Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы: Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____А.В. Бушманов
«__» _____ 2018 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка программного обеспечения для системы «Конфигурируемый дом»

Исполнитель
студент группы 455об _____ (подпись, дата) А.Е. Демьяненко

Руководитель
доцент, канд. техн. наук _____ (подпись, дата) С.Г. Самохвалова

Консультант:
по части безопасности
и экологичности
доцент, канд. техн. наук _____ (подпись, дата) А.Б. Булгаков

Нормоконтроль
инженер кафедры _____ (подпись, дата) В.В. Романико

Благовещенск 2018

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав. кафедрой
_____А.В. Бушманов
«___»_____2018 г.

З А Д А Н И Е

К бакалаврской работе студента Демьяненко Александра Евгеньевича.

1. Тема бакалаврской работы: Разработка программного обеспечения для системы «Конфигурируемый дом»

(утверждена приказом от 23.04.2018 №914-УЧ)

2. Срок сдачи студентом законченной работы: _____г.

3. Исходные данные к бакалаврской работе: отчёт по преддипломной практике.

4. Содержание бакалаврской работы: анализ деятельности объекта автоматизации, исследование вопросов информационной безопасности, разработка прототипов системы, рассмотрение аспектов безопасности.

5. Консультант по бакалаврской работе Булгаков Андрей Борисович – раздел рассмотрения аспектов безопасности и экологичности.

6. Дата выдачи задания: _____.

Руководитель бакалаврской работы: Самохвалова Светлана Геннадьевна, доцент, канд.техн.наук.

Задание принял к исполнению _____ А.Е. Демьяненко

РЕФЕРАТ

Бакалаврская работа содержит 74 с., 35 рисунка, 4 таблицы, 1 диаграмму, 21 источник.

ПРОЕКТИРОВАНИЕ, РАЗРАБОТКА, СИСТЕМА, ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ, ЗАЩИТА ИНФОРМАЦИИ, ИНТЕРНЕТ ВЕЩЕЙ, УМНЫЙ ДОМ, УДАЛЕННЫЙ ДОСТУП, БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Целью бакалаврской работы является разработка программного обеспечения для системы «Конфигурируемый дом» (сокращенно «SCHome») для удаленного управления техникой в доме или на предприятии.

В настоящей работе разработана система «SCHome», обеспечивающая удаленное управление оборудованием в доме. Так же была проанализирована работа локальной вычислительной сети (ЛВС) системы, проанализированы виды, классификации и способы предотвращения угроз ЛВС. Разработан Интернет-магазин для реализации системы «SCHome». Проведено исследование аспектов безопасности жизнедеятельности.

Система «SCHome» позволит значительно снизить тепло- и электро-затраты, а также автоматизировать некоторые аспекты жизни человека. Реализованный удаленный доступ позволит безопасно управлять домом, или получать подробную информации о его состоянии. Осуществление продажи сборных комплектов с информацией по сборке, документацией и бесплатным программным обеспечением, позволит вовлечь школьников, студентов, любителей радиотехники и программирования в изучение технологий «Интернета вещей», и «Умного дома».

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей бакалаврской работе использованы ссылки на следующие стандарты и нормативные документы:

ГОСТ 2.104-68 ЕСКД Основные надписи

ГОСТ 2.105-95 ЕСКД Общие требования к текстовым документам

ГОСТ 2.106-96 ЕСКД Текстовые документы

ГОСТ 2.111-68 ЕСКД Нормоконтроль

ГОСТ 2.306-68 ЕСКД Обозначение графических материалов и правил нанесения их на чертежах

ГОСТ 2.316-68 ЕСКД Правила нанесения на чертежах надписей, технических требований и таблиц

ГОСТ 2.701-84 ЕСКД Схемы. Виды и типы. Общие требования к выполнению

ГОСТ 2.721-74 ЕСКД Обозначения условно-графические в схемах. Обозначения общего применения

ГОСТ 3.1103-83 ЕСКД Основные надписи

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

РД от 30.03.1992 АС защита от НСД. Классификация АС и требования по ЗИ

ГОСТ 12.0.003-2015. Система стандартов по безопасности труда. Опасные и вредные производственные факторы. Классификация

СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронно-вычислительным машинам и организации работы

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

SCHome – система «Конфигурируемый дом»;

ЛВС – локальная вычислительная сеть;

ИТ – информационные технологии;

OSI – базовая эталонная модель взаимодействия открытых систем;

IP (Internet Protocol);

OSPF (Open Shortest Path First) – протокол динамической маршрутизации;

RIP (Routing Internet Protocol) – протокол маршрутной информации;

ICMP (Internet Control Message Protocol) – протокол межсетевых управляющих сообщений;

SNMP (Simple Network Management Protocol) – простой протокол сетевого управления;

МЭ – межсетевой экран;

VPN (Virtual Private Network) – виртуальная частная сеть;

RFID (Radio Frequency IDentification) – радиочастотная идентификация;

NFC (Near Field Communication) – ближняя бесконтактная связь;

ОС – операционная система;

БД – база данных;

ЭВМ – электронно-вычислительная машина;

ПЭВМ – персональная электронно-вычислительная машина

ВВЕДЕНИЕ

На сегодняшний день информационные технологии играют значительную роль в жизни человека. Все больше технологических процессов автоматизируются, в том числе и системы жизнеобеспечения и безопасности.

Система «Конфигурируемый дом» (сокращенно «SCHome») является комплексом аппаратных и программных средств на основе технологий «умного дома» и «интернета вещей» (Internet of Things). Основная концепция системы заключается в объединении техники/оборудования и датчиков в единую информационную систему.

В связи с тем, что в доме или на работе достаточно большое количество различного оборудования, система построена на использовании технологии беспроводной локальной сети устройствами на основе стандартов IEEE 802.11 – Wi-Fi. По локально-вычислительной сети передаются данные о показаниях датчиков, команды оборудованию и бытовой технике. Для дальнейшего развития системы необходим удаленный доступ к локальной сети и его организация ведет к рискам потери конфиденциальной информации и несанкционированному доступу к системе. Поэтому при подключении к Интернету локальной сети необходимо позаботиться об обеспечении ее информационной безопасности.

Целью разработки предложений по созданию системы защиты информации в локальной вычислительной сети является обеспечение предоставления надежного и защищенного доступа к конфиденциальной информации для определенного круга пользователей.

Основными задачами, которые должны быть решены в результате написания курсовой работы, являются:

- создание защищённой среды для надёжного и безопасного функционирования информационно-вычислительной сети;

- обеспечение безопасного информационного взаимодействия пользователя и системы, а также между подключенным к системе оборудованием;

- организация защиты информационных ресурсов системы, как от атак извне (Интернет), так и изнутри.

1 ИССЛЕДОВАНИЕ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ СИСТЕМЫ «SCHOME»

Главной проблемой ЛВС является обеспечение информационной безопасности. Обеспечение безопасности ЛВС представляет собой организацию контрмер несанкционированному внедрению в процессы функционирования ЛВС, а также модификации, хищения, разрушения или вывода из строя её составных частей, другими словами это – защита всех компонентов ЛВС – программного обеспечения, аппаратных средств, данных.

Предпосылками того, что информация, обрабатываемая в ЛВС, особенно уязвима, являются:

- большой объём передаваемой, обрабатываемой, и хранимой информации в компьютерах (микроконтроллерах, оборудовании);

- централизация в хранилищах данных информации различного уровня важности и конфиденциальности;

- расширенный круг доступа пользователей к информации, хранящейся в системе, и к ресурсам вычислительной сети;

- широкое использование сети Internet и другие, основанные на данной технологии каналы связи;

- автоматизированный обмен информацией между компонентами системы.

Угроза информационной безопасности – возможная опасность (реально существующая или потенциальная) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты, наносящего ущерб собственнику или пользователю, проявляющегося в опасности искажения, раскрытия или потери информации. Реализация угрозы называется атакой.

Целями реализация угрозы информационной безопасности могут являться:

- нарушение конфиденциальности информации. Информация, хранимая и обрабатываемая в ЛВС, как правило имеет для ее владельца большую ценность. Использование информации другими лицами наносит интересам владельца значительный ущерб;

- нарушение целостности информации. Потеря целостности информации – угроза близкая к её раскрытию. Ценная информация имеет вероятность быть утраченной или обесцененной путём её несанкционированного изменения или уничтожения. Ущерб от подобных действий может быть намного больше, чем при нарушении конфиденциальности,

- нарушение (полное или частичное) работоспособности ЛВС (нарушение доступности). Вывод из строя компонентов сети (некорректное изменение режима работы), а также их подмена (модификация) могут привести к отказу компьютерной системы от потока информации, получению неверных результатов, или отказам при обслуживании.

- несанкционированный доступ к управлению системой, ее компонентами. Перехват управления дверным замком, бытовой техникой, системой пожаротушения и т д. Ущерб от этого в разы может быть выше, чем при других нарушений, так как это приведет к ущербу имущества и/или здоровья пользователя.

Использование информационных технологий (ИТ) всегда подразумевает и повышенное внимание к вопросам информационной безопасности. Частичное или полное уничтожение информационного ресурса, а также его временная недоступность или несанкционированное использование могут нанести любой информационной системе и ее владельцу значительный материальный ущерб. Внедрение ИТ, без защиты информации, может быть экономически невыгодным в результате определенных потерь конфиденциальных данных, обрабатываемых и хранящихся в ЛВС.

Поэтому одно из основных направлений развития ИТ – обеспечение информационной безопасности компьютерных систем и сетей.

Реализация решений, обеспечивающих безопасность информационных ресурсов, ведет к существенному повышению эффективности всего процесса информатизации в организации, обеспечивая конфиденциальность, целостность и подлинность той информации, которая циркулирует в локальных и глобальных информационных средах.

Главным свойством, отличающим ЛВС от автономных компьютеров, считается обмен информацией меж сетевыми узлами, связанными линиями передачи данных.

Объединение компьютеров в компьютерные сети позволяет значительно, если не во много раз, повысить эффективность использования компьютерной системы в целом. Увеличение эффективности же достигается за счёт возможности обмена информацией между участниками сети, а также за счёт возможности использования на каждом компьютере общих сетевых ресурсов (информации, внешних устройств, внешней памяти, программных приложений).

Исходя из этого, модель незащищённой локальной вычислительной сети системы представлена на рисунке 1.

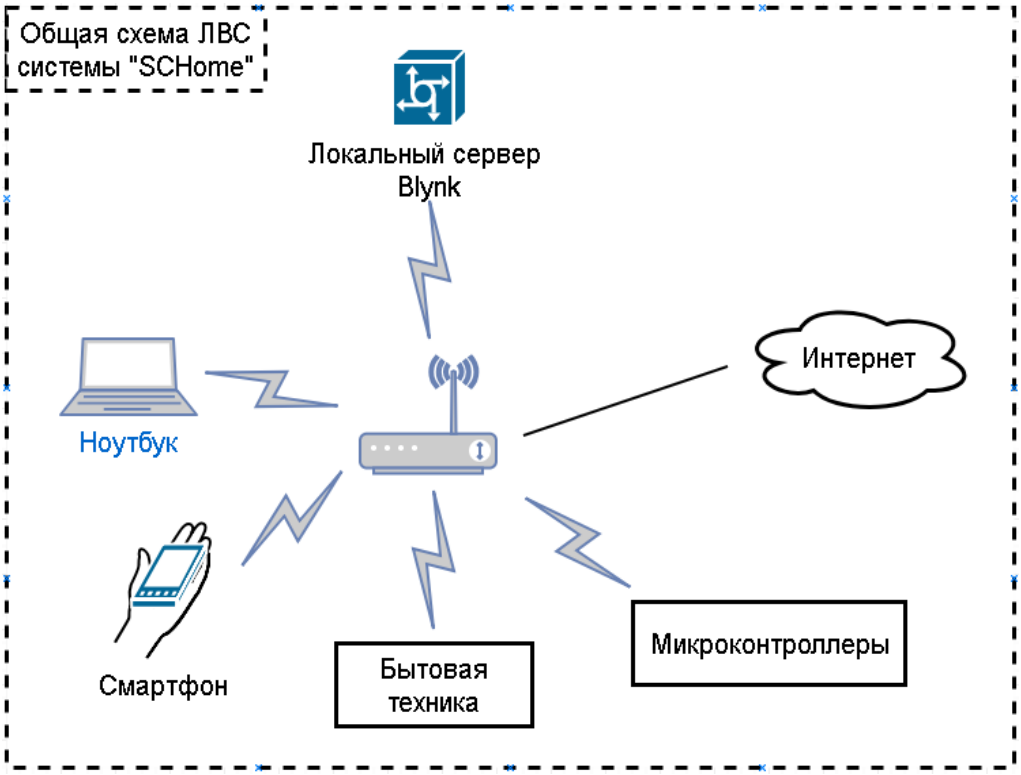

Рисунок 1 – Модель незащищённой ЛВС системы

2 АНАЛИЗ ВОЗМОЖНЫХ ТИПОВ АТАК И МОДЕЛИ НАРУШИТЕЛЯ, ОСУЩЕСТВЛЯЮЩЕГО АТАКИ НА ЛОКАЛЬНУЮ СЕТЬ

2.1 Анализ сетевого трафика

Анализ сетевого трафика – изучение логики работы ЛВС, получение происходящих в системе событий, в момент появления этих событий, команд, передаваемых друг другу участников системы. Изучение происходит после перехвата обменных пакетов на канальном уровне.

Помимо этого, анализ сетевого трафика позволяет перехватить поток информации, которой обмениваются компоненты ЛВС. Таким образом, в случае успешной атаки, атакующий получает на удалённом объекте несанкционированный доступ ко всей данным, которые передаются между двумя сетевыми объектами. Но, при этом, атакующий не имеет возможности модифицировать трафик. Информацию, которую может перехватить атакующий, к примеру, может быть незашифрованные логин и пароль пользователя или идентифицирующий микроконтроллер ключ, передаваемые по сети.

2.2 Подмена доверенного объекта или субъекта ЛВС

Одним из основных вопросов безопасности ЛВС является идентификация и аутентификация, а точнее их недостаточность, удаленных друг от друга объектов. Необходимо осуществлять однозначную идентификацию передаваемых между объектами взаимодействия сообщений.

Каждый объект в ЛВС имеет свой уникальный сетевой адрес (на канальном уровне модели OSI – это аппаратный адрес сетевого адаптера, на сетевом уровне – адрес определяется в зависимости от используемого протокола сетевого уровня (например, IP-адрес). При этом, сетевой адрес не рекомендуется использовать для идентификации объектов ЛВС, так как сетевой адрес очень просто подделывается.

Допустимо использовать в связке с другими способами идентификации объекта.

Довольно часто для служебных сообщений в ЛВС передаются одиночные, не требующих подтверждения, сообщения, то есть виртуальное соединение не производится. В этом случае, атакующий передает свое сообщение (служебное сообщение) от имени сетевого управляющего устройства (маршрутизатор, роутер и т.п.), реализовав, таким образом, несанкционированное управление объектом системы. Подобные действия могут привести к серьезным нарушениям работоспособности объекта и ЛВС в целом.

2.3 Ложный объект ЛВС

Если в ЛВС не решены проблемы, описанные выше, а именно проблемы идентификации управляющих устройств (например, маршрутизаторов, микроконтроллеров), то подобная ЛВС подвергнется следующей атаке, заключающейся в изменении маршрутизации и внедрении ложного объекта в систему. Также в случае использования алгоритмов удаленного поиска для взаимодействия объектов (при соответствующей инфраструктуре сети), существует большой риск несанкционированного внедрения ложного объекта в систему.

2.3.1 Внедрение в ЛВС ложного объекта путём навязывания ложного маршрута

На сегодняшний день, глобальные сети – это совокупность связанных между собой (через сетевые узлы) сегментов сети, при этом данные передаются от источника к приёмнику по маршруту, который является последовательностью узлов сети. В каждом маршрутизаторе имеется таблица маршрутизации, в которой для каждого адресата хранится оптимальный маршрут. Также таблицы маршрутизации существуют и у любых хостов глобальной сети. Для осуществления оптимальной и эффективной маршрутизации в ЛВС существуют специальные управляющие протоколы для обмена информацией между маршрутизаторами, такие как OSPF (Open Shortest Path First), RIP (Routing Internet Protocol). Также применяются протоколы ICMP (Internet Control Message Protocol) для уведомления хостов о новом маршруте, и SNMP (Simple Network Management Protocol) для удалённого управления

маршрутизаторами. Все данные протоколы – протоколы управления сетью, что, в свою очередь, означает удаленное изменение маршрутизации в сети Интернет.

