УДК 004

Яненко О.В. студентка гр. 125-21-5
Науковий керівник: Олішевський І. Г., асистент кафедри БІТ
(Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна)

КРИПТОГРАФІЯ В СУЧАСНОМУ СВІТІ

Мета дослідження. Визначити значення криптографії для сучасного суспільства Завдання дослідження: вивчити літературу з даного питання і інформаційні ресурси; дати визначення основних понять; розглянути методи захисту інформації в криптографії.

Методи дослідження. аналіз літератури та інформаційних ресурсів комп'ютерної мережі Internet; вивчення різних способів шифрування**.**

Основна частина.

На сьогоднішній день, криптографія займає в житті кожної людини важливе місце. Будь-яка людина хоча б раз в день стикається з шифруванням даних. Все більша і більша кількість інформації передається по тих каналах зв'язку, які вимагають особливої захищеності даних.

Сучасна криптографія повністю заснована на математиці. Основне завдання, яке переслідує математика в криптографії - це криптографічна стійкість, тобто здатність протистояти теоретичному і практичному взлому.

Практичне застосування криптографії стало невід'ємною частиною життя сучасного суспільства - її використовують в електронній комерції, електронний документообіг (включаючи електронні підписи), телекомунікації та інших областях. Після поширення комп'ютерів в діловій сфері практична криптографія зробила в своєму розвитку величезний стрибок.

Сучасний період розвитку криптографії (з кінця 70-х років по теперішній час) відрізняється зародженням та розвитком нового напрямку - це криптографія з відкритим ключем. Її поява знаменується не тільки новими технічними можливостями, а й порівняно широким поширенням криптографії для використання приватними особами.

У наш час всезростаючого потоку обміну інформацією, до якого відноситься все більше і більше інформації про наше повсякденне життя (цифровізація всього і вся, починаючи від щоденника і медичної карти, і закінчуючи фінансовими операціями на ринках цінних паперів), стійке і надійне шифрування є не просто необхідним, а життєво важливою умовою безпеки.

Як прості приклади можна привести: обмін повідомленнями в корпоративній пошті великих компаній; листування в різних інтернет месенджерах (telegram, whatsapp та ін.); електронний щоденник учня; ЗНО, лікарська інформація; взагалі будь-яка інформація про персональні дані. Навіть звичайне управління електронними приладами будинку (так званий розумний будинок) має здійснюватися по шифрованих каналах даних, щоб

уникнути втручання в їх роботу зловмисників. Зараз комунальні послуги і все, що пов'язано з ЖКГ, активно йде в цифровий світ, обмін даними в системі також має бути безпечним від втручання ззовні, і шифрування - якраз метод, що дозволяє цього досягти. Зараз будь-яка передача даних повинна бути шифрованою, якщо вона не призначається широкому колу осіб (публічна інформація).

Шифрування публічним ключем - алгоритм шифрування, що застосовується сьогодні в різних модифікаціях буквально у всіх комп'ютерних системах. Є два ключі: відкритий і секретний.

Відкритий ключ - це якесь дуже велике число, що має тільки два дільника, крім одиниці і самого себе. Ці два подільника є секретним ключем, і при перемножуванні дають публічний ключ. Наприклад, публічний ключ - це 1961, а секретний - 37 і 53. Відкритий ключ використовується для того, щоб зашифрувати повідомлення, а секретний - щоб розшифрувати. Без секретного ключа розшифрувати повідомлення неможливо. Коли ви відправляєте свої особисті дані, припустимо, банку, або ваша банківська картка зчитується банкоматом, то всі дані шифруються відкритим ключем, а розшифрувати їх може тільки банк з відповідним секретним ключем. Суть в тому, що математично дуже важко знайти подільники дуже великого числа.

Дослідивши і проаналізувавши знайдену інформацію, можна зробити висновок, що криптографія відіграє важливу роль в сучасному світі. Сучасна криптографія утворює окремий науковий напрям на стику математики і інформатики - роботи в цій галузі публікуються в наукових журналах, організовуються регулярні конференції. Практичне застосування криптографії стало невід'ємною частиною життя сучасного суспільства - її використовують в таких галузях як електронна комерція, електронний документообіг (включаючи цифрові підписи), телекомунікації та інших.

Висновок. Криптографія є одним з найбільш потужних засобів забезпечення конфіденційності і контролю цілісності інформації. Багато в чому вона займає центральне місце серед програмно-технічних регуляторів безпеки. Наприклад, для портативних комп'ютерів, фізично захистити які вкрай важко, застосування криптографія дозволяє гарантувати конфіденційність інформації.

Перелік посилань

1. Златопольский Д.М. Простейшие методы шифрования текста. /Д.М. Златопольский - М.: Чистые пруды, 2007
2. Молдовян А. Криптография. /А. Молдовян, Н.А. Молдовян, Б.Я. Советов - СПб: Лань, 2001
3. Криптография: Базовые знания о науке шифрования (http://www. furfur. me/fu rfur/culture/culture/166567-kriptografiya).