МЕТОД ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ЇЇ ШИФРУВАННЯ

Гуменюк І. В., Хоменко В. Д.
Житомирський військовий інститут імені С. П. Корольова, м. Житомир

Аналіз досвіду ведення бойових дій на території України свідчить про інтенсивне зростання діяльності видів технічної розвідки (ТР) іноземних держав щодо здобування інформації, що містить державну таємницю. Розвідка безперервно ведеться з використанням багатофункціональних космічних, повітряних, наземних систем та комплексів. При цьому провідні країни світу продовжують модернізувати власні розвідувальні служби, нарощувати можливості та технічні характеристики засобів ТР. За таких умов проблема захисту інформації від несанкціонованого доступу (НСД) та/або її використання, зміни, знищення набуває важливого значення. Таким чином, метою даного дослідження є удосконалення методу захисту мовної інформації, що зберігається та передається мережею ІТС, на основі використання відомих криптографічних методів шифрування. Конкретні реалізації систем захисту інформації можуть істотно відрізнятися, враховуючи відмінності методів й алгоритмів передачі даних. Усі вони повинні забезпечувати рішення сукупності взаємопов'язаних завдань, а саме забезпечення: цілісності інформації, її достовірності та точності, а також захищеності від навмисних і ненавмисних спотворень; доступності інформації (використання її в будь-який момент); конфіденційності інформації.

Успішне вирішення цих завдань можливе шляхом виконання організаційно-технічних заходів або застосування криптографічного захисту інформації. Останній в більшості випадків є більш ефективним.

Розглянемо деякі алгоритми шифрування. Одним із розповсюджених у застосуванні є стандарт розширеного шифрування Advanced Encryption Standard (AES), на основі якого розроблено велику кількість ефективних алгоритмів.

Інший клас алгоритмів використовує методи перестановки для шифрування текстових файлів і зображень. Аналіз сучасної науково-технічної літератури показав, що для шифрування мовних файлів широко застосовують алгоритм Rivest-Shamir-Adleman (RSA). Цей метод малоефективний для шифрування повних (несегментованих) аудіофайлів. Деякі дослідні праці у сфері системних методів обробки інформації зосереджені на зменшенні часу за рахунок шифрування окремих частин (кадрів, сегментів тощо) аудіофайла.

Отже, результати аналізу науково-практичних джерел свідчать про те, що для вирішення завдання захисту інформації від НСД до неї шляхом застосування криптографічних методів шифрування аудіофайлів розроблена достатня кількість. Для своєчасного виявлення та протидії НСД необхідно застосовувати запропонований авторами метод шифрування мовної інформації з використанням симетричних алгоритмів. Верифікація цього методу свідчить про його високу криптостійкість, надійність та ефективність. Його доцільно застосовувати в умовах відсутності засобів захисту інформації при передачі каналами мереж військового призначення.