Застосування криптоаналізу для дослідження стійкості систем захисту інформації

В.В. Багрій, *студент,*
О.П. До́ренський, *викладач*
Кіровоградський національний технічний університет

Криптоаналіз призначений для визначення надійності шифру, перевірки його стійкості [1]. Метою застосування криптоаналізу насамперед є знаходження уразливих місць у розповсюджених системах захисту даних, а також визначення надійності й трудомісткості розкриття закритої інформації та розкриття зашифрованої інформації без повного набору необхідних даних [1, 2]. Слід зазначити, що криптоаналіз і криптографія мають протилежні напрямки і є одними з напрямів криптології [2].

Результати криптоаналізу конкретного шифру називають криптографічною атакою на цей шифр. Успішну криптографічну атаку, що дискредитує систему, називають зломом або розкриттям [1].

Дослідження [2] показало, що сучасна наука виділяє чотири основних і три додаткових методи криптоаналізу. До основних відносять: атака на основі шифротексту; атака на основі відкритих текстів і відповідних шифротекстів; атака на основі підібраного відкритого тексту (можливість вибрати текст для шифрування); атака на основі адаптивно підібраного відкритого тексту. Додатковими методами криптоаналізу є Атака на основі підібраного шифротексту, Атака на основі підібраного ключа, Бандитський криптоаналіз.

Таким чином, задача застосування криптоаналізу для дослідження стійкості систем захисту інформації (СЗІ) є актуальною задачею та є перспективною для практичної реалізації й подальшого впровадження. Метою науково-дослідної роботи є дослідження криптоаналізу щодо його практичного застосування для аналізу стійкості систем захисту інформації.

У сучасному програмному забезпеченні (ПЗ) криптоалгоритми широко застосовуються не тільки для шифрування даних, але й для автентифікації і перевірки цілісності [4]. На сьогоднішній день існують добре відомі й апробовані криптоалгоритми (як із симетричними, так і несиметричними ключами), криптостійкість яким або доведена математично, або заснована на необхідності розв'язку математично складної задачі (факторизації, дискретного логарифмування тощо) [5]. Таким чином, вони не можуть бути розкриті інакше як повним перебором або рішенням зазначеної задачі.

З іншого боку, у комп'ютерному й навколокомп'ютерному світі увесь час з'являється інформація про помилки або "прогалини" у тій або іншій програмі (у т.ч. що застосовує криптоалгоритми), або про те, що вона була зламана (cracked). Це створює недовіру як до конкретних програм, так і до можливості взагалі захистити що-небудь криптографічними методами не тільки від спецслужб, але й від хакерів.

Тому знання історії атак і "прогалин" у криптосистемах, а також розуміння причин, з яких вони мали місце, є однією з необхідних умов розробки захищених систем [1, 5]. Перспективним напрямком досліджень у цій області є аналіз успішно проведених атак або виявлених уразливостей у криптосистемах з метою їхнього узагальнення, класифікації й виявлення причин і закономірностей їхньої появи й існування.

За аналогією з таксономією причин порушення безпеки ОС виділимо наступні причини ненадійності криптографічних програм: 1) неможливість застосування стійких криптоалгоритмів; 2) помилки в реалізації криптоалгоритмів; 3) неправильне застосування криптоалгоритмів; 4) людський фактор. Причини ненадійності криптосистем наведено на рисунку 1.

