвимости, а также возможные последствия в случае пренебрежения средствами защиты.

3. РАЗРАБОТКА МОДЕЛИ УЯЗВИМОСТЕЙ СИСТЕМЫ ЗАЩИТЫ «УМНОГО ДОМА»

3.1. Модель нарушителя

Методы действий, применяемые злоумышленником, кардинально зависят от типа системы автоматизации. Системы автоматики делятся на централизованные и децентрализованные.

Централизованный метод реализации технологии «Умный дом» по своей сути представляет собой объединение разнообразных датчиков и контролеров в единую сложную телекоммуникационную сеть с центральным контроллером [9]. В роли центрального контроллера может применяться сервер, в качестве которого используется любой современный компьютер, и программное обеспечение с поддержкой необходимого программного софта и протоколов. В названии отражена главная суть подхода — к центральному контроллеру системы подключены все основные и вспомогательные блоки, при этом все компоненты оснащены собственными микроконтроллерами, но взаимодействуют они исключительно при помощи центрального контроллера.

В таком случае злоумышленник либо должен внедриться во внутренние цепи процессорного узла, либо подключается к измерительным или исполнительным цепям. Стоит отметить, что многие из протоколов, используемых для управления объектами, являются уязвимыми по своей сути, а многие другие, как правило, будучи использованными для построения подсистем, зачастую при неправильной интеграции приводят к появлению уязвимостей. Если говорить о первом виде программного обеспечения, то есть о программном обеспечении, отвечающем за функционирование самой сети «Умного дома», то это программное обеспечение, работающее на низком уровне и отвечающее за передачу управляющих датаграмм по витой паре или импульсов по силовой линии непосредственно от устройства к устройству или от сервера к устройствам и обратно. Во втором случае бороться с злоумышленником можно, контролируя целостность измерительных и исполнительных цепей.

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 [9]. 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.

Модель (образ) нарушителя представляет собой его комплексную характеристику, отражающую его возможное психологическое состояние, уровень физической и технической подготовленности, осведомленности, которая позволяет оценить степень его способности в практической реализации проникновения.

Основная задача нарушителя безопасности системы «Умный дом» состоит, как правило, в реализации НСД к информационным или аппаратным ресурсам, системы и «обходе» средств защиты. Модель угроз представляет собой перечень возможных способов достижения цели нарушителя, сценариев наиболее вероятных его действий при несанкционированном проникновении.

Рассмотрим, кто может являться нарушителем безопасности системы «Умный дом».

Внутренними нарушителями (осуществляют атаки, находясь в пределах контролируемой зоны), могут быть:

- легальные пользователи «Умного дома», не имеющие полномочий административного управления;
- легальные пользователи «Умного дома», имеющие полномочия административного управления (разработчики (сопровождающие) «Умного дома», владелец).

Внешними нарушителями (осуществляют атаки из-за пределов контролируемой зоны), могут быть:

- сотрудники предприятий – поставщиков решений «Умного дома»;
- посторонние лица, пытающиеся получить доступ к системе случайным образом (например, конфликт настроек оборудования у соседа

и помехи по передающим каналам в результате легального пользователя соседом техникой);

– представители преступных организаций.

Анализируя угрозы, которые были определены в таблице 2.1 видно, что злоумышленник может преследовать различные цели, поэтому и модель его действий в каждом случае будет разной.

Мотивы:

- а) корыстный интерес;
- б) идейные соображения;
- в) самоутверждение;
- г) месть;
- д) вандализм;
- е) принуждение.

Основные направления реализации угроз:

- а) непосредственное обращение к системе через интернет;
- б) внедрение в проводные и беспроводные линии, для перехвата информации;
- в) модификация средств защиты, позволяющая реализовать угрозы ИБ;
- г) внедрение в технические средства программных или технических механизмов.

Для осуществления доступа к ресурсам системы «Умный дом» нарушитель может использовать следующие каналы атак:

- физический доступ к программно-аппаратным средствам системы, кража оборудования;
- хакерскими атаками через сеть интернет на сервер;
- канал утечки за счет ПЭМИН;
- получение доступа в сеть системы путем использования уязвимостей протоколов сетевого взаимодействия;
- несанкционированное отключение средств защиты.

Построенная модель действий нарушителей показала, что система имеет ряд уязвимостей, через которые могут быть реализованные выше перечисленные угрозы.

Наиболее уязвимым местом в системе «Умного дома», которым наверняка воспользуются злоумышленники, является его подключение к сети Интернет. Большинство таких систем постоянно подключены к сети Интернет для того, чтобы иметь возможность следить за состоянием дома удаленно. Опытный хакер сможет получить доступ к серверу «Умного дома», обойдя межсетевой экран [10].

Даже в самой защищенной системе можно найти слабое место. «Умный дом» состоит из сервера и множества сенсоров. Очень часто эти сенсоры подключены к серверу посредством Wi-fi сети или Bluetooth соединений, такое подключение гораздо удобнее, ведь в этом случае не требуется прокладывать провода. Это и является основным слабым местом, ведь Wi-fi соединения уязвимы, а их протоколы шифрования можно взломать даже без использования специальных устройств. Отметим также, что подключение по беспроводным каналам характерно не только для сенсоров, но и для автоматического освещения, термостата, кондиционера, существуют даже дверные замки, управляемые по Bluetooth.

Чем может быть опасен взлом такой системы? Во-первых, злоумышленник может получить контроль над всеми системами «Умного дома», если установлен беспроводной замок на входной двери – его можно будет открыть, а приложив массу усилий можно спровоцировать возгорание. Также если в этой сети установлены видеорекамеры – злоумышленник сможет получать всю информацию, которую они передают на сервер.

Чтобы обезопасить свой дом от любых попыток взлома. Во-первых, желательно избежать беспроводных подключений между основными модулями системы. Во-вторых, использовать только временные подключения к сети Интернет, это поможет избежать не только целенаправленных атак, но также снизит риск проникновения вредоносных программ на сервер. Если

беспроводные подключения используются в «Умном доме» - необходимы глушилки Wi-fi/Bluetooth в местах, где беспроводная сеть выходит за пределы дома или офиса.

3.2. Модель уязвимостей

Исходя из вероятных угроз, построим двухдольный граф уязвимостей и средств и механизмов защиты [8].

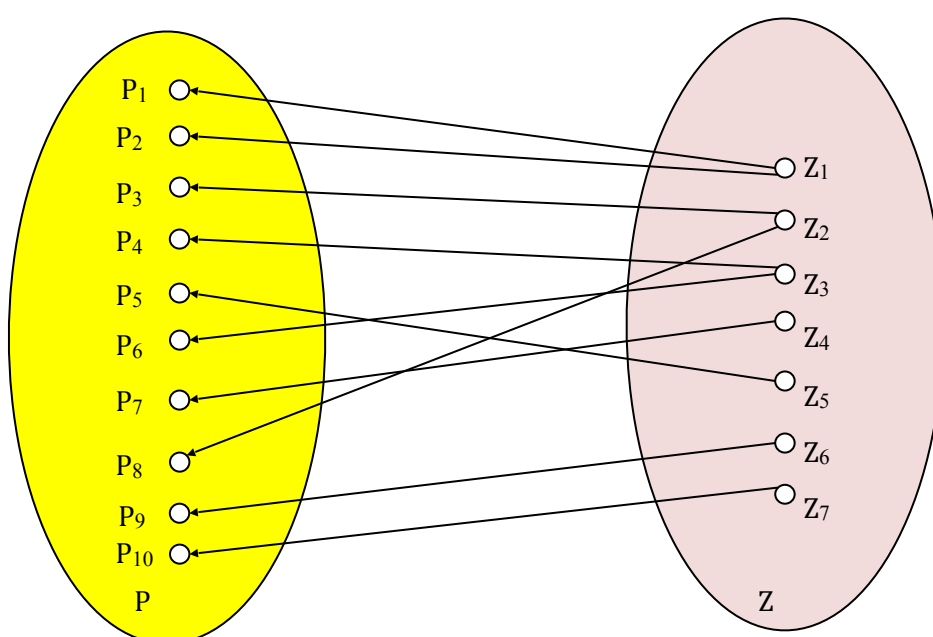


Рисунок 3.1 - Двухдольный граф уязвимостей и средств и механизмов защиты

Множество уязвимостей P :

- P_1 – отсутствие (неэффективность) механизмов защиты периметра сети;
- P_2 – подключение системы к сети интернет;
- P_3 – отсутствие (неэффективность) механизмов защиты трафика;
- P_4 – отсутствие (неэффективность) механизмов защиты системы от неправильных действий пользователей;
- P_5 – отсутствие (неэффективность) физической охраны объекта;

- P_6 – выход проводников, в которых могут быть наводки излучений, за пределы контролируемой зоны;
- P_7 – наличие акустоэлектрических преобразователей (датчики охранной, пожарной сигнализации и т.д.), подключенных к проводным линиям;
- P_8 – недостаточная защита протоколов передачи, а также слабая процедура авторизации и идентификации пользователей;
- P_9 – отсутствие системы автономного электропитания;
- P_{10} – использование нелегального ПО, низкая квалификация персонала, отсутствие тестирования закупаемого ПО.

