УДК 338.47 DOI 10.36910/6775.24153966.2021.71.13

С.П. Арпентій
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України
вул. Миколи Василенка, 3, м. Київ, 03113
ORCID ID: 0000-0003-3326-3942
Researcher ID : AAN-8442-2021

КОДУВАННЯ ІНФОРМАЦІЇ В ІНФОКОМУНІКАЦІЯХ, ЯК ОДИН З ПЕРСПЕКТИВНИХ НАПРЯМКІВ ЗАХИСТУ ІНФОРМАЦІЇ

У статті розкрито принцип кодування інформації в інфокомунікаціях, як один з перспективних напрямків захисту інформації. визначено головні проблеми передачі інформації та принципи формування захищеного каналу передачі інформації в інформаційно-комунікаційних системах. Підкреслено, що в сучасних інформаційно-комунікаційних системах широко застосовується модульне подання інформації та шифрування інформації, коли інформація шифрується на стороні передавача та дешифрується на стороні приймача. Показана структурна схема системи кодування інформації для захисту інформації в інформаційно-комунікаційних системах, в якій поряд з перешкодостійким кодом використовується перемежування символів переданого повідомлення. Описано операції шифрування, дешифрування та перемежування. Зазначається, що процедура перемежування полягає в перестановці символів кодового слова і відновленні вихідної послідовності після передачі її по каналу. Запропоновано алгоритм роботи системи комплексного захисту інформації в інформаційно-комунікаційних системах, який наведено у вигляді блок-схеми. Детально описано принцип роботи системи комплексного захисту інформації. Обґрунтовано методи подання інформації щодо визначення рівня захисту. Описано дію вектора безпеки та сформовано механізм подання результату. Підкреслено, що якщо застосування сигналу системи комплексного захисту інформації в інформаційно-комунікаційних системах призводить до позитивного результату, то на графіку це відбивається за допомогою вектора з напрямком вгору; якщо застосування сигналу системи комплексного захисту інформації в інформаційно-комунікаційних системах завершується помилками, то на графіку це відбивається за допомогою вектора з нахилом вниз. Графічно представлено діаграми вагових приналежностей безпеки у межах часового розподілу системи комплексного захисту інформації в інформаційно-комунікаційних системах. Наголошено, що при використанні надлишкового кодування сукупність елементів пам'яті можна розглядати як канал передачі інформації в інформаційно-комунікаційних системах, в якому остання передається не в просторі, а в часі.

Ключові слова: *кодування, інформація, шифрування, захист, інфокомунікації, передача, шифр, безпека.*

С.П. Арпентий

КОДИРОВКА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИЯХ, КАК ОДИН ИЗ ПЕРСПЕКТИВНЫХ НАПРАВЛЕНИЙ ЗАЩИТЫ ИНФОРМАЦИИ

В статье раскрыто принцип кодирования информации в инфокоммуникациях, как одно из перспективных направлений защиты информации. определены основные проблемы передачи информации и принципы формирования защищенного канала передачи информации в информационно-коммуникационных системах. Подчеркнуто, что в современных информационно-коммуникационных системах широко применяется модульное представление информации и шифрования информации, когда информация шифруется на стороне передатчика и дешифруется на стороне приемника. Показана структурная схема системы кодирования информации для защиты информации в информационно-коммуникационных системах, в которой наряду с помехоустойчивым кодом используется чередования символов передаваемого сообщения. Описаны операции шифрования, дешифрования и чередования. Отмечается, что процедура чередования состоит в перестановке символов кодового слова и восстановлении исходной последовательности после передачи ее по каналу. Предложен алгоритм работы системы комплексной защиты информации в информационно-коммуникационных системах, который приведен в виде блок-схемы. Подробно описан принцип работы системы комплексной защиты информации. Обоснованы методы представления информации по определению уровня защиты. Описаны действие вектора безопасности и сформирован механизм предоставления результата. Подчеркнуто, что если применение сигнала системы комплексной защиты информации в информационно-коммуникационных системах приводит к положительному результату, то на графике это отражается с помощью вектора с направлением вверх; если применение сигнала системы комплексной защиты информации в информационно-коммуникационных системах завершается ошибками, то на графике это отражается с помощью вектора с наклоном вниз. Графически представлены диаграммы весовых принадлежностей безопасности в пределах временного распределения системы комплексной защиты информации в информационно-коммуникационных системах. Отмечено, что при использовании избыточного кодирования совокупность элементов памяти можно рассматривать как канал передачи информации в информационно-коммуникационных системах, в котором последняя передается не в пространстве, а во времени.

