ной техникой. По мнению многих специалистов, новые информационные образовательные технологии на основе компьютерных средств позволяют повысить эффективность занятий на 20-30 %. Внедрение компьютера в сферу образования стало началом революционного преобразования традиционных методов и технологий обучения и всей отрасли образования.

УДК 004.7(076)

МЕТОДИКА ИСПОЛЬЗОВАНИЯ ВИРТУАЛЬНОЙ МАШИНЫ DOSBOX ДЛЯ ОБУЧЕНИЯ И ОСВОЕНИЯ СЛУШАТЕЛЯМИ КРИПТОГРАФИЧЕСКОГО ПАКЕТА PGP

THE METHOD OF DOSBOX-VIRTUAL MACHINE USE FOR TEACHING PGP-CRYPTOGRAPHY

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

Рассматривается проблема обучения студентов практическим навыкам работы по схеме криптографии с открытым ключом.

This article is dedicated to the problem of training students in practical skills of cryptography scheme with public-key.

Несмотря на то, что к 2016 году накоплено огромное количество литературы и наработок по теме защиты информации, в настоящее время всё равно наблюдается неослабевающий интерес к методам защиты информации в различных информационных системах. Это обусловлено тем, что в информационные технологии продолжают вовлекаться массы людей, представляющие широкий социальный срез населения, куда могут попасть не вполне благополучные и не вполне благонадёжные категории пользователей, ищущих свой интерес в нарушениях штатной работы информационных систем, во взломе компьютерных сетей организаций [1].

Учебной программой дисциплины «Методы защиты информации» предусмотрено практическое освоение криптографических пакетов с открытым ключом. Таким программным обеспечением является единственный пакет – PGP (Pretty-Good-Privacy), основанный на алгоритме асимметричного шифрования RSA.

С середины 90-годов пакет PGP распространял сам его «отец-основатель» Филипп Циммерманн (Philip Zimmermann) [2], основавший PGP-корпорацию. Но в 2010 году PGP-корпорация была приобретена фирмой Symantec [3]. Теперь пакет PGP доступен только от фирмы Symantec, лицензия на который стоит более $ 150. Дороговизна – одна из причин, по которой этот пакет мы не скоро увидим в компьютерном классе вуза.

Вторая причина в особенностях самого пакета PGP последней версии. Фирма Symantec продаёт сейчас пакет PGP 10-й версии. PGP-10, являясь проприетарным про-

граммным продуктом, как и большинство программ, разработанных под Windows, имеет хронические «болячки», заключающиеся: в разбрасывании файлов по разным каталогам; создании не вполне очевидных записей в системном реестре и в сокрытии многих деталей работы криптографического алгоритма с открытым ключом.

Авторам не удалось в учебных целях вычленить из рабочих файлов программы PGP-10 открытый и закрытый ключи; не удалось также «обмануть» программу и зашифровать файл, не имея электронной почты. Программа при инсталляции настойчиво ищет на машине почтового клиента Thunderbird, Outlook и ему подобные и шифрует файлы с целью непременной отсылки по электронной почте, через интернет некому адресату.

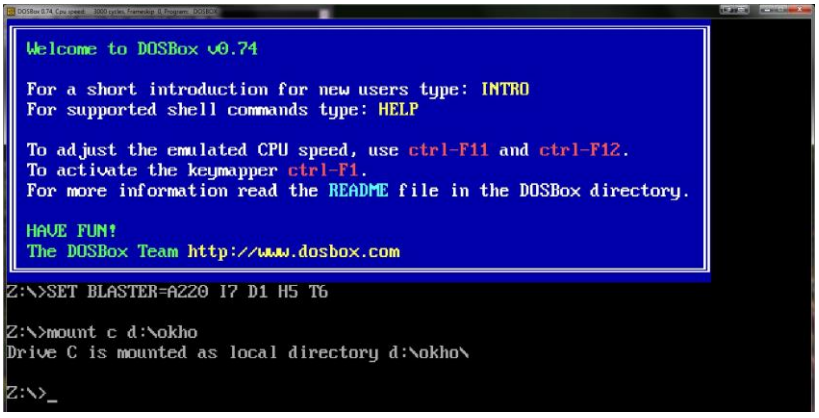
В описании PGP-10.2 присутствуют следующие строки «PGP Corporation представила персональный пакет защиты и шифрования данных, где реализованы средства автоматического исполнения для организации корпоративной защиты. Полностью автоматическая работа пакета PGP Desktop *скрывает от пользователя все действия по кодированию или декодированию данных*».

