

3. Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 138562. 20.03.2014. Бюл. № 8.
 4. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений: Патент на полезную модель № 139532. 20.04.2014. Бюл. № 11.
 5. Мобильный компьютер с аппаратной защитой доверенной операционной системы: Патент на полезную модель № 147527. 10.11.2014. Бюл. № 31.
 6. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений: Патент на полезную модель № 151264. 27.03.2015. Бюл. № 9.
 7. Рабочая станция с аппаратной защитой данных для компьютерных сетей с клиент-серверной или терминальной архитектурой: Патент на полезную модель № 153044. 27.06.2015. Бюл. № 18.
 8. *Конявский В. А.* Компьютер с вирусным иммунитетом // Информационные ресурсы России. 2015. № 6. С. 31–34.
-

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНОЙ МАШИНЫ DOSBOX ПРИ ИЗУЧЕНИИ КРИПТОГРАФИЧЕСКОГО ПАКЕТА PGP

В. А. ГАНЖА, О. И. ЧИЧКО

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

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 программным 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 вычлениить 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 неперенной отсылки по электронной почте, через интернет некому адресату.

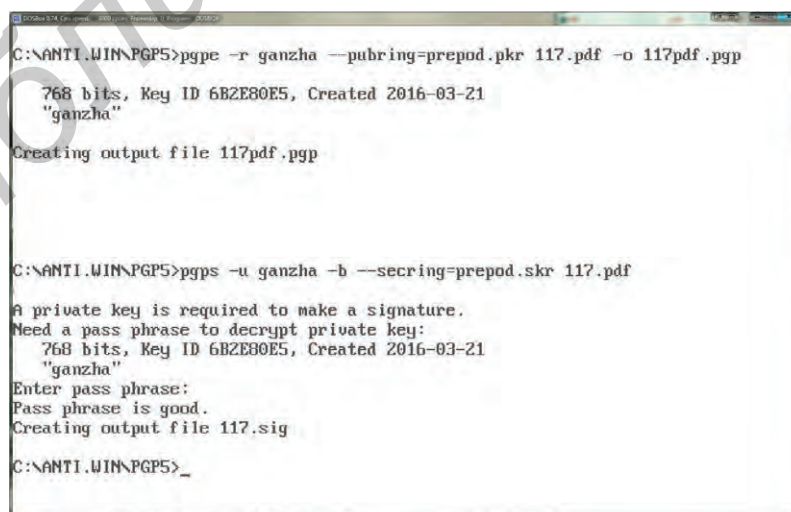
В описании PGP 10.2 присутствуют следующие строки «PGP Corporation представила персональный пакет защиты и шифрования данных, где реализованы средства автоматического исполнения для организации корпоративной защиты. Полностью автоматическая работа пакета PGP Desktop скрывает от пользователя все действия 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 пакета PGP и 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: замечательная 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 — вполне простая программа и к тому же с открытым исходным кодом, то есть бесплатная в отличие от других виртуальных машин.

На рисунке 1 показано окно запущенной виртуальной среды DOSBox, где в качестве виртуального диска C: смонтирована ветка реальной файловой системы хостовой машины d:\anti.win\PGP5.



```
C:\ANTI.WIN\PGP5>pgpe -r ganzha --pubring=prepod.pkr 117.pdf -o 117pdf.pgp
768 bits, Key ID 6B2E80E5, Created 2016-03-21
" ganzha "
Creating output file 117pdf.pgp

C:\ANTI.WIN\PGP5>pgps -u ganzha -b --secring=prepod.skr 117.pdf

A private key is required to make a signature.
Need a pass phrase to decrypt private key:
768 bits, Key ID 6B2E80E5, Created 2016-03-21
" ganzha "
Enter pass phrase:
Pass phrase is good.
Creating output file 117.sig

C:\ANTI.WIN\PGP5>_
```

Рис. 1. Окно запущенной виртуальной среды DOSBox

На копии экрана (рисунок 1) представлена работа двух команд со всеми ключами. Первая — `pgre` шифрует файл `117.pdf` в закодированный файл `117pdf.pgp`; вторая команда `pgps` — создаёт электронную подпись `117.sig` для этого же файла `117.pdf`.

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 лабораторные 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.

ЛИТЕРАТУРА

1. *Ганжа В. А., Сидорик В. В., Чичко О. И.* Компьютерные сети. Информационная безопасность и сохранение информации. Учебно-методическое пособие. Минск БГУИР, 2014. — С. 128.
2. <http://philzimmermann.com/RU/background/index.html>
3. <https://www.symantec.com/products/information-protection/encryption>
4. <http://www.dosbox.com/>
5. *Левин М.* PGP. Кодирование и шифрование информации с открытым ключом. — М. Бук-пресс, 2006, — С. 166.

КРИПТОГРАФИЮ — НА СЛУЖБУ ЕГЭ!

М. М. ГРУНТОВИЧ

Закрытое акционерное общество «ОКБ САПР», Москва, Россия

В статье предлагается метод обеспечения конфиденциальности, целостности и неотказуемости при рассылке информации из центра с использованием типовых ключевых `USB`-токенов, при котором получить доступ к ее содержанию могут не менее двух из трех ее получателей.

Ключевые слова: шифрование, целостность, неотказуемость, разделение секрета.

Введение

Как-то перед нами была поставлена задача разработать безопасную систему рассылки контрольно-измерительных материалов КИМ ЕГЭ. Задача, на первый взгляд, типовая, однако у заказчика была еще одна вводная: для вскрытия контрольно-измерительных материалов необходимо присутствие не менее двух человек из трех представителей регионального центра тестирования.