При этом типе атаки, злоумышленник старается достигнуть определенной цели – изменение исходной маршрутизации на объекте ЛВС до состояния, при котором измененный маршрут проходил через объект атакующего (ложный объект).

При одном из способов атакующий посылает по сети специальные служебные сообщения для изменения маршрутизации. Данные сообщения определены управляющими сетью протоколами, и оправляются от имени сетевых управляющих устройств (таких как маршрутизатор). В случае успеха, злоумышленник получает полный контроль над потоком данных, передаваемых между двумя объектами ЛВС, и это открывает ему дальнейшую возможность приема, анализа и передачи сообщений, получаемых от объектов ЛВС.

К такому типу атак относится и пример с развертыванием поддельной точки доступа Wi-Fi. Точка имеет такое же название, как и настоящая, и участник сети, может незаметно для пользователя подключиться к ней, «попав в руки» к злоумышленнику.

2.3.2 Внедрение в ЛВС ложного объекта через использование недостатков алгоритмов удалённого поиска

Часто бывает так, что удаленные объекты ЛВС изначально не имеют достаточно необходимой для адресации сообщений информации. В роли этой информации в основном выступают логические и аппаратные адреса объектов ЛВС (IP-адрес, адрес сетевого адаптера). Именно поэтому используют различные алгоритмы удаленного поиска, для получения такой информации. Алгоритмы представляют собой передачу по сети определенного вида поисковых запросов, и ожидание ответов с искомой информацией на эти запросы.

При использовании алгоритмов удаленного поиска в ЛВС, существует риск перехвата посланного запроса и отправки на него ложного ответа. В от-

вете, атакующий указывает данные, которые приводят к адресации на свой (ложный) объект. И в результате, через ложный объект ЛВС, проходит весь поток данных между объектами взаимодействия.

При другом варианте внедрения в ЛВС ложного объекта, атакующий эксплуатирует недостатки алгоритма удаленного поиска. На атакуемый объект передается заранее подготовленный злоумышленником ложный ответ, но при этом, поисковый запрос не принимается, так как необязательно дожидаться приема запроса, чтобы посылать ложные ответы на них.

К примеру, в системе «SCHome» планировалась реализация механизма подключения к системе «умной» бытовой техники, использующая методы запросов к удаленному серверу производителя этой техники, но в связи с угрозой, описанной выше, была отложена на неопределенный срок.

2.3.3 Использование ложного объекта для организации удалённой атаки на ЛВС

После получения контроля над проходящим потоком информации меж объектами ложный объект ЛВС применяет различные методы воздействия на перехваченные данные:

- селекционирует поток данных и сохраняет ее на ложном объекте ЛВС;
- модифицирует информацию;
- подменивает информацию;
- вызывает отказ в обслуживании.

Селекции – сохранение в файле всех пакетов обмена, получаемых ложным объектом. Однако подобный способ перехвата данных недостаточно информативен. В пакетах обмена есть служебные поля, которые не несут никакой пользы для атакующего. Поэтому, для того чтобы получить сам файл, злоумышленнику необходимо провести динамический семантический анализ потока данных на ложном объекте.

Модификация информации бывает двух видов:

- модификация передаваемых данных;

- модификация передаваемого кода.

Модификация передаваемых данных – одна из функций, обладаемая системой воздействия. В результате селекции потока перехваченной информации и его анализа система может распознавать тип передаваемых файлов (исполняемый или текстовый). Соответственно, в случае обнаружения текстового файла или файла данных появляется возможность модифицировать проходящие через ложный объект данные. Особую угрозу эта функция представляет для ЛВС обработки конфиденциальной информации.

Другим видом модификации может быть модификация передаваемого кода. Ложный объект, может выделить из потока данных исполняемый код, проводя семантический анализ проходящего через него потока данных.

Информация, проходящая через ложный объект может быть не только модифицирована ни и подменена. Модификация информации приводит к ее частичному искажению, а подмена – к ее полному изменению. В случае, когда в ЛВС не имеется средств аутентификации адреса отправителя, то есть инфраструктура ЛВС позволяет с одного объекта системы передавать на другой атакуемый объект бесконечное число анонимных запросов на подключение от имени других объектов. Тогда при подобной атаке возникает отказ в обслуживании – нарушается работоспособность соответствующей службы на атакованном объекте, возникает невозможность получения удаленного доступа

Вторая вид этой типовой удалённой атаки состоит в передаче с одного адреса такого количества запросов на атакуемый объект, какое позволит трафик (направленный «шторм» запросов). Если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то очередь запросов переполняется, отказывает одна из телекоммуникационных служб, ЭВМ останавливает свою работу, так как система не может ничего поделать, пока не обработает большое количества ложных запросов.

Отказ в обслуживании – злоумышленник передает на атакуемый объект некорректный запрос. При этом возможно зацикливание процедуры обработки запроса и зависание системы.

3 ЗАЩИТА ЛОКАЛЬНОЙ СЕТИ

Обеспечение информационной безопасности локальной сети – достаточно непростая задача. Это связано с тем, что существует множество самых разнообразных опасностей, угрожающих размещенной в ЛВС информации. Поэтому, очень легко упустить какую-либо из угроз, при разработке комплекса защитных мер. А это, в свою очередь ведет к большому риску ущерба для пользователей и владельцу ЛВС.

3.1 Главные цели сетевой безопасности

На данный момент, экспертами выделено три главных цели при построении системы сетевой безопасности. Это конфиденциальность, целостность и доступность данных. Кроме этого, при разработке проекта определяются дополнительные задачи. Но в рамках данной выпускной квалификационной работы они рассматриваться не будут, в отличие от главных целей, которые обязательны для каждого проекта защиты ЛВС.

Целостность данных – особо важная цель системы сетевой защиты. Целостность данных означает полное сохранение информации в исходном виде. Информация должна иметь гарантию того, что в результате технических сбоев или действий хакеров она не будет уничтожена. Данные не должны быть изменены в случае подменены злоумышленниками или каких-либо неисправностей. Самая сложная задача в сетевой безопасности – именно обеспечение целостности информации, так как необходимо учесть довольно большое число различных угроз.

Вторая цель – конфиденциальность информации. На сегодняшний день многие люди выносят эту задачу на первый план, так как предрасположены завышать угрозу, исходящую от хакеров. Это мнение в корне не верно, так как это не совпадает со статистикой. Согласно последним исследованиям, примерно в половина всех случаев потери важных данных это результат сбоев в системе электропитания. Ну а большая часть из оставшихся инцидентов повлекли за собой различные технические сбои. Случаи же утери информа-

ции в результате действий хакеров и остальных злоумышленников занимают малую долю всех инцидентов. Именно поэтому обеспечение конфиденциальности информации является второй по важности задачей после сохранения ее целостности.

Третья цель любой системы сетевой безопасности – доступность данных. Это означает, что каждый пользователь в любой момент времени (не считая особых случаев, таких как тех.обслуживание и т.п.) имеет доступ ко всей необходимой для его работы информации. Обычно эту цель разбивают на две задачи. Первая – это обеспечение стабильной работы аппаратных средств: серверов, принтеров, рабочих станций и т. п. Вторая – разделение доступа к информации между различными группами пользователей.

3.2 Анализ методов и средств защиты информации, применяемых в локальных сетях

Для того чтобы обеспечить надёжную защиту ЛВС, в системе информационной безопасности должны быть реализованы самые прогрессивные и перспективные технологии информационной защиты. К ним относятся:

- криптографическая защита данных для обеспечения конфиденциальности, целостности и подлинности информации;
- технологии аутентификации для проверки подлинности объектов и субъектов сети;
- технологии межсетевых экранов для защиты ЛВС от внешних угроз при подключении к общедоступным сетям связи;
- технологии виртуальных защищённых каналов и сетей VPN для защиты, передаваемой по открытым каналам связи информации;
- гарантированная идентификация пользователей путём применения токенов (smart-карт, touch-memory, RFID- и NFC-карт и т. п.);
- технологии обнаружения вторжений (intrusion detection) для активного исследования защищённости информационных ресурсов;
- технологии защиты от вирусов с использованием специализированных комплексов антивирусной профилактики и защиты;

- централизованное управление системой информационной безопасности на базе единой политики безопасности;
- комплексный подход к обеспечению информационной безопасности, реализующий рациональное сочетание технологий и средств информационной защиты.

Криптография – методологическая основа современных систем обеспечения безопасности информации в системе и ЛВС. Криптография — это совокупность методов преобразования данных. Они направлены на защиту этих данных, изменив до неузнаваемости и бесполезности для незаконных пользователей. Данные преобразования решают три главные проблемы защиты данных: конфиденциальность, целостность и доступность передаваемой или сохраняемой информации. Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

У каждого зарегистрированного в системе субъекта (пользователя или действующим от его имени процесса) имеется некоторая информация, которая этот субъект идентифицирует (например, число или строка символов). Это и есть идентификатор субъекта. Перед получением доступа ресурсам ЛВС, пользователь проходит процесс первичного взаимодействия с ЛВС, включающий в себя идентификацию и аутентификацию.

Идентификация – процедура распознавания пользователя по его идентификатору (имени).

Аутентификация – процедура проверки подлинности заявленного пользователя, процесса или устройства.

После того, как субъект был идентифицирован и аутентифицирован выполняется его авторизация.

Авторизация – процедура предоставления субъекту определенных полномочий и ресурсов в системе. Другими словами, авторизация – установка сферы действия пользователя и доступные ему ресурсы устанавливает сферу его действия и доступные ему ресурсы.

Межсетевым экраном (МЭ) является специализированный комплекс межсетевой защиты. Такой комплекс обычно называется брандмауэром или firewall. МЭ делит общую сеть на две части и реализует набор правил. Данные правила определяют условия прохождения из одной части общей сети в другую пакетов с данными через условную границу. В большинстве случаев эта граница проходит между ЛВС и глобальной сетью Internet.

Концепция построения VPN состоит в следующем: постройка виртуального защищенного туннеля между двумя узлами, которым нужно обменяться информацией, для обеспечения целостности и конфиденциальности данных, передаваемых через открытые сети. Доступ к VPN чрезвычайно затруднён всем возможным внешним злоумышленникам.

С помощью технологий Intrusion Detection возможно распознать существующие уязвимости и атаки, выявить старые или появившиеся новые уязвимости, а также противопоставить им соответствующие средства защиты.

7. Технологии защиты от вирусов с использованием специализированных комплексов антивирусной профилактики и защиты.

Существует несколько видов спецпрограмм для защит от компьютерных вирусов, осуществляющих обнаружение и уничтожение компьютерных вирусов. Данные программы называются антивирусами (антивирусными программами). Этот метод особенно важен касательно сервера системы Blynk. В операционной системе Raspbian (Debian-подобная), из которой запускается сервер должна присутствовать антивирусная программа. В таблице 1 представлены данные о найденных уязвимостях за 2016, 2017 годы и за все время ведения статистики.

В связи с тем, что система «SCHome» устанавливается не только в домах, но и на предприятиях, то корпоративные сети предприятий тоже относятся к ЛВС.

Система информационной безопасности – важнейший компонент системы управления ЛВС. Данная система должна выполнять задачи:

- централизованное и оперативное осуществление управляющих воздействий на средства сетевой безопасности;
- проведение регулярных аудитов и мониторингов, дающих, для принятия оперативных решений, объективную информацию о текущем состоянии информационной безопасности.

Таблица 1 – Найденные уязвимости в ОС за 2016-2017гг.

Название ОС	Производитель	Общее число уязвимостей за 2017 год	Общее число уязвимостей за 2016 год	Общее число уязвимостей за все время ведения статистики
Android	Google	**666**	**523**	1357
Linux Kernel	Linux	381	217	**1921**
Iphone Os	Apple	293	161	1277
Windows 10	Microsoft	226	172	451
Windows Server 2016	Microsoft	212	39	251
Windows Server 2008	Microsoft	212	133	981
Mac Os X	Apple	210	215	1888
Windows Server 2012	Microsoft	201	156	606
Windows 7	Microsoft	197	134	838
Windows 8.1	Microsoft	192	154	542
Windows Rt 8.1	Microsoft	124	139	438
Debian Linux	Debian	95	327	1029
Fedora	Fedora project	84	120	441
Ubuntu Linux	Canonical	66	279	867
Watchos	Apple	65	77	231
Windows Vista	Microsoft	64	125	814
Opensuse	Opensuse Project	58	5	119
Leap	Opensuse Project	57	2	60
Leap	Novell	48	260	349
XEN	XEN	44	28	228

3.3 Способы защиты информации

Способы защиты информации в ЛВС делятся на несколько видов, представленных на рисунке 2:

1) препятствие – физическая преграда на пути злоумышленника к защищаемой информации (на территорию и в помещения с аппаратными средствами).

2) управление доступом – защита информации, при которой выполняется урегулирование использования ресурсов системы (программных, технических средств и т.п.). Управление доступом также означает следующие функции защиты:

a) идентификация пользователей, персонала и ресурсов системы, то есть каждому объекту присваивается персональное имя, код, пароль, и в дальнейшем, этот объект опознается по предъявленному им идентификатору;

b) разрешение и создание условий работы в пределах установленного регламента;

c) проверка полномочий, а именно проверка соответствия запрашиваемых ресурсов, процедур, дня недели, времени суток установленному регламенту;

d) соответствующее реагирование при попытках несанкционированных действий;

e) регистрация обращений к защищаемым ресурсам.

3) принуждение – персонал и пользователи ЛВС соблюдают правила обработки и использования защищаемой информации. При нарушении правил следует материальная, административная или уголовная ответственности.

4) регламентация – разработка и реализация в процессе функционирования ЛВС комплексов мероприятий, которые создают условия обработки и хранения в ЛВС информации, приводящих к снижению возможности несанкционированного доступа к ней. Необходимо строго регламентировать

структуру ЛВС (архитектура зданий, размещение аппаратных средств, оборудование помещений), организацию и обеспечение работы всего обрабатывающего информацию персонала, для эффективной защиты.

5) маскировка – защита информации в ЛВС путем ее криптографических преобразований. Криптографическое закрытие информации также является единственным способом надежной защиты при ее передаче по линиям связи на большое расстояние.

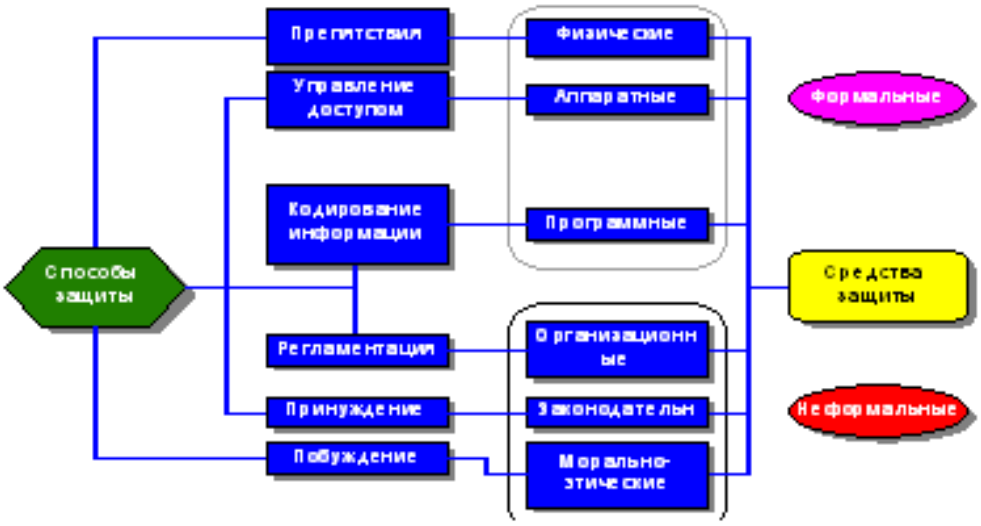

Рисунок 2 – Способы и средства защиты информации в ЛВС

Все рассмотренные выше способы защиты информации реализуются применением различных средств защиты. Средства защиты разделяются на программные, технические, законодательные, организационные и морально-этические средства.