Ключевые слова: *кодирование, информация, шифрование, защита, Инфокомуникации, передача, шифр, безопасность.*

S.P. Arpentii

CODING OF INFORMATION IN INFOCOMMUNICATIONS, AS ONE OF THE PROMISING AREAS OF INFORMATION PROTECTION

The article reveals the principle of coding information in infocommunications, as one of the promising areas of information protection. the main problems of information transfer and principles of formation of the protected channel of information transfer in information and communication systems are defined. It is emphasized that in modern information and communication systems modular presentation of information and encryption of information is widely used, when information is encrypted on the transmitter side and decrypted on the receiver side. The block diagram of the information encoding system for information protection in information and communication systems is shown, in which the interleaving of the symbols of the transmitted message is used along with the noise-tolerant code. Encryption, decryption and interleaving operations are described. It is noted that the interleaving procedure is to rearrange the characters of the codeword and restore the original sequence after transmitting it on the channel. The algorithm of the system of complex information protection in information and communication systems is offered, which is given in the form of a block diagram. The principle of operation of the system of complex information protection is described in detail. Methods of presenting information on determining the level of protection are substantiated. The action of the safety vector is described and the mechanism of presenting the result is formed. It is emphasized that if the application of the signal of the complex information protection system in information and communication systems leads to a positive result, then the graph is reflected by a vector with an upward direction; if the application of the signal of the complex information protection system in information and communication systems ends in errors, then the graph is reflected by a vector with a downward slope. Graphs of weight security accessories within the time distribution of the system of complex information protection in information and communication systems are graphically presented. It is emphasized that when using redundant coding, the set of memory elements can be considered as a channel for transmitting information in information and communication systems, in which the latter is transmitted not in space but in time.

Key words: *encryption, information, encryption, protection, infocommunications, transmission, cipher, security.*

Постановка проблеми. Масовість інформації, що передається по каналах зв'язку, зростає з геометричною прогресією. Кожен байт переданої інформації потребує захисту та контролю. В умовах необхідної передачі даних по сучасним каналам зв'язку необхідно вирішувати два завдання: захищати дані від атмосферних перешкод і можливих несправностей апаратури, а також забезпечувати секретність інформації, що передається. Теорія завадостійкого кодування дозволяє вирішувати завдання захисту даних від атмосферних перешкод і можливих несправностей апаратури. Різні методи шифрування даних дозволяють вирішити питання забезпечення секретності інформації, що передається.

Фундаментальною основою сучасної наукової думки щодо формування безпечного каналу передачі даних стали роботи К. Шеннона [1]. Саме відомий американський вчений вперше довів, що, з одного боку, теоретично можна досягти передачі інформації майже без помилок, і, з іншого боку, можливий досконалий шифр для забезпечення секретності переданих повідомлень. Сформовані, обґрунтовані та доведені математичні основи завадостійкого кодування і криптографії закладені в роботах К. Шеннона є основою сучасної криптографічної науки

Незважаючи на багато спільних рис кодування та криптографія мають відмінні риси, що є причиною їх незалежного розвитку і малого впливу друг на друга, саме спільне застосування цих напрямків є актуальною проблематикою сьогодення на тлі стрімкого розвитку інфокомунікацій.

Аналіз останніх досліджень і публікацій. Методологія наукової думки, у сфері захисту інформації, охоплює висвітлення питань формування захищеного простору та безпечної передачі інформації у межах захищеного простору. На протязі багатьох років низка вчених проводили дослідження та здійснювали вдосконалення методів та засобів реалізації механізмів захисту інформації.

Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв та В. В. Сінюгін [2] розглядають питання, що належать до галузі інформаційної безпеки. Авторами висвітлені основи організації захисту інформації, методи оцінювання захищеності та основні положення побудови комплексних систем захисту інформації.

Методи та засоби стеганографічного захисту інформації на основі вейвлет-перетворень дослідили В. В. Лукічов, В. А. Лужецький та А. С. Васюра [3]. У монографії розглянуто моделі та методи стеганографічного захисту інформації і визначено якості, що впливають на стійкість вбудованих даних. Наведено узагальнені методи і моделі неадаптивного та адаптивного вбудовування даних у зображення, які враховують взаємозв'язки між стеганографічними перетвореннями.

