УДК 004.056

К.В. Димова,
преподаватель кафедры информационных технологий и систем
Дальневосточного государственного университета путей сообщений
(г. Хабаровск)
Р.А. Ешенко,
канд. техн. наук, доцент кафедры информационных технологий и систем
Дальневосточного государственного университета путей сообщения
(г. Хабаровск)

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ С УЧЕТОМ ВЫБОРА ОПТИМАЛЬНЫХ МЕТОДОВ ШИФРОВАНИЯ

В данной статье рассматриваются такие определения, как персональные данные, их сбор и хранение, понятие оператора, обрабатывающего большие объемы информации. Описывается подбор наиболее оптимального метода варианта системы защиты информации. В качестве критерия выбора системы защиты информации предлагаются способы шифрования с закрытым и открытым ключами.

Ключевые слова: *персональные данные, менеджер паролей, информационная безопасность, криптография, открытый ключ, закрытый ключ.*

This article examines certain definitions as personal data, its collection and storage, concept of the operator processing large amounts of information. The selection of the most optimal method of information security system is described. Methods of encryption with private and public keys are proposed as a criterion for choosing an information security system.

Keywords: *personal data, password manager, information security, cryptography, public key, private key.*

Защита персональных данных – актуальная проблема, которая существует на сегодняшний день. Довольно остро стоит данная проблема на больших предприятиях, объем информации которых достигает небывалых масштабов.

Проблемы информационной безопасности актуализируются на предприятиях с ростом информационных ресурсов, баз данных, с применением информационных технологий.

К персональным данным относится любая информация, прямо или косвенно относящаяся к физическому лицу [1]. На больших предприятиях с персональными данными, как правило, работает оператор, обрабатывающий большой поток информации. К оператору относится государственный орган, муниципальный орган или физическое лицо, организующий или осуществляющий работу с данными. В компетенции оператора входит определе-

ние цели обработки, состав персональных данных, которые подлежат обработке.

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации [1]. Таким образом, оператор обязан самостоятельно или с привлечением на договорной основе юридических лиц либо индивидуальных предпринимателей (имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации) осуществлять оценку эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности [2].

В состав мер по обеспечению безопасности персональных данных, входят:

– идентификация и аутентификация;

– защита машинных носителей информации, на которых хранятся и производится обработка персональные данных;

– антивирусная защита;

– защита информационной системы, ее средств систем связи и передачи данных, и т.д.

Таким образом, защита персональных данных является важной государственной задачей [2]. На основании этого и возникает необходимость в создании различного программного обеспечения, помогающего обеспечить некоторые функции по защите персональных данных [3].

Менеджер паролей –один из видов программного обеспечения, предназначенный для хранения персональных данных с применением криптографических методов защиты.

Шифрование является одним из самых распространенных методов обеспечения безопасности персональных данных. При шифровании создаются такие условия, что похищенная информация при отсутствии специального ключа не представляет собой никакой ценности. Это способ изменения сообщения, другого документа, обеспечивающий искажение его содержимого. Для восстановления зашифрованной информации требуется ключ и знание правил шифрования. Под ключом понимается конкретное секретное состояние параметров алгоритмов шифрования и дешифрования [4]. Шифровальные методы подразделяются на два направления:

1. Симметричные классические методы с секретным ключом. Данные методы используют один ключ на зашифровку и дешифровку (рисунок 1).

2. Асимметричные методы с открытым ключом. Данные методы подразумевают два различных ключа для зашифровки и дешифровки. При данном методе один из ключей назначается секретным, а второй – открытым.

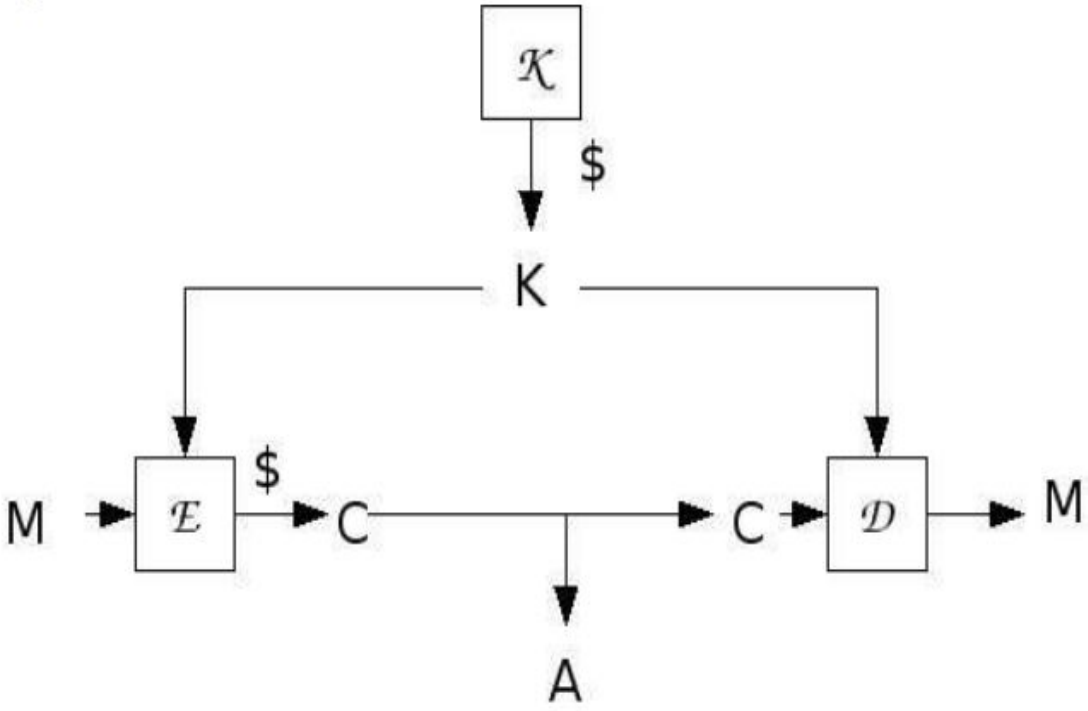

Рисунок 1 – Схема симметричного шифрования

Формально симметричная схема шифрования может быть описана следующим образом:

$$SE = (K, E, D), \qquad (1)$$

где *K* – это алгоритм генерации ключа К;

E (M, K) = C – алгоритм шифрования открытого текста М на ключе К, результатом которого является шифротекст С;

D(C, K) = M – алгоритм расшифрования шифротекста С на ключе К, результатом которого является открытый текст М.

Наиболее важный компонент схемы симметричного шифрования – используемый в ней алгоритм шифрования. На данный момент выделяют блочные и поточные алгоритмы шифрования:

1. Блочные шифры. Обрабатывают информацию блоками определённой длины (обычно 64, 128 бит, как, например, в DES или AES), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами.

2. Поточные шифры, в которых шифрование проводится над каждым битом, либо байтом исходного (открытого) текста с использованием функции гаммирования.

Таким образом, обладая высокой скоростью шифрования, одноключевые криптостистемы позволяют решать многие важные задачи защиты информации.

На основании вышеизложенного разработано приложение, реализующее функцию хранения и защиты конфиденциальных данных (рисунок 2).

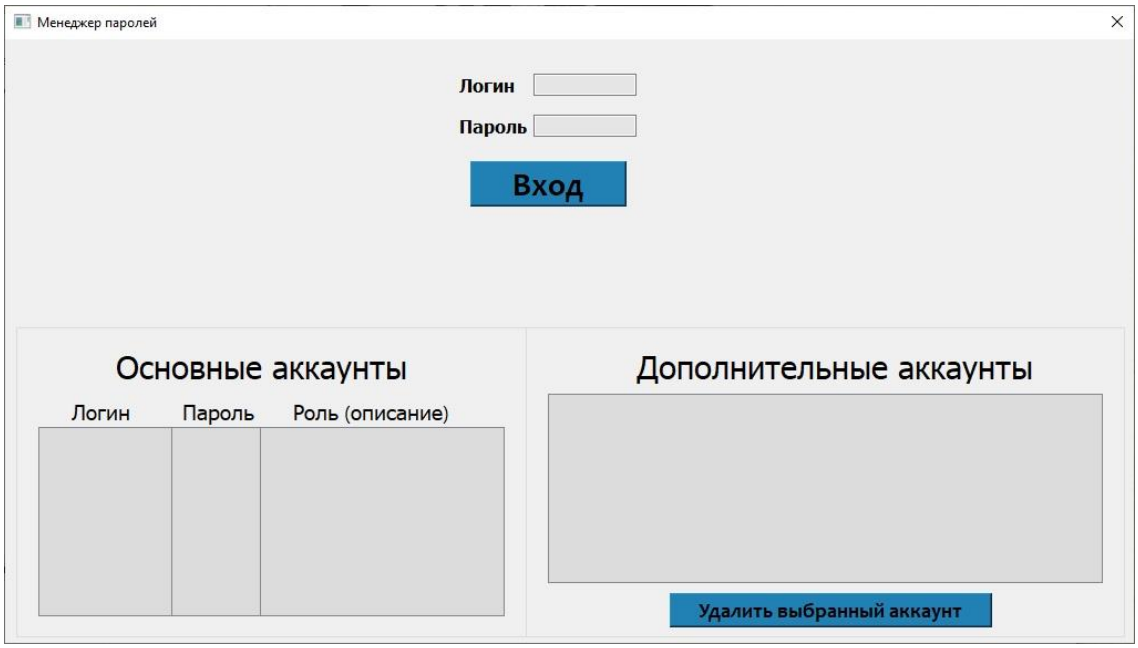

Рисунок 2 – Главное окно программы

Программа написана на языке программирования Python. Используется симметричный метод шифрования, который гарантирует, что зашифрованное сообщение не может быть обработано или прочитано без ключа.

Данная программа адаптирована для сотрудников крупных предприятий и организаций и предназначена для создания, добавления и хранения конфиденциальных данных сотрудника внутри организации (таблица «Основные аккаунты»), а также для хранения личных данных сотрудника от других информационных ресурсов, используемых за пределами предприятия (окно «Дополнительные аккаунты»).

Список использованных источников

1 О персональных данных : федер. закон от 27.07.2006 г. № 152-ФЗ (в ред. от 31.12.2017 г.) // www.consultant.ru/document/cons_doc_LAW_ (дата обращения 01.06.2019).

2 Приказ ФСТЭК России от 18.02.2013 г. № 21 // fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (дата обращения 03.06.2019).

3 Приказ ФСТЭК России от 11.02.2013 г. № 17 // https://fstec.ru (дата обращения 31.05.2019).

4 Назначение и структура алгоритмов шифрования // https://www.ixbt.com/soft/alg-encryption.shtml (дата обращения 03.06.2019).