УДК 004.056.55:004.312.2

Р.П. Мельник[1], О.Г. Мельник[1], С.В. Гончар[1], В.Г. Бабенко[2]

[1] Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси
[2] Одеська національна академія зв'язку ім. О.С. Попова, Одеса

МЕТОД ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ЯК СКЛАДОВА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДСНС УКРАЇНИ

У статті розроблений метод захисту конфіденційної інформації ДСНС України на основі використання операцій розширеного матричного криптографічного перетворення. Проведено перевірку реалізації операцій розширеного матричного криптографічного перетворення на відповідність вимогам програмного пакета статистичного тестування NIST STS.

Ключові слова: *державні інформаційні ресурси, захист інформації, конфіденційна інформація, розширені матричні операції.*

Актуальність проблеми

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод громадянина з метою зміцнення конституційного ладу, суверенітету й територіальної цілісності країни, становлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства [1].

В статті 6 Закону України «Про засади внутрішньої і зовнішньої політики» [2] зазначено, що «основними засадами внутрішньої політики у сфері національної безпеки і оборони є: …своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у …інформаційній сфері». У Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» [3], який прийнято для подальшого вдосконалення системи забезпечення інформаційних ресурсів держави, проведення єдиної державної політики в Україні у сфері забезпечення інформаційної безпеки держави, визначено термін державні інформаційні ресурси, під яким розуміють інформацію, що є власністю держави та необхідність захисту якої визначено законодавством.

Загрози інтересам держави можуть проявлятися у вигляді отримання протиправного доступу до відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести значних збитків державі.

Таким чином, виникає необхідність постійного уточнення як внутрішніх, так і зовнішніх загроз державним інформаційним ресурсам, що в свою чергу, впливатиме на організацію комплексної системи захисту державних інформаційних ресурсів, забезпечуватиме актуальність проведення досліджень у вказаному напряму. Тому важливою проблемою є постійне підвищення якості систем захисту інформації.

Якщо раніше проблема захисту інформації була актуальною тільки для спеціальних служб, то згодом вона стала актуальною для всіх організацій, підприємств та відомств, в тому числі й для Державної служби України з надзвичайних ситуацій (ДСНС України) [4], де оперативність, достовірність і конфіденційність інформації має величезне значення для безпеки людей та гарантування національної безпеки в цілому.

Оперативна доставка інформації в процесі повсякденної діяльності всіх галузевих служб і підрозділів ДСНС України, оперативна взаємодія з органами державного управління та місцевого самоврядування, іншими міністерствами та відомствами супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер.

На сьогоднішній день вважається, що забезпечення інформаційної безпеки повинно носити комплексний характер, тому пропонуються нові комплексні рішення для захисту інформаційних ресурсів. Проте організація інформаційної безпеки повинна носити не просто комплексний характер, але ще й засновуватися на всебічному аналізі можливих наслідків, при якому важливо не упустити будь-які суттєві аспекти [1].

Аналіз останніх досліджень

Серед останніх досліджень і публікацій варто виділити: [5, 6], де розглянуто особливості впровадження інформаційних технологій в управлінську діяльність структурних підрозділів ДСНС України і проблеми організації системи захисту інформації, та [7], де вивчено й обґрунтовано доцільність застосування спеціалізованих логічних функцій у захисті оперативної інформації інформаційно-аналітичної системи ДСНС України.

Формулювання цілей статті

Метою даного дослідження є розробка методу захисту конфіденційної інформації ДСНС України на основі використання операцій розширеного матричного криптографічного перетворення.

Виклад основного матеріалу

За останні декілька десятиліть відбулися якісні зміни в процесах управління на всіх ієрархічних рівнях за рахунок інтенсивного впровадження сучасних інформаційних технологій. Їх швидкий розвиток призвів до зростання цінності інформації як для суспільства взагалі, так і для кожної окремої людини зокрема. Водночас почала зростати небезпека втручання в роботу інформаційних систем для несанкціонованого зчитування інформації. Значення та вагомість наслідків таких втручань з часом збільшилися настільки, що навіть розвинені держави, їх промислові та фінансові структури стали заручниками своїх інформаційних технологій.

