МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

MINISTRY OF DEFENCE OF UKRAINE
Military Institute of Telecommunications and Informatization Technologies named after Heroes of Kruty

Системи і технології зв'язку, інформатизації та кібербезпеки
Випуск № 2 (2)

Communication, informatization and cybersecurity systems and technologies
ISSUE № 2 (2)

У збірнику викладені статті наукових та науково-педагогічних працівників, докторантів, ад'юнктів (аспірантів), курсантів, здобувачів інституту та інших установ (організацій) за наступними науковими напрямами:

перспективи розвитку телекомунікаційних систем, комплексів та засобів спеціального призначення;

захист інформації в спеціальних інформаційно-комунікаційних системах;

стан і розвиток автоматизованих систем управління військами та зброєю;

інформаційні системи та мережі, системи підтримки прийняття рішень спеціального призначення;

бойове застосування систем зв'язку та автоматизації Збройних сил України;

теорія і практика кібербезпеки та інформаційної боротьби в комп'ютеризованих системах і мережах.

Запрошуємо до співробітництва всі зацікавлені установи та організації, які проводять наукові дослідження та науково-технічні розробки за даними напрямами.

The book containes articles of scientific and teaching staff, post graduate students, adjuncts, institute applicants and other institutions (organizations) applicants in the following fields:

prospects of telecommunications systems, development, facilities and means of special purpose;

in special information protection and communication systems;

automated systems state and development of army weapons;

information systems and networks, decision support systems for special purposes;

combat use of communications systems and automation of Armed Forces of Ukraine;

theory and practice of cyber security and information warfare in computerized systems and networks.

All interested institutions and organizations, who conduct research and development in the directions state, are invited for cooperation.

Київ – 2022 – Kyiv

УДК 621
ББК Ц4 (4Укр) 39
З – 415

Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. В. А. Романюка. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2022. № 2 (2). 80 с.

ISSN 2786-6610

Науковий профіль видання:
125 – Кібербезпека;
126 – Інформаційні системи та технології;
255 – Озброєння та військова техніка

Засновник – Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
(код за ЄДРПОУ 24978555).
Свідоцтво про державну реєстрацію видання: КВ № 25184-15124 Р від 20.07.2022.
Адреса редакції: 01011, м. Київ, вул. Князів Острозьких, 45/1. Тел. 256-22-73.
Електронна адреса: naukaviti@gmail.com

Відповідальний за випуск Гришенко Н. О.
Зам. 266. Друк. арк. 15,25.
Ум.-друк. арк.14,18. Обл.-вид. арк. 13,19. Формат паперу 60×84/8.
Тираж 100 прим. (безкоштовно).
Адреса друкарні ВІТІ імені Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

ISSN 2786-6610

З М І С Т

CONTENTS

УДК.621.391

Боголій С. М. ORCID: 0000-0001-8110-6322 (ВІТІ)
канд. техн. наук Гурський Т. Г. ORCID: 0000-0001-7646-853X (ВІТІ)
Макарчук В. І. ORCID: 0000-0002-3997-4684 (ВІТІ)
Хижий О. І. (НУОУ)

ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ МОБІЛЬНИХ РАДІОМЕРЕЖ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ АДАПТИВНОГО ДІАГРАМОУТВОРЕННЯ

Радіомережі класу MANET (далі – мобільні радіомережі, МР) знаходять все ширшого застосування для організації тактичного військового радіозв'язку за останні роки. Завадозахищеність таких радіомереж може бути значно вищою порівняно з класичними радіомережами (з ретранслятором або без нього) за рахунок можливості багатократної ретрансляції повідомлень.

Перспективним напрямком підвищення завадозахищеності МР на фізичному рівні є застосування антенних решіток (АР) з можливістю керування напрямком основного випромінювання, що дозволяє забезпечити максимальні значення відношення сигнал/завада на входах приймачів окремих радіостанцій на маршруті передачі інформації. У той же час, для забезпечення максимальної завадозахищеності у таких МР необхідне урахування особливостей формування діаграм направленості антен радіостанцій мережі, просторових координат радіостанцій та постановників завад.

У статті проведено аналіз завдань, які виникають при впровадженні технології адаптивного діаграмоутворення в МР в умовах активної радіоелектронної протидії, основними з яких є наступні: визначення просторових координат власної станції, кореспондентів мережі та постановника навмисних завад; розрахунок оптимального кута орієнтації основного пелюстка діаграми направленості антени при прийомі сигналу від сусідніх кореспондентів з урахуванням взаємного розташування радіостанцій та постановника завад; практична реалізація обміну координатною інформацією між радіостанціями.

Урахування та розв'язання цих завдань дозволить забезпечити ефективну реалізацію протоколів маршрутизації у мобільній радіомережі з АР та підвищити завадозахищеність як на окремих інформаційних напрямках, так і радіомережі в цілому.

Ключові слова: *мобільна радіомережа, антенна решітка, відношення сигнал/завада, завадозахищеність, діаграмоутворення, маршрутизація, навмисна завада, інформаційний канал, службовий канал.*

S. Boholii, T. Hurskyi, V. Makarchuk, A. Khyzhyi. Increasing the anti-jammingness of mobile radio networks with adaptive beamforming.

MANET radio networks (mobile radio networks, MRN) are increasingly used for tactical military radio communications in recent years. Anti-jammingness of such radio networks can be much higher compared to conventional radio networks (with or without a repeater) due to the possibility of multiple relay of messages.

A promising direction to increase the noise immunity of MRN at the physical level is the use of antenna arrays (AR) with the ability to control the direction of the main radiation, which allows to ensure maximum values of signal-to-interference ratio at the inputs of individual radio stations. At the same time, in order to ensure maximum noise immunity in such MRNs, it is necessary to take into account the peculiarities of the formation of directional diagrams of antennas of radio stations of the network, spatial coordinates of radio stations and jammers.

The article analyzes the tasks that arise when implementing the technology of adaptive charting in MRN in the conditions of active electronic countermeasures, the main ones are the following: determination of the spatial coordinates of the own station, network correspondents and the jammer; calculation of the optimal angle of orientation of the main lobe of the antenna pattern when receiving a signal from neighboring correspondents, taking into account the mutual location of radio stations and the jammer; practical implementation of the exchange of coordinate information between radio stations.

Taking into account and solving these tasks will ensure the effective implementation of routing protocols in the mobile radio network with the AR, and increase interference protection in both individual information areas and the radio network as a whole.

Keywords: *mobile radio network, antenna array, signal-to-interference ratio, anti-jammingness, beamforming, routing, intentional interference, data channel, service channel.*

Постановка завдання в загальному вигляді

За останні роки радіозв'язок в тактичній ланці управління військами все більше організовується у вигляді мобільних радіомереж класу MANET – Mobile Ad Hoc Networks [1; 2]. Такі мережі мають низку суттєвих переваг, порівняно і з традиційними військовими симплексними (напівдуплексними) радіомережами, і зі стільниковими та транкінговими мережами загального користування: децентралізоване управління, відсутність фіксованої

інфраструктури, мобільність усіх вузлів мережі, можливість багатократної ретрансляції інформаційних повідомлень на шляху від відправника до отримувача тощо [3].

Водночас, питання підвищення ефективності функціонування мобільних радіомереж в умовах активного радіоелектронного подавлення досліджені недостатньо. Зокрема, поряд із традиційними способами забезпечення завадозахисту у МР з'являються додаткові – за рахунок використання направлених антен (адаптивних АР), а також можливості створення декількох альтернативних маршрутів передачі повідомлень.

Аналіз публікацій за темою дослідження

Роботи, присвячені проблемі підвищення завадозахищеності радіомереж, пропонують її вирішення, переважно на фізичному рівні еталонної моделі взаємодії відкритих систем: за рахунок технологій розширення спектра – псевдовипадкове перестроювання робочих частот (ППРЧ) [4; 5] та шумоподібні сигнали ШСС (так зване пряме розширення) [5–7], просторової фільтрації та схем подавлення завад різного роду [5; 8; 9]. На канальному рівні підвищення завадозахищеності можливе за рахунок завадостійкого кодування [10; 11].

Використання просторової фільтрації навмисних завад на практиці обмежувалося діапазонами робочих частот військових радіозасобів, які не дозволяли виготовити прийнятні за масо-габаритними показниками антенні пристрої. При переході у більш високі діапазони частот (сотні МГц, одиниці ГГц) цілком можливим є застосування складних антенних систем, адаптивних АР або АР з комутацією променя [8; 12]. Застосування АР дозволить забезпечити просторову фільтрацію завад та сигналів та збільшити рівень корисного сигналу на прийомі.

В роботі [13] проведено аналіз ефективності методів формування діаграми спрямованості АР для мобільних радіомереж. Але методи, розглянуті в [13], забезпечують ефективну роботу МР в умовах низьких шумів в каналі зв'язку та малоефективні в умовах потужних завад.

В роботі [14] розглянуто методи адаптивного діаграмоутворення для підвищення завадозахищеності прийому, але у загальному вигляді, без урахування особливостей функціонування мобільних радіомереж. Крім цього, методи, розглянуті в [13; 14], мають достатньо високу обчислювальну складність.

В роботі [15] показано ефективність адаптивного формування нулів діаграми направленості адаптивної АР в МР в умовах навмисних завад, але не наведено рекомендацій щодо реалізації алгоритму діаграмоутворення.

В роботі [16] запропоновано методику управління направленістю випромінювання АР з круговим розташуванням випромінюючих елементів у мобільній радіомережі в умовах навмисних завад. Однак в [16] вирішується завдання передачі інформації кореспонденту, для якого може бути забезпечене найбільше відношення сигнал/завада (ВСЗ) на вході приймача. Передбачається, що далі цей кореспондент за тим же принципом буде ретранслювати інформацію, поки вона не досягне отримувача. В реальних мережах це може призвести до надмірного використання пропускної спроможності окремих каналів зв'язку та мережі в цілому. Таким чином, на мережевому рівні необхідно враховувати особливості діаграмоутворення у мобільній мережі при визначенні кореспондентів (вузлів), які можуть взяти участь у побудові необхідного маршруту в умовах активного радіоелектронного подавлення.

Тому, *метою статті є урахування особливостей адаптивного діаграмоутворення при реалізації протоколів маршрутизації у мобільних військових радіомережах в умовах постановки навмисних завад.*

Виклад основного матеріалу

Антенними решітками, які порівняно просто реалізувати на практиці у військових тактичних радіомережах, є антенні системи з комутацією променя (з керуванням напрямком основного випромінювання) з круговим розташуванням випромінюючих елементів (рис. 1) [16].

Нехай центр кола, на якому розташовуються елементи КАР, співпадає з центром сферичної системи координат. Якщо $\bar{R}(A)$ – радіус-вектор точки спостереження A, то його кутові координати визначаються кутами θ і φ, де $\theta \in [0, \pi)$ – відкладається від осі OZ у

вертикальній площини, $\varphi \in [0,2\pi)$ – відкладається від осі *OX* в горизонтальній (азимутальній) площині.

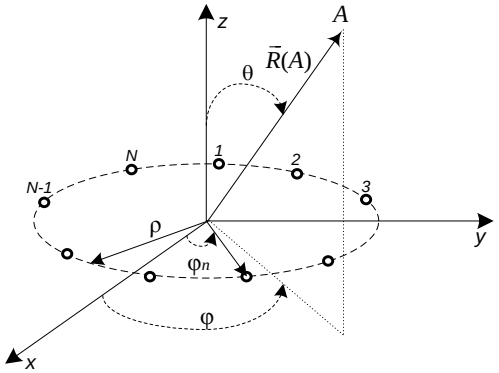


Рис. 1. АР з круговим розташуванням випромінюючих елементів

Просторова напруженість електричного поля для АР з рівномірним розташуванням *N* елементів по колу з радіусом ρ визначається за формулою [16]:

$$E(\theta,\varphi) = \sum_{n=1}^{N} E_0 \exp[\mathrm{j}\kappa_\lambda \rho \sin(\theta)\cos(\varphi - \varphi_n) + \mathrm{j}\psi_n], \quad (1)$$

де $E_0 = 1$ – значення величини (θ, φ) для неспрямованого випромінювача;

$\kappa_\lambda = 2\pi/\lambda$ – хвильове число;

$\varphi_n = 2\pi n / N$ – кутове розміщення *n*-го елемента на колі в азимутальній площині;

ψ_n – фазовий зсув *n*-го елемента КАР, що визначається за формулою:

$$\psi_n = \kappa_\lambda \rho \sin(\theta_0)\cos(\varphi_0 - \varphi_n),$$

де (θ_0, φ_0) – напрям максимуму ДН КАР.

Якщо усі радіостанції МР розташовані в горизонтальній площині, то $\theta = \theta_0 = 90°$.

Коефіцієнт направленої дії (КНД) КАР кількісно можна визначити через просторовий розподіл напруженості електричного поля $E(\theta,\varphi)$ [12]:

$$D(\theta,\varphi) = \frac{|E(\theta,\varphi)|^2}{\frac{1}{4\pi}\int_0^{2\pi}\int_0^{\pi} |E(\theta,\varphi)|^2 \sin(\theta) d\theta d\varphi}. \quad (2)$$

Приклади діаграм направленості, розрахованих за виразом (2) для різних значень радіуса решітки ρ та кута орієнтації φ_0, наведено на рис. 2, 3.

Результати розрахунків КСД для різних значень *N* та ρ зведено у таблиці 1 для $\varphi_0 = 0$ та у таблиці 2 для $\varphi_0 = \pi/4$.

Результати розрахунків для інших значень φ_0 приблизно такі ж самі. При цьому ширина діаграми спрямованості, незалежно від кількості елементів *N*, змінюється від приблизно 85° для $\rho = 0{,}25\lambda$ до близько 15°–20° для $\rho = \lambda$ і менше 10° для $\rho = 1{,}5\lambda$.

Аналіз графіків, наведених на рис. 2 і 3, таблиці 1 та виразів (1) і (2), дозволяє зробити наступні висновки:

АР з круговим розташуванням випромінюючих елементів забезпечують однакову ширину ДС по усіх напрямах в азимутальній площині;

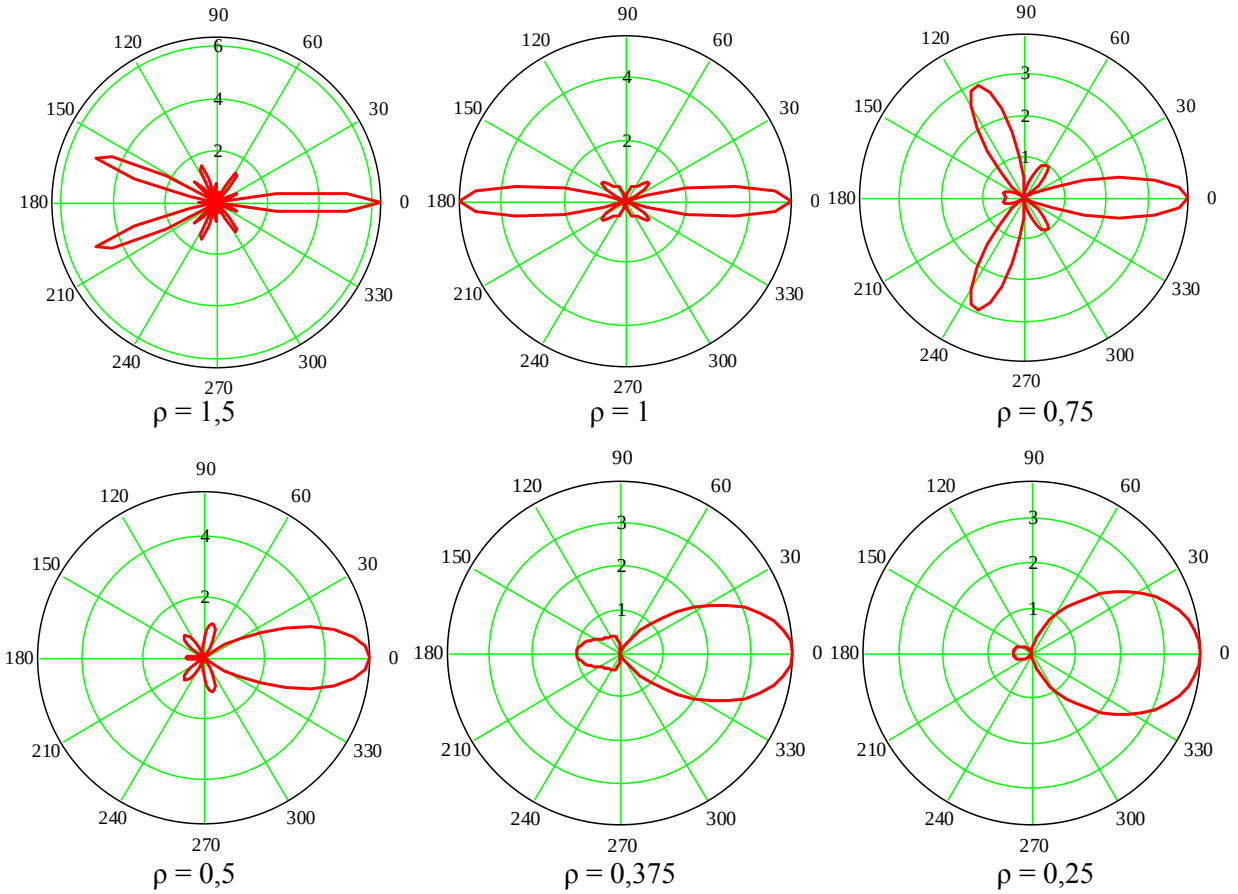


Рис. 2. Вигляд ДН КАР з $N = 6$, $\varphi = 0$

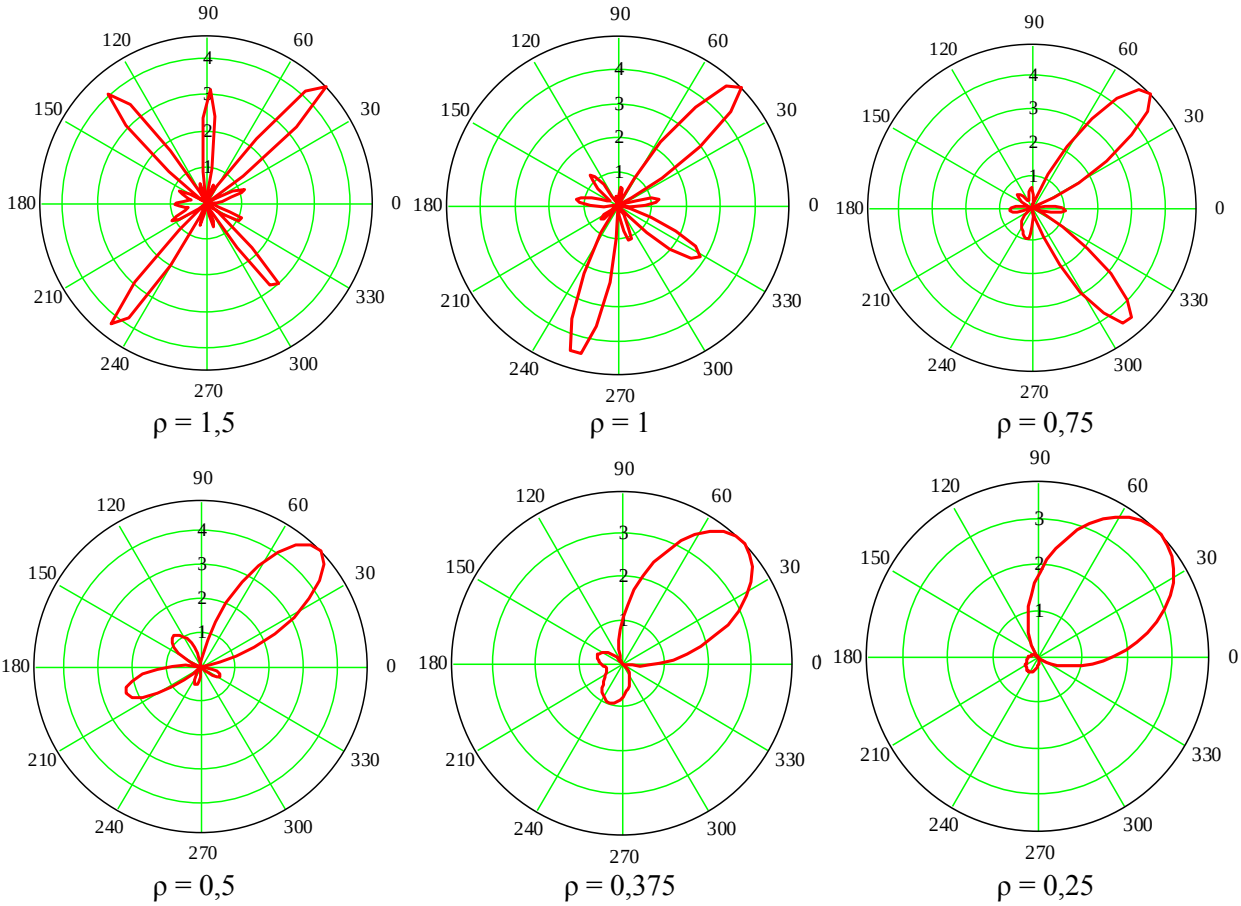


Рис. 3. Вигляд ДН КАР з $N = 6$, $\varphi = \pi/4$

Таблиця 1

N	ρ							
	0,25λ	0,375λ	0,5λ	0,675λ	0,75λ	λ	1,25λ	1,5λ
3	2,88	2,46	3,06	1,91	2,48	2,66	2,24	3,45
4	4	2,93	2,12	4,58	4	3,87	4	5,78
6	3,78	4,45	5,4	3,14	3,94	5,27	5,03	6,33
8	3,79	4,46	6,19	6,44	5,28	7,31	7,69	7,4
10	3,79	4,46	6,31	7,56	8,01	5,4	11,09	11,23
12	3,79	4,46	6,31	7,79	8,58	8,78	6,41	12,02

Таблиця 2

N	ρ							
	0,25λ	0,375λ	0,5λ	0,675λ	0,75λ	λ	1,25λ	1,5λ
3	2,87	2,3	3	2,6	2,91	2,59	3,53	2,67
4	3,27	3,18	5,7	2,98	2,9	4,67	4,9	2,7
6	3,8	4,36	4,86	4,16	4,93	4,97	6,1	4,65
8	3,8	4,46	6,19	6,44	5,28	7,31	7,67	7,4
10	3,8	4,46	6,31	7,6	7,85	6,13	8,14	9,3
12	3,8	4,46	6,31	7,8	8,63	7,97	9,8	7,05

зі збільшенням числа випромінюючих елементів N значення КСД $D(\varphi_0,\varphi)$ в напрямі максимуму ДН φ_0 збільшується (при величині радіуса решітки від 0,5λ і більше), а ширина ДС на рівні половинної потужності $2\Delta\varphi^{\circ}_{0,5}$ зменшується;

зі збільшенням радіуса КАР зменшується ширина головного пелюстка ДН і збільшується, відповідно, значення КНД, але при цьому зростає і рівень бічних пелюстків, що може призводити до збільшення рівня внутрішньосистемних завад.

В робочому діапазоні частот військових УКХ-радіозасобів забезпечення великих значень ρ можливе при роботі в області достатньо великих значень робочої частоти (300 МГц і більше).

Використання адаптивних АР дозволяє в умовах впливу навмисних завад здійснювати їх просторову фільтрацію за рахунок орієнтації провалів ДН у напрямку на їх джерело. При цьому, якщо ширина головного пелюстка ДН занадто мала, може виникнути ситуація, коли радіостанція не зможе забезпечити достатній рівень сигналу для зв'язку з жодним з кореспондентів мережі при необхідному рівні ослаблення завади. Чим більша ширина головного пелюстка ДН, тим вища ймовірність успішної передачі інформації в умовах навмисних завад. Таким чином, оптимальне значення ширини ДН антени, а отже і параметра ρ, залежить від кількості радіостанцій у мережі та їх розташуванні на місцевості. Проведені розрахунки показують можливість роботи в області ρ = 0,25λ…0,675λ при N = 6, ρ = 0,25λ…1,0λ при N = 12.

Для забезпечення максимальної ефективності передачі інформації в умовах навмисних завад необхідно вирішити ряд завдань:

1) визначення кожною радіостанцією власних координат;
2) визначення координат постановника завад;
3) обмін координатною інформацією між радіостанціями мережі;
4) визначення такого кута орієнтації максимуму ДН на кожну з сусідніх радіостанцій, при якому значення ВСЗШ буде максимальним під час отримання інформації від цієї радіостанції;
5) урахування ВСЗШ на кожного з сусідніх кореспондентів при реалізації протоколу маршрутизації у радіомережі;
6) розробка чітких правил обміну та оновлення координатної інформації та даних щодо очікуваної сигнально-завадової обстановки при відповідній орієнтації приймальної антени.

Розглянемо особливості практичної реалізації цих завдань.

Визначення власних координат та координат сусідніх радіостанцій. При використанні направлених антен для забезпечення максимального підсилення на передавальному та приймальному боці радіолінії кореспонденти повинні знати кутове розташування один одного.

Існують два основні методи позиціонування:

перший заснований на використанні геоінформаційних даних систем супутникового позиціонування;

другий полягає у визначенні напрямку на джерело сигналу на основі процедур математичної обробки комплексного вектору просторово-часових відліків сигналу на виходах аналого-цифрового перетворювача адаптивної АР.

Сучасні радіостанції мають вбудований GPS-приймач та можуть періодично повідомляти сусідам власні координати шляхом розсилки GPS-звітів. Під сусідніми будемо розуміти радіостанції, з якими забезпечується радіовидимість.

Водночас, доцільно періодично перевіряти коректність отриманих даних за допомогою другого методу, оскільки засоби РЕБ противника можуть подавлювати канали прийому сигналів геопозиціонування, що призведе до спотворення оцінки координат.

Механізм розсилки інформації про власне місцезнаходження потребує окремої розробки.

Визначення координат постановника завад. До складу системи управління кожної радіостанції (системи управління радіомережею) повинна входити підсистема завадозахисту [17], яка вирішує завдання збору інформації про систему радіоелектронного подавлення (РЕП) противника, ідентифікації поточної стратегії системи РЕП та управління засобами завадозахисту з метою забезпечення заданих показників функціонування в умовах активної радіоелектронної протидії.

Наявність у радіозасобах кругових АР дозволяє використовувати їх, за необхідності, як пеленгатор для визначення просторового напрямку на джерело радіовипромінювання (ДРВ) [18]. Крім цього, для підвищення точності визначення координат ДРВ можуть бути використані декілька радіостанцій (метод тріангуляції). Отримувати дані про координати засобів РЕП противника та їх характеристики можна і від власної системи радіоелектронної розвідки у єдиному інформаційному середовищі поля бою, створюваному програмно-апаратними засобами автоматизованого управління військами.

Таким чином, вважатимемо, що підсистема завадозахисту радіостанції (радіомережі) визначає інформацію про координати постановника (постановників) завад (ПЗ) та їх зміни, ідентифікує тип завади та визначає її очікуваний рівень на вході приймача радіостанції.

Визначення кута орієнтації максимуму ДН на сусідні радіостанції. Нехай на антену радіостанції № 2 (РС 2) приходить корисний сигнал від радіостанції № 1 (РС 1) та сигнал від постановника завад (рис. 4). Очевидно, що існує таке значення кута основного випромінювання приймальної антени φ_0, при якому відношення рівня корисного сигналу до рівня завади буде максимальним, і воно, як правило, не відповідає чіткій орієнтації основного пелюстка на кореспондента – замість $\varphi_0 = \varphi_{12}$ отримаємо $\varphi_0 = \varphi'_{12}$.

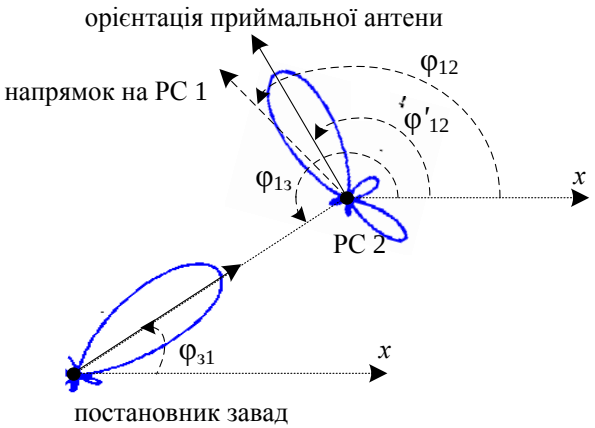


Рис. 4. Подавлення завад за рахунок просторової фільтрації у приймальній антені

Якщо рівні корисних сигналів сусідніх радіостанцій та рівень завади оцінюються та відомі на вході приймача кожної радіостанції МР, то відношення сигнал/(шум + завада) (ВСЗШ) на вході радіостанції *i* у напрямку на радіостанцію *j* визначається як різниця рівнів сигналу та завади:

$$SINR_{ij}(\varphi_{0ij}) = P_{cij} - P_{зi}. \quad (3)$$

Як видно з рис. 4 за рахунок повороту кута φ_0 у межах спрямування основного пелюстка на кореспондента можна досягнути достатньо високого ослаблення завади при незначному ослабленні корисного сигналу.

Оптимальним кутом орієнтації ДН КАР φ_{0ij} буде кут, при якому забезпечується максимальнеВСШЗ.

Оскільки форма ДН КАР змінюється залежно від напрямку основного випромінювання φ_0, орієнтацію антени у поточний момент часу необхідно враховувати при проведенні розрахунків ДН. Іншим варіантом може бути реалізація системи автоматичного підстроювання антени, завданням якої є забезпечення однакового розташування випромінюючих елементів відносно початку координат (наприклад, напрямок прямої, яка з'єднує центр решітки з випромінюючим елементом № 1 завжди відповідає $\varphi_0 = 0^o$ у прийнятій полярній системі координат).

Урахування очікуваного ВСЗШ для кожного з сусідніх кореспондентів при реалізації протоколу маршрутизації у радіомережі.

Для МР з КАР, враховуючи необхідність забезпечити знання кожним вузлом мережі координат (або просторового напрямку) сусідніх вузлів, найбільш перспективним є застосування методів координатної маршрутизації [3], основною перевагою яких порівняно з методами, що не використовують координатну інформацію, є значне зменшення обсягу службового трафіку.

При розробці методу КМ для МР з КАР необхідно вирішити наступні завдання: збір інформації про стан мережі, зберігання маршрутів, обчислення маршруту передачі пакету (визначення правил вибору одного чи декількох вузлів-ретрансляторів).

Реалізація збору інформації про стан мережі можлива хвильовим, зондовим або проактивним способами, а також гібридним, який передбачає, що кожен вузол мережі збирає інформацію про координати сусідніх вузлів на глибину маршрутної зони $R_{мз}$ проактивно, а за її межами – зондовим способом [19]. Вибір конкретного способу може залежати від розмірності мережі, вимог до величини затримок при побудові маршруту тощо.

Зберігання маршрутів при координатній маршрутизації передбачає підтримання кожним вузлом таблиці місцезнаходження сусідніх вузлів наступного формату: ідентифікатор адресата *j*, його координати $(x, y, z)_j$, швидкість v_j, напрямок переміщення γ_j, час оновлення даної інформації t_j. Крім цього, необхідно обрати спосіб зберігання інформації про місцеположення – автономний (кожен вузол ініціює процес збору інформації про стан мережі та зберігає у своїй маршрутній таблиці) або розподілений (передбачає призначення деяких вузлів домашніми агентами, які відповідають за зберігання інформації про місцезнаходження тих чи інших вузлів).

Вибір ретранслятора полягає у визначенні напрямку пошуку адресата та визначенні розмірів зони його передбачуваного знаходження. Обчислення маршруту може бути реалізовано декількома способами [3]: випадково з обмеженням вибору за певними правилами (наприклад, у прямокутній області певного розміру) або фіксований вибір ретрансляторів. У роботі [20] проведено порівняння декількох варіантів реалізації протоколу LAR (Location Aided Routing) для МР з направленими антенами за формою зони запиту: прямокутна зі змінними розмірами, у формі краплі, трикутна, еліпсоїдальна. Для прийнятої топології мережі встановлено, що при низькій щільності розташування вузлів на місцевості усі варіанти приблизно однакові за ефективністю (кількістю необхідної службової інформації для функціонування протоколу), водночас, при збільшенні щільності вузлів найменшої кількості службових заголовків потребує спосіб із зоною запиту у формі краплі.

Застосування КАР потребує також урахування даних про систему РЕП противника, прогнозування змін сигнальної та завадової обстановки з урахуванням даних про переміщення вузлів мережі один відносно одного та постановників завад.

При зміні координат на деяку величину ΔX j-го вузла (або постановника завад відносно нього) рівень сигналу i-го вузла ($i = 1,\ldots, n$, де n – кількість вузлів у зоні радіовидимості вузла j) на вході приймача j-го вузла P_{ij} при взаємній орієнтації антен одна на одну зміниться незначно, разом з тим, оскільки форма ДН КАР (інтенсивність та напрямки бічних та заднього пелюстків) суттєво залежить від напрямку основного випромінювання, рівень завади $P_{зj}$ на вході приймача може суттєво зрости порівняно з попереднім положенням. Відповідно, ВСШЗ на вході приймача j-го вузла стане значно меншим. Враховуючи те, що сусідніх вузлів у j-го вузла може бути декілька, розрахунок очікуваного ВСШЗ$_{ij}$ після зміни координат на ΔX доцільно здійснювати сусіднім вузлам, для чого вони повинні знати його оновлені координати (або просторовий напрямок) та рівень завади на вході приймача у точці X_j.

Таким чином, після оновлення даних в таблиці місцезнаходження сусідніх вузлів (табл. 3), кожен вузол, який є сусідом j-го вузла, здійснює розрахунок максимально можливого $SINR_{ij}$, яке можна забезпечити шляхом керування направленістю випромінювання КАР (вираз (3)).

Таблиця 3

Таблиця сусідніх вузлів для *i*-го вузла

Номер вузла	**1**	**2**	**3**	***i***	***n***
Параметри вузла	$(x, y, z)_1$	$(x, y, z)_2$	$(x, y, z)_3$	$(x, y, z)_j$	$(x, y, z)_n$
	v_{j1}	v_{j2}	v_{j3}	v_{ji}	v_{jn}
	γ_{j1}	γ_{j2}	γ_{j3}	γ_{ji}	γ_{jn}
	t_{j1}	t_{j2}	t_{j3}	t_{ji}	t_{jn}
	ВСШЗ$_{j1}$	ВСШЗ$_{j2}$	ВСШЗ$_{j3}$	ВСШЗ$_{ji}$	ВСШЗ$_{jn}$

Чим більше придатних для ведення зв'язку сусідніх вузлів має радіостанція, тим краще, оскільки забезпечується більша кількість альтернативних маршрутів передачі інформації з заданою пропускною спроможністю.

Оскільки в процесі побудови маршруту можуть брати участь і радіостанції, оснащені тільки всенаправленими антенами (портативні та ранцеві), при зміні власних координат або координат постановника завад, або появі нового ПЗ, вони також здійснюють усі необхідні розрахунки стосовно сусідніх радіостанцій.

Після розрахунку оновленого очікуваного значення ВСШЗ у напрямку на i-ту станцію кожна радіостанція розсилає службовим каналом уточнені дані.

Розглянемо за приклад фрагмент МР (рис. 5), що містить 9 радіостанцій (вузлів), оснащених круговими АР. Нехай радіостанція № 1 повинна передати дані для радіостанції № 9. На приймачі радіозасобів впливає постановник навмисних завад. Кожен вузол володіє інформацією про власні координати, а також координати сусідніх вузлів та постановника завад і, таким чином, визначає, які з вузлів можуть приймати від нього інформацію із задовільною якістю, а які – ні.

На рис. 5 стрілки, зображені суцільною лінією, відповідають задовільним ділянкам мережі, де у відповідному напрямку можлива передача інформації із заданою якістю (забезпечується мінімально необхідне ВСШЗ). Стрілки, виконані пунктирними лініями, показують, що в даний час відповідні ділянки будуть непридатними при впливі навмисних завад, створюваних постановником, ідентифікованим підсистемою завадозахисту.

