электронное периодическое издание

ЭКОНОМИКА и социум

ISSN 2225-1545
№ 4(13) - 2014

ПЕРИОДИЧЕСКОЕ ИЗДАНИЕ

«Экономика и социум»

http://www.iupr.ru

УДК 004.02:004.5:004.9

ББК 73+65.9+60.5

ISSN 2225-1545

Свидетельство о регистрации
средства массовой коммуникации
Эл № ФС77-45777
от 07 июля 2011 г.

Выпуск № 4(13) (октябрь-декабрь, 2014). Сайт: http://www.iupr.ru

Наранович О.И., к.ф.-м.н.
доцент,
кафедра ИСТ
Омельянович А.А.
студент 5 курса
Барановичский государственный университет
Республика Беларусь, г. Барановичи

ПЕРЕДАЧАДОКУМЕНТОВ ПО ЭЛЕКТРОННОЙ ПОЧТЕ С ПРИМЕНЕНИЕ СОВРЕМЕННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

При обработке непрерывного потока информации, все большую актуальность приобретают процессы автоматизации работ рутинного характера. В связи с этим, для эффективного управления предприятием, ежегодно разрабатываются программы, позволяющие решать возникающие проблемы.

Для большинства государственных организаций и коммерческих фирм характерно наличие множества филиалов и структурных подразделений, находящихся на значительном расстоянии между собой.

Создание автоматизированной системы облегчит отправку документов между подразделениями предприятий, а также позволит сохранить их конфиденциальность. Отправляющей стороне достаточно будет сделать пару кликов мышью, чтобы зашифровать документы и отправить их на почтовый адрес. В свою очередь, принимающей стороне не нужно каких-либо особых знаний компьютерных технологий для того, чтобы получить документы.

Таким образом, автоматизированная система шифрования и передачи документов для отдела маркетинга любого торгового предприятия позволит осуществлять безопасную передачу данных между структурными подразделениями в автоматическом режиме, без проведения рутинных операций.

Программный продукт реализован в виде Windows-приложения, позволяющего работать в многопользовательском режиме в корпоративной сети предприятия.

В процессе выполнения работы проанализированы известные технология шифрования и защиты документов, выявлены прогрессивные стороны в распространенных подходах. С учетом повсеместного и бурного развития компьютеризации всех аспектов жизнедеятельности общества: внедрение компьютерных технологий в широкие сферы социальной жизни, характеризующегося требованием реализации функций шифрования с использованием малых объемов ресурсов (памяти, логических элементов и т.п.) и обеспечения необходимой защиты информации пользователей открытых сетей типа Интернет от несанкционированного доступа, требуют развития такого направления как «облегченная криптография»[1].

Общими свойствами алгоритмов облегченной криптографии являются низкие требования:

- к требуемой площади кристалла, на котором алгоритм может быть аппаратно реализован;
- вычислительной мощности микропроцессора, на котором выполняются вычисления;
- оперативной памяти вычислительного устройства и т.п. [1].

В связи с этим целью исследовательской работы является разработка автоматизированной системы шифрования документов и передачи их по электронной почте для отдела маркетинга ЧТУДП «Торговый Дом «Лагуна».

Разработка программного продукта велась с использованием современных информационных компьютерных технологий: среда разработки MicrosoftVisualStudio 2010 и язык программирования C#; СУБД Firebird 2.5; в результате анализа современных способов шифрования для реализации в автоматизированной системе были выбраны современные криптоалгоритмы AES и RSA.

Алгоритм AES применяется для наиболее важных документов, информация из которых никоим образом не должна попасть в третьи руки. Алгоритм RSA менее эффективен, зато требует меньше затрат ресурсов ЭВМ, поэтому данный алгоритм шифрования применяется к документам важность которых не столь велика. Данная комбинация алгоритмов шифрования позволяет сбалансировать такие показатели программы как надежность и скорость работы.

Программа состоит из 11 классов:

1. FormAutor — класс, предназначенный для авторизации пользователей;
2. HeadForm — основной класс программы, из которого вызываются все остальные классы;
3. FunctionClass — класс, содержащий методы подключения к базе данных и методы автозаполнения элементов форм;
4. UsersForm — класс, реализующий добавление нового пользователя;
5. EditUser — класс, реализующий редактирование выбранного пользователя;
6. DeleteUserForm — класс, реализующий удаление выбранного пользователя;
7. ChangeUserPass — класс, предназначенный для смены пароля пользователя;
8. NewMagForm — класс, предназначенный для добавления нового магазина;
9. EditMagForm — класс, предназначенный для редактирования выбранного магазина;
10. DeleteMagForm — класс, предназначенный для удаления выбранного магазина;
11. EmailSettingsForm — класс, реализующий изменение настроек подключения к почтовому серверу.

