Безопасность платежной системы обеспечивается выполнением следующих параметров:
– взаимодействие с сервером производится только по зашифрованному соединению HTTPS;
– для авторизации сервера используется SSL сертификат;
– серверная инфраструктура приложения должна соответствовать стандарту PCI DSS.

Применение данной модели позволяет сократить время на выполнение платежей, исключить ошибки при повторном ручном вводе реквизитов платежа. При этом клиентское приложение не получает и не обрабатывает данные банковских карт пользователей, поэтому к нему не предъявляется требований по какой-либо сертификации со стороны международных платежных систем.

Список использованных источников:

1. Шаньгин, В. Защита информации в компьютерных системах и сетях / В. Шаньгин. — Москва, 2012. — 371 с.
2. PCI Security Standards Council: PCI SSC Data Security Standards. [Электронный ресурс]. – Режим доступа: https://www.pcisecuritystandards.org/security_standards/. – Дата доступа: 10.03.2015
3. PayOnline.ru: Система электронных платежей. [Электронный ресурс]. – Режим доступа: http://www.payonline.ru/. – Дата доступа: 10.03.2015

ПРОГРАММНОЕ СРЕДСТВО ВИДЕООБЩЕНИЯ ПО СЕТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ленкевич В. Д.

Курмаз Ю. П. – ассистент

В 21 веке человек, независимого от своего социального статуса и материального положения, огромную часть времени проводит за компьютером на просторах всемирной сети Интернет. Несмотря на это, род деятельности может быть разный: работа, учеба, отдых, прослушивание музыки, просмотр видео, ведение личного блога. Действительно, этот список можно продолжать бесконечно. В это время важно оставаться «на связи» так, чтобы это было максимально удобно для пользователя, ведь мобильный телефон не всегда может помочь, находясь два абонента в разных точках земного шара. Решить эту проблему призваны программные средства, предназначенные для общения пользователей в сети Интернет.

Использование подобных приложений позволяет совершать звонки, видео звонки, обмен файлами, обмен мгновенными сообщениями с другими пользователями, независимо от их географического местоположения. Данный класс программных средств пользуется большой популярностью в крупных коммерческих фирмах и корпорациях. Работа в команде – это неотъемлемая составляющая любого проекта или бизнес идеи. Для этого превосходно подойдут такие функции как демонстрация экрана и групповая видеоконференция.

На данный момент, на рынке находится большое количество программных средств общения по сети Интернет. Далее приведены самые мощные, многофункциональные и популярные из них:

1. «Skype» - родоначальник данного класса программных средств, который получил мировое признание. К плюсам необходимо отнести высокую защищенность канала передачи данных, высокое качество связи, возможность совершать звонки на стационарные и мобильные телефоны, поддержку всех видов ОС: Windows, Linux, OS X. Поддержку всех видов мобильных ОС: iOS, Android, Windows Phone, Symbian, Bada, BlackBerry OS. К минусам – большое количество отображаемой рекламы, большое количество платных функций, нет возможности производить запись разговора или видеоконференции.
2. «WhatsApp» - программное средство для мобильных операционных систем. Плюсом является упрощенный процесс регистрации и возможность передачи данных с одного мобильного устройства на другое. Минусом – данное программное средство только для мобильных устройств, не реализована функция видео звонка, бесплатная лицензия сроком на один год.
3. «Viber» - программное средство, как для мобильных операционных систем, так и для настольных персональных компьютеров. К плюсам необходимо отнести упрощенный процесс регистрации и кроссплатформенность. К минусам – рекламные акции, некоторые функции являются платными, нет возможности произвести видео звонок.
4. «RaidCall» - программное средство для настольных операционных систем. Плюсом является быстрая и легкая настройка программы, низкая загрузка аппаратных ресурсов, возможность создавать видео трансляции. Минусом – непростой интерфейс для начинающего пользователя.

Ни в одном из существующих аналогов нет возможности записи разговора или видеоконференции с последующим сохранением, необходимом формате, на жесткий диск компьютера. Зачастую, пользователю необходимо еще раз прослушать информацию, которую до него хотел донести собеседник, в спокойной обстановке, будь то студент университета, который пожелает еще раз прослушать информацию после лекции «online», или менеджер в офисе, после очередного распоряжения вышестоящего по должности. Основным плюсом данного программного средства будет реализация этой функции.