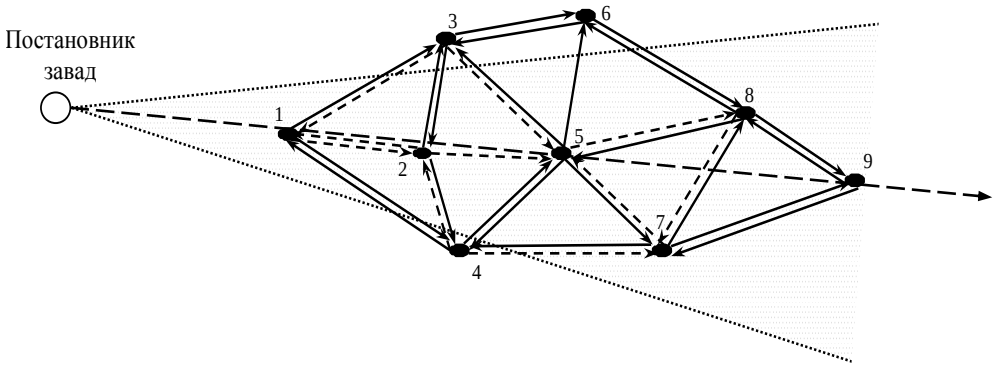


Рис. 5. Приклади побудови можливих маршрутів передачі між вузлами 1 та 9

З рис. 5 видно, що придатними маршрутами для передачі у напрямку 1 – 9 є „1 – 3 – 6 – 8 – 9”, „1 – 4 – 5 – 7 – 9” та „1 – 4 – 5 – 7 – 8 – 9”. Якщо метрикою при побудові маршруту є мінімальна затримка (мінімальна кількість ретрансляцій) при забезпеченні мінімально необхідної швидкості передачі даних, то кращими є перші два маршрути, з яких буде обрано той, який забезпечить вищу пропускну спроможність. Також очевидно, що маршрути для зворотного інформаційного напрямку будуть відрізнятися. Придатні маршрути у зворотному напрямку: „9 – 8 – 6 – 3 – 2 – 4 – 1”, „9 – 8 – 5 – 3 – 2 – 4 – 1” та „9 – 7 – 4 – 1”.

Розробка чітких правил оновлення інформації про місцеположення радіостанцій МР та ПЗ. Механізм розсилки інформації про власне місцезнаходження, обміну даними щодо координат постановників завад та очікуваних значень ВСШЗ між сусідніми радіостанціями тощо потребує окремої розробки. Його можна реалізувати наступними способами:

з використанням ненаправлених антен на передачу та прийом у визначені моменти часу;

почерговою передачею радіостанцією з направленою антеною у напрямку на окремих кореспондентів (груп кореспондентів) з ненаправленими антенами;

шляхом чіткого орієнтування антен кореспондентів одна на одну (за останніми даними).

Останній спосіб повинен передбачити досить частий обмін GPS-звітами з урахуванням швидкості взаємного переміщення сусідніх радіостанцій. Крім цього, він потребує резервування значної частини загальної пропускної спроможності каналу для почергової передачі однієї й тієї ж інформації усім сусіднім радіостанціям.

Окремої уваги потребує визначення періодичності, з якою необхідно оновлювати вказану службову інформацію. Якщо радіостанції нерухомі відносно одна одної та відносно ПЗ, потреби у оновленні цієї інформації немає, якщо ж хоча б один із вказаних РЕЗ рухається, необхідно достатньо часто здійснювати оновлення розрахунків.

Оскільки від забезпечення коректного обміну службовою інформацією залежить ефективність і можливість функціонування МР з адаптивним діаграмоутворенням, для забезпечення високої завадозахищеності службового каналу доцільно застосувати низькошвидкісні коригувальні коди, здатні забезпечити прийом інформації в умовах низьких відношень сигнал/шум, а також технологію розширення спектра.

Висновки. Таким чином, основними завданнями, які пов’язані з ефективним впровадженням адаптивних АР у мережі MANET, є наступні:

визначення кутових координат джерел радіовипромінювань (кореспондентів та джерел завад);

адаптивне управління формуванням діаграми направленості АР;

постійний контроль сигнально-завадової обстановки у напрямках на кореспондентів мережі;

удосконалення протоколів маршрутизації передачі повідомлень з урахуванням поточної сигнально-завадової обстановки;

розробка ефективного протоколу обміну службовою інформацією (який має здійснюватися із оптимальною періодичністю), що стосується координат радіостанцій та

постановників завад, а також сигнально-завадової обстановки (очікуваних значень відношення сигнал/завада, які будуть забезпечені при оптимальній орієнтації антени приймальної станції).

Напрямком подальших досліджень є розробка удосконаленого методу координатної маршрутизації для реалізації в перспективних мобільних радіомережах тактичної ланки управління з використанням АР в умовах впливу навмисних завад.

ЛІТЕРАТУРА

1. Романюк В. А. Напрямки підвищення ефективності функціонування тактичних мобільних радіомереж // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: доповіді та тези доповідей виступів учасників VII науково-практичного семінару, м. Київ, 24 жовтня 2013 р. Київ.: ВІТІ ДУТ, 2013. С. 40–56.

2. Кувшинов О. В., Гурський Т. Г., Гриценок К. М., Шишацький А. В. Аналіз режимів роботи та перспектив бойового застосування військових УКХ радіостанцій іноземного виробництва // Збірник наукових праць ВІТІ. 2018. Вип. 1. С. 43–50.

3. Бунин С. Г., Войтер А. П., Ильченко М. Е., Романюк В. А. Самоорганизующиеся радиосети со сверхширокополосными сигналами. Київ: НПП „Издательство „Наукова думка" НАН Украины", 2012. 444 с.: ил.

4. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. Санкт-Петербург: Самиздат, 2013. 166 с.

5. Борисов В. И. Помехозащищенность систем радиосвязи: основы теории и принципы реализации. Москва: Наука, 2009. 358 с.

6. Борисов В. И., Зинчук В. М., Лимарев А. Е. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей певдослучайной последовательностью. Москва: Радио и связь, 2003. 640 с.

7. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва: Радио и связь, 1985. 384 с.

8. Борисов І. В., Гурський Т. Г., Ільїнов М. Д., Гриценок К. М. Підвищення ефективності функціонування систем радіозв'язку за рахунок використання адаптивних антенних решіток // Збірник наукових праць ВІТІ. 2015. Вип. 1. С. 16–24.

9. Уидроу Б. Адаптивная обработка сигналов / Б. Уидроу, С. Стирнз; пер. с англ. под ред. В. В. Шахгильдяна. Москва: Радио и связь, 1989. 440 с.

10. Золотарев В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: справочник. Москва: Горячая линия – Телеком, 2004. 126 с.: ил.

11. Банкет В. Л. Сигнально-кодовые конструкции в телекоммуникационных системах. Одесса: Фенікс. 2009. 180 с.

12. Ерохин Г. А., Чернов О. В., Козырев Н. Д., Кочержевский В. Д. Антенно-фидерные устройства и распространение радиоволн. Москва: Горячая линия – Телеком. 2007. 531 с.

13. M. Tarique. Selection of optimal beamforming algorithm for mobile Ad Hoc networks // Wireless Engineering and Technology. 2017. № 8. Pp. 20–36.

14. Adaptive beamforming algorithms for anti-jamming / [Rana Liaqat Ali, Anum Ali, Anisur-Rehman and. oth.] // International Journal of Signal Processing, Image Processing and Pattern Recognition. 2011. Vol. 4. № 1. Pp. 95–105.

15. Performance of adaptive beam nulling in multihop ad-hoc networks under jamming / [S. Bhunia, V. Behzadan, P. A. Regis, S. Sengupta] // High Performance Computing and Communications (HPCC). 2015. IEEE 17th International Conference. Pp. 1236–1241.

16. Гриценок К. М., Гурський Т. Г. Методика формування діаграми спрямованості кільцевої антенної решітки радіостанції мобільної радіомережі в умовах навмисних завад // Збірник наукових праць ВІТІ. 2018. Вип. № 3. С. 6–16.

17. Кувшинов О. В. Адаптивне управління засобами завадозахисту військових систем радіозв'язку // Збірник наукових праць ВІКНУ. 2009. Вип. 17. С. 125–130.

18. Москалец Н. В. Сравнительный анализ методов оценки направления прихода сигналов // Радиотехника. 2017. Вып. 188. С. 126–135.

19. Миночкин А. И., Романюк В. А. Маршрутизация в мобильных радиосетях – проблема и пути ее решения // Зв'язок. 2006. № 3. С. 42–50.

20. Ramanathan R. A Radically New Architecture for Next Generation Mobile Ad Hoc Networks // In IEEE Proceeding Mobicom, 2005. Pp. 132–139.

УДК 621.3
д-р техн. наук Кузавков В. В. ORCID: 0000-0002-0655-9759 (ВІТІ)
Михайлюк С. С. (ВІТІ)
Погребняк С. В. ORCID: 0000-0002-9104-7781 (ВІТІ)

АНАЛІЗ ПАРАМЕТРІВ НАДІЙНОСТІ ОБ'ЄКТІВ РАДІОЕЛЕКТРОННОЇ ТЕХНІКИ З НАДЛИШКОВІСТЮ

До складу складних технічних систем належить ефективність функціонування радіоелектронної техніки, яка залежить від надійності їх підсистем та елементів.

У статті показано, що надмірність, яка широко застосовується для забезпечення нормального функціонування складних систем у реальних умовах експлуатації, є фундаментальним поняттям у загальній теорії й практиці надійності. Наведено класифікацію і дана характеристика основних методів резервування як способу підвищення надійності, відзначено їхні достоїнства й недоліки та зроблено висновок про доцільність комплексного використання різних видів надмірності.

Ключові слова: *надійність, об'єкти радіоелектронної техніки, надмірність, резервування.*

V. Kuzavkov, S. Mykhailiuk, S. Pogrebnyak. Analysis of reliability parameters of radio electronic equipment facilities with redundancy

The composition of complex technical systems includes the effectiveness of the functioning of electronic equipment, which depends on the reliability of their subsystems and elements.

The article defines the basic concepts of reliability theory. It is shown that redundancy, which is widely used to ensure the normal functioning of complex systems in real operating conditions, is a fundamental concept in the general theory and practice of reliability. The classification and characteristics of the main redundancy methods are given as a way of increasing reliability, their merits and demerits are noted, and a conclusion is drawn about the expediency of the comprehensive use of various types of redundancy.

Keywords: *reliability, objects of radio-electronic equipment, redundancy, redundancy.*

Постановка завдання

Розглянуто особливості елементної та структурної надійності об'єктів радіоелектронної техніки.

Аналіз останніх публікацій

У спеціальній науковій літературі розглядаються загальні підходи до системотехнічного проєктування телекомунікаційних мереж [1], а також їх математичні моделі і методи аналізу надійності [2–5]. Відповідно до загальної практики, оцінка кількісних значень показників надійності об'єктів радіоелектронної техніки проводиться як на етапах проєктування, так і під час її експлуатації.

Сучасні об'єкти радіоелектронної техніки відносяться до великих систем. Прикладами складних систем можуть служити: телекомунікаційні мережі; радіолокаційні системи; різні види автоматизованих систем, призначених для вдосконалення організації та управління процесами обробки інформаційних потоків (автоматизовані системи управління процесами тощо).

Питання особливостей побудови та аналізу поведінки великих систем розглядаються в [4], а підходи та приклади практичної реалізації методик кількісної оцінки показників надійності об'єктів радіоелектронної техніки розглядаються в [6–8]. Зокрема, в [9; 10] наводяться способи підвищення якості функціонування складних систем, а питання кількісної оцінки структурної надійності об'єктів радіоелектронної техніки досліджені в [10; 11].

Метою статті є аналіз параметрів надійності для об'єктів радіоелектронної техніки з надлишковістю при повній вихідній інформації.

Виклад основного матеріалу

Найбільш повною характеристикою будь-якої складної технічної системи є її якість – сукупність властивостей, які обумовлюють її придатність задовольняти певні потреби відповідно до свого призначення протягом установленого часу. Цю сукупність властивостей можна умовно розбити на дві групи характеристик:

ті, які визначають можливості системи виконувати певні функції відповідно до свого призначення за умови, та які визначають здатність системи зберігати свої можливості в заданих межах за певних умов експлуатації, а також почасові, матеріальні й трудові витрати на підтримку системи в працездатному стані;

експлуатаційно-технічні характеристики. До їхнього числа відносять показники надійності систем, характеристики контролю працездатності, обслуговування та ремонту, повноти й достатності запасного майна і приладів та інші характеристики.

Із визначення й складу експлуатаційно-технічних характеристик можна зробити наступні висновки, що забезпечення високих експлуатаційно-технічних характеристик апаратури є не самоціллю, а засобом забезпечення високої надійності, тобто високої ефективності систем.

Існуюча залежність між надійністю та іншими експлуатаційно-технічними властивостями системи є основою комплексного підходу до розрахунку й забезпечення основних експлуатаційно-технічних характеристик, який полягає в одночасному і взаємозалежному їхньому дослідженні на всіх етапах розробки, випробувань і експлуатації нових систем.

У загальному випадку надійність – це комплексна властивість, яка залежить не тільки від показників апаратурної надійності, але визначається також характером навантаження на систему й цілим рядом організаційно-технічних заходів і факторів, які впливають на загальний процес функціонування системи: режимами технічного обслуговування, якістю контролю, структурою й організацією системи ремонту тощо.

Урахування всіх цих факторів при розрахунках показників надійності дозволяє не тільки більш повно враховувати реальні можливості систем, а також більш обґрунтовано обирати шляхи та методи забезпечення їхнього нормального функціонування в процесі тривалої експлуатації.

У теорії надійності використовуються наступні поняття стану об'єкту контролю: працездатний, непрацездатний.

Працездатний стан (працездатність) – стан об'єкта, який характеризується його здатністю виконувати усі потрібні функції.

Непрацездатний стан (непрацездатність) – стан об'єкта, за яким він нездатний виконувати хоч би одну з потрібних функцій.

Основною подією, яка пов'язана зі зміною стану об'єкта, є відмова. Поняття відмови є фундаментальним у теорії й практиці надійності. З її визначення повинне починатися будь-яке дослідження надійності технічних систем. Критерій відмови – ознака чи сукупність ознак порушення працездатного стану об'єкта, встановлені у нормативній та (або) конструкторській (проєктній) документації.

У поняття складної системи зазвичай вкладають наступний зміст:

складну систему можна розчленувати на кінцеве число підсистем, а кожну підсистему, у свою чергу, – на кінцеве число більш простих підсистем тощо, доти, поки не одержимо елементи системи (під елементами системи розуміють об'єкти, які в умовах даної задачі не підлягають розчленовуванню на частини);

елементи складної системи функціонують у взаємодії один з одним;

властивості складної системи визначаються не тільки властивостями окремих елементів, але й характером взаємодії між елементами.

Таким чином, відмінними рисами складної системи є наявність великої кількості взаємозалежних і певним чином взаємодіючих між собою різнорідних елементів.

Забезпечення надійності складних технічних систем являє собою єдиний процес, що охоплює всі основні етапи їхнього життєвого циклу. Отже, забезпечення високої надійності складних технічних систем – це комплексна проблема, що охоплює широке коло наукових (математичних, фізико-технічних, біологічних), інженерних (проєктно-конструкторських, експлуатаційних) й економічних аспектів. Рішення цієї проблеми пов'язане з реалізацією численних організаційних і технічних, а часто і фундаментальних наукових досліджень, що вимагають великих витрат часу та коштів і дотичних різних галузей науки, техніки та народного господарства.

Як відомо з [12–15], при досягнутих рівнях надійності комплектуючих елементів й якості проєктно-конструкторських і виробничо-технологічних робіт основним шляхом забезпечення надійності складних систем є введення різних видів надмірності. Тому поняття надмірності є фундаментальним у загальній теорії надійності.

Під надмірністю розуміють сукупність додаткових засобів і (або) можливостей, які використовуються для забезпечення нормального функціонування складних систем в умовах впливу дестабілізуючих внутрішніх і зовнішніх факторів. У цей час розрізняють і використовують для забезпечення надійності п'ять видів надмірності: структурну, інформаційну, функціональну, навантажувальну й почасову.

Резервування – спосіб забезпечення надійності об'єкта за рахунок використання надмірності.

Резерв – сукупність додаткових засобів і (або) можливостей, використовуваних для резервування.

Серед існуючих методів резервування вже діючих систем особливу увагу приділяємо функціональному та навантажувальному резервуванню, при якому використовується здатність елементів об'єкта виконувати додаткові функції (при функціональному резервуванні) або сприймати додаткові навантаження понад номінальні (при навантажувальному резервуванні).

Ці види резервування звичайно утворяться в складних просторово-рознесених системах за рахунок структурного й функціонального ускладнення апаратури і зв'язку між її елементами, а також шляхом раціональної організації застосування систем. Труднощі практичного використання даних видів надмірності пов'язані з необхідністю в ряді випадків додаткового перетворення форми інформації, погіршенням її точності й вірогідності, зниженням пропускної здатності тощо.

Кожен з видів резервування окремо має певні достоїнства й недоліки, які необхідно враховувати при виборі й обґрунтуванні методів підвищення надійності. Разом з тим, дослідження показали [12–15], що ефективність введення надмірності, як методу підвищення надійності, може бути істотно підвищена при комплексному використанні різних її видів. Об'єктивна можливість і необхідність такого підходу обумовлена наступними причинами:

у багатьох технічних об'єктах реально існують різні види надмірності, передбачені при проєктуванні, які володіють не тільки частковими, але й загальними властивостями відносно впливу на надійність. Тому вивчення надмірності, її видів, способів введення й використання, її ролі й місця в загальній програмі забезпечення надійності повинне проводитися комплексно з єдиних методологічних позицій;

у багатьох випадках один вид надмірності (наприклад, структурна, інформаційна, функціональна або навантажувальна) може служити засобом, що забезпечує наявність у системі іншого виду надмірності (наприклад, почасової);

спільне використання різних видів надмірності дає можливість частково компенсувати недоліки, які властиві окремим видам, і підсилити їхні достоїнства. При цьому виграш у надійності не є мультиплікативною функцією виграшів, що досягаються в системі з одним видом надмірності, а істотно більшою.

Для того щоб властивості надійності можна було «вимірювати» (оцінювати), введено кількісні показники надійності – кількісні характеристики одного або декількох властивостей, які визначають надійність. Розрізняють одиничні показники надійності, які характеризують одну із властивостей, і комплексні показники, які характеризують кілька властивостей, що визначають надійність об'єкта.

Для кількісної оцінки безвідмовності використовуються одиничні показники, основні з яких приводяться нижче.

Імовірність безвідмовної роботи $P(t)$ – це імовірність того, що в межах заданого напрацювання t відмова об'єкта не виникне, тобто:

$$P(t) = Імов\{t_н \geq t\},\ t \geq 0,$$

де $t_н$ – випадкова величина, що характеризує напрацювання до відмови.

Імовірність протилежної події є *імовірність відмови*

$$F(t) = Імов\{t_н < t\}.$$

Очевидно, що $P(t) + F(t) = 1,$

де $F(t)$ – інтегральна функція розподілу випадкової величини $t_н$.

Щільність розподілу напрацювання до відмови $f(t)$ можна одержати як похідну від функції розподілу $F(t)$:

$$f(t)=\frac{dF(t)}{dt}=-\frac{dP(t)}{dt},$$

звідки знаходимо:

$$F(t)=\int_0^t f(u)du,\quad P(t)=\int_t^\infty f(u)du\,.$$

Інтенсивність відмов $\lambda(t)$ – це умовна щільність імовірності виникнення відмови невідновлюваного об'єкта, обумовлена за умови, що до розглянутого моменту часу t відмова не виникла.

Відповідно до визначення:

$$\lambda(t)=\frac{f(t)}{P(t)}=\frac{1}{1-F(t)}\frac{dF(t)}{dt}=-\frac{1}{P(t)}\frac{dP(t)}{dt}.$$

Середнє напрацювання до відмови – це математичне сподівання напрацювання об'єкта до першої відмови:

$$T_0=\int_0^\infty tf(t)\,dt\,. \tag{1}$$

Провівши інтегрування в (1) по частинах, отримаємо:

$$T_0=\int_0^\infty P(t)\,dt=\int_0^\infty (1-F(t))\,dt\,.$$

Середнє напрацювання на відмову $T_н$ – це відношення сумарного напрацювання відновлюваного об'єкта до математичного сподівання числа його відмов протягом цього напрацювання, тобто:

$$T_н=\frac{1}{n}\sum_{i=1}^{n}t_{нi}\,,$$

де $t_{нi}$ – напрацювання об'єкта між $(i-1)$ і i-ю відмовами;

n – математичне сподівання числа відмов протягом сумарного напрацювання.

Властивість ремонтопридатності об'єктів прийнято «вимірювати» часом приведення об'єкта в працездатний стан – часом відновлення $t_в$, що є випадковою величиною. Тому показники ремонтопридатності використовують такі ж імовірнісні характеристики, як і у випадку безвідмовності, а саме: $F_в(t)$ – імовірність відновлення у заданий час; $f_в(t)$ – щільність розподілу часу відновлення; $\mu(t)$ – інтенсивність відновлення; $T_в$ – середній час відновлення.

Імовірність відновлення в заданий час $F_в(t)$ – це імовірність того, що час відновлення працездатного стану об'єкта не перевищить задане значення:

$$F_в(t)=Імов\{t_в\le t\}.$$

Так само як і $F(t)$, $F_в(t)$ – це функція розподілу випадкової величини $t_в$. Імовірність невідновлення в заданий час:

$$Імов\{t_в>t\}=1-F_в(t)\,.$$

За аналогією зі щільністю $f(t)$ щільність розподілу часу відновлення $F_в(t)$ виражається формулою:

$$f_в(t)=\frac{dF_в(t)}{dt}\,.$$

Інтенсивність відновлення $\mu(t)$ – це умовна щільність імовірності відновлення працездатності об'єкта, певна для розглянутого моменту часу за умови, що до цього моменту відновлення не було завершено. Відповідно до визначення:

$$\mu(t)=\frac{f_{\text{в}}(t)}{1-F_{\text{в}}(t)}.$$

Середній час відновлення $T_{\text{в}}$ – це математичне сподівання часу відновлення працездатного стану об'єкта після відмови, тобто:

$$T_{\text{в}}=\int_0^\infty t f_{\text{в}}(t)dt=\int_0^\infty [1-F_{\text{в}}(t)]\,dt.$$

Показники довговічності можна умовно розділити на дві групи. Показники першої групи основані на терміні служби, а показники другої – на понятті «ресурс». До цих показників відносять середній термін служби, гамма-процентний термін служби, середній ресурс і гамма-процентний ресурс.

Показниками збережуваності є середній термін зберігання й гамма-процентний термін зберігання. Визначення показників довговічності й збережуваності приводяться в ДСТУ 2860-94 [5].

Відзначимо, що всі розглянуті вище показники надійності є одиничними й дозволяють кількісно оцінювати тільки окремі властивості надійності. Крім них у цей час широко використовуються комплексні показники, що враховують дві властивості надійності – безвідмовність і ремонтопридатність. Такими комплексними показниками надійності є: нестаціонарний $K_{\text{г}}(t)$ і стаціонарний $K_{\text{г}}$ коефіцієнти готовності; $K_{\text{тв}}$ – коефіцієнт технічного використання; $K_{\text{ог}}(t)$ – коефіцієнт оперативної готовності.

Згідно з ДСТУ 2860-94 [5] нестаціонарний коефіцієнт готовності $K_{\text{г}}(t)$ залежить від часу. У сталому режимі функціонування об'єкта (при $t\to\infty$) ця залежність від часу зникає й ми приходимо до стаціонарного коефіцієнта готовності $K_{\text{г}}$.

Стаціонарний коефіцієнт готовності $K_{\text{г}}$ – це значення коефіцієнта готовності, визначене для умов роботи об'єкта, коли середній параметр потоку відмов і середній час відновлення залишаються постійними:

$$\lim_{t\to\infty}K_{\text{г}}(t)=K_{\text{г}}=\frac{T_{\text{н}}}{T_{\text{н}}+T_{\text{в}}}. \qquad (2)$$

Формула (2) добре відображає фізичну сутність коефіцієнта готовності як відносну частку часу, протягом якого об'єкт перебуває в працездатному стані.

У ряді випадків використовується такий показник як коефіцієнт простою $K_{\text{пр}}$, що характеризує відносну частку часу, протягом якого об'єкт перебуває в непрацездатному стані, тобто:

$$K_{\text{пр}}=1-K_{\text{г}}=\frac{T_{\text{в}}}{T_{\text{н}}+T_{\text{в}}}.$$

Коефіцієнт технічного використання $K_{\text{тв}}$ – це відношення математичного сподівання сумарного часу перебування об'єкта в працездатному стані $\text{M}[t_{\text{пр}\Sigma}]$ за деякий період експлуатації до математичного сподівання сумарного часу перебування об'єкта в працездатному стані $\text{M}[t_{\text{пр}\Sigma}]$ та у простоях, обумовлених технічним обслуговуванням $\text{M}[t_{\text{то}\Sigma}]$ і ремонтом $\text{M}[t_{\text{в}\Sigma}]$ за той же період:

$$K_{\text{тв}}=\frac{\text{M}[t_{\text{пр}\Sigma}]}{\text{M}[t_{\text{пр}\Sigma}]+\text{M}[t_{\text{то}\Sigma}]+\text{M}[t_{\text{в}\Sigma}]}.$$

Розглянуті вище комплексні показники $K_{\text{г}}$ і $K_{\text{тв}}$ є характеристиками надійності, усередненими для тривалого періоду експлуатації. У багатьох випадках цього виявляється недостатньо, тому що виникає необхідність оцінки можливості виконання об'єктом деякої

задачі (функції), що вимагає безперервної безвідмовної роботи об'єкта в ході заданого часу. Для оцінки такої можливості введено показник – коефіцієнт оперативної готовності.

Коефіцієнт оперативної готовності $K_{\text{ог}}(t, t+t_0)$ – це імовірність того, що об'єкт виявиться в працездатному стані в довільний момент часу t, крім планованих періодів, протягом яких застосування об'єкта за призначенням не передбачається, і, починаючи із цього моменту, буде виконувати необхідну функцію протягом заданого інтервалу часу $(t, t+t_0)$.

Для сталого режиму експлуатації (при $t \to \infty$) і довільних законах розподілу випадкових величин t_i і $t_{\text{в}}$ справедлива наступна формула для коефіцієнта оперативної готовності:

$$\lim_{t\to\infty} K_{\text{ог}}(t, t+t_0) = K_{\text{ог}}(t_0) = \frac{1}{T_{\text{н}} + T_{\text{в}}} \int_{t_0}^{\infty} [1 - F(t)]dt, \qquad (3)$$

де $F(t)$ – функція розподілу напрацювання об'єкта між відмовами.

При $F(t) = 1 - e^{-\lambda t}$ формула (3) приймає наступний вид:

$$K_{\text{ог}}(t_0) = K_{\text{г}} e^{-\lambda t_0} = \frac{T_{\text{н}}}{T_{\text{н}} + T_{\text{в}}} e^{-\frac{t_0}{T_0}}.$$

Висновки

У статті визначено основні одиничні і комплексні показники надійності, проведено розрахункові співвідношення. Серед існуючих методів підвищення показників надійності обрано метод функціонального та навантажувального резервування.

Напрямком подальшої роботи є підвищення живучості угруповання телекомунікаційних засобів та її підвищення шляхом використання всіх видів надлишковості.

ЛІТЕРАТУРА

1. Волочій Б. Ю. Системотехнічне проектування телекомунікеаційних мереж. Практикум: навч. посіб. / Б. Ю. Волочій, Л. Д. Озірковський. Львів: Видавництво Львівської політехніки, 2012. 128 с.

2. Бобало Ю. Я. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем. Монографія / Ю. Я. Бобало, Б. Ю. Волочій, О. Ю. Лозинський, Б. А. Мандзій, Л. Д. Озірковський, Д. В. Федасюк, С. В. Щербаковських, В. С. Яковина. Львів: Видавництво Львівської політехніки, 2013. 300 с.

3. ДСТУ В 3265-95. Зв'язок військовий. Терміни та визначення. Київ: Держстандарт України. 40 с.

4. Денисов А. А. Теория больших систем управления: учеб. пособ. / А. А. Денисов, Д. Н. Колесников. Ленинград: Энергоиздат. 288 с.

5. ДСТУ 2860-94 Надійність техніки. Терміни та визначення. Київ: Держстандарт України. 76 с.

6. Глазунов Л. П. Основы теории надежности автоматических систем управления: учеб. пособ. / Л. П. Глазунов, В. П. Грабовецкий, О. В. Щербаков. Ленинград: Энергоиздат. 208 с.

7. Маслов А. Я. Эксплуатация автоматизированных систем управления. Воениздат, 1984. 485 с.

8. Нетес В. А. Надежность сетей связи: тенденции последнего десятилетия // Электросвязь. 1998. № 1. С. 25–27.

9. Хиленко В. В. Проблеми розбудови і підвищення якості мережі спільноканальної сигналізації: структурна надійність мережі // Зв'язок. 2002. № 6. С. 21–25.

10. Рижаков В. А. Кількісне оцінювання структурної надійності систем зв'язку // Зв'язок. 2004. № 4. С. 53–57.

11. Харыбин А. В. О подходе к решению задачи выбора методологии оценки структурной надежности и живучести информационных систем критического применения // Радіоелектронні і комп'ютерні системи. 2006. № 6918. С. 61–71.

12. ДСТУ 2864-94. Надійність техніки. Експериментальне оцінювання та контроль надійності. Основні положення. Київ: Держстандарт України. 30 с.

13. ДСТУ 3004-95. Надійність техніки. Методи оцінки показників надійності за експериментальними даними. Київ: Держстандарт України. 123 с.

14. ДСТУ 3433-96. Надійність техніки. Моделі відмов. Основні положення. Київ: Держстандарт України. 42 с.

15. ДСТУ 3524-97. Надійність техніки. Проектна оцінка надійності складних систем з урахуванням технічного і програмного забезпечення та оперативного персоналу. Основні положення. Київ: Держстандарт України. 21 с.

UDC 004.056.5 Lavryk I. V. ORCID: 0000-0002-3433-9083 (MITIT)
DScTech, S. R. F Chevardin V. E. 0000-0002-1070-4568 (MITIT)
Marchuk O. V. ORCID: 0000-0003-4224-5113 (MITIT)

ASSESSMENT OF THE SECURITY LEVEL OF MODERN STANDARDIZED CRYPTOGRAPHIC TRANSFORMATIONS

Лаврік І. В., Чевардін В. Є., Марчук О. В. Оцінка рівня безпеки сучасних стандартизованих криптографічних перетворень.

Сучасні системи криптографічного захисту інформації, які будуються на основі математичних перетворень в кільці, групі та групі точок еліптичних кривих, більше не вважаються перспективним напрямком для подальшого розвитку систем захисту інформації. Це пов'язано з появою реального квантового комп'ютера, що призвело до активізації нового етапу розвитку криптосистем, який умовно називають постквантовими стабільними криптографічними алгоритмами.

У даній статті наводиться оцінка рівня безпеки існуючих стандартизованих криптосистем і перспективних криптоалгоритмів, потенційно стійких до квантового криптоаналізу. Рівень безпеки існуючих асиметричних криптосистем для квантового криптоаналізу є поліноміальним. Показано залежність криптографічної стійкості алгоритму від розміру загальносистемних параметрів. Наведені обмеження для проведення квантового криптоаналізу на теперішній час.

У статті наведені значення загальносистемних параметрів криптосистеми на основі еліптичних кривих, які можуть дати час для переходу до постквантової криптографії. Також показані такі криптосистеми, як SIKE, SIDH, які мають запас криптостійкості до квантового криптоаналізу та можливість побудови на їх основі постквантового алгоритму електронного цифрового підпису та інкапсуляції ключів.

Ключові слова: *постквантова криптографія, квантовий криптоаналіз, алгоритм Шора, RSA, ECC.*

Modern systems of cryptographic protection of information, which are based on mathematical transformations in the ring, group, and group of points of elliptic curves are no longer considered a promising area for further development of information security systems. This is due to the emergence of the real quantum computer, which led to the activation of a new stage in the development of cryptosystems, which are conventionally called post-quantum stable cryptographic algorithms.

This article provides an assessment of the existing standardized cryptosystems security level and promising crypto-algorithms potentially resistant to quantum cryptanalysis. The security level of existing asymmetric cryptosystems for quantum cryptanalysis is polynomial. The dependence of the algorithm security level on the size of the system-wide parameters is shown. The limitations for conducting quantum cryptanalysis at the present time are given.

The article gives the values of system-wide parameters of the elliptic curves cryptosystem, which can give time for the transition to post-quantum cryptography. Also shown are such cryptosystems as SIKE, SIDH, which have a margin of cryptoresistance to quantum cryptanalysis and the possibility of building a post-quantum electronic digital signature and key encapsulation algorithm of on their basis.

Keywords: *postquantum cryptography, quantum cryptanalysis, Shor's algorithm, RSA, ECC.*

1. Statement of the problem and relevance of the research

Nowadays, the security level is one of the main indicators of information security which is transmitted and processed in information systems. The security level of the algorithm is based on the complexity of solving certain mathematical problems (factorization of large integers, solving a discrete logarithm, etc.). The complexity of computing these problems on modern computers is sub-exponential or exponential. However, the appearance of the first quantum computer made it obvious the possibility of using Shor's [1] and Grover's [2] cryptanalysis algorithms to solve certain mathematical problems with polynomial complexity, which endangered the existing cryptographic information protection algorithms [3].

The creation of a quantum computer capable of computing Shor's cryptanalysis algorithm or Grover's unordered database search algorithm for standardized cryptosystems may cause threats to the security of critical infrastructure objects.

2. Main part.

Well-known algorithms for asymmetric transformation in a ring, a group, and a group of elliptic curve points are RSA, DSA, ECC, ECDSA, ECRSA, and others similar to them. Most attacks on such cryptosystems are aimed at finding the private key. Thus, for the RSA cryptosystem, the resistance

against such kind of attack is based on the complexity of the factorization of module N. It is believed that the best factorization algorithm is the algorithm of the general lattice of the numerical field or its modification. The time complexity [5] of such algorithms is subexponential and is calculated by expression (1):

$$O(\exp(\delta + o(1)(lnN)^{\gamma})\,(lnlnN)^{1-\gamma}),\ \delta = 1.92, \gamma = \frac{1}{3}. \quad (1)$$

Shor's algorithm has polynomial complexity. It can decompose a large prime number into prime factors in a time approximately equal to (2):

$$O(4n^3), \quad (2)$$

it requires the following number of qubits (3):

$$O(2n), \quad (3)$$

where n – module size.

Example 1:

Let`s evaluate the RSA-512 cryptographic algorithm cryptanalysis complexity for Shor's algorithm (2, 3):

$$O(4n^3) = O(4 \times 512^3) = O(536870912) \approx O(11{,}5 \times 10^{10}).$$

The required number of qubits to implement the specified algorithm:

$$O(2n) = 2 \times 512 = 1024.$$

Table 1 shows the estimation values of the quantum cryptanalysis algorithm parameters for the RSA cryptosystems.

