І.В. Крижанівська, к.т.н., доц.
В.Б. Крижанівський, к.ф.-м.н., доц.
Житомирський державний технологічний університет

ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ ПРИ ВИВЧЕННІ МАТЕРІАЛІВ З КУРСУ «БЕЗПЕКА ПРОГРАМ І ДАНИХ»

Сучасні комп'ютерні технології спричинили можливість перенесення у віртуальне середовище багатьох форм і способів навчання. Одним з логічних етапів розвитку нових форм навчання є створення віртуальних лабораторій, які містять у собі цифрові аналоги лабораторій університету, з усіма необхідними інструментами.

Особливо важлива роль віртуалізації у питаннях пов'язаних з безпекою програм та даних. В цьому випадку досить часто необхідно працювати з операційною системою (ОС) з правами адміністратора та втручатися в налаштування важливих служб. Але в процесі навчання природнім чином виникають помилки, які можуть привести до подальшої некоректної роботи ОС. Якщо б такі експерименти проводились на реальних комп'ютерах, то після кожної лабораторної роботи потрібно було б переналаштовувати значну частину комп'ютерів в лабораторії. Метою даної роботи є опис використання віртуальної лабораторії під час вивчення матеріалів курсу «Безпека програм та даних».

Відомо, що питання безпеки сьогодні є одними з найактуальніших. Кількість інформації з різних джерел з цього приводу просто астрономічна. В рамках одного курсу просто неможливо розглянути усі аспекти інформаційних технологій, які пов'язані з безпекою. Тому задача курсу буде досягнута, якщо у студента сформується свого роду «дорожня карта» для орієнтації в цій області. З точки зору авторів формування такої «дорожньої карти» слід починати з базової моделі безпеки, яка передбачає три складові: конфіденційність, цілісність і доступність. В подальшому, базову модель слід розширювати. Напрямок визначається реальними задачами, які з'являються перед фахівцем. Але це вже відбувається на тлі добре засвоєних базових знань.

Для засвоєння практичних навичок, які пов'язані з цілісністю і доступністю, в курсі «Безпека програм і даних» передбачається цикл лабораторних робіт наступного змісту.

1. Методи розгортання мережевої інфраструктури (метод дублювання дисків з використанням утиліти Sysprep; метод віддаленої установки з використанням сервера віддаленого встановлення ОС (RIS)).

2. Забезпечення безпеки зберігання даних (технологія створення тіньових копій даних; архівація даних (backup); створення відмовостійких томів для зберігання даних (RAID)).

3. Дослідження можливостей центру забезпечення безпеки Windows Security Center (налаштування виключень для вбудованого брандмауера Windows за допомогою локальних політик).

4. Системи аналізу захищеності корпоративної мережі (виявлення уразливостей) на прикладі продуктів: Microsoft Baseline Security Analyzer і XSpider.

5. Захист від шкідливого програмного забезпечення на прикладі Windows Defender.

Наступний цикл робіт переслідує задачу формування навичок, пов'язаних із забезпеченням конфіденційності.

1. Злам шифрів за допомогою частотного аналізу текстів. Студенту пропонується чотири шифровані тексти (кожен наступний шифротекст є складнішим для зламу, ніж попередній). Мета даної роботи продемонструвати головного «ворога» криптографів і головного «друга» криптоаналітиків – статистику появи в тексті літер та їх послідовностей.

2. Симетрична криптосистема на прикладі стандарту DES. Хоча цей стандарт вже замінений на AES, сам алгоритм шифрування залишається важливим тому, що він базується на мережі Фейстеля, яка залишається одним з дієвих механізмів для розробки нових шифрів.

3. Асиметрична криптосистема на прикладі алгоритму RSA.

4. Криптосистема PGP. В даній роботі використовуються асиметрична та симетрична криптосистеми для створення реального захищеного каналу між двома поштовими скриньками. В дійсності, ми маємо справу з поєднанням цілих трьох програм: поштового клієнту Thunderbird (або Mozilla Mail), плагіну Enigmail і, власне, криптосистеми GnuPG. Всі три - вільні і безкоштовні продукти (free open source software). Результат - захист листування без особливих надзусиль. З теоретичної точки зору в даній роботі студент отримує цілісне уявлення про спільну роботу трьох найважливіших криптографічних примітивів: асиметричної криптосистеми, симетричної криптосистеми та алгоритму хешування. З їх допомогою реалізується три сервіси: 1. Автентифікація повідомлень (рис. 1); 2. Шифрування повідомлень (рис. 2); 3. Автентифікація та конфіденційність повідомлень одночасно.