Множество средств и механизмов защиты Z :

- Z_1 – совершенствование защиты сети (межсетевые экраны, фаерволы, антивирусы), усложнение процедуры аутентификации пользователя в сеть при удаленном доступе, хранение в аппаратных модулях безопасности;
- Z_2 – защита каналов и протоколов передачи информации, путем усложнения протоколов (запрос/ответ);
- Z_3 – правильная установка системы специалистами в пределах контролируемой зоны;
- Z_4 – защита проводных линий;
- Z_5 – сигнализация, видеокамеры, имитация присутствия;
- Z_6 – наличие автономного источника электропитания;
- Z_7 – использование лицензированного ПО, квалифицированные специалисты.

Полученная модель уязвимостей показывает, что система не идеальна и угрозы, воздействующие на нее, могут нанести ущерб системе и пользователю.

3.3. Оценка риска выделенных угроз и уязвимостей «Умного дома»

После определения угроз и уязвимостей необходимо оценить

вероятность их объединения и возникновения риска.

Оценка вероятности угроз должна учитывать природу угроз и особенности, присущие различным группам угроз [11].

1. Преднамеренные угрозы. Вероятность преднамеренных угроз зависит от мотивации, знаний, компетенции и ресурсов, доступных потенциальному злоумышленнику, а также от привлекательности активов для реализации атак.

2. Случайные угрозы. Вероятность случайных угроз может оцениваться с использованием статистики и опыта.

Вероятность таких угроз может зависеть от близости организации к источникам опасности, таким как автомагистрали и железнодорожные пути, а также заводы, имеющие дело с опасными материалами, химическими веществами или бензином. Также географическое положение организации оказывает влияние на возможность возникновения экстремальных погодных условий. Вероятность человеческих ошибок (одна из наиболее распространенных случайных угроз) и поломки оборудования также должны быть оценены.

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 [9].

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:

1. Высокое влияние на систему (ВВ) – влияние на конфиденциальность, целостность и доступность элементов системы

может причинить организации (владельцам) значительный или катастрофический ущерб.

2. 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).

3. 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. Вероятна реализация одной 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.

Уязвимости, так же, как и угрозы, могут быть оценены по трехуровневой качественной шкале. Значение уровня уязвимости показывает, насколько вероятно успешное осуществление угрозы с использованием данной уязвимости в случае, если эта угроза будет реализовываться. Соответствующие качественные уровни уязвимости могут быть определены, например, следующим образом:

1. В – вероятно. Уязвимость легко использовать, и существует слабая защита или защита вообще отсутствует.

2. С – возможно. Уязвимость может быть использована, но существует определенная защита.

3. Н – маловероятно. Уязвимость сложно использовать, и существует хорошая защита.

Уровень риска для выделенных угроз и уязвимостей «Умного дома» представлен в таблице 3.1.

Таблица 3.1 – Уровень риска для выделенных угроз и уязвимостей «Умного дома»

№	Угрозы	Уязвимости	Вероятность угроз	Уровень уязвимости	Класс актива	Уровень риска
1	2	3	4	5	6	7
1	Хакерские атаки на центральный сервер	Слабые пароли, отсутствие парольной политики, отсутствие системы обнаружения вторжений	Высокая	С	ВВ	Высокий
2	Влияние вирусных и троянских программ на работу системы	Отсутствие механизмов защиты системы от неправильных действий пользователя	Высокая	С	ВВ	Высокий

Продолжение таблицы 3.1 – Уровень риска для выделенных угроз и уязвимостей «Умного дома»

1	2	3	4	5	6	7
3	Перехват информации, передаваемой по проводным и беспроводным каналам связи	Возможность доступа злоумышленника к проводным каналам сети. Отсутствие механизмов защиты трафика	Высокая	С	ВВ	Высокий
4	Ошибки пользователя	Неэффективность механизмов защиты системы от неправильных действий пользователей	Высокая	В	НВ	Средний
5	Кража (злоумышленный вывод из строя аппаратуры) системы «Умного дома»	Неэффективность физической охраны объекта	Средняя	Н	СВ НВ	Средний
6	Утечка информации через побочные электромагнитные излучения и наводки (ПЭМИН)	Наличие ПЭМИН компьютерной техники. Выход проводников, в которых могут быть наводки излучений, за пределы контролируемой зоны	Средняя	С	СВ	Средний

Продолжение таблицы 3.1 – Уровень риска для выделенных угроз и уязвимостей «Умного дома»

1	2	3	4	5	6	7
7	Утечка информации по акустоэлектрическому каналу	Наличие акустоэлектрических преобразователей (датчики охранной, пожарной сигнализации и т.д.), подключенных к проводным линиям	Средняя	С	СВ	Средний
8	Сетевое компрометирующее воздействие	Недостаточная защита протоколов, слабая процедура авторизации и идентификации	Средняя	С	СВ	Средний
9	Перебои в сети электропитания	Отсутствие системы автономного электропитания	Низкая (если есть автономный источник электропитания) Высокая (если автономного электропитания нет)	Н В	ВВ	Средний Высокий

10	Ошибки программного обеспечения	Использование нелегального ПО, низкая квалификация персонала	Средняя Высокая	С	ВВ	Высокий
----	---------------------------------	--	--------------------	---	----	---------

Исходя из результатов оценки уровней риска для выделенных угроз и уязвимостей, самыми опасными являются те угрозы, при которых злоумышленник может получить контроль над всей системой «Умного дома». Таковыми угрозами являются:

1. Хакерские атаки на центральный сервер.
2. Влияние вирусных и троянских программ на работу системы.
3. Ошибки программного обеспечения.
4. Перехват информации, передаваемой по проводным и беспроводным каналам связи.

Реализация данных угроз может привести к катастрофическим последствиям для всей системы.

3.4.CUJO – система защиты для «Умного дома»

Проанализировав возможные угрозы и уязвимости системы «Умный дом», а также проведя оценку уровней риска для выделенных угроз и уязвимостей, был сделан вывод, что реализация данных угроз может привести к серьезным последствиям для всей системы.

Для того чтобы защитить «Умный» дом от несанкционированного доступа, предлагается использовать новейшую разработку группы калифорнийских исследователей – специальное устройство под названием CUJO.

CUJO представляет собой небольшой блок, который подсоединяется к домашней сети Wi-Fi и отслеживает любую подозрительную активность в сети [12]. Компактное изобретение применяет алгоритм машинного обучения, которое позволяет различать систематическую активность «умных» устройств от возможной угрозы. CUJO информирует пользователя о несанкционированном доступе посредством приложения для устройств на базе Android и iOS. Также устройство отображает текущие статусы

подключения, отправляет предупреждение и позволяет дистанционно контролировать соединения.

Данное изобретение использует многослойный подход при обеспечении безопасности. CUJO сочетает в себе брандмауэр (межсетевой экран), антивирус и фильтр [13]. Его основное отличие от традиционных программных решений заключается в том, что входящий трафик анализируется ещё до попадания на компьютер, то есть до того, как смогут нанести ущерб.

В устройстве есть два разъёма Ethernet – входной и выходной. Входящие пакеты подвергаются анализу не только путём сверки с общеизвестными вредоносными программами, но и по своим уникальным методикам, которые анализируют поведенческие данные в облаке CUJO. Несомненно, часть данных передастся по зашифрованному каналу на облако, но от этого нам не избавиться. И уже после всех этих действий пакеты направляются на выходной разъём. К выходному разъёму Ethernet можно подключить роутер и раздавать почищенную уже безопасную информацию на все подключенные устройства. Схема работы CUJO выглядит так:



Рисунок 3.1 – Схема работы CUJO

CUJO будет всегда устанавливать нужные нам обновления, не останавливая свою работу. Данное устройство обладает такими техническими характеристиками [13]:

- двоядерный процессор Cavium с тактовой частотой 1 ГГц;
- оперативная статическая память – 2 Гб;
- два Ethernet-порта на 1 Гб каждый.