Организационные средства защиты – организационно-правовые мероприятия для обеспечения защиты информации, которые осуществляются в процессе разработки, внедрения и эксплуатации ЛВС. Организационные мероприятия охватывают все структурные элементы ЛВС на всех этапах: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Законодательные средства защиты – законодательные акты страны, которыми регламентируются правила использования и обработки информации

ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты – различные нормы, сложившиеся традиционно или складывающиеся по мере распространения ЭВМ в стране или обществе. Эти нормы обязательны, в отличие от законодательных мер, но не соблюдая их, человек обычно теряет авторитет, престижа.

Средства защиты, рассмотренные выше делятся на два типа:

1) формальные – защитные функции выполняются исключительно по заранее установленной процедуре и без присутствия человека;

2) неформальные – определяющиеся целенаправленной деятельностью людей средства, либо средства, которые регламентируют подобную деятельность.

3.4 Идентификация и аутентификация

Идентификацию и аутентификацию считаются основой программно-технических средств безопасности, так как все остальные сервисы обслуживают уже именованные субъекты. Идентификация и аутентификация можно представить, как «проходная» на предприятии, так как почти всегда выполняются в первую очередь.

Идентификация – процесс именования субъекта (пользователя или действующего от имени этого пользователя процесса). Аутентификация – проверка, посредством которой вторая сторона убеждается в подлинности субъекта. Обычно, субъект подтверждает свою подлинность, предъявляя одну из сущностей:

- «нечто, что он знает» – личный идентификационный номер, пароль, ключ и т.п.;
- «нечто, чем он владеет» – личную карточку или любое другое устройство подобного назначения;
- «нечто, что является частью его самого» – свои биометрические характеристики, такие как отпечатки пальцев, голос и т.п.

Но не всегда возможно произвести надежную идентификацию и аутентификацию по ряду некоторых причин.

Система основана на информации в том виде, в каком она была получена; источник данных неизвестен. К примеру, атакующий воспроизвел ранее перехваченную информацию. Тогда следует обезопасить ввод и передачу идентификационной и аутентификационной информации, что довольно трудно это реализовать в сетевой среде.

Существует возможность, что любые аутентификационные сущности могут быть скомпрометированы, украдены, подделаны.

Имеется обратная взаимосвязь между надежностью аутентификации, и удобством пользователя (или системного администратора). Например, будет лучше, если пользователь с определенной частотой вводит аутентификационные данные (чтобы снизить риск использования системы другим человеком), но это приведет к увеличению вероятности подглядывания за вводом. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это повышает вероятность подглядывания за вводом.

Чем выше надежность средства защиты, тем выше и его цена. Необходим компромисс между доступностью по цене, надежностью, и удобством использования и администрирования. Как правило, этого компромисса достигают за счет использования двух первых из перечисленных выше принципиальных механизмов проверки аутентичности.

Пароли являются самым распространенным средством аутентификации. Система сравнивает введенный пароль и пароль, заранее определенный для конкретного пользователя; если пароли совпадают – проверка считается пройденной, и субъект доказал свою подлинность. Но в последнее время все больше набирает популярность секретные криптографические ключи – они обеспечивают наибольшую эффективность, зачастую являясь одновременно и идентификационной и аутентификационной информацией.

Парольная аутентификация – проста и привычна для пользователя, так как она давно встроена в операционные системы и сервисы. На данный момент, пароли распространены среди многих организаций, так как обеспечивают приемлемый для этих организаций уровень безопасности. Тем не менее, это самое слабое средство проверки подлинности. Надежность паролей напрямую зависит от способностей человека запоминать их и хранить в тайне. Тем не менее, ввод пароля можно подсмотреть, пароль можно подобрать методом брутфорса (перебором). Файл паролей может быть зашифрован, но открыт для чтения, и тогда его может перекачать к себе на ЭВМ злоумышленник и подобрать пароль полным перебором.

Пароли также уязвимы к электронному перехвату – это наиболее принципиальный недостаток, который невозможно возместить обучением пользователей или улучшением администрирования. Использование криптографии – единственный выход при передаче по линиям связи.

Однако, существует ряд действий, повышающие надежность систем паролей:

- наложить технические ограничения (например, длина пароля больше 8 знаков, содержащий буквы, цифры, спецсимволы);
- управлять сроком действия паролей, периодически менять их;
- ограничить число неудачных попыток входа для затруднения применения метода подбора;
- ограничить доступ к файлу паролей;
- обучение и воспитание пользователей;
- использовать программные генераторы паролей, создающие с помощью некоторых алгоритмов легко запоминающиеся пароли.

В специфических организациях с высокими требованиями к безопасности применяются устройства контроля биометрических характеристик. Такие устройства сложны и имеют высокую цену.

Администрирование службы идентификации и аутентификации является важной, но в то же самое время и трудной задачей. Хороший админи-

стратор постоянно поддерживает конфиденциальность, целостность и доступность информации, находящейся в ЛВС, а это довольно непросто, т.к. ЛВС чаще всего является сетевой разнородной средой. Немаловажным стоит отметить, что целесообразно использовать централизацию информации по максимуму, наряду с автоматизацией, используя средства централизованного администрирования или выделенные серверы проверки подлинности. Основой централизации данных может служить сетевые сервисы, предоставляемые некоторыми операционными системами. Также централизация может облегчить работу пользователям, так как позволяет реализовать концепцию единого входа в ЛВС. Пользователь один раз проходит проверку подлинности и, в пределах своих полномочий, получает доступ ко всем ресурсам сети.

3.5 Управление доступом

Средства управления доступом – средства, осуществляющие спецификацию и контроль действий, которые пользователи и процессы могут выполнять над информацией и ресурсами системы. Логическое управление доступом – это основной механизм многопользовательских систем. Он обеспечивает целостность, конфиденциальность объектов и их доступность через запрещение обслуживания неавторизованных пользователей. Логическое управление доступом определяет для каждой пары (субъект-объект) множество допустимых операций, а также контролирует выполнение порядка, установленного в системе.

Контроль прав доступа осуществляется различными частями программной среды – системой управления базами данных (СУБД), ядром операционной системы, посредническим программным обеспечением, дополнительными средствами безопасности и т.д.

В момент, когда принимается решение о предоставлении доступа анализируется следующая информация:

- идентификатор субъекта;
- атрибуты субъекта;
- место действия;

- время действия;
- внутренние ограничения сервиса.

Часто над средствами логического управления доступом устанавливают ограничивающий интерфейс, лишающий пользователя возможности совершения несанкционированных, исключив из числа видимых ему объектов те, к которым у него нет доступа.

4 РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ «SCHOME»

В настоящее время информационные технологии применяются повсеместно: от ключа домофона до переработки угля в синтопливо. Автоматизация некоторых отдельных процессов или внедрение целых систем, в подавляющем большинстве случаев, приводит к увеличению эффективности этих систем. Это связанно со стремлением человека улучшить все вокруг себя, чтобы облегчить себе жизнь. Почти половину жизни человек проводит у себя дома, и совершенно естественно, что он начал пробовать повсюду внедрять информационные технологии. И совсем недавно, примерно два десятилетия назад, появилось понятие «Умный дом».

Технология «Умный дом» – это интеллектуальная система управления домом, обеспечивающая автоматическую и согласованную работу всех систем жизнеобеспечения и безопасности. Такая система самостоятельно распознает изменения в помещении и реагирует на них соответствующим образом. Основной особенностью такой технологии является объединение отдельных подсистем и устройств в единый комплекс, управляемый при помощи автоматики.

Экспериментальные системы умных домов умеют самостоятельно принимать решения, например, оставить ли включенным отопление, если жильцы вышли из дома, или закрыть форточку. А реальные системы позволяют конфигурировать почти любое оборудование в доме.

Подобная система должна обладать следующими свойствами:

- комфортность (система должна иметь интуитивный (естественный) интерфейс управления);

- масштабируемость (возможность добавления датчиков, при добавлении нового оборудования);

- конфигурируемость (возможность изменять поведение одного оборудования, в зависимости от показаний датчиков);

- доступная цена (система должна быть недорогой, чтобы окупиться как можно скорее и получить широкое распространение).

Исходя из всех этих свойств были разработаны несколько прототипов.

4.1 Прототип системы на основе смартфона

Так как критерием разрабатываемой системы является цена и конфигурируемость, то в системе применяется платформа разработки устройств – Arduino. Внешний вид Arduino представлен на рисунке 3.

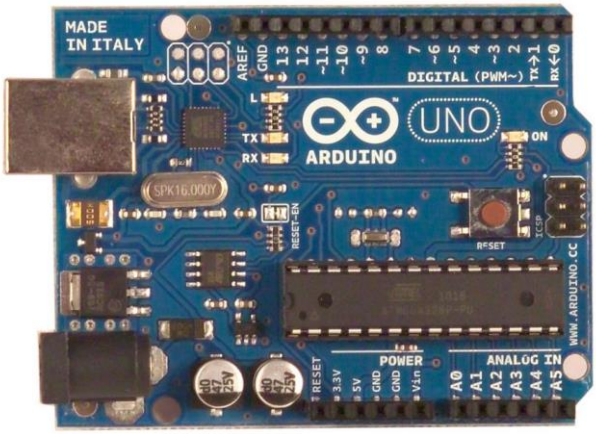

Рисунок 3 – Микроконтроллер Arduino

Критерий комфортность достигается путем включения в систему смартфона на базе ОС Android. Смартфон стал неотъемлемой частью жизни человека, обладает набором датчиков, графическим, командным, голосовым интерфейсом. Последний является наиболее удобным и естественным для человека.

На диаграмме 1 отображена доля ОС на смартфонах (на конец 2017 г.).

Голосовые команды распознает Android-приложение «Ассистент Дуся», где они им обрабатываются. Пользователь может сам настроить реакцию ассистента на них, путем создания скриптов, либо воспользовавшись готовыми. Интерфейс и меню скриптов представлены на рисунке 4. Скрипты, запускаются внутри ассистента, и посылают различные интенты (Intent) с параметрами отдельному приложению (сервису) без графического пользовательского интерфейса (GUI). При получении интента,

сервис открывает последовательное соединение (Serial) с Arduino через шину USB, и передает микроконтроллеру параметры, предварительно переведенные посимвольно в биты. Получив эти параметры, Arduino выполняет свою программу, выполняя определеные действия, такие как включение/выключение реле или поворот сервомотора на заданный угол и т.д.

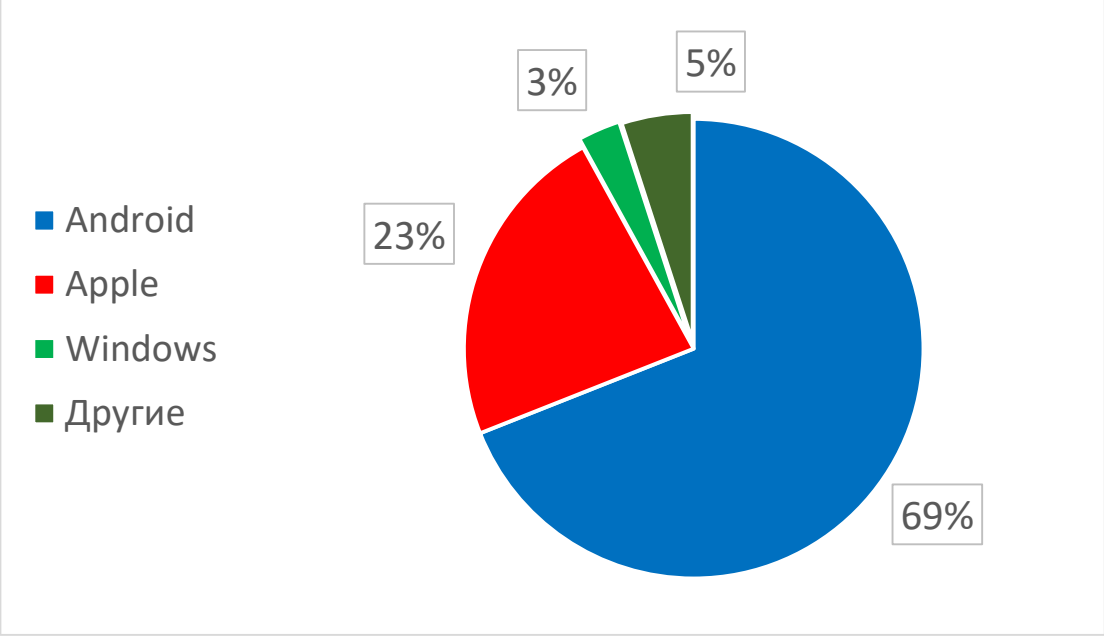

Диаграмма 1 – Доля ОС на рынке мобильных устройств

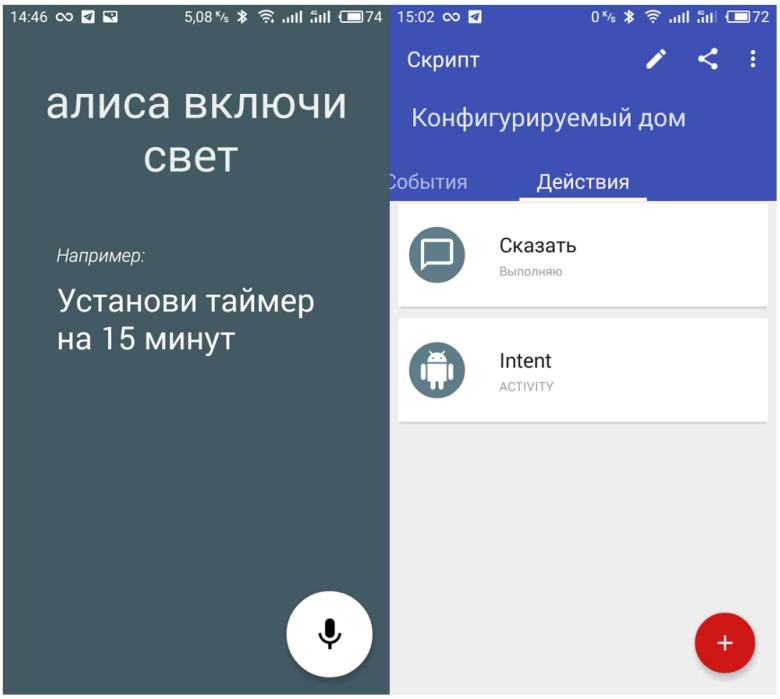

Рисунок 4 – Интерфейс главного экрана и меню скриптов ассистента «Дуся»

В последствие, для простоты отладки, приложению-сервису был добавлен графический интерфейс (рисунок 5).

Общая схема системы «Конфигурируемый дом» представлена на рисунке 6.

