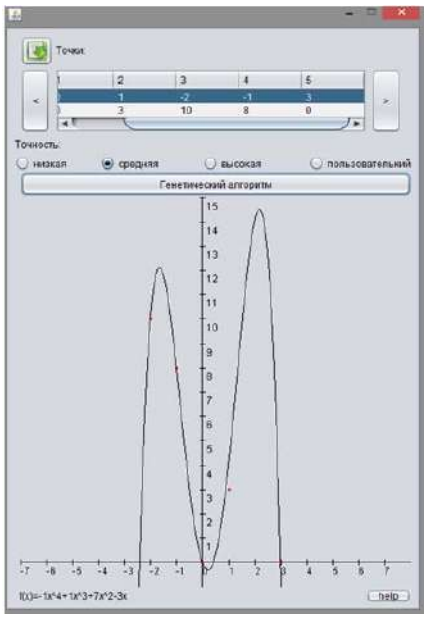

Рисунок 2 — Отображение результатов вычисления генетическим алгоритмом со средней точностью

Для работы приложения необходимо 2 Гб или более оперативной памяти, процессор Intel Pentium 1.87GHz, свободное место в размере 1 Мб на жестком диске, установленные на устройстве ОС Windows XP и выше, а также установленная среда выполнения Java-приложений Java Runtime Environment (JRE) или инструментальный пакет для разработчиков Java Development Kit (JDK) версии 1.8.0.

Разработанный программный продукт можно использовать для исследования изменения протекающего процесса, зная его промежуточные состояния, что позволяет применять приложение в различных сферах деятельности для анализа и прогнозирования.

Список цитируемых источников

1. *Глазачев, К. И.* Разработка параллельных алгоритмов глобальной оптимизации / К. И. Глазачев, А. Н. Коварцев // Перспективные информационные технологии ПИТ-2012 : науч. тр. / Самар. науч. центр РАН. — Самара, 2012. — С. 87—91.

2. *Емельянов, В. В.* Теория и практика эволюционного моделирования / В. В. Емельянов, В. М. Курейчик. — М. : ФИЗМАТЛИТ, 2003. — 432 с.

УДК 004.9

Д. М. Маратов, С. А. Попова
Учреждение образования «Барановичский государственный университет», Барановичи

ПРОГРАММНОЕ СРЕДСТВО ШИФРОВАНИЯ ДАННЫХ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX

Введение. Криптография (греч. скрытая рукопись) — это наука и искусство создания секретного кода. Шифрование данных — процесс искажения информации в целях её сокрытия от неавторизованных лиц, а также предоставление доступа авторизованным пользователям.

Компьютер-отправитель при шифровании и передаче данных по сети преобразует эту информацию в непонятную путаницу, называемую «шифротекстом». Обратное преобразование в читаемое состояние возможно при помощи определённого секретного ключа, сообщающего компьютеру-получателю, как расшифровать входящую зашифрованную информацию.

Разного рода шифры использовались еще за тысячи лет до нашего времени, а машины, которые могли зашифровать и расшифровать сообщения, были разработаны задолго до того, как появился современный компьютер. В современном мире крупнейшие компании и государственные службы выполняют шифрование данных, чтобы скрыть ценную информацию, обеспечить ее безопасность и сохранность. Сегодня шифрование

собственных данных является необходимым условием и для пользователя персонального компьютера, что обусловливает актуальность данной темы.

