УДК 003.26:004.056.55
DOI https://doi.org/10.32838/2663-5941/2021.2-1/29

Мельник О.Г.
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України

Мельник Р.П.
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України

РОЗРОБЛЕННЯ МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ ДЛЯ ЗДІЙСНЕННЯ УПРАВЛІННЯ СИЛАМИ ТА ЗАСОБАМИ ЦИВІЛЬНОГО ЗАХИСТУ В УМОВАХ ДЕЦЕНТРАЛІЗАЦІЇ

Дослідження присвячено розробленню сучасного методу захисту інформації інформаційно-аналітичних систем цивільного захисту Державної служби України з надзвичайних ситуацій і Центрів безпеки громадян в умовах децентралізації для здійснення надійного та швидкого управління, координації дій.

Визначено управлінські процеси, які відбуваються в інформаційно-аналітичних системах цивільного захисту і потребують захисту інформації, в результаті чого побудовано діяльнісну модель державного управління у сфері цивільного захисту в умовах децентралізації. Доведено, що всі стратегічні дії в умовах реформування місцевого самоврядування супроводжуються складними інформаційними процесами, більшість із яких мають конфіденційний характер і потребують надійного захисту.

Розроблено метод захисту інформаційних ресурсів Державної служби України з надзвичайних ситуацій і Центрів безпеки громадян на основі розширених матричних операцій криптографічного перетворення, а також розроблено модель процесу реалізації операцій розширеного матричного криптографічного перетворення.

Перевірено статистичні властивості результатів розширеного матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів. Побудовано статистичний портрет програмної реалізації методу захисту інформації на основі розширених матричних операцій криптографічного перетворення. Проведено тестування за методикою NIST Statistical test Suite, на основі якого зроблено висновок, що запропонований метод розширеного матричного криптографічного перетворення придатний для використання в інформаційно-аналітичних системах цивільного захисту Державної служби України з надзвичайних ситуацій і Центрів безпеки громадян.

Ключові слова: *інформаційно-аналітична система, цивільний захист, Центр безпеки громадян, діяльнісна модель державного управління, розширені матричні операції криптографічного перетворення.*

Постановка проблеми. Захист населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій (далі – НС) шляхом запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період – одна з основних функцій держави [1]. Організація цивільного захисту в Україні безпосередньо пов'язана з національною безпекою. Так, згідно зі статтею 12 [2] Державна служба України з надзвичайних ситуацій (далі – ДСНС України) входить до складу сил безпеки, на які Конституцією та законами України покладено функції із забезпечення національної безпеки держави.

Нині в Україні активно відбувається реформування місцевого самоврядування та територіальної організації влади [3]. Реформа децентралізації створила передумови для формування нової якості послуг, які отримують мешканці об'єднаних територіальних громад (далі – ОТГ). У межах секторальної децентралізації створюються Центри безпеки громадян (далі – ЦБГ), що насамперед дозволяють громадам забезпечити належний рівень безпеки життєдіяльності громадян, ефективно організувати свою роботу з питань цивільного захисту. Тому державна політика України в сфері місцевого самоврядування повинна спиратися саме на інтереси жителів

територіальних громад, безпеку їх життєдіяльності, захист від НС.

Згідно з «Концепцією реформування місцевого самоврядування та територіальної організації влади в Україні» [3] до основних повноважень органів місцевого самоврядування на різних рівнях адміністративно-територіального устрою належить гасіння пожеж, забезпечення громадської безпеки, охорони навколишнього природного середовища, надання послуг швидкої медичної допомоги, первинної охорони здоров'я, з профілактики хвороб, санітарно-епідеміологічного захисту. Якісне виконання усіх зазначених вище функцій у період активної діджиталізації країни передбачає обмін великою кількістю інформації, яку нині розглядають як один із основних ресурсів розвитку суспільства, а інформаційні системи й технології – як засіб підвищення продуктивності та ефективності роботи людей. Тому інформація є найцінішим і дорогим ресурсом. Інформаційна технологія визначає процеси передачі та розповсюдження, зберігання і обробки інформації, її використання з певною метою. Усі ці процеси повинні бути швидкими, найменш витратними, максимально корисними, зручними та автоматизованими.