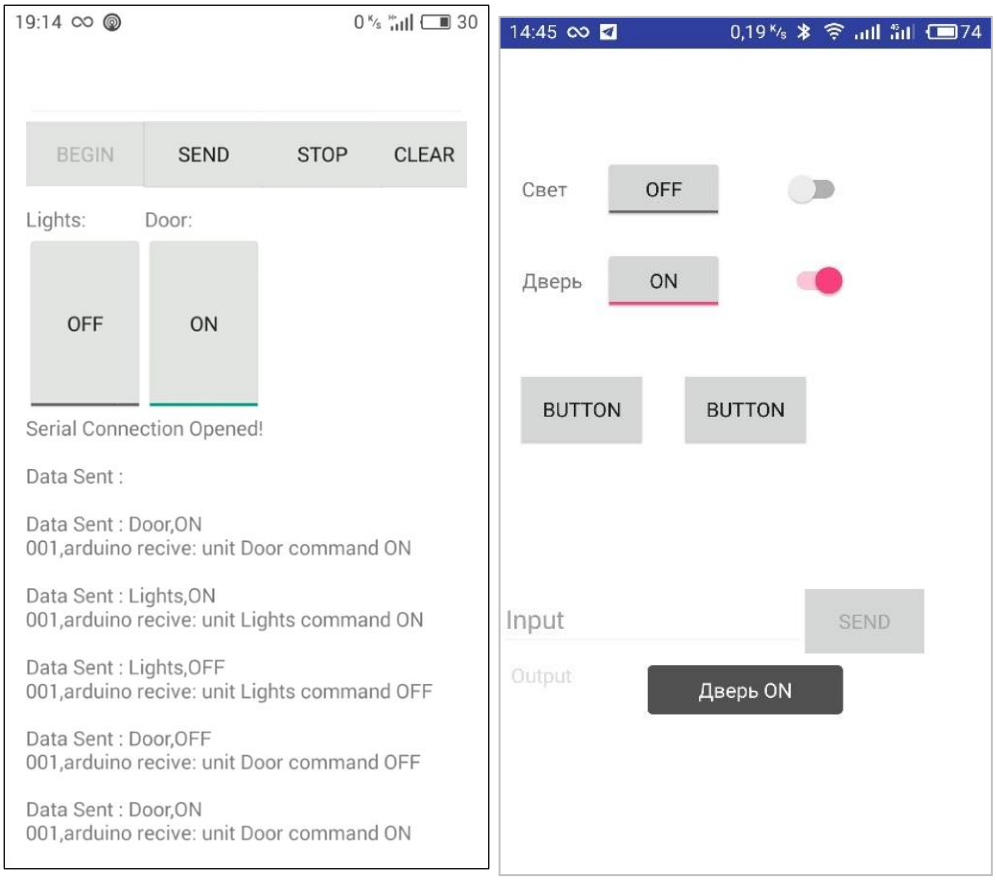

Рисунок 5 – Графический интерфейс приложения-сервиса

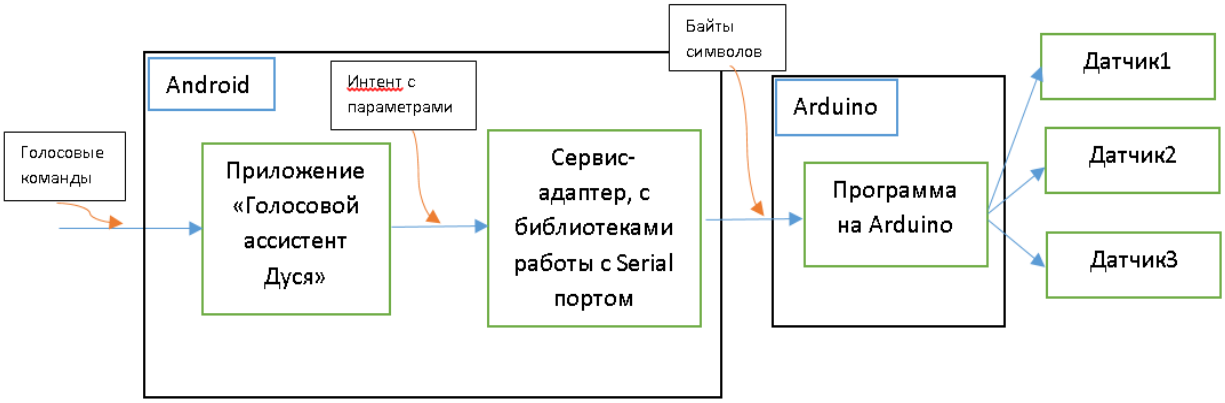

Рисунок 6 – Общая схема работы системы

Так же, имеется возможность замены шины USB на передачу данных с помощью Bluetooth-модуля (HC-05). Данный модуль подключается к Arduino проводами, и он так же использует Serial-соединение для передачи данных по Bluetooth-каналу.

Таким образом, пользователь получает возможность управлять отдельными объектами своего дома голосом с минимальными затратами на внедрение системы.

4.2 Прототип системы на основе локального сервера

После проведения анализа работы прототипа были выяснены некоторые недостатки. Одним из них – использование USB- и Bluetooth-соединения микроконтроллеров и смартфона, а именно преимущество в мобильности смартфона сводилось на нет (USB – 1.2м, Bluetooth – 3м). Поэтому была поставлена задача создать прототип системы на основе ЛВС.

Так как на данный момент практически у каждого в доме присутствует роутер с возможностью создания локальной сети по технологии Wi-Fi, то было принято решение заменить Arduino на платформу разработки устройств NodeMCU (рисунок 7).

NodeMCU – это платформа на основе модуля ESP8266. Плата предназначена для удобного управления различными схемами на расстоянии посредством передачи сигнала в локальную сеть или интернет через Wi-Fi. К ней и будет подключаться несколько датчиков/устройств (реле, датчики движения и т.д.).

Рисунок 7 – Внешний вид NodeMCU

В системе используется несколько NodeMCU, и все они подсоединяются через Wi-Fi к микрокомпьютеру Rasberry Pi.

Raspberry Pi – одноплатный компьютер компактного размера (рисунок 8). Имеет разъём HDMI для подключения монитора, USB-порты для подключения USB устройств, GPIO разъём для подключения низкоуровневой периферии, Ethernet-порт для подключения к сети. Используемая модель – RaspberryPi Model B имеет процессор ARM 700Ghz, 512Мб оперативной памяти.

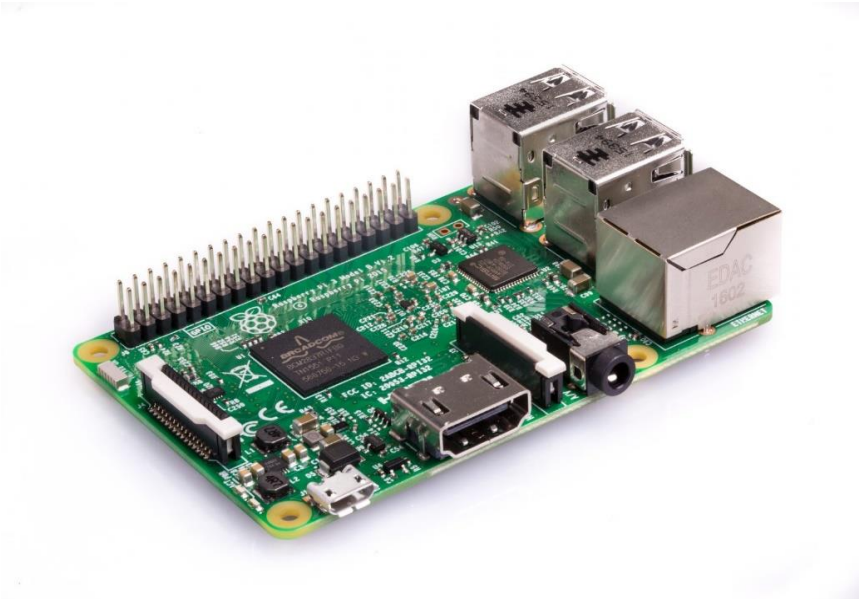

Рисунок 8 – Микрокомпьютер Raspberry Pi

Смартфон подсоединяется в данной системе к локальному серверу, который размещен на Raspberry Pi. Сервер – open-source сервер Blynk, позволяющий управлять различными микроконтроллерами и платами через различные протоколы, а именно обмениваться данными с ними посредством простых команд.

Общая схема представлена на рисунке 9.

Голосовые команды распознает Android-приложение «Ассистент Дуся». Пользователь также может сам настроить реакцию ассистента на голосовые команды, создав скрипт, либо воспользовавшись готовым.

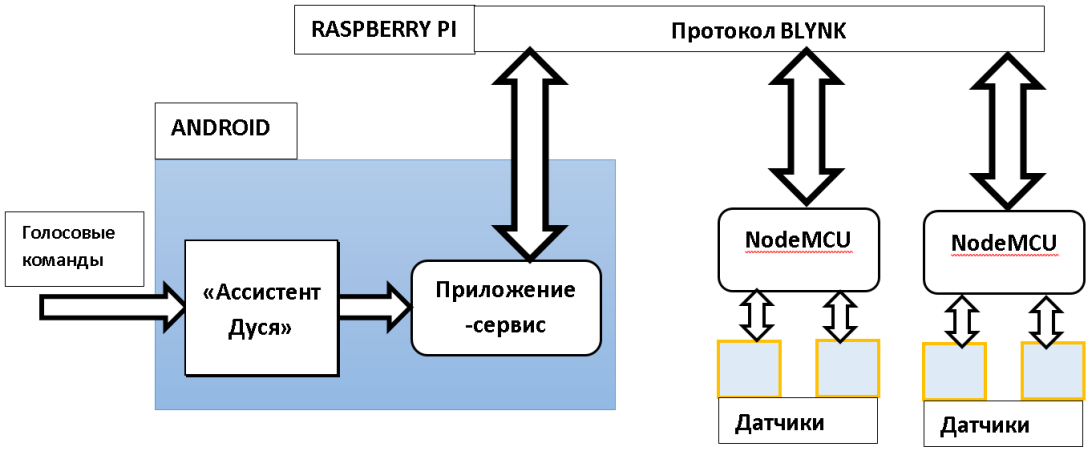

Рисунок 9 – Общая схема системы

При получении интента сервис открывает соединение (Wi-Fi, Bluetooth, USB) и передает через Raspberry Pi по протоколу Blynk в NodeMCU. Получив эти параметры, микроконтроллер выполняет свою программу, выполняя определенные действия, такие как включение/выключение реле или поворот сервомотора на заданный угол и т.д.

На данный момент, этот прототип размещен в доме, и используется для управления светом над рабочим столом, а также для автоматического (через промежуток времени и/или в зависимости от измеряемой влажности почвы) полива горшечных растений на подоконнике. Полив так же, как и управление светом, может быть осуществлен удаленно (из другой комнаты) по нажатию кнопки в приложении на смартфоне.

4.3 Разработка устройства отладки системы «SCHome»

Так как основным свойством системы является масштабируемость, то в системе возможно наращивание огромного количества всевозможных датчиков и оборудования. Это со временем приводит к сложностям дальнейшей установке, настройке, тестирования новых датчиков. Для решения этих трудностей, целесообразно разработать устройство отладки системы.

Данное устройство должно выполнять следующие функции:

- отображение списка микроконтроллеров, включенных в систему;
- отображение списка оборудования, подключенное к системе;
- отображение текущего состояния микроконтроллеров, портов входа-выхода;
- изменение логического сигнала на выходах микроконтроллеров;
- считывание данных с модуля акселерометра и пульсометра, подключенных к устройству и передача их в систему.

Данное устройство должно быть мобильным, беспроводным, поэтому оно должно получать электроэнергию от съемного аккумулятора. Обмен данными должен происходить через беспроводной канал связи.

Проанализировав информацию в интернете, мы обнаружили подходящие типы беспроводной связи на основе 4 модулей (рисунок 10):

nRF24L01+ – Модуль NRF24L01 позволяет передавать данные через радиоканал частотой 2,4ГГц, скоростью 250–2000 Кбит/сек. Особенностью данного модуля является его низкая цена, широкий диапазон каналов, дальность приема сигнала до 100м по прямой видимости, наличие «спящего» режима, незащищенное соединение «точка-точка» со вторым аналогичным модулем.

HC-06 – Беспроводной модуль для приема/передачи данных в Arduino проектах по протоколу Bluetooth. Радиус действия до 10 м, Скорость передачи данных составляет 1200–1382400 бод, рекомендуемое напряжение 6В.

LoRaWAN module – Беспроводной модуль предачи данных по радиоканалу частотой 868МГц. Особенностью является экстремально большая

дальность передачи (свыше 20 км) за счет низкой скорости передачи данных (250-5470 бит/сек), высокая цена.

ESP8266-12E – Беспроводной модуль передачи данных по WiFi (протокол 802.11 b/g/n) частотой 2,4ГГц. Имеет разные режимы работы (в том числе и низкого энергопотребления), высокую скорость передачи данных, низкая цена, WPA/WPA2 шифрование.

Из этих вариантов наиболее подходит модуль ESP8266-12E (далее ESP) – так как, во-первых, обладает низкой ценой, во-вторых, канал передачи данных шифруется, и в-третьих, в отличие от остальных модулей, ему не требуется приемное устройство, представляющее собой второй аналогичный модуль. ESP передает обменивается данными с системой «Конфигурируемый дом» напрямую, через WiFi-роутер, который уже использует система.

Для реализации логики на стороне разрабатываемого устройства необходимо включить в него микроконтроллер или использовать вычислительные возможности самого ESP. Для простоты разработки устройства было решено использовать платформу разработки устройств NodeMCU.

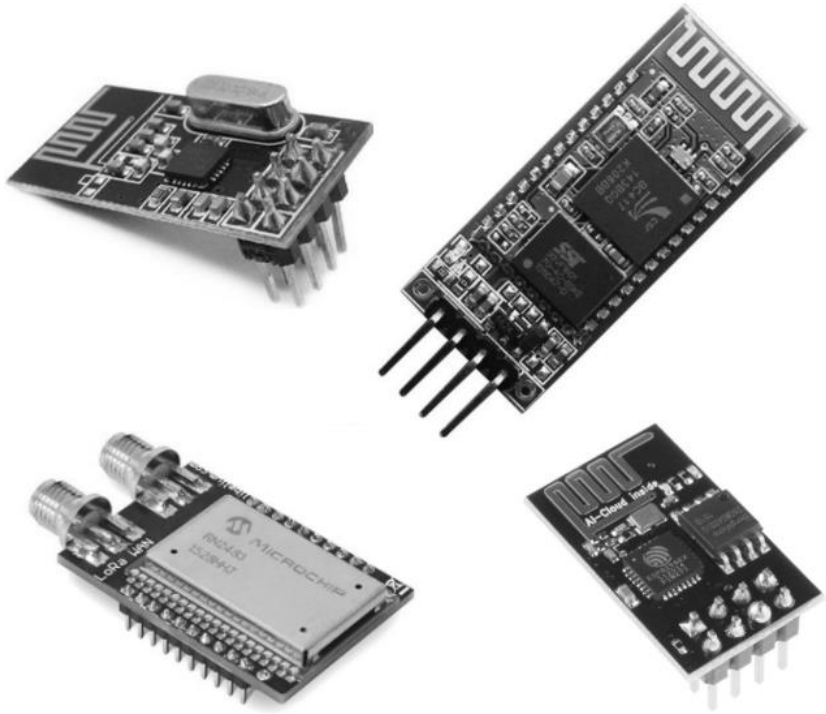

Рисунок 10 – Беспроводные модули nRF24L01+, HC-06, LoRaWAN module, ESP8266-12E

NodeMCU платформа на основе модуля ESP. Микропроцессор ESP обладает тактовой частотой 80 МГц (возможно повысить до 160 МГц). Также NodeMCU обладает 4 Мб Flash-памяти. Размер платы NodeMCU — 6 * 3 см. Плата довольно компактная, это позволяет использовать ее в малогабаритных устройствах. Выводы NodeMCU расположены так, что ее без проблем можно установить в макетную плату (breadboard). На лицевой части платы разъем Micro USB, через который загружаются программы(скетчи).

Именно к NodeMCU подключаются все остальные датчики устройства отладки:

1) LCD-дисплей MT-16S2H – индикация 2-х строк по 16 символов;

2) энкодер (датчик угла) – инкрементный с кнопкой;

3) CJMU-10DOF – модуль, состоящий из гироскопа, акселерометра, магнитометра, барометра/термометра;

4) MAX30100 – датчик оптоэлектронный измерения пульса.

На LCD-дисплей выводится текущая информация, полученная NodeMCU от системы или от датчиков CJMU-10DOF, MAX30100. Энкодером осуществляется навигация по программе NodeMCU (прокрутка списков устройств, выбор одного из них, установка логического уровня на выходе и т.п.). Дисплей подключен через шину передачи данных SPI, когда как CJMU-10DOF, через шину I2C.

Общая схема устройства представлена на рисунке 11.