4 ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ МАГИСТЕРСКОЙ РАБОТЫ

4.1 Планирование разработки модели уязвимостей системы защиты в объектах типа «Умный дом»

Планирование разработки модели уязвимостей системы защиты в объектах типа «Умный дом» наглядно иллюстрируется с помощью метода сетевого планирования и управления (СПУ).

Система СПУ включает в себя [14]:

- составление перечня этапов и определение продолжительности выполнения работ;
- построение сетевого графика;
- расчет основных параметров сетевого графика.

Весь комплекс разработки подразделяется на этапы. По каждому из этапов рассчитывается трудоемкость, исполнители и продолжительность работ.

Для определения трудоемкости используется вероятностная оценка времени выполнения работ.

Ожидаемое время выполнения этапа определяется по формуле:

$$t_{\text{ож}} = \frac{3 \cdot t_{\text{min}} + 2 \cdot t_{\text{max}}}{5}, \quad (4.1)$$

где t_{min} – минимально необходимое время на выполнение этапа работ при наиболее благоприятных условиях, дней;

t_{max} – максимальные затраты времени на выполнение работы по данному этапу при неблагоприятных условиях, дней.

Степень правильности определения $t_{\text{ож}}$ проверяется расчетом дисперсии (разброса между минимальной и максимальной оценками времени). Дисперсия определяется по формуле:

$$\sigma^2(t) = \left(\frac{t_{max}-t_{min}}{5}\right)^2 \quad (4.2)$$

Если дисперсия меньше или равна 1, то временные оценки работ считаются выбранными корректно, что говорит о малой степени неопределенности в значениях максимальной и минимальной продолжительности работ.

Результаты расчета приведены в таблице 4.1.

Таблица 4.1 – Продолжительность этапов работ

Этапы проектирования	Временные оценки			Дисперсия	Исполнители		Продолж., дни
	t_{min}	t_{max}	$t_{ож}$		Специалист	Кол-во	
Составление и утверждение ТЗ	1	3	2	0,16	консультант инженер	1 1	2
Обзор литературных источников	2	4	3	0,16	инженер	1	3
Анализ системы «Умный дом»	4	5	5	0,04	инженер	1	5
Анализ угроз и уязвимостей	4	5	5	0,04	инженер	1	5
Модель действий нарушителя	4	5	5	0,04	инженер	1	5
Разработка модели уязвимостей системы защиты «Умного дома»	10	12	11	0,16	инженер	1	11
Оценка риска выделенных угроз и уязвимостей	5	6	6	0,04	инженер	1	6
Методы борьбы с уязвимостями	4	5	5	0,04	инженер	1	5
Экономическое обоснование	4	5	5	0,04	экономист	1	5

Разработка мер по охране труда	4	5	5	0,04	инженер	1	5
Выводы	2	3	3	0,04	инженер	1	3
Оформление графической части	7	9	8	0,16	инженер	1	8

Продолжение таблицы 4.1 – Продолжительность этапов работ

Этапы проектирования	Временные оценки			Дисперсия	Исполнители		Продолж., дни
	t_{min}	t_{max}	$t_{ож}$		Специалист	Кол-во	
Оформление отчета	2	3	3	0,04	консультант инженер	1 1	3
Итого	53	70	66	100	-	3	66

4.2 Построение сетевого графика

Сетевой график представляет собой информационно - динамическую модель, в которой изображаются взаимосвязи и результаты всех работ, необходимых для достижения поставленной цели проектирования [14].

Таблица 4.2—Перечень работ сетевого графика

№	Наименования работы	Код работы	Продолж., дни
1	Составление и утверждение ТЗ	0-1	2
2	Обзор литературных источников	1-2	3
3	Анализ системы «Умный дом»	2-3	5
4	Анализ угроз и уязвимостей	3-4	5
5	Модель действий нарушителя	3-5	5
6	Разработка модели уязвимостей системы защиты «Умного дома»	4-6	11
7	Оценка риска выделенных угроз и уязвимостей	5-6	6
8	Методы борьбы с уязвимостями	6-7	5

9	Экономическое обоснование	7-8	5
10	Разработка мер по охране труда	8-9	5
11	Выводы	9-10	3
12	Оформление графической части	10-11	8
13	Оформление отчета	11-12	3
Итого			66

При построении сетевого графика используются два графических элемента: работы и события.

Работа - это процесс, требующий затрат времени, наличия исполнителей и материальных ресурсов. Событиями называются результаты проведенных работ, на графике события показываются кружками с номером. Сетевой график строится по данным таблиц 4.1, 4.2 и представлен на рисунке 4.1.

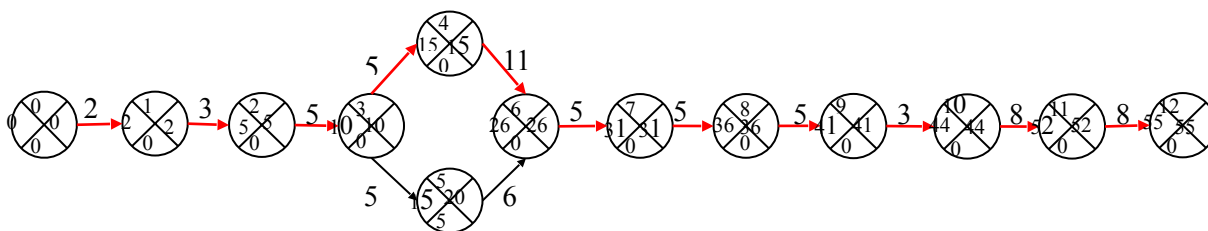


Рисунок 4.1- Сетевой график плана выполнения работ

4.3 Расчет параметров сетевого графика

Параметры работ и путей приведены в таблицах 4.3, 4.4 соответственно.

Таблица 4.3 – Параметры работ сетевого графика

Код работы	t_{ij}	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$	$R_{п}$	$R_{св}$
0 – 1	2	0	0	2	2	0	0
1 – 2	3	2	2	5	5	0	0
2 – 3	5	5	5	10	10	0	0
3 – 4	5	10	10	15	15	0	0

3 – 5	5	10	15	15	20	5	0
4 – 6	11	15	15	26	26	0	0
5 – 6	6	15	20	21	26	5	0
6 – 7	5	26	26	31	31	0	0
7 – 8	5	31	31	36	36	0	0
8 – 9	5	36	36	41	41	0	0
9 – 10	3	41	41	44	44	0	0
10 – 11	8	44	44	52	52	0	0
11 – 12	3	52	52	55	55	0	0

Таблица 4.4 – Параметры путей сетевого графика

№	№ событий	Продолжительность работ	L_i	Резерв в t_i	K_{ni}
1	0-1-2-3-4-6-7-8-9-10-11-12	2-3-5-5-11-5-5-3-8-3	55	0	1
2	0-1-2-3-5-6-7-8-9-10-11-12	2-3-5-5-6-5-5-5-3-8-3	50	5	0,69

В таблицах использованы следующие обозначения:

t_{ij} – время выполнения работы;

$T_{p.n. ij}$ – ранний срок начала работы;

$T_{п.н. ij}$ – поздний срок начала работы;

$T_{p.o. ij}$ – ранний срок окончания работы;

$T_{п.о. ij}$ – поздний срок окончания работы;

$R_{п. ij}$ – полный резерв времени работы;

$R_{с. ij}$ – свободный резерв времени работы;

L_i – длина i -го пути;

Δt_i – резерв времени i -го пути;

$L'_{кр}$ – общая часть i -го и критического пути;

$K_{н. i}$ – коэффициент напряженности i -го пути.

Коэффициент напряженности i -го пути определяется по формуле:

$$K_{н.і} = \frac{L_i - L'_{кр}}{L_{кр} - L'_{кр}} \quad (4.3)$$

где $L_{кр}$ – длина критического пути.

Таким образом, построен график событий, сетевой график, таблица списка работ, найден критический путь. Им является путь 0-1-2-3-4-6-7-8-9-10-11-12 имеющий длину 55 дней. При последовательном выполнении этих же работ продолжительность составила бы 66 дней. Отсюда видно, что имеет смысл выполнять работы по сетевому графику, т.к. наблюдается сокращение срока выполнения на 11 дней.

4.4. Определение затрат на разработку и проектирование

4.4.1 Расчет основной заработной платы

Затраты по этой статье состоят из планового фонда зарплаты всех категорий работников, занятых разработкой проекта.

Расчет зарплаты ведется на основании данных таблицы 4.1 и 4.2.

Расчет приводится в таблице 4.5.