Table 1

Module size, bits	Required number of qubits	The complexity of quantum cryptanalysis	The complexity of quantum cryptanalysis
512	1024	$0{,}5 \times 10^8$	$1{,}6 \times 10^{19}$
768	1536	$1{,}8 \times 10^9$	$9{,}9 \times 10^{22}$
1024	2048	$4{,}3 \times 10^9$	$1{,}2 \times 10^{26}$
2048	4096	$3{,}4 \times 10^{10}$	$1{,}35 \times 10^{35}$
3072	6144	$11{,}5 \times 10^{10}$	5×10^{41}
15360	30720	$1{,}5 \times 10^{13}$	$9{,}2 \times 10^{80}$

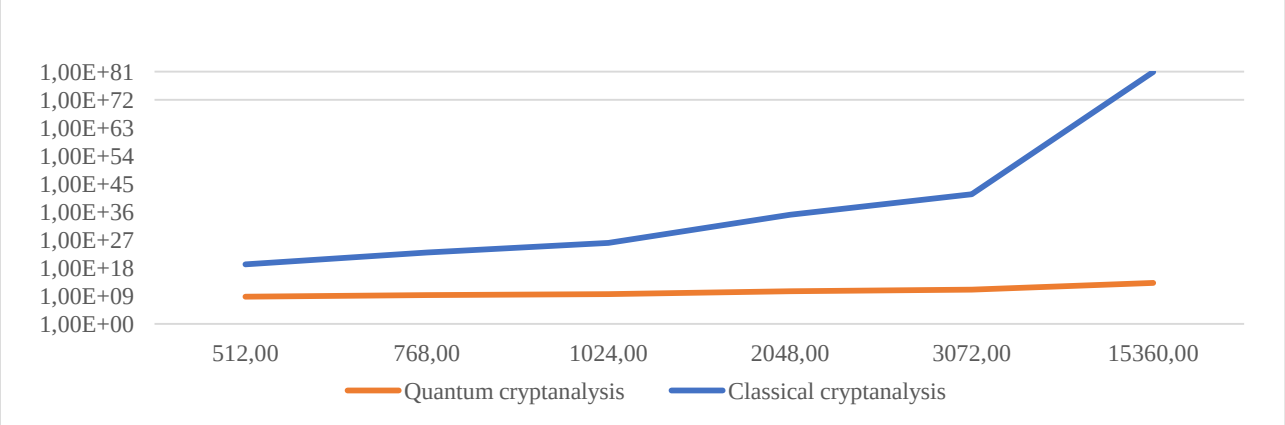


Fig. 1. Complexity of RSA cryptanalysis

From the results of analytical evaluations (Table 1) and the graph (Fig. 1), we can see that even with a key length of 15360 bits, only $1{,}5 \times 10^{13}$ operations are needed on a quantum computer, which means that this algorithm can be broken in polynomial time.

Problems of the elliptic curves discrete logarithm can be solved using ρ-Pollard's and λ-methods, it`s complexity is estimated by expression (4):

$$O\left(\sqrt{q}\right), \tag{4}$$

where $q = 2n$, and n – base point size.

In addition, in the general case, Shor's quantum algorithm is capable to solve the logarithmic equation [4] with an approximate complexity:

$$O(360n^3). \tag{5}$$

For this, you need to use a quantum computer with the number of the qubits equal to:

$$O(7n + 4log_2 n + 10). \tag{6}$$

Example:

Let`s evaluate the complexity of classical and quantum algorithms of discrete logarithms in a group of points of an elliptic curve with the base point order size ord(E) = 110 bits.

The complexity of classical cryptanalysis for the specified algorithm will be:

$$O\left(\sqrt{q}\right) = \sqrt{2^{110}} = 36\,028\,797\,018\,963\,968 \approx 3{,}6 \times 10^{16}.$$

The complexity of quantum cryptanalysis for the specified algorithm will be:

$$O(360n^3) = 479\,160\ \ 000 \approx 0{,}5 \times 10^{9}.$$

For this implementation, you need to use a quantum computer with the number of the qubits equal to:

$$O(7n + 4log_2 n + 10) = 7 \times 110 + 4log_2 110 + 10 = 807.125\ldots \approx 808.$$

Table 2 shows the parameter estimation values of the quantum cryptanalysis algorithm for cryptosystems on elliptic curves.

Table 2

Basepoint size, bits	Required number of qubits	The complexity of quantum cryptanalysis	The complexity of quantum cryptanalysis
110	808	$0{,}5 \times 10^{9}$	$3{,}6 \times 10^{16}$
163	1181	$1{,}5 \times 10^{9}$	$3{,}4 \times 10^{24}$
224	1610	4×10^{9}	$5{,}2 \times 10^{33}$
256	1834	6×10^{9}	$3{,}4 \times 10^{38}$
509	3609	$4{,}7 \times 10^{10}$	$4{,}1 \times 10^{76}$
571	4044	$6{,}7 \times 10^{10}$	$8{,}8 \times 10^{85}$
1024	7218	$3{,}8 \times 10^{11}$	$1{,}3 \times 10^{154}$
2048	14390	$3{,}1 \times 10^{12}$	$1{,}8 \times 10^{308}$

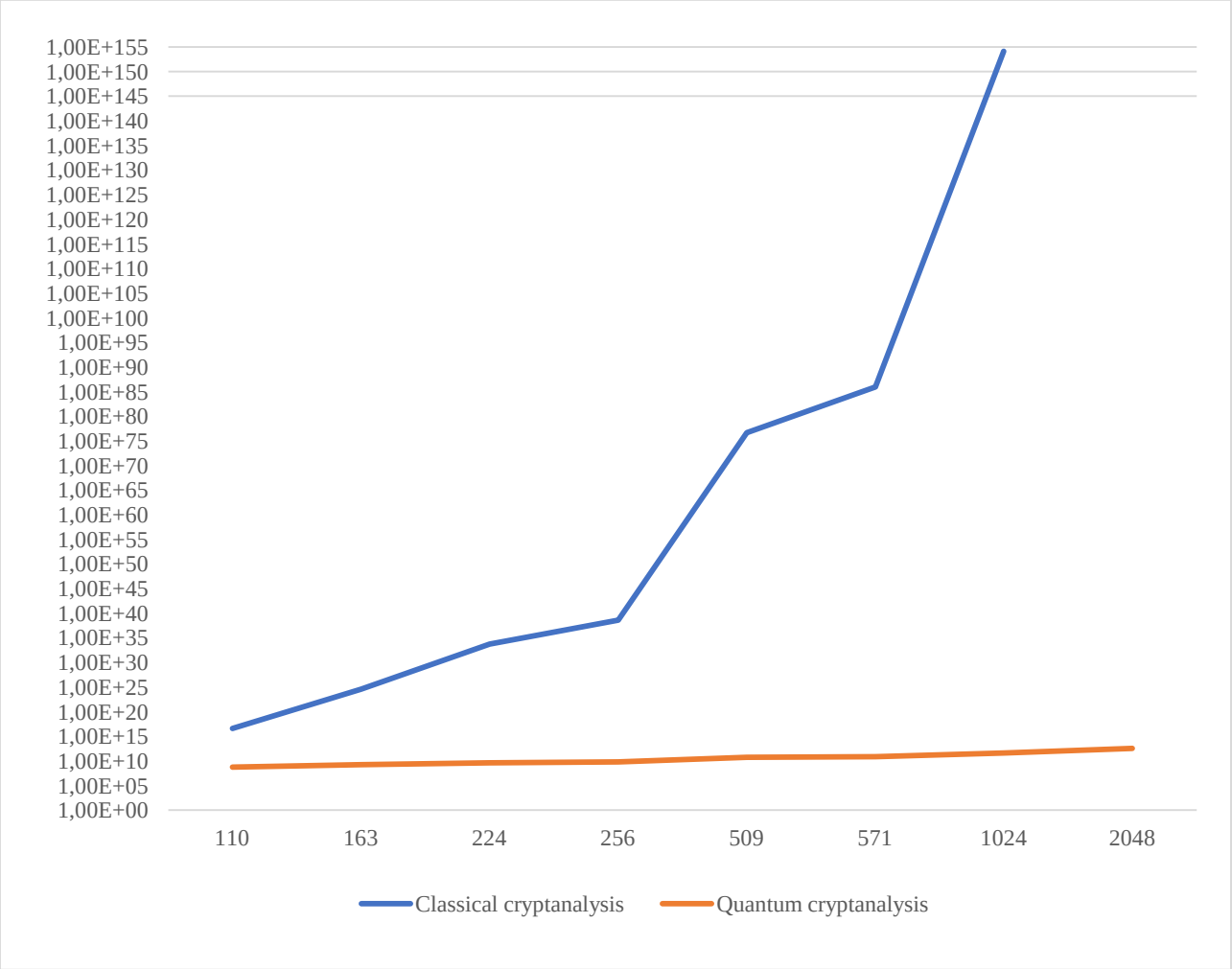


Fig. 2. Complexity of ECC cryptanalysis

From the results of analytical evaluations (Table 2) and the graph (Fig. 2), we can see that increasing the base point order size does not significantly increase cryptographic stability during quantum cryptanalysis, unlike classical cryptanalysis. This allows an attacker to perform quantum cryptanalysis in polynomial time.

Also, a comparison of analytical estimates, based on NIST recommendations [10] (Table 1, Table 2) shows that ECC requires a much smaller length of keys to ensure a comparable security level , which is provided by long RSA keys [6], but the implementation of ECC quantum cryptanalysis requires a smaller qubits number (Table 3).

Table 3

RSA key length, bits Required number of qubits	ECC key length, bits Required number of qubits
2048 4096	224 1610
3072 6144	256 1834

In both cases, quantum cryptanalysis requires a large number of qubits, which makes it impossible. However, eventually, such a computer will be created, so the transition to new algorithms resistant to quantum cryptanalysis must be done in advance.

New cryptographic transformations and the possibilities of their application published in open sources over the last 10 years are listed in Table 4 [8].

Table 4

Algorithm, Main cryptographic assumption	Used operations	Public Key length (bits) depending on the selected parameters	Private Key length (bits) depending on the selected parameters	Ability to create a digital signature	Ability to encrypt/ decrypt data
NTRU, NTRU PRIME, Falcon lattice-based	Matrix multiplication	NTRU – 699–2401 NTRU PRIME – 897–2067 Falcon – 897, 1793	NTRU – 935–2983 NTRU PRIME – 1125–3059 Falcon – 1281, 2305	+	+
Rainbow multivariable polynomials	Matrix multiplication, solving a linear system of equations	60192–1930600	64–1408736	+	–
SPHINCS+, Picnic hash-based	Hash functions (sha256/512, sha2, sha3)	SPHINCS+ – 64–128 Picnic – 33–65	SPHINCS+ – 7856–49856 Picnic – 49–97	+	–
McElice Codes usage	Matrix multiplication, decoding	McElice – 261120–1357824	McElice – 6452–14080	+	+
SIKE, SIDH (supersingular) isogeny walk problem	Operations with elliptic curves	SIDH – 134–564 SIKE – 197–564	SIDH – 28–48 SIKE – 350–644	–	+
Based on isomorphic transformations in the elliptic curves group of points [7]	Operations with elliptic curves	Dual_EC_DRBG – 256–521	Dual_EC_DRBG – 256–521	+	–

3. SIDH analysis.

One of the current areas of research is the development of new cryptographic algorithms using existing platforms and libraries of software functions that will meet the growing requirements for cryptographic stability of algorithms in the face of the increasing power of quantum computers. Algorithms based on the isogeny of the elliptic curve are a promising direction for the development of postquantum cryptosystems. So, let`s take a closer look at operations, used in SIDH algorithm.

Let the elliptic curve be given by the Weierstrass equation:

$$y^2 = x^3 + Ax + B \ mod \ p, \tag{7}$$

where $A = 1, B = 1, p = 19$ The order of the curve is equal to $\#E_p = 21$. The points of this curve are shown in Table 5.

Table 5

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
(0,1)	(0,18)	(2,7)	(2,12)	(5,6)	(5,13)	(7,3)	(7,16)	(9,6)	(9,13)	(10,2)
P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	-
(10,17)	(13,8)	(13,11)	(14,2)	(14,17)	(15,3)	(15,16)	(16,3)	(16,16)	*O*	-

Curve (7) has 2 subgroups with orders 3 and 7. For example, for a group of order 3, these are the points: (2,7), (2,12), *O*.

Definition 1. Group [11].

The set *G* with the binary operation "*" defined on it is called a group if:

1) operation "*" is associative, that means that for any $a,\ b,\ c \in G,\ \ a * a * (b * c) = (a * b) * c\ \ c;$

2) there is a neutral (single) element $e \in G$, that $e * a = a * e = a$ for all $a \in G$;

3) for every element $a \in G$ exists opposite element $a^{-1}:\ a * a^{-1} = a^{-1} * a = e.$

Definition 2. Subgroup [11].

A subgroup H of a group G is a subset of H, which is also a group concerning the same group operation defined in group G.

Definition 3. Lagrange's theorem [11].

Let G be a finite group. Then,

$$|G| = (G: H) \times |H|. \tag{8}$$

Definition 4. Bijection.

A bijection is a mapping in which each element of one set corresponds to exactly one element of another set, with an inverse mapping having the same property defined.

Definition 5. Isomorphism, homomorphism, automorphism.

The mapping $f: H \rightarrow G$ is called:

– homomorphism, if for any

$$h_1, h_2 \in H: f(h_1 \cdot h_2) = f(h_1) \times f(h_2); \tag{9}$$

– isomorphism, if *f* is homomorphism and bijection;

– automorphism, if *f* is an isomorphism and *H* = *G*.

Definition 6. Isogeny [11].

The isogeny of the elliptic curve is a non-constant rational mapping of the curve E_1 over a finite field *F* into the curve E_2, which is also called a group homomorphism and is given as:

$$(\mathrm{x};\ \mathrm{y}) \rightarrow (\mathrm{f1}(\mathrm{x};\ \mathrm{y})/\mathrm{f2}(\mathrm{x};\ \mathrm{y}), \mathrm{g1}(\mathrm{x};\ \mathrm{y})/\mathrm{g2}(\mathrm{x};\ \mathrm{y})), \tag{10}$$

where *f1*, *f2*, *g1*, *g2* – are polynomials.

Example:

Let`s obtain the isogeny of the elliptic curve (7).

The isogeny of the curve can be obtained using the Vélu algorithm with the isogeny nucleus $\mathrm{C}: \{O, (2, 7), (2, 12)\}$, where the nucleus of isogeny is a cyclic subgroup of simple order. We obtain the isogeny curve by the Vélu algorithm. Let us take curve (7).

Vélu algorithm for $\mathrm{C}: \{\boldsymbol{O}, (\mathbf{2}, \mathbf{7}), (\mathbf{2}, \mathbf{12})\}$

1. Dropping a point at infinity.
2. Finding C_2 is a set of points of a pair order. *R* – the rest of the points. There are no points of a pair order in sub-group *C*.
3. Breaking *R* into two parts R_+ and R_-. For R_+we choose the point (2;7). Point (2;12) is opposite, because $7 = -12 \bmod 19$
4. Set S = {(2,7)} Cycle consist of one step because the *S* set includes one point.

$$Q = (2, 7), \text{ coordinates are } x_Q = 2, y_Q = 7.$$
$$g_Q^x = 3 * 2^2 + 1 = 13$$
$$g_Q^y = -2 * 7 = 5$$
$$v_Q = 2 * 13 = 7$$
$$u_Q = 5^2 = 6$$
$$v = 7$$
$$w = 6 + 2 * 7 = 1$$
$$A' = 1 - 5 * 7 = 4$$

$$B' = 1 - 7 * 1 = 13$$

We calculate rational reflection $(s, y) \to (\alpha, \beta)$, using the nucleus $(x, y) \to (\alpha, \beta)$ of the curve (7).

$$\alpha = x + \sum_{Q \in S} \left(\frac{v_Q}{(x - x_Q)} + \frac{u_Q}{(x - x_Q)^2} \right)$$

$$\alpha = x + \frac{7}{x-2} + \frac{6}{(x-2)^2} = \frac{x^3 - 4x^2 + 11x - 8}{x^2 - 4x + 4}$$

$$\beta = y - \sum_{Q \in S} \left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2} \right)$$

$$\beta = \frac{x^3 y - 6x^2 y + 5xy - 6y}{x^3 - 6x^2 + 12x - 8}$$

Reflection $\varphi: (x, y) \to (\alpha, \beta)$

We calculate rational reflection$(s, y) \to (\alpha, \beta)$, using the nucleus $(x, y) \to (\alpha, \beta)$ of curve $E_1: y^2 = x^3 + x + 1 \; mod \; 19$ on curve $E_2: y^2 = x^3 + 4x + 13 \; mod \; 19$.

Table 6

№	*Point coordinates of* E_1curve	*Point coordinates of* E_2curve
1.	(0,1)	(17, 15)
2.	(7,16)	
3.	(14,17)	
4.	(0,18)	(17, 4)
5.	(7,3)	
6.	(14,2)	
7.	(5,6)	(8, 5)
8.	(10,2)	
9.	(16,16)	
10.	(5,13)	(8, 14)
11.	(10,17)	
12.	(16,3)	
13.	(9,6)	(14, 1)
14.	(13,11)	
15.	(15,3)	
16.	(9,13)	(14, 18)
17.	(13,8)	
18.	(15,16)	
19.	(2,7)	*O*
20.	(2,12)	
21.	*O*	

Vélu algorithm for C: $\{\boldsymbol{O}, (\mathbf{10}, \mathbf{2}), (\mathbf{10}, \mathbf{17}), (\mathbf{14}, \mathbf{2}), (\mathbf{14}, \mathbf{7}), (\mathbf{15}, \mathbf{3}), (\mathbf{15}, \mathbf{16})\}$

1. Dropping a point at infinity.

2. Finding C_2 is a set of points of a pair order. R – the rest of the points. There are no points of a pair order in sub-group C.

3. Breaking R into two parts R_+ and R_-. For R_+we choose points (10, 2), (14, 2), (15, 3). Points (10, 17), (14, 17), (15, 16) are opposite, because $2 = -17 \bmod 19$ and $3 = -16 \bmod 19$

4. Set $S = \{(10,2),(14,2),(15,3)\}$
The cycle consists of three steps because the S set includes three points.

First step:

$$Q = (10,2), \text{coordinates are } x_Q = 10, y_Q = 2.$$
$$g_Q^x = 3 * 10^2 + 1 = 16$$
$$g_Q^y = -2 * 2 = 15$$
$$v_Q = 2 * 16 = 13$$
$$u_Q = 15^2 = 16$$

Second step:

$$Q = (14,2), \text{coordinates are } x_Q = 14, y_Q = 2.$$
$$g_Q^x = 3 * 14^2 + 1 = 0$$
$$g_Q^y = -2 * 2 = 15$$
$$v_Q = 2 * 0 = 0$$
$$u_Q = 15^2 = 16$$

Third step:

$$Q = (15,3), \text{coordinates are } x_Q = 15, y_Q = 3.$$
$$g_Q^x = 3 * 15^2 + 1 = 11$$
$$g_Q^y = -2 * 3 = 13$$
$$v_Q = 2 * 11 = 3$$
$$u_Q = 13^2 = 17$$
$$v = 13 + 0 + 3 = 16$$
$$w = (16 + 10 * 13) + (16 + 14 * 0) + (17 + 15 * 3) = 15$$
$$A' = 1 - 5 * 16 = 16$$
$$B' = 1 - 7 * 15 = 10$$

We calculate rational reflection$(s, y) \to (\alpha, \beta)$:

$$\alpha = x + \sum_{Q \in S}\left(\frac{v_Q}{(x - x_Q)} + \frac{u_Q}{(x - x_Q)^2}\right),$$

$$\alpha = x + \left(\frac{13*(x-10)+16}{(x-10)^2} + \frac{0*(x-14)+16}{(x-14)^2} + \frac{3*(x-15)+17}{(x-15)^2}\right),$$

$$\beta = y - \sum_{Q \in S}\left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2}\right),$$

$$\beta = y - \left(\begin{array}{c}\frac{13y+(13y-7)(x-10)-12(x-10)}{x^3-11x^2+15x-12} + \frac{13y}{x^3-4x^2+18x-8} + \\ + \frac{15y+(3y-9)(x-15)-10(x-15)}{x^3-7x^2+10x-12}\end{array}\right),$$

Reflection φ: $(x, y) \to (\alpha, \beta)$

Table 7

Point of E_2	**(12, 7)**						
Point of E_1	(0,1)	(2,7)	(5,13)	(7,3)	(9,13)	(16,16)	(13,11)
Point of E_2	**(12, 12)**						
Point of E_1	(0,18)	(2,12)	(5,6)	(7,16)	(9,6)	(16,3)	(13,8)
Point of E_2	**O**						
Point of E_1	(10,2)	(10,17)	(14,2)	(14,17)	(15,3)	(15,16)	O

The general idea of the protocol is that with the help of publicly available parameters Alice and Bob perform separate calculations of isogenies of degree l_A^a and l_B^b, respectively, calculating the isogeny of large order over the secret nucleus (Fig. 4).

Public SIDH parameters include:

- A prime number p of the form $l_A^a l_B^b \cdot f \pm 1$, where l_A^a and l_B^b are small prime numbers, a and b are natural integers, and f is a cofactor.
- Supersingular elliptic curve, $E_0(F_{p^2})$.
- Points $\{P_A, Q_A\}$ generated from $E_0[l_A^a]$ over $\mathbb{Z}/l_A^a\mathbb{Z}$ and points $\{P_B, Q_B\}$ generated from $E_0[l_B^b]$ over $\mathbb{Z}/l_B^b\mathbb{Z}$.

The protocol consists of two rounds which can be divided into the following steps:

Calculating the secret nucleus $R = \langle [m]P + [n]Q \rangle$ for base points $\{P, Q\}$, where m and n are private keys.

Calculation of isogeny over the secret nucleus, $\varphi: E \to E/\langle R \rangle$, using the Vélu algorithm for the supersingular curve E.

Calculate the mappings of the base points of the base of the other side, $\{\varphi(P_{opp}), \varphi(Q_{opp})\}$, for the first round.

Thus, for the first round, Alice and Bob calculate the isogeny $\varphi_A: E_0 \to E_A = E_0/\langle [m_A]P + [nA]Q$. They apply isogeny to the base points of the other side. After the first round, Alice sends Bob $(E_A, \{\varphi_A(P_B), \varphi_A(Q_B)\})$. Bob sends Alice $(E_B, \{\varphi_B(P_A), \varphi_B(Q_A)\})$ through the unprotected channel. The second round consists of a similar calculation of isogeny, but with the public keys, they exchanged. Alice calculates $\varphi'_A: E_B \to E_{AB} = E_B/\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$, Bob calculates $\varphi'_B: E_A \to E_{BA} = E_A/\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B) \rangle$ To obtain a general secret, Alice calculates the j-invariant of E_{AB}, and Bob of E_{BA}.

The safety assumption is based on the difficulty of calculating isogeny between supersingular elliptic curves for which there is no subexponential algorithm known for quantum computers. Alice generates private keys $m_A, n_A \in \mathbb{Z}/l_A^a\mathbb{Z}$, which are not divisible by l_A^a. Bob also generates private keys $m_B, n_B \in \mathbb{Z}/l_B^b\mathbb{Z}$, which are not divisible by l_B^b .

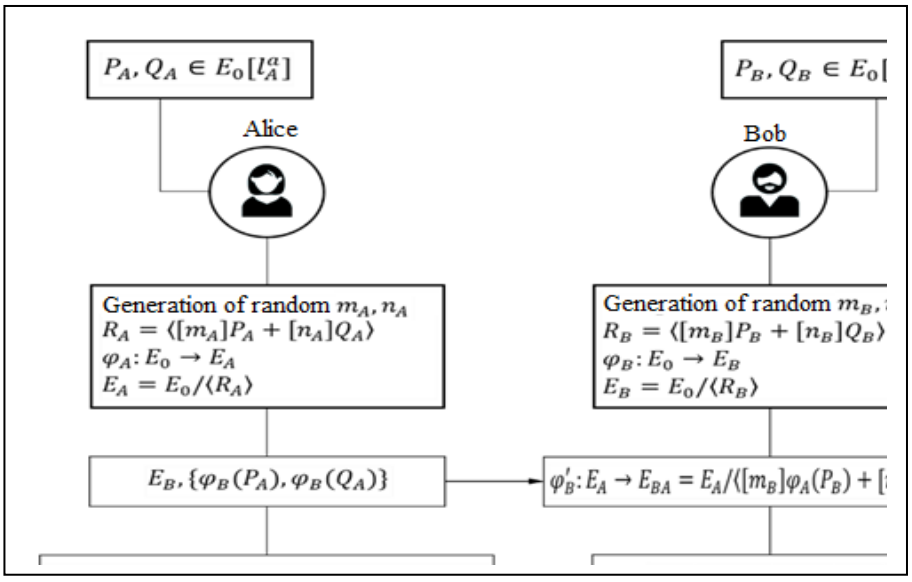


Fig. 3. SIDH algorithm scheme

Research on the security level, done with algorithms based on elliptic curves isogenies in [9] shows that for classical cryptanalysis needed time is equal to $3{,}4 \times 10^{38}$ with classical memory $1{,}8 \times 10^{19}$, and that a quantum key recovery on AES-128 costs $1{,}2 \times 10^{24}$ gates (which allows for

$1{,}1 \times 10^{12}$ queries and $1{,}2 \times 10^{24}$ quantum time), and neglect polynomial factors. Then this would require $p \sim 5280$ bits, that is, multiplying by 10 the parameter size.

4. Conclusion.

This paper provides an assessment of the security level of the existing standardized cryptosystems, the main cryptographic assumption of which is based on the complexity of integer factorization and solving the problem of discrete logarithms and promising crypto-algorithms potentially resistant to quantum cryptanalysis. The security level of existing asymmetric cryptosystems to quantum cryptanalysis is polynomial, and system-wide parameters size increasing will not significantly increase the security level. The current limitation for quantum cryptanalysis is the required number of qubits.

The length of the system-wide parameters of a cryptosystem based on elliptic curves can be increased to 2048 bits, in this case, a quantum computer must have 14390 qubits to crack such a cryptosystem. It gives some time for the transition to post-quantum cryptography. It should also be noted that such cryptosystems as the SIKE, SIDH algorithms have a margin of crypto resistance to quantum cryptanalysis and the possibility of building a post-quantum algorithm of electronic digital signature and key encapsulation on their basis.

The work also presented potential candidates for the post-quantum cryptography standard, their differences, and the possibilities of their application

REFERENCES

1. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor // S IAM J. Comput. 1997. 26 (5). P. 1484–1509.

2. Grover L. K. A fast quantum mechanical algorithm for database search / L. K. Grover // Proceeding of the 28th ACM Symposium on Theory of Computation, New York: ACM Press. 1996. P. 212–219.

3. Lily Chen. Report on Post-Quantum Cryptography / Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone // NISTIR 8105. 2016. P. 2.

4. Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring / Shor, P. W. // In: Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124–134.

5. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Восточно-Европейский журнал передовых технологий. Харків, 2014. Том 6, № 1 (67). С. 8–15.

6. Kerry Maletsky. RSA vs. ECC Comparison foe Embedded systems / Kerry Maletsky // Microchip. 2020.

7. Чевардін В. Е. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой / В. Е. Чевардін, А. В. Бессалов // Прикладна радіоелектроніка. 2012. Том 11. № 2. С. 234–237.

8. liboqs. Open-source C library for quantum-safe cryptographic algorithms. URL: https://github.com/open-quantum-safe/liboqs.

9. Xavier Bonnetain. Quantum Security Analysis of CSIDH / Xavier Bonnetain, Andre Schrottenloher // Advances in Cryptology – EUROCRYPT 2020. Pp. 493–522.

10. NIST SP 800-57 § 5.6.1. P. 62–64. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p1r3.pdf.

11. Applied algebra. Part 1. Basics of abstract algebra: tutorial / L. V. Kovalchuk, Y. Y. Yaremchuk. Vinnytsya: VNTU, 2015. 99 p.

УДК 004.85
канд. техн. наук Макарчук О. М. ORCID: 0000-0002-0374-369X (ВІТІ)
Бовда В. Е. ORCID: 0000-0002-4072-771X (ВІТІ)
Остапчук В. М. (ВІТІ)

КОМБІНОВАНИЙ АЛГОРИТМ НАВЧАННЯ НЕЙРОННИХ МЕРЕЖ ПРЯМОГО ПОШИРЕННЯ

Суть навчання нейронних мереж прямого поширення полягає в мінімізації функції середньоквадратичної помилки виходу. Ця функція мультимодальна, тобто має декілька локальних мінімумів. Для пошуку мінімуму таких функцій найчастіше використовуються градієнтні і стохастичні методи, які не гарантують знаходження глобального мінімуму. У статті аналізуються градієнтний алгоритм зворотного поширення помилки і стохастичний метод рою частинок для навчання нейронних мереж прямого поширення, вказані їх переваги і недоліки. Пропонується об'єднати переваги обох методів у комбінованому алгоритмі.

Процес навчання за допомогою комбінованого алгоритму здійснюється в два етапи. На першому етапі стохастичний метод рою частинок проводить задану кількість епох навчання і визначає множину точок, в околиці яких можуть знаходитись точки локального мінімуму. На другому етапі градієнтний алгоритм зворотного поширення помилки знаходить локальний мінімум для кожної точки і вибирає з них оптимальний. Якщо задане значення середньоквадратичної помилки виходу не досягнуто, то етапи навчання повторюються.

Для оцінки ефективності запропонованого підходу до навчання нейронних мереж проведена серія порівняльних експериментів з використанням відомої бази даних розпізнавання комп'ютерних атак KDD Cup 1999 Data. В експериментах порівнювались результати навчання нейронної мережі прямого поширення для методу рою частинок, алгоритму зворотного поширення помилки і комбінованого алгоритму. Результати експериментів довели перевагу комбінованого алгоритму.

Ключові слова: *нейронна мережа, градієнтний метод, метод рою частинок, алгоритм зворотного поширення помилки.*

O. Makarchuk, V. Bovda. V. Ostapchuk Combined algorithm for training neural networks of direct propagation

The essence of learning neural networks of direct propagation is to minimize the function of the root mean square error of the output. This function is multimodal, ie it has several local minima. To find the minimum of such functions, gradient and stochastic methods are most often used, which do not guarantee finding the global minimum. The article analyzes the gradient algorithm of inverse error propagation and the stochastic method of particle swarm for training neural networks of direct propagation, their advantages and disadvantages are indicated. It is proposed to combine the advantages of both methods in a combined algorithm.

The learning process using a combined algorithm is carried out in two stages. At the first stage, the stochastic method of particle swarm conducts a given number of learning epochs and determines the set of points in the vicinity of which there may be points of local minimum. In the second stage, the gradient backpropagation algorithm finds the local minimum for each point and selects the optimal one. If the set value of the standard error of the output is not reached, the learning steps are repeated

To evaluate the effectiveness of the proposed approach to the training of neural networks, a series of comparative experiments using the well-known database of computer attack recognition KDD Cup 1999 Data. The experiments compared the results of training the direct propagation neural network for the particle swarm method, the inverse error propagation algorithm, and the combined algorithm. The experimental results proved the superiority of the combined algorithm.

Keywords: *neural networks, gradient method, particle swarm method, error backpropagation algorithm.*

Постановка завдання. Штучні нейронні мережі (ШНМ) знаходять все ширше застосування в різних сферах. Більшість з них являють собою багатошарові персептрони з прямим поширенням сигналу [1]. Важливим питанням практичної побудови ШНМ є її навчання, тобто адаптація до розв'язання конкретної задачі. ШНМ навчається шляхом зміни її параметрів. Розрізняють дві групи методів навчання: детерміністські та стохастичні.

Класичним детерміністським методом навчання є ітераційний алгоритм зворотного поширення помилки (АЗПП). В основі алгоритму лежить градієнтний метод найшвидшого спуску [2], який дозволяє мінімізувати середньоквадратичну помилку виходу (СПВ) за рахунок корекції ваг нейронів. Перевагою алгоритму є наявність добре розробленого математичного апарату, хороша збіжність до точки екстремуму і швидкодія.

Однак АЗПП має і ряд недоліків [2]:

функція обчислення СПВ є мультимодальною. Локальні мінімуми можуть суттєво відрізнятись значенням цільової функції. АЗПП знаходить точку локального мінімуму, який може бути не тільки не глобальним, але і менш ефективним за інші локальні мінімуми;

функція активації нейронів повинна мати похідну по всьому діапазону зміни аргументу, що не завжди виконується для деяких типів нейронних мереж;

алгоритм чутливий до початкової ініціалізації синаптичних ваг нейронів, оскільки вона визначає точку, з якої починається градієнтний спуск.

Стохастичні методи здійснюють псевдовипадкові зміни параметрів ШНМ з метою зменшення СПВ. Загальна ітераційна формула стохастичного пошуку має вигляд:

$$X_{k+1} = X_k + \zeta_k ,$$

де X_k і X_{k+1} – значення аргументів цільової функції на поточному і наступному кроці;

ζ_k – випадкова величина.

Існує декілька різновидів стохастичних методів, з яких при навчанні ШНМ найчастіше використовується метод рою частинок (МРЧ). Цей метод шукає точки екстремуму паралельно по всьому просторі визначення функції. Він також не гарантує знаходження глобального екстремуму, але з декількох локальних дозволяє вибрати кращий. Недоліком МРЧ є труднощі з налаштуванням параметрів рою, повільна збіжність до дна точки екстремуму і низька швидкодія.

Аналізуючи АЗПП і МРЧ, можна помітити, що вони певною мірою взаємно компенсують недоліки один одного. У зв'язку з вищевказаним сформульовано такі задачі дослідження:

1. Експериментально перевірити, наскільки суттєво локальні мінімуми функції обчислення СПВ відрізняються один від одного.

2. Запропонувати і дослідити спосіб підвищення ефективності навчання за рахунок комбінованого використання АЗПП і МРЧ.

Очевидно, другу задачу є сенс розв'язувати, коли локальні мінімуми можуть відрізнятися суттєво.

Аналіз останніх публікацій. Практичне використання нейронних мереж почалося після розробки АЗПП. З тих часів алгоритм не зазнав суттєвих змін і проблема локальних мінімумів залишилась [1].

Використання МРЧ для навчання ШНМ аналізувалось в [3–8]. Основні зусилля направлялись на обґрунтування методики налаштування параметрів рою для розв'язання конкретних задач. Зазначалось, що в цілому МРЧ дає кращі результати, ніж класичний АЗПП, так як пошук проводиться по всій області визначення цільової функції і декілька частинок рою можуть знаходитись в околиці локальних мінімумів.

Ідея комбінувати АЗПП і МРЧ в процесі навчання ШНМ досліджувалась в [6], але схема реалізації суттєво відрізнялась від запропонованої в статті. В даній схемі на кожній ітерації навчання спочатку працює АЗПП, а потім його результати корегуються МРЧ. На нашу думку, така схема не гарантує від попадання в неефективну точку локального мінімуму, оскільки околицю пошуку визначає АЗПП.

Метою статті є дослідження ефективності навчання ШНМ за допомогою запропонованого комбінованого алгоритму (КА), в якому поєднується робота АЗПП і МРЧ.

Виклад основного матеріалу. Процес навчання ШНМ за допомогою КА приведено на рис. 1. Він складається з двох етапів:

на першому етапі працює МРЧ. Він проводить N (визначається експериментально) епох навчання і формує множину точок-кандидатів на можливі точки мінімуму;

на другому етапі АЗПП досліджує точки-кандидати на мінімум. Процес продовжується до досягнення умов закінчення навчання. Якщо умови не досягнуті, то процес навчання повертається до першого етапу. МРЧ продовжує свою роботу з точки зупинки.

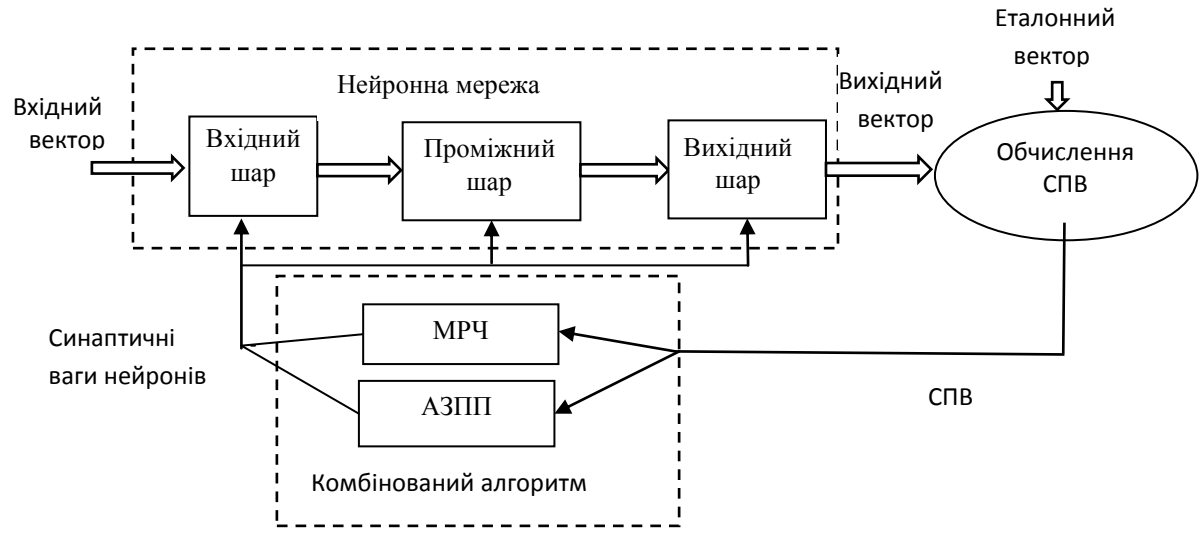


Рис. 1. Схема навчання нейронної мережі за допомогою комбінованого алгоритму

Існує декілька варіантів реалізації МРЧ [3]. Ідея методу була частково запозичена з досліджень поведінки скупчень живих істот (косяків риб, зграй птахів, натовпу людей тощо). Спочатку створюється сукупність (рій) частинок, які розкидані випадковим чином по всій області пошуку і кожна частинка має випадковий вектор швидкості. У кожній точці, де побувала частинка, розраховується значення цільової функції. При цьому кожна частинка запам'ятовує, яке (і де) краще значення цільової функції вона особисто знайшла. Також кожна частинка знає, де розташована точка, що є кращою серед усіх точок, які розвідали частинки. На кожній ітерації частинки коректують свою швидкість (модуль і напрямок), щоб з одного боку бути ближче до кращої точки, яку частинка знайшла сама (автори алгоритму назвали цей аспект поведінки «ностальгією»), і, в той же час, наблизитися до точки, яка в даний момент є глобально кращою. Через деяку кількість ітерацій частинки повинні зібратися поблизу найбільш хорошої точки, хоча можливо, що частина частинок залишиться десь у відносно непоганому локальному екстремумі, але головне, щоб хоча б одна частинка виявилася поблизу глобального екстремуму.