Л.М. Дегтярьова та О.О. Сідокур [4] розкрили механізм контролю цілісності даних в локальних мережах. Науковцями підкреслено, що система захисту повинна перехоплювати функцію читання файлу, запускати процедуру контролю і потім (при необхідності, вже після відновлення файлу з еталонної копії) видавати цю функцію на обробку в ядро операційної системи. Але якщо контроль цілісності реалізується програмно, то виникає проблема контролю цілісності і коректності функціонування власне контролюючої програми, тому в загальному випадку здійснення контролю реалізується апаратною частиною.

Матеріали [5] відображають загальні питання інфокомунікацій, питання обробки зображень і даних, а також захисту інформації в інформаційно-комунікаційних системах.

Із зарубіжних авторів варто відзначити такі роботи як: A. Zemliachenko, R. Kozhemiakin, B. Vozel, V. Lukin [6], A. Zemliachenko, S. Abramov, V. Lukin, B. Vozel, K. Chehdi [7], E. Christophe, C. Mailhes, P. Duhamel [8], T. Skauli [9], B. Vozel, K. Chehdi, L. Klaine, V. Lukin, S. Abramov [10], I. Van Zyl Marais, W.H. Steyn, J.A. du Preez [11], S. Prasad, L.M. Bruce and J. Chanussot, Springer [12], W. Lin, C.-C. Jay Kuo [13], O.K. Al-Chaykh, R.M. Mersereau [14] та інші.

Основна увага, науковців присвячена питанню розробки, модернізації та впровадження новітніх механізмів криптографічного захисту, однак мало уваги приділено ефективності їх застосуванню в інфокомунікаціях, саме тому питання кодування інформації в інфокомунікаціях, як один з перспективних напрямків захисту інформації є актуальним та потребує детального опрацювання.

Постановка завдання. Розкрити принципи кодування інформації в інфокомунікаціях, як один з перспективних напрямків захисту інформації.

Викладення основного матеріалу дослідження. В сучасних інформаційно-комунікаційних системах широко застосовується модульне подання інформації, коли кодове слово довжини *a* розбивається на блоки (модулі) довжини *b*. Для боротьби з помилками всередині модулів застосовується цілий ряд кодів, таких як коди Ріда-Соломона (РС), Бартона і інші. Однак кодеки цих кодів досить складні, володіють невисокою швидкодією при корекції багаторазових помилок.

Також застосовується шифрування інформації, коли інформація шифрується на стороні передавача та дешифрується на стороні приймача. Для підвищення рівня безпеки додатково застосовують перемежування інформації. Засіб перемежування певним чином перемішує (міняє місцями) символи переданого повідомлення (або кодового слова). Основна причина розробки та використання перемежувача – бажання рознести розташовані поруч (згруповані) помилки в повідомленні («розмазати» помилки за повідомленням) з метою спрощення і скорочення в часі процедури виправлення таких помилок порівняно простими кодами.

На рис. 1 показана структурна схема системи кодування інформації для захисту інформації в інформаційно-комунікаційних системах, в якій поряд з перешкодостійким кодом використовується перемежування символів переданого повідомлення.

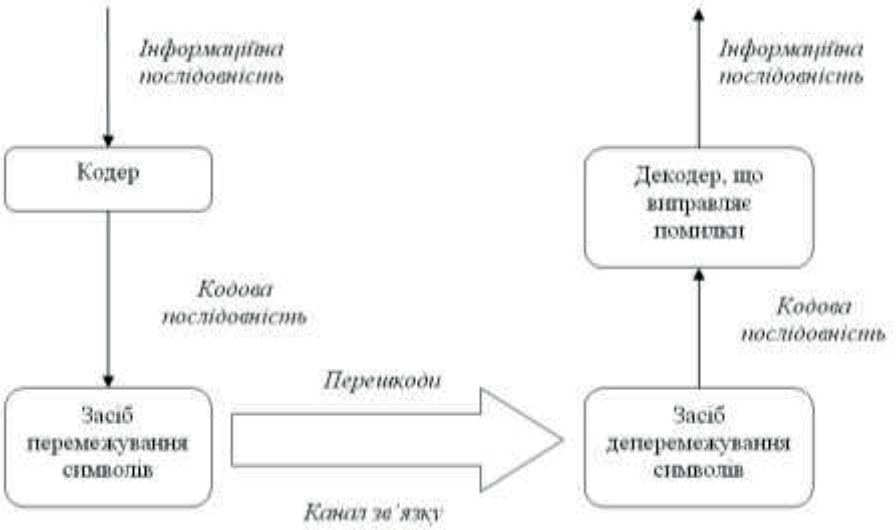

Рис. 1. Структурна схема системи кодування інформації для захисту інформації в інформаційно-комунікаційних системах