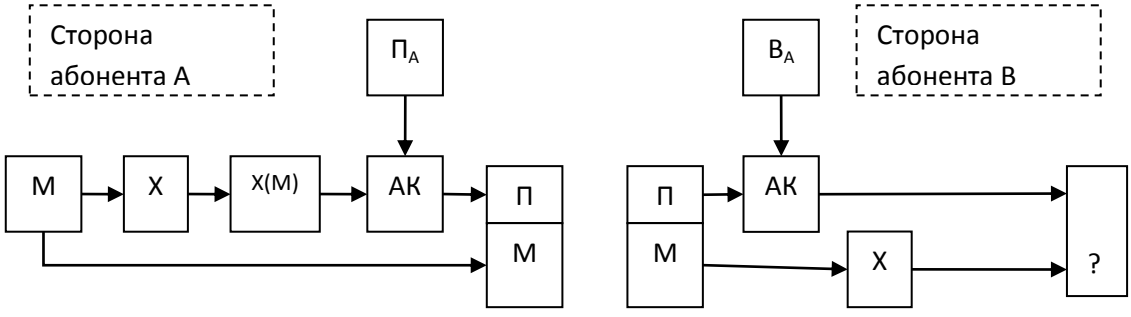

Рис. 1. Схема автентфікації повідомлення

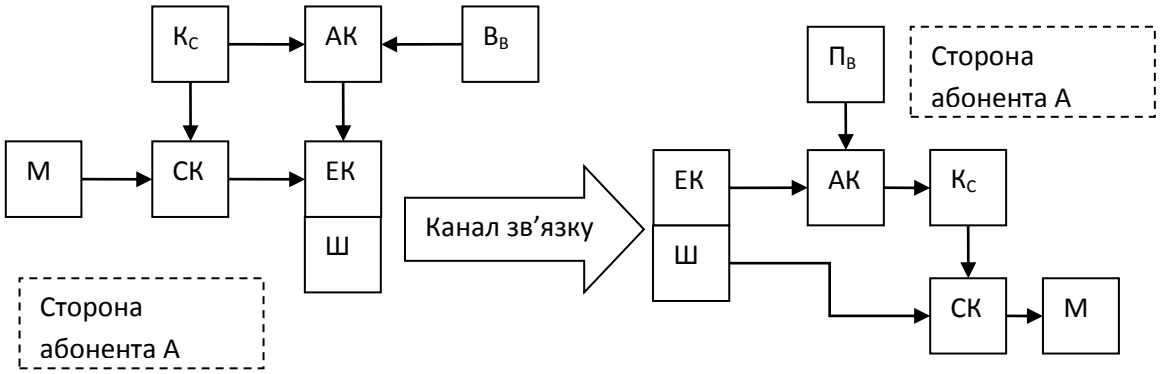

Рис. 2. Схема шифрування повідомлення

На рисунку 1 абонент А підписує повідомлення М, абонент В в даному випадку перевіряє підпис абонента А. Умовні позначення на обох схемах означають наступне. М – повідомлення, яке шифрується або підписується. Х – алгоритм хешування. Х(М) – результат роботи алгоритму хешування. АК – асиметрична криптосистема, наприклад RSA. $П_А$ – приватний ключ абонента А. П – підпис абонента А. Фактично підписом абонента А є зашифрований на приватному ключі А хеш повідомлення М. Тепер на стороні абонента В підпис дешифровується за допомогою $В_А$ – відкритого ключа абонента А. Отримаємо хеш, який був отриманий з повідомлення на етапі підписування. ? – порівняння хешів, один з яких отриманий в результаті дешифрування, а другий в результаті повторного хешуваня повідомлення М. Якщо за якихось причин у повідомленні М відбулися зміни, то хеші, очевидно, не співпадуть. В цьому випадку повідомлення вважається неавтентичним.

Рисунок 2 зображує процедуру шифрування. Абонент А шифрує повідомлення М, а абонент В дешифрує його. Для цього використовується симетрична криптосистема СК, наприклад DES. Ключ $К_С$ для неї генерується випадковим чином і лише на один сеанс зв'язку. Для того щоб передати його абоненту В використовується асиметрична криптосистема АК. З її допомогою $К_С$ шифрується на відкритому ключі абонента В. Утворюється так званий електронний конверт ЕК. З цього електронного конверту лише абонент В може відновити сеансовий ключ $К_С$ за допомогою свого приватного ключа $П_В$.

Таким чином у віртуальних лабораторіях забезпечується підтримка науково-практичних досліджень студентів і контроль на всіх етапах навчального процесу.