На кожному кроці координата частинки X_{k+1} обчислюється за формулою:

$$X_{k+1} = X_k + V_{k+1},$$

де X_k і X_{k+1} – значення аргументів цільової функції на поточному і наступному кроці;

V_{k+1} – швидкість частинки.

Аргументами є синаптичні ваги нейронів.

Існує декілька варіантів реалізації методу, які відрізняються методикою обчислення V_{k+1} [4–5]. В найбільш поширеному варіанті швидкість частинки обчислюється за формулою:

$$V_{k+1} = \omega_k V_k + \varphi_p r_p (p_k - X_k) + \varphi_g r_g (g_k - X_k),$$

де ω_k – коефіцієнт інерції;

φ_p, φ_g – вагові коефіцієнти;

r_p, r_g – випадкові числа в інтервалі (0, 1);

p_k – координата кращого рішення для даної частинки;

g_k – координата кращого рішення для рою.

Коефіцієнти ω_k, φ_p, φ_g підбираються експериментально для конкретної задачі.

Для розв'язання поставлених задач дослідження необхідно окреслити конкретну область використання ШНМ, визначити структуру нейронної мережі, реалізувати, навчити її і провести ряд експериментів для набору статистики. Для навчання ШНМ потрібно створити власну базу даних навчальних і тестових прикладів або вибрати одну з публічних баз.

Дослідження проводились на базі даних KDD Cup 1999 Data для розпізнавання комп'ютерних атак [9]. Вибір обумовлено актуальністю дослідження засобів протидії комп'ютерним атакам і доступністю цієї бази даних для навчання ШНМ.

База даних KDD Cup 1999 Data містить відомості про комп'ютерні атаки різних типів (DOS, R2l, U2R, Probing). База містить близько 5 000 000 записів. Кожен запис в цій базі є образом мережевого з'єднання. З'єднання – послідовність TCP-пакетів за деякий кінцевий час, протягом якого дані передаються від IP-адреси джерела на IP-адресу приймача (і в зворотному напрямку), використовуючи деякий протокол.

Окремий запис містить 41 параметр мережевого трафіку та промаркований як «атака» або «не атака». Наприклад, перший параметр визначає тривалість з'єднання, другий – вказує протокол, що використовується, третій – цільову службу і т. д.

Нейронна мережа складається зі вхідного шару (41 нейрон по числу вхідних параметрів), проміжного шару (16 нейронів згідно з рекомендаціями в [8]), вихідного шару (2 нейрони). Один нейрон класифікує наявність атаки, інший – відсутність атаки. Для навчання нейронної мережі випадково вибирались навчальні та тестові приклади стосовно DOS-атак.

Перша серія експериментів з використанням АЗПП проводилась з метою визначити, наскільки суттєво відрізняються точки локального мінімуму за значенням СПВ. Експерименти відрізнялись початковою ініціалізацією ваг нейронів і закінчувались досягненням точки локального мінімуму. Недоліком підходу є те, що на кожному кроці не враховується інформація про попередні кроки. Експерименти довели, що АЗПП в процесі навчання може зупинятись в локальних точках мінімуму СПВ, які суттєво (на порядок і більше) відрізняються за ефективністю. Тому використання пошуку на множині локальних мінімумів у процесі навчання має сенс.

У другій серії експериментів визначалась середня кількість оброблених прикладів навчання для досягнення заданої СПВ кожним з вищезгаданих методів навчання. Результати експериментів приведені в таблиці 1.

Таблиця 1

Середньоквадратична помилка виходу	**Середня кількість оброблених прикладів**		
	АЗПП	**МРЧ**	**КА**
0,25	128	111	87
0,1	322	236	211
0,05	745	608	502
0,025	1452	1132	880
0,01	2720	2218	1873

Аналізуючи дані таблиці, можна відмітити, що КА для навчання потрібно менше еталонних прикладів, ніж його конкурентам. Ця перевага має суттєве значення, коли база еталонних прикладів обмежена. Зі зменшенням кількості оброблених прикладів зменшується і тривалість навчання.

Наступна серія експериментів проводилась з метою оцінки ефективності КА порівняно з АЗПП і МРЧ. Кожний експеримент повторювався тричі з однаковою початковою ініціалізацією ваг нейронів, але з різними методами навчання. Кожний повтор закінчувався по досягненню заданої кількості епох. В експерименті визначався кращий метод навчання. Результати показали, що АЗПП був кращим за показником мінімуму СПВ в 19 % експериментів, МРЧ – в 32 % і КА – в 49 %.

Тестування навчених досліджуваними методами ШНМ показало, що КА забезпечує також меншу (на 33 % порівняно з АЗПП і 24 % порівняно з МРЧ) ймовірність хибного розпізнавання DOS-атаки.

Висновок. Таким чином, запропонований алгоритм навчання ШНМ об'єднує переваги градієнтного АЗРП і стохастичного МРЧ та дозволяє скоротити кількість навчальних прикладів для досягнення заданої СПВ. Пропонується використовувати його переваги при побудові систем захисту від комп'ютерних атак на основі ШНМ.

В подальших дослідженнях планується оцінити ефективність запропонованого підходу до навчання інших типів ШНМ, зокрема рекурентних.

ЛІТЕРАТУРА

1. Хайкин С. Нейронные сети: полный курс. 2-е изд., испр. Пер. с англ. Москва: ООО «И. Д. Вильямс», 2006. 1104 с.

2. Уайлд, Д. Дж. Методы поиска экстремума. Москва: Главная редакция физико-математической литературы издательства «Наука», 2017. 268 с.

3. Карпенко А. П., Селиверстов Е. Ю. Обзор методов роя частиц для задачи глобальной оптимизации (Particle Swarm Optimization) // Наука и образование: электронное научно-техническое издание. 2009. № 3. URL: http://technomag.edu.ru/doc/116072.html.

4. Е. В. Пальчевский, О. И. Христодуло. Разработка импульсной нейронной сети с возможностью скоростного обучения для нейтрализации DDoS-атак //Программные продукты и системы. 2019. Том 32, № 4. С. 613–627.

5. Воробьева Ю. Н., Катасева Д. В., Катасев А. С., Кирпичников А. П. Нейросетевая модель выявления DDoS-атак // Вестник технологического университетата. 2018. Т. 21. № 2. С. 94–98.

6. Частикова В. А., Власов К. А., Картамышев Д. А. Обнаружение ddos-атак на основе нейронных сетей с применением метода роя частиц в качестве алгоритма обучения // Фундаментальные исследования 2014. № 8. С. 829–832.

7. Титюнников А. В., Кароль А. Д., Бессчетнов А. В. Применение метода роя частиц в качестве обучения нейронных сетей // CyberLeninka: научная электронная библиотека. URL: https://cyberleninka.ru/article/n/primenenie-metoda-roya-chastits-v-kachestve-obucheniya-neyronnyh-setey/viewer.

8. SaiedA., Overill R., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Net-works. Neurocomputing, 2016, vol. 172, pp. 385–393.

9. KDD Cup 1999 Data // UCI Knowledge Discovery in Databases Archive. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

УДК 004.7.056.5

Остапук О. І. ORCID: 0000-0001-6557-9525 (ВІТІ)
Плугова О. Б. ORCID: 0000-0001-7848-7806 (ВІТІ)
Лазута Р. Р. ORCID: 0000-0003-3254-9690 (ВІТІ)
д-р техн. наук Міночкін А. І. ORCID: 0000-0001-5723-5052 (ВІТІ)

ВАРІАНТ АРХІТЕКТУРИ ТА ФУНКЦІОНУВАННЯ ПІДСИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕВОЮ БЕЗПЕКОЮ

В останні роки спостерігається стрімке зростання інформаційних та особливо телекомунікаційних технологій, що базуються на порівняно простих, зрозумілих та доступних алгоритмічних, технічних рішеннях, реалізованих в стандартних протоколах мережі Internet (електронна пошта, SMTP, IMAP, файловий обмін FTP, маршрутизація RIP, OSPIF та ін.). Все це призвело до їх виключного застосування практично в усіх створюваних мережах зв'язку як загального користування, так і, на жаль, в телекомунікаційних мережах системи зв'язку спеціального призначення, для яких відкритість, практична незахищеність, а не рідко й недостатня ефективність застосування протоколів обов'язково передбачає використання ресурсоємних системотехнічних рішень, що забезпечить задану ефективність та інформаційну безпеку функціонування таких мереж.

Функціонування мультисервісних мереж з високими показниками за ефективністю в умовах інформаційної протидії та досить жорстоких вимог до них з боку користувачів (посадових осіб органів управління) можливе тільки при вирішенні цілого комплексу задач із забезпечення інформаційної безпеки.

Вирішальну роль в цьому процесі відводиться автоматизованій системі управління мережею.

У статті розглянуто варіант архітектури та функціонування підсистеми управління мережевою безпекою за стандартами ISO.

Ключові слова: *мультисервісні мережі, інформаційна безпека, управління мережевою безпекою.*

A. Ostapuk, O. Pluhova, R. Lazuta, A. Minochkin. **Version of architecture and functioning of the network security management subsystem.**

In recent years, there has been a rapid growth of information and especially telecommunications technologies based on relatively simple, clear and accessible algorithmic, technical solutions implemented in standard Internet protocols (e-mail, SMTP, IMAP, FTP file sharing, RIP routing, OSPIF and others) all This has led to the exclusive use of almost all existing communication networks, both public and, unfortunately, in telecommunications networks of special purpose communication systems, for which openness, practical insecurity, and often insufficient efficiency of protocols necessarily involves the use of resource-intensive system solutions. will provide the set efficiency and information security of functioning of such networks.

Operation of multiservice networks with high efficiency in the conditions of information counteraction and rather rigid requirements to them from users (officials of bodies of Management), is possible only at the decision of the whole complex of tasks on maintenance of information security.

The automated network management system plays a crucial role in this process.

The article considers the variant of architecture and functioning of the network security management subsystem according to ISO standards.

Keywords: *multiservice networks, information security, network security management.*

Постановка завдання. Достатня складність мереж, що входять до складу мультисервісних мереж зв'язку (абонентські мережі, мережі доступу, транспортна мережа, мережі послуг прикладного рівня) та впроваджуваних в них механізмів захисту інформації, збільшення кількості вразливостей, пов'язаних з використанням стандартних протоколів, наявність потенційних помилок чи «закладок» в програмному забезпеченні засобів телекомунікацій, засобів надання послуг зв'язку та управління, можливості супротивника в кібератаках обумовлює необхідність розробки достатньо складних автоматизованих комплексів управління мережевою безпекою. До складу цих комплексів, як правило, повинні входити потужні адаптивні засоби виявлення та аналізу загроз.

Такі комплекси здатні не тільки контролювати працездатність засобів захисту інформації в кожній мережі, а й суттєво підвищити захищеність елементів мультисервісної мережі зв'язку від інформаційного впливу, існуючих помилок в конфігурації кожної мережі, сприяти виявленню можливих шляхів атакуючих дій різних категорій супротивника, визначенню критичних мережевих ресурсів, а також здатність підготовки даних з коригування або вибору нової політики безпеки, адекватній існуючій загрозі. Стаття направлена на пошук шляхів реалізації головних задач управління мережевою безпекою в рамках системи управління.

Мета статті: пошук шляхів реалізації головних задач управління мережевою безпекою в рамках системи управління.

Викладення основного матеріалу. Стандарти ISO з управління мережевою безпекою (ISO 7498-2, ISO 10164-7, 10164-8, 10164-9, ISO/IEC 17799:2000 та інші), а також рекомендації МСЕ – Т (X.800, M.3016.0-M.3016.4, Y.2701 та ін.) висувають ряд вимог до архітектури безпеки, механізмів її забезпечення.

Управління мережевою безпекою передбачає включення до складу 8 прикладних процесів «механізмів безпеки» (рис. 1) [1; 2].

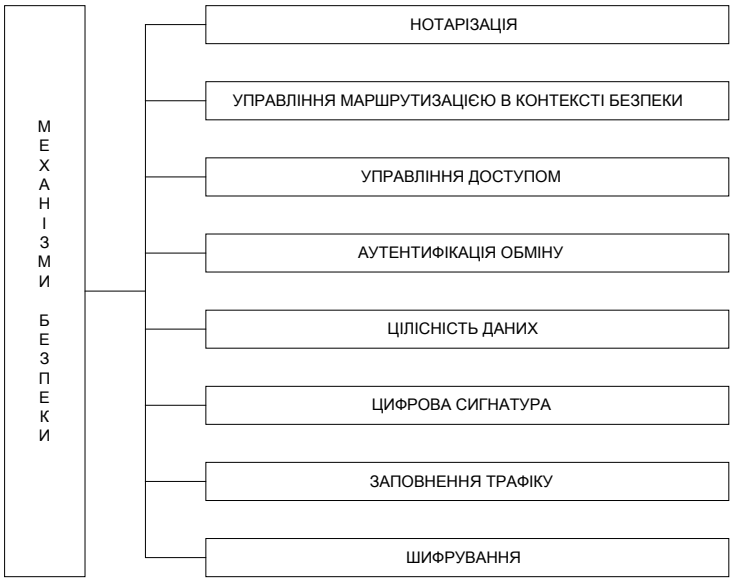


Рис. 1. Вбудовані механізми безпеки

Механізм «Нотарізація» гарантує, що третя особа для гарантії правильності інформації використовує не тільки її зміст, а також відомості про джерело інформації, хронометраж та доставку адресату.

Механізм «Управління маршрутизацією в контексті безпеки» містить правила, які дозволяють при передачі пакетів (повідомлень) уникати певних підмереж, направлень чи трактів передачі інформації з метою забезпечення заданого рівня безпеки.

Механізм «Управління доступом» використовується для запобігання несанкціонованому доступу до ресурсу мережі (якщо доступ заборонено) або запобігти використанню його несанкціонованим способом.

Механізм «Аутентифікація обміну» використовується тоді, коли ідентичність особи чи прикладного процесу повинна бути перевіреною раніше, ніж наданий доступ до певного ресурсу мережі.

Механізм «Цілісність даних» використовується, щоб гарантувати, що дані про обмін, взаємодію чи просто змінені несанкціонованим способом.

Механізм «Цифрова сигнатура» (або унікальний набір байтів) використовується для гарантії того, що отримувач даних – саме та особа, кому адресовані ці дані, і що пакет даних не був змінений чи пошкоджений. Для цього використовуються криптографічні методи захисту інформації в протокольному блоці (PDU).

Механізм «Заповнення трафіку» використовує спеціальні біти, октети чи інші блоки даних, які додаються в кінці протокольних блоків (PDU).

Механізм «Шифрування» використовується для закриття даних чи іншої інформації криптографічними методами. Функціонування підсистеми управління мережевою безпекою повинно забезпечуватися рядом служб безпеки, які підтримують прикладні процеси управління (рис. 2) [3; 4].

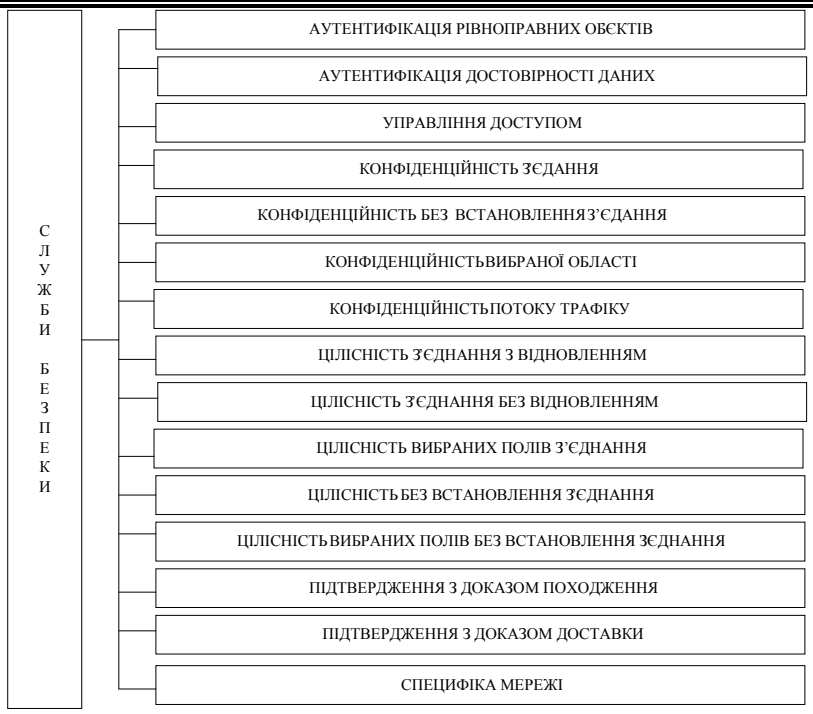


Рис. 2. Служби підсистеми управління мережевою безпекою

Служба «Аутентифікація рівноправних об’єктів» використовується для гарантування зв’язку з рівноправним об’єктом, як єдиним, що допустимий.

Служба «Аутентифікація достовірності даних» використовується для того, щоб гарантувати, що джерело даних саме те, що замовив користувач.

Служба «Управління доступом» гарантує, що несанкціонований користувач не отримає доступ до ресурсу мережі.

Служба «Конфіденційність з’єднання» гарантує, що дані N-го користувача мережі в К-му з’єднанні з М-користувачем чи з J-ресурсом мережі засекречені.

Служба «Конфіденційність без встановлення з’єднання» гарантує конфіденційність даних кожного кінцевого користувача.

Служба «Конфіденційність вибраної області» використовується, щоб забезпечити конфіденційність деяких елементів даних всередині можливих баз даних.

Служба «Конфіденційність потоку трафіку» гарантує, що буде забезпечене запобігання аналізу трафіку користувача потенційним порушенням.

Служба «Цілісність з’єднання з відновленням» гарантує, що всі дані кінцевого користувача відносно К-го з’єднання будуть захищені від змін чи вставок. Ця служба також вдається до спроб відновлення даних у випадку необхідності.

Служба «Цілісність з’єднання без відновлення» виконує ті самі функції, але без відновлення даних в цій службі.

Служба «Цілісність вибраних полів з’єднання» гарантує збереження вибраних полів всередині блоків даних послуг (SDU) шляхом захисту від змін, видання, вставки чи відтворення.

Служба «Цілісність без встановлення з’єднання» забезпечує збереження одиночного SDU відносно змін і відтворення.

Служба «Цілісність вибраних полів без встановлення з’єднання» гарантує, що вибрані поля всередині протокольного блоку даних PDU без встановлення логічного з’єднання не змінені.

Служба «Підтвердження з доказом походження» надає послугу, що забезпечує безсумнівну ідентифікацію відправника і гарантує, щоб він не зміг спростувати факт передачі даних.

Служба «Підтвердження з доказом доставки» надає відправнику даних послугу, яка гарантує, що дані були доставлені й отримувач не зможе заперечувати отримання даних.

Служба «Специфіка мережі» забезпечує адаптацію інших служб підсистеми управління мережевою безпекою до особливостей функціонування конкретної телекомунікаційної мережі мультисервісної мережі зв’язку.

Підсистема управління мережевою безпекою з одного боку є підсистемою оперативно-технічного управління, а з іншого – підсистемою системи комплексної безпеки телекомунікаційної мережі й повинна постійно взаємодіяти як з елементами системи управління, так і з засобами забезпечення безпеки (рис. 3) [5].

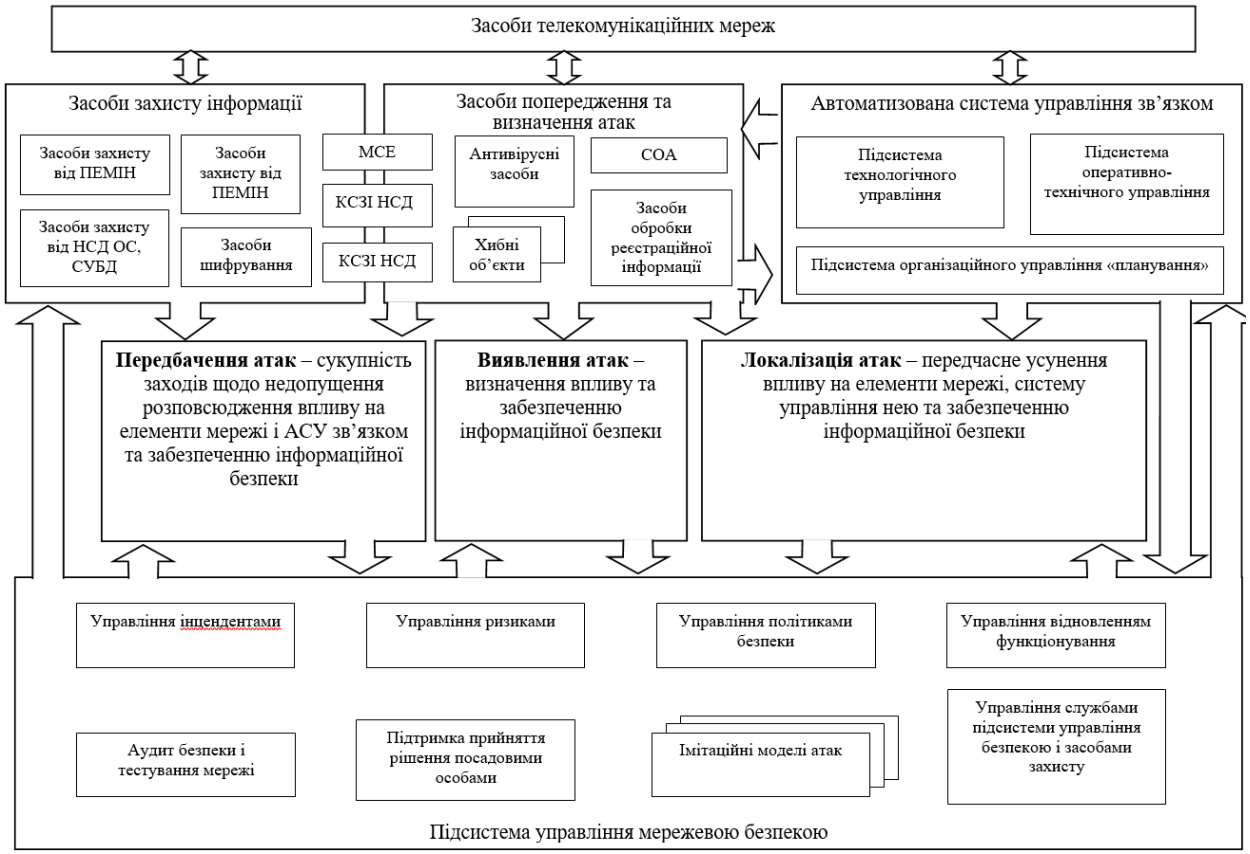


Рис. 3. Функціональна архітектура підсистеми управління мережевою безпекою

Функціонально архітектура підсистеми управління мережевою безпекою, як правило, містить різні програмно-апаратні засоби, що виконують функції управління службами підсистеми та засобами захисту, ризиками, конфліктами, політиками безпеки, відновленням функціонування мережі після впливу та атак на неї; здійснює аудит безпеки та тестування мережі, підтримку обґрунтованих рішень посадовими особами по безпеці, а також імітаційне моделювання наслідків атак і втручання потенційних порушників.

Джерелом інформації моніторингу стану мережі в контексті безпеки є дані, отримані від комплексів засобів захисту інформації від несанкціонованих дій (КЗЗІ НД), випадкових впливів та аварійних ситуацій (КЗЗІ ВВАС), від підсистеми технологічного управління, від засобів попередження та виявлення атак на елементи телекомунікаційної мережі та її систему управління (систему виявлення атак або СВА, антивірусні засоби і т. п.)

Логічна архітектура підсистеми управління мережевою безпекою складається із керуючих та керованих елементів і будується за схемами «агент – менеджер» та «клієнт – сервер» (рис. 4) [6].

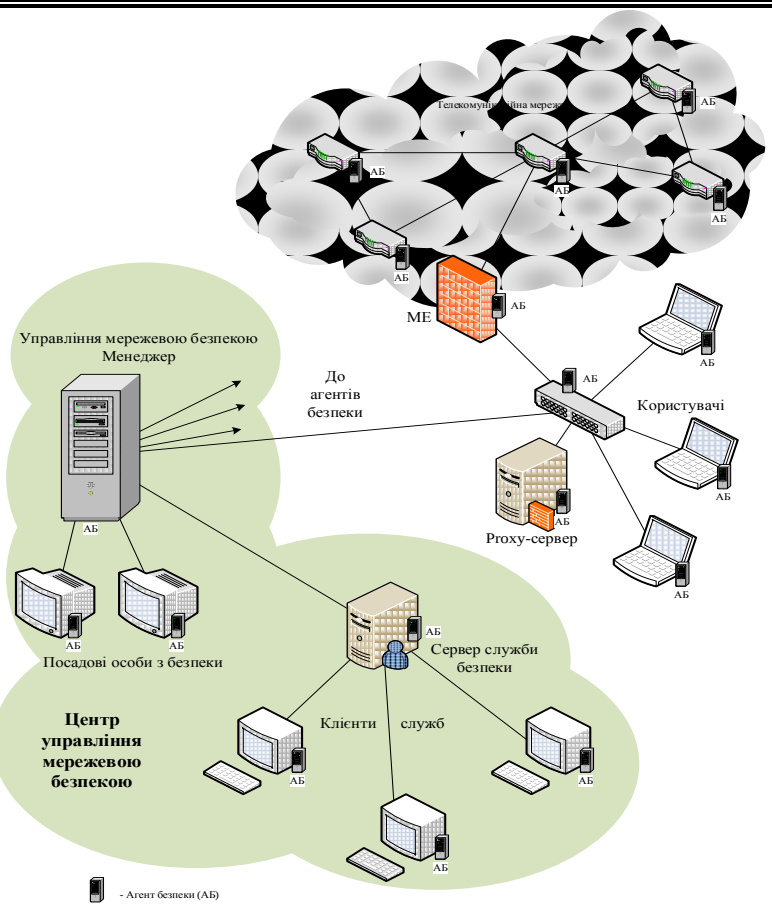


Рис. 4. Логічна архітектура підсистеми управління мережевою безпекою

Локальний агент безпеки (АБ) являє собою програму, що розміщена на кінцевому пристрої (клієнт, сервер, шлюз) та виконує наступні функції захисту:

– аутентифікація об’єктів політики безпеки, включаючи інтеграцію різних сервісів аутентифікації;
– визначення користувача в мережі та подій, пов’язаних з даним користувачем;
– забезпечення централізованого управління засобами безпеки та контролю доступу;
– управління ресурсами в інтересах додатків, підтримка управління доступом до ресурсів прикладного рівня;
– захист та аутентифікація трафіку;
– послідовне протоколювання, моніторинг, тривожна сигналізація;
– локальний антивірусний захист.

Одним із головних модулів локального агента є модуль, який інтерпретує локальну політику безпеки і розподіляє виклики між рештою модулів та компонентами.

АБ, встановлені на різних елементах мережі, направлені на захист даних та інших інформаційних ресурсів. Так, АБ, встановлений на будь-якому персональному комп’ютері, орієнтований на захист користувача, що є клієнтом в додатках «клієнт – сервер».

АБ, встановлений на сервері додатків, орієнтований на забезпечення захисту серверних компонентів розподілених додатків.

АБ, встановлений на шлюзовому комп’ютері, забезпечує розв’язку сегментів мережі всередині різних об’єктів чи між об’єктами.

Головною функцією центру управління є опис, зберігання та управління мережевою політикою безпеки в масштабі всієї мережі, трансляція мережевої політики в локальні політики безпеки пристроїв захисту, завантаження пристроїв захисту та контроль стану всіх агентів безпеки. Для організації розподіленої схеми управління безпекою в мережі може бути встановлено декілька серверів управління мережевою безпекою.

Висновок. Розглянутий варіант архітектури підсистеми управління мережевою безпекою може бути використаний при функціонуванні мультисервісних мереж з високими показниками щодо ефективності в умовах інформаційної протидії та досить жорстких вимог до них з боку різних користувачів (посадових осіб органів управління).

Ефективність функціонування підсистеми управління мережевою безпекою може бути оцінена деяким функціоналом якості, розрахунок якого буде проведено в подальших дослідженнях.

Напрями подальших досліджень: відпрацювання методики ефективності функціонування підсистеми управління мережевою безпекою.

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC 7498-2-99. Інформаційні технології. Взаємозв’язок відкритих систем. Базова еталонна модель. 4.2. Архітектура захисту інформації.

2. ДСТУ ISO/IEC 10164-7. Інформаційні технології. Взаємозв’язок відкритих систем. Адміністративне керування системами. Частина 7. Функція сповіщення за допомогою сигнального пристрою про захист. [Чинний від 01.01.2015]. Київ: Держстандарт України, 2015.

3. ДСТУ ISO/IEC 10164-8:2015. Інформаційні технології. Взаємозв’язок відкритих систем. Адміністративне керування системами . Частина 8. Функція аудиторського спостереження за безпекою. [Чинний від 01.01.2015]. Київ: Держстандарт України, 2015.

4. ДСТУ ISO/IEC 10164-9:2015. Інформаційні технології. Взаємозв’язок відкритих систем. Адміністративне керування системами. Частина 9. Об’єкти й атрибути для контролю за доступом. [Чинний від 01.01.2015]. Київ: Держстандарт України, 2015.

5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. ИД «Форум»: ИНФА – М, 2008.

6. Буренин А. Н., Винниченко А. В. Проблемы управления информационной безопасностью в процессе функционирования систем управления телекоммуникационными сетями специального назначения // Телекоммуникационные технологии. 2018. № 4. С. 12–20.

УДК 623.746 канд. техн. наук Панченко І. В. ORCID: 0000-0001-5690-3813 (ВІТІ)

АНАЛІЗ БОЙОВОГО ЗАСТОСУВАННЯ МУЛЬТИРОТОРНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ РОБОТИ СПЕЦІАЛЬНОГО ОЗБРОЄННЯ

Під час повномасштабного вторгнення росії Збройні сили України (ЗСУ) почали активно використовувати як засоби повітряної розвідки безпілотні літальні апарати (БпЛА) цивільної групи мультироторного типу (квадрокоптери). БпЛА такого типу мають зручний ***інтерфейс*** *програмного забезпечення, орієнтований на максимальну психологічну і зорову зручність для користувача. Їх пілотування можливе без спеціальної підготовки. Вони також мають низьку вартість.*

Лідером у сфері виробництва цивільних БпЛА є китайська компанія DJI. Цією компанією також розроблена система електронної ідентифікації БпЛА AeroScope. Це комплекс активного захисту, моніторингу та безпеки БпЛА.

російські військові використовують такі комплекси для знищення українських операторів, які ведуть розвідку за допомогою квадрокоптерів DJI.

У зв'язку з цим постає пріоритетне завдання розробки методики використання цивільних систем подвійного призначення в підрозділах ЗСУ.

У статті проаналізовано систему виявлення БпЛА AeroScope, її варіанти, проведена оцінка можливості дальності детекції комплексу.

На основі проведеного аналізу та розрахунків запропоновано базовий алгоритм протидії виявлення БпЛА системою AeroScope як основа методики використання мультироторних БпЛА в умовах воєнного стан.у

Ключові слова: *безпілотний літальний апарат, квадрокоптер, система моніторингу та безпеки, моніторинг.*

I. Panchenko. ANALYSIS OF THE COMBAT APPLICATION OF MULTIROTOR UAVS OF SPECIAL WEAPON WORK CONDITIONS

During the full-scale invasion of Russia, the Armed Forces of Ukraine (AFU) began to actively use unmanned aerial vehicles (UAVs) of the civilian group of multi-rotor type (quadrocopters) as means of aerial reconnaissance. UAVs of this type have a convenient software interface focused on maximum psychological and visual comfort for the user. Their piloting is possible without special training. They also have a low cost.

The Chinese company DJI is the leader in the production of civilian UAVs. This company also developed the AeroScope electronic identification system for UAVs. This is a complex of active protection, monitoring and security of UAVs.

the Russian military uses such complexes to destroy Ukrainian operators conducting reconnaissance using DJI quadcopters.

In this regard, the priority task of developing a methodology for the use of civil dual-purpose systems in the units of the Armed Forces appears.

The article analyzes the AeroScope UAV detection system, its variants, and evaluates the possibility of the complex's detection range.

Based on the analysis and calculations, a basic algorithm for countering UAV detection by the AeroScope system is proposed as the basis of the methodology for using multi-rotor UAVs in military conditions.

Keywords: *unmanned aerial vehicle, quadcopter, monitoring and security system, monitoring*.

Постановка завдання в загальному вигляді

При вирішенні завдань оснащення Збройних сил України (ЗСУ) військовою технікою забезпечення підрозділів тактичного рівня засобами індивідуальної розвідки не вважалися питанням нагальної потреби аж до початку активної фази збройної агресії росії.

В умовах військового стану і обмежених можливостей фінансування це питання стало особливо актуальним. Тому під час повномасштабного вторгнення, дякуючи небайдужим громадянам і волонтерам, в підрозділах ЗСУ рівня відділення/взвод/рота масово стали з'являтися безпілотні літальні апарати (БпЛА) цивільної групи (дрони, квадрокоптери).

Це зумовлено їхньою низькою вартістю, наявністю «юзабіліті інтерфейсу» з можливістю пілотування БпЛА без спеціальної підготовки, а також ускладненням визначення походження таких БпЛА для противника у разі їх втрати.

Засоби ураження сучасних і перспективних комплексів ППО не дозволяють забезпечувати гарантоване ураження БпЛА, особливо малошвидкісних і малорозмірних.

Для вирішення низки задач широко застосовують БпЛА (переважно – малі БпЛА) терористичні угруповання й особи, що ведуть протизаконну діяльність. Це доступ за периметр

об'єктів, що охороняються, та ведення там спостереження; точкове знищення окремих важливих осіб; закид саморобних засобів ураження; нанесення пошкоджень будівлям, пам'ятникам культури, об'єктам інфраструктури і транспортним засобам; транспортування заборонених засобів чи їх перекидання на територію, що охороняється; перешкоджання повітряному руху в аеропортах.

БпЛА цивільної групи з урахуванням технічних можливостей використовуються спеціальними підрозділами ЗСУ з метою ведення повітряної розвідки, коригування вогню артилерії, нанесення та уточнення результатів вогневого ураження, а також оцінки якості маскування позицій військ.

З початком повномасштабної агресії росії з 24 лютого 2022 року з'ясувалась нова проблема – застосування ворогом системи безпеки AeroScope. Ця система аналізу і контролю повітряного простору розроблена як технологія моніторингу БпЛА для забезпечення конфіденційності та безпеки своїх даних.

Тому виникли питання забезпечення протидії роботі таких систем ворога та розробки базових алгоритмів захисту.

Аналіз публікацій за темою дослідження

Для розробки методики протидії, з використанням літературних джерел і вебресурсів [1–6], проаналізовано будову, види, характеристики та принцип дії квадрокоптерів різних фірм-виробників та систем стеження за об'єктом.