Сучасні інформаційні технології потребують організації високого рівня захисту даних, оскільки оперативна доставка інформації в процесі повсякденної діяльності в умовах децентралізації, а саме створення ЦБГ в ОТГ, оперативна взаємодія з органами державного управління та місцевого самоврядування, іншими міністерствами та відомствами супроводжуються складними інформаційними процесами [4], більшість із яких мають конфіденційний характер.

Стратегічно правильним вирішенням проблеми захисту інформації є використання досягнень криптографії, оскільки вона розширює можливості захисту інформації та забезпечує її безпеку в мережі. Тому перед нами ставилося важливе науково-технічне завдання – розроблення сучасного методу захисту інформації інформаційно-аналітичних систем для здійснення надійного та швидкого управління силами й засобами цивільного захисту в умовах децентралізації та координації дій.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень і публікацій варто виділити [5], де обґрунтовано необхідність створення комплексних систем захисту інформації в розподілених корпоративних мережах, в яких обробляється інформація з обмеженим доступом. У наукових роботах [6; 7] розроблено метод захисту конфіденційної інформації ДСНС України на основі використання операцій розширеного матричного криптографічного перетворення та запропоновано впровадження в телекомунікаційну мережу ДСНС України удосконаленої системи моніторингових спостережень за інцидентами з розрахунком можливості реалізації загроз безпеки інформації. Наукове дослідження [8] присвячене проєктуванню сучасних методів і технічних засобів цивільного захисту, що стали основою для створення інформаційних систем із попередження виникнення пожеж і передачі оперативної інформації для прийняття управлінських рішень.

Активний розвиток інформатизації в системі ДСНС України та ОТГ у сфері цивільного захисту зумовлює значне зростання відомчих інформаційних активів, у тому числі конфіденційного характеру, вимагає ухвалення адекватних і своєчасних рішень по нарощуванню потенціалу системи захисту інформації в області протидії нанесення шкоди інформаційній безпеці, що зростає в міру інтенсифікації розвитку інформаційних технологій. Це дозволяє стверджувати, що наукове дослідження щодо удосконалення захисту інформації в інформаційно-аналітичній системі цивільного захисту, а саме розробки та застосування методу розширеного матричного криптографічного перетворення, є доцільним.

Постановка завдання. Метою дослідження є визначення управлінських процесів, які відбуваються в інформаційно-аналітичних системах ДСНС України та ЦБГ, що потребують захисту інформації, розроблення методу захисту інформаційних ресурсів ДСНС України та ЦБГ.

Для досягнення зазначеної мети необхідно вирішити такі задачі:

– побудувати діяльнісну модель державного управління в сфері цивільного захисту в умовах децентралізації;

– розробити метод захисту інформаційних ресурсів ДСНС України та ЦБГ на основі розширених матричних операцій криптографічного перетворення;

– перевірити статистичні властивості результатів розширеного матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів.

Виклад основного матеріалу дослідження. Опираючись на викладене вище, побудуємо сучасну діяльнісну модель державного управління в сфері цивільного захисту в умовах децентраліза-

Рис. 1. Діяльнісна модель державного управління в сфері цивільного захисту в умовах децентралізації

ції (рис. 1). Так, зовнішні орієнтири (наприклад, за статистикою понад 40% усіх пожеж відбуваються у сільській місцевості, під час яких травмуються та гинуть люди, зазнають значних матеріальних збитків громади. Оскільки в ОТГ об'єднується велика кількість населених пунктів, це призводить до значного збільшення часу прибуття пожежно-рятувальних підрозділів до найбільш віддалених частин ОТГ) мають вплив на формування цільового компоненту в сфері цивільного захисту.

Згідно з новою редакцією Закону України «Про місцеве самоврядування в Україні» [9] в складі повноважень, що виконуються радою громади чи її виконавчим органом, визначено окремим блоком повноваження у сфері цивільного захисту (частина 13 статті 35 законопроєкту). В разі прийняття Верховною Радою України цього Закону основним завданням ОТГ буде забезпечення захисту населення і територій від НС.