Быть может это и хорошо для рядового пользователя, но совершенно недопустимо при обучении будущего программиста, будущего специалиста по информационным технологиям. Для этой категории обучаемых необходимо полностью показать и продемонстрировать всю «кухню», всю анатомию работы криптоалгоритма RSA.

Оптимальным вариантом оказалась одна из первых 16-разрядных версий пакета PGP-5, который бесплатно распространялся ещё Филиппом Циммерманном и который без проблем запускается в консоли любой 32-разрядной машины Windows XP/7. Однако в большинстве минских вузов произошло поголовное обновление компьютерных классов на 64-разрядные машины, а в 64-разрядной консоли пакет PGP-5 работать не может.

Выход только в использовании виртуальной машины. Опять-таки, для компьютерного класса вуза выбор оказался предопределён: виртуальная машина Vmware не подходит, поскольку достаточно тяжеловесна, капризна и далеко не бесплатна. Виртуальная машина DOSBox версии 0.74 [4] оказалась самым подходящим вариантом, она в качестве гостевой операционной системы может быть инсталлирована и запущена в любой 64-разрядной среде. DOSBox – очень простая программа и к тому же с открытым исходным кодом, то есть бесплатная в отличие от других виртуальных машин.

На рисунке показано окно запущенной виртуальной среды DOSBox, где в качестве виртуального диска C: смонтирована ветка реальной файловой системы хостовой машины d:\okno.



Окно запущенной виртуальной среды DOSBox

Простота использования и небольшой набор команд способствует быстрому обучению и освоению студентами пакета DOSBox. Эта программа была установлена на компьютерах в нашем учебном классе.

С помощью этого пакета в компьютерном классе удалось выполнить практические работы по всем стандартным вопросам [5] освоения пакета PGP, предусмотренные учебной программой:

- использование функции симметричного шифрования по алгоритму IDEA;
- создание пары ключей для работы по алгоритму RSA;
- обмен ключом шифрования по алгоритму Диффи-Хеллмана;
- рассылка открытого ключа студентами группы друг другу и организация локального обмена зашифрованными сообщениями;
- расшифровывание полученных сообщений личным ключом;
- создание цифровой подписи личным ключом;
- верификация цифровой подписи списка предложенных файлов.

1. Ганжа, В.А. Компьютерные сети. Информационная безопасность и сохранение информации: учеб.-метод. пособие / В.А. Ганжа, В.В. Сидорик, О.И. Чичко. – Минск : БГУИР, 2014. – С. 128.
2. Филипп Циммерманн – разработчик PGP [Электронный ресурс]. – Режим доступа : http://philzimmermann.com/RU/background/index.html. – Дата доступа : 26.03.2016.
3. Symantec Encryption Solutions (Protect Information anywhere and ensure regulatory compliance) [Электронный ресурс]. – Режим доступа : https://www.symantec.com/products/information-protection/encryption. – Дата доступа : 26.03.2016.
4. DOSBox [Электронный ресурс]. – Режим доступа : http://www.dosbox.com. – Дата доступа : 26.03.2016.
5. Левин, М. PGP. Кодирование и шифрование информации с открытым ключом / М. Левин. – М. : Бук-пресс, 2006, – С. 166.

УДК 378,004.9

СОВРЕМЕННЫЕ ДИСТАНЦИОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ МЕТОДИКИ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ РЕСУРСОВ

MODERN DISTANCE LEARNING METHODS USING ELECTRONIC RESOURCES

Донской А.Д., Сабо С.Е.
Donskoy A., Sabo S.
Московский государственный областной Технологический университет
Королев, Россия

На основе опыта работы в дополнительном образовании, рассматриваются вопросы использования дистанционных обучающих технологий.

On the basis of experience in additional education, the use of distance learning technologies is discussed.