ционному преподаванию только квалифицированных специалистов;
- тщательный профессиональный отбор преподавателей экономических дисциплин (преподавателей, не занимающихся научной работой, следует привлекать лишь для выполнения рутинных учебных работ (рефераты, обозрения, теоретические работы);
- расширение важнейших практических форм обучения слушателей: практические, лабораторные, семинарские занятия за счет сокращения часов лекционных занятий;
- усиление творческого аспекта экономического обучения;
- усиление отраслевой специализации преподавания экономических дисциплин слушателям технической ориентации.

УДК 378.1

КРИПТОГРАФИЯ И ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ОПЕРАЦИОННЫХ СИСТЕМАХ LINUX И WINDOWS

Ганжа В.А.
Белорусский государственный университет информатики и радиоэлектроники
Чичко О.И.
Белорусский национальный технический университет
Минск, Беларусь

Описываются возможности использования различных операционных сред для решения задач защиты информации пользователя в рамках возможностей традиционного метода шифрования с асимметричным ключом. Приводятся примеры работы пакетов одинакового функционального назначения, но в разных операционных системах, использующих разные команды и ключи интерфейса командной строки. Показывается, что, несмотря на внешнее различие интерфейса программ и различия операционных систем, достигается один и тот же результат.

В настоящее время на фоне общего удешевления аппаратных средств и увеличения функциональных возможностей этих аппаратных средств мы наблюдаем развитие сектора настольных и переносных ОС (операционных систем). В результате острой конкурентной борьбы сейчас превалируют три клона таких ОС: ОС клона Macintosh; ОС Linux; и ОС Microsoft. Авторы этой маленькой заметки далеки от мысли приводить здесь сравнительный анализ всех этих систем – это замысел для большой обзорной статьи. Наша цель другая. Сейчас мы наблюдаем тенденцию миграции пользователей от одной ОС к другой. В силу полной проприетарности систем Macintosh (англ. proprietary software; от proprietary – частное, патентованное, в составе собственности и software – программное обеспечение), их дороговизны и незначительного присутствия в Белоруссии, мы не будем их здесь рассматривать; хотя эти ОС отличает высокое качество аппаратной составляющей, надёжное программное обеспечение и красивый дружественный графический интерфейс пользователя.

Вот почему дальше мы поговорим лишь о ОС Linux и Microsoft. Хочется заострить внимание читателей на проблемах безопасности информации, которую предоставляют эти ОС обычному пользователю. В своей работе [1] авторы подробно

остановились на некоторых аспектах информационной безопасности, в общем, и применительно к конкретной ОС Microsoft Windows в частности. В этой работе была продемонстрирована эффективность простейших криптографических средств защиты информации пользователя, корни которых восходят к классическим работам Шеннона, которые можно найти в сборнике [2].

Апробация этих идей была проведена в течение нескольких лет преподавания авторами дисциплины «Безопасность информации и обеспечение надёжности компьютерных систем» при подготовке инженеров-программистов.

После изложения лекционно-теоретического материала, слушателям переподготовки предлагались практические задания, описанные в [1]. Цикл упражнений включал в себя вычисление хэш-функций по стандартному алгоритму MD-5. Слушателям было предложено также несколько упражнений, использующих программу стеганографии. Эти программы от сторонних производителей адаптированы под ОС Windows и используют её графический интерфейс.

Следующий каскад упражнений предлагал слушателям выполнить ряд заданий по освоению пакета PGP (Pretty Good Privacy) в состав которого входит:

- овладение шифрованием данных с использованием симметричного ключа;
- создание пары ключей для асимметричного шифрования;
- создание зашифрованного сообщения с помощью открытого ключа;
- декодирование принятого зашифрованного сообщения с помощью приватного ключа;
- создание цифровой подписи.
- верификация цифровой подписи.

Эта версия пакета PGP первоначально работала в консоли систем UNIX, а потом была адаптирована разработчиками метода асимметричного шифрования для работы в консоли MS DOS и использует интерфейс командной строки, который как нельзя лучше подходит как «полигон» для обучения будущих инженеров-программистов.

Как было отмечено в начале этой заметки, в последнее время ОС клона Linux потеснили ОС фирмы Microsoft, хотя всё равно не имеют существенного значения для массового пользователя настольных ОС, и вызывают интерес только среди профессионалов, какими являются будущие инженеры программисты.

Как решаются проблемы безопасности в ОС Linux? Какие средства предлагает эта ОС? Рассмотрим эти вопросы под углом зрения тех же задач, которые были затронуты здесь выше и в [1]. Желание авторов было добиться минимальными средствами тех же целей в параллельной ОС Linux при миграции грамотного пользователя (слушателя, будущего инженера-программиста) от ОС фирмы Microsoft к ОС Linux.

В ОС Linux для многих программ из вышеперечисленных, нет необходимости искать стороннего разработчика, поскольку многие из них встраиваются в ОС и присутствуют там сразу же после инсталляции. Ниже описываются две такие программы: вычисление хэш-функции и пакет PGP.

В системах Linux присутствует небольшая программа, запускающаяся по команде md5sum, которая вычисляет значения хэш-функций заданных файлов по алгоритму MD5. Эта небольшая программа позволяет пользователю совершать все распространённые манипуляции для создания и проверки контрольных сумм, описанных авторами в [1] для ОС Windows:

- создавать в командной строке 128-битную контрольную сумму одного задан-

ного файла или нескольких файлов;
- перенаправлять и записывать эти контрольные суммы в файл, с целью дальнейшей обработки и анализа;
- читать контрольную сумму MD5 из командной строки и сверять её с контрольной суммой файла;
- читать список контрольных сумм MD5 из сохранённого файла и сверять их с контрольной суммой проверямых файлов.

Функции программы PGP, работающей в ОС Windows, в Linux системе доступны при выполнении команды gpg2. Она тоже встроена в систему Linux и может работать как в консоли, так и использовать графическую оболочку KDE или GNOME. Эта программа позволяет пользователю выполнять все следующие функции, предусмотренные при работе кодирования данных по методу асимметричного шифрования:
- создание в интерактивном режиме публичного и приватного ключей пользователя;
- использование различных алгоритмов шифрования для создаваемой пары ключей, в зависимости от поставленной задачи (для подписи, для шифрования);
- установка срока действия, длины, идентификатора и пароля для создаваемой пары ключей;
- кодирование отправляемых по электронной почте сообщений, кодирование данных из файла в файловой системе с использованием публичного ключа;
- расшифровка входящих сообщений по электронной почте, расшифровка данных из файла в файловой системе с использованием закрытого (приватного) ключа и пароля;
- создание цифровой подписи сообщения с использованием закрытого (приватного) ключа и пароля;
- верификация цифровой подписи сообщения с использованием публичного ключа.

Вышеприведенные методики освоения шифрования в параллельных ОС помогают слушателям, будущим инженерам-программистам, осуществить миграцию между различными операционными системами и адаптироваться в незнакомой среде.

1. Ганжа, В.А. Безопасность информации и обеспечение надёжности компьютерных систем: учебно-методическое пособие для слушателей системы повышения квалификации и переподготовки / В.А. Ганжа, В.В. Сидорик, О.И. Чичко. – Минск: БНТУ, 2010. – 67 с.
2. Шеннон, К. Э. Работы по теории информации и кибернетике: [Сборник статей]. Пер. с англ. / С предисл. А. Н. Колмогорова. Под ред. Р. Л. Добрушина и О. Б. Лупанова. – М.: Изд. иностр. лит., 1963. – 829 с.