Основная часть. Проводя анализ современных Windows- и Unix-подобных операционных систем (далее — ОС), в частности, дистрибутивов Linux BSD, Debian и FreeBsd, было замечено, что они не используют по умолчанию шифрование данных, т. е. файлов, хранящихся на жестких дисках персональных компьютеров, и они открыты для доступа. Конечно, можно поставить пароль пользователя при входе в систему и тем самым создать иллюзию того, что обеспечена защита данных от несанкционированного доступа. Для этого было проведено тестирование компьютеров под управлением ОС Linux без активации шифрования данных, но с защитой паролем при входе в систему. Чтобы на каждом из этих компьютеров получить доступ к файлам без «взлома» пароля, понадобился флеш-накопитель с предустановленной ОС Arch Linux или другим дистрибутивом и немного знаний системного администрирования. На первом этапе необходимо подключить флеш-накопитель и загрузить компьютер, после чего в командной строке необходимо определить нужные накопители и разделы при помощи команды ls-blk, при этом ds по умолчанию является суперпользователем root. Далее следует монтировать нужные нам диски и разделы при помощи команды mount /dev/sdxX /path, где /dev/sdxX является разделом накопителя или самим накопителем. Таким образом, можно перейти в требуемые директории монтированных разделов и, соответственно, иметь полный доступ к файлам, хранящимся на них. Например, можно подключить еще один внешний накопитель, а затем скопировать или переместить на него файлы данных разделов, а при помощи команды arch-chroot можно получить права суперпользователя уже не снаружи, а на установленной ОС выполнить подобного рода действия.

В ходе проведенного тестирования было доказано, что, не имея шифрования данных, хранящихся на диске, их можно легко и без каких-либо ограничений похитить, повредить, уничтожить и т. д.

Учитывая вышеизложенное, была поставлена цель — разработать программное средство для выполнения шифрования данных, находящихся на накопителе компьютера под управлением ОС Linux, для их защиты от несанкционированного доступа. Объектом исследования является процесс шифрования данных. Предметом исследования являются программные средства реализации алгоритмов шифрования данных. В качестве алгоритма шифрования был выбран Twofish — блочный шифр с симметричным ключом, размером блока в 128 бит и размером ключа до 256 бит [1].

Разрабатываемое программное средство получило название “Sisyph”, имеет расширение .o и является консольным приложением. В качестве технических средств был использован язык программирования C++, текстовый редактор Vim, набор компиляторов Gnu gcc и ОС Arch Linux. Для выполнения шифрования в командной строке достаточно написать команду запуска программы, передав в качестве аргумента путь к файлу или директории. Представим окна шифрования файла (рисунок 1) и директории (рисунок 2) соответственно.

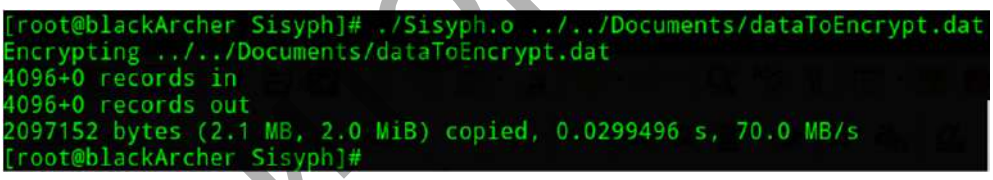

Рисунок 1 — Шифрование одного файла

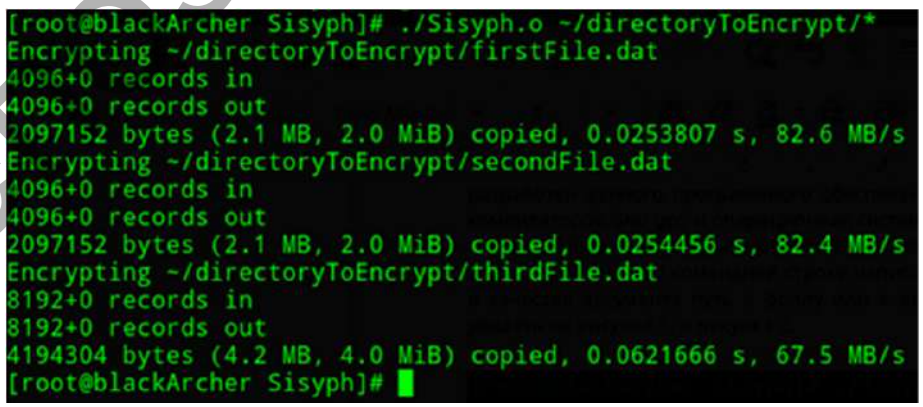

Рисунок 2 — Шифрование директории

При передаче в качестве аргумента пути к файлу или директории автоматически генерируется ключ шифрования длиной в 256 бит. Можно использовать свой ключ шифрования. Для этого требуется запустить программу без аргументов (рисунок 3).