Операція декодування в два етапи дозволяє майже повністю позбавитися від впливу перешкод. На першому етапі проводиться перетворення груп (пакетів) помилок в групу випадкових (зазвичай одиночних) помилок. На другому етапі сигнал обробляється за допомогою класичних методів боротьби з випадковими помилками (лінійні ітеративні коди, згорткові коди, турбо-коди), що повинно призводити до повної корекції помилок.

Процедура перемежування полягає в перестановці символів кодового слова і відновленні вихідної послідовності після передачі її по каналу. При перемежуванні забезпечується перетворення біт вхідної послідовності у вихідну послідовність без зміни її довжини. Однак чим більше глибина перемежування (мінімальна відстань – в бітах, на яку розносяться сусідні символи вхідної послідовності), тим більше затримка.

У загальному випадку вибір глибини перемежування залежить від двох чинників. З одного боку, чим більше відстань між сусідніми символами, тим більшої довжини пакет помилок може бути виправлений. З іншого боку, чим більше глибина перемежування, тим складніше апаратно-програмна реалізація устаткування і більше затримка сигналу.

Ключовим питанням в дослідженнях з комплексного захисту інформації в інформаційно-комунікаційних системах (ІКС) є визначення параметрів і критеріїв захищеності інформації. З цією метою розроблені методи формування правил розмежування доступу, які включають в себе класифікацію компонент доступу і загроз безпеки інформації, розробку моделі порушника і оцінку можливості реалізації загроз. Дослідження поведінки ІКС під впливом погроз порушника, правил розмежування доступу дозволили визначити функції системи розмежування доступу і її структуру. За допомогою розроблених моделей розмежування доступу до інформації в ІКС, визначено та досліджено параметри засобів захисту каналів доступу, засобів управління доступом до захищених даних та запропоновано методи їх кількісної оцінки.

Алгоритм роботи системи комплексного захисту інформації в інформаційно-комунікаційних системах наведено у вигляді блок-схеми на рисунку 2.

Для безумовного розмежування доступу до ресурсів ІКС розроблені алгоритми реалізації правил розмежування доступу, що гарантують їх повноту і несуперечність в умовах неоднозначності розподілу відомостей між компонентами ІКС. Аналіз доступу суб'єкта до об'єкту, що охороняється виконується наступним чином. У разі відкриття суб'єктом доступу до об'єкту, що охороняється, зазвичай виконується за допомогою функцій типу Create або Open, система управління безпекою переглядає список елементів цього об'єкту, що охороняється для пошуку елемента, в якому зберігається ідентифікатор безпеки суб'єкта [3]. Якщо такий елемент у списку елементів не знайдений, то потік отримує відмову в доступі до об'єкту. Якщо ж такий елемент знайдений, то система перевіряє тип цього елемента. Якщо SID суб'єкта збігається з SID власника об'єкта і запитуються стандартні права доступу, то доступ надається незалежно від вмісту елементів. Далі система послідовно порівнює SID кожного елементу зі списку з SID маркера. Якщо виявляється відповідність, виконується порівняння маски доступу з перевіреними правами. Для заборонених елементів навіть при частковому збігу прав доступ негайно відхиляється. Для успішної перевірки дозвільних елементів необхідно щоб відбувся збіг всіх прав. Кожна програма «налаштованого» сигналу, який був згенерований заданою системою роботи в традиційних просторах, дасть певний результат: «успіх» або «невдача». Конкретний результат потім відбивається в додатковому вимірі ефективності застосовуваної системи комплексного захисту інформації в інформаційно-комунікаційних системах.

Цю ефективність можна позначати різними графічними символами. Один з найпростіших – «хрестики і нулики».

Але ми оберемо інший спосіб, при якому результат представляється у вигляді спрямованої стрілки-вектора:

– якщо застосування сигналу системи комплексного захисту інформації в інформаційно-комунікаційних системах призводить до позитивного результату, то на графіку це відбивається за допомогою вектора з напрямком вгору;

– якщо застосування сигналу системи комплексного захисту інформації в інформаційно-комунікаційних системах завершується помилками, то на графіку це відбивається за допомогою вектора з нахилом вниз.