У будь-якому випадку всі ці стратегічні дії в умовах реформування місцевого самоврядування супроводжуються складними інформаційними процесами, більшість із яких мають конфіденційний характер. Сучасні інформаційні технології потребують організації високого рівня захисту даних ОТГ. Стратегічно правильним вирішенням проблеми захисту інформації є використання досягнень криптографії, оскільки вона розширює можливості захисту інформації та забезпечує її безпеку в мережі. У [6] доведено, що використання розширених матричних функцій криптографічного перетворення підвищує швидкодію обробки даних у криптосистемах за рахунок паралельного процесу виконання операцій криптоперетворення.

Швидкодія обробки даних і конфіденційність прийняття управлінських рішень є найважливішими параметрами інформаційного обміну між центральним органом виконавчої влади, який реалізує державну політику у сфері цивільного захисту, в ролі якого виступає ДСНС України, та ЦБГ ОТГ. Тому впровадження сучасних інформаційних і телекомунікаційних технологій забезпечить результативність виконання завдань в області цивільного захисту.

Нами розроблений метод захисту інформаційних ресурсів ДСНС України та ЦБГ на основі розширених матричних операцій криптографічного перетворення:

1. На основі даних пароля сформулювати первинну, не вироджену матрицю криптографічного перетворення.
2. Корекція матриці криптографічного перетворення на основі псевдовипадкової послідовності.
3. Перевірка правильності синтезу матриці криптографічного перетворення.
4. Криптографічне перетворення інформації на основі матриць криптографічного перетворення.
5. На основі псевдовипадкової послідовності будуються операції розширеного матричного криптографічного перетворення у випадково вибраній кількості.

6. Криптографічне перетворення інформації на основі розширеного матричного криптографічного перетворення.

7. Перехід до наступного циклу криптографічного перетворення (пункту 2) за наявності вхідної інформації.

Модель процесу реалізації операцій розширеного матричного криптографічного перетворення представлена на рис. 2.

Перевіримо статистичні властивості результатів розширеного матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів. Статичний портрет програмної реалізації алгоритму модифікованого розширеного матричного криптографічного перетворення тестового файлу зображено на рис. 3.

Досліджувана послідовність пройшла комплексний контроль за методикою NIST STS (NIST Statistical test Suite). Такий набір тестів був запропонований під час проведення конкурсу на новий національний стандарт США блокового шифрування. Цей набір використовувався для дослі-