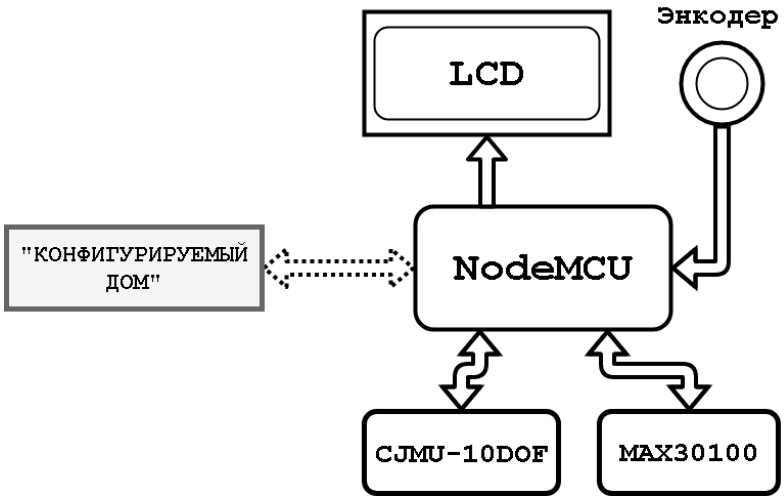

Рисунок 11 – Общая схема устройства отладки

На данный момент собран прототип отладочного устройства, и были выявлены следующие моменты:

1) значительную часть электроэнергии потребляет LCD-дисплей;

2) LCD-дисплей занимает большую часть выходов NodeMCU (8 из 13 имеющихся цифровых выходов);

3) размер экрана позволяет выводить на него очень мало информации одновременно;

4) данные об устройствах хранятся только до перезагрузки устройства.

Первые три проблемы решаются заменой LCD-дисплея на OLED-дисплей, который имеет пониженное энергопотребление, соединяется с NodeMCU по шине I2C (2 из 13 цифровых выходов) и имеет достаточный размер для отображения информации (128 точки на 64 точек). Есть два решения четвертой проблемы: хранить данные в системе «SCHome» или хранить данные на SD-карте, подключенной через модуль считывания SD-карт к NodeMCU.

В итоге, разработка удобного рабочего прототипа отладочного устройства приведет к ускорению внедрения и отладки системы «Конфигурируемый дом».

4.4 Разработка интернет-магазина для системы «SCHome»

В настоящее время Интернет становится все более развитой средой для осуществления коммуникаций с потребителями. В тоже время, существенным является и тот факт, что Интернет становиться удобной и достаточно дешевой «торговой площадкой». Все большее количество фирм старается представить свою продукцию в on-line среде. При этом такое представление не ограничивается только лишь созданием промо-сайтов и размещением рекламных баннеров и статей в электронных журналах и на информационных порталах. С развитием Интернет-среды развивается и само предложение. Теперь люди могут не только получать интересующую их информацию, но и совершать покупки. При этом с помощью Интернет-магазинов можно приоб-

ретать товары совершенно разных категорий, как элементарные потребительские, так и высокотехнологичные.

Интернет-магазин – это сайт, содержащий подробный каталог товаров с описанием и изображением. Основное отличие от обычного интернет-каталога состоит в том, что товары, представленные в интернет-магазине можно не только увидеть, но и заказать, не вставая с места и не прерывая увлекательного путешествия по просторам Интернет. При этом каждый Интернет-магазин обладает собственной базой данных, где хранится информация о покупателях и о продажах товаров.

Для того чтобы распространить систему «SCHome», было решено разработать Интернет-магазин. В ходе разработки был получено техническое задание и Интернет-магазин (работающий в тестовом режиме).

Целями и задачами, которые должен решать сайт, является розничная продажа через Интернет магазин комплектов готовых решений системы, а также реализация технической поддержки покупателей.

На начальном этапе были сформулированы требования к дизайну.

1) стиль сайта: простой, легкий, удобный.

2) впечатление, которое должен произвести сайт на пользователя: внушить доверие, показать, что на сайте предлагается качественная продукция.

3) в результате посещения сайта пользователь должен увидеть товары и полезную информацию, почувствовать удобство, уверенность в профессионализме продавца, и совершить покупку.

4) обязательные элементы для всех страниц: логотип, контактные данные компании.

5) примерная желаемая цветовая гамма: белый, серый, синий.

6) основные требования к графическому дизайну: простой, легкий, не мешающий восприятию информации и навигации.

Интернет-магазин(сайт) компании состоит из нескольких модулей:

1) новости (должна отображаться информация об акциях, обновление каталога товара и т.п.);

2) информация об организации

3) каталог товаров (отображает информацию о товарах: их описание, цену, фото)

4) FAQ (здесь покупатель может ознакомиться с ответами на часто задаваемыми вопросами)

5) форма заказа товаров.

6) форум (здесь покупатель может задать свой вопрос, если не нашел ответа в FAQ).

Сайт написан на языке PHP версии 7.1, а в качестве базы данных(БД) используется MySQL. БД должна хранить информацию о зарегистрированных пользователях сайта, покупателях, товарах, заказах, а также хранить содержание новостей и форума.

Основные функциональные подсистемы Интернет-магазина:

- функциональная информационная подсистема сайта предназначена для информирования пользователей, она включает информацию о магазине, новости, рекламную информацию о товарах, контактную информацию;

- коммуникативная функциональная подсистема – присутствует система обратной связи, обеспечивающая взаимодействие с клиентами – контактная информация: адрес, телефон, адрес электронной почты;

- административная функциональная подсистема сайта включает в себя регистрацию, и авторизацию клиентов Интернет-магазина для оказания технической поддержки;

- функциональная подсистема осуществления интернет-торговли, обеспечивающая выбор и заказ товаров.

Логическая структура представлена на рисунке 26.

Физическая структура сайта представляет собой совокупность структурированных файлов, распределенных в файловой системе по иерархическому принципу. Физическая структура сайта представлена на рисунках 12-14.

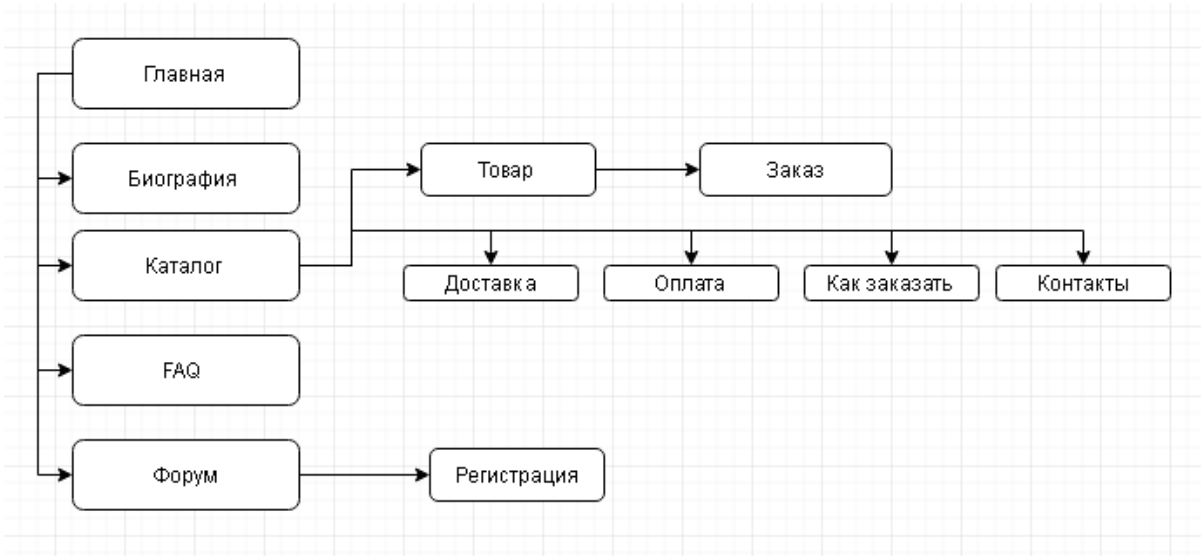

Рисунок 12 – Логическая структура сайта

boot	Папка с ф...	04.04.2017 23:1...	drwx------	6607 601
css	Папка с ф...	04.04.2017 23:4...	drwx------	6607 601
js	Папка с ф...	05.05.2017 22:3...	drwx------	6607 601
pic	Папка с ф...	09.05.2017 21:2...	drwx------	6607 601
public_html	Папка с ф...	28.04.2017 1:13...	drwx------	6607 601

Рисунок 13 – Физическая структура сайта

bio.php	195	Файл "PHP"	08.04.2017 13:1...	-rw-------	6607 601
bootstrap-collapse.js	4 398	файл Java...	08.04.2017 13:1...	-rw-------	6607 601
bootstrap.js	69 707	файл Java...	08.04.2017 13:1...	-rw-------	6607 601
creative.php	1 251	Файл "PHP"	09.05.2017 23:1...	-rw-------	6607 601
faq.php	74	Файл "PHP"	08.04.2017 13:1...	-rw-------	6607 601
forum.php	3 906	Файл "PHP"	08.04.2017 13:1...	-rw-------	6607 601
index.php	1 153	Файл "PHP"	09.04.2017 13:1...	-rw-------	6607 601
item.php	2 369	Файл "PHP"	07.05.2017 0:18...	-rw-------	6607 601
login.php	8 065	Файл "PHP"	10.05.2017 0:03...	-rw-------	6607 601
mail.php	4 610	Файл "PHP"	05.05.2017 23:5...	-rw-------	6607 601
mailmessage.php	1 575	Файл "PHP"	05.05.2017 23:5...	-rw-------	6607 601
model.php	2 929	Файл "PHP"	05.05.2017 23:1...	-rw-------	6607 601
order.php	4 983	Файл "PHP"	06.05.2017 0:00...	-rw-------	6607 601
register.php	2 760	Файл "PHP"	08.04.2017 13:1...	-rw-------	6607 601
tempBott.php	738	Файл "PHP"	10.05.2017 0:06...	-rw-------	6607 601
tempTop.php	5 877	Файл "PHP"	09.05.2017 23:4...	-rw-------	6607 601

Рисунок 14 – Физическая структура сайта (содержимое папки public_html)

Файловая система сайта, где приведено назначение каждого файла представлена в таблице 2.

Таблица 2 – Файловая система сайта

Название файла	Назначение файла
boot	Каталог, содержащий bootstrap-файлы (css, js)
css	Каталог, содержащий файлы стилей сайта
js	Каталог, содержащий JavaScript-файлы
pic	Каталог, содержащий используемые на сайте изображения
bio.php	Файл страницы Биография
bootstrap-collapse.js	Bootstrap-плагин
bootstrap.js	Bootstap-плагин
creative.php	Файл каталога
faq.php	Файл страницы FAQ
forum.php	Файл страницы Форум
index.php	Файл главной страницы
item.php	Файл карточки товара
login.php	Файл, реализующий авторизацию пользователя на странице forum.php
mail.php	Файл, содержащий в себе функцию отправки письма
mailmessage.php	Файл, содержащий шаблон письма, отправляемого пользователю после заказа товара
model.php	Файл, содержащий SQL-запросы к БД
order.php	Файл, содержащий форму заказа, некоторые запросы к БД
register.php	Файл, реализующий регистрацию пользователей на сайте
tempBott	Файл, содержащий шаблон подвала
tempTop	Файл, содержащий шаблон шапки

Стилевое решение шапки и главного меню сайта представлено на рисунке 15.

Рисунок 15 – Шапка и главное меню сайта

Стилевое решение подвала сайта представлено на рисунке 16. Цветовые спецификации можно рассмотреть на рисунке 17.

Рисунок 16 – Подвал сайта

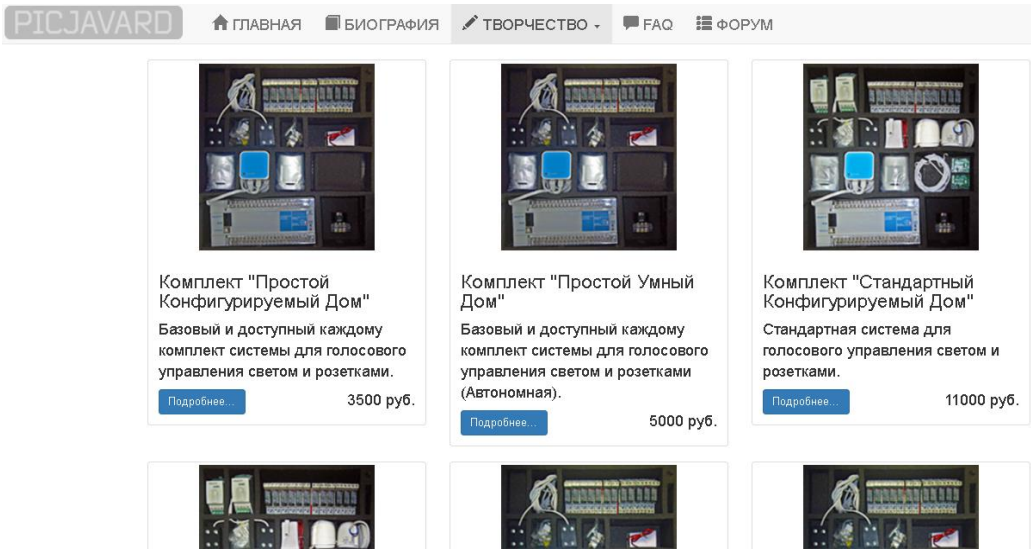

Рисунок 17 – Цветовые спецификации

Интернет-магазин включает в себя базу данных, в которой хранится различная информация. База данных будет содержать информацию о новостях, а именно заголовок новости, содержание новости, дату размещения новости, а также путь к размещенному на сервере изображению к новости. Для отображения каталога товаров необходимы название товара, краткое описание товара, полное описание товара, цена, и путь к размещенному на сервере изображению товара. Для осуществления работы форума в БД будет храниться дата и время размещения сообщения содержание сообщения, и при необходимости пути к размещенным на сервере изображениям, прикрепленные зарегистрированными пользователями к сообщению. Для возможности оставлять вопрос на форуме БД должна хранить информацию о зарегистрированных пользователях, а именно логин, пароль, его IP-адрес. Также для разграничения групп пользователей (обычный пользователь, модератор на

форуме, администратор, редактор, оператор по техобслуживанию) – путь к размещенному на сервере изображению пользователя(аватара), дата регистрации/получения прав модератора, и соответственно номера групп. БД должна хранить информацию о заказе, а именно – название товара, ФИО покупателя, его электронный почтовый ящик, номер телефона, способ доставки, город, почтовый индекс, адрес (улица, дом, квартира), способ оплаты, а также статус заказа.

На основе информации хранящейся в БД будет осуществляться авторизация пользователей, редактирование контента сайта (новости, информация о товаре и т.д.), формирование письма с данными о заказе, а операторами Call-центра осуществляться поиск и изменение информации о заказе.

В результате проектирования и реализации были выделены и сформированы следующие сущности, описанные в таблице 3, разработана концептуально-инфологическая модель (рисунок 18-19).

Таблица 3 – Спецификация сущностей

Название сущности	Описание сущности	Количество экземпляров
users	Содержит информацию о зарегистрированных пользователях	неогр.
personal	Содержит информацию о личном кабинете пользователя	неогр.
order	Содержит информацию о заказах	неогр..
news	Хранит данные о новостях и акциях	1000
item	Хранит информацию о товарах	100
image	Содержит в себе пути и имена изображений	неогр.
chat	Хранит информацию о сообщениях на форуме	неогр.

В результате был получен Интернет-магазин готовых решений системы «SCHome».

Данный Интернет-магазин создан для:

1) информирования постоянных покупателей о поступлении новой продукции;

2) привлечения новых потенциальных потребителей;

3) автоматизации получения заявок на покупку товаров;

4) продвижения торговой организации «SaLaDe» в Интернете.