Аналіз літератури показав, що на ринку квадрокоптерів є безліч моделей різного класу, які відрізняються тактико-технічними характеристиками і вимагають активного захисту.

Метою даної статті є висвітлення базового алгоритму протидії виявлення *БпЛА комплексом безпеки AeroScope.*

Викладення основного матеріалу

Основними виробниками цивільних БпЛА є такі компанії як DJI, Autel, SJRC та інші.

В таблиці 1 наведені види та характеристики найбільш популярних цивільних БпЛА.

Таблиця 1

Дрони	**Злітна вага,** *(г)*	**Максимальна швидкість,** *(км/год)*	**Максимальна висота зльоту,** *(м)*	**Максимальний час польоту (без вітру),** *(хв)*	**Максимальний час зависання (без вітру),** *(хв)*	**Максимальна відстань польоту (без вітру),** *(км)*	**Максимальна стійкість до швидкості вітру:** *(км/год)*
DJI MAVIC 2 PRO	907	72	6000	31	29	18	29–38
DJI MAVIC 2 ZOOM	905	72	6000	31	29	18	29–38
DJI MAVIC 2 Enterprise Advanced	909	72	6000	31	29	18	29–38
DJI MAVIC 3	89	68,4	6000	46	40	30	43,2
DJI MAVIC 3 CINE	899	68,4	6000	46	40	30	43,2
AUTEL EVO II	895	45	7000	40	35	25	61,2

У період військового протистояння збройної агресії в форматі проведення АТО/ООС з 2014 року до 24 лютого 2022 року основною проблемою використання цивільних БпЛА підрозділами оперативної ланки Збройних сил України було набуття досвіду пілотування.

З початком повномасштабної агресії росією з 24 лютого 2022 року виникла нова проблема, а саме застосування ворогом комплексу активного захисту, моніторингу та безпеки AeroScope.

Слід зазначити, що в Україні ІТ-спільнотою було розроблено власний анонімайзер «Ольга», який здатний певним чином приховувати ідентифікатори та координати зльоту БпЛА

виробництва компанії DJI. Але даний апаратно-програмний комплекс не здатний повністю вирішити питання щодо прихованого керування БпЛА, тому що є факт передачі даних за допомогою радіоканалу.

Під час проведення сучасних військових та спеціальних дій для виявлення БпЛА використовують шляхи оптичного, акустичного або радіоелектронного сканування радіоефіру. Електронна система спостереження надає інформацію про те, що БпЛА знаходиться десь поряд з оператором, але не конкретно про те, де він знаходиться і в якому напрямку летить.

Таке спостережне виявлення зазвичай є першим кроком до локалізації та ідентифікації БпЛА, щоб з'ясувати, чи є він дружнім чи ворожим.

Локалізація визначення конкретної позиції, швидкості та напряму руху безпілотника є ключем до вживання захисних заходів. Для цього використовуються радари великої та малої дальності, які допомагають збільшити час відповіді для прийняття певних контрзаходів [1].

Виробник системи AeroScope (рис. 1) – китайська компанія DJI. Основне призначення комплексу – забезпечення безпеки в районах критичної інфраструктури громадського сектору, таких як аеропорти, АЕС, державні установи, в'язниці й т. ін.

AeroScope здатний виявляти більшість популярних у світі БпЛА мультироторного типу. Комплекс ідентифікує лінії зв'язку між БпЛА та його пультом керування, відстежує та аналізує інші електронні сигнали БпЛА. Комплекс моніторингу дозволяє в режимі реального часу сканувати та відстежувати до 50 цільових БпЛА, а також їх оператора за пультом керування, визначати їх геолокації, висоту, напрямок руху, швидкість, модель і навіть серійний номер [2].

Російські військові використовують комплекси AeroScope компанії DJI для знищення українських операторів, які ведуть розвідку за допомогою квадрокоптерів DJI.

На даний час відомо про розробку DJI трьох варіантів комплексу AeroScope: AeroScope G-16, AeroScope G-8 та DJI AeroScope Mobile. Перші два комплекси – це стаціонарні рішення. Їх головна відмінність – радіус дії.

Третій варіант є мобільним/переносним рішенням.

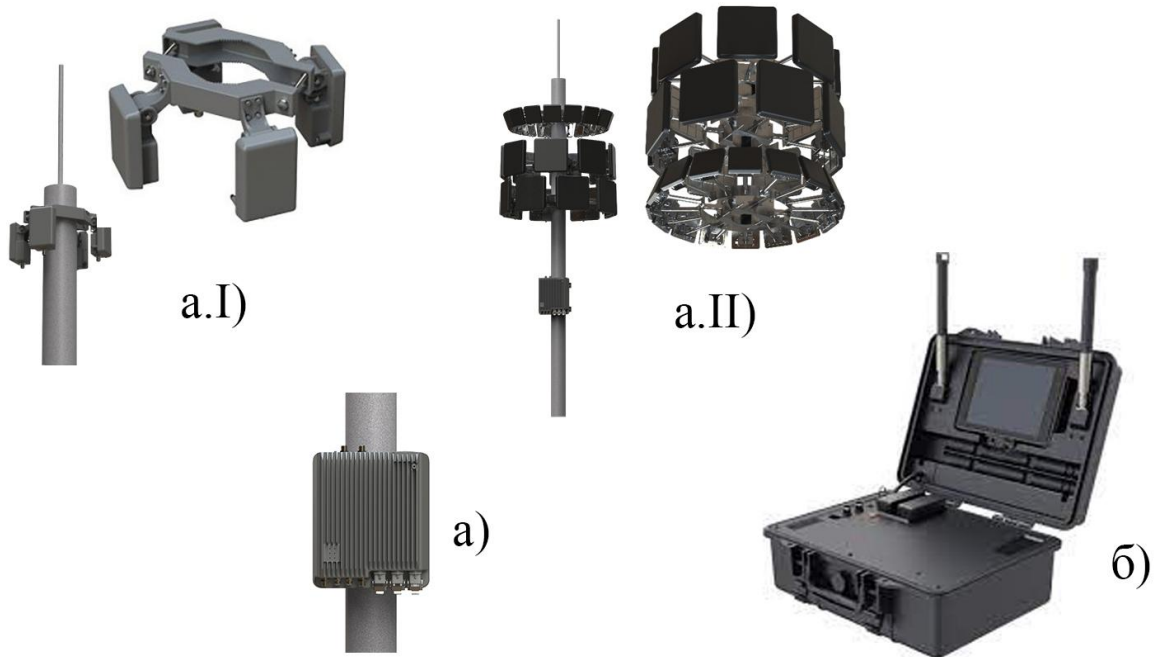


Рис. 1. Комплекс активного захисту, моніторингу та безпеки AeroScope:
а – стаціонарний комплект (*а.I* – G-8; *а.II* – G-16); *б* – мобільний комплект

Відомо, що 15 березня найбільш потужна стаціонарна система AeroScope G-16 була встановлена російськими військами в чорнобильській зоні відчуження [3].

Дальність виявлення AeroScope залежить, в першу чергу, від відкритості рельєфу в місці установки, рівня перешкод у районі моніторингу, ступеня посилення сигналу (ненаправлена

антена = 0dB, G8 = 8dB), спрямованості антени та типу протоколу передачі даних (OcuSync, LightBridge (LB/LB2), IEEE 802.11b/g (Wi-Fi)), що використовується БпЛА.

Було проведено оцінку можливості дальності детекції об'єктів, завдяки існуючій теоретичній формулі розрахунку втрат даних у вільному просторі (P_L):

$$P_L = \left(\frac{\lambda}{4\pi R} \right)^2 . \quad (1)$$

Знайдемо

$$S_N = \frac{P_{EIR} + R_x G + P_L}{k_n + k_з}, \quad (2)$$

де P_{EIR} – еквівалентна ізотропна випромінювана потужність є добутком потужності радіочастотного сигналу, який підводиться до антени, на абсолютний коефіцієнт підсилення антени R_xG:

$$R(dB) = \frac{R_x - 22 - (k_n + k_з) - S_N}{2} . \quad (3)$$

Враховуючи, що R_xG = 8 dB для 2,4 ГГц антени G8, k_n – поправочний коефіцієнт, який становить від 0 до 9 dB; $k_з$ – коефіцієнт впливу завад, що вимірюються в Assistense2 для AeroScope, маємо:

$$R = \frac{1 - k_з}{2}$$, коли k_n=0 та S_N = -7 для SDR

та

$$R = \frac{-8 - k_з}{2}$$, коли k_n=9 та S_N = -7 для SDR.

Параметри протоколів, що використовуються для зв'язку, наведені в таблиці 2.

Таблиця 2

Параметри протоколів передачі даних

	IEEE 802.11b/g (WiFi)	**LightBridge (LB/LB2)**	**DJI OcuSync**
S_N *(dB)*	0	-2	-7
BW (МГц)	5	10	10

де *BW* – смуга пропускання, МГц.

Отримані дані впливу завад на відстань детекції системи AeroScope наведені в таблиці 3.

Таблиця 3

Вплив завад на відстань детекції

Завади(вимірюються в Assistense 2 для AeroScope)	**Протокол IEEE 802.11 b/g (WiFi)**		**Протокол LightBridge (LB/LB2)**		**Протокол DJI OcuSync**	
	K_n **= 0**	K_n **= 9**	K_n **= 0**	K_n **= 9**	K_n **= 0**	K_n **= 9**
-102	28 км	8 км	25 км	14 км	47 км	17 км
-96	14 км	4 км	13 км	5 км	24 км	9 км
-90	7 км	2 км	7 км	3 км	12 км	4,5 км
-84	15 км	1 км	3,5 км	1,5 км	6 км	2,3 км
-78	1800 м	500 м	1800 м	800 м	3 км	1,2 км

Розрахунки опосередковано підтверджуються відомими даними з тактико-технічних характеристик [2], з яких знаємо, що стаціонарний комплекс моніторингу БпЛА AeroScope G-16

може виявляти БпЛА на відстані до 50 км. Також підтверджено, що в деяких випадках відстань спрацьовування радара становила близько 160 км.

За даними аналітичної компанії Gartner у 2020 році DJI поставила в росію 200 комплексів AeroScope [4].

При цьому Збройні сили України не можуть використовувати наявні комплекси AeroScope в зв'язку з тим, що майже всі комплекси AeroScope, які до 24 лютого 2022 року були поставлені в Україну, перестали працювати всюди, де їх використовували, включаючи атомні електростанції. Зникла й технічна можливість під'єднати нові пристрої.

росіяни використовують в Україні розширену версію системи DJI AeroScope з радіусом дії 50 км, привезену із Сирії, для цілевказання власним ракетам. Артудари російських військ по точках старту квадрокоптерів DJI є не поодинокими і мають цілеспрямований і масовий характер [5].

Враховуючи, що українська армія здебільшого звертає увагу на досвід західних країн, не дивлячись на те, що 24 квітня 2022 року компанія DJI зробила офіційну заяву про тимчасове призупинення будь-якої підприємницької діяльності в росії та Україні [6], загроза використання прихованого механізму контролю і відключення БпЛА, закладеного на рівні виробника, зберігається. Тому постає як пріоритетне завдання розробка методики використання цивільних систем подвійного призначення в підрозділах Збройних сил України.

Дії, які пропонуються використовувати за базовий алгоритм при роботі з цивільними БпЛА:

1. Для можливості роботи з укриття провести модернізацію пультового обладнання (рис. 2) за рахунок обладнання виносними антенами, з фідером довжиною 10 метрів або більше.

У такий схемі необхідно враховувати можливі втрати в кабелі і для компенсації втрат необхідно використовувати підсилювач сигналу для недопущення зменшення потужності та, як наслідок, зменшення дальності взаємодії пілота та БпЛА.

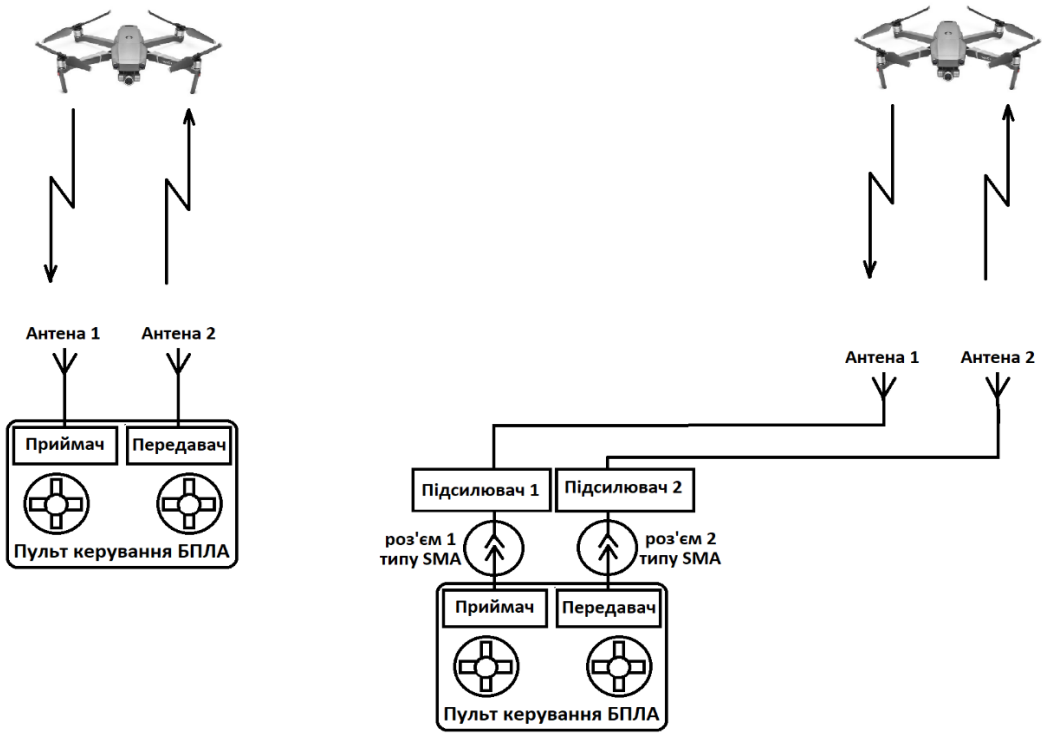
2. Використання пристрою в режимі виконання завдання «планування місії» польотного завдання без використання активних систем позиціонування.

3. Використання програмного забезпечення, що змінює геолокацію оператора та БпЛА, наприклад fakeGPS.

4. Не нехтувати правилами роботи оператора в умовах дій ворожої системи РЕР.

Для зменшення впливу використання радарів типу DJI AeroScope до мінімуму та унеможливлення ураження пілотів пропонується дотримання наступних правил пілотування:

- ніколи не проводити посадку БпЛА у місці зльоту. Чим далі приземлення від точки зльоту, тим краще;
- не повторювати одне й теж польотне завдання з використанням одного й того же маршруту двічі й більше разів. Обов'язкове використання різних точок зльоту та точок посадки для кожного польотного завдання. Пам'ятаємо, що AeroScope зберігає базу польотів і може спрацювати на випередження, якщо проаналізувати попередні польоти;
- обов'язково відключаємо геолокацію на телефоні/планшеті. Або використовуємо планшет без GPS. Наприклад, планшет серії ipad mini без SIM-карти і тільки з Wi-Fi. В ньому є тільки режим A-GPS, що не є повноцінним GPS;
- після зльоту необхідно відійти як можна далі від точки зльоту. За можливості, використання номера обслуги як «стартера» для запуску, в той момент коли оператор знаходиться на віддаленні. Після запуску БпЛА помічник відразу відходить до безпечного місця. Пам'ятаємо, що радар бачить включення БпЛА;
- проведення посадки БпЛА «на руку», швидке вимкнення і відхід до безпечного місця.



а) *б)*

Рис. 2. Модернізація пульта керування БпЛА для можливості віддаленого керування з укриття: *а* – типова схема керування БпЛА; *б* – варіант модифікації для роботи з укриття

Додатково, враховуючи сучасний стан озброєння ЗСУ розвідувальними БпЛА, підрозділів ЗСУ оперативної ланки та необхідність використання цивільних систем БпЛА при відсічі збройної агресії, необхідно зробити глобальні **висновки.**

Висновки:

1. Використання цивільних БпЛА вимагає проведення додаткових випробувань та збору даних про виявлення, відстеження, ідентифікацію та технології боротьби з БпЛА.

2. Недосконаліть існуючих процедур із закупівлі озброєння та військової техніки для ЗСУ призводить до ризику навмисного блокування ворогом при закупівлі критичних для війська товарів, що відповідають STANAG та вимогам безпеки, за рахунок використовування відкритості процедур та звичних йому методів гібридного впливу.

3. Виробники військової техніки повинні розділяти відповідальність за сприяння в обмеженні доступу до систем контролю вразливих об’єктів для польотів.

ЛІТЕРАТУРА

1. Панченко І. В., Восколович О. І., Колтовсков Д. Г., Бернацький А. П., Слотвінська Л. І., Петрова Д. В. Основи теорії і практики використання безпілотних авіаційних комплексів ретрансляторів: навч. посіб. Київ: ВІТІ, 2021. 248 с.
2. DJI Aeroscope // DJI. URL: https://www.dji.com/aeroscope.
3. Як китайський виробник квадрокоптерів DJI може допомагати РФ у війні // Texty.org.ua: незалежне онлайн-видання. URL: https://texty.org.ua/fragments/106162/yak-kytajskyj-vyrobnyk-kvadrokopteriv-dji-mozhe-dopomahaty-rf-u-vijni-rozsliduvannya-ep/.
4. Gartner: website. URL: https://www.gartner.com/en/documents/delivery-large-batch-radar-systems-russia.
5. Дрони на війні, або Як виробник квадрокоптерів DJI може допомагати РФ // Broadcast: електронний журнал. URL: https://broadcast.net.ua/uk/tech-articles/6342-droni-na-vijni-abo-yak-virobnik-kvadrokopteriv-dji-mozhe-dopomagati-rf-u-vijni.
6. DJI Reassesses Sales Compliance Efforts In Light Of Current Hostilities // DJI. URL: https://www.dji.com/newsroom/news/dji-statement-on-sales-compliance-efforts.
7. E-Katalog: вебсайт. URL: https://ek.ua/list/943/dgi/.
8. E-Katalog: вебсайт. URL: https://ek.ua/ua/ek-list.php.brands (autel).

УДК 004.056.5
канд. техн. наук Самойлов І. В. ORCID: 0000-0002-8251-9257 (ІСЗЗІ КПІ)
д-р техн. наук Чевардін В. Є. ORCID: 0000-0002-1070-4568 (ВІТІ)
канд. техн. наук Конотопець М. М. ORCID: 0000-0002-6963-1877 (ІСЗЗІ КПІ)
канд. техн. наук Сторчак А. С. ORCID: 0000-0002-5267-3122 (ІСЗЗІ КПІ)

ПОСЛІДОВНИЙ МЕТОД НАСТРОЙКИ НЕЧІТКИХ ВІДНОШЕНЬ ІНТЕРВАЛЬНОГО ТИПУ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

На сьогодні актуальною науково-технічною проблемою є створення систем оцінки захищеності інформаційних систем від загроз, які можуть опрацьовувати нечітку інформацію. Дані систем дозволяють визначати, які дії ефективні для мінімізації та попередження загроз. Нечітка модель будується на основі композиційного правила виведення Заде, в якому носієм інформації є матриця нечітких відношень „загрози – збитки", що зв'язує вектор мір значимості загроз і вектор мір значимості збитків. При проєктуванні подібних систем на базі нечітких відношень необхідно визначати множину її параметрів (Ω_I – множина параметрів, які визначають модель системи на базі нечітких відношень I типу, та Ω_{II} – множина параметрів, які визначають модель системи на базі нечітких відношень II типу). На сьогоднішній день для настройки нечітких систем інтервального типу використовується незалежний метод, який передбачає визначення множини Ω_{II} з „нуля", не використовуючи результати настройки множини параметрів Ω_I, що призводить до збільшення часу настройки.

У статті запропоновано послідовний метод настройки нечітких відношень інтервального типу, який передбачає спочатку визначення множини параметрів нечітких відношень I типу за допомогою генетико-нейронного алгоритму, а потім на їх базі настройку тільки додаткових параметрів, що дозволяє зменшити середній час настройки нечіткої моделі та оцінити вплив невизначеності на точність оцінки.

Ключові слова: *нейро-нечітка мережа, нейронна мережа, невизначеність, нечіткі відношення, нечіткі множини, інтервальна функція належності, загрози, збитки.*

I. Samoylov, V. Chevardin, N. Konotopets, A. Storchak. A sequential method of tuning interval-type fuzzy relations for assessing the security of information systems.

Today, an urgent scientific and technical problem is the creation of systems for assessing the security of information systems from threats that can process fuzzy information. These systems allow you to determine what actions are effective to minimize and prevent threats. The fuzzy model is built on the basis of the Zadeh compositional inference rule, in which the information carrier is the matrix of fuzzy "threat-damage" relations connecting the vector of measures of the significance of threats and the vector of measures of significance of damage. When designing such systems based on fuzzy relations, it is necessary to determine a set of its parameters (Ω_I - a set of parameters that determine a system model based on fuzzy relations of type I and Ω_{II} - a set of parameters that define a system model based on fuzzy relations of type II). To date, for tuning interval-type fuzzy systems, an independent method is used, which assumes the determination of the set Ω_{II} from "zero", without using the results of tuning the set of parameters Ω_I, which leads to an increase in the setup time.

The article proposes a sequential method for adjusting fuzzy relations of interval type, which firstly provides for the determination of a set of parameters of fuzzy relations of type I using a genetic-neural algorithm, and then, on their basis, adjustment of only additional parameters, which makes it possible to reduce the average tuning time of a fuzzy model and assess the effect of uncertainty on the accuracy of the assessment.

Keywords: *neural-fuzzy network, neural network, uncertainty, fuzzy relations, fuzzy sets, interval membership function, threats, losses.*

Постановка завдання. На сьогодні актуальною науково-технічною проблемою є створення систем оцінки захищеності інформаційних систем від загроз, які можуть опрацьовувати нечітку інформацію. Дані систем дозволяють визначати, які дії ефективні для мінімізації та попередження загроз. На основі аналізу захищеності можна прогнозувати можливий збиток від реалізації загрози, його оцінку та рекомендувати необхідні дії. У базах знань таких систем міститься не тільки кількісна інформація, що характеризує стан інформаційної системи, а й якісна інформація, яка являє собою експертні оцінки. Для формалізації експертної інформації при моделюванні причинно-наслідкових зв'язків зручно використовувати теорію нечітких множин [1; 2]. Нечітка модель будується на основі композиційного правила виведення Заде [3], в якому носієм інформації є матриця нечітких відношень „загрози – збитки", що зв'язує вектор мір значимості загроз і вектор мір значимості збитків.

Аналіз останніх публікацій. При проєктуванні систем оцінки захищеності інформаційних систем від загроз виникає проблема моделювання і мінімізація наслідків невизначеності.

В роботах [4–6] розглядаються методичні аспекти побудови нечітких систем, що здатні оперувати з різними типами невизначеності. В нечітких системах I типу використовуються точні функції належності, коли ступінь належності є чітким числом, тобто невизначеність, щодо значень слів, повністю ігнорується. В нечітких системах II типу з'являється можливість моделювати невизначеність, пов'язану зі значенням слів за рахунок введення інтервальних функцій належності. Останні дозволяють оперувати з різними видами невизначеності, що виникають в реальних системах оцінки захищеності інформаційних систем.

У загальному випадку, при проєктуванні подібних систем на базі нечітких відношень, необхідно визначити множину її параметрів. Нехай: Ω_{I} – множина параметрів, які визначають модель системи на базі нечітких відношень I типу (параметри функцій належності вхідних (вихідних) змінних до нечітких термів загроз (збитків) та параметри концентрації функцій належності нечітких множин збитків); Ω_{II} – множина параметрів, які визначають модель системи на базі нечітких відношень II типу (параметри нижніх і верхніх функцій належності вхідних (вихідних) змінних до нечітких термів загроз (збитків) та параметри концентрації нижніх і верхніх функцій належності нечітких множин збитків, що задають інтервали значень нечітких відношень). Між множинами Ω_{I} та Ω_{II} згідно з [4] виконується співвідношення: $\Omega_{\text{I}} \subset \Omega_{\text{II}}$, тобто при проєктуванні систем II типу використовуються додаткові параметри Ω'. Для настройки нечітких систем II типу в роботі [4] використовується *незалежний метод*, який передбачає визначення множини Ω_{II} з „нуля", не використовуючи результати настройки множини параметрів Ω_{I} нечіткої системи I типу, що призводить до збільшення часу настройки.

Мета роботи. Запропонувати *послідовний метод* настройки, який передбачає спочатку визначення множини параметрів Ω_{I}, а потім на їх базі настройку тільки додаткових параметрів Ω', що дозволить зменшити середній час настройки нечіткої моделі та оцінити вплив невизначеності на точність оцінки захищеності інформаційних систем.

Виклад основного матеріалу. Нехай навчальна вибірка задана у вигляді M пар експериментальних даних:

$$\left\langle \hat{X}_p, \hat{Y}_p \right\rangle,\ p = \overline{1, M},$$

де $\hat{X}_p = \left(\hat{x}_1^p, \hat{x}_2^p, \ldots, \hat{x}_n^p\right)$ – вектор значень вхідних змінних в експерименті номер p;

$\hat{Y}_p = \left(\hat{y}_1^p, \hat{y}_2^p, \ldots, \hat{y}_m^p\right)$ – вектор значень вихідних змінних в експерименті номер p.

Припустимо, що $\tilde{s}_j,\ j = \overline{1,\ m}$ – деякий збиток, який розглядається як нечітка множина II типу. Нечітка множина, за допомогою якої формалізується терм $\tilde{s}_j$, являє собою сукупність пар: $\tilde{S}_j = \left\{ \frac{\mu_1^{\tilde{s}_j}}{d_1}, \frac{\mu_2^{\tilde{s}_j}}{d_2}, \cdots, \frac{\mu_n^{\tilde{s}_j}}{d_n} \right\}$, де $\{d_1,\ d_2,\ \ldots,\ d_n\} = D$ – універсальна множина загроз, на якій задається нечітка множина $\tilde{s}_j$; $\mu_i^{\tilde{s}_j}$ – вторинна функція належності елемента $d_i \in D,\ i = \overline{1,\ n}$ нечіткій множині $\tilde{s}_j$ [7].

Нехай $\underline{Q} = \left(\underline{q}_1, \underline{q}_2, \ldots, \underline{q}_m\right)$ і $\overline{Q} = \left(\overline{q}_1, \overline{q}_2, \ldots, \overline{q}_m\right)$ – вектори параметрів концентрації нижніх і верхніх функцій належності збитків $\tilde{s}_j$ такі, що матриця нечітких відношень має вигляд:

$$R = \begin{bmatrix} \left[\underline{r}_{11}^{\underline{q}_1}, \overline{r}_{11}^{\overline{q}_1}\right] & \left[\underline{r}_{12}^{\underline{q}_2}, \overline{r}_{12}^{\overline{q}_2}\right] & \ldots & \left[\underline{r}_{1m}^{\underline{q}_m}, \overline{r}_{1m}^{\overline{q}_m}\right] \\ \left[\underline{r}_{21}^{\underline{q}_1}, \overline{r}_{21}^{\overline{q}_1}\right] & \left[\underline{r}_{22}^{\underline{q}_2}, \overline{r}_{22}^{\overline{q}_2}\right] & \ldots & \left[\underline{r}_{2m}^{\underline{q}_m}, \overline{r}_{2m}^{\overline{q}_m}\right] \\ \ldots & \ldots & \ldots & \ldots \\ \left[\underline{r}_{n1}^{\underline{q}_1}, \overline{r}_{n1}^{\overline{q}_1}\right] & \left[\underline{r}_{n2}^{\underline{q}_2}, \overline{r}_{n2}^{\overline{q}_2}\right] & \ldots & \left[\underline{r}_{nm}^{\underline{q}_m}, \overline{r}_{nm}^{\overline{q}_m}\right] \end{bmatrix}. \qquad (1)$$

З урахуванням матриці (1) співвідношення, яке визначає залежність „загрози – збитки" для нечіткої системи діагностики ІІ типу, можна записати в такому вигляді:

$$Y = f\left(X,\, C_X\,,\, P_{\tilde{D}},\, Q_{\tilde{R}},\, P_{\tilde{S}}\right), \tag{2}$$

де X – множина вхідних змінних;

Y – множина вихідних змінних;

$P_{\tilde{D}} = \left(\underline{G}_{\tilde{D}},\, \overline{G}_{\tilde{D}},\, C_{\tilde{D}}\right)$ – вектори параметрів нижніх і верхніх функцій належності вхідних змінних до нечітких термів загроз;

$P_{\tilde{S}} = \left(\underline{G}_{\tilde{S}},\, \overline{G}_{\tilde{S}},\, C_{\tilde{S}}\right)$ – вектори параметрів нижніх і верхніх функцій належності вихідних змінних до нечітких термів збитків;

C_X – вектор параметрів концентрації функцій належності, що моделюють неточність вхідних змінних.

Задача настройки нечітких відношень інтервального типу може бути сформульована так: необхідно підібрати такі вектори параметрів нижніх і верхніх функцій належності вхідних (вихідних) змінних та параметрів концентрації нижніх і верхніх функцій належності збитків, а при наявності неточних вхідних даних і вектори параметрів концентрації функцій належності, що моделюють цю неточність, які забезпечують мінімальну відстань між теоретичними і експериментальними виходами об'єкта:

$$\sum_{p=1}^{M}\left[\sum_{j=1}^{m}\left[f_j\left(\hat{X}_p,\, C_X\,,\, P_{\tilde{D}},\, Q_{\tilde{R}},\, P_{\tilde{S}}\right) - \hat{y}_j^{\,p}\right]^2\right] = \min_{C_X\,, P_{\tilde{D}}, Q_{\tilde{R}}, P_{\tilde{S}}}. \tag{3}$$

В роботі для настройки нечітких відношень інтервального типу пропонується використовувати послідовний метод, суть якого полягає в тому, що настройка таких нечітких відношень здійснюється не з нуля, а використовується результат настройки нечітких відношень І типу. В даному випадку на другому етапі пропонується використовувати нейро-мережевий метод [8; 9]. Етапи настройки приведені в табл. 1, перші три рядки якої відповідають генетико-нейронному етапу настройки нечітких відношень І типу [10]. На другому етапі при розв'язанні задачі оптимізації (3) до вектора параметрів додаються вектори нижніх та верхніх границь координат максимуму функцій належності $\underline{G}_{\tilde{D}}$, $\overline{G}_{\tilde{D}}$, $\underline{G}_{\tilde{S}}$, $\overline{G}_{\tilde{S}}$ та нижніх і верхніх границь параметрів концентрації $\underline{Q}_R$, $\overline{Q}_R$. Параметри концентрації функцій належності $C_{\tilde{D}}$ та $C_{\tilde{S}}$ залишаються без змін. У випадку наявності вхідних даних з відомим середнім відхиленням до вектора змінних, що настроюються, додаються вектори параметрів концентрації функцій належності, що моделюють неточність вхідних даних C_X.

Таблиця 1

Етапи настройки нечітких відношень інтервального типу

Модель		Параметри настройки			Кількість параметрів настройки	Метод
		Вхідні змінні	Вихідні змінні	Нечіткі відношення		
Точні ФН	Точні вхідні дані	G_D	G_S	Q_R	$n + m$	Генетичний алгоритм
		G_D, C_D	G_S, C_S	Q_R	$2n + 3m$	Нейронна мережа
	Неточні вхідні дані	G_D, C_D, C_X	G_S, C_S	Q_R	$3n + 3m$	
ФН інтервального типу	Точні вхідні дані	$\underline{G}_{\tilde{D}}, \overline{G}_{\tilde{D}}, C_{\tilde{D}}$	$\underline{G}_{\tilde{S}},\ \overline{G}_{\tilde{S}}, C_{\tilde{S}}$	$\underline{Q}_R,\ \overline{Q}_R$	$4n + 4m$	
	Неточні вхідні дані	$\underline{G}_{\tilde{D}}, \overline{G}_{\tilde{D}}, C_{\tilde{D}}, C_X$	$\underline{G}_{\tilde{S}},\ \overline{G}_{\tilde{S}}, C_{\tilde{S}}$	$\underline{Q}_R,\ \overline{Q}_R$	$5n + 4m$	

На рис. 1 представлена структура інтервальної нейро-нечіткої мережі, а зміст вузлів показаний в табл. 2.

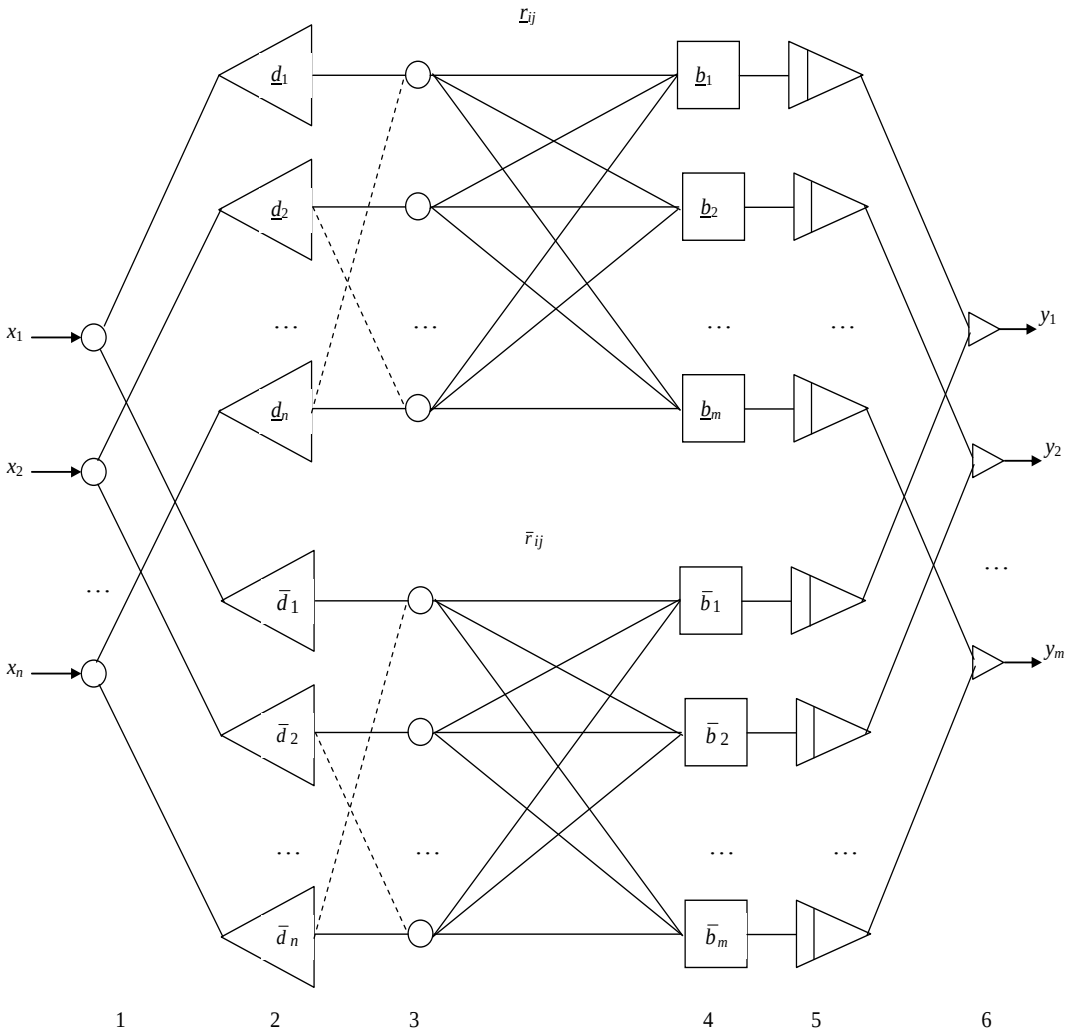


Рис. 1. Структура інтервальної нейро-нечіткої мережі

З рисунка видно, що інтервальна нейро-нечітка мережа складається з нижнього і верхнього фрагментів, що використовують нижні і верхні функції належності вхідних змінних та нижні і верхні границі нечітких відношень відповідно. Нейро-нечітка модель на рис. 1 отримана шляхом імплантації матриць нечітких відношень в нейронну мережу таким чином, що вагами дуг, які підлягають настроюванню, є нижні і верхні границі нечітких відношень. Представлена нейро-нечітка мережа має шість шарів: шар 1 – входи об'єкта; шар 2 (3) – нечіткі терми загроз $\mu^{\tilde{d}_i}$, $i=\overline{1,n}$, або їх комбінація; шар 4 – нечіткі терми збитків $\mu^{\tilde{s}_j}$, $j=\overline{1,m}$; шар 5 – операція пониження типу, тобто перехід від нечіткої множини II типу до нечіткої множини I типу; шар 6 – операція дефазифікації, тобто перетворення результатів нечіткого логічного виведення в чітке число.