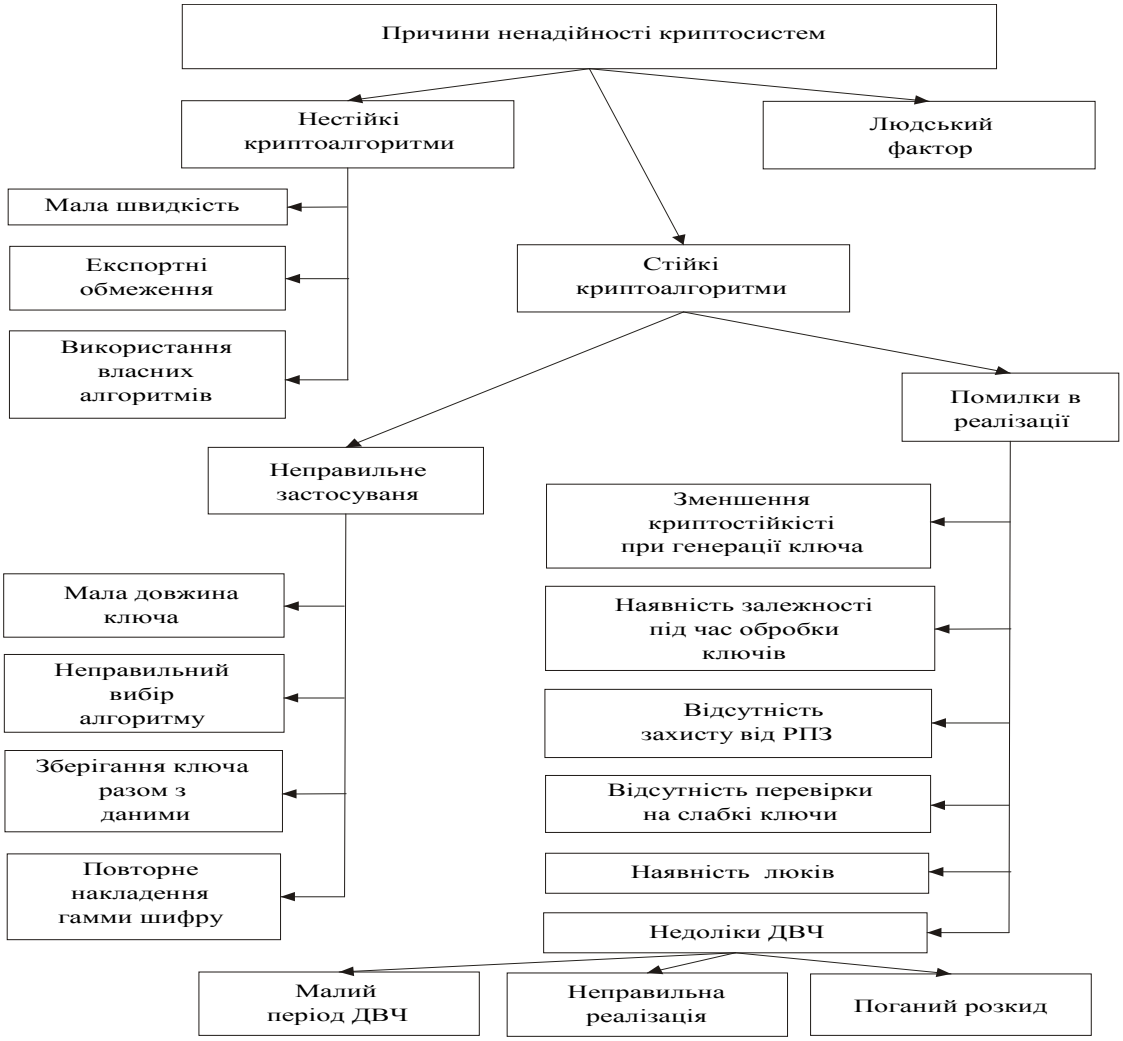

Рисунок 1 – Причини ненадійності криптосистем

Реалізацію криптоаналізу можливо здійснити за допомогою одного з методів: диференційний криптоаналіз, криптоаналіз зі зв'язаними ключами, лінійний криптоаналіз, метод зустрічі посередині. При цьому для прогамної реалізації доцільно використати нейромережні алгоритми [3].

Отже, для розв'язку задачі дослідження стійкості систем захисту інформації (СЗІ) за допомогою криптоаналізу доцільною є розробка програмного забезпечення, яке виконує відповідні функції. Для практичної реалізації системи прийнято проектне рішення використовувати структуру, що самонавчається, яка залежно від вихідних даних і ступеня навченості, буде "вирішувати", яким чином діяти в тій або іншій ситуації. При цьому параметри окремих елементів нейрокомп'ютерної мережі (персептронів), визначаються вагами на входах і виходах (рисунок 2). Безсумнівнимим перевагами даного підходу є те, що всі сучасні системи захисту свідомо уразливі до подібних методів криптоаналізу, а також забезпечується висока швидкість розкриття.