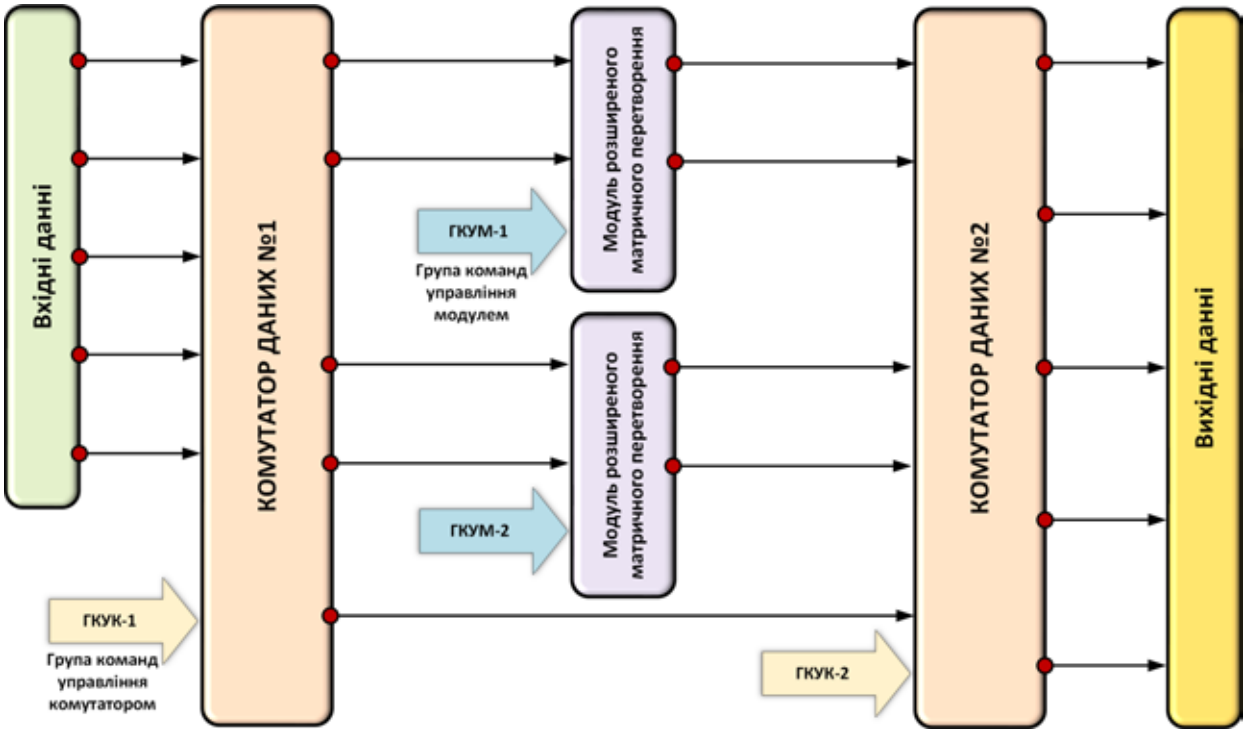

Рис. 2. Модель процесу реалізації операцій розширеного матричного криптографічного перетворення

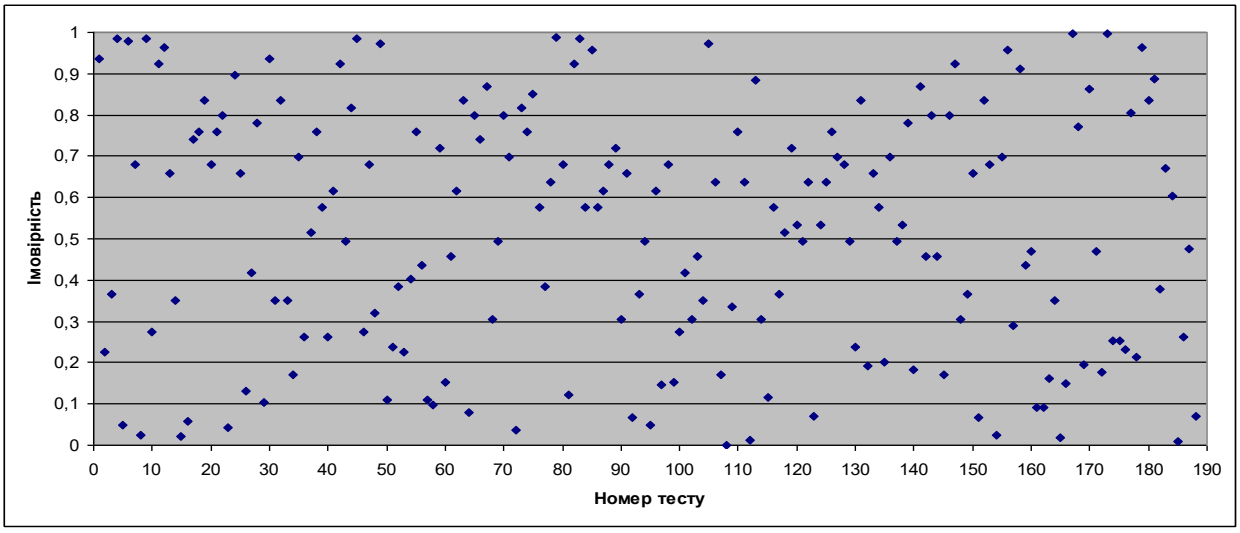

Рис. 3. Статистичний портрет програмної реалізації методу захисту інформації на основі розширених матричних операцій криптографічного перетворення

дження статистичних властивостей кандидатів на новий блоковий шифр. Нині методика тестування, запропонована NIST, є найбільш поширеною у розробників криптографічних засобів захисту інформації.

Відповідно до результатів оцінки програмної реалізації операцій розширеного матричного перетворення кількість тестів, у яких тестування пройшли понад 99% послідовностей, становить 127 (68%), а кількість тестів, у яких тестування пройшли більше 96% послідовностей, 189 (100%).

Аналіз результатів тестування дозволив зробити висновок, що запропонований метод розширеного матричного криптографічного перетворення придатний для використання в інформаційно-аналітичних системах цивільного захисту ДСНС України та ЦБГ.

