КІБЕРБЕЗПЕКА КРИТИЧНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Миколайко О. О.
Науковий керівник - канд. техн. наук, доц. Піскачова І.В.
Харківський радіотехнічний коледж
(61057, м. Харків, вул. Сумська 18/20, група КІ-437), тел. (057) 712-35-37)
e-mail: piskachova@khntusg.info

Завдяки стрімкому розвитку новітніх інформаційно-телекомунікаційних систем (ІТС) з'явилися проблеми, зумовлені більшою вразливістю ІТС щодо стороннього кібернетичного впливу. Тому постала необхідність створення надійної системи кібернетичної безпеки, відсутність якої може призвести до втрати критичної інформації ІТС будь-якої державної або приватної установи. Підвищення активності користувачів, а також стрімко зростаюча кількість способів і методів пошуку й збору інформації з різних джерел та її добування із закритих електронних джерел, розвиток соціальних мереж сприяють активізації кіберзлочинників. Глобальна мережа перетворюється на засіб організації різних кібератак, несанкціонованого доступу до чужих сайтів, створення сайтів-двійників тощо. Дієвий опір таким діям дуже складно чинити. Це призвело до більш стрімкого розвитку криптології – науки про захист інформації, шляхом її перетворення. Криптологія поєднує два напрямки – криптографію й криптоаналіз. Криптографія займається пошуком і дослідженням методів перетворення інформації з метою приховання її змісту. Основні напрямки використання криптографічних методів - передача конфіденційної інформації з каналів зв'язку, установлення дійсності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді. Криптоаналіз - дослідження можливості розшифровування інформації без знання ключів.

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги: зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа; число операції, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення й відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів; число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів, повинне мати строгу нижню оцінку й виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень) або вимагати неприйнятно високих витрат на ці обчислення; знання алгоритму шифрування не повинне впливати на надійність захисту та ін.

В роботі проведена розробка програмного забезпечення для шифрування та дешифрування текстової інформації за допомогою традиційних шифрів з симетричним ключем на мові програмування Python. Рішення таких задач допомагає обрати найбільш надійний шифр у подальшому.