Наскільки актуальна проблема захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- несанкціонований доступ – 2 %
- укорінення вірусів – 3 %;
- технічні відмови апаратури мережі – 20 %;
- цілеспрямовані дії персоналу – 20 %;
- помилки персоналу (недостатній рівень кваліфікації) – 55 %.

Однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор).

За даними статистики групи компаній «Лабораторія Касперського» в 2013 році виникло більше 170 тисяч атак на сервери корпорацій та державних установ, а Україна знаходиться на шостому місці по розміщенню небезпечного програмного забезпечення, саме тому в нашій країні все більше уваги приділяється проблемам захисту інформації та інформаційній безпеці.

Відповідно до вимог законів України «Про інформацію», «Про державну таємницю» та «Про захист інформації в інформаційно-телекомунікаційних системах» основним об'єктом захисту в інформаційних системах є інформація з обмеженим доступом, що становить державну або іншу, передбачену законодавством України, таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження.

Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Сучасні темпи розвитку інформаційних технологій вимагають і від структурних підрозділів ДСНС України високого рівня захисту конфіденційної інформації. Колективне використання інформаційних ресурсів потребує відповідного захисту дисків і каталогів, окремих папок і файлів, а також усіх локальних і глобальних мереж від несанкціонованого втручання інформаційних зловмисників, вірусів і небезпечних програм. Тому **актуальним завданням** залишається постійне підвищення якості систем захисту інформації структурних підрозділів ДСНС України.

Однією із складових інженерно-технічного напряму захисту інформації є криптографічні засоби захисту – апаратні, програмні та програмно-апаратні засоби, які реалізують захист інформації за допомогою криптографічних перетворень, які, в свою чергу, є основою криптографічних методів, що створюються з метою виключення несанкціонованого доступу до інформації та її незаконного отримання.

На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі та зберігання.

В основі криптографічних методів лежить поняття криптографічного перетворення інформації, виробленого за певними математичними законами, з метою виключити доступ до даної інформації сторонніх користувачів, а також з метою забезпечення неможливості безконтрольної зміни інформації з боку тих же самих осіб.

В результаті обчислювального експерименту за допомогою спеціального програмного забезпечення [8] було знайдено групу трирозрядних логічних функцій, на основі яких будуються операції криптографічного перетворення, які не досліджувалися раніше.

Відповідно до [9] трирозрядні елементарні функції для криптографічного перетворення інформації залежно від її складності поділяються на:

- функції перестановки розрядів;
- функції на основі додавання за модулем 2 (матричні функції);
- розширені матричні функції;
- функції, в яких інформація керує перестановками;
- функції, що керуються інформацією.

Для спрощення процесу дослідження елементарні функції криптографічного перетворення було класифіковано на прямі та обернені елементарні функції.

Визначено групу елементарних функцій, які на сьогоднішній день не досліджувалися – це елементарні функції розширеного матричного перетворення.

До цієї групи функцій відносяться:

Прямі функції

$$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3,$$
$$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3,$$
$$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$
$$f_{75} = x_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3,$$
$$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3,$$
$$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$
$$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3,$$
$$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3,$$
$$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3,$$
$$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3,$$
$$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$
$$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3,$$

Обернені функції

$$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3,$$
$$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3,$$
$$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3,$$
$$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$
$$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3,$$
$$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3,$$
$$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3,$$
$$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3,$$
$$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$
$$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$
$$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$
$$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3.$$

Встановлено, що елементарні функції розширеного матричного перетворення включають в себе лінійну й нелінійну складові.