Таблица 4.5 – Расчет основной заработной платы

Должность исполнителя	Количество, чел.	Месячный оклад, грн.	Средне-дневная зарплата, грн.	Кол-во дней работы	Сумма зарплаты, грн.
Консультант	1	5000	227,27	5	1136,35
Инженер	1	4500	204,54	55	11249,7

Экономист	1	4800	218,18	5	1090,90
Итого	3	-	-	-	13476,95

4.4.2 Отчисления на социальное страхование и другие фонды

Эти отчисления определяются в процентном отношении к сумме основной и дополнительной зарплаты в соответствии с установленным нормативом 22% и составляют:

$$ЗП_{\text{осн}} \cdot 0,22 = 13476,95 \cdot 0,22 = 2964,93 \text{ грн}$$

4.4.3 Определение затрат на материалы и комплектующие

В эту статью включается стоимость основных и вспомогательных материалов (бумага, носители информации, картридж и т.д.), покупных полуфабрикатов и комплектующих изделий, необходимых для разработки проекта [14]. Расчет приводится в табл. 4.6.

Транспортно-заготовительные расходы принимаются равными 5% от стоимости материалов.

Таблица 4.6 – Затраты на материалы

Наименование материала	Кол-во	Цена за единицу, грн/шт.	Общая стоимость, грн.
Бумага для принтера, уп.	1	60	60
Flash-диск на 4Gb, шт.	2	95	190
Картридж для принтера, шт	1	180	180
Канцтовары, набор	1	70	70
Итого	-		500
Транспортно-заготовительные расходы			25
Всего с учетом транспортно – заготовительных расходов			525

4.4.4 Затраты на специальное оборудование

В эту статью включены расходы на приобретение, транспортировку, монтаж и отладку оборудования.

Также сюда входят затраты на оплату времени работы оборудования, которые определяются по формуле:

$$C_{\text{мо}} = P_{\text{э}} \cdot t_{\text{м}}, \quad (4.4)$$

где $C_{\text{мо}}$ – затраты на оплату времени работы оборудования, грн.,

$P_{\text{э}}$ – эксплуатационные расходы на один час рабочего времени оборудования, грн./час,

$t_{\text{м}}$ – время, требующееся для проектирования, час.

Оборудование требуется для выполнения работ продолжительностью 55 дней. Умножив на длительность рабочего дня (8ч.) получим время работы компьютера $66 \cdot 8 = 440$ ч. Принтер в общей сложности был задействован 8 часов. Эксплуатационные расходы на один час рабочего времени оборудования определяются по смете расходов на содержание и эксплуатацию оборудования (таблица 4.8) и годовому эффективному фонду времени ($\Phi_{\text{эф}} = 1800$ ч. при односменной работе).

Амортизационные отчисления определяют по формуле:

$$A = \frac{\Phi_{\text{б}} \cdot N \cdot H_{\text{а}}}{100\%} \quad (4.5)$$

где $\Phi_{\text{б}}$ - балансовая стоимость вычислительной техники, грн;

N - количество ПК;

$H_{\text{а}}$ - норма амортизационных отчислений на полное восстановление вычислительной техники, % ($H_{\text{а}} = 50\%$).

Подставив в формулу значения балансовой стоимости используемого

компьютера ПК ARTLINE Home H43v05/ AMD Athlon x4 840(3.1 ГГц)/ RAM 8 Gb / HDD 1 Tb, монитор LG Flatron LG 27MP68VQ-P (которая определяется как стоимость компьютера 8399грн. и монитора 7141грн., плюс 5% транспортные расходы и составляет 16317грн.), многофункциональное устройство Epson L364 (стоимость – 5189грн. и 5% транспортные расходы составят 5448,45грн.) и нормы амортизационных отчислений 50%, получим:

$$A=(16317+5448,45) \cdot 0,5=10882,73 \text{ грн.}$$

Затраты на электроэнергию рассчитываются по формуле:

$$E_{el} = \sum_{i=1}^m H_e \cdot C'_e \cdot \Phi_{эф, час} \cdot \text{Цена, грн.} \quad (4.6)$$

где H_e – норма затрат энергии на единицу оборудования, которое использует данный вид энергоресурсов за единицу времени;

C'_e – стоимость единицы данного вида энергоресурса, грн.;

m – количество единиц оборудования, которое использует данный вид энергии.

Таблица 4.7 – Расчет стоимости энергоресурсов

Оборудование	Вид энергоресурса	Норма затрат, кВт/час.	$\Phi_{эф, час}$	Цена, грн.	Стоимость энергоресурсов, грн.
Компьютер	электроэнергия	0,4	528	1,1	232,32
Принтер	электроэнергия	0,2	8	1,1	1,76

Итого	-	-	536	-	234,08
-------	---	---	-----	---	--------

Расходы на текущий ремонт оборудования принимаются равными 5% от балансовой стоимости оборудования и составляют 321 грн.

Прочие расходы принимаются равными 5% от суммы всех предыдущих статей расходов на содержание и эксплуатацию оборудования и составляют 188,27 грн.

Смета расходов на содержание и эксплуатацию оборудования представлена в таблице 4.8.

Таблица 4.8 – Смета расходов на содержание и эксплуатацию оборудования

Статья расходов	Сумма, грн
Амортизация оборудования	10882,73
Эксплуатация оборудования	234,08
Текущий ремонт оборудования	321
Прочие расходы	188,27
Итого	11626,1

Разделив итоговое значение таблицы 4.8 на фонд времени 1800ч. получим эксплуатационные расходы на 1 час машинного времени:

$$P_э = 11626,1 / 1800 = 6,5 \text{ грн./ч.};$$

А за все время разработки:

$$C_{мо} = 440 \cdot 6,5 = 2860 \text{ грн.}$$

4.4.5 Накладные расходы

К накладным расходам относятся затраты на общее управление и

общехозяйственные нужды, содержание и эксплуатацию зданий. Накладные расходы принимаются равными 60% от основной заработной платы производственного персонала [14]:

$$C_{\text{нр}} = 13476,95 \cdot 0,6 = 8086,17 \text{ (грн)}.$$

Результаты калькуляционных расчётов приведены в таблице 4.9

Таблица 4.9 – Калькуляция сметной стоимости разработки проекта

Статья калькуляции	Сумма, грн	Удельный вес к итогу, %
Основные материалы	525	1,9
Общая заработная плата	13476,95	48,3
Накладные расходы	8086,17	29
Отчисления на социальное страхование	2964,93	10,6
Расходы на оплату машинного времени	2860	10,2
Итого	27913,05	100

4.5 Оценка экономической эффективности от реализации магистерской работы

Маркетинговые исследования, проектные разработки, прямой подсчет экономической эффективности по которым не представляется возможным, оценивают с помощью балльной системы [14].

Балльная оценка проводится по следующим важнейшим показателям:

- важность разработки K_1 ;
- возможность использования результатов разработки K_2 ;
- теоретическая значимость и степень новизны исследования K_3 ;
- сложность разработки K_4 .

Таблица 4.10 - Шкала для оценки важности разработки K_1

№ п/п	Показатель	Баллы
1	Инициативная работа, не является частью комплексной программы, или задачей ведомственных органов	1
2	Работа, выполняемая по договору о научно-технической помощи	3
3	Работа представляет часть ведомственной программы	5
4	Работа представляет часть ведомственной комплексной программы	7
5	Работа представляет часть международной комплексной программы	8

Таблица 4.11 - Шкала оценки возможности использования результатов разработки К₂

№ п/ п	Показатель	Баллы
1	В данном подразделении	1
2	В данной организации	3
3	Во многих организациях	5
4	В масштабах страны	8

Таблица 4.12 - Шкала оценки теоретической значимости и уровня новизны исследования К₃

№ п/п	Показатель	Баллы
1	Анализ, обобщение и классификация известной информации. Подобные результаты были известны в исследуемой области	2
2	Получение новой информации, дополняющей знания о сущности изучаемых процессов, не известных в исследуемой области	3
3	Получение новой информации, меняет представление о сущности изучаемых процессов, не известных ранее	5
4	Создание новых теорий, методик	6

5	Получение информации, способствующей формированию направлений, неизвестных ранее	8
---	--	---

Таблица 4.13 - Шкала оценки показателей сложности исследования К₄

№ п/п	Показатель	Баллы
1	Работа выполняется одним подразделением, расходы менее 10000 грн.	1
2	Работа выполняется одним подразделением, расходы 10000-50000 грн.	3
3	Работа выполняется одним подразделением, расходы 50000-100000 грн.	5
4	Работа выполняется с участием многих подразделений, расходы 100000-500000 грн.	7
5	Работа выполняется несколькими организациями, расходы более 500000 грн.	8

Выбираем значения коэффициентов К₁, К₂, К₃, К₄ в соответствии с таблицами.