Вектор ефективності безпеки – це графічний спосіб позначення результату операції: напрямок вгору – успіх, вниз – невдача. Думка про поводження з системою за принципом «від противного може викликати здивування.

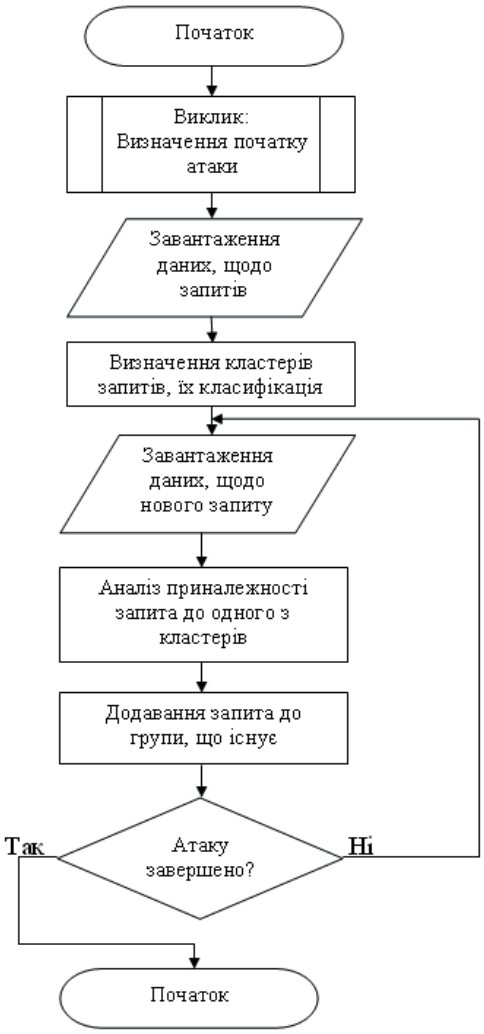

Рис. 2. **Блок-схема алгоритму роботи системи комплексного захисту інформації в інформаційно-комунікаційних системах**

Вектор ефективності безпеки – це графічний спосіб позначення результату операції: напрямок вгору – успіх, вниз – невдача. Думка про поводження з системою за принципом «від противного може викликати здивування.

Якщо спосіб працювати по сигналу, не передбачений його конструкторським задумом, то очікування успіху було б неприродним. Система комплексного захисту інформації в інформаційно-комунікаційних системах створена, щоб генерувати сигнали, що забезпечують успіх при «нормальному» застосуванні. «Здвоєна» схема відображення результатів в додатковому вимірі ефективності сигналів передбачає варіанти як «нормального» порядку дій, так і «зворотного» того, який викликаний умовами застосування системи комплексного захисту інформації в інформаційно-комунікаційних системах.

Однак, неважко уявити і варіанти «асиметричної відповіді» системи, коли результати застосування генерованих сигналів – «прямого» і «зворотного» – можуть бути зовсім не протилежними.

Задамо значення ефективності безпеки відповідно до множини:

$$U = \{0; 0.1; 0.2; 0.3; 0.4; 0.5; 0.6; 0.7; 0.8; 0.9; 1\}$$

таким чином:

V= $\mu_v(u) = u, u \in U$ висока: ;

BV= $\mu_{bv}(u) = \sqrt{u}, u \in U$ більш висока: ;

DV= $\mu_{dv}(u) = u^2, u \in U$ дуже висока: ;

ZV= $\mu_{zv}(u) = \begin{cases} 1, u = 1, \\ 0, u < 1, \end{cases}, u \in U$ занадто висока: ;

N= $\mu_n(u) = 1 - u, u \in U$ низька: ;

BN= $\mu_{bn}(u) = \sqrt{1-u}, u \in U$ більш низька: ;

DN= $\mu_{dn}(u) = (1-u)^2, u \in U$ дуже низька: ;

ZN= $\mu_{zn}(u) = \begin{cases} 0, \mathbf{u = 1}, \\ \mathbf{1}, u < \mathbf{1}, \end{cases}, u \in U$ занадто низька: .

Відповідно до схеми реалізації запропонованої методології оцінювання ефективності безпеки аналізуються вагові приналежності за відповідними позиціями $q_0 \div q_6$.

При використанні надлишкового кодування сукупність елементів пам'яті можна розглядати як канал передачі інформації в інформаційно-комунікаційних системах, в якому остання передається не в просторі, а в часі.