Висновки. В цьому дослідженні вперше розв'язано важливе науково-технічне завдання розроблення сучасного методу захисту інформації інформаційно-аналітичних систем ДСНС України та ЦБГ для здійснення надійного та швидкого управління силами й засобами цивільного захисту в умовах децентралізації та координації дій.

Вперше побудовано діяльнісну модель державного управління в сфері цивільного захисту в умовах децентралізації. Розроблено метод захисту інформаційних ресурсів ДСНС України та ЦБГ на основі розширених матричних операцій криптографічного перетворення та перевірено статистичні властивості результатів розширеного матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів.

Список літератури:

1. Кодекс цивільного захисту України від 02.10.2012 № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text (дата звернення: 01.03.2021).

2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 01.03.2021).

3. Про схвалення Концепції реформування місцевого самоврядування та територіальної організації влади в Україні : розпорядження Кабінету Міністрів України від 01.04.2014 № 333-р. URL: https://zakon.rada.gov.ua/laws/show/333-2014-%D1%80#Text (дата звернення: 01.03.2021).

4. Барило О.Г., Потеряйко С.П., Тищенко В.О. Інформаційне забезпечення органів державного управління у надзвичайних ситуаціях. *Науковий вісник Академії муніципального управління. Серія: Управління.* 2013. Вип. 4. С. 77–84.

5. Козачок В.А., Коваленко Ю.Б. Особливості побудови комплексних систем захисту інформації в розподілених корпоративних мережах. *Сучасний захист інформації.* 2015. № 1. С. 41–47.

6. Мельник Р.П., Мельник О.Г., Гончар С.В., Бабенко В.Г. Метод захисту конфіденційної інформації як складник управління інформаційною безпекою ДСНС України. *Системи обробки інформації*. 2014. Вип. 4 (120). С. 145–148.

7. Мельник Р.П., Мельник О.Г., Чепурний Г.П. Підвищення інформаційної безпеки телекомунікаційної системи ДСНС України шляхом моніторингу інцидентів та оцінки ризику реалізації загроз безпеки. *Наукові праці : науково-методичний журнал.* 2016. Вип. 271. Т. 283. Комп'ютерні технології. С. 65–69.

8. Мельник О.Г., Мельник Р.П. Проєктування засобів цивільного захисту для управління пожежною безпекою житлового фонду. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки.* 2020. Том 31 (70) № 5. С. 88–93.

9. Законопроекти для обговорення. URL: https://decentralization.gov.ua/law_discussion/project (дата звернення: 01.03.2021).

Melnyk O.G., Melnyk R.P. DEVELOPMENT OF THE METHOD OF INFORMATION PROTECTION OF INFORMATION AND ANALYTICAL SYSTEMS FOR MANAGEMENT OF FORCES AND MEANS OF CIVIL PROTECTION IN CONDITIONS OF DECENTRALIZATION

The research is devoted to the development of a modern method of information protection of information-analytical systems of civil protection of The State Emergency Service of Ukraine and Safety Centers of Citizens in the context of decentralization for reliable and rapid management, coordination.

The management processes that take place in the information-analytical systems of civil protection that require information protection are determined, as a result of which the activity model of public administration in the field of civil protection in the conditions of decentralization is built. It is proved that all strategic actions in the conditions of local self-government reform are accompanied by complex information processes, most of which are confidential and need reliable protection.

The method of protection of information resources of The State Emergency Service of Ukraine and Safety Centers of Citizens on the basis of extended matrix operations of cryptographic transformation is developed,

and also the model of process of realization of operations of extended matrix cryptographic transformation is developed.

The statistical properties of the results of the extended matrix cryptographic transformation of text information on the example of electronic information resources are checked. A statistical portrait of the software implementation of the method of information protection on the basis of extended matrix operations of cryptographic transformation is constructed. Testing was performed according to the NIST Statistical test Suite methodology, based on which it was concluded that the proposed method of extended matrix cryptographic transformation is suitable for use in information-analytical systems of civil protection of The State Emergency Service of Ukraine and Safety Centers of Citizens.

Key words: *information-analytical system, civil protection, Safety Centers of Citizens, activity model of public administration, extended matrix operations of cryptographic transformation.*