К₁ – 1 балл (инициативная работа, не является частью комплексной программы, или задачей ведомственных органов)

К₂ – 5 баллов (возможность использования результатов разработки во многих организациях).

К₃ – 3 балла (получение новой информации, дополняющей знания о сущности изучаемых процессов, не известных в исследуемой области)

К₄ – 3 балла (работа выполняется одним подразделением, расходы 10000-50000 грн.).

Общая оценка находится как произведение коэффициентов:

$$P_c = K_1 \cdot K_2 \cdot K_3 \cdot K_4$$

$$P_c = 45 \text{ баллов}$$

Удельный эффект на каждый балл - 5000 грн.

Общий эффект от разработки составляет:

$$E = P_c \cdot 5000$$

$$E = 225000 \text{ грн}$$

Экономическая эффективность от реализации дипломной работы определяется с помощью коэффициента эффективности, характеризующий долю общего эффекта от разработки, который приходится на одну грн. затрат (себестоимости). Находим коэффициент эффективности по формуле (4.7):

$$K_{\text{э}} = E / K_{\text{н и р}} \quad (4.7)$$

$$K_{\text{э}} = 225000 / 20910,68 = 10,76$$

Так как $K \geq 1$, то разрабатываемый проект является эффективным.

В ходе работы было произведено экономическое обоснование в разработке модели уязвимостей системы защиты «Умных домов». Сетевой график, был найден и рассчитан критический путь выполнения работ. Он составил 55 дней, что не превышает установленного срока на исследование данной работы. Выполнив расчет сметы расходов на реализацию дипломной работы, которая включает в себя: стоимость материалов, спецоборудования, заработную плату сотрудников, отчисления на социальное страхование и накладные расходы, а также с использованием балльной системы оценки была рассчитана и установлена экономическая эффективность работы. Коэффициент экономической эффективности составил 10,76, что говорит об эффективности данной работы.

Таким образом, исследование вопроса уязвимостей системы защиты «Умных домов», является очень перспективным и экономически выгодным проектом.

5. ОХРАНА ТРУДА И БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

5.1 Анализ потенциальных опасностей

Задачей дипломного проекта является разработка модели уязвимостей системы защиты в объектах типа «Умный дом». В процессе работы предусматривается проведение работ в помещении (вычислительном центре), оборудованном персональными компьютерами с визуальными дисплейными терминалами.

Человек при работе с ВДТ подвергается воздействию комплекса неблагоприятных факторов, обусловленных характером производственного процесса условия труда. К общим относятся:

- поражение электрическим током из-за нарушений правил электробезопасности, неисправности электрического оборудования, отсутствия или неисправности заземляющего контура, что может привести к электрически травмам, потери трудоспособности или к летальному исходу;
- негативное воздействие специфической работы на опорно-двигательный аппарат, зрительные и слуховые анализаторы, что приводит к эмоциональным нагрузкам, перенапряжению;
- воздействие ионизирующего излучения, выделяющегося при работе с монитором, может привести к снижению иммунитета, кожным заболеваниям;
- накопление статических зарядов от работающего ВДТ может привести к заболеванию кожи;
- недостаточное освещение вследствие неисправности осветительных приборов или неправильного расчета может привести к повышенной нагрузке на глаза, дискомфорту, быстрой утомляемости;
- неудовлетворительные параметры микроклимата, из-за повышенной влажности, может привести к нарушению состояния здоровья, дискомфортным теплоощущениям, ухудшающие самочувствие и понижающие работоспособность;

- возгорание из-за нарушения правил пожарной безопасности, что может привести к повреждению оборудования либо к летальному исходу людей;

- негативные последствия из-за неадекватного поведения рабочих в условиях ЧС.

5.2. Мероприятия по обеспечению безопасности

При работе в вычислительном центре главным опасным фактором является электричество.

Для защиты от поражения электрическим током (включая случаи ошибочных действий обслуживающего персонала) предусмотрены следующие аспекты:

- надежно изолированы токоведущие части производственного оборудования, являющиеся источниками опасности, а также проведены в недоступных для людей местах;

- заземлены металлические части производственного оборудования, которые могут вследствие повреждения изоляции оказаться под электрическим напряжением опасной величины;

- предусмотрено в схеме электрических цепей производственного оборудования устройство, централизованно отключающее от питающей сети все электрические цепи.

На основании ГОСТ 12.2.007.0-75 «Изделия электротехнические. Общие требования безопасности» электробезопасность обеспечивается:

- техническими способами и средствами защиты;
- организационными и техническими мероприятиями;
- конструкцией электроустановок.

Технические способы и средства защиты, обеспечивающие электробезопасность, установлены с учетом условий внешней среды: помещение по степени опасности и поражения электрическим током

относится к категории «Помещения без повышенной опасности».

Исключительно важное значение для предотвращения электротравматизма имеет правильная организация обслуживания действующих электроустановок, проведения ремонтных, монтажных и профилактических работ. При этом под правильной организацией понимается строгое выполнение ряда организационных и технических мероприятий и средств, установленных действующими «Правилами безопасної експлуатації електроустановок» (НПАОП 40.1-1.21-98), «Правилами установки электроустановок» (ПУЭ). Рекомендуется установить в помещении автоматические отключатели, устройство заземления контура согласно ГОСТ 12.2.007.0-75 «Изделия электротехнические. Общие требования безопасности».

Для обеспечения безопасности работ в действующих электроустановках выполняются следующие организационные мероприятия в соответствии с ГОСТ 12.1.009-79 «Электробезопасность. Общие требования и номенклатура видов защиты»:

- назначение лиц, ответственных за организацию и производство работ;
- оформление работы нарядом или устным распоряжением;
- допуск к работе;
- надзор во время работы;
- оформление перерыва в работе, переводов на другое рабочее место, окончания работы.

При организации труда связанного с использованием ЭВМ, для сохранения здоровья работающих, предотвращения профессиональных заболеваний и поддержки работоспособности предусмотрены внутреперерывные регламентированные перерывы для отдыха (СанПиН 2.2.2.542-96 Приложение 15 «Время регламентированных перерывов в зависимости от продолжительности рабочей смены»)

Внутреперерывные режимы труда и отдыха должны предусматривать

дополнительные непродолжительные перерывы в периоды, которые предшествуют появлению объективных и субъективных признаков утомления и снижения работоспособности.

При выполнении на протяжении дня работ, которые принадлежат к разным видам трудовой деятельности, за основную работу с ЭВМ следует считать такую, что занимает не меньше 50% времени на протяжении рабочей смены должны предусматриваться:

- перерывы для отдыха и употребления еды (обеденные перерывы);
- перерывы для отдыха и личных потребностей (согласно с трудовыми нормами);
- дополнительные перерывы, которые вводятся для отдельных профессий с учетом особенностей трудовой деятельности.

Длительность обеденного перерыва определяется действующим законодательством о труде и Правилами внутреннего трудового распорядка предприятия (организации, учреждения).

Во всех случаях, когда производственные обстоятельства не позволяют применить регламентированные перерывы, длительность непрерывной работы с ЭВМ не должна превышать 4 часа.

С целью уменьшения негативного влияния монотонности является целесообразным изменять содержание работы: сменять чтение текстов на ввод и редактирование информации, делать короткие перерывы.

Согласно «Правилам устройства электроустановок» (ПУЭ) сопротивление защитного заземления в помещении составляет не больше 4 Ом.

Значения напряженности электростатического поля на рабочих местах с ВДТ ПЭВМ (как в зоне экрана дисплея, так и на поверхностях оборудования, клавиатуры, печатного устройства) должны не превышать предельно допустимых в соответствии с ДСанПіН 3.3.2.007-98 додаток 6 «Допустимі параметри електромагнітних неіонізуючих випромінювань і электростатичного поля». Допустимые уровни напряженности полей зависят

от времени пребывания на рабочих местах. Предельно допустимый уровень напряженности электростатических полей равен 60 кВ/м в 1 ч.

Для меньшего воздействия ионизирующего излучения на оператора заменяем монитор на основе электронно-лучевой трубки на монитор на основе активной матрицы (жидкокристаллический монитор, TFT), например на LG FLATRON L1752TQ.

Защита от статического электричества осуществляется двумя путями:

- уменьшением интенсивности образования электрических зарядов;
- устранением образовавшихся зарядов статического электричества.

5.3 Мероприятия по промышленной санитарии и гигиене труда

Помещения для работы с ВДТ должны быть оборудованы системами отопления, кондиционирование воздуха, или приливно–вытяжной вентиляцией в соответствии со СанПиН 2.04.05–91 «Отопление, вентиляция и кондиционирование». Нормируемые параметры микроклимата, ионного состава воздуха, содержанию вредных веществ должны отвечать требованиям ДСН 3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень», ГОСТ 12.1.005–88 «Общие санитарно-гигиенические требования к воздуху рабочей зоны». В производственных помещениях на рабочих местах с ВДТ должны обеспечиваться оптимальные значения параметров микроклимата: температуры, относительной влажности и подвижности воздуха (ГОСТ 12.1.005–88).