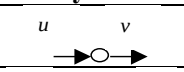
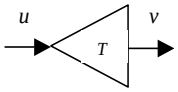
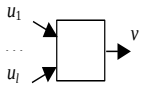
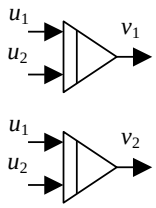
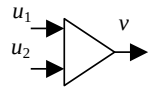
Число вузлів в шарах 2, 3, 4, 5 нейро-нечіткої мережі подвоюється, оскільки інтервальна нейро-нечітка мережа складається з двох частин, що відповідають верхній і нижній мережам I типу і визначають верхню та нижню границі ступеня належності вихідної нечіткої множини.

Дуги графа на рис. 1 зважені таким чином: нижніми і верхніми функціями належності входів до нечітких термів загроз – дуги між 2-м і 3-м шарами; нижнім і верхнім границями нечітких відношень – дуги між 3-м і 4-м шарами; нижніми і верхніми функціями належності виходів до нечітких термів збитків – дуги між 4-м і 5-м шарами. Ваги дуг між іншими шарами дорівнюють одиниці.

Суть настройки нейро-нечіткої мережі інтервального типу полягає в підборі таких ваг дуг (параметрів нижніх і верхніх функцій належності вхідних (вихідних) змінних, параметрів концентрації нижніх і верхніх нечітких множин збитків), які мінімізують різницю між теоретичними і експериментальними виходами об'єкта.

Таблиця 2

Елементи інтервальної нейро-нечіткої мережі

Вузол	**Назва**	**Функція**	
	Вхід	$v = u$	
	Нечіткий терм загрози	$v = \mu^T(u)$ $v = \sup[\min(\mu^*(u), \mu^T(u))]$	
	Нечіткий терм збитку	$v = \mu^{s_j} \max\limits_{i=1,n}(u_i)$	
	Пониження типу	для лівої границі	для правої границі
		$v_1 = \dfrac{\sum\limits_{k=1}^{N} y_j^k h_k^l}{\sum\limits_{k=1}^{L(X)} u_1 + \sum\limits_{k=L(X)+1}^{N} u_2}$ $h_k^l = \begin{cases} u_2, & \text{ÿêùî} \quad k \le L(X) \\ u_1, & \text{ÿêùî} \quad k > L(X) \end{cases}$	$v_2 = \dfrac{\sum\limits_{k=1}^{N} y_j^k h_k^r}{\sum\limits_{k=1}^{R(X)} u_1 + \sum\limits_{k=R(X)+1}^{N} u_2}$ $h_k^r = \begin{cases} u_2, & \text{ÿêùî} \quad k \le R(X) \\ u_1, & \text{ÿêùî} \quad k > R(X) \end{cases}$
	Дефазифі-кація	$v = \dfrac{u_1 + u_2}{2}$	

Розглянемо задачу оптимізації (3). В цьому випадку для настройки параметрів моделі *F* використовується система рекурентних співвідношень:

$$\underline{q}_j(t+1) = \underline{q}_j(t) - \eta_q \frac{\partial E_t}{\partial \underline{q}_j(t)}; \qquad \overline{q}_j(t+1) = \overline{q}_j(t) - \eta_q \frac{\partial E_t}{\partial \overline{q}_j(t)};$$

$$\underline{g}^{\tilde{d}_i}(t+1) = \underline{g}^{\tilde{d}_i}(t) - \eta_g \frac{\partial E_t}{\partial \underline{g}^{\tilde{d}_i}(t)}; \qquad \overline{g}^{\tilde{d}_i}(t+1) = \overline{g}^{\tilde{d}_i}(t) - \eta_g \frac{\partial E_t}{\partial \overline{g}^{\tilde{d}_i}(t)};$$

$$c^{\tilde{d}_i}(t+1) = c^{\tilde{d}_i}(t) - \eta_c \frac{\partial E_t}{\partial c^{\tilde{d}_i}(t)};$$

$$\underline{g}^{s_j}(t+1) = \underline{g}^{s_j}(t) - \eta_g \frac{\partial E_t}{\partial \underline{g}^{s_j}(t)}; \qquad \overline{g}^{s_j}(t+1) = \overline{g}^{s_j}(t) - \eta_g \frac{\partial E_t}{\partial \overline{g}^{s_j}(t)};$$

$$c^{s_j}(t+1) = c^{s_j}(t) - \eta_c \frac{\partial E_t}{\partial c^{s_j}(t)}, \tag{4}$$

які мінімізують критерій

$$E_t = \frac{1}{2}\left(f_j(t) - \hat{y}_j(t)\right)^2,$$

де $f_j(t)$, $\hat{y}_j(t)$ – теоретичний і експериментальний виходи об'єкта оцінки на *t*-ому кроці настройки;

$\underline{q}_j(t)$, $\overline{q}_j(t)$ – нижнє і верхнє значення параметра концентрації функції належності збитку на *t*-ому кроці настройки;

$\underline{g}^{\tilde{d}_i}(t)$, $\overline{g}^{\tilde{d}_i}(t)$, $c^{\tilde{d}_i}(t)$ – параметри функцій належності вхідних змінних до нечітких термів загроз на *t*-ому кроці настройки;

$\underline{g}^{\tilde{s}_j}(t)$, $\overline{g}^{\tilde{s}_j}(t)$, $c^{\tilde{s}_j}(t)$ – параметри функцій належності вихідних змінних до нечітких термів збитків на *t*-ому кроці настройки;

η_g, η_c, η_w – параметри настройки.

Якщо враховувати неточність вхідних даних, то до системи рекурентних співвідношень (4) слід додати співвідношення: $c_i^*(t+1) = c_i^*(t) - \eta_c \frac{\partial E_t}{\partial c_i^*(t)}$, де $c_i^*(t)$ – параметр концентрації функцій належності вхідних змінних на *t*-ому кроці настройки.

Аналогічно правилу „back-propagation", алгоритм навчання нейро-нечіткої мережі інтервального типу складається з двох фаз. На першій фазі обчислюються модельні значення виходів об'єкта оцінки (f_1, f_2, …, f_m), що відповідають заданій архітектурі мережі. На другій фазі обчислюється значення нев'язки (E_t) і перераховуються ваги міжнейронних зв'язків (4).

Висновки. Таким чином, для настройки нечітких відношень інтервального типу пропонується використовувати послідовний метод, який передбачає спочатку визначення множини параметрів нечітких відношень I типу за допомогою генетико-нейронного алгоритму, а потім на їх базі настройку тільки додаткових параметрів, що дозволяє зменшити середній час настройки нечіткої моделі та оцінити вплив невизначеності на точність оцінки. Результати експериментів доводять, що використання інтервальних нечітких відношень і функцій належності II типу дозволяють мінімізувати наслідки невизначеності через неточні навчальні вибірки.

Напрямом подальших досліджень є удосконалення послідовного методу настройки нечіткої моделі за рахунок вибору іншої системи нечітких термів, що описують загрози і збитки, що можливо дозволить зменшити середній час настройки та оцінити вплив невизначеності на точність оцінки.

ЛІТЕРАТУРА

1. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. Винница: УНІВЕРСУМ-Вінниця, 1999. 320 с.

2. Минаев Ю. Н., Филимонова О. Ю. Методы и алгоритмы решения задач идентификации и прогнозирования в условиях неопределенности в нейросетевом логическом базисе. Москва: Горячая линия – Телеком, 2003.

3. Заде Л. Понятие лингвистической переменной и её применение к принятию приближенных решений. Москва: Мир, 1976. 167 с.

4. Mendel J. Uncertain Rule-Based Fuzzy Logic Systems: Introduction and New Direction. Prentice Hall PTR, USA. 2001. 520 p.

5. Mordeson J. N. Fuzzy Mathematics in Medicine. 2009. 257 p.

6. Exact analytical inversion of interval type-2 TSK fuzzy logic systems with closed form inference methods // Applied Soft Computing, 37. 2015. P. 60–70.

7. Герасимов Б. М., Самойлов І. В. Алгоритм побудови матриці нечітких відношень для системи діагностування комп'ютерних мереж // Сучасні інформаційні технології у сфері безпеки та оборони: науково-практичний журнал Національної Академії оборони України. 2008. № 1. С. 8–11.

8. Ротштейн А. П., Митюшкин Ю. И. Нейро-лингвистическая идентификация нелинейных зависимостей // Кибернетика и системный анализ. 2000. № 2. С. 37–44.

9. Rotshtein, A. Rakytyanska, H. Fuzzy Evidence in Identification, Forecasting and Diagnosis, Springer, Berlin: Heidelberg, 2012. 314 p.

10. Ротштейн А. П., Ракитянская А. Б. Идентификация нелинейных зависимостей нечеткими базами знаний с генетико-нейронной настройкой // Известия РАН. Теория и системы управления. 2005. № 1. С. 110–117.

УДК 621.004.9

д-р техн. наук Толюпа С. В. ORCID: 0000-0002-1919-9174 (КНУ)
канд. техн. наук Штаненко С. С. ORCID: 0000-0001-9776-4653 (ВІТІ)
Побережець Т. В. ORCID: 0000-0001-8007-8614 (ВІТІ)
Лозунов В. К. (в/ч А0307)

МЕТОДИКА ПРОЄКТУВАННЯ РОБОТИЗОВАНИХ СИСТЕМ В БАЗІСІ САПР *INTEL QUARTUS PRIME*

У даний час при розробці роботизованих систем все більше застосовуються програмовані логічні інтегральні мікросхеми (ПЛІС).

Істотною перевагою ПЛІС є їхня універсальність і можливість швидкого програмування під виконання функцій практично будь-якого цифрового пристрою роботизованої системи. ПЛІС являє собою напівфабрикат, на основі якого розробник, що володіє персональним комп'ютером, має можливість проєктування цифрового пристрою в рекордно короткі терміни. Забезпечується це нескладними і відносно недорогими апаратними засобами програмування та спеціальним програмним забезпеченням, що називається системою автоматизованого проєктування (САПР).

ПЛІС – це електронний компонент, який використовується для створення цифрових інтегральних схем. На відміну від звичайних цифрових мікросхем, логіка роботи ПЛІС задається за допомогою програмування спеціальних засобів: програматорів і програмного забезпечення. Програмування на ПЛІС здійснюється за допомогою мов опису апаратури Verilog HDL і VHDL. На верхньому рівні ці мови дуже схожі – модель апаратури описується у вигляді взаємодіючих блоків (модулів) і для кожного з них визначається інтерфейс і реалізація. Інтерфейси модулів описують вхідні, вихідні і двосторонні порти, завдяки яким модулі з'єднуються один з одним з метою обміну даними, а також управління сигналами. Реалізація задає елементи внутрішнього стану і порядок обчислення значень вихідних інтерфейсів на основі цього стану і значень вхідних портів, а також правила поновлення внутрішнього стану.

У статті розкриті етапи проєктування цифрових пристроїв роботизованих систем за допомогою ПЛІС, розглянуті принципи побудови і функціонування основних вузлів комбінаційних схем, на логічних елементах реалізована одна із заданих функцій, яка в подальшому запрограмована на ПЛІС за допомогою САПР Quartus Prime із вбудованим симулятором ModelSim-Altera .

Ключові слова: *логічна схема, функція, мова опису апаратури, програмована логічні інтегральна мікросхема, система автоматизованого проєктування.*

S. Toliupa, S. Shtanenko, T. Poberezhets, V. Lozunov. Methodology for designing robotic systems based on CAD Intel Quartus Prime.

At present, programmable logic integrated circuits (FPGAs) are increasingly used in the development of robotic systems. A significant advantage of FPGAs is their versatility and the ability to quickly program to perform the functions of almost any digital device of a robotic system. FPGA is a semi-finished product, on the basis of which a developer with a personal computer has the ability to design a digital device in record time. This is provided by simple and relatively inexpensive software hardware and special software called computer-aided design (CAD). FPGA is an electronic component used to create digital integrated circuits. Unlike conventional digital chips, the logic of FPGA operation is set by programming using special tools: programmers and software. FPGA programming is performed using the description languages Verilog HDL and VHDL. At the upper level, these languages are very similar - the hardware model is described in the form of interacting blocks (modules) and for each of them is defined interface and implementation. Module interfaces describe the input, output, and two-way ports through which modules connect to each other for data exchange as well as control signals. The implementation sets the elements of the internal state and the order of calculating the values of the output interfaces based on this state and the values of the input ports, as well as the rules for updating the internal state. The article reveals the stages of designing digital devices of robotic systems using FPGA, considers the principles of construction and operation of the main nodes of combinational circuits, logical elements implemented one of the specified functions, which is subsequently programmed on FPGA using CAD Quartus Prime with built-in simulators Models.

Keywords: *logic circuit, function, hardware description language, programmable logic integrated circuit, computer-aided design system.*

Постановка завдання. На сьогоднішній день на театрі воєнних дій все більше спостерігається використання роботизованих систем, які вже без сумнівів відіграють вирішальну роль на полі бою, а згодом, на думку експертів, в подальшому повинні частково замінити людину. Створення таких систем висуває жорсткі вимоги до самих цифрових пристроїв зі швидкодії, функціональних можливостей, габаритів, потужностей, надійності, вартості та інших параметрів. Найбільш ефективним підходом вирішення цієї проблеми є орієнтація при створенні сучасних роботизованих систем на новітню елементну базу.

Яскравим прикладом такої елементної бази є програмовані логічні інтегральні мікросхеми (ПЛІС), які органічно поєднують в собі широкі можливості і гнучкість замовних інтегральних схем з доступністю і зручністю застосування традиційної «жорсткої» логіки.

Мікросхеми такого типу являють собою матрицю програмованих логічних елементів з *CPLD* (*Complex Programmable Logic Device*), *FPGA* (*Field-Programmable Gate Array*), *FLEX* (*Flexible Logic Element Matrix*) та *SoC* (*System-on-Chip*) архітектурою, між якими прокладені електричні комутовані з'єднання. Це дозволяє конфігурувати окремі компоненти і створювати зв'язку між ними шляхом завантаження в ПЛІС потоку даних, що включає необхідні електричні кола і вузли комутації. В результаті з існуючих у складі ПЛІС програмованих логічних елементів створюється необхідна цифрова схема, яка за необхідності може бути легко модифікована [1].

Аналіз останніх досліджень. На сьогоднішній день існує багато наукових робіт, присвячених проєктуванню цифрових пристроїв. Зокрема, робота [2] присвячена придбанню початкових відомостей з проєктування цифрових пристроїв як з використанням ручних методів мінімізації булевих функцій, так і з використанням системи автоматизованого проєктування (САПР) ПЛІС, а також вивчення деяких повноважень з управління логічним синтезом схем.

Робота [3] являє собою введення в САПР і дає загальне уявлення про типові етапи проєктування ПЛІС, від ідеї до готового виробу. Описано два підходи до проєктування схем в ПЛІС: перший – графічне введення, коли користувач креслить схеми електричних кіл, використовуючи готові шаблони, другий – кодовим описом логічних схем.

У роботі [4] розглянуті питання проєктування софт-процесорів, що конфігуруються, або які здатні надати проєкту в базісі ПЛІС всі елементи стандартної мікроконтролерної системи, включаючи можливість програмування отриманого пристрою за допомогою звичайних мов високого рівня.

Мета статті. У статті авторами на відмінність від попередніх робіт розглянуто трудомісткість етапів проєктування цифрових пристроїв, а саме опис алгоритму та його декомпозиція на частини, враховуючи специфіку застосування, а також розглянутий процес проєктування, що полягає у вирішенні задачі синтезу структури на прикладі комбінаційної схеми, яка задається булевою функцію як невід'ємною складовою роботизованої системи з подальшою реалізацією в базісі САПР *Intel Quartus Prime*.

Виклад основного матеріалу. Проєктування цифрових пристроїв, як основа будь-якої роботизованої системи на основі ПЛІС, містить наступні основні етапи:

формулювання концепції – постановка задачі та концептуальний опис алгоритму функціонування пристрою, що розробляється;

введення проєкту – представлення цифрового пристрою, що проєктується в «зрозумілому» для програмного засобу вигляді (принципова схема, часові діаграми, текстовий файл на спеціальній мові програмування *AHDL*, *VHDL*, *Verilog HDL*);

компіляція проєкту – логічний синтез, мінімізація, розведення і укладання проєкту в ПЛІС, а також створення файлів в спеціальному форматі, що містять всю інформацію для програмування мікросхеми;

верифікація проєкту – функціональне або тимчасове моделювання, а також часовий аналіз цифрового пристрою, що проєктується. Зазвичай, це робиться за допомогою побудови часових діаграм, де стан входів задаються користувачем, а стан виходів визначаються за допомогою програмного засобу, виходячи з закладеного алгоритму функціонування пристрою, що розробляється. При виявленні помилок або збоїв в роботі пристрою проводиться повернення до етапу створення проєкту з метою виправлення помилки. Процес повторюється до виправлення всіх помічених неточностей, завдяки чому ще до програмування ПЛІС вдається локалізувати в проєкті переважну більшість помилок;

програмування і тестування – кінцевий етап проєктування. Залежно від типу ПЛІС, що використовується і схемотехнічного рішення її апаратного обрамлення в пристрою, що розробляється, цей етап здійснюється або за допомогою програматора, або безпосередньо на робочій платі, в тому числі і динамічно, під час роботи пристрою.

Процес проєктування та верифікації цифрових пристроїв виконується засобами САПР. Одним з трудомістких етапів на етапі проєктування є постановка завдання, що полягає в описі алгоритму і його декомпозиції на частини, кожна з яких являє собою алгоритм, який має відоме апаратне уявлення [5].

Будь-який алгоритм можна представити послідовністю функціональних операторів:

$$F_i(X,\ Y) = (y_1^i,\ y_2^i,\ \ldots,\ y_r^i),$$

де X – множина вихідних даних;

Y – множина проміжних результатів, отриманих у процесі виконання оператора – F_i.

Узагальнена архітектура реконфігурованого пристрою може бути представлена у вигляді:

$$S = < P,\ A,\ F >,$$

де $P = \{P_i\}$ – множина об'єктів управління ($i = \overline{1, n}$);

$A_i = \{A_{ij}\}$ – множина алгоритмів управління, що реалізують функцію відображення $A_i : X_{ij} \to Y_{ij}$ множина вхідних сигналів $\{X_{ij}\}$ в множині вихідних сигналів $\{Y_{ij}\}$ для i-го об'єкта ($j = \overline{1, m}$);

$F = \{F_k\}$ – множина файлів конфігурації ($k = m \times n$), що визначають структури реалізації алгоритмів A_{ij} об'єктів управління P_i.

Якщо при апаратній реалізації алгоритм A_{ij} не вдається розмістити в один кристал, то цей алгоритм розбивається на фрагменти, що виконуються послідовно. Складність фрагментів алгоритму при цьому визначається логічною ємністю кристала. Відповідні цим фрагментам файли конфігурації F_{kl} завантажуються в кристал послідовно. Конфігурація кристала ПЛІС здійснюється шляхом запису файла конфігурації, сформованого за допомогою системи САПР *Intel Quartus Prime*.

Обсяг пам'яті, необхідний для зберігання множини F файлів конфігурації, буде визначатися величиною:

$$\Xi = q \times z \times k,$$

де z – число фрагментів алгоритму A_{ij};

q – обсяг пам'яті, необхідний для зберігання одного файла конфігурації.

Розглянутий алгоритм може бути основою для побудови моделі цифрового пристрою, що проєктується.

Враховуючи той факт, що сучасні роботизовані системи відносяться до програмно-реконфігурованих пристроїв (ПРП), в яких фіксоване поле заданої розмірності, налаштоване спеціально для виконання певного заданого алгоритму або його частини, постає питання забезпечення реалізації цього алгоритму оптимальним способом з точки зору часу його виконання і витрат апаратних ресурсів.

Для визначення оптимальної кількості рівнів програмованих компонентів (за які використовується ПЛІС) необхідно розглядати обробляючу систему (процесор) ПРП як інформаційну систему, вся інформація в якій віднесена до трьох сфер станів: зберігання, транспортування і перетворення. Очевидно, що при певних співвідношеннях між об'єктами інформації в цих сферах можна отримати оптимальні технічні параметри ПРП. Оптимальною вважається така структурна реалізація моделі ПРП, для якої відповідно до прийнятих критеріїв знайдені оптимальна кількість рівнів і оптимальне співвідношення між узагальненими характеристиками компонент на кожному рівні, а також між відповідними характеристиками компонент сусідніх рівнів.

Модель цифрового пристрою, що проєктується, може бути представлена четвіркою [6]:

$$S = < \Omega,\ A,\ B,\ D >,$$

де Ω – множина математичних методів для предметної області, що лежать в основі функціонування пристрою;

A – множина алгоритмів реалізації методу;

$B = \{b\}$ – алфавіт конструктивів, з яких синтезується структура;

D – процедура опису проєкту (опис об'єкта).

Таким чином, процес проєктування полягає у вирішенні задачі синтезу структури на основі конструктивів $\{b\}$ алфавіту B для виконання певного алгоритму, що реалізує метод Ω, що лежить в основі функціонування структури, відповідно до вимог специфікацій. Результатом процедури є опис проєкту мовою програмування в базісі САПР *Intel Quartus Prime.*

Запропоновано синтез структурної реалізації послідовності алгоритмів, коли метод (M) представляється послідовністю алгоритмів:

$$A_i, \forall i = \overline{1, \dots, n};$$

$$\Omega = \bigcup_i A_i .$$

У програмно-реконфігурованих пристроях спочатку задана базова (нульова) архітектура, реалізована на ПЛІС у вигляді функціонального поля фіксованої розмірності, контролера шини *host*-комп'ютера, поля пам'яті, а також добре структурованої бібліотеки файлів конфігурацій (БФК) структурних реалізацій методів (алгоритмів), що виконують відображення алгоритму в структурну реалізацію ($F : A_i \to B_i$). Кожен алгоритм має відображення ($F : A_i \to B_i$) в структурну реалізацію (B_i), яка являє собою файл конфігурації для кристала ПЛІС. У загальному випадку є кілька варіантів реалізації алгоритму (наприклад, послідовний, послідовно-паралельний і паралельний):

$$B_i = \bigcup_i A_{ij} .$$

Кожен варіант характеризується параметрами швидкодії (час виконання t_{ij}) й апаратними витратами (q_{ij}).

Припускаємо, що потужність множини t_{ij} є достатньою для реалізації широкого набору алгоритмів. У тому випадку, якщо необхідна реалізація t_{ij}-го алгоритму в бібліотеці відсутній, то необхідно за допомогою інструментальних засобів САПР створити її і включити як стандартний елемент в бібліотеку.

Таким чином, завдання оптимізації зводиться до впорядкованого призначення кожної i-ї вершини графа реалізованого алгоритму B_{ij}-го елемента бібліотеки з метою отримання екстремального значення деякого критерію якості. Будь-який оператор відображається тільки одним елементом з бібліотеки. В результаті визначається структура, яка реалізує заданий граф.

Тоді рішення задачі може бути отримано методами цілочисельного математичного програмування.

Завдання оптимізації полягає у визначенні мінімуму цільової функції, а критерієм якості є сумарний час виконання всіх алгоритмів і витрати обладнання:

$$\sigma_1 \sum_i \sum_j t_{ij} \lambda_{ij} + \sigma_2 \sum_i \sum_j q_{ij} \lambda_{ij} = \min \left(\forall i = \overline{1, \dots, n};\ j = \overline{1, \dots, k}\right)$$

при обмеженнях

$$\sum_i \sum_j t_{ij} \lambda_{ij} \le T_0 ; \quad \sum_i \sum_j q_{ij} \lambda_{ij} \le Q_0 ; \quad \sum_j x_{ij} = 1 (\forall i = \overline{1, \dots, n};\ j = \overline{1, \dots, k}),$$

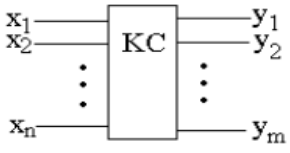
де σ_1, σ_2 – вагові коефіцієнти, які можуть бути визначені експертним шляхом;

Q_0 – гранично допустимі апаратні затрати;

T_0 – гранично допустимі часові затрати.

Теоретичною базою при проєктуванні цифрових пристроїв як основа сучасної роботизовано системи є булева алгебра, двійкова арифметика та теорія кінцевих автоматів. Функцією алгебри логіки (булева функція) називається функція, яка як і її аргументи, може приймати лише два значення: 0 або 1. Булеві функції є описом комбінаційних схем.

Розглянемо синтез комбінаційної схеми. Логічну схему, яка має n входів $X = \{x_1, x_2, \dots, x_n\}$ та m виходів $Y = \{y_1, y_2, \dots, y_m\}$, можемо представити у вигляді (рис. 1) [7].



$$\left.\begin{aligned} y_1 &= y_1(x_1, x_2, \dots, x_n), \\ y_2 &= y_2(x_1, x_2, \dots, x_n), \\ &\dots\dots\dots\dots\dots\dots \\ y_m &= y_m(x_1, x_2, \dots, x_n). \end{aligned}\right\} \quad (1)$$

Рис. 1. Комбінаційна схема

Логічна схема називається комбінаційною, якщо значення множини $Y = \{y_1, y_2, \dots, y_m\}$ її виходів можуть бути виражені як система m булевих функцій від множини вхідних змінних $X = \{x_1, x_2, \dots, x_n\}$ наступного вигляду:

Кожна функція $y_i = y_i(x_1, x_2, \dots, x_n)$ при $i = 1, 2, \dots, m$ визначає значення на виході схеми $y_i \in \{0, 1\}$ для будь-якого двійкового набору $(e_1, e_2, \dots, e_n)$, $e_j \in \{0, 1\}$ при $j = 1, 2, \dots, n$, який подається на незалежні входи схеми.

Система (1) описує залежність між входами та виходами схеми, але не дає представлення про її внутрішню структуру. Функціонування комбінаційної схеми можемо представити також у вигляді таблиці істинності, яка має 2^n рядків (по рядку для кожного набору вхідних змінних) та $(n+m)$ стовпців (n стовпців для входів та m стовпців для виходу схеми). Задача синтезу комбінаційної схеми складається з побудови схеми для заданої булевої функції або системи булевих функцій на основі певної системи логічних елементів. Як правило, початковий опис для синтезу схеми задається або у вигляді таблиці істинності, або в аналітичній формі у вигляді системи (1).

При вирішенні задачі синтезу комбінаційної схеми, що реалізує задану булеву функцію, попередньо проводиться мінімізація булевої функції та подальше спрощення мінімальної форми шляхом факторизації і декомпозиції. Комбінаційна схема будується в заданому базисі, як правило, з урахуванням коефіцієнта об'єднання по входах і коефіцієнта розгалуження по виходу.

В якості прикладу розглянемо булеву функцію

$$f(x, y, z) = xy \vee \bar{y}z \vee \bar{x}y\bar{z} \vee yz \vee \overline{x \vee \bar{y} \vee z},$$ для якої:

1. Побудуємо логічну схему, яка реалізує булеву функцію $f(x, y, z)$ за допомогою логічних елементів «І», «АБО», «НІ» та знайдемо затримку та ціну за Квайном.

2. Напишемо таблицю істинності даної функції.

3. Знайдемо фактичні змінні функції $f(x, y, z)$.

4. Використовуючи основні еквівалентності, перетворимо дану формулу в еквівалентну до неї, при цьому не містить фіктивних змінних. Побудуємо логічну схему, знайдемо її затримку та ціну за Квайном [8–11].

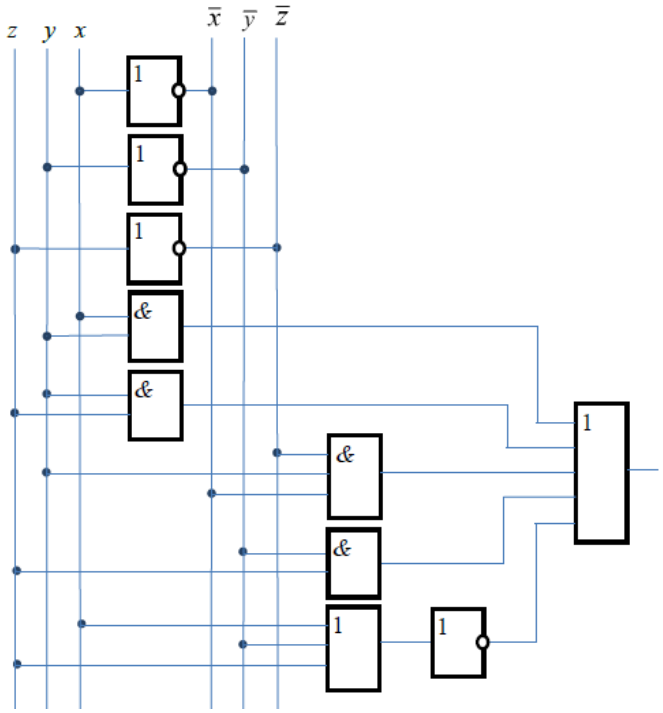


Рис. 2. Логічна схема, яка реалізує булеву функцію $f(x, y, z) = xy \vee \bar{y}z \vee \bar{x}y\bar{z} \vee yz \vee \overline{x \vee \bar{y} \vee z}$

Розв'язок

1. Для схеми на рис. 2 затримка – $T = 4\tau$, ціна за Квайном – $S_Q = 21$.

2. Побудуємо таблицю істинності (табл. 1), визначимо порядок виконання операцій відповідно до їх пріоритетності: $f_1 = \bar{x}$; $f_2 = \bar{y}$; $f_3 = \bar{z}$; $f_4 = x \vee f_2 \vee z$; $f_5 = \bar{f}_4$; $f_6 = xy$; $f_7 = f_2 \cdot z$; $f_8 = f_1 \cdot y \cdot f_3$; $f_9 = yz$; $f = f_5 \vee f_3 \vee f_7 \vee f_8 \vee f_9$.

Таким чином, кількість операцій, необхідних для отримання векторного значення функції, дорівнює десяти. Виходячи з цього, таблиця істинності має наступний вигляд (табл. 1):

Таблиця 1

x	y	z	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f
0	0	0	1	1	1	1	0	0	0	0	0	0
0	0	1	1	1	0	1	0	0	1	0	0	1
0	1	0	1	0	1	0	1	0	0	1	0	1
0	1	1	1	0	0	1	0	0	0	0	1	1
1	0	0	0	1	1	1	0	0	0	0	0	0
1	0	1	0	1	0	1	0	0	1	0	0	1
1	1	0	0	0	1	1	0	1	0	0	0	1
1	1	1	0	0	0	1	0	1	0	0	1	1

3. Розглянемо пари наборів, які є сусідами для змінної x, із значеннями функцій на цих наборах:

$$f(0, 0, 0) = f(1, 0, 0) = 0;\ f(0, 0, 1) = f(1, 0, 1) = 1;$$
$$f(0, 1, 0) = f(1, 1, 0) = 1;\ f(0, 1, 1) = f(1, 1, 1) = 1.$$

Таким чином x – фіктивна змінна.

Розглянемо пари наборів по змінній y. Так як $f(0, 0, 0) \neq f(0, 1, 0)$, то y – істотна змінна.

Розглядаючи пари наборів по змінній z, знаходимо, що $f(0, 0, 0) \neq f(0, 0, 1)$, тому z – істотна змінна.

Отримали, що $f(x, y, z) = g(y, z)$, при цьому таблиця істинності функції $g(y, z)$ має вигляд (табл. 2):

Таблиця 2

y	0	0	1	1
z	0	1	0	1
$g(y, z)$	0	1	1	1

За таблицею 2 визначаємо $g(y, z) = y \vee z$, тобто $f(x, y, z) = y \vee z$.

Застосовуючи основні еквівалентності, перетворюємо формулу до вигляду, яка не містить фіктивної змінної:

$$f(x, y, z) = xy \vee \bar{y}z \vee \bar{x}y\bar{z} \vee yz \vee \overline{x \vee \bar{y} \vee z} = xy \vee \bar{y}z \vee \underline{\bar{x}y\bar{z}} \vee yz \vee \underline{\bar{x}y\bar{z}} = xy \vee \underline{\bar{y}z} \vee \bar{x}y\bar{z} \vee \underline{yz} =$$

$$= xy \vee z(\bar{y} \vee y) \vee \bar{x}y\bar{z} = xy \vee z \cdot 1 \vee \bar{x}y\bar{z} = xy \vee z \vee \underline{\bar{x}y\bar{z}} = xy \vee (z \vee \bar{z})(z \vee \bar{x}y) = xy \vee 1 \cdot (z \vee \bar{x}y) =$$

$$= \underline{xy} \vee z \vee \underline{\bar{x}y} = y(x \vee \bar{x}) \vee z = y \cdot 1 \vee z = y \vee z.$$

Таким чином функція $f(x, y, z) = y \vee z$, а логічна схема представлена на рис. 3, при цьому затримка схеми складає $T = \tau$ та ціна за Квайном – $S_Q = 2$.

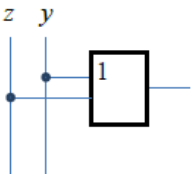
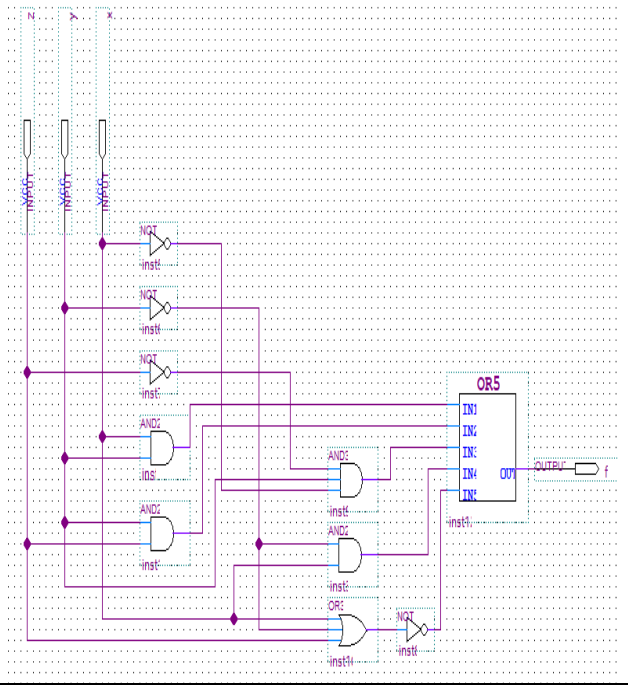


Рис. 3. Логічна схема, яка реалізує булеву функцію

$$f(x, y, z) = xy \vee \bar{y}z \vee \bar{x}y\bar{z} \vee yz \vee \overline{x \vee \bar{y} \vee z}$$

Проєктування комбінаційної схеми, яка реалізує булеву функцію роботизованої системи, здійснюється в середовищі САПР *Intel Quartus Prime* з вбудованим симулятором *ModelSim-Altera* та представлена у вигляді схемотехнічного редактора (рис. 4, *а*) та вихідного коду на мові опису апаратури *Verilog HDL* (рис. 4, *б*) [12–15].



