УДК 003.26

Жарський Віктор, ст. магістратури факультету кібернетики; науковий керівник – к. пед. н., доцент Лотюк Ю. Г. (Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука, м. Рівне)

СТВОРЕННЯ МЕРЕЖЕВИХ КРИПТОГРАФІЧНИХ СИСТЕМ ОБМІНУ ДАНИХ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ УКРАЇНИ (НА ПРИКЛАДІ ПВНЗ «МЕГУ ІМ. АКАД. С. ДЕМ'ЯНЧУКА»)

Анотація. *У статті досліджено основні підходи до створення криптографічної системи, яка вміє зашифровувати та розшифровувати дані, які захищено передаються в мережі. Проаналізовано рішення і вибрано необхідні технології та актуальне апаратне забезпечення. Розроблено програмний комплекс керування апаратним забезпеченням, який включає певний шифр, користувацький модуль і модуль спряження.*
Ключові слова: *криптографія, передача даних, інформаційно-комунікаційні технології.*

Аннотация. *В статье исследованы основные подходы к созданию криптографической системы, которая умеет зашифровывать и расшифровывать данные, защищенные передаются в сети. Проанализированы решения и выбрано необходимые технологии и актуальный аппаратное обеспечение. Разработан программный комплекс управления аппаратным обеспечением, который включает определенный шифр, пользовательский модуль и модуль сопряжения.*
Ключевые слова: *криптография, передача данных, информационно-коммуникационные технологии.*

Annotation. *This article explores the main approaches to the creation of a cryptographic system that can encrypt and decrypt data that is transmitted to the protected network. Existing solutions is analyzed, and the necessary technology and actual hardware are select and shown. The software system of hardware management that includes a cipher, a custom module and a module of interface is developed.*
Keywords: *cryptography, data, information and communication technology.*

У наш час в інформаційний простір швидкими темпами впроваджуються новітні досягнення комп'ютерних та телекомунікаційних технологій. Комп'ютерні системи активно задіюються у фінансових, промислових, торгових і соціальних сферах. Внаслідок цього різко зріс інтерес користувачів до проблем захисту інформації. Захист інформації, що є сукупністю

організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації і держави. В останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу (НСД) до конфіденційної інформації.

Серед всього спектру методів захисту даних від небажаного доступу, особливе місце займають криптографічні методи. Криптогра́фія (від грецького kryptós – прихований і gráphein – писати) – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації сторонніми особами) і автентичності (цілісності і підтвердженності авторства) інформації. Криптографія розвинулась з практичної потреби передавати важливі конфіденційності відомості найнадійнішим чином. Для аналізу даних в криптографії використовується інструментарій абстрактної алгебри та теорії ймовірностей, а також використовуються відкриті алгоритми шифрування на основі використання обчислювальних засобів.

Криптографічний захист інформації це вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування або відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо [1].

На сьогоднішній день одним із перспективних напрямів розвитку шифрування інформації є використання розширеного спектра операцій криптографічного перетворення для вдосконалення існуючих та побудови нових алгоритмів захисту даних. У роботах [2; 3] запропоновано ряд нових операцій криптографічного перетворення на основі булевих функцій. Однак залишається невирішеним ряд задач і проблем, зокрема, побудова операцій криптографічного перетворення з великою кількістю змінних, розробка методів використання операцій перетворення для шифрування. Вирішення поставлених задач забезпечує підвищення якості та ефективність систем мережевої інформаційної безпеки. Проте, недостатньо вивченим залишається питання оптимізації роботи мережевих криптографічних систем. Розв'язуванню цієї проблеми і присвячене дане магістерське дослідження.

У роботах учених [4; 5] описаний новий перспективний метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення. Реалізація цього методу передбачає парольне формування первинної невиродженої матриці криптографічного перетворення на початковому етапі. Для виконання вимог, що забезпечують існування невиродженої матриці перетворення, її синтез проводиться на основі послідовного додавання за модулем двох її рядків. Кількість доданків для синтезу кожного рядка матриці, а також номери доданків або рядків визначаються паролем. Оскільки формування первинної матриці криптографічного перетворення є основним і найважливішим етапом розробленого нами методу, то нами було розроблено цілком новий алгоритм формування первинної матриці шляхом використання операції перестановок.

Метою нашої статті є розробка мережевої системи для шифрування та дешифрування даних за допомогою існуючих криптографічних алгоритмів. Для цього використано кілька алгоритмів шифрування, такі як RSA, DES, GOST тощо.