Для этого установлен кассетный кондиционер LG T18LN – потолочный кассетный кондиционер LG современного и стильного дизайна с широкими функциональными возможностями, с быстрым охлаждением и возможностью широкого распределения потока воздуха в 4 направлениях.

Вычислительный центр расположен на втором этаже производственного здания. Необходимо определить сколько компьютеризированных рабочих мест, оснащенных визуальными

дисплейными терминалами (ВДТ) можно установить в данном помещении и как их расположить в соответствии с установленными нормами и правилами по охране труда. Размеры помещения (вычислительного центра): длина $a = 9$ м, ширина $b = 5$ м, высота $h = 2,85$ м.

Прежде всего, необходимо проанализировать подходит ли данное помещение для того, чтобы разместить в нем компьютеризированные рабочие места.

Согласно НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» недопустимо расположение помещений, предназначенных для работы с ВДТ в подвалах и цокольных этажах. Также запрещается размещение взрывоопасных помещений категории А и Б (НАПБ Б.03.002-2007 «Нормы определения категорий помещений, зданий и наружных установок по взрывопожарной и пожарной безопасности») и производств с мокрыми технологическими процессами рядом с помещением, где располагается ЭВМ (ПЭВМ), а также над такими помещениями, или под ними. Кроме того, производственные помещения для работы с ВДТ не должны граничить с помещениями, в которых уровень шума и вибрации превышает допустимые значения.

Выбранное помещение соответствует вышеуказанным требованиям, поэтому переходим к следующему этапу, а именно, к определению количества компьютеризированных рабочих мест, которые можно разместить в данном помещении. Поскольку площадь помещения составляет $S_{\text{пом}} = 45$ м², а площадь, на которой располагается одно рабочее место с ВДТ согласно ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин», должна составлять не менее 6 м², то в данном помещении можно разместить максимум 7 компьютеризированных рабочих мест. В вычислительном центре располагается 5 рабочих мест.

Проверим, соответствует ли это число нормативу относительно минимального объема помещения на одно рабочее место с ВДТ

($V_{P.M.min} = 20 \text{ м}^3$). Объем помещения составляет $128,25 \text{ м}^3$, а также объем, приходящийся на одно компьютеризированное рабочее место – $V_{P.M.} = 25,7 \text{ м}^3$. Таким образом, норматив по объему помещения на одно рабочее место с ВДТ выполняется.

Планирование размещения компьютеризированных рабочих мест в помещении проводим с учетом следующих требований:

- рабочие места с ВДТ размещаются на расстоянии не менее 1 м от стены со световыми проемами;
- расстояние между боковыми поверхностями ВДТ должно быть не менее 1,2 м;
- расстояние между тыльной поверхностью одного ВДТ и экраном другого не должно быть меньше 2,5 м;
- проход между рядами рабочих мест должен быть не менее 1 м.

Необходимо также учесть размеры мебели на компьютеризированных рабочих местах, в частности рабочего стола. Согласно НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» рекомендуемые размеры стола для рабочего места с ВДТ составляют: высота – 800 мм, ширина – 600-1400 мм, глубина – 800-1000 мм. Принимаем, что рабочий стол имеет следующие размеры: высота – 800 мм, ширина – 1200 мм, глубина – 900 мм.

Лучше разместить компьютеризированные рабочие места вдоль стены с окном. Это позволит исключить зеркальное отблечение на экране ВДТ источника естественного света (окна) и попадание последнего в поле зрения оператора, что ухудшает условия его зрительной работы.

Комфортные и безопасные условия труда – один из основных факторов влияющих на производительность людей, работающих с ВДТ ПЭВМ.

Помещения для работы с ВДТ должны иметь естественное и искусственное освещение в соответствии с ДБН В.2.5-28-2006 «Природне і штучне освітлення». Естественное освещение осуществляется через световые

отверстия, ориентированные преимущественно на север или северо-восток и обеспечивать коэффициент естественной освещенности (КЕО) не ниже чем 1,5%. Рабочие места программистов расположены подальше от окон и таким образом, что оконные проемы находятся сбоку. Если экран дисплея обращен к оконному проему, необходимы специальные экранирующие устройства. Окна снабжены светорассеивающими шторами, регулируемые жалюзи или солнцезащитной пленкой с металлизированным покрытием. Все нормы по освещенности берутся согласно ДБН В.2.5-28-2006.

В тех случаях, когда одного естественного освещения недостаточно, устраивают совмещенное освещение. При этом дополнительное искусственное освещение применяют не только в темное, но и в светлое время суток.

Наиболее приемлемыми для помещений, где работают ЭВМ, являются люминесцентные лампы ЛБ (белого света) мощностью 20, 40 или 80 Вт.

Для исключения засветки экранов дисплеев прямыми световыми потоками светильники общего освещения располагают сбоку от рабочего места, параллельно линии зрения программиста и стене с окнами.

Расчет освещения по методу коэффициента использования светового потока [15]:

Рассчитаем количество ламп необходимых для освещения помещения размером 9м*5м*2.85 м освещенностью $E_p = 400$ лк. Имеем помещение со светлыми потолком и стенами, серым покрытием пола. Коэффициент отражения потолка 70%, стен 50% и пола 30%. Для освещения используются люминесцентные лампы типа ЛБ (так как высота помещения менее 6 м и используется при исполнении точных работ) в светильниках ЛПО.

Находим индекс помещения по формуле (4.1):

$$i = \frac{A \cdot B}{H_p \cdot (A + B)} \quad (4.1)$$

где A и B – длина и ширина помещения, м;

H_p – расчетная высота подвеса светильника над рабочей поверхностью, м.

$$H_p = H - h - h' = 2.85 - 0.075 - 0.8 = 1.98 \text{ м.}$$

где H – высота помещения, м;

h_c – расстояние светильников от перекрытия (свес), м;

h_{pp} – высота рабочей поверхности над полом, м.

Подставив значения в формулу (4.1), получим:

$$i = \frac{9 \cdot 5}{1.98 \cdot (9 + 5)}; i = 1,6.$$

Принимаем коэффициент запаса $k=1.5$ и коэффициент неравномерности освещения $Z = \frac{E_{cp}}{E_{min}} = 1.1$

При индексе $i=1.6$ получаем $\eta=56\%$.

Расстояния между соседними светильниками:

$$L = H_p \cdot \lambda = 1.6 \cdot 1.4 = 2.24$$

где λ – оптимальное относительное расстояние между светильниками, $\lambda = 1.4$.

Число рядов светильников в помещении: $N_p = \frac{5}{2.24} = 2$

Определяем необходимый световой поток ламп в каждом ряду по формуле (4.2):

$$\Phi_p = \frac{E_n \cdot S \cdot Z \cdot k}{N_p \cdot \eta}, \text{ ЛМ} \quad (4.2)$$

где E_n - нормированная освещенность для данного вида работ, лк;

- площадь помещения, м²;

S

k - коэффициент запаса;

z - коэффициент неравномерности освещенности;

η - коэффициент использования светового потока;

N_p - число рядов светильников в помещении.

Подставим значения в формулу (4.2):

$$\Phi_p = \frac{400 \cdot 45 \cdot 1.1 \cdot 1.5}{2 \cdot 0.56};$$

$$\Phi_p = 26518 \text{ лм}$$

Если в светильнике установить по две лампы ЛБ ($n=2$) мощностью 40 Вт и световым потоком $\Phi_{\text{л}}=3000\text{лм}$, то количество светильников в ряду найдем по формуле (4.3):

$$N = \frac{\Phi_p}{n \cdot \Phi_{\text{л}}} \quad (4.3)$$

Подставим значения в формулу(4.3):

$$N = \frac{26518}{2 \cdot 3000};$$

$$N = 4 \text{ (количество светильников в ряду)}$$

Таким образом, для освещения данного помещения необходимо 2 ряда светильников, в каждом ряду по 4 светильника типа ЛПО2/40 (мощностью 40Вт и длиной 1.2м).

Сиденья, входящие в конструкцию оборудования регулируются (за счет

поворота и регулирования по горизонтали и вертикали) в соответствии с требованиями ГОСТ 12.2.032-78 «Рабочее место при выполнении работ сидя». Конструкцией сиденья предусмотрены подлокотники, опора для спины и подставка для ног, соответствующие антропометрическим данным и отвечающие гигиеническим требованиям.