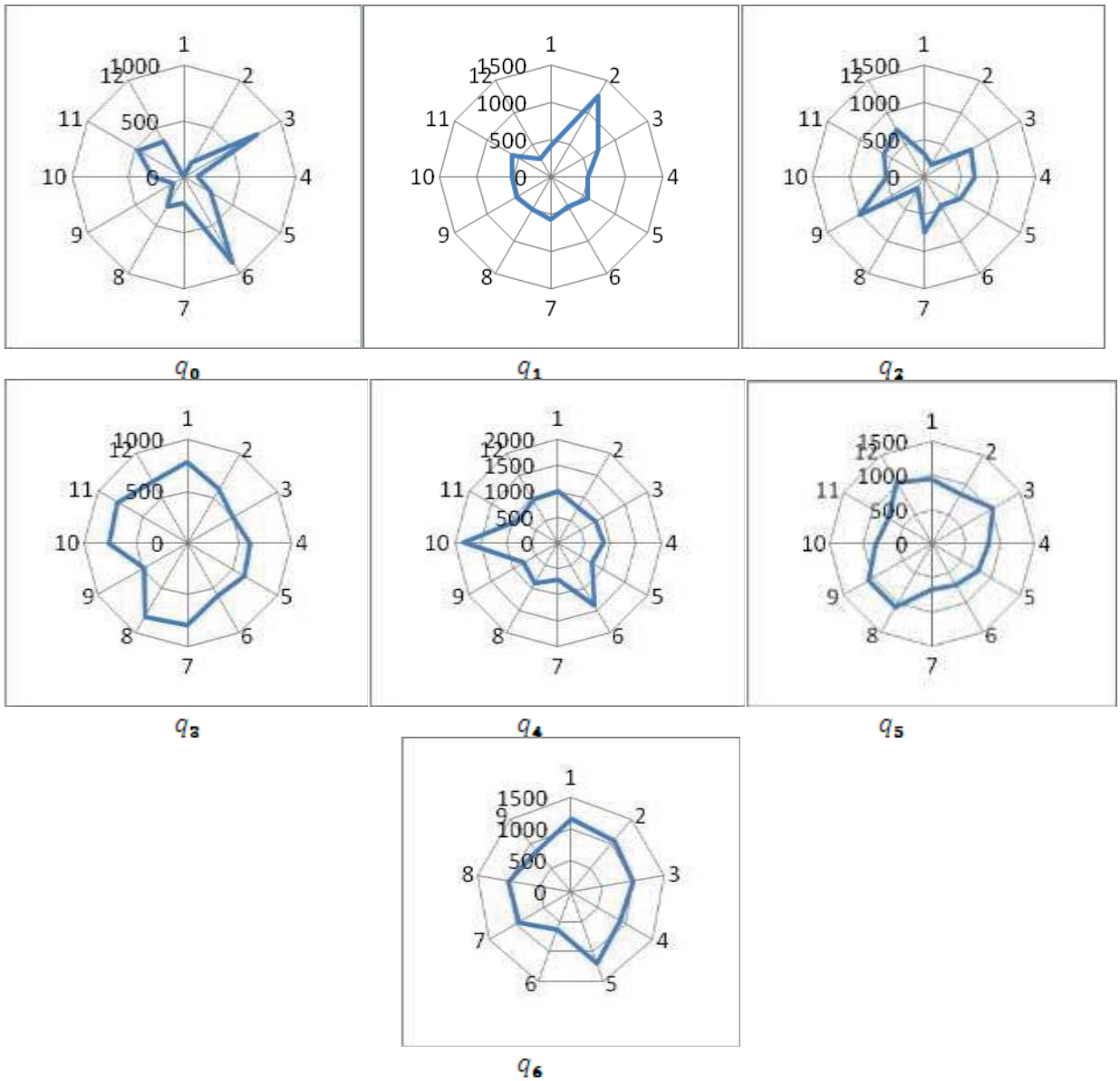

Рис. 3. **Діаграми вагових приналежностей безпеки у межах часового розподілу системи комплексного захисту інформації в інформаційно-комунікаційних системах**

Ця особливість призводить до розгляду систем зберігання як специфічного каналу передачі інформації в інформаційно-комунікаційних системах. Виникаючі при цьому ситуації добре описуються за допомогою узагальненої моделі каналу зберігання [6].