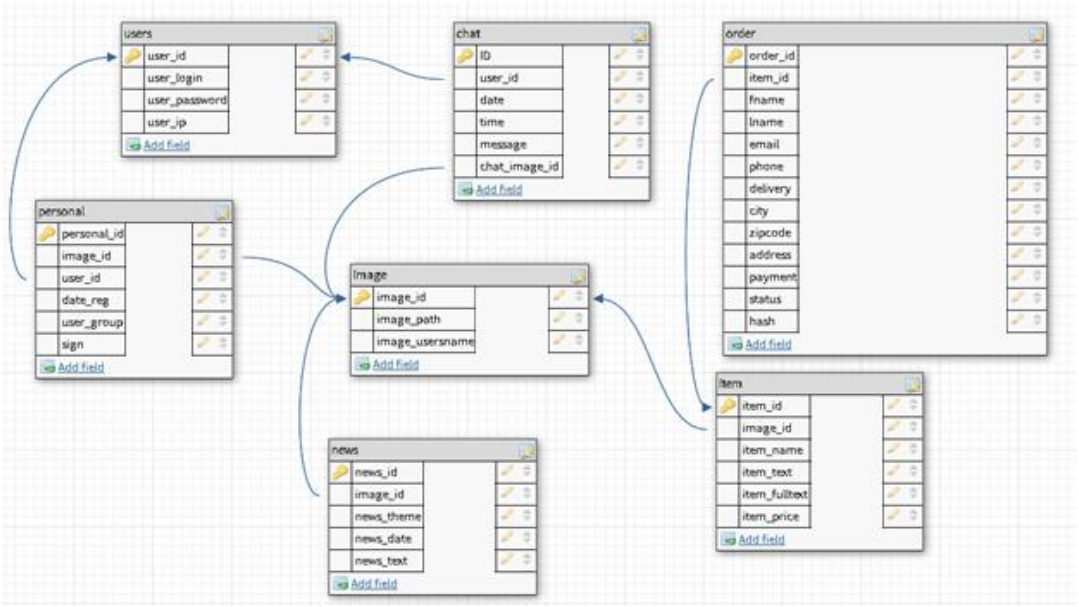

Рисунок 18 – Концептуально-инфологическая модель. Логический уровень

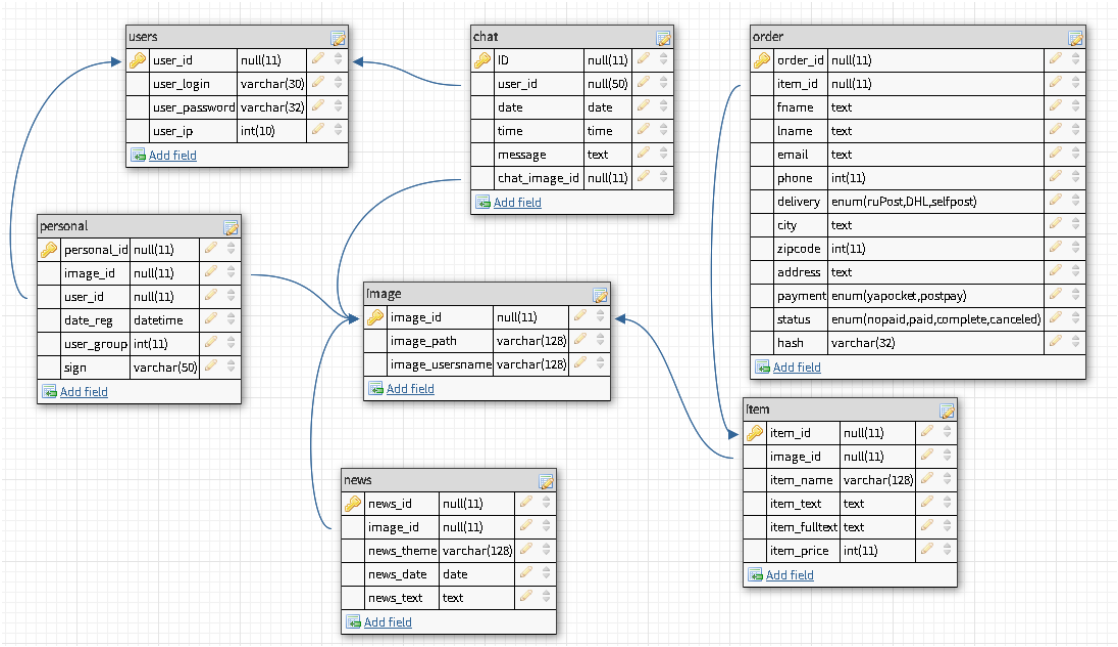

Рисунок 19 – Концептуально инфологическая модель. Физический уровень

При разработке сайта были проанализированы современные веб-технологии, позволяющие создавать сайты, сформулированы техническое задание, структура сайта, разработан дизайн и спроектирована база данных.

Наиболее подходящими для разработки веб-приложения были выбраны следующие средства: PHP, JavaScript, CSS, и MySQL.

4.5 Дальнейшее развитие системы «SCHome»

Необходимо произвести довольно большой объем работ, для того чтобы система стала достаточно популярной в пределах дальневосточного федерального округа, а также уменьшения результата соотношения «цена/качество».

К примеру, для реализации удобного для пользователя голосового интерфейса необходимо соглашение с разработчиком приложения «Ассистент Дуся» о предоставлении API приложения взамен на сотрудничество (партнерство). А это предполагает, в свою очередь, создания юридического лица, в виде индивидуального предпринимателя или организации, что ведет к дополнительным расходам. Помимо этого, необходимо так же связаться с компанией-разработчиками Blynk-протокола, чтобы уточнить вопросы о механизмах обеспечения безопасности передачи данных, реализованным этим протоколом.

Так как прототипы уже спроектированы, то теперь для увеличения эффективности системы необходимо подобрать компоненты (микроконтроллеры, датчики), которые устарели за время разработки прототипов. К этому относится и NodeMCU – необходимо избавиться от ненужных компонентов, присутсвующих на данной плате – в дальнейшем, закупать отдельные модули ESP8266-12, так как они имеют в разы меньший размер, и прошивать их уже разработанной программами для прототипа.

Для отладочного устройства также нужно подобрать более дешевые или более востребованные компоненты (сенсорный экран), подготовить печатную плату, на которой будут они размещены, смоделировать и распечатать на 3D-принтере корпус, разработать крепеж, с помощью которого устройство будет крепиться на руке. Все это необходимо проработать, прежде чем устройство отладки превратится в удобный для конечного пользова-

теля инструмент управления системой «SCHome». Также планируется переработка устройства в полноценный коммуникатор.

Для массового распространения системы необходимо вывести Интернет-магазин из тестового режима, но перед этим необходимо продумать, состав, оформление, цену продаваемого продукта (самосборных, полусборных или готовых комплектов системы). Вариантов доставки и оплаты должно быть достаточно много, на главной странице периодически должны возникать новости (пополнения товара, новинки, акции), для привлечения/удержания аудитории в магазине. Форум, Тех.поддержка должны постоянно и безотказно работать. И нельзя забывать про продвижение проекта в целом в СМИ и соц.сетях. Все это требует человеческих ресурсов, а именно персонала, который будет заниматься этими вопросами.

На данный момент, скорость разработки данной системы минимальна – для ускорения разработки необходимо привлекать в команду разработчиков новых программистов, радиоэлектротехников, электриков, специалистов в области «Интернет вещей» и «Умный дом», веб-разработчиков, SSM-специалистов.

После решения всех вопросов и проблем, описанных выше, в каждой установленной в домах, и особенно на предприятиях, системе будет находится огромное количество датчиков. Поэтому может возникнуть очередная проблема обработки большого потока входящих данных. Для решения этой проблемы рационально будет использовать технологию нейросетей.

5 РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ СИСТЕМЫ «SCHOME»

5.1 Установка фаервола (Firewall)

Для Linux доступно множество брандмауэров. Большинство из них используют базовый проект iptables для обеспечения фильтрации пакетов. Этот проект находится над системой netfiltering Linux. Iptables устанавливается по умолчанию на Raspbian, но не настроен. Настройка его может быть сложной задачей, и существует один проект, который обеспечивает более простой интерфейс, чем iptables, – UFW, что означает «Uncomplicated Fire Wall». Это инструмент брандмауэра по умолчанию в Ubuntu и может быть легко установлен на Raspberry Pi:

```
sudo apt install ufw
```

Рисунок 20 – Установка UFW

UFW – довольно простой инструмент командной строки, хотя для него есть некоторые графические интерфейсы. Ниже будут описаны некоторые из основных параметров командной строки. Обратите внимание, что UFW нужно запускать с привилегиями суперпользователя, поэтому всем командам предшествует sudo. Также возможно использовать опцию --dry-run любые команды UFW, которые указывают на результаты команды без внесения каких-либо изменений.

Включение брандмауэра, который также обеспечит его запуск при загрузке:

```
sudo ufw enable
```

Рисунок 21 – Включение службы брандмауэра

Отключение брандмауэра и отключение запуска при загрузке:

```
sudo ufw disable
```

Рисунок 22 – Выключение службы брандмауэра

Разрешение определенному порту иметь доступ:

```
sudo ufw allow 22
```

Рисунок 23 – Разрешение на доступ к порту

Отказ в доступе на порт также очень прост:

```
sudo ufw deny 22
```

Рисунок 24 – Запрет на доступ к порту

Вы также можете указать, какую службу вы разрешаете или отказываете в порту:

```
sudo ufw deny 22/tcp
```

Рисунок 25 – Запрет службы в порту

Указание сервиса, если вы известен порт, который он использует. В этом примере доступ службы ssh через межсетевой экран:

```
sudo ufw allow ssh
```

Рисунок 26 – Разрешение службы

В команде status перечислены все текущие настройки брандмауэра:

```
sudo ufw status
```

Рисунок 27 – Получение служебной информации

Правила могут быть довольно сложными, позволяя блокировать определенные IP-адреса, указывая, в каком направлении разрешен трафик, или

ограничивать количество попыток подключения, например, чтобы помочь победить атаку «Отказ в обслуживании» (DoS). Вы также можете указать, что правила устройства должны применяться к (например, eth0, wlan0). Для получения подробной информации см. Справочную страницу ufw (man ufw), но здесь приведены примеры более сложных команд.

Ограничить попытки входа в ssh-порт с помощью tcp: это отрицает соединение, если IP-адрес попытался подключиться шесть или более раз за последние 30 секунд:

```
sudo ufw limit ssh/tcp
```

Рисунок 28 – Получение служебной информации

Запретить доступ к порту 30 с IP-адреса 192.168.2.1:

```
sudo ufw deny from 192.168.2.1 port 30
```

Рисунок 29 – Пример реализации блокировки доступа

5.2 Настройка VPN

При реализации удаленного доступа к системе лучше всего использовать технологию VPN.

VPN создается на базе общедоступной сети Интернет. И если связь через Интернет имеет свои недостатки, главным из которых является то, что она подвержена потенциальным нарушениям защиты и конфиденциальности, то VPN могут гарантировать, что направляемый через Интернет трафик так же защищен, как и передача внутри локальной сети. В тоже время виртуальные сети обеспечивают существенную экономию затрат по сравнению с содержанием собственной сети глобального масштаба.

Для того чтобы была возможность создания VPN на базе оборудования и программного обеспечения от различных производителей необходим некоторый стандартный механизм. Таким механизмом построения VPN является протокол Internet Protocol Security (IPSec). IPSec описывает все стандартные

методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования, используемые конечными точками туннеля и механизмы обмена и управления ключами шифрования между этими точками. Из недостатков этого протокола можно отметить то, что он ориентирован на IP.

Другими протоколами построения VPN являются протоколы PPTP (Point-to-Point Tunneling Protocol), разработанный компаниями Ascend Communications и 3Com, L2F (Layer-2 Forwarding) – компании Cisco Systems и L2TP (Layer-2 Tunneling Protocol), объединивший оба вышеназванных протокола. Однако эти протоколы, в отличие от IPSec, не являются полнофункциональными (например, PPTP не определяет метод шифрования)

Говоря об IPSec, нельзя забывать о протоколе IKE (Internet Key Exchange), позволяющем обеспечить передачу информации по туннелю, исключая вмешательство извне. Этот протокол решает задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами, в то время как IPSec кодирует и подписывает пакеты. IKE автоматизирует процесс передачи ключей, используя механизм шифрования открытым ключом, для установления безопасного соединения. Помимо этого, IKE позволяет производить изменение ключа для уже установленного соединения, что значительно повышает конфиденциальность передаваемой информации.

Инкапсуляция – обеспечивает мультиплексирование нескольких транспортных протоколов по одному каналу;

Протокол LCP – PPP задает гибкий LCP для установки, настройки и проверки канала связи. LCP обеспечивает согласование формата инкапсуляции, размера пакета, параметры установки и разрыва соединения, а также параметры аутентификации. В качестве протоколов аутентификации могут использоваться PAP, CHAP и др.;

Протоколы управления сетью – предоставляют специфические конфигурационные параметры для соответствующих транспортных протоколов. Например, IPCP протокол управления IP.

Для формирования туннелей VPN используются протоколы PPTP, L2TP, IPsec, IP-IP.

Протокол PPTP – позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например, Internet.

Протокол L2TP – позволяет шифровать и передавать IP-трафик с использованием любых протоколов, поддерживающих режим “точка-точка” доставки дейтаграмм. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (ATM).

Протокол IPsec – позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям.

Протокол IP-IP – IP-дейтаграмма инкапсулируется с помощью дополнительного заголовка IP. Главное назначение IP-IP – туннелирование многоадресного трафика в частях сети, не поддерживающих многоадресную маршрутизацию.

Для технической реализации VPN, кроме стандартного сетевого оборудования, понадобится шлюз VPN, выполняющий все функции по формированию туннелей, защите информации, контролю трафика, а нередко и функции централизованного управления.

Для организации VPN «тунелирования» необходимо развернуть сервер VPN в системе, а именно в Raspberry Pi (где уже развернут сервер Blynk), а также выполнить проброс портов на роутере, и настроить подключение на удаленном устройстве пользователя.

Для развертывания VPN сервера необходимо выполнить последовательность действий:

1 этап – установка пакета VPN.

sudo apt-get install pptpd

2 этап – редактирование настройки VPN сервера(pptpd-options).

sudo nano /etc/ppp/pptpd-options

name pptpd

refuse-pap

refuse-chap

refuse-mschap

require-mschap-v2

require-mppe-128

ms-dns 8.8.8.8

nodefaultroute

lock

nobsdcomp.

3 этап – редактирование настройки VPN сервера(pptpd.conf).

sudo nano /etc/pptpd.conf

option /etc/ppp/pptpd-options

logwtmp

localip 192.168.0.1

remoteip 192.168.18.2-254

bcrelay eth0, где localip — «Внутренний» IP адрес VPN сети сервера (обычно, 192.168.0.1), remoteip — диапазон IP адресов, которые сервер будет выдавать подключенным компьютерам.