Производительность труда и самочувствие сотрудника во многом зависят от состояния окружающей среды и, прежде всего, от изменения температуры, влажности, скорости движения воздуха, атмосферного давления, теплового излучения. Человек работоспособен и чувствует себя хорошо, если температура окружающего воздуха находится в пределах 18-22°C, относительная влажность составляет 40-60 %, а скорость движения воздуха 0,1-0,2 м/с (ДСН 3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень»).

5.4 Мероприятия по пожарной безопасности

Общие требования пожарной безопасности изложены в НАПБ А. 01.001-2004 «Правила пожарной безопасности Украины».

Для отвода теплоты от ЭВМ в производственных помещениях ВЦ постоянно действует мощная система кондиционирования. Поэтому кислород, как окислитель процессов горения, имеется в любой точке помещения ВЦ.

Одной из наиболее важных задач пожарной защиты является защита строительных помещений от разрушений и обеспечение их достаточной прочности в условиях воздействия высоких температур при пожаре. Таким образом, здания для ВЦ и части здания другого назначения, в которых предусмотрено размещение ЭВМ, должны быть 1 и 2 степени огнестойкости.

В служебных помещениях вывешены «Планы эвакуации людей при пожаре», регламентирующие действия персонала в случае возникновения очага возгорания и указывающие места расположения пожарной техники.

Эвакуационные выходы располагаются, рассредоточено, а их количество из зданий – не менее двух. При количестве работающих в смене до 50 человек предусмотрен второй (запасный выход) на наружную лестницу.

К средствам тушения пожара, предназначенных для локализации небольших возгораний, относятся пожарные стволы, внутренние пожарные водопроводы, огнетушители, сухой песок, асбестовые одеяла и т. п.

В зданиях пожарные краны устанавливаются в коридорах, на площадках лестничных клеток и входов.

Для обнаружения начальной стадии загорания и оповещения службу пожарной охраны используют системы автоматической пожарной сигнализации (АПС).

Залы ЭВМ, помещения для внешних запоминающих устройств, подготовки данных, сервисной аппаратуры, архивов, копировально-множительного оборудования и т.п. необходимо оборудовать дымовыми пожарными извещателями. В этих помещениях в начале пожара при горении различных пластмассовых, изоляционных материалов и бумажных изделий выделяется значительное количество дыма и мало теплоты.

Исходя из того, что в вычислительных центрах имеются в больших количествах бумага, пластмассы, резина и другие горючие материалы при отсутствии горючих газов и жидкостей, данные помещения, согласно НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків і зовнішніх установок по вибухопожежній і пожежній безпеці», относятся к категории В пожароопасных производств.

Для тушения возгораний в ВЦ предполагается использование ручных огнетушителей следующих типов из расчета 2 шт., на каждые 20 м² площади помещения:

- углекислотные ОУ-2, ОУ-5, ОУ-8;
- углекислотно-бромэтиловые ОУБ-7;
- порошковые ОП-3.

Данные типы огнетушителей позволяют тушить электроустановки,

находящиеся под напряжением.

Противопожарную защиту обеспечивают следующие меры:

- максимально возможное применение негорючих и трудно горючих материалов;
- ограничение количества горючих веществ и их надлежащее размещение;
- предотвращение распространения пожара за пределы очага;
- применение средств пожаротушения;
- эвакуация людей;
- применение средств коллективной и индивидуальной защиты;
- применение средств пожарной сигнализации.

5.5 Мероприятия по обеспечению безопасности в чрезвычайных ситуациях. Организация гражданской обороны на промышленном объекте

Гражданская оборона на промышленном объекте организуется с целью защиты персонала объекта и населения, проживающего вблизи от него, от чрезвычайных ситуаций природного, техногенного и военного характера.

Основными задачами ГО на объекте являются:

- 1) защита персонала объекта и населения от ЧС;
- 2) повышение устойчивости функционирования объекта в ЧС;
- 3) проведение аварийно-спасательных и других неотложных работ в очагах поражения и зонах катастрофического затопления.

Организационные мероприятия предусматривают разработку и планирование действий руководящего, командно-начальствующего состава отдела по делам ГО и ЧС, служб и формирований ГО по защите персонала объекта, проведению аварийно-спасательных и других неотложных работ.

Инженерно-технические мероприятия ГО – это комплекс

мероприятий, осуществляемых инженерно-техническими методами и средствами и направленных на предотвращение или уменьшение возможных потерь и разрушений, повышение устойчивости работы объекта в чрезвычайных ситуациях.

Экономические мероприятия предусматривают такой подход к выполнению всего комплекса работ, который обеспечил бы их эффективность при минимальных капитальных затратах.

Экологические мероприятия представляют собой продолжение комплекса работ данного направления, которые должны вестись каждым объектом с целью максимально возможного уменьшения вредного воздействия продуктов технологического цикла на окружающую среду.

За организацию защиты персонала объекта и населения от ЧС отвечает система гражданской обороны объекта.

Начальником гражданской обороны объекта является его руководитель. Он подчиняется ведомству, а в оперативном отношении начальнику гражданской обороны города, на территории которого расположен объект.

На крупных промышленных объектах, как правило, есть штатный заместитель начальника гражданской обороны, который в мирное время является основным организатором всех подготовительных мероприятий по гражданской обороне.

Заместителем начальника гражданской обороны по рассредоточению и эвакуации персонала назначается обычно заместитель руководителя объекта по общим вопросам. Он разрабатывает план рассредоточения работающего персонала и их семей, организует подготовку мест в загородной зоне, перевозку туда людей.

Заместителем начальника ГО по инженерно-технической части назначается главный инженер предприятия, который непосредственно руководит службами, а также осуществляет техническое руководство аварийно-спасательными и другими неотложными работами.

Заместителем начальника ГО по материально-техническому снабжению назначается заместитель руководителя объекта по этим вопросам, руководящий службой материально-технического снабжения.

На всех объектах, как правило, создаются отделы по делам ГО и ЧС, которые комплектуются из должностных лиц. Для решения задач, возлагаемых на ГО, на объектах, располагающих соответствующей базой, создаются следующие службы:

- 1) оповещения и связи;
- 2) охраны общественного порядка;
- 3) противопожарная;
- 4) медицинская;
- 5) аварийно-техническая;
- 6) убежищ и укрытий;
- 7) энергетики и светомаскировки;
- 8) радиационной и химической защиты;
- 9) транспорта и др.

Убежища должны отвечать требованиям:

- 1) обеспечивать защиту от любых поражающих факторов и от теплового воздействия пожаров на поверхности не менее двух суток;
- 2) быть построенными вне зон и очагов пожаров и затоплений;
- 3) иметь входы с той же степенью защиты, что и основные помещения, а на случай завала – аварийные выходы;
- 4) иметь подходы, свободные от складирования опасных, горючих и сильно дымящих веществ, а также подъездные пути;
- 5) иметь основные помещения высотой более 2,2 м, а уровень пола должен быть выше уровня грунтовых вод более чем на 20 см;
- 6) иметь фильтровентиляционное оборудование, обеспечивающее очистку воздуха от примесей и подачу в убежище не менее 2 м³ воздуха в час на одного человека.

Если убежище находится в зоне заражения с уровнями радиации

после ядерного взрыва, то время безопасного пребывания в нем укрываемых людей составит от нескольких часов до одних суток.

Убежища укомплектовываются работоспособным оборудованием:

1) фильтровентиляционное оборудование обеспечивает очистку и обеззараживание воздуха, поступающего в убежище;

2) водопровод, запас воды в проточных емкостях из расчета 6 л питьевой и 4 л технической (для санитарно-гигиенических потребностей) на человека на весь расчетный срок пребывания в убежище;

3) водяное, электрическое или другое отопление, которое включается с началом заполнения убежища;

4) канализация (санузлы) выполняется на базе общих сетей, но должны быть приемники фекальных вод, которые обеспечат нормальную жизнедеятельность при авариях на общих сетях и не допустят затопления убежища;

5) освещение (основное, аварийное) не должно потреблять кислород;

6) противопожарный инвентарь, инструменты, оборудование и материалы тушения пожаров;

7) в убежище должен быть медицинский пункт;

8) для контроля систем жизнеобеспечения в убежище имеются соответствующие контрольно-измерительные средства измерения, прибор химической разведки (ВПХР) и измеритель мощности дозы ИМД-21с (или ДП-64, ДП-5, ИМД-5);

9) в убежище хранится необходимая документация: план убежища и правила эксплуатации систем и элементов убежища;

10) аварийная электростанция, если она имеется, размещается в отдельном изолированном помещении с тамбуром;

11) каждое убежище обслуживается специальным формированием ГО (убежищ и укрытий). Его личный состав прибывает по сигналу и выставляет посты.