а)

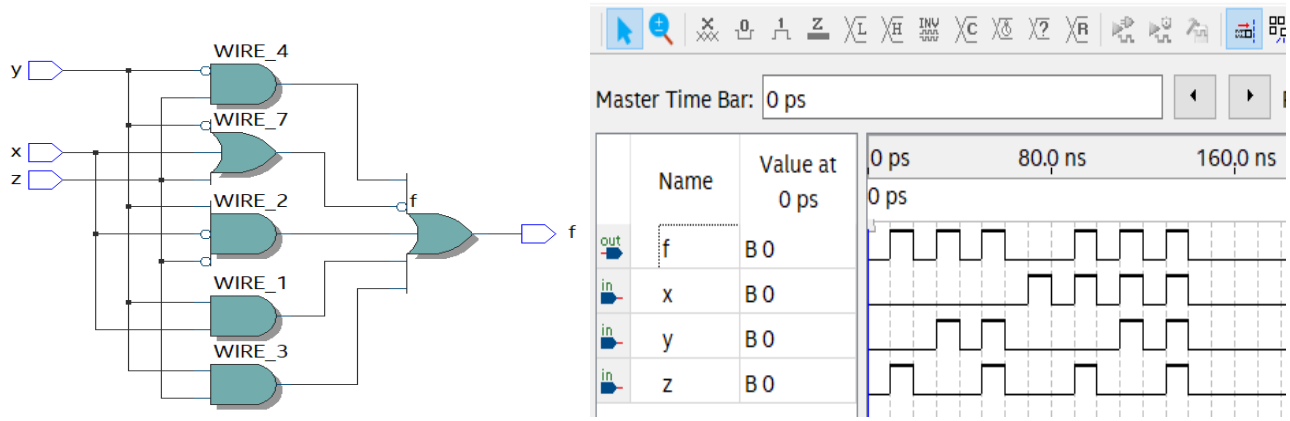
```
module logic_function(z, y, x, f);
input wire z; input wire y; input wire x;
output wire f;
wire WIRE_10;
wire WIRE_1; wire WIRE_2; wire
WIRE_3; wire WIRE_4;
wire WIRE_5; wire WIRE_7; wire
WIRE_8; wire WIRE_9;
assign  WIRE_1 = x & y;
assign  WIRE_3 = y & z;
assign  WIRE_7 = WIRE_10 | z | x;
assign  f = WIRE_1 | WIRE_2 | WIRE_3 |
WIRE_4 | WIRE_5;
assign  WIRE_4 = WIRE_10 & z;
assign  WIRE_9 =  ~x;
assign  WIRE_10 =  ~y;
assign  WIRE_8 =  ~z;
assign  WIRE_5 =  ~WIRE_7;
assign  WIRE_2 = WIRE_8 & y & WIRE_9;
endmodule
```

б)

Рис. 4. Комбінаційна схема по заданій логічній функції (*а*) та її *Verilog HDL*-код (*б*)

Далі представлено дизайн комбінаційної схеми, яка реалізує булеву функцію на рівні регістрових передач – *Register Type Level* (*RTL*) (рис. 5, *а*), що дає можливість в подальшому структурувати вихідний код та провести функціональне тестування, шляхом подачі на вхідні сигнали тестових комбінацій з подальшим аналізом вихідних сигналів у вигляді часових діаграм (рис. 5, *б*), які повною мірою відображають таблицю істинності.

Порівнюючи таблицю істинності (табл. 1) та результати моделювання (рис. 5, *б*), бачимо, що комбінаційна схема, яка проєктується, працює правильно.



а) *б*)

Рис. 5. *RTL* – дизайн функції $f(x, y, z) = xy \vee \bar{y}z \vee \bar{x}y\bar{z} \vee yz \vee \overline{x \vee \bar{y} \vee z}$ (*а*) та функціональне моделювання по заданій логічній функції (*б*)

Впевнившись в коректності роботи комбінаційної схеми, переходимо до програмування та конфігурації ПЛІС шляхом використання конфігуруючого файлу, який згенерований асемблером *Intel Quartus Prime*.

В подальшому за кінцевий функціональний пристрій, який програмується, використовується налагоджена плата *DE10-Nano* на основі *FPGA Cyclone V* 5CSEBA6U2317.

Висновок. Таким чином, використаний в роботі підхід налагодження логічної схеми спрощує тестування моделі та робить дану методику прийнятною, а також доступною для більшості програмно-реконфігурованих цифрових пристроїв, які використовуються в роботизованих системах шляхом підтвердження адекватності отриманих результатів на часових діаграмах *ModelSim*. За рахунок використання засобів налагодження можливо запобігти ряду помилок, які виникають в процесі створення роботизованих системах, а також підтвердити або спростувати адекватність роботи представленої симульованої моделі, яка в подальшому програмується на кристалі ПЛІС.

ЛІТЕРАТУРА

1. Семенець В. В. Проектування цифрових систем з використанням мови VHDL: навч. посібник / В. В. Семенець, І. В. Хаханова, В. І. Хаханов. Харків: ХНУРЕ, 2003. 492 с.

2. Строгонов А. В. Проектирование комбинационных схем в базисе ПЛИС // Компоненты и технологи. 2008. № 5. С. 148–151.

3. Акчурин А. Д. Основы работы в среде Quartus II: уч.-метод. пособ. / А. Д. Акчурин, К. М. Юсупов, А. А. Колчев. Казань: КФУ, 2017. 49 с.

4. Тарасов И. Е. Проектирование конфигурируемых процессоров на базе ПЛИС // Компоненты и технологи. 2006. № 2. С. 78–83.

5. Попов А. Ю. Проектирование цифровых устройств с использованием ПЛИС: учеб. пособ. Москва: Изд-во МГТУ им. Н. Э. Баумана, 2009. 80 с.

6. Слюсарь В. В. Методика проектирования программно-реконфигурируемых устройств на базе ПЛИС / В. В. Слюсарь, Р. М. Романов // Оборонный комплекс – научно-техническому прогрессу России. 2010. № 1. С. 48–52.

7. Довгий П. С. Синтез комбинационных схем. Учебное пособие к курсовой работе по дисциплине «Дискретная математика» / П. С. Довгий, В. И. Поляков. Санкт-Петербург: СПбГУ ИТМО, 2009. 64 с.

8. Исмагилова Е. И. Булевы функции и построение логических схем: учеб. пособие / Е. И. Исмагилова. Москва: МИРЭА, 2015. 160 с.

9. Харрис Д. М. Цифровая схемотехника и архитектура компьютера: учеб. пособие. 2-е изд., перераб, и доп. USA: Morgan Kaufman, 2013. 1625 с.: ил.

10. Сергиенко И. В. Задачи дискретной оптимизации. Проблемы, методы решения, исследования / И. В. Сергиенко, В. П. Шило. Киев: Наукова думка, 2003. 261 с.

11. Тарасов И. Е. ПЛИС Xilinx. Языки описания аппаратуры VHDL и Verilog, САПР, приемы проектирования // Горячая линия – Телеком, 2022. 358 с.

12. Vaibbhav Taraate. PLD Based Designwith VHDL RTL Design, Synthesisand Implementation – Springer Nature Singapore Pte Ltd, 2017. 423 p.

13. Строгонов А. В. Реализация Verilog-проектов в базисе академических ПЛИС с применением САПР VTR7.0 // Компоненты и технологи. 2017. № 5. С. 12–17.

14. Bogdan Belean. Application-Specific Hardware Architecture Designwith VHDL. Springer International Publishing, 2018. 191 p.

15. Ратушний П. М. ПЛІС та їх програмування: лабораторний практикум / П. М. Ратушний, О. М. Жагловська, К. В. Огородник. Вінниця: ВНТУ, 2018. 57 с.

УДК 621.391

Фесенко О. Д. ORCID: 0000-0002-2114-5327 (ВІТІ)
канд. техн. наук Бєляков Р. О. ORCID: 0000-0001-9882-3088 (ВІТІ)
канд. техн. наук Радзівілов Г. Д. (ВІТІ)

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ БЕЗПЛАТФОРМНОЇ ІНЕРЦІАЛЬНОЇ НАВІГАЦІЙНОЇ СИСТЕМИ БПЛА НА ОСНОВІ НЕЙРОМЕРЕЖЕВИХ АЛГОРИТМІВ

Об'єктом дослідження є процес керування траєкторією безпілотних літальних апаратів (БпЛА) в автономному режимі польоту на основі нейромережевих алгоритмів. Проведене дослідження базується на застосуванні чисельно-аналітичного підходу вибору сучасних технічних рішень побудови типових моделей безплатформних інерціальних навігаційних систем (БІНС) для мікро- і малих БпЛА з подальшим підкріпленням припущень в середовищі імітаційного моделювання, що дозволило: по-перше, зімітувати роботу системи управління БпЛА на базі МЕМС-технології (використання Мікроелектромеханічних систем) та мікрокомп'ютерів Arduino та відслідкувати її роботу під час зникнення GPS-сигналу; по-друге, експериментально визначити характер впливу структури вибраної нейронної мережі на процес формування навігаційних даних. Таким чином, для оцінки ефективності запропонованих рішень із побудови БІНС було проведено порівняльний аналіз застосування двох алгоритмів ELM (Extreme Learning Machine) – Kalman та WANN (Wavelet Artificial Neural Network) – RNN (Recurrent Neural Network) – Madgwick у вигляді двох експериментів. Метою експериментів було визначено: дослідження впливу кількості нейронів прихованого рівня нейронної мережі на точність апроксимації навігаційних даних; визначення швидкості процесу адаптивного навчання нейромережевих алгоритмів БІНС БпЛА. Результат експериментів показав, що застосування алгоритму на основі ELM – Kalman забезпечує кращу точність навчання нейромережі БІНС порівняно з алгоритмом WANN – RNN – Madgwick. Однак, необхідно зазначити, що точність навчання покращувалась зі зростанням кількості нейронів в структурі прихованого рівня <500, що підвищує обчислювальну складність та збільшує час процесу навчання, що може ускладнити практичну реалізацію із використанням обладнання мікро- та малих БпЛА.

O. Fesenko, R. Bieliakov, H. Radzivilov. Simulation modeling of free shipless inertial navigation system UAV based on neural network algorithms.

The object of the article is the process of controlling the trajectory of unmanned aerial vehicles (UAVs) in autonomous flight mode based on neural network algorithms. The study is based on the application of numerical-analytical approach to the selection of modern technical solutions for building standard models of platformless inertial navigation systems (BINS) for micro- and small UAVs with subsequent reinforcement of assumptions in the simulation environment, which allowed: MEMS-based technology (using microelectromechanical systems) and Arduino microcomputers, and monitor its operation during the disappearance of the GPS signal; secondly, to experimentally determine the nature of the influence of the structure of the selected neural network on the process of formation of navigation data. Thus, to evaluate the effectiveness of the proposed solutions for the construction of BINS, a comparative analysis of the application of two ELM (Extreme Learning Machine) algorithms - Kalman and WANN (Wavelet Artificial Neural Network - RNN (Recurrent Neural Network) - Madgwick in the form of two experiments. The purpose of the experiments was determined: the study of the influence of the number of neurons of the latent level of the neural network on the accuracy of the approximation of navigation data; determination of the speed of the process of adaptive learning of neural network algorithms BINS UAV. The results of the experiments showed that the use of the algorithm based on ELM - Kalman provides better accuracy of learning the BINS neural network compared to the WANN - RNN - Madgwick algorithm. However, it should be noted that the accuracy of training improved with the number of neurons in the structure of the latent level <500, which increases computational complexity and increases the learning process, which may complicate practical implementation using micro- and small UAV equipment.

Ключові слова: *нейронна мережа, траєкторія польоту, точність навчання нейронної мережі, імітаційне моделювання, навігаційні дані.*

Вступ. У військовій сфері перевага надається мініатюрному класу безпілотних літальних апаратів у зв'язку із високою мобільністю, дешевизною, легкістю маскування, високою маневреністю, водночас зростає необхідність розробок алгоритмів інтелектуальних систем супроводження БпЛА в автономному режимі польоту незалежно від глобальних систем позиціювання. Однак, при малих розмірах безпілотників виникають обмеження на застосування класичних платформних інерціальних навігаційних систем та відповідно зростає складність розробки і впровадження інтелектуальних систем керування траєкторією польоту БпЛА [1].

Відомо, що визначення даних позиціювання мініатюрного типу БпЛА, як правило, відбувається на базі інтегрованої МЕМС безплатформної інерціальної навігаційної системи на базі мікрокомп'ютерів типу Arduino. Алгоритми функції керування маршрутом польоту під час

зникнення сигналу глобальних супутникових систем описують із застосуванням методів нейромережевих алгоритмів [2], синтезованих, здебільшого, на базі алгоритмів фільтрації Калмана, використовуючи данні МЕМС-датчиків та модуля глобальної системи позиціювання (GPS) [3].

Відомо, що інерціальні навігаційні системи на базі МЕМС-датчиків мають високу чутливість, що призводить до виникнення похибок оцінки встановлення кутової швидкості, визначення курсу, яка становить Δ_ω∈ {0.66…1.16} °/с. [4; 5], відповідно без корегування GPS-навігації, похибки МЕМС інерціальної навігаційної системи збільшуються із часом.

У результаті раптового зникнення сигналів ГСП, інерціальна навігаційна система починає працювати в автономному режимі – тільки на основі показників МЕМС-датчиків (акселерометр, гіроскоп, магнітометр) [6], та відомо, що структура моделі похибок МЕМС-датчиків БІНС через нестабільністьність окремих складових, особливо в період кореляції, близький до періоду зникнення сигналу ГСП (від 10 с до 300 с), може стати критичною для коректного управління траєкторією польоту БпЛА [4; 5].

Крім того, під час маневрування БпЛА в динамічному середовищі в автономному режимі польоту до навігаційної системи МЕМС на базі нейромережевих алгоритмів висувають вимоги:

похибка відхилення від цільової траєкторії Т(Δ_ωБПЛА)≤ {0.012…0.18} °/с [6; 8; 9];

період навчання нейромережі t_(lerning rate)≤{20…100} с., обумовлено обмеженням фізичним сховищем пам'яті мікроконтролера Arduino Nano та встановленням необхідного довірчого інтервалу репрезентативності навчальної вибірки еталонних навігаційних параметрів [7; 8];

швидкість адаптивного навчання нейромережі t_(adaptive learning rate) ≤{ 0.034…0.05} с, тобто процес донавчання нейромережі в реальному часі.

Невиконання вище зазначених вимог може призвести до відхилення від цільової траєкторії до 400 метрів на 1 кілометр польоту, що показано в роботі [10].

Аналіз наукових праць предметної області. В науковому дослідженні [11] показано ефективний метод компенсації похибок МЕМС інерціальної навігаційної системи на основі рекурентної нейронної мережі LSTM – RNN. Однак було встановлено, що під час польоту БпЛА структура нейромережі ускладнюється, що накладає додаткове обчислювальне навантаження на мікрокомп'ютер навігаційної системи.

В роботі [12] представлено метод інерціальної навігації на основі модифікованого фільтра Калмана в поєднанні з алгоритмом оберненого поширення помилки нейромережі для мінімізації обчислювального навантаження. Запропонований вдосконалений фільтр Калмана на основі нейронних мереж показав кращі результати під час процесу обчислення оцінки навігаційних параметрів (початковий кут зсуву), однак модель не враховує залежність похибок БІНС на т-1 кроці, коли діючі шумові характеристики відносно попередніх не визначені.

Автори статті [13] запропонували вдосконалений метод фільтрації Калмана за допомогою нейронної мережі з радіальною базовою функцією для зменшення впливу динамічного середовища на визначення траєкторії БпЛА після втрати сигналу GPS. Результат показав, що за допомогою запропонованого методу вдалося досягти зменшення впливу динамічних варіацій шумових характеристик БІНС БпЛА після втрати GPS-сигналу, але це призводить до зростання обчислювальної складності відносно часу роботи і може бути використане за відсутності обмежень на масо-габаритні показники навігаційного обладнання БпЛА.

В роботі [14] запропонований метод фільтрації вибірки вихідних даних гіроскопа на основі генетичного нейромережевого алгоритму пошуку нейронної архітектури NAS – RNN. Результат показав, що при застосуванні алгоритму NAS – RNN стандартне відхилення показників

МЕМС-гіроскопу зменшилося порівняно з відхиленням при LSTM – RNN, але використання алгоритму NAS – RNN призводить до збільшення часу, необхідного на пошук та навчання адаптивної моделі нейромережевої структури навігаційної системи.

На сьогодні, в галузі машинного навчання все більше зростає популярність алгоритмів автоматичного пошуку моделі нейромережевих структур, що дозволяє максимально точно підібрати модель нейромережі для вирішення цільової задачі, враховуючи обмеження.

Один із відомих методів автоматизованого машинного навчання є алгоритм агностичної мережі підбору нейронної архітектури WANN [15], на відміну від традиційних алгоритмів WANN замість підлаштування вагових коефіцієнтів використовує варіаційний процес на основі генетичного методу підбору архітектури нейромереж з загальним ваговим коефіцієнтом, що скорочує час на адаптацію вибраної архітектури нейронної мережі для вирішення цільової задачі.

В роботі [7] алгоритм WANN вперше був застосований для вирішення задач автономної навігації БпЛА, а саме процесу компенсацій похибок гіроскопу кутового прискорення інерціальної навігаційної системи МЕМС. Експериментальний аналіз трьох алгоритмів штучних нейронних мереж пошуку нейронної архітектури Neural Architecture Search recurrent neural network (NAS-RNN), короткої та довготривалої рекурентної мережі Long short-term memory recurrent neural network (LSTM-RNN) та агностичної мережі підбору архітектури Weight Agnostic Neural Networks (WANN) показали, що при застосуванні NAS-RNN значення стандартного відхилення тривісних вимірювань гіроскопу зменшилися відповідно на 44,0 %, 34,1 % та 39,3 %.

Однак, для реалізації в реальному часі вище зазначених нейромережевих алгоритмів на базі технології МЕМС малогабаритних мікрокомп'ютерів Arduino, як правило, потребують процесу квантування нейромережі [16] (для зниження розмірності архітектури нейромережі), але точність таких нейромереж знижується на 20–30 %.

На сьогодні для розробки інтелектуальних систем навігації переважно застосовують динамічні нейронні мережі [17], які дозволяють уникнути процесу квантування без втрати точності нейромережевої моделі. Тому, пропонується розглянути альтернативні алгоритми на основі екстремального машинного навчання ELM, які були представлені в [18; 19].

Таким чином, **метою статті** є експеримент застосування нейромережевих алгоритмів як систем керування траєкторією БпЛА в автономному режимі польоту, суть якого полягає в процесі зменшення відхилення від цільової траєкторії БпЛА в умовах раптового зникнення сигналів GPS.

Стаття складається з трьох розділів, в яких розкривається аналіз основних алгоритмів адаптації (RLS, LMS), та представлено концептуальне завдання застосування лінійного нейронного регулятора для фільтрації сигналів в адаптивних антенних решітках.

Виклад основного матеріалу

У загальному вигляді, модель траєкторії БпЛА будується на основі даних навігаційної системи глобальної системи позиціювання GPS та процесів роботи МЕМС інерціальної системи навігації вдосконаленого фільтру Маджвіка, яка в сутності являє собою 18-мірний вектор стану, що показано в рівнянні:

$$P = \left[\phi_{E,N,U}\ \Delta V_{E,N,U}\ \Delta P_{l,\lambda,h}\ \Delta g_{x,y,z}\ \Delta a_{x,y,z}\ \Delta m_{x,y,z}\right]^T,$$

де $\phi_{E,N,U}$ − вектор похибки орієнтації відносно платформи БпЛА, який являє собою проєкцію обертання Землі на осі (east-north-up);

$\Delta V_{E,N,U}$ − похибки даних швидкості БпЛА відносно локальної системи координат БпЛА;

$\delta_{l,\lambda,h}$ − похибка довготи, широти та висоти;

$\Delta g_{x,y,z}$ – похибки постійного відхилення гіроскопа в системі координат відносно МЕМС-датчиків;

$\Delta a_{x,y,z}$ – похибки постійного зміщення акселерометра;

$\Delta m^E_{x,y,z}$ – похибки магнітометра (феромагнітний вплив) відносно визначення магнітної півночі;

індекс Е – еталонна модель магнітного поля.

В момент раптового зникнення сигналу глобальної системи позиціювання для визначення оцінки позиціювання безпілотного літального апарату, тобто (швидкість і положення БпЛА), застосовується алгоритм нейронної мережі для заміни сигналу GPS для прогнозування позиції БпЛА в просторі.

Експериментальне дослідження процесів керування траєкторією БпЛА під час зникнення сигналів GPS представлено у двох експериментах.

Експерименти проводились в програмному середовищі Simulink Matlab (версія 2020.b) та мови програмування Python з використанням бібліотек Google Tensor Flow (версія 2.1.0) з відкритим кодом, для глибокого навчання використовуючи реальний набір даних датчиків БІНС. Експериментальна платформа зібрана на основі макетної плати ProsKit Bx-4123.

У середовищі Matlab побудована модель процесу зникнення сигналу глобальних систем позиціювання протягом 300 секунд польоту БпЛА (рис. 1).

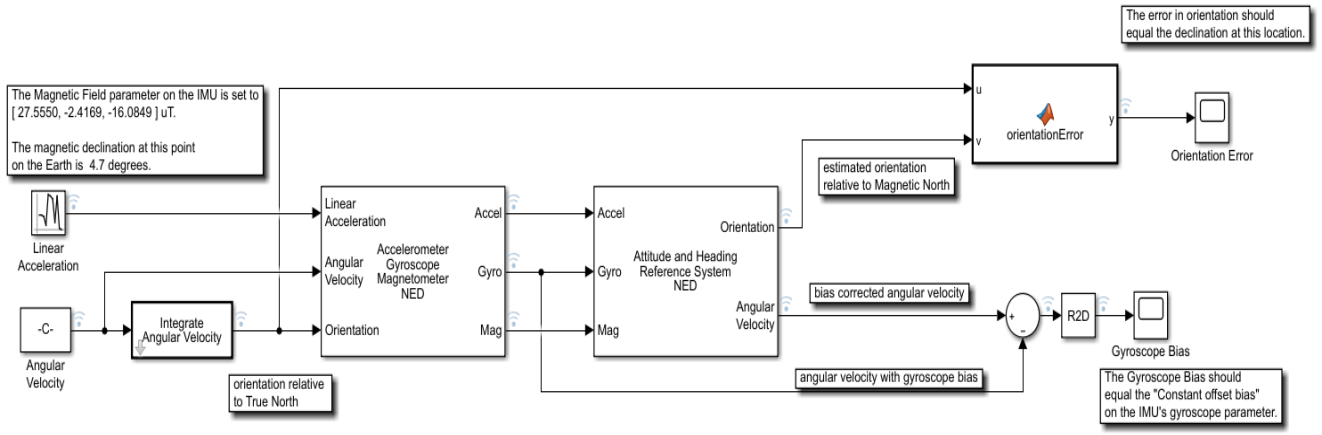


Рис. 1. Імітаційна модель обробки навігаційних параметрів Simulink Matlab

Враховуючи вихідні дані, обмеження та допущення, здійснюється оцінка позиціювання БпЛА (швидкість і положення БпЛА) з використанням алгоритму ELM – Kalman [19] та WANN –RNN Madgwick [16].

Вхідні дані:

Q={ $q1(\phi_{E,N,U}), q2(\varepsilon V_{E,N,U}), q3(\varepsilon P_{l,\lambda,h})$ } – вектор еталонних параметрів позиціювання БпЛА.

Вихідні дані:

T={ $q1(\phi_{E,N,U}+\Delta_{t+1}), q2(V_{E,N,U}+\Delta_{t+1}), q3(P_{l,\lambda,h}+\Delta_{t+1})$ } – цільові вихідні параметри прогнозування траєкторії БпЛА в автономному режимі польоту під час зникнення сигналу GPS.

Обмеження:

$\mathrm{T}(\Delta_{\omega\text{БПЛА}}) \leq \{0.012 \ldots 0.18\}^{\circ}\frac{1}{\mathrm{c}}$ – відхилення від цільової траєкторії БпЛА в автономному режимі польоту [4–6];

період навчання нейромережі – $t_{lerning\ rate} \leq \{10 \ldots 100\}$c;

швидкість адаптивного навчання нейромережі – $t_{\text{adaptive learning}\,rate} \leq \{0.034 \ldots 0.05\}$c.

Цільова функція: $F(\mathrm{T}(\Delta_{\omega\text{БПЛА}})) \rightarrow min \Rightarrow \min_{\beta}\left\|H\beta - T^{`}\right\| \Rightarrow optimum(NNA)$.

Допущення: швидкість польоту БпЛА є сталою.

Під час експерименту для забезпечення коректного зняття вимірів гіроскопа (прискорення, кутової швидкості) використовується датчик інерціальної навігаційної системи MEMS
MPU-9250. Далі сигнал, отриманий на вході датчика, демодулюється та проходить через 16-бітний АЦП. Швидкість АЦП (Sample Rate) може програмно варіюватися від 3,9 до 8000 вибірок в секунду (Samples per second, SPS).

На наступному етапі відбувається процес компенсації впливу вібрації чутливих елементів датчика в діапазоні 20–25 Гц за допомогою вбудованого фільтра низьких частот та зчитування даних на мікрокомп'ютерну платформу Arduino Nano.

Процес розрахунку орієнтації БпЛА в автономному режимі польоту відбувається за рахунок обробки даних прискорення та даних магнітного поля.

Відомо, що основним датчиком, який впливає на визначення кута курсу БпЛА в режимі повного автономного польоту без урахування сигналу GPS, є показник магнітометра, тобто дані

курсу (визначення направлення магнітної півночі), тому для коректності було імітовано ефект феромагнітного збурення, за допомогою магніту який поступово наближався до датчика магнітометра, цю дію повторювали тричі. Перші два рази застосовували магнітний вплив тільки на 2-3 секунди, тоді як в третій раз вплив було здійснено статично (до кінця експерименту), в результаті значення відрізнялось від норми опорного вектора магнітного поля (≈0,55 Гауса).

Результати дослідження

Експеримент 1. Мета експерименту – визначення впливу кількості нейронів прихованого рівня нейронної мережі на точність апроксимації навігаційних даних.

На графіку (рис. 2) порівнюється результат роботи алгоритмів БІНС, використовується популярна метрика похибок Root Mean Square Error (RMSE) для вимірювання різниці між значеннями прогнозування моделі й еталонної моделі (із опорними навігаційними параметрами, отриманими з GPS). А саме, було здійснено оцінку точності визначення навігаційних параметрів БІНС на основі нейромережевих алгоритмів. Таким чином, результат імітації параметрів сигналу GPS:

ELM – Kalman блакитною лінією (результат 500 нейронів – точність відсотковому співвідношенні до моделі із опорним сигналом GPS (RMSE) – 93,2 %);

WANN –RNN Madgwick зеленою лінією (результат 500 нейронів – RMSE – 81,3 %).

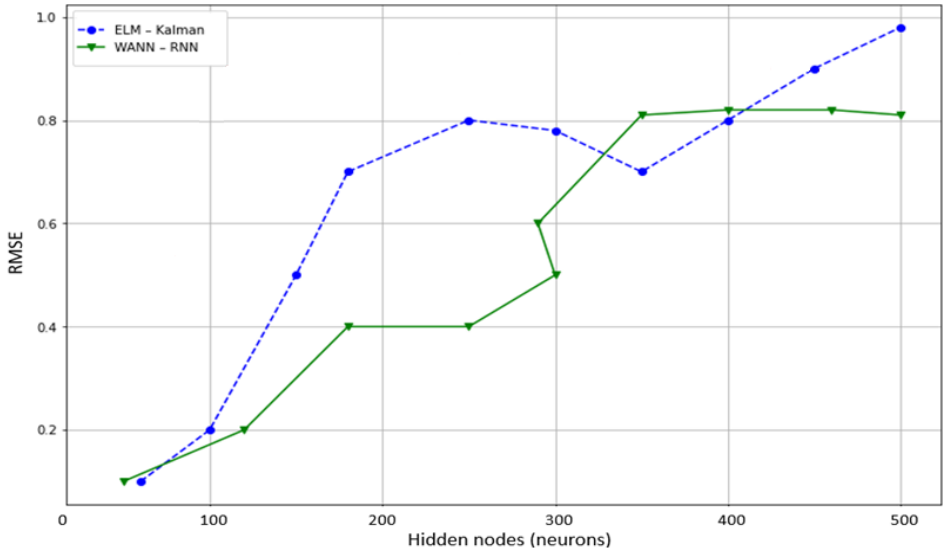


Рис. 2. Графік оцінки точності RMSE навігаційних параметрів БІНС на основі нейромережевих алгоритмів із різною кількістю нейронів Hidden nodes (neurons) прихованого рівня

Експеримент 2. Мета експерименту – визначення швидкості процесу адаптивного навчання нейромережевих алгоритмів БІНС БпЛА.

Експеримент полягав в тому, що при тестуванні навченої нейромережі на її вхід подавалися тестові вектори, відмінні від використаних в навчальній послідовності.

В результаті експерименту встановлено (рис. 3):

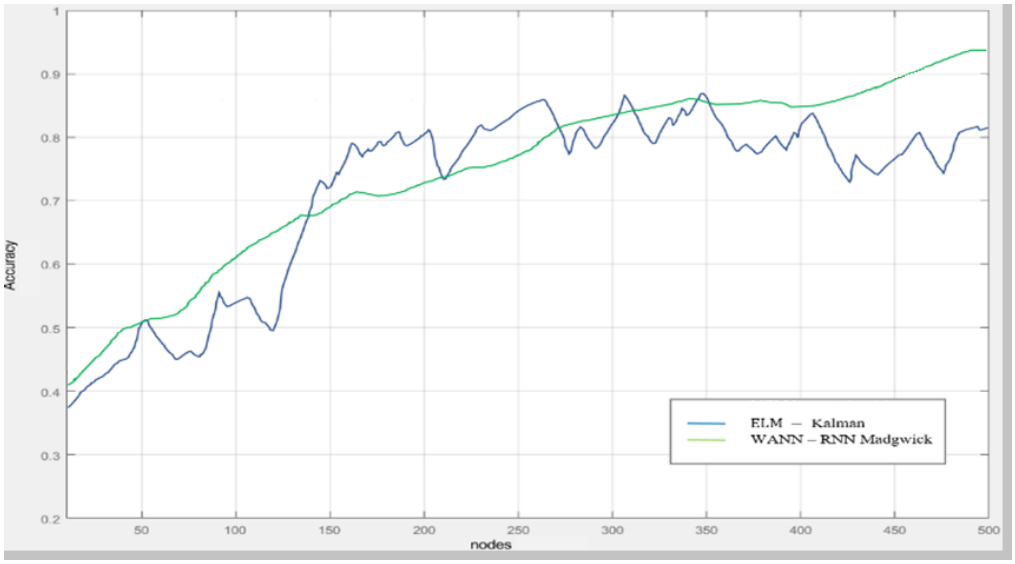


Рис. 3. Графік точності (Accuracy/c) адаптивного навчання БІНС залежно від кількості нейронів (nodes) та типу нейромережевого алгоритму

БІНС на основі нейронної мережі ELM – Kalman (швидкість навчання склала 0,8 /с, точність RMSE – 80,2 %);

БІНС на основі неромережевого алгоритму WANN – RNN Madgwick (швидкість навчання 0,81 /с, точність RMSE – 65,4 %).

Результат експериментів показав, що застосування алгоритму на основі ELM – Kalman забезпечує кращу точність навчання нейромережі БІНС і є швидшою порівняно з алгоритмом WANN – RNN – Madgwick на 2,23 %.

Однак необхідно зазначити, що точність навчання покращувалась зі зростанням кількості нейронів в структурі прихованого рівня < 500, що підвищує складність обчислювального навантаження та збільшується час процесу навчання, що може ускладнити практичну реалізацію із використанням обладнання мікро- та малих БпЛА.

Висновки.

Таким чином, у статті показано застосування нейромережевих алгоритмів як систем імітації параметрів опорних сигналів для керування траєкторією БпЛА в автономному режимі польоту.

Основним завданням є зменшення відхилення від цільової траєкторії БпЛА в умовах раптового зникнення сигналів GPS.

Проаналізовано тенденції розвитку науково-прикладних рішень застосування нейромережевих алгоритмів для систем керування траєкторією мікро- та малих БпЛА у складі безплатформних інерціальних навігаційних систем.

Було здійснено імітаційне моделювання в середовищі Matlab на основі вихідних даних моделі траєкторії БпЛА (з урахуванням еталонних параметрів GPS) для дослідження процесу управління траєкторією БпЛА з використанням нейронних мереж в періоди зникнення GPS-сигналів.

Експериментально встановлено, що застосування алгоритму на основі ELM – Kalman забезпечує кращу точність навчання нейромережі БІНС порівняно з алгоритмом WANN – RNN – Madgwick.

Напрямком подальших досліджень слід вважати розробку методик роботи нейрорегулятора у розрізі впливу навмисних електромагнітних впливів.

ЛІТЕРАТУРА

1. Fendy Santoso, Matt Garratt, Anavatti, S.G. (2018). State-of-the-art intelligent flight control systems in unmanned aerial vehicles. IEEE Transactions on Automation Science and Engineering, Volume: 15, Issue: 2, April 2018, 613-627. https://doi.org/10.1109/TASE.2017.2651109.

2. Yimin Zhou, Jiao Wan, Zhifei Li, Zhibin Song.(2017). GPS/INS integrated navigation with BP neural network and Kalman filter. 2017 IEEE International Conference on Robotics and Biomimetics (ROBIO), Date Added to IEEE Xplore: 26 March 2018. https://doi.org/10.1109/ROBIO.2017.8324798.

3. C. Sun, W. He, W. Ge, and C. Chang. (2017). Adaptive neural network control of biped robots. IEEE Transactions on Systems, Man, and Cybernetics: Systems, Volume: 47, Issue: 2, 2017, 315–326. https://doi.org/10.1109/TSMC.2016.2557223.

4. Веремеенко К. К., Красильщиков М. Н., Сыпало К. А. (2008). Управление и наведение беспилотных маневренных летательных аппаратов на основе современных информационных технологий. Москва: Физматлит.

5. Ding, S., Ma, G., Shi, Z. (2014). A rough RBF neural network based on weighted regularized extreme learning machine. Neural processing letters, vol. 40, no. 3, 245–260. View at: https://link.springer.com/article/10.1007/s11063-013-9326-5.

6. Xiaoji Niu, Sameh Nassar, Naser El-Sheimy. (2007). An accurate land-vehicle MEMS IMU/GPS navigation system using 3D auxiliary velocity updates. Navigation, 54(3): September 2007, 177–188. https://doi.org/10.1002/j.2161-4296.2007.tb00403.x.

7. Фесенко О. Д., Бєляков Р. О., Радзівілов Г. Д., Гулій В. С. Експериментальний аналіз застосування нейронних мереж для керування траєкторією польоту БпЛА // Збірник наукових праць ВІТІ. 2020. № 1. Дата доступу 02.02.2022. URL: http://www.viti.edu.ua/files/zbk/2020/11_1_2020.pdf.

8. Тихонов В. А. Нейросетевая модель алгоритма бесплатформенной инерциальной навигационной систем / Мат. 3 Межд. симп. Аэрокосмические приборные технологии, 2–4 июня 2004 г. С. 47–50.

9. Fakharian, A., Gustafsson, T., Mehrfam, M. (2011). Adaptive kalman filtering based navigation: an IMU/GPS integration approach. IEEE conference on networking, sensing and control 2011, 181–185.

10. Jiang, S. Chen, Y. Chen et al. (2018). A MEMS IMU de-noising method using long short term memory recurrent neural networks (LSTM-RNN). Sensors, vol. 18, no. 10, 3470, 2018. View 02.02.2022. https://www.mdpi.com/1424-8220/18/10/3470.

11. Gross, J., Gu, Y., Gururajan, S., et al. (2013). A comparison of extended kalman filter, sigma-point kalman filter, and particle filter in GPS/INS sensor fusion. AIAA Guidance, Navigation, & Control Conference. View at: https://arc.aiaa.org/doi/10.2514/6.2010-8332.

12. Tianjun Liu, Xinglong Tan, Jian Wang, Yipeng Ning. (2018). An optimal radial basis function neural network enhanced adaptive robust Kalman filter for GNSS/INS integrated systems in complex urban areas. Sensors 2018, 18 (9), 3091. https://doi.org/10.3390/s18093091.

13. Elsken Thomas, Metzen Jan Hendrik, Hutter Frank (2019). Neural architecture search: A Survey. Journal of Machine Learning Research. 20 (55), 1–21. View at: https://www.jmlr.org/papers/volume20/18-598/18-598.pdf.

14. Adam Gaier, David Ha. (2019). Weight agnostic neural networks. Submitted on 11 Jun 2019 (v1), last revised 5 Sep 2019 (this version, v2). View at: https://arxiv.org/abs/1906.04358.