4 этап – настройка пользователей VPN.

nano /etc/ppp/chap-secrets

username pptpd password *, где username — имя пользователя VPN,password — его пароль.

nano /etc/sysctl.conf

net.ipv4.ip_forward=1

nano /etc/rc.local

PPTP IP forwarding

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

5 этап – перезагрузка Raspberry Pi.

reboot

Все выше перечисленные действия выполняются в командной строке Raspberry Pi, внешний вид которой представлен на рисунке 30

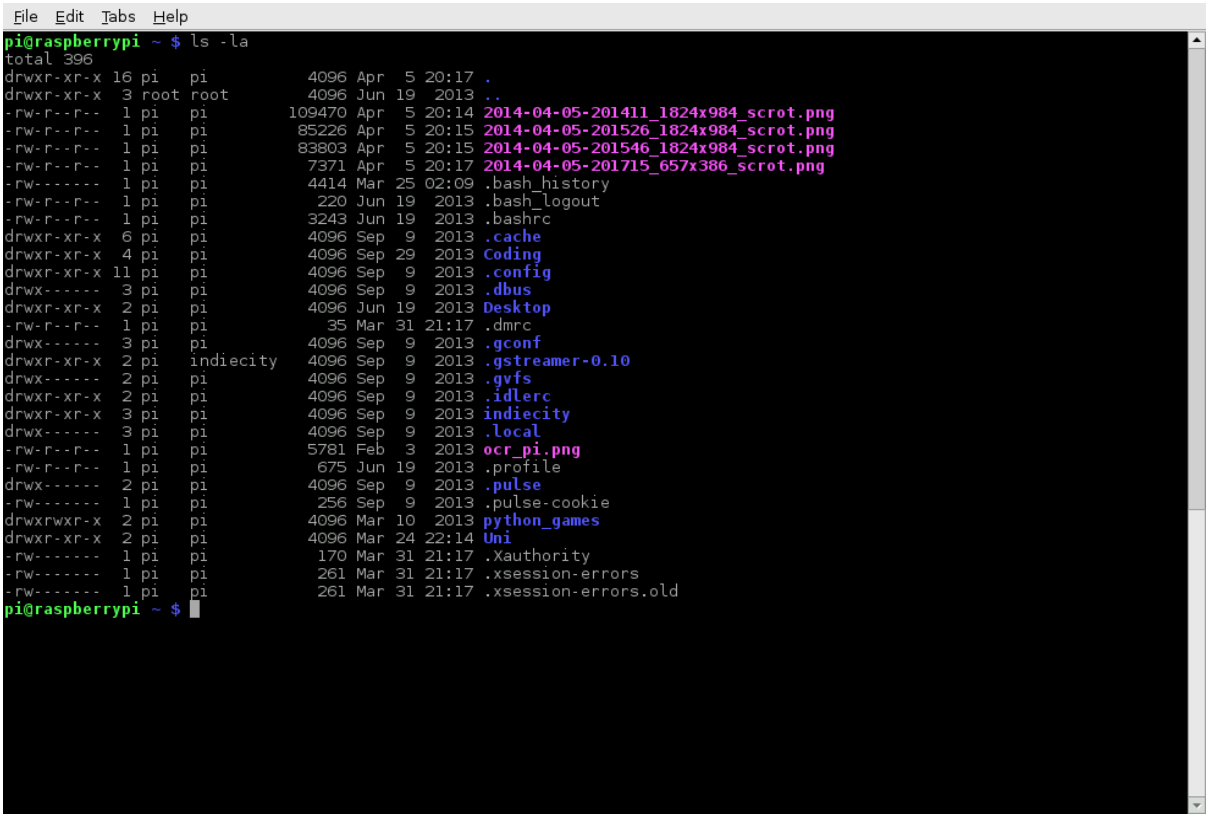

Рисунок 30 – Внешний вид консоли Raspberry Pi

Для настройки на удаленном устройстве пользователя (смартфон) необходимо скачать любое приложение для соединения по VPN из Play Market. Затем в настройках указать адрес подключения. Графический интерфейс представлен на рисунке 31.

В данном приложении реализованы принципы идентификации и аутентификации (рисунок 32).

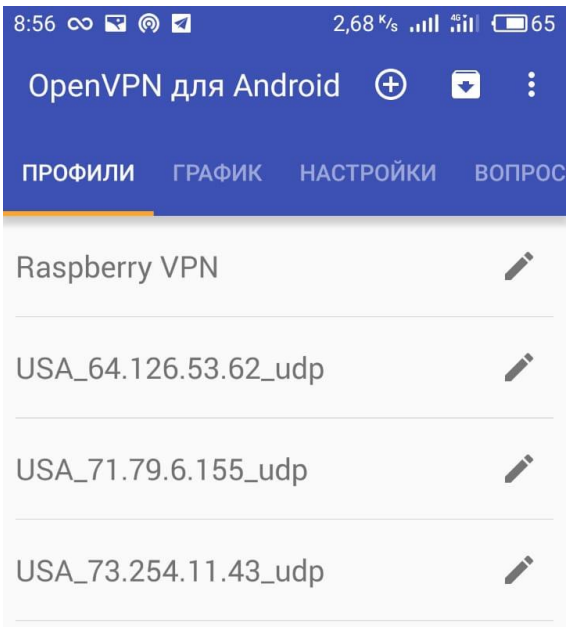

Рисунок 31 – Графический интерфейс приложения для соединения к VPN

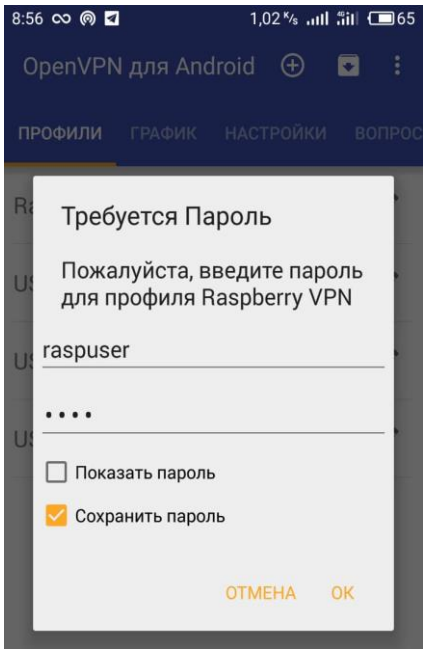

Рисунок 32 – Окно авторизации приложения

Общая схема ЛВС системы после проведения мероприятий по повышению защиты информации представлена на рисунке 33.

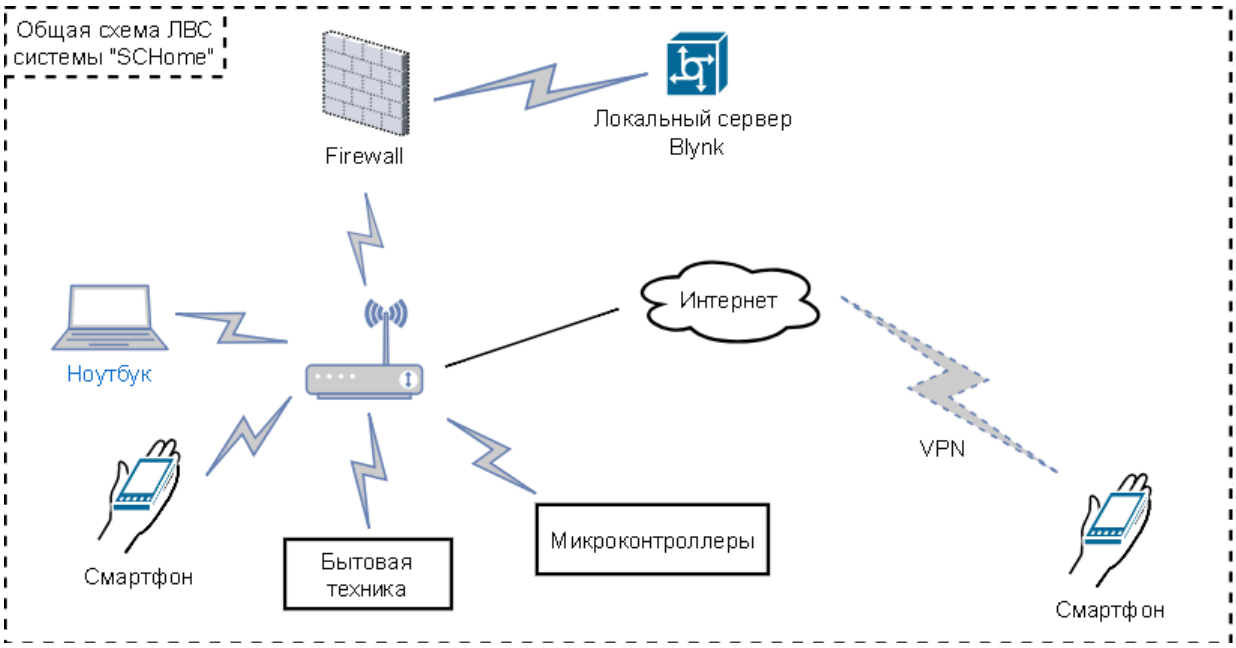

Рисунок 33 – Улучшенная схема ЛВС системы

6 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

Полноценное функционирование Интернет-магазина и технической поддержки системы подразумевает наличие рабочих мест, а те – наличие помещения, где они размещены. Поэтому необходимо организовать данные места в соответствии нормативными документами и стандартами (СанПин) а также побеспокоиться об сохранении здоровья сотрудников при работе с ЭВМ, разработав рекомендации и комплекс физических упражнений.

6.1 Безопасность

6.1.1 Опасные и вредные факторы на рабочем месте пользователя ПЭВМ

При работе с ЭВМ необходимо соблюдать требования, установленные стандартом СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

По ГОСТу 12.0.003-2015 при работе с ПЭВМ опасными и наносящими вред здоровью факторами являются:

- электростатические поля;
- электромагнитное излучение;
- опасность поражения электрическим током;
- повышенная или пониженная температура воздуха рабочей зоны;
- выделение в воздух рабочей зоны ряда химических веществ;
- повышенная или пониженная влажность воздуха;
- отсутствие или недостаток естественного света;
- недостаточная искусственная освещенность рабочей зоны;
- утомляемость глаз;
- монотонность трудового процесса;
- нервно-эмоциональные перегрузки;
- повышенный уровень шума.

Для предотвращения или снижения действий различных вредных факторов на пользователя ПЭВМ были сформулированы требования, предъявля-

емые к помещениям, освещению, уровню шума, к организации рабочего места, а также разработаны рекомендации к пользователю ПЭВМ.

6.1.2 Организация рабочего места

В соответствии с СанПиНом 2.2.2/2.4.1340–03, к рабочему месту, оборудованному ПЭВМ, предъявляются следующие требования:

- высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 – 800 мм; при отсутствии такой возможности высота рабочей поверхности должна составлять 725 мм;

- рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм;

- поверхность сиденья должна иметь ширину и глубину не менее 400 мм, иметь с закругленный передний край, регулироваться в пределах 400 – 550 мм и углами наклона вперед до 15 град. и назад до 5 град. угол наклона спинки в вертикальной плоскости должен обеспечивать ±30 градусов;

- стационарные или съемные подлокотники сиденья должны иметь длину не менее 250 мм и ширину 50 – 70 мм, регулироваться над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350 – 500 мм;

- рабочее место пользователя ПЭВМ должно быть оборудовано подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах 150 мм и по углу наклона опорной поверхности подставки до 20 град.

- клавиатура должна располагаться на поверхности стола на расстоянии 100 – 300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

Согласно СанПиН 2.2.2/2.4 1340–03, на одно рабочее место с ПЭВМ, на котором нет периферийного оборудования и установлен ЖК монитор, требуется 4,5 м^2, в противном случае, одно рабочее место с ПЭВМ должно зани-

мать 6 м^2, так же расстояние между боковыми стенками мониторов не должна быть меньше чем 1,2 м, свет от окон должен падать слева или справа.

На рисунке 34 представлено рекомендуемое размещение пользователя ПЭВМ.

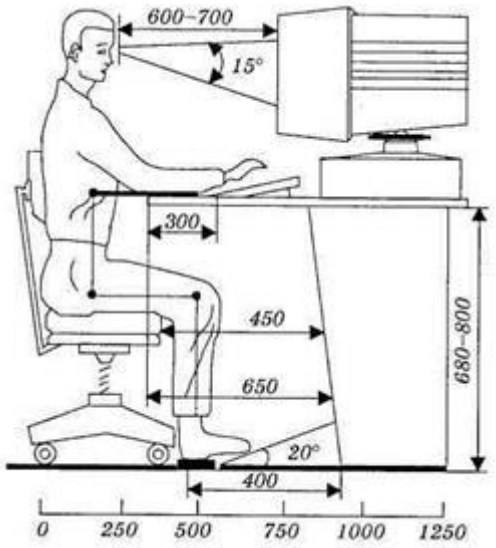

Рисунок 34 – Размещение пользователя за ПЭВМ

6.1.3 Освещение

Одним из важных требований, предъявляемых к помещениям с ПЭВМ является освещение. Правильное освещение повышает производительность труда, поскольку снижается нагрузка на зрительный аппарат. Плохое освещение, наоборот, приводит к быстрой утомляемости, ослаблении внимания при работе за ПЭВМ, ослеплении и раздраженности при чрезмерной яркости.

Виды освещения:

- естественное;
- искусственное;
- совмещенное;
- аварийное.

Естественное освещение обязательно должно присутствовать в любом помещении, где находится рабочий персонал. В зависимости от расположения, оно может быть боковым, верхним или комбинированным.

Искусственное освещение используется в основном в темное время суток. Оно должно обеспечивать равномерное освещение всего рабочего пространства, в случае, когда при расположении источников света учитывается размещение рабочих мест, речь идет о локализованном искусственном освещении.

Совмещенное освещение необходимо при недостаточности естественного. Данный тип освещения часто используется при введении точных работ, где требуется максимальная точность.

Аварийное освещение используется в случае отключения общего освещения.

В СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» четко изложены требования к освещению на рабочих местах, оборудованных ПЭВМ. Согласно данным требованиям коэффициент естественной освещённости не должен быть ниже 1,2 % в зонах с неустойчивым снежным покровом и не ниже 1,5 % на остальной территории. В помещении должно быть организовано односторонне боковое естественное освещение, при недостаточной видимости требуется применять искусственное освещение. Для обеспечения требуемого освещения следует использовать люминесцентные лампы, имеющие высокую световую отдачу и спектральный состав излучаемого света близкий к естественному. Освещённость на поверхности стола должна соответствовать 300 – 500 лк. Соотношение яркости между рабочими поверхностями не должна превышать 3:1 – 5:1, а между рабочими поверхностями и поверхностями стен и оборудования 10:1. Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка – 0,7 – 0,8; для стен – 0,5 – 0,6; для пола – 0,3 – 0,5.

6.1.4 Шум

Не менее важным опасным и вредным фактором при работе за ПЭВМ является повышенный уровень шума. Повышенный уровень шума приводит

к понижению качества условий труда, раздражимости, потери внимания, головную боль.

Согласно СанПиН 2.2.2/2.4.1340–03, шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки нормируется. Уровень шума для помещения, в котором человек работает за ПЭВМ не должен превышать 50 дБ. В таблице 4 представлены значения уровней звукового давления в октавных полосах частот и уровней звука, создаваемого ПЭВМ.

Таблица 4 – Допустимые значения уровней звукового давления в октавных полосах частот и уровня звука, создаваемого ПЭВМ

Уровни звукового давления в октавных полосах со среднегеометрическими частотами									Уровни звука, дБ
31,5 Гц	63 Гц	125 Гц	250 Гц	500 Гц	1000 Гц	2000 Гц	4000 Гц	8000 Гц	
86 дБ	71 дБ	61 дБ	54 дБ	49 дБ	45 дБ	42 дБ	40 дБ	38 дБ	50

6.1.5 Микроклимат

Микроклимат производственных помещений – комплекс нормированных показателей, таких как температура, влажность, тепловое излучение и другие, которые оказывают влияние на теплообмен человека и определяют самочувствие, работоспособность, здоровье и производительность труда. Отсюда и важнейшая задача охраны труда – поддержание микроклимата рабочего места в пределах гигиенических норм.

На рабочих местах источником существенных выделений является ПЭВМ, который повышает температуру человека, что приводит к снижению работоспособности и производительности, также ПЭВМ повышает температуру всего помещения в целом. В следствии этого, поддержание температуры на требуемом уровне позволит обеспечить безопасность и комфортность при работе за ПЭВМ.

Для поддержания микроклимата в помещении используются системы вентиляции. Система вентиляции – система смены воздуха в помещении, ко-

торая предназначена для поддержания метеорологических параметров помещения и подачи чистого воздуха с наружи. Для обеспечения наиболее комфортных условий применяют систему естественной вентиляции, а в весеннее и летнее время года дополнительно устанавливают систему кондиционирования для полного нормирования микроклиматических параметров в рабочем помещении для создания комфортных условий труда.

Для поддержания постоянной температуры, влажности и очистки от вредных веществ используются системы кондиционирования. Данные системы позволяют решить проблему, связанную с задержанием углекислого газа в помещении.

Система отопления поддерживает заданную, постоянную и равномерную температуру воздуха в рабочих помещениях в холодный период года. Расчет системы отопления производится на возмещение потерь тепла через ограждающие конструкции здания и на нагрев холодного воздуха, который проникает в помещение.

Существуют несколько видов систем отопления:

- водяные;
- паровые;
- воздушные;
- комбинированные.

Системы водяного отопления наиболее эффективны в санитарно-гигиеническом отношении, а также их достоинство заключается в том, что они надежны и обеспечивают возможность регулировать температуру в широких пределах. Такие системы часто используются в помещениях, в которых расположены рабочие места с ПЭВМ. При этом в холодный период года температура в помещении не должна превышать 22 – 24 °С, а в теплый период года – 20 – 25 °С. Относительная влажность воздуха должна составлять 40 – 60 %, скорость движения воздуха не превышать 0,1 м/с.