Большинство программных средств такого рода имеет возможность установки либо на мобильные операционные системы, либо на настольные операционные системы. Важной задачей будет реализация

разрабатываемого приложения, как для популярных настольных ОС, так и для популярных мобильных операционных систем.

Также большинство существующих аналогов не позволяют вести «трансляцию в реальном времени». Одним из плюсов разрабатываемого программного средства будет являться «вещание в прямом эфире» с возможностью обмена мгновенными сообщениями с автором эфира. Это позволит удобно организовать трансляции типа: «преподаватель - студенты» или «руководящее звено - служащие».

Большая доля внимания будет уделена проектированию максимально простого и интуитивно понятного пользовательского интерфейса. Независимо от операционной системы, за основу будет взят единый графический интерфейс. При первом запуске программы пользователю будет предложено ознакомиться с основными возможностями программного средства. Процесс регистрации и авторизации будет максимально упрощен, с возможностью выполнять эти процедуры через различные социальные сети.

Все функции разрабатываемого приложения будут абсолютно бесплатны.

С учетом всего вышеперечисленного можно сформировать список общих требований к разрабатываемому программному средству:

1. Программное средство должно позволять совершать голосовые звонки;
2. Программное средство должно позволять совершать видео звонки;
3. Программное средство должно позволять совершать обмен мгновенными текстовыми сообщениями между пользователями;
4. Программное средство должно позволять совершать обмен файлами между пользователями;
5. Программное средство должно предоставлять возможность записи разговора или видео звонка с последующим сохранением на жесткий диск ПК;
6. Программное средство должно предоставлять возможность трансляции в реальном времени;
7. Программное средство должно предоставлять возможность демонстрации экрана устройства собеседника.

Список использованных источников:

1. Skype [Электронный ресурс]. – 2015. – Режим доступа: http://www.skype.com/ru
2. WhatsApp [Электронный ресурс]. – 2015. – Режим доступа: http://www.whatsapp.com
3. Viber [Электронный ресурс]. – 2015. – Режим доступа: http://www.viber.com/ru
4. RaidCall [Электронный ресурс]. – 2015. – Режим доступа: http://www.raidcall.com.ru

ПРОГРАММНОЕ СРЕДСТВО ЗАЩИТЫ ПОЧТОВЫХ СООБЩЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Таразевич С. Ю.

Прохорчик Р. В. – м. т. н., ассистент

В настоящее время электронные средства передачи информации практически вытеснили классические. Одним из самых актуальных вопросов является обеспечение конфиденциальности и целостности передаваемых данных, так как, как правило, данные хранятся на серверах, неподконтрольных пользователям.

Основной проблемой, представляющей угрозу конфиданциальности электронных сообщений, является то, что они хранятся на удаленных серверах, следовательно, пользователь никогда не может быть уверен, что его информация не будет доступна третьим лицам. В последнее время поступает довольно много сообщений об утечках информации с серверов различных крупных компаний, что подтверждает существование проблем с конфиденциальностью при таком подходе к организации хранения данных [2]. Существует много решений, использущих шифрование пользовательской информации на удаленных серверах, но данный подход также не гарантирует конфиденциальность, так как нет уверенности в добросовестности компаний, предоставляющих даные услуги. С другой стороны, у хранения данных на сторонних серверах есть ряд существенных преимуществ: доступ к информации через сеть интернет, не требуются аппаратные ресурсы пользователя. Таким образом, хранение информации на удаленных серверах, при обеспечении ее конфиденциальности, во многих случаях является оптимальным решением.

Для обеспечения конфиденциальности данных при хранении их на удаленном сервере можно использовать шифрование на стороне клиента. При данном подходе данные будут зашифрованы до отправки их на сервер, что, при использовании криптостойкого алгоритма шифрования, позволит защитить их от третьих лиц, не полагаясь на защитные механизмы удаленного сервера.

Для реализации шифрования электронных писем наиболее оптимальным вариантом будет использование симметричного алгоритма шифрования по следующим причинам:

- при наличии ключа любой пользователь сможет расшифровать сообщение, при ассиметричном алгоритме необходимо шифровать сообщение для каждого адресата отдельно с использованием его открытого ключа.

- скорость работы симметричных алгоритмов выше, чем асимметричных [1].

Можно выделить 2 стратегии создания ключей при использовании симметричного алгоритма