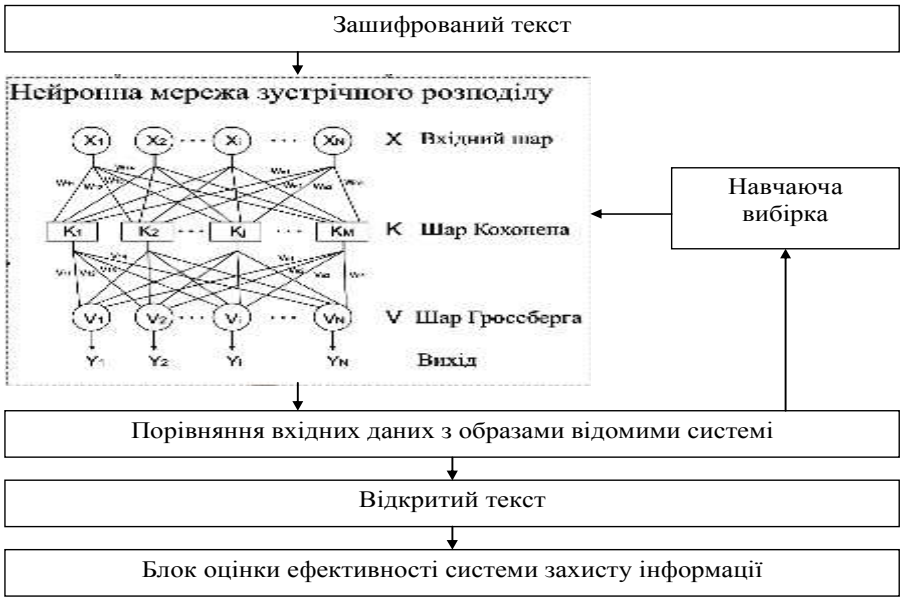

Рисунок 2 – Функціональна схема запропонованої системи дослідження стійкості СЗІ

Як видно з рисунка 2, спочатку на вхід системи подається навчаюча вибірка, за допомогою якої відбувається навчання нейронної мережі. Потім в програмі відкривається зашифрований текст. Нейронна мережа намагається розпізнати алгоритм шифрування та розшифрувати його без ключа, що відбувається за допомогою порівняння вхідних даних з образами, відомими системі після навчання. Після розшифрування тексту відбувається додавання нової інформації до бази знань. З кожним наступним використанням програма має все більше інформації для дешифрування. У якості системи криптоаналізу використана нейронна мережа зустрічного розподілу, що має три шари: вхідний шар, X; шар Кохонена, K; шар Гроссберга, V (рисунок 2).

Нейронна мережа зустрічного розподілу навчається на вибірці пар векторів (X,Y) задачі подання відображення XY. Чудовою особливістю цієї мережі є здатність навчання і відображення сукупності XY у себе. При цьому, завдяки узагальненню, з'являється можливість відновлення пари (XY) за одним відомом компонентом (X або Y). При пред'явлені на етапі розпізнавання тільки вектора X (з нульовим початковим Y) виконується пряме відображення – відновлюється Y, і навпаки, при відомому Y може бути відновлений відповідний йому X. Можливість рішення як прямої, так і зворотної задачі, а також гібридної задачі по відновленню окремих відсутніх компонентів робить дану нейромережну архітектуру унікальним інструментом.

У доповіді детально розглядатимуться принципи реалізації та функціональні можливості розробленого програмного забезпечення дослідження стійкості СЗІ, його основні характеристики, галузі застосування та методика впровадження.

Список літератури

1. Жданов О.Н. Криптоанализ классических шифров. / О.Н. Жданов, И.А. Куденкова. – Красноярск: СГАУ, 2008. – 348 с.
2. Брюс Шнайдер. Прикладная криптография. 2-е изд. – М: "Диа Софт", 2000. – 368 с.
3. Вороновский Г.К. Генетические алгоритмы, искусственные нейронные сети и проблемы виртуальной реальности. / Г.К. Вороновский, А.В. Махотило – Х.: "Основа", 2007. – С. 67-81.
4. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии – М.: Издательство Московского центра непрерывного математического образования, 2000. – 290 с.