Загальний вираз для отримання елементарних функцій криптографічного перетворення:

$$f = \hat{x}_i \cdot \hat{x}_j \vee \hat{x}_i \cdot \hat{x}_l \vee \bar{\hat{x}}_i \cdot \bar{\hat{x}}_j \cdot \bar{\hat{x}}_l,$$

де $\hat{x}_i$ – змінні, що можуть набувати прямих або інверсних значень.

Як видно з даного виразу, лінійна складова представлена одним аргументом, який додається по модулю до логічного добутку двох інших аргументів, який є нелінійною складовою елементарної функції. Дані логічні умови й стали підґрунтям розробки методу синтезу елементарних функцій розширеного матричного криптографічного перетворення, на основі яких будуються операції криптографічного перетворення для систем захисту інформації [10].

Для проведення подальших досліджень проаналізовано форми представлення елементарних функцій та операцій криптографічного перетворення. Показано, що найбільш доцільно використовувати поліноміальне та дискретно-алгебраїчне представлення, тому що вони спрощують процес доведення коректності виконання криптографічних операцій.

Розроблено правила синтезу операцій криптографічного перетворення. Варіанти реалізації правил наведені на рис. 1.

Результати програмної реалізації методу на основі операцій розширеного матричного представлення було оцінено за допомогою статистичних тестів NIST Statistical test Suite (NIST STS) [10].

на основі першого елемента

$$F^k = \begin{bmatrix} \boxed{x_1} \oplus (\hat{x}_2 \cdot \hat{x}_3) \\ x_2 \oplus (\hat{x}_1 \cdot \bar{\hat{x}}_3) \\ x_3 \oplus (\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2) \end{bmatrix}$$

на основі другого елемента

$$F^k = \begin{bmatrix} x_1 \oplus (\hat{x}_2 \cdot \bar{\hat{x}}_3) \\ \boxed{x_2} \oplus (\hat{x}_1 \cdot \hat{x}_3) \\ x_3 \oplus (\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2) \end{bmatrix}$$

на основі третього елемента

$$F^k = \begin{bmatrix} x_1 \oplus (\bar{\hat{x}}_2 \cdot \bar{\hat{x}}_3) \\ x_2 \oplus (\bar{\hat{x}}_1 \cdot \hat{x}_3) \\ \boxed{x_3} \oplus (\hat{x}_1 \cdot \hat{x}_2) \end{bmatrix}$$

Рис. 1. Варіанти реалізації правил синтезу операцій криптографічного перетворення

Даний набір тестів був запропонований в ході проведення конкурсу на новий національний стандарт США блокового шифрування.

Цей набір використовувався для дослідження статистичних властивостей кандидатів на новий блоковий шифр.

Сьогодні методика тестування, запропонована NIST STS є найбільш поширеною у розробників криптографічних засобів захисту інформації.

Операції розширеного матричного криптографічного перетворення були використані для покращення статистичних властивостей псевдовипадкової послідовності, згенерованої за допомогою вбудованого програмного датчика random.

Для проведення якісного аналізу статистичних характеристик результатів шифрування з використанням операцій розширеного матричного криптографічного перетворення було проведено тестування невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти та текстового файлу.

Результати тестування описаних послідовностей вказані в табл. 1.

Таблиця 1

Оцінка програмної реалізації операцій розширеного матричного перетворення (РМП)

Об'єкти тестування	Кількість тестів, у яких тестування пройшли більше 99 % послідовностей	Кількість тестів, у яких тестування пройшли більше 96 % послідовностей
Генератор RANDOM-РМП	127 (68 %)	189 (100 %)
Криптографічне перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти на основі операцій РМП	132 (70 %)	189 (100 %)
Криптографічне перетворення текстового файлу на основі операцій РМП	127 (68 %)	189 (100 %)

Отримані результати реалізації операцій розширеного матричного криптографічного перетворення показали, що метод захисту інформаційних ресурсів ДСНС України на основі розширених матричних операцій криптографічного перетворення відповідає вимогам програмного пакета статистичного тестування NIST STS.

