Илья Чигрин,
Славянский университет Республики Молдова

КРИПТОГРАФИЧЕСКИЕ ПРИЛОЖЕНИЯ ШИФРОВАНИЯ. ТЕХНОЛОГИЯ АУТЕНТИФИКАЦИИ И ЗАЩИТЫ ДАННЫХ PGP

In work practical receptions of adjustment and feature of work with cryptographic system PGP are shown. Variants of enciphering of the text, a file, a disk are considered, specific functions of work of the program are briefly described.

Ключевые слова: *шифрование, криптография, технология открытых и закрытых ключей*

Поскольку симметричная криптография была некогда единственным способом пересылки секретной информации, цена надёжных каналов для обмена ключами ограничивала её применение только узким кругом организаций, которые могли её себе позволить, в частности, правительствами и крупными банковскими учреждениями. Появление шифрования с открытым ключом стало технологической революцией, предоставившей стойкую криптографию массам. PGP (Pretty Good Privacy) объединяет в себе лучшие стороны симметричной криптографии и криптографии с открытым ключом.

Целью работы является исследование на практике особенностей криптографического шифрования и защиты данных.

Предметом исследования является изучение функций и возможностей работы с ключами в криптографической системе PGP.

Удобство работы с PGP обусловлено как возможностью создания собственной пары ключей (открытый и секретный) – значок PGP в трее, пункт PGPkeys, так и получения своего публичного ключа в файле с расширением .asc. и сообщение его своим адресатам в меню Keys-Export. Точно так же при получении публичных ключей от своих адресатов их можно занести в PGPkeys, воспользовавшись меню Keys-Import.

Основными функциями криптографического шифрования в программе PGP являются: шифрование текста (Clipboard – Encrypt, Clipboard – Decrypt and Verify), шифрование файлов (PGP – Encrypt, Decrypt and Verify), создание зашифрованного диска (PGPdick – New Disk, Publick Key или Passphrase, PGPdisk – Mount Disk). Также в составе PGP есть интересные дополнительные возможности:

1. WIPER, т.е. программа для удаления файлов, исключающая возможность их последующего восстановления. **WIPER** перед удалением файла забивает его символами «a», что позволяет, не беспокоится о возможности восстановления информации.

2. ТАБЛЕТКА – определение Spoof-спрятанных в файл различными способами вредоносных ко-

дов, троянов, вирусов с помощью клавиатурных шпионов – key logger в комплексе с антивирусными программами. Хорошим для этого примером служат Xinch и Pinch, скорее всего более известные среди тех, у кого уже крали ICQ семизнаки или читали почту (возможных вариантов много). В основном это проработанный key loggerp, который не требует установки, и может быть прикреплён к любому файлу, даже к картинке в сети Internet, EXE файлу и любому документу. Хочется заметить, что более известные антивирусы, такие как NOD32/ Kaspersky / Avira / Avast, к спрятанной троянской программе относятся по-разному. Всё зависит от того, каким способом её спрятали. Например, Avira вообще может сообщить, что файл чист даже при незаурядном скрытии трояна. Xinch и Pinch нуждаются в настройках. Поскольку они идентичны, рассмотрим настройку Xinch. При этом используются файлы: Builder.exe – компиляция трояна и Parser.exe – расшифровка отчетов. Пример настройки на отправку по SMTP (т.е., по почте, самый легкий вариант) показан на **Рис.1.** Примеры будут приходить на почту topmail.kz, так как на нее стабильно приходят отчеты. Нам нужно заполнить поле «Свойства SMTP". В поле «сервер» нужно указать SMTP сервер вашей почтовой службы (сервер исходящих сообщений). В данном случае – это mail.topmail.kz. Дальше выбираем «Узнать IP" (узнаем IP нашего сервера – обязательно) и получаем 194.226.128.5. В поле «От кого» указываем электронный адрес, с которого нам будут высылаться отчеты (можно зарегистрировать себе там же 2-й почтовый ящик, а можно не регистрировать). В поле «Кому» – указываем e-mail, на который будут высылаться отчеты. «Порт» – как по умолчанию стоит 25, так и оставляем (это стандартный порт протокола SMTP). "Интервал» – собственно указываем временной интервал между отправкой отчетов (в секундах). Дальше на вкладке «Тест» – проверяем, все ли правильно мы настроили с отправкой отчетов. Если появляется сообщение «Соединение отсутствует»**,** то необходимо повторить настройки.

В случае правильно выполненных процедур и действий появляется сообщение, представленное на рис.2. Рекомендуется обязательно отметить вкладку «пароли». Кроме указанных, можно воспользоваться функциями и дополнительными процедурами. ***Функции:*** *самоуничтожение трояна (Удалиться), перезагрузка компьютера жертвы, удаление файлов (удаляет все, что можно на диске C:), автозагрузка (выбираете способы автозагрузки ксинча), таймер (указываете время активирования троя).* ***Дополнительно:*** добавление иконки, прикрепление файла (до 500-700 кб.), возможность загрузки и запуска файла жертвой с заданного URL, вывод сообщения после запуска трояна, выбор метода сжатия.

Завершающим этапом является выставление способа отправки (SMTP) в меню «компиляция» – вкладка «Скомпилировать» – рис. 3.