Інформація, **яка може** бути прочитана, осмислена і зрозуміла без яких-небудь спеціальних засобів, називається *відкритим текстом* або незашифрованою інформацією (plaintext, clear text). Метод перетворення відкритого тексту таким чином, щоб унеможливити його прочитання, називається шифруванням (encryption або enciphering). Шифрування відкритого тексту приводить до його перетворення в незрозумілі символи, які не сприймаються людиною, що називають шифртекстом (ciphertext). Шифрування дозволяє сховати інформацію від тих, для кого вона не призначена, незважаючи на те, що вони можуть мати доступ до самого шифротексту. Протилежний процес по звертанню шифротексту в його початковий вид, називається розшифруванням (decryption або deciphering).

Криптографія може бути «стійкою», а може бути «слабкою», як описано в наведеному прикладі. Криптографічна стійкість виміряється тим, скільки знадобиться часу і ресурсів, щоб із шифротексту відновити вихідний відкритий текст для читання. Результатом стійкої криптографії є шифротекст, що винятково складно «зламати» без оволодіння визначеними інструментами по дешифруванню. Поки що не доведено, що краще шифрування, яке доступне сьогодні, зможе «встояти» проти обчислювальних можливостей комп'ютерів, доступних завтра [6].

Криптографічний алгоритм, або шифр, – це математична формула, що описує процеси шифрування і розшифрування. Щоб зашифрувати відкритий текст за допомогою криптографічної системи, необхідно працювати з ключовим словом, числом або фразою. Те саме повідомлення одним алгоритмом, але різними ключами буде перетворюватися в різний шифротекст. Захищеність шифротексту цілком залежить від двох факторів: стійкості криптографічного алгоритму і таємності ключа. Криптографічний алгоритм плюс усілякі ключі і протоколи, що приводять їх у дію, складають криптосистему. У традиційній симетричній криптографії той самий ключ використовується як для шифрування, так і для розшифрування даних. Data Encryption Standart (DES) є прикладом симетричного алгоритму, що широко застосовувався на Заході з 70-х років у банківській і комерційних сферах. В даний час його замінив Advanced Encryption Standard (AES) [7; 8].

Симетричне шифрування має ряд переваг. Перша перевага – швидкість операцій шифрування. Це особливо корисно для шифрування даних, що залишаються у користувача. Однак, симетричне шифрування, використане саме по собі як засіб захисту цінних даних, що пересилаються через мережу, може виявитися досить витратним, просто через складність передачі таємного ключа. Для встановлення криптографічного зв'язку за допомогою

симетричного алгоритму, відправникові й одержувачеві потрібно попередньо погодити ключ і тримати його в таємниці. Якщо вони знаходяться в географічно віддалених місцях, то повинні вдатися до допомоги довіреного посередника, наприклад, надійного кур'єра, щоб уникнути компрометації ключа в ході транспортування. Зловмисник, що перехопив ключ на шляху, зможе пізніше читати, змінювати і підробляти будь-яку інформацію, зашифровану або завірену цим ключем. Глобальна проблема симетричних шифрів складається в складності керування ключами: як ви доставите ключ одержувачеві без ризику, що його перехоплять [9].

В класах реалізована окремо методи шифрування та дешифрування вони окремо реалізовують зашифровування та розшифровування інформації. Також реалізований класи підключення до мережі та відправлення інформації по мережі. Хоча криптографічна система використовує багато математичних й інформаційних концепцій, ми розглянемо тільки самі основні. Криптографічна мережева система передбачає використання мови C# де реалізовано багато різних класів.

Наведемо алгоритм реалізації шифрування. Якщо позначити через M відкрите, а через C шифроване повідомлення, то процеси шифрування та дешифрування можна записати у вигляді рівностей:

$$\begin{aligned} E_{k_1}(M) &= C; \\ D_{k_2}(C) &= M, \end{aligned} \tag{1}$$

в яких алгоритми шифрування E та дешифрування D повинні задовольняти рівності:

$$D_{k_2}(E_{k_1}(M)) = M. \tag{2}$$

Для різних шифрів задача дешифрування має різну складність. Рівень складності задачі визначає головну властивість шифру – здатність протистояти спробам отримати захищену інформацію. Тоді говорять про криптографічну стійкість шифру (або просто стійкість), розрізняючи більш стійкі та менш стійкі шифри. Методи відкриття шифрів розробляє наука, що називається криптоаналізом [10].