6.1.6 Анализ помещения с ПЭВМ

Работа с ПЭВМ производится в помещении, которое имеет площадь 18м^2. В помещении находится два рабочих места с ПЭВМ, содержащих ЖК-монитор, клавиатуру и мышь. Данное помещение полностью соответствует требованиям СанПиН 2.2.2/2.4 1340–03, поскольку на одно рабочее место приходится 9м^2. Габариты рабочей поверхности и сидений также соответствуют всем требованиям. Размещены рабочие места соответственно справа и слева, относительно оконных проемов, что удовлетворяет требованиям к естественному освещению. Окна оборудованы регулируемыми жалюзи. В соответствии с техническими требованиями помещения оборудовано защитным заземлением. Температура помещения поддерживается в диапазоне от 22 ℃ до 25 ℃, имеется кондиционер для регулирования температуры воздуха.

Схема помещения представлена на рисунке 35.

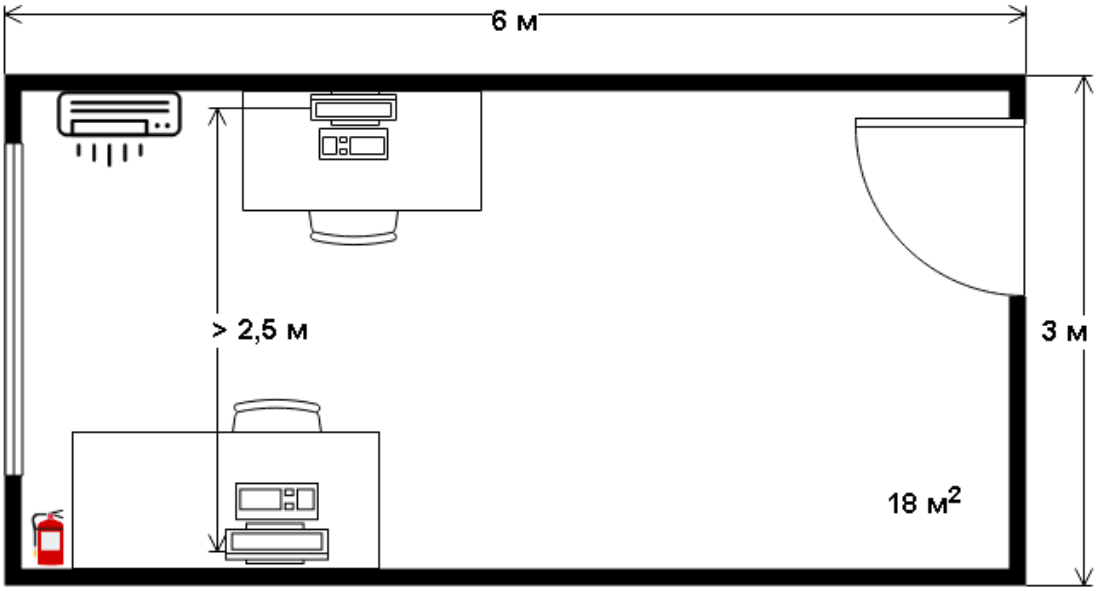

Рисунок 35 – Схема помещения с ПЭВМ

Таким образом, данное помещение соответствует всем предъявляемым нормам, согласно СанПиН 2.2.2/2.4 1340–03.

6.2 Экологичность

ПЭВМ состоит из большого количества компонентов, содержащие токсичные вещества и представляющие угрозу для человека, а также для окружающей среды. К таким веществам относятся:

- ртуть (поражает мозг и нервную систему), находится в подсветке ЖК-мониторов;

- щелочи (прожигают слизистые оболочки и кожу), находятся в щелочных аккумуляторах источников бесперебойного питания;

- никель и цинк (могут вызывать дерматит), находится в материнской плате и батареях питания для ноутбуков;

- поливинилхлорид (разрушает нервную систему и вызывает раковые заболевания), находится в кабелях, которые подключаются к электронным устройствам.

Поэтому ПЭВМ требует специальных комплексных методов утилизации. Этот комплекс мероприятий включает в себя: сортировка металлических и неметаллических частей; металлические части отправляются на переплавку для последующего производства; неметаллические части компьютера утилизируются специальным способом.

В настоящее время создается и внедряется малоотходная технология в ряде отраслей промышленности, однако полный перевод ведущих отраслей промышленности на безотходную технологию потребует решения большого комплекса весьма сложных технологических, конструкторских и организационных задач.

6.3 Чрезвычайные ситуации

6.3.1 Аварийные ситуации

При работе могут возникнуть следующие аварийные ситуации:

- обрыв проводов питания;

- неисправность заземления;

- повреждение электрооборудования;

- повреждение инженерных коммуникаций;

- повреждение конструктивных элементов здания или помещения.

Во всех случаях обнаружения аварийной ситуации или появления резких ухудшений самочувствия, а также в любых других ситуациях, которые создают непосредственную угрозу жизни или здоровью людей, необходимо:

- остановить производство работ;

- при наличии пострадавших, обеспечить оказание первой помощи;

- при необходимости, обеспечить отключение электроэнергии;

- обеспечить открывание аварийных выходов и эвакуацию персонала;

- доложить о принятых мерах руководителю работ и действовать в соответствии с полученными указаниями;

- доложить оперативному дежурному;

Сотрудник, находящийся вблизи места происшествия, несчастного случая, должен оказать доврачебную помощь пострадавшему, доложить об этом оперативному дежурному, начальнику отдела. При обнаружении человека, попавшего под напряжение, немедленно отключить электропитание и освободить его от действия тока.

6.3.2 Меры пожарной безопасности на рабочих местах

При расстановке технологического и другого оборудования должно быть обеспечено наличие проходов к путям эвакуации и эвакуационным выходам.

Персональный компьютер и монитор должны быть установлены на надежную опору (тумбочку, подставку, кронштейн и т. п.), не допускающую его от падения. Запрещается устанавливать ПК:

- в нишах мебельных «стенок», в тумбочках и т.п.;

- ближе 1 метра от электронагревательных приборов и от горючих предметов (тюлей, занавесок, гардин, штор; декоративных украшений, новогодних ёлок и т. п.);

- ближе 0.7 метров от проходов, путей передвижения и эвакуации людей.

Перед началом эксплуатации персонального компьютера требуется провести следующий ряд действий:

- провести внешний осмотр места установки персонального компьютера и монитора и убедиться в выполнении требований безопасности, предъявляемых выше;

- провести внешний осмотр ПК и монитора, электрошнура, электровилки и убедиться в их исправности, если корпус, электрошнур, электровилка, задняя крышка повреждены, то ПК эксплуатировать запрещается;

- при наличии на, над и около ПК и монитора горючих предметов (салфеток, накидок, книг, газет, декоративных украшений и т. п.) и емкостей с жидкостью (вазы с живыми цветами) – убрать их;

- убедиться в том, что вентиляционные отверстия в задней крышке ПК и монитора не закрыты какими-либо предметами;

- убедится в наличии возле ПК противопожарной ткани или огнетушителя.

Данные меры безопасности при работе на ПЭВМ позволят сократить риск возникновения пожара.

6.4 Комплексы физических упражнений для сохранения и укрепления индивидуального здоровья и обеспечения полноценной профессиональной деятельности

При длительной и/или напряженной работе с ПЭВМ, а также при его неправильной эксплуатации нередко возникают проблемы со здоровьем. В основном эти проблемы связаны со зрением и опорно-двигательным аппаратом. Для предотвращения этого, необходимо придерживаться рекомендаций при работе с ПЭВМ. Например, 15-минутный перерыв после 1,5-2-часовой работы, а во время этого перерыва необходимо встать со своего рабочего места и провести небольшой комплекс упражнений, для снятия затечности и напряженности мышц.

В целом, рекомендуется следующие формы самостоятельных занятий:

- утренняя гигиеническая гимнастика;

- лечебная гимнастика (гимнастика для глаз);

- занятия физкультурой по избранной программе;

- физкультурная пауза во время работы;

- элементы самомассажа;

- закаливание организма.

Для людей (сотрудников, студентов), страдающих близорукостью, разработаны специальные упражнения типа лечебной физкультуры.

Работники с близорукостью высокой степени (6.0 дптр и более) должны выполнять следующие общие правила:

- следовать рекомендациям офтальмолога и терапевта;

- учитывать состояние здоровья;

- физическую нагрузку соразмерять с возрастом и тренированностью организма;

- помнить об ограничениях, связанных с состоянием органа зрения при выполнении некоторых видов упражнений. Так с близорукостью более 6,0 диоптрий, а также с хроническими изменениями на глазном дне нежелательны упражнения с продолжительными и напряженными переходами из положения сидя в положение лежа и обратно;

- противопоказаны упражнения, связанные с сотрясением тела (прыжки, подскоки) и требующие напряжения.

Так как рабочие места с ЭВМ, в подавляющем большинстве случаев – сидячие, у многих людей, работающих за ЭВМ, наблюдается сутулость, что говорит о слабости мышц задней поверхности туловища, которая может способствовать появлению и прогрессированию близорукости. Поэтому наряду с упражнениями для глаз необходимо выполнять упражнения для укрепления мышц шеи и спины.

Общеразвивающие упражнения:

1) Лежа на спине, руки вперед – в стороны. Выполнять окрестные движения прямыми руками в течение 15-20 с. Следить за движением кисти одной, затем другой руки. Дыхание произвольное.

2) Лежа на спине, руки вперед – в стороны. Махи одной ногой к разноименной руке. Повторить 6-8 раз каждой ногой. Смотреть на мысок. Мах выполнять быстро. Во время маха – выдох.

3) Лежа на спине, руки вперед. Выполнять окрестные движения руками, опуская и поднимая их. Следить за кистью одной, затем другой руки. Выполнять 15-20 с.

4) Сидя на полу, упор руками сзади, прямые ноги. Поочередно поднимать и опускать ноги. Выполнять 15-20 с. Смотреть на мысок одной ноги.

5) Сидя на полу, упор руками сзади. Правую ногу отвести вправо, вернуть в исходное положение. То же повторить другой ногой влево 6-8 раз каждой ногой. Смотреть на мысок.

6) Сидя на полу, упор руками сзади, прямая нога слегка приподнята. Выполнять круговые движения ногой в одном и другом направлении. Повторить 10-15 с каждой ногой. Смотреть на носок.

7) Стоя, руки опущены. Поднять руки вверх, затем опустить. Смотреть сначала на правую кисть руки, затем на левую. Вновь перевести взгляд на правую кисть. Выполнять движения глазами в одном и другом направлении 15-20 с. Менять направление движения глаз через 5 с.

8) Стоя, смотреть только вперед на какой-либо предмет. Повернуть голову направо, затем налево. Повторить 8-10 раз в каждую сторону.

9) Стоя, смотреть только вперед на какой-либо предмет. Голову поднять, затем опустить, не изменяя взгляда. Повторить 10 раз. Смотреть на какой-либо предмет.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы разработана система управления домом «SCHome», прототипы системы, Интернет-магазин. В ходе работы был произведен анализ работы ЛВС системы «SCHome», также проанализированы виды, классификации и способы предотвращения угроз ЛВС. Рассмотрены такие вопросы как:

- возможные угрозы локальной сети;
- главные цели сетевой безопасности;
- средства защиты информации;
- способы защиты информации;
- развертывание VPN:
- программные средства защиты информации.

Если в системе «SCHome» принять меры, описанные в данной работе, то локальная сеть будет иметь большую гарантию защиты от несанкционированного вторжения или потери данных. Но никакие средства защиты не могут гарантировать стопроцентную безопасность данных сети.

Так же были проанализированы угрозы безопасности жизнедеятельности, разработаны рекомендации по работе с системой (с ЭВМ), а также составлен комплекс физических упражнений для сохранения и укрепления здоровья людей, работающих с данной системой.

Система «SCHome» позволит значительно снизить тепло- и электрозатраты, а также автоматизировать некоторые аспекты жизни человека, давая ему больше времени выполнение более важных вещей, не отвлекаясь на рутинные. А реализованный удаленный доступ позволит безопасно управлять домом, находясь в отпуске, или получать подробную информацию о его состоянии. Осуществление продажи сборных комплектов с подробной информацией по сборке и бесплатным программным обеспечением, позволит вовлечь больше школьников, студентов, любителей радиотехники и программирования в изучение технологий «Интернета вещей», и «Умного дома».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Демьяненко А.Е. Проект разработки информационной системы «Конфигурируемый дом». // Молодёжь XXI века: шаг в будущее: материалы XVIII региональной научно- практической конференции (18 мая 2017 года) – Благовещенск: Изд-во БГПУ, 2017. – С. 1012-1013.

2 Самохвалова С.Г., Демьяненко А.Е. Разработка интернет-магазина готовых решений системы «Конфигурируемый дом». // Экономика и социум: международный научно-практический электронный журнал – Институт управления и социально-экономического развития, 2017. – № 12 (43).

3 Самохвалова С.Г., Демьяненко А.Е. Разработка программного обеспечения для системы «Конфигурируемый дом» // Современные проблемы науки: материалы Российской национальной научной конференции с международным участием (22 декабря 2017 г.). – Часть I. – Благовещенск Амурский гос. ун-т, 2017. – С. 128-130

4 Дейтел П. Android для программистов: создаем приложения / П. Дейтел, Х. Дейтел, Э. Дейтел, М. Моргано. – СПб.: Питер, 2013. – 560 с.

5 Макконнелл С. Совершенный код. Мастер-класс / С. Макконнелл. – М.: Издательство «Русская Редакция»; СПб.: Питер, 2008. – 896 стр.

6 Олифер, В.Г. Основы сетей передачи данных / В.Г. Олифер, Н.А. Олифер. – СПб: Питер, 2009. – 663с.

7 Дейт, К. Дж. Введение в системы баз данных / К.Дж. Дейт. – Киев: Вильямс, 2008. – 846с.

8 Коннолли, Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика / Т. Коннолли. – М.: Издательский дом «Вильямс», 2008. – 1120 с.

9 Димов, Э.М. Проектирование информационных систем: учебное пособие / Э.М. Димов, А.Р. Диязитдинова. – Самара: Издательство Поволжского гос. Академии, 2008. – 112 с.

10 Брэндл, Д. Защита и безопасность в сетях Linux. Для профессионалов (+CD) / Д. Брэндл. – СПб.: Питер, 2002. – 480 с.

11 Баррет, Д. Java профессионалам / Д. Баррет. – Киев: БХВ, 2011. – 412 с.

12 http://docs.blynk.cc/: [Электронный ресурс]: Руководство по использованию Blynk. – 22.12.2017.

13 Белов, А.В. Самоучитель разработчика устройств на микроконтроллерах AVR / А.В. Белов. – СПб.: Наука и техника, 2008. – 530 с.

14 Новиков, Ю.В. Основы микропроцессорной техники : учебное пособие / Ю.В. Новиков, П.К. Скоробогатов. – 4-е изд. испр. – М.: Интернет-Университет информационных технологий БИНОМ. Лаборатория знаний, 2009. – 358 с.

15 Шилдт, Г. Java 8. Полное руководство. / Г. Шилдт. – М.: Издательский дом «Вильямс», 2015. – 1376 с.

16 Петин, В.А. Микрокомпьютеры Raspberry Pi. Практическое руководство. / В.А. Петин. – СПб.: BHV, 2015. – 240 с.

17 Даккет, Д. HTML и CSS. Разработка и дизайн веб-сайтов / Д. Даккет. – М.: Эксмо, 2013. – 480 с.

18 http://php.net/: [Электронный ресурс]: PHP: Hypertext Preprocessor. – 03.04.2017.

19 https://blynkapi.docs.apiary.io/#: [Электронный ресурс]: Blynk HTTP RESTful API. Apiary. – 15.06.2017.

20 ГОСТ 12.0.003-2015. Система стандартов по безопасности труда. Опасные и вредные производственные факторы. Классификация. – Введ. 2017-03-01. – М.: Стандартинформ, 2016. – 10 с.

21 СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы : утв. постановлением гл. гос. санитар. врача Рос. Федерации от 30.05.2003 №118. – М.: Рид Групп, 2011. – 32 с.