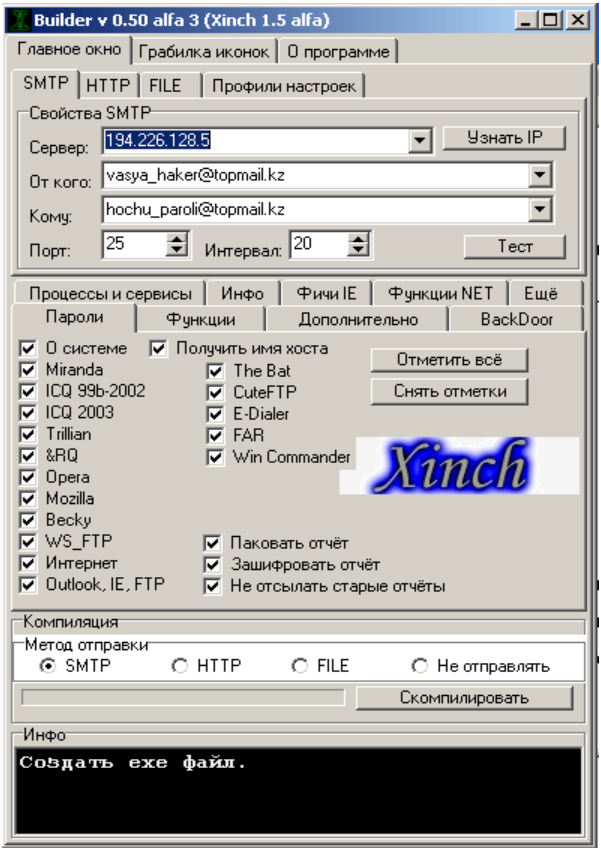

Рис.1. **Окно программы – пример настройки электронной почты**

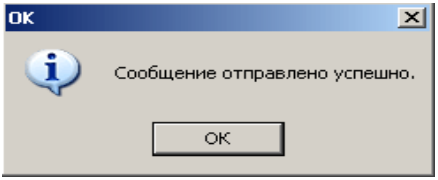

Рис.2. **Окно программы – подтверждение отправки сообщения**

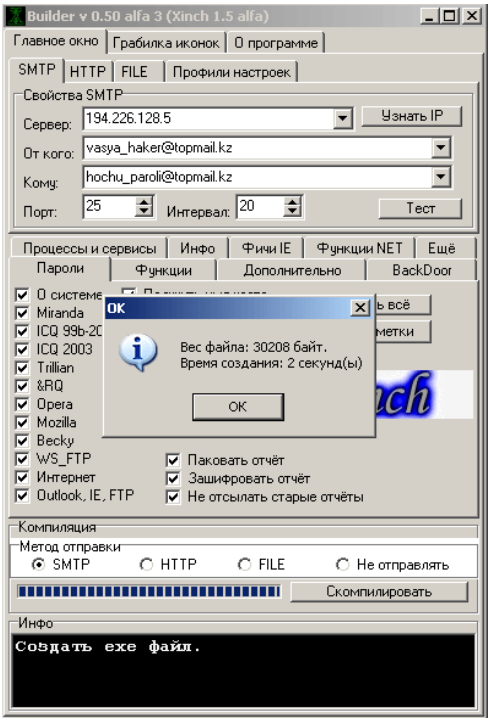

***Рис.3.* Окно программы – вкладка «Скомпилировать»**

Подводя итог, хотелось бы отметить, что большинство антивирусных программ не в силах справится с новыми вирусами, ещё не побывавшими в «лаборатории» по разработке «противоядия», и большинство компьютеров, возможно, заражены новичками, но пользователь об этом не сможет узнать, пока не обновится антивирус. Но к этому времени злоумышленник уже получит нужные ему данные, только в том случае, если его антивирус не снабжён достаточно хорошим элементом определения вредоносного программного обеспечения. В данных условиях использование криптографического приложения PGP является эффективной технологией для обеспечения защиты и аутентификации данных. Используя его, можно быть уверенным, что никто не сможет прочитать или изменить Вашу информацию. Защита гарантирует, что только получатель информации сможет воспользоваться ей. Оказавшись в чужих руках, она будет совершенно бесполезной, поскольку ее невозможно декодировать. Аутентификация будет гарантировать, что если некоторая информация

была создана Вами и выложена для публичного доступа, то она действительно поступила от Вас и не была никем фальсифицирована или изменена в пути. Кроме этого, PGP основана на криптографической системе, известной как «открытый ключ», которая может быть использована на ненадежных каналах. Это делает ее идеальной для обеспечения защиты информации, передаваемой по таким сетям, как Internet.

Литература и источники:

1. Масленников М.Е. *Практическая криптография*. – СПб.: Издательство БХВ-Петербург, 2003 г. / Учебник+CD диск, 464 с.: ил.
2. Чмора А.Л. *Современная прикладная криптография*. – М.: Издательство «Гелиос АФВ», 2001. – 240 с.
3. http://www.host.ru/support/hosting/pgp.html
4. https://www.pgpru.com

Kristina Gjeorgjieva
Faculty of Economics, University "Ss. Kiril and Methodius" – Skopje, Macedonia

INFORMATION AND INFORMATION SECURITY – FUNDAMENTAL FACTOR FOR ECONOMIC AND SOCIAL DEVELOPMENT

The information represents universal and essential recourse for the development of a society. The collection and accumulation of the information in modern societies and organization areas, based on knowledge, is the basic of the innovation processes and development. Due to the considerable importance of the information from an economic and social aspect, the need of safety appears, that is information security.

Man's development and his evolution are due to the information exchange. The knowledge has been transmitted and accumulated through the process of information exchange, also, has been transmitted the understanding, notification, consciousness, experience and changes caused by the human with the active relation towards the surroundings. In its early evolution, the man communicated through gestures, sounds, signs which were the first signal bearers of information, for later on to evolve the speech and the letter as a man to man communication. Due to the evolution process of the man and society, as well as the technology, today the information is exchanged on rela-