МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
им. Н.Э. Баумана

Кафедра «Системы обработки информации и управления»

ОТЧЕТ

по курсу «Теория защиты информации»

Тема: «Система по управлению многоквартирным домом»

ИСПОЛНИТЕЛИ: _Дыньков А.Д. _____
_ Рудченко Е.А. _____
ФИО подпись

группа ИУ5-82

"__"_____2021 г.

ПРЕПОДАВАТЕЛЬ: __Варламов О.О____
ФИО

_____
подпись

"__"_____2021 г.

Москва - 2021

Оглавление

1. Цель работы

Целью работы является создание системы по управлению многоквартирным домом. Данное решение призвано упростить и централизовать обслуживание дома, систем безопасности, общения и файлообмена, тем самым увеличить уровень комфорта и безопасности жителей, а также повысить экономию затрат на обслуживание дома.

2. Задачи работы

2.1. Разработка модели системы;
2.2. Разработка сетевой составляющей системы;
2.3. Разработка методов защиты информации пользователей;
2.4. Анализ работы сети;

3. Создание модели

Для начала нужно определиться с архитектурой построения системы.
Существует два вида архитектуры системы управления многоквартирным домом:

- Децентрализованная
- Централизованная.

Децентрализованная архитектура основывается на том, что все узлы в сети равноправные.
Централизованная архитектура предполагает наличие сервера, который управляет подключенными к нему модулями.
Под наши задачи, лучше всего подходит централизованная система, т.к. она является наиболее экономной.
Если планировать систему как централизованную, у нее можно выделить следующие уровни:

- уровень 1: пользовательские системы управления, к ним относят: web-интерфейс, с которого осуществляется контроль системы;
- уровень 2: связь сервера с пользовательским интерфейсом, на этом уровне передается информация между пользователем и сервером;
- уровень 3: сервер, дает возможность пользовательской системе взаимодействовать с файловой системой, мессенджером и периферией;

• уровень 4: связь сервера с файловой системой, мессенджером и периферией, на этом уровне передается информация между сервером и данными/периферией;
• уровень 5: данные и периферия.

Одной из основных частей системы является интерфейс, с которым и будет сталкиваться пользователь. Поэтому рассмотрим, какие элементы интерфейса необходимы для разработки.

- Окно мессенджера жильцов, с возможностью создания и выбора диалогов между
  жильцами, занесенными в базу данных, как проживающих в данном доме;
- Окно просмотра и сбора информации с камер видео наблюдения;
- Окно просмотра/добавления актуальных новостей и голосований;
- Виртуальная доска «Тикетов» заданий жильцов для выполнения консьержем;
- Личное/групповое облачное хранилище для каждого жителя дома;

Серверная часть веб-приложения разрабатывается с использованием технологии C++ и располагается на ноутбуке.

4. Разработка сети на основе стека TCP/IP

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol, протокол управления передачей/протокол интернета) — сетевая модель, описывающая процесс передачи цифровых данных. Она названа по двум главным протоколам, по этой модели построена глобальная сеть — интернет.

TCP (протокол управления передачей) — надежный, он обеспечивает передачу информации, проверяя дошла ли она, насколько полным является объем полученной информации и т.д. TCP дает возможность двум хостам производить обмен пакетами через установку соединения. Он предоставляет услугу для приложений, повторно запрашивает потерянную информацию, устраняет дублирующие пакеты, регулируя загруженность сети. TCP гарантирует получение и сборку информации у адресата в правильном порядке.

UDP (протокол пользовательских датаграмм) — ненадежный, он занимается передачей автономных датаграмм. UDP не гарантирует, что всех датаграммы дойдут до получателя. Датаграммы уже содержат всю необходимую информацию, чтобы дойти до получателя, но они все равно могут быть потеряны или доставлены в порядке отличном от порядка при отправлении.

UDP обычно не используется, если требуется надежная передача информации. Использовать UDP имеет смысл там, где потеря части информации не будет критичной для приложения, по этому выбор сделан в пользу протокола TCP.

5. Методы защиты информации пользователей

Испытанный метод защиты информации от несанкционированного доступа - шифрование (криптография). Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст - ciphertext) или зашифрованных данных - в открытые по определенным правилам с применением определенных правил, содержащихся в ключах (шифре).