Висновки і перспективи подальших досліджень. У роботі досліджено механізм кодування інформації в інфокомунікаціях, як один з перспективних напрямків захисту інформації.

Застосування моделі каналу зберігання інформації в інформаційно-комунікаційних системах дозволяє більш повно узгодити стан каналу з введеною надмірністю, зменшити її,

сформувати вимоги до коригуючого коду, запропонувати ефективні методи і коди для захисту пам'яті від багаторазових помилок. Коди, що виправляють дефекти, дозволяють узгодити записувану інформацію зі станом дефектів при використанні невеликої інформаційної надмірності і складності обробки.

Перспективи подальших досліджень ґрунтуються на розробці інформаційної системи комплексного захисту інформації в інфокомунікаціях, з підвищеним рівнем безпеки.

Література:

1. Shannon C.E. Communication in the presence of noise. Proc. *Institute of Radio Engineers*. 1949. Vol. 37, No. 1. C. 10-21.

2. Комплексні системи захисту інформації : навчальний посібник / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін ; ВНТУ. Вінниця : ВНТУ, 2018. 118 с.

3. Методи та засоби стеганографічного захисту інформації на основі вейвлет-перетворень : монографія / В. В. Лукічов, В. А. Лужецький, А. С. Васюра ; ВНТУ. Вінниця : ВНТУ, 2014. 160 с.

4. Механізм контролю цілісності даних в локальних мережах / Дегтярьова Л.М., Сідокур О.О. *Проблеми інфокомунікацій* : Матеріали другої всеукраїнської науково-технічної конференції. Полтава: ПолтНТУ; Київ: НТУ; Харків: НТУ«ХПІ»; Київ: ДУТ; Харків: УкрДУЗТ; Мінськ: БНТУ; Полтава: ВКСС ВІТІ, 2018. С. 14-16.

5. Наукомісткі технології в інфокомунікаціях: обробка, захист та передача інформації: Монографія / під загальною редакцією В. М. Безрука, В. В. Баранніка. Харків. : Видавничтво «Стиль-издат», 2018. 327 с.

6. Prediction of Compression Ratio in Lossy Compression of Noisy Images / A. Zemliachenko, R. Kozhemiakin, B. Vozel, V. Lukin. *Proceedings of TCSET 2016* (Lviv-Slavske, February, 2016, Ukraine). P. 693-697.

7. Compression Ratio Prediction in Lossy Compression of Noisy Images / A. Zemliachenko, S. Abramov, V. Lukin, B. Vozel, K. Chehdi. *Proceedings of IGARSS*, July 2015. Milan, Italy. P. 3497-3500.

8. Christophe E. Hyperspectral Image Compression: Adapting SPIHT and EZW to Anisotropic 3-D Wavelet Coding / E. Christophe, C. Mailhes, P. Duhamel. *IEEE Transactions on Image Process*. 2008. Vol. 17, No. 12. P. 2334-2346.

9. Skauli T. Sensor noise informed representation of Hyperspectral data, with benefits for image storage and processing. *Optics Express*. 2011. Vol. 19, No. 14. P. 13031-13046.

10. Noise identification and estimation of its statistical parameters by using unsupervised variational classification / B. Vozel, K. Chehdi, L. Klaine, V. Lukin, S. Abramov. *Proceedings of ICASSP*. 2006. Vol. II. P. 841-844.

11. Van Zyl Marais I. On-board image quality assessment for a small low earth orbit satellite / I. Van Zyl Marais, W.H. Steyn, J.A. du Preez. *Proceedings of the 7th IAA Symposium on Small Satellites for Earth Observation*. 2009. https://www.researchgate.net/publication/229016689_Onboard_image_quality_assessment_for_a_small_low_earth_orbit_satellite (Last accessed: 02.11.2020).

12. Christophe E. Hyperspectral Data Compression Tradeoff. "Optical Remote Sensing. Advances in Signal Processing and Exploitation Techniques," Edited by S. Prasad, L.M. Bruce and J. Chanussot, Springer. 2011. Vol. VIII. P. 9-29.

13. Lin W., Jay Kuo C.-C. Perceptual Visual Quality Metrics: A Survey *Journal of Visual Communication and Image Representation*. 2011. Vol. 22, No 4. P. 297-312.

14. Al-Chaykh O.K. Lossy compression of noisy images. *IEEE Transactions on Image Processing*. 1998. Vol. 7, No 12. P. 1641-1652.