Історія розвитку протоколу TCP/IP – зародився в результаті досліджень, профінансованих Управлінням перспективних науково-дослідних розробок (Advanced Research Project Agency, ARPA) уряду США в 1970-х роках. Цей протокол був розроблений для того, щоб обчислювальні мережі дослідницьких центрів в усьому світі могли бути об'єднані у формі віртуальної «мережі мереж» (internetwork). Первісна мережа Інтернет була створена в результаті перетворення існуючого конгломерату обчислювальних мереж, що носили

назву ARPAnet, за допомогою TCP/IP. Великий внесок у розвиток стеку протоколів TCP/IP, що одержав свою назву завдяки популярним протоколам IP і TCP, вніс університет Берклі, реалізувавши протоколи стека у своїй версії ОС UNIX. Популярність цієї операційної системи привела до широкого поширення протоколів TCP, IP та інших протоколів стека. Сьогодні цей стек використовується для зв'язку комп'ютерів світової інформаційної мережі Інтернет, а також у багатьох корпоративних мережах.

Протокол мережевого рівня TCP/IP забезпечує взаємодію мереж різної архітектури. Основним протоколом мережного рівня технології TCP/IP є міжмережевий протокол IP та його допоміжні протоколи: адресний протокол ARP; реверсний адресний протокол RARP (Reverse ARP); протокол діагностичних повідомлень ICMP (Internet Control Message Protocol), який надсилає повідомлення вузлам мережі про помилки на маршруті, які виникають при передачі пакетів.

Головне завдання міжмережевого протоколу IP – це маршрутизація пакетів даних між різнотипними комп'ютерними мережами. Для розв'язання цього завдання протокол IP підтримує IP-адресацію мереж та вузлів, використовує таблицю маршрутизації пакетів, виконує, за необхідності, фрагментацію та дефрагментацію цих пакетів.

Функціонування мережевого рівня також забезпечує низка протоколів динамічної маршрутизації RIP, OSPF, які динамічно формують маршрути таблиці маршрутизації за алгоритмами вектора VDA (Vector Distance Algorithm) і стану зв'язку LSA (Link State Algorithm) відповідно; протоколів політики зовнішньої маршрутизації EGP (Exterior Gateway Protocol) та BGP (Border Gateway Protocol).

Практичне застосування інфраструктур відкритого ключа на сертифікатах виявляє ряд недоліків та проблемних питань. Серед них необхідно виділити значну вартість, психологічну неприйнятність, недостатній рівень уніфікації тощо. Головним принципом таких систем є те, що в якості відритого ключа асиметричної пари, (причому незалежно від методу перетворення), використовуються відкриті дані користувача, наприклад e-mail, почтова адреса, тощо. Проведені дослідження та порівняльний аналіз показали, що наведені стандарти визначають формати даних та модель генерації та передачі параметрів, ключів та повідомлень між сервером та користувачами, протоколи взаємодії, у тому числі вироблення та узгодження ключів, шифрування та електронного цифрового підпису та інші. Проаналізовані стандарти не вирішують проблему безпечної передачі ключових даних та параметрів, вони лише вимагають від реальних систем таких функцій. Тобто, можна сказати, що проаналізовані стандарти не вирішують проблем, які властиві системам на базі ідентифікаторів (довіри до УГК та безпечного отримання відкритих параметрів та ключів). Тому необхідно проводити подальші дослідження оптимальних рішень зазначених проблем.

1. Указ Президента України від 22 травня 1998 р., N 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні». **2.** Лужецький В. А. Використання операції множення за модулем в симетричних бло-ков их шифрах / В. А. Лужецький,О. В. Дмитришин // Системи обробки інформації. – 2010. – № 5. – С. 9–14. **3.** Дмитришин О. В. Методи і засоби блокового шифрування підвищеної стійкості на основі арифметичних операцій за модулем : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.05 / О. В. Дмитришин. – Вінниця, 2012. – 18 с. **4.** Голуб С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації : зб. наук. праць. – Вип. 3 (101), Т. 1. – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 119–122. **5.** Бабенко В. Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації : зб. наук. праць. – № 9 (107). – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 163–168. **6.** http://uk.wikipedia.org/wiki/Криптографія [Інтернет ресурс] **7.** http://ru.wikipedia.org/wiki/RSA [Інтернет ресурс] **8.** http://ru.wikipedia.org/wiki/DES **9.** http://uk.wikipedia.org/wiki/Симетричні алгоритми шифрування. [Інтернет ресурс] **10.** Горбенко И. Д. Криптографическая защита информации в информационных системах. Курс лекций / И. Д. Горбенко. – ХНУРЭ. – 2002.