Известные криптографические методы защиты информации можно разбить на два класса:

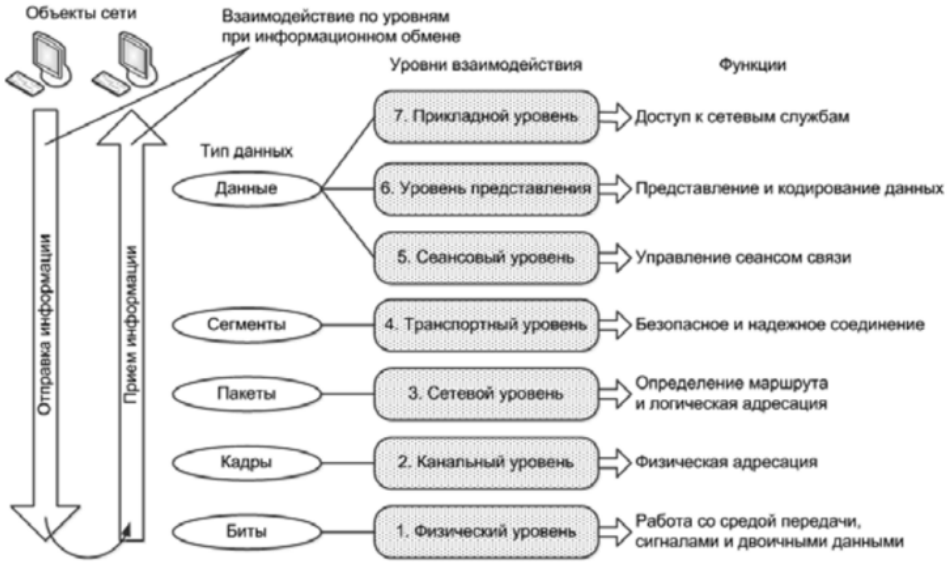
- Обработка информации путем замены и перемещения букв, при котором объем данных не меняется (шифрование);
- Сжатие информации с помощью замены отдельных сочетаний букв, слов или фраз (кодирование).

К алгоритмам шифрования предъявляются определенные требования:

- Высокий уровень защиты данных против дешифрования и возможной модификации;
- Защищенность информации должна основываться только на знании ключа и не зависеть от того, известен алгоритм или нет (правило Киркхоффа);
- Малое изменение исходного текста или ключа должно приводить к значительному изменению шифрованного текста (эффект «обвала»);
- Область значений ключа должна исключать возможность дешифрования данных путем перебора значений ключа;

- Экономичность реализации алгоритма при достаточном быстродействии;
- Стоимость дешифрования данных без знания ключа должна превышать стоимость данных.

В соответствии с эталонной моделью компьютерных сетей OSI (Open Systems Interconnection), разработанной в 1984 г. Международной организацией по стандартам, выделяется семь уровней системного взаимодействия. Модель OSI представляет собой абстрактную модель взаимодействия компьютеров, приложений и других устройств в телекоммуникационной сети.



Верхние три уровня предназначены для связи с конечным пользователем, а нижние четыре - ориентированы на выполнение коммуникационных функций в реальном масштабе времени.

При канальном шифровании, т.е. шифровании данных на нижнем уровне сети, обрабатываются данные, направляемые по каждому каналу связи, причем должен расшифровываться каждый входящий поток информации с последующим перешифрованием исходящего.

Отправка информации в открытом виде по любому каналу поставит под угрозу безопасность всей сети в целом. В связи с этим стоимость реализации канального шифрования в больших сетях может оказаться достаточно высокой. Кроме того, при использовании данного вида шифрования потребуется защищать каждый узел компьютерной сети, через который проходит передаваемая информация. Это связано с необходимостью защиты

конфиденциальной информации, ознакомление с которой допустимо только для определенных сотрудников, а для остальных необходимо ограничить доступ к этим данным.

При сквозном шифровании, выполняемом на верхних уровнях коммуникационных сетей, обработка передаваемой информации осуществляется на одном из верхних уровней только в отношении содержательной части передаваемого сообщения с дополнением служебной информации, необходимой для маршрутизации информационной посылки. После этой обработки сформированный пакет направляется на более низкие уровни для передачи адресату. При таком шифровании уже нет необходимости в дополнительной «парной» обработке (расшифрование и шифрование) на каждом промежуточном узле сети, поскольку информационное сообщение остается зашифрованным на протяжении всего маршрута передачи данных.