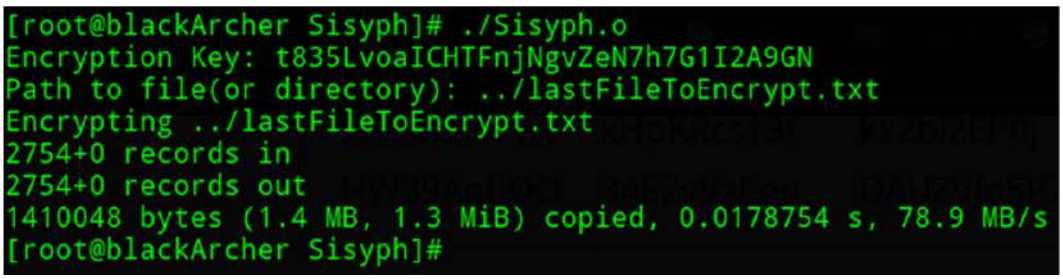

Рисунок 3 — Шифрование данных собственным ключом

Все зашифрованные файлы имеют расширение .Sisyph, чтобы отметить, какие файлы были зашифрованы, а какие нет. Для того чтобы расшифровать данные, хранящиеся в файле, необходимо при запуске программы передать в качестве аргумента Decrypt и путь к файлу (рисунок 4).

Рисунок 4 — Расшифрование файла

Заключение. Программное средство “Sisyph” позволяет зашифровать и расшифровать данные, хранящиеся на диске, а при дальнейшей доработке, как работа в сети, может стать полезным инструментом администрирования.

Список цитируемых источников

1. Обзор алгоритма шифрования Twofish [Электронный ресурс]. — Режим доступа: https://www.schneier.com/academic/twofish/ . — Дата доступа: 18.01.2017.

УДК 004.9

А. В. Мачкасова, О. Н. Горбунова
Федеральное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный университет имени Г. Р. Державина», Тамбов, Российская Федерация

О НЕКОТОРЫХ ИТ-ПРОДУКТАХ ДЛЯ МАЛОГО БИЗНЕСА

Введение. Целью данной статьи является изучение различных информационных технологий на предприятиях малого бизнеса. Объектом исследования в работе выступают информационные технологии, предметом исследования является их применение предприятиями малого бизнеса. Актуальность выбранной темы исследования не вызывает сомнения. Использование современных информационных технологий для крупного и среднего бизнеса становится неотъемлемой частью работы любого предприятия, а также входит в обиход частных предпринимателей и малого бизнеса.

Основная часть. Малое предпринимательство (малый бизнес) — предпринимательство, опирающееся на деятельность небольших фирм, малых предприятий, формально не входящих в объединения. Деятельность субъектов малого и среднего предпринимательства в России регулируется принятым 24 июля 2007 года Федеральным законом 209-ФЗ «О развитии малого и среднего предпринимательства в Российской Федерации», в котором указаны критерии отнесения предприятия к малому предпринимательству.

Потребности малого бизнеса стимулируют производителей ИТ-систем на создание различных специализированных продуктов, которые учитывают своеобразие деятельности и особенности использования ИТ-систем этими субъектами экономики.

Рассмотрим некоторые популярные программы, которые использует большинство предприятий малого бизнеса. Пакет Microsoft Office можно по праву назвать самой используемой программой в современном предпринимательстве. Основные приложения пакета MS Office:

– Microsoft Office Word — текстовый редактор, который предназначен для создания и изменения текстовых документов;