Работа с электронной почтой

После авторизации в разработанной автоматизированной системе для выгрузки файлов на электронную почту необходимо выбрать пункт меню «Файл->Выгрузить в магазин» (рисунок 1).

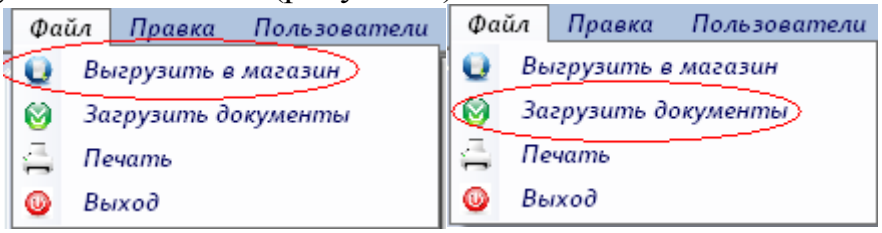

Рисунок 1 — Выгрузка и загрузка файлов

Если скорость подключения к сети Интернет будет слишком низкая для передачи либо подключение будет отсутствовать – появится соответствующее предупреждение (рисунок 2).

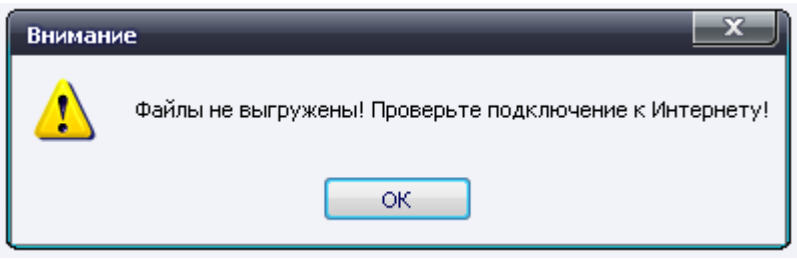

Рисунок 2 — Неудачная передача файлов

Если подключение к почтовому серверу прошло успешно – начнется процесс формирования письма и его отправка на электронную почту (рисунки 3).Этапы формирования электронного письма:

1. Подключение к почтовому серверу.
2. Шифрование файлов с помощью алгоритма RSA либо AES.
3. Формирование архива с паролем, и добавление в него файлов.
4. Формирование электронного сообщения с вложением.
5. Проверка «электронного ящика» на наличие старых писем. Если обнаружено старое письмо – происходит его удаление с помощью методов протокола POP3.
6. Отправка письма на электронную почту по протоколу SMTP.
7. Закрытие соединения с почтовым сервером.

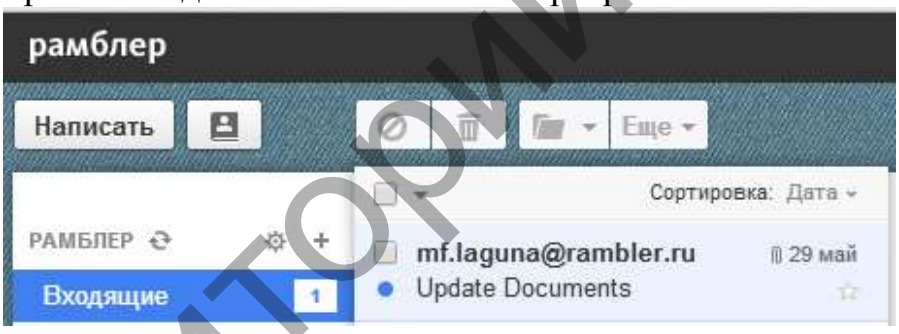

Рисунок 3 — Результат отправки письма

Для загрузки файлов из электронной почты необходимо выбрать пункт меню «Файл->Загрузить документы» (рисунки1, 4). Если подключение к почтовому серверу прошло успешно – начнется процесс чтения письма. Этот процесс состоит из следующих этапов:

1. Подключение к почтовому серверу.
2. Проверка «почтового ящика» на наличие письма.
3. Чтение письма.
4. Распаковка архива с файлами.
5. Замена старых папок на новые и перемещение в них файлов.
6. Применение обновлений в программе.
7. Закрытие соединения с почтовым сервером.

Рисунок 4 — Результат загрузки и преобразования папок

Разработанный программный продукт позволяет сотрудникам данного предприятия значительно снизить временные и финансовые затраты на отправку документов отдаленным структурам, а также, сохранить их конфиденциальность.

Использованные источники:

1. Поляков А.С. Анализ возможностей алгоритмов международного стандарта «Облегченная криптография» - ISO/IEC 29192-2:2012 / А.С. Поляков, В.Е. Самсонов // Информатика. – 2014. -- № 3. – С.107-112.