Недостатком такого способа защиты является передача дополненной служебной информации в незашифрованном виде, поэтому возможно несанкционированное получение ряда полезных данных (например, о расписании сеансов связи). Кроме того, в случае применения сквозного шифрования могут возникать затруднения в способах кодирования из-за различия в используемых коммуникационных протоколах и интерфейсах в зависимости от типов компьютерных сетей и элементов этих сетей.

При комбинированном шифровании, использующем возможности как канального, так и сквозного шифрования, передаваемую информацию можно защитить лучше всего, однако при этом пропорционально возрастает и стоимость защиты данных.

Большинство средств криптографической защиты данных реализуется с помощью специализированных аппаратных устройств, устанавливаемых на передающей и приемной сторонах - шифратора и дешифратора, которые осуществляют соответственно шифрование и дешифрование передаваемой информации. Применение специализированной аппаратуры для шифрования обусловливает относительно высокую стоимость реализации, однако наблюдается определенное преобладание аппаратных средств по сравнению с программными методами. В основном рассматриваются преимущества аппаратных решений, относящиеся к скорости обработки информации и к обеспечению физической защиты компонентов. Считается, что аппаратные средства в состоянии более быстро осуществить необходимые операции по

обработке данных, чем программы - реализовать сложные криптографические алгоритмы.

Программное шифрование представляет собой результат реализации криптографического алгоритма программными средствами. Достоинства в использовании программных средств заключаются в возможности тиражирования путем обычного копирования, в относительной простоте их модификации и использования.

Преобразование информации, в результате которого обеспечивается изменение объема памяти, занимаемой данными, называется *кодированием.* Кодирование текстовой информации может проводиться фактически с помощью кодовых таблиц путем замены одних символов другими. При этом может осуществляться и определенное сжатие передаваемого информационного пакета. Если информация зашифрована с помощью простой подстановки, то расшифровать ее можно было бы, определив частоты появления каждой буквы в шифрованном тексте и сравнив их с частотами букв русского алфавита. Таким образом, существует возможность определения подстановочного алфавита, в результате чего расшифровывается текст.

Анализ методов шифрования, применяемых в настоящее время, показывает, что, несмотря на достаточно широкое их использование, они не вполне свободны от недостатков и оставляют определенное поле для совершенствования и разработки новых методов защиты информации, передаваемой по каналам связи. Учитывая динамику развития методов управления документами, включая их формирование, целесообразно комплексировать процессы создания и защиты формируемых документов.

6. Анализ работы сети

Благодаря возможностям протокола TCP и шифрованию мы можем создать безопасную систему по управлению многоквартирным домом, организовать в ней безопасное хранение и передачу данных, общение жильцов и обеспечить комфортное проживание.

7. Выводы

В результате данной работы был разработан прототип системы «умного дома». В его возможности входят: ведение базы показателей температуры, влажности, освещенности и ее отражение на web-странице с помощью счетчиков и графиков; управление через веб-страницу яркостью света;

включение и выключение периферии с высоким напряжением через вебстраницу; управление ноутбуком через веб-страницу. По моему мнению, для дальнейшего развития систем «умный дом» необходим единый стандарт. Он должен обеспечивать универсальное подключение как датчиков, так и периферийных устройств. Во-первых, это может способствовать снижению цен на устройства, которые требуются для построения системы. Во-вторых, это позволит упростить процесс проектирования и реализации таких систем. В будущем, построение системы «умного дома» должно напоминать игру в конструктор.

8. Список источников

1. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 с.
2. Бабенко, Л.К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко. - М.: Гелиос АРВ, 2015. - 921 с.
3. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. - М.: КомКнига, 2012. - 306 с.
4. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2016. - 186 с.
5. Вельшенбах, М. Криптография на Си и C++ в действии. Учебное пособие / М. Вельшенбах. - М.: Триумф, 2014. - 462 с.
6. Горев, А И; Симаков А А Обеспечение Информационной Безопасности / А Горев А И; Симаков А. - Москва: ИЛ, 2016. - 494 с.
7. Грибунин, Вадим Геннадьевич Цифровая стеганография / Грибунин Вадим Геннадьевич. - М.: Солон-Пресс, 2016. - 589 с.
8. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. - М.: ИНФРА-М, 2015. - 869 с.
9. Зубов, А.Н. Математика кодов аутентификации / А.Н. Зубов. - М.: Гелиос АРВ, 2014. - 319 с.