Пост 1 – у каждого входа. При заполнении убежища через него

осуществляется пропуск людей. Он распределяет поток прибывающих, обеспечивая размещение детей, больных и престарелых. По сигналу «Закрыть убежище» постовые закрывают дверь, и один из них постоянно находится у двери.

Пост 2 – в аппаратной. Включает фильтровентиляционную аппаратуру (ФВА) и следит за работой всего оборудования, показаниями средств измерений. Выполняет команды по установлению режима вентиляции.

Пост 3 – специалист перед заполнением убежища включает освещение во всех помещениях, закрывает ставни лазов, регулирует заглушки вытяжной вентиляции, выполняет переключения по схеме воздухообеспечения убежища, а затем поддерживает порядок при размещении людей.

5.6 Выводы по разделу «Охрана труда и безопасность в чрезвычайных ситуациях»

Для обеспечения электробезопасности согласно ГОСТ 12.2.007.0-75 «Изделия электротехнические. Общие требования безопасности» применены отдельно либо в сочетании друг с другом следующие технические средства защиты: защитное заземление (зануление), защитное отключение, электрическое разделение сети, изоляция токоведущих частей (рабочая, дополнительная, усиленная, двойная), изоляция рабочего места.

Согласно СанПиН 2.2.2.542-96 Приложение 15 «Время регламентированных перерывов в зависимости от продолжительности рабочей смены» для снижения эмоциональных нагрузок, перенапряжений от специфической работы на ЭВМ предусмотрены внутреперерывные регламентированные перерывы для отдыха. Работа за ЭВМ не должна превышать 4 часов.

Для меньшего воздействия ионизирующего излучения на оператора заменяем монитор на основе электронно-лучевой трубки на монитор на основе активной матрицы (жидкокристаллический монитор, TFT), например

на LG FLATRON W1942S.

Для достаточного освещения кроме системы общего освещения дополнительно устанавливаются светильники местного освещения. Искусственное освещение в помещении осуществляется системой общего равномерного освещения, для чего установлены люминесцентные лампы типа ЛБ (ДБН В.2.5-28-2006 «Природне і штучне освітлення»).

Для того, чтобы обеспечивались оптимальные значения параметров микроклимата согласно требованиям ДСН 3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень» устанавливаем кассетный кондиционер LG T18LN – с широкими функциональными возможностями, с быстрым охлаждением и возможностью широкого распределения потока воздуха в 4 направлениях.

Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты. В служебных помещениях вывешены «Планы эвакуации людей при пожаре», регламентирующие действия персонала в случае возникновения очага возгорания и указывающие места расположения пожарной техники.

С целью защиты персонала промышленного объекта и населения, проживающего вблизи от него, от чрезвычайных ситуаций природного, техногенного и военного характера проводятся организационные, инженерно-технические, экономические и экологические мероприятия ГО.

ЗАКЛЮЧЕНИЕ

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. В связи с этим возникает множество вопросов, связанных с безопасностью и надежностью систем, построенных по технологии «Умный дом».

Из анализа литературы по данной теме, очевидно, что система защиты для объектов типа «Умный дом», как и любая комплексная система защиты, не может быть идеальной и неизменной для каждого пользователя. С целью обеспечения максимальной защиты информации, ценной для пользователя, и безопасности всех жильцов «Умного дома», система должна быть адаптированной под условия и образ жизни владельца дома. В данной работе основной задачей была разработка модели уязвимостей системы защиты в объектах типа «Умный дом». Было выделено, что основным преимуществом, но в то же время и недостатком является подключение к интернету, и возможность удаленного доступа к данной системе. Для построения модели уязвимостей была построена модель нарушителя. Основная задача нарушителя состоит, как правило, в реализации НСД к информационным или аппаратным ресурсам системы и «обходе» средств защиты. Приведенный анализ угроз и уязвимостей в таблице 2.1, показал, что система подвергается опасностям, как внутренним (вирусы и атаки на центральный компьютер), так и нанесенных извне (перехват информации, передаваемой по проводным и беспроводным линиям, которые выходят за пределы контроля). После оценки уровней риска для выделенных угроз и уязвимостей было определено, что самыми опасными являются те угрозы, при которых злоумышленник может получить контроль над всей системой «Умного дома». Таковыми угрозами являются:

1. Хакерские атаки на центральный сервер.
2. Влияние вирусных и троянских программ на работу системы.
3. Ошибки программного обеспечения.
4. Перехват информации, передаваемой по проводным и беспроводным каналам связи.

Следует отметить, невозможно добиться полного устранения этих угроз, так как имеет место прямая связь с центральным компьютером и подключением к интернету. Своевременная диагностика системы, и обновления антивирусных программ смогут снизить вероятность угроз на систему.

Несколько рекомендаций о том, как обезопасить «Умный дом» от любых попыток взлома:

Во-первых, избегайте беспроводных подключений между модулями системы.

Во-вторых, используйте только временные подключения к сети Интернет, это поможет избежать не только целенаправленных атак, но также снизит риск проникновения вредоносных программ на сервер. Если Вы вынуждены использовать беспроводные подключения в «Умном доме» - устанавливайте глушилки Wi-Fi/Bluetooth в местах, где беспроводная сеть выходит за пределы здания или квартиры.

Дальнейшее развитие технологий стандартов автоматизации приведет к полной зависимости от интернета и телефона. Дома станут полностью автоматизированы, а значит решение проблем уязвимостей системы защиты «Умных домов» станут неотъемлемой задачей для каждого человека.

СПИСОК ЛИТЕРАТУРЫ

1. Категория «Умный дом» [Электронный ресурс] / О Умном доме – Режим доступа: \www/ URL: http://umdomu.ru/index.php/page/o_umnom_dome/.
2. Категория «Умный дом» [Электронный ресурс] / Что такое «Умный дом»? – Режим доступа: \www/ URL: <http://www.dom-electro.ru/что-такое-умный-дом/>.
3. Умный дом [Электронный ресурс] / – Режим доступа: \www/ URL: <http://smarton.com.ua/>.
4. Категория В мире электроники [Электронный ресурс] / Система «Умный дом»: описание и разновидности – Режим доступа: \www/ URL: <http://micro-tech.ru/stati/umnyj-dom-opisanie-sistemy.html>.
5. Андреев Н.К Magic House централизованный мониторинг и управление зданием // Системы безопасности. - 2004. - №4(58). - С. 38-39.
6. Роберт К. Элсенпитер Умный дом строим сами / перевод с англ./ Роберт К. Элсенпитер, Тоби Дж. Велт – М.:КУДРИЦ-ОБРАЗ, 2005. – 384с.
7. Международный стандарт ISO/IEC 27002 – Информационные технологии. Свод правил по управлению защитой информации/ Компания «Технорматив» - перевод на русский язык, 2007. – 171с.
8. Модель угроз и классификация несанкционированных воздействий в Автоматизированных системах [Электронный ресурс] – Режим доступа: \www/ URL: <http://m-g.ru/about/articles/105.html/>.
9. 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. – С. 30-34.
10. Исследование уязвимостей систем Умного дома / А.В. Стариковский, И.Ю. Жуков, Д.М. Михайлов и др. // Спецтехника и связь. – 2012. – Выпуск №2. – С. 55-57.
11. Павлов С.К Интеграция инженерных систем в единой системе

контроля и управления зданием / С.К. Павлов // Системы безопасности. – 2004. - №2. – С. 22-24.

12.Акаева А.А CUJO – система защиты для «Умного дома» / А.А. Акаева, С.И. Лизунов // Неделя науки – 2016: тезисы докладов науч.-техн. конф. – Запорожье: ЗНТУ, 2016.

13.Category «Technology» [Electronic resource] / CUJO. The Smart Way To Fight Home Hacking – Access mode: \www/ URL: <https://www.indiegogo.com/projects/cujo-the-smart-way-to-fight-home-hacking#/> - 10.09.2015.

14.Методичні вказівки по економічному обґрунтуванню дипломних проектів для студентів спеціальності 8.090801 «Мікроелектроніка та напівпровідникові прилади» / Уклали: Варинська Л.О., Антоненко Т.А. - Запоріжжя: ЗНТУ, 2002. – 26 с.

15.Методичні вказівки до лабораторних робіт з дисципліни «Охорона праці у галузі» для студентів усіх спеціальностей / Упоряд.: Б.В. Дзюндзюк, Б.О. Малик, Г.В. Пронюк - Запоріжжя: ЗНТУ, 2008. – 42 с.