Висновки

В статті запропоновано метод використання розширених матричних операцій для криптографічного захисту інформації.

Оцінка якісних показників показала, що використання отриманих операцій забезпечує підвищення криптостійкості та швидкості реалізації алгоритмів криптографічного захисту інформації залежно від задач проектування.

Список літератури

1. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : «МК-Прес», 2005. – 432 с.

2. Закон України «Про засади внутрішньої і зовнішньої політики» : затверджений і введений в дію Постановою Верховної Ради України № 2411-VI від 01.07.2010 р.

3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» : затверджений і введений в дію Постановою Верховної Ради України № 3475-IV від 23.02.2006 р.

4. Сучасні телекомунікаційні мережі у цивільному захисті : підручник / [Щербак Г.В., Мельнікова Л.І., Рубан І.В., Садовий К.В., Сумцов А.В.] – Х., 2007. – 255 с.

5. Малець І.О. Впровадження інформаційних технологій в управлінську діяльність підрозділів Міністерства надзвичайних ситуацій / І.О. Малець, Ю.І. Грицюк // Науковий вісник НЛТУ України: збірник науково-технічних праць. – Львів: РВВ НЛТУ України, 2011. – Вип. 21.14. – С. 326-331.

6. Грицюк Ю.І. Практичні проблеми організації системи захисту інформації у структурних підрозділах Міністерства надзвичайних ситуацій України / Ю.І. Грицюк, І.О. Малець // Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту : матеріали міжнародної наукової конференції. – Євпаторія-Херсон : ХНТУ, 2010. – Т. 2. – С. 265-272.

7. Рудницкий В.Н. Защита оперативной информации в информационно-аналитической системе МЧС / В.Н. Рудницкий, Р.П. Мельник, О.Г. Мельник // Материалы XXIV межд. научно-практической конф. по проблемам пожарной безопасности, посвященной 75-летию создания института. – Россия : Балашиха, 2012.– С. 83-85.

8. Миронець І.В. Методики синтезу функцій декодування на основі спеціалізованих логічних функцій / І.В. Миронець, В.Г. Бабенко // Проблеми інформатизації: зб. тез доп. Міжнар. наук.-техн. семінар. – Черкаси, 2009. – Вип. 1 (3). – С. 47-50.

9. Бабенко В.Г. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / В.Г. Бабенко, О.Г. Мельник, Р.П. Мельник // Безпека інформації. – 2013. – Т. 19, № 1. – С. 56-59.

10. Мельник Р.П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації / Р.П. Мельник // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 9 (107). – С. 145-147.

Надійшла до редколегії 24.03.2014

Рецензент: д-р техн. наук, проф. В.М. Рудницький, Черкаський державний технологічний університет, Черкаси.

МЕТОД ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ КАК СОСТАВЛЯЮЩАЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ГСЧС УКРАИНЫ

Р.П. Мельник, О.Г. Мельник, С.В. Гончар, В.Г. Бабенко

В статье разработан метод защиты конфиденциальной информации ГСЧС Украины на основе использования операций расширенного матричного криптографического преобразования. Проведена проверка реализации операций расширенного матричного криптографического преобразования на соответствие требованиям программного пакета статистического тестирования NIST STS.

Ключевые слова: *государственные информационные ресурсы, защита информации, конфиденциальная информация, расширенные матричные операции.*

METHOD OF PROTECTION OF CONFIDENTIAL INFORMATION AS A COMPONENT OF INFORMATION SECURITY OF STATE EMERGENCY SERVICES OF UKRAINE

R.P. Melnyk, O.G. Melnyk, S.V. Gonchar, V.G. Babenko

In the article a method for the protection of confidential information of State emergency services of Ukraine operations through the use of advanced cryptographic transformation matrix. Audited the operations of the expanded matrix of cryptographic transformations for compliance with the statistical software package testing NIST STS.

Keywords: *public information resources, information security, confidential information, advanced matrix operations.*