15. Itay Hubara, Matthieu Courbariaux, Daniel Soudry, Ran El-Yaniv, Yoshua Bengio. (2018). Quantized neural networks: training neural networks with low precision weights and activations. Journal of Machine Learning Research 18, 1–30. View at: https://jmlr.org/papers/v18/16-456.html.

УДК: 355.469.1

Чередниченко О. Ю. (ВІТІ)
Процюк Ю. О. (ВІТІ)
Шемендюк О. В. (ВІТІ)
канд. техн. наук Лебідь Є. В. (ВІТІ)

АНАЛІЗ ДОСВІДУ БОЙОВОГО ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРОТИ ЗЕНІТНО-РАКЕТНИХ КОМПЛЕКСІВ У ВІЙСЬКОВОМУ КОНФЛІКТІ В НАГІРНОМУ КАРАБАСІ

Аналіз останніх військових конфліктів і локальних війн в Україні, Сирії, Лівії та інших регіонах планети наочно демонструє, що практично в кожному з них має місце новий формат ведення бойових дій, руйнуються класичні уявлення про форми та методи збройної боротьби на полі бою, вносяться суттєві корективи у стратегію і тактику досягнення переможних для кожної сторони результатів. Одним із них став так званий "карабаський конфлікт" між Вірменією та Азербайджаном за контроль над територією Нагірного Карабаху. Події вересня –листопада 2020 р. в науковому середовищі отримали назву "війна дронів". Саме завдяки сучасним дронам Азербайджан завоював перевагу в повітрі та використав її для досягнення стратегічної переваги у війні. Сучасні безпілотні літальні апарати (БпЛА) здатні не лише ефективно виявляти противника вдень та вночі, наводити на нього власні вогневі засоби, але й самостійно знищувати його на значній відстані від поля бою.

У статті розглянуто застосування масованого нальоту БпЛА проти зенітно-ракетних комплексів (ЗРК) протиповітряної оборони (ППО) у військовому конфлікті на території Нагірного Карабаху. Таке застосування БпЛА на засоби ЗРК ППО призвело до швидкого вичерпання їх бойового ресурсу і, як наслідок, подальшої нездатності цих комплексів вирішувати завдання за своїм призначенням. Аналіз результатів бойового застосування засобів ППО проти сучасних БпЛА показав, що дальність виявлення ЗРК апаратурою БпЛА стала порівняно однаковою, а часом і перевищує її. В ході військового конфлікту в Нагірному Карабасі була розроблена нова тактика застосування БпЛА, яка дозволяє забезпечити гарантоване ураження ЗРК і тим самим здійснити функціональне придушення системи ППО і забезпечити завоювання переваги в повітрі. Для науково-обґрунтованого підтвердження можливості успішного знищення зенітного ракетно-гарматного комплексу (ЗРГК) групою БпЛА проведено аналітико-імітаційне моделювання та зроблені відповідні висновки для вирішення військового конфлікту на Донбасі.

O. Cherednychenko, Y. Protsiuk, O. Shemendiuk, E. Lebed. Analysis of the experience of the combat use of unmanned aerial vehicles against anti-aircraft missile systems in the military conflict in Nagorno-Karabakh.

An analysis of the latest military conflicts and local wars in Ukraine, Syria, Libya and other regions of the planet clearly demonstrates that practically in each of them there is a new format of warfare, traditional ideas about the forms and methods of armed struggle on the battlefield are being destroyed, and significant adjustments are being made. in the strategy and tactics of achieving victorious results for each side. One of them was the so-called "Karabakh conflict" between Armenia and Azerbaijan over control over the territory of Nagorno-Karabakh. The events of September-November 2020 in the scientific community have been called the "drone war". It was thanks to modern drones that Azerbaijan gained air superiority and used it to achieve a strategic advantage in the war. Modern unmanned aerial vehicles (UAVs) are able not only to effectively identify the enemy day and night, direct their own firepower at him, but also independently destroy him at a considerable distance from the battlefield.

The article discusses the use of a massive UAV raid against anti-aircraft missile systems (SAM) of air defense (air defense) in a military conflict on the territory of Nagorno-Karabakh. Such use of UAVs for air defense air defense systems led to the rapid depletion of their combat resource and, as a consequence, the further inability of these complexes to solve tasks according to their intended purpose. An analysis of the results of the combat use of air defense systems against modern UAVs showed that the detection range of the air defense missile system by the UAV equipment has become relatively the same, and sometimes even exceeds it. In the course of the military conflict in Nagorno-Karabakh, a new tactic for the use of UAVs was developed, which makes it possible to ensure the guaranteed defeat of the air defense missile system and thereby carry out the functional suppression of the air defense system and ensure the gains of air superiority. For a scientifically substantiated confirmation of the possibility of successful destruction of an anti-aircraft missile-gun complex (AMC) by a UAV group, analytical and simulation modeling was carried out and appropriate conclusions were drawn to resolve the military conflict in Donbass.

Ключові слова: *безпілотний літальний апарат, протиповітряна оборона, протидія безпілотним літальним апаратам, зенітно-ракетний комплекс, зенітний ракетно-гарматний комплекс, зенітно-артилерійський комплекс, бойова ефективність, бойова живучість.*

Постановка завдання. У даний час з появою середніх і малих безпілотних літальних апаратів (БпЛА) тактика їх застосування проти зенітно-ракетних комплексів (ЗРК)

протиповітряної оборони (ППО) в ході військових конфліктів останніх років суттєво змінилася. Досвід останніх військових конфліктів свідчить, що застосування масованого нальоту БпЛА на засоби ЗРК ППО веде до швидкого вичерпання бойового ресурсу ЗРК і подальшої їх нездатності відбити удар вже пілотованої авіації, а також крилатих ракет високоточної зброї (ВТЗ). Саме тому виникла необхідність дослідити застосування масованого нальоту БпЛА на засоби ЗРК ППО з урахуванням викликів сьогодення.

Аналіз останніх досліджень і публікацій [1–7] показав, що в ході військових конфліктів останніх років засобів ППО проти сучасних БпЛА вони із засобів захисту поступово стали об'єктами "полювання" для БпЛА противника. Так, наприклад, дальність виявлення зенітних ракетно-гарматних комплексів (ЗРГК) апаратурою БпЛА часом навіть перевищує (при впливі навмисних перешкод) дальність виявлення БпЛА апаратурою ЗРГК. Крім того, досвід застосування БпЛА в ході військового конфлікту в Нагірному Карабасі показав, що БпЛА застосовуються у складі груп, які вирішують як розвідувальні, так і ударні завдання одночасно. Вплив перешкод призводить як до зниження дальності виявлення БпЛА з боку радіолокаційної станції (РЛС) ЗРГК, так і до зниження ймовірності правильного цілевказівки зенітним керованим ракетам (ЗКР). У результаті розмір зони ураження ЗРГК засобами, розміщеними на ударному БпЛА, також можна порівняти з розміром зони ураження БпЛА.

Метою статті є аналіз та систематизація нової тактики бойового застосування груп БпЛА для ураження ЗРК і придушення системи ППО.

Виклад основного матеріалу дослідження

Внаслідок військового протистояння в Нагірному Карабасі була розроблена нова тактика застосування БпЛА – застосування легких і дешевих БпЛА масовано, групами, під прикриттям більш важких розвідувальних БпЛА, обладнаних засобами радіолокаційної (РЛР), оптико-електронної розвідки (ОЕР) і комплексами радіоелектронного придушення (РЕП), в рамках вирішення завдань ураження ЗРК і ЗРГК систем ППО. Аналіз бойового застосування показав надзвичайно низький рівень бойової живучості ЗРГК в умовах масованого застосування БпЛА.

Незалежно від того, як буде складатися подальший розвиток подій у військових конфліктах, спостерігається тенденція підвищення ефективності застосування БпЛА для придушення ППО, завоювання переваги в повітрі і поразки основних сухопутних засобів озброєння. Це дозволяє зробити висновок про можливу близьку зміну стратегії ведення воєн в частині застосування БпЛА. У війнах найближчого майбутнього можливе масове багатоетапне застосування груп легких розвідувальних і розвідувально-ударних БпЛА, а також "БпЛА-камікадзе".

Подальший розвиток тактики групового застосування БпЛА істотно ускладнить умови функціонування ЗРК і ЗРГК, а також потребує кардинального перегляду ідеології створення систем ППО [1].

Війна у Нагірному Карабасі

Восени 2020 року розпочався військовий конфлікт між Вірменією й Азербайджаном в Нагірному Карабасі. Характерною рисою даного конфлікту було масоване застосування з боку Азербайджану БпЛА для знищення засобів озброєння та живої сили Вірменії.

На озброєння Азербайджану безпосередньо перед початком конфлікту надійшли турецькі БпЛА Bayraktar TB2, оснащені керованими авіабомбами MAM з лазерним наведенням, а також ізраїльські БпЛА Heron TP і Hermes 4507, баражуючі "БпЛА-камікадзе" Sky Striker і Harop. Крім того, в Азербайджані, на спільному з Ізраїлем підприємстві випускалися БпЛА Aerostar, а також "БпЛА-камікадзе" Orbiter-1K і Orbiter-3 [2].

Вірменія в останні роки закупівлею БпЛА не займалася. При цьому вона сама розробляє розвідувальний БпЛА легкого класу "Крунк", який не призначений для вирішення ударних завдань. Станом на початок конфлікту на озброєнні ЗС Вірменії стояли різні системи ППО радянського та російського виробництва, при цьому прикриття повітряного простору безпосередньо над територією Нагірного Карабаху забезпечували ЗРК "Оса" і "Стріла" які орієнтовані на знищення літаків та гелікоптерів і не призначені для боротьби з БпЛА (рис. 1) [3]. Раніше Вірменія закуповувала у Росії ЗРК "Тор", які можна було б ефективно застосовувати проти БпЛА, проте на території Нагірного Карабаху їх не розміщували [2].

Рис. 1. Розміщення засобів ППО на початок військового конфлікту в Нагірному Карабасі [3]

З початком бойових дій в Нагірному Карабасі, як показано в роботах [2–4], азербайджанські збройні сили за підтримки турецьких військових фахівців розгорнули масове групове застосування ударних БпЛА, з урахуванням досвіду застосування БпЛА в Сирії та Лівії. Без застосування БпЛА у війні в Нагірному Карабасі вірменські системи ППО були б цілком спроможні щодо стримування азербайджанської авіації. Не випадково, навіть отримавши перевагу в повітрі, Азербайджан дуже обмежено використовував свою пілотовану авіацію, так як ЗРК, що залишались на озброєнні Вірменії, продовжували являти для них серйозну загрозу. Однак Вірменія виявилася абсолютно не готова до війни з масовим використанням БпЛА, тактику якої хусити відпрацювали в Ємені, а турки – в Сирії та Лівії. Результатом масованого застосування груп БпЛА Bayraktar TB2, спільно з “БпЛА-камікадзе” Sky Striker, Harop і Orbiter, стало практично повне знищення вірменських ЗРК “Оса” і “Стріла-10”, розміщених в Нагірному Карабасі, в перші дні конфлікту. В перший день війни по позиціях цих ЗРК був нанесений заздалегідь підготовлений удар, який позбавив оборону Нагірного Карабаху, за оцінками фахівців, до 80 % комплексів ППО – 6 ЗРК “Оса” і 3 ЗРК “Стріла-10” при втратах в 4 БпЛА [4; 5]. Отже, за рахунок масовості і раптовості застосування, забезпечивши обмін 2,25 ЗРК на 1 БпЛА, завоювання переваги в повітрі дало можливість Азербайджану за допомогою БпЛА безперервно, в цілодобовому режимі, і безперешкодно атакувати вірменські мотострілкові та механізовані частини, завдаючи їм істотні втрати ще до того, як вони вступали в бій з силами Азербайджану. Це значно полегшило наступ азербайджанської армії і дозволило добитися істотних тактичних успіхів. При цьому комплекси ППО, що залишилися на озброєнні Вірменії, такі як С-300ПС та С-300ПТ, не призначені для боротьби з БпЛА, в зв’язку з чим вони не можуть бути ефективно використані для оборони повітряного простору Вірменії і Нагірного Карабаху від цього нового типу загроз. Більш того, в результаті грамотно спланованої операції силами БпЛА були знищені 2 пускові установки і 2 РЛС зі складу ЗРК С-300ПС. За інформацією ЗМІ [6; 7] один зі знищених ЗРК С-300ПС входив до складу системи ППО Вірменії і знаходився на відкритій місцевості без будь-якого додаткового прикриття. Причиною тому послужило те, що на першому етапі військового конфлікту Азербайджан використовував літаки Ан-2 в безпілотному виконанні, щоб виявити місце розташування вірменських систем ППО. Літаки були збиті, але це дозволило розкрити місце розташування як ЗРК С-300ПС, так і ЗРК ближнього радіусу дії “Оса” і “Стріла-10М3”, які здійснювали його прикриття. Після знищення ЗРК ближнього радіусу дії ЗРК С-300ПС залишився без прикриття і пускова установка 5П85С, а також РЛС типу 36Д6, що

входять до складу ЗРК, були вражені за допомогою "БпЛА-камікадзе" ізраїльського виробництва Нагор.

Таке масове ефективне застосування БпЛА для виявлення і знищення спочатку системи ППО, а в подальшому – живої сили і озброєння сухопутних військ, яке було використано у війні в Нагірному Карабасі, зустрічається у світовій практиці вперше і отримало в ЗМІ назву "війна дронів". Азербайджанська сторона широко розповсюдила в ЗМІ відеозаписи високоточних ударів БпЛА по вірменських позиціях. Основні цілі ударів – це, перш за все, засоби ППО, потім – бронетанкові колони на марші, танки і артилерія на позиціях, рідше – склади, сховища і казарми [2; 3]. Після знищення основних сил системи ППО в Нагірному Карабасі вірменська сторона виявилася нездатна швидко заповнити їх ресурс за рахунок нових ЗРК. Вона опинилася в ситуації, коли противник, завоювавши перевагу в повітрі, використовує її для досягнення стратегічного переваги у війні. Це робить неминучим зростання кількості втрат і наростання проблем в обороні сухопутних військ від масованих ударів БпЛА з повітря.

Таблиця 1

Приблизні показники середнього розміну кількості знищених БпЛА на кількість знищених ЗРК і ЗРГК системи ППО

Військовий конфлікт	Показник розміну
Війна в Сирії (2017–2019 рр.)	1 ЗРГК за 5 БпЛА
Війна в Лівії (2019 р.)	1 ЗРГК за 2,8 БпЛА
Війна в Нагірному Карабасі (2020 р.)	2,25 ЗРК за 1 БпЛА

Аналіз поліпшення показника розміну "БпЛА за ЗРК" (табл. 1) паралельно з удосконаленням тактики групового застосування БпЛА дозволяє зробити наступні висновки. Незалежно від того, як складеться подальший розвиток подій у війні за Нагірний Карабах, очевидна тенденція підвищення ефективності застосування БпЛА для завоювання панування в повітрі і знищення основних сухопутних засобів озброєння – бронетехніки. Це дозволяє зробити висновок про можливу близьку зміну стратегії ведення воєн в частині застосування БпЛА.

У війнах найближчого майбутнього можливе масове багатоетапне застосування груп легких розвідувальних і розвідувально-ударних БпЛА, а також "БпЛА-камікадзе". На першому етапі – для розвідки противника. На етапі нанесення першого удару – для виявлення і знищення засобів ППО, а в подальшому – знищення літаків і гелікоптерів пілотованої авіації на землі і в повітрі. Після завоювання переваги в повітрі – знищення бронетехніки й живої сили сухопутних військ, об'єктів тилу та критичної державної інфраструктури.

Моделювання групової атаки БпЛА на ЗРГК

Для науково-обґрунтованого підтвердження можливості успішного знищення ЗРГК групою БпЛА проведено аналітико-імітаційне моделювання. Зокрема, розглянута умовна задача відображення нальоту групи БпЛА на об'єкт ЗРГК. При цьому об'єкт ЗРГК являє собою ділянку місцевості, в центрі якого знаходиться ЗРГК. Завданням ЗРГК є ураження всіх БпЛА, які намагаються увійти в зону його відповідальності з радіусом 2 км (рис. 2) шляхом застосування своїх засобів ураження.

Моделювання даної тактичної задачі представлено в роботі [1], а результати моделювання – на рис. 2.

На відстані 25 км від ЗРГК розташовується 10-кілометрова зона (світло-сіре кільце), з якої одночасно стартує невпорядкована однорідна група БпЛА. Кожен БпЛА має свій номер. Політ кожного БпЛА здійснюється автономно в секторі 90^0 і не синхронізується з іншими членами групи. Розглядаються БпЛА літакового типу зі стартовою масою 10 кг.

Дальність виявлення БпЛА за допомогою оптико-електронної системи (ОЕС) та радіолокаційної станції (РЛС), що входять до складу ЗРГК, залежно від висоти польоту, становить 1,5–2,5 км. Таким чином, кількість повітряних цілей становить 15 одиниць, що летять зі швидкостями від 100 км/год до 300 км/год на висотах 200–800 м [1].

Середнє значення ймовірності ураження одиночної повітряної цілі вогневими засобами ЗРГК $P_{пор} \approx 0{,}26$.

Запас засобів ураження ЗРГК становить 16 одиниць: 16 черг по 100 снарядів або 16 зенітних ракет чи їх поєднання в різному співвідношенні. Пріоритетність цілі p визначалося за критерієм мінімально наявного часу t для застосування засобів ураження ЗРГК [1]:

$$p=min\ \{t_i \mid t_i \frac{D_i \cos\varphi_i}{V_i \cos\theta_i \cos\psi_i} + \frac{\delta_i}{\omega_{пов}}\},$$

де D_i – похила дальність до i-го БпЛА;

φ_i – кут місця i-го БпЛА;

V_i – швидкість польоту i-го БпЛА;

θ_i – кут нахилу траєкторії руху i-го БпЛА;

ψ_i – відносний курс польоту i-го БпЛА;

δ_i – кут неузгодженості осі спрямованості засобу ураження ЗРГК і азимута i-го БпЛА;

$\omega_{пов}$ – кутова швидкість повороту осі спрямованості засобу ураження ЗРГК;

i-номер БпЛА;

p – пріоритет впливу по БпЛА.

Результати ранжирування БпЛА за критерієм пріоритетності показані на рис. 3, а на рис. 4 – потрібні кути довороту осей спрямованості засобів ураження ЗРГК (стовбурів зенітних гармат або направляючих зенітних ракет) для стрільби по БпЛА.

Фізичний час модельованого нальоту групи БпЛА на об'єкт, що не прикривається, склав 10 хв.

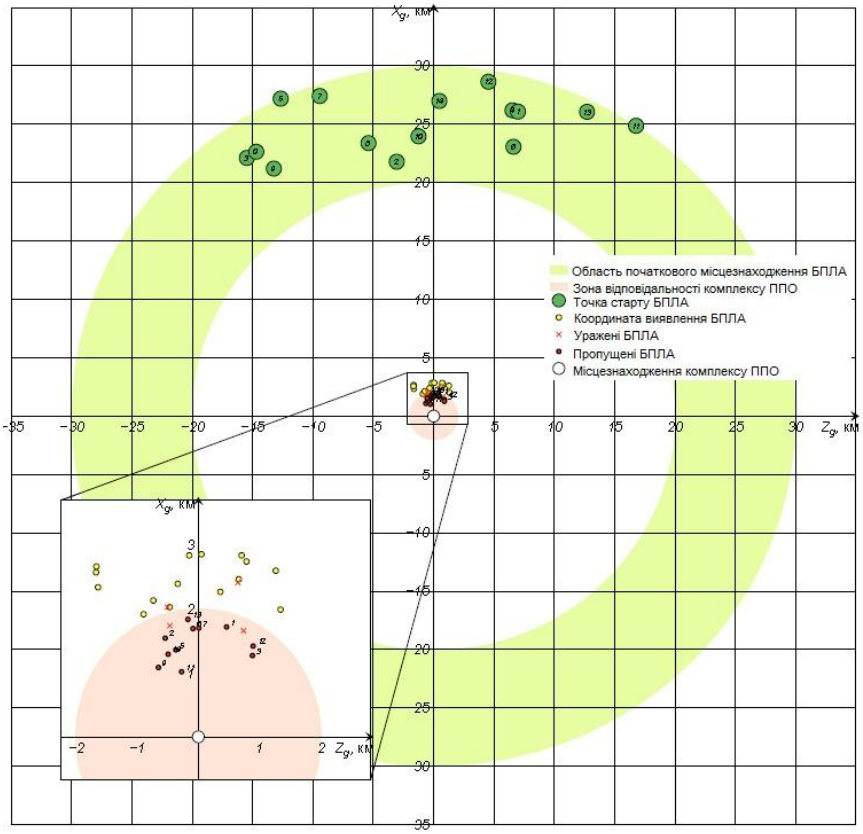


Рис. 2. Результати моделювання нальоту групи БпЛА на ЗРГК [1]

В результаті моделювання можна зробити наступні висновки [1]:

– ЗРГК не забезпечив прикриття об'єкта: 10 з 15 БпЛА увійшли в зону відповідальності ЗРГК і змогли застосувати свої засоби ураження;

– великі кути довороту осей засобів ураження ЗРГК на перші 10 БпЛА (рис. 4) призвели до фізичної неможливості поразки цих цілей;

– ЗРГК витратив весь свій боєзапас, не виконавши поставлене завдання з прикриття об’єкта.

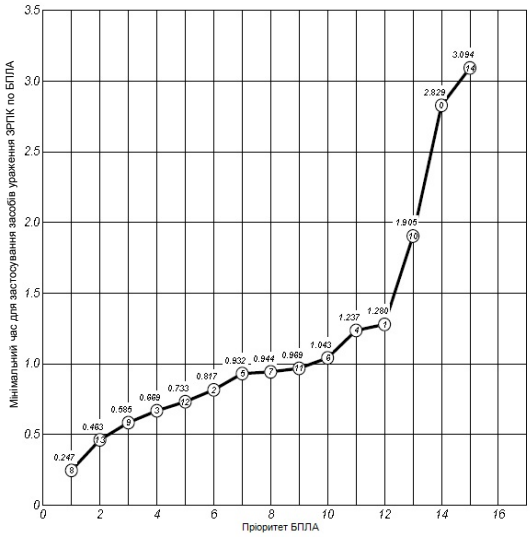


Рис. 3. Результати розподілу пріоритетності цілей в групі БпЛА [1]

Основний висновок – результати моделювання переконливо доводять низьку живучість ЗРГК в умовах масованого нальоту групи БпЛА і теоретично підтверджують можливість успішного ураження ЗРК і ЗРГК систем ППО групами БпЛА, що було зафіксовано у Нагірному Карабасі. Результати моделювання досить переконливо демонструють, що групове застосування БпЛА вже сьогодні є серйозним фактором для придушення комплексів ППО малими витратами. Подальший розвиток технології групового застосування БпЛА істотно ускладнить умови функціонування комплексів ППО [1].

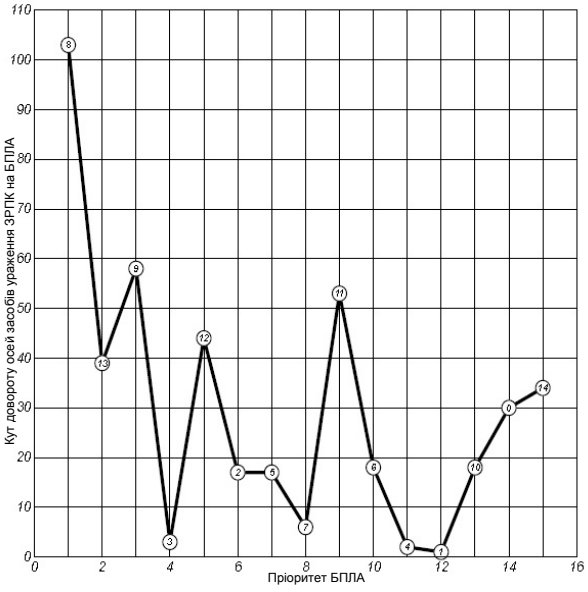


Рис. 4. Результати визначення кутів довороту осей засобів ураження ЗРГК на БпЛА по їх пріоритетам [1]

При цьому системним недоліком системи управління вогнем деяких ЗРГК і ЗРК (наприклад, “Панцир-С1/С2” і “Тор-М1/М2”) є те, що їх зенітна керована ракета (ЗКР) вимагає управління протягом всього польоту, а кількість одночасно обстрілюваних цілей обмежена 3-4. При цьому одночасно обстрілювані цілі повинні знаходитися в зоні огляду РЛС наведення.

В результаті неможлива одночасна робота по цілям, атакуючим з різних напрямків, а якщо врахувати, що для ураження небезпечних або складних цілей можуть знадобитися одночасно дві ЗКР, то ситуація ще більше ускладнюється. Дана проблема має системний характер, і збільшення боєкомплекту ЗКР не буде являтися виходом із ситуації, тому що інтенсивність роботи ЗРК за програмними цілями все одно буде обмежена невеликою кількістю каналів одночасного наведення ЗКР на ціль. При цьому, як наголошується в роботі [8], це ще не враховуються можливості БпЛА нести апаратуру РЕП і формувати помилкові цілі. У цьому випадку ймовірність ураження БпЛА в групі ще більше знизиться, а витрата боєприпасів ЗРК – істотно зросте.

Висновки для Збройних сил України

Бойові дії із застосуванням БпЛА у Нагірному Карабаху дали гарний матеріал керівництву Збройних сил для його детального вивчення та оптимальної адаптації до своїх потреб та наглядно продемонстрували перспективні потреби військ на полі бою:

Збільшення кількості БпЛА у своїх бойових порядках безпілотних систем, включно з додатковою закупівлею Bayraktar TB2 і в подальшому власне їх виробництво чи більш досконалих аналогів вітчизняного виробництва. Пришвидшити роботи з Туреччиною щодо розгортання виробництва на території України БпЛА на кшталт Bayraktar TB2 як стартового проєкту з переходом на нові ударно-розвідувальні зразки БпЛА – з максимальним розширенням локалізації і додаванням до проєкту нових можливостей від українських компаній. Обумовити модернізацію закуплених Bayraktar TB2. Зокрема, за рахунок компонування апарату блоками для SATCOM, що призначені для супутникового зв'язку з БпЛА. З застосуванням системи SATCOM будуть зняті обмеження на використання розвідувально-ударного потенціалу БпЛА незалежно від дальності польоту БпЛА.

Розробити типовий ряд модульних лазерних головок самонаведення для засобів враження, що здатні взаємодіяти з лазерними підсвітлювачами оптико-електронної системи Wescam CMX-15D. Провести аналіз вітчизняних засобів/розробок РЕБ наземного та повітряного базування з огляду на їхню реальну ефективність та необхідну спроможність ускладнювати роботу РЛС та ЗРК противника. Як штатних, так і перспективних – відповідно до планів постачань нових ЗРК в Західний та Південний військовий округи ЗС Російської Федерації.

Висновки. У статті представлені результати аналізу досвіду бойового застосування груп БпЛА у військових конфліктах останніх років, зокрема, в Нагірному Карабасі. Аналіз дозволив розкрити основні недоліки сучасних комплексів ППО, як об'єктів поразки, а також провести детальний аналіз групового застосування БпЛА та їх ефективності при роботі по цілях такого типу. Елементом новизни роботи є узагальнення досвіду бойового застосування груп БпЛА для придушення системи ППО, а також виявлення системних недоліків і технологічних рішень, які використовуються в комплексах ППО, що призводять до зниження їх бойової ефективності і живучості в умовах застосування проти них груп БпЛА. Матеріал статті може використовуватися для формування вихідних даних для моделювання та дослідження бойової ефективності і живучості ЗРК і ЗРГК в умовах застосування груп БпЛА. Також дана стаття може бути корисна військовим фахівцям при оцінці параметрів групи БпЛА, які гарантовано долають зону ППО супротивника при вирішенні своїх цільових завдань. Все це мають врахувати Збройні сили України та швидко провести детальну роботу з огляду на загрозу агресора над нашими кордонами і в глибині нашої держави. Адже ворог так само аналізує і робить висновки з того, що саме нового і важливого продемонстрував у різних формах та способах черговий збройний конфлікт із застосуванням безпілотних комплексів.

Подальшим напрямком наукових досліджень може бути розвиток технології групового застосування БпЛА.

ЛІТЕРАТУРА

1. Ростопчин В. В. Ударные беспилотные летательные аппараты и противовоздушная оборона – проблемы и перспективы противостояния // ResearchGate. URL: https://www.researchgate.net/publication/331772628_Udarnye_bespilotnye_letatelnye_apparaty_i_protivovozdusnaa_oborona_problemy_i_perspektivy_protivostoania.

2. Аксенов П. Война дронов в Карабахе: как беспилотники изменили конфликт между Азербайджаном и Арменией // BBC News. URL: https://www.bbc.com/russian/features-54431129 (дата звернення: 06.10.2020).

3. Рожин Б. Нагорный Карабах стал первой войной эпохи ударных беспилотников // Федеральное агенство новостей. URL: https://riafan.ru/1320335-nagornyi-karabakh-stal-pervoi-voinoi-epokhi-udarnykh-bespilotnikov (дата звернення: 12.10.2020).

4. Тучков В. Воздушную фазу битвы за Карабах Ереван уже проиграл // Свободная Пресса. URL: https://svpressa.ru/war21/article/277832/ (дата звернення: 06.10.2020).

5. В Карабахе турецкие Bayraktar TB2 уничтожили советские “Осы” и “Стрелы” // Lenta.ru. URL: https://lenta.ru/news/2020/09/29/bayraktartb2/ (дата звернення: 29.09.2020).

6. В Сети появились снимки уничтоженного ЗРС С-300 ВС Армении // Военное обозрение. URL: https://topwar.ru/176473-v-seti-pojavilis-snimki-unichtozhennogo-zrs-s-300-vs-armenii.html (дата звернення: 26.10.2020).

7. Даманцев Е. Беспрепятственное поражение радара 36Д6 и самоходной ПУ 5П85С армянского С-300ПС: повод для пафосных реляций азербайджанских СМИ или очередные заблуждения? // Военное обозрение. URL: https://topwar.ru/176019-besprepjatstvennoe-porazhenie-radara-36d6-i-samohodnoj-pu-5p85s-armjanskogo-s-300ps-povod-dlja-pafosnyh-reljacij-azerbajdzhanskih-smi-ili-ocherednaja-porcija-nelepyh-zabluzhdenij.html (дата звернення: 14.10.2020).

8. Тимохин А. Решение проблемы «насыщающих» атак ПВО // Военное обозрение. URL: https://topwar.ru/157073-reshenie-problemy-nasyschajuschih-atak-pvo-ono-est-i-nad-nim-rabotajut.html (дата звернення: 22.04.2019).

АВТОРИ НОМЕРА

1. ***Бовда Владіслав Едуардович*** – старший науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

2. ***Боголій Сергій Миколайович*** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

3. ***Бєляков Роберт Олегович*** – кандидат технічних наук, доцент, докторант НОВ Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

4. ***Гурський Тарас Григорович*** – кандидат технічних наук, доцент, заступник начальника кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

5. ***Конотопець Микола Миколайович*** – кандидат технічних наук, доцент, доцент інституту Державної служби спеціального зв'язку та захисту інформації України.

6. ***Кузавков Василь Вікторович*** – доктор технічних наук, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

7. ***Лаврік Іван Васильович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

8. ***Лазута Роман Романович*** – провідний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

9. ***Лебідь Євген Віцентійович*** – кандидат технічних наук, заступник начальника факультету з навчальної та наукової роботи – начальник навчальної частини факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

10. ***Лозунов Володимир Костянтинович*** – головний спеціаліст відділу супроводження та розвитку АСУ в/ч А0307.

11. ***Макарчук Василь Іванович*** – старший науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

12. ***Макарчук Олександр Мусійович*** – кандидат технічних наук, доцент, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

13. ***Марчук Олександр Віталійович*** – викладач кафедри кібербезпеки факультету бойового застосування систем управління та зв'язку Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

14. ***Міночкін Анатолій Іванович*** – заслужений працівник освіти України, доктор технічних наук, професор, провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

15. ***Михайлюк Сергій Станіславович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

16. ***Остапчук Віктор Миколайович*** – начальник Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

17. ***Остапук Олександр Іванович*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

18. ***Панченко Ігор В'ячеславович*** – кандидат технічних наук, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

19. ***Плугова Ольга Богданівна*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

20. ***Побережець Тетяна Василівна*** – науковий співробітник науково-дослідного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

21. ***Погребняк Сергій Васильович*** – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

22. ***Процюк Юрій Олександрович*** – провідний науковий співробітник науково-дослідної лабораторії Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

23. ***Радзівілов Григорій Данилович*** – кандидат технічних наук, заступник з наукової роботи начальника Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

24. ***Самойлов Ігор Володимирович*** – кандидат технічних наук, доцент, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

25. ***Сторчак Антон Сергійович*** – кандидат технічних наук, старший викладач інституту Державної служби спеціального зв’язку та захисту інформації України.

26. ***Толюпа Сергій Васильович*** – доктор технічних наук, професор, професор кафедри кібербезпеки Київського національного університету імені Тараса Шевченка, м. Київ, Україна.

27. ***Фесенко Олексій Дмитрович*** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

28. ***Хижий Олександр Ігорович*** – слухач Національного університету оборони України імені Івана Черняховського.

29. ***Чевардін Владислав Євгенійович*** – доктор технічних наук, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

30. ***Шемендюк Олександр Віталійович*** – начальник відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

31. ***Чередниченко Олексій Юрійович*** – старший науковий співробітник науково-дослідної лабораторії Наукового центру зв’язку та інформатизації систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

32. ***Штаненко Сегрій Станіславович*** – кандидат технічних наук, доцент, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

ПАМ'ЯТКА АВТОРУ

Рукопис статті потрібно подавати разом із зазначеними нижче документами українською мовою:

– *актом експертизи* (1 примірник);

– *рецензіями (зовнішньою або внутрішньою)* – за підписом провідного ученого, який працює в даному напряму досліджень;

– *довідкою про автора (авторів).*

Рукопис подається у двох видах: на флеш-пам'яті або CD, розпечатаний на лазерному принтері (1 примірник), у текстовому редакторі – **Microsoft Word 10**, а також може бути надісланий за електронною адресою: **naukaviti@gmail.com.**

Формат аркуша – **А4 (210 мм × 297 мм).**

Розмір полів: зліва – **20 мм**, справа – **20 мм**, зверху – **20 мм**, знизу – **20 мм.**

Стиль – **normal** (звичайний), інтервал між рядками – **1,0**, абзацний відступ – **1 см.** Шрифт – **Times New Roman № 12**, із виключенням переносів.

Анотацію друкують курсивом, шрифт **Times New Roman № 10.** Анотацію та ключові слова приводять українською та англійською мовами. Обсяг кожної з них не менше 1800 знаків з побілами, включаючи ключові слова. Анотація повинна бути структурована таким чином: вступ, проблематика, мета, матеріали й методи, результати, висновки. Іншими словами, анотація повинна відображати послідовну логіку опису результатів, описувати основну мету дослідження та підсумовувати найбільш значимі результати. Скорочення слів в анотації не застосовувати.

Після анотації 3–4 ключові слова українською, англійською мовами. Список використаних джерел оформляється 11 шрифтом, згідно з ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання (не використовувати тире «–»).

Етапи представлення статті для науковців інституту:

1. Стаття подається на розгляд головному редактору та після погодження – відповідальному редактору.

2. Після позитивного розгляду редколегією стаття подається коректору (кімната № 5 редакційно-видавничого відділу) для вичитки та корегування.

Виправлення електронного варіанта статті.

Друкування виправленого варіанта статті, отримання розпису коректора про виправлення помилок, що були виявлені, на останньому аркуші статті.

3. Виправлена стаття передається разом із супровідними документами відповідальному редактору для формування комп'ютерного макета збірника.

Не зараховуються праці, у яких відсутній повний опис наукових результатів, що засвідчує їх, достовірність, або в яких повторюються результати, опубліковані раніше в інших наукових працях, що входять до списку основних (Постанова ВАК України від 10.02.99 № 1 – 02/3).

Статті, які містять загальновідому науково-технічну інформацію, плагіат, не розглядаються й не друкуються.

В один випуск «Системи і технології зв'язку, інформатизації та кібербезпеки» приймається не більше однієї статті за темою дисертації (Постанова ВАК України від 10.02.99 № 1 – 02/3).

Тексти статей та їхні копії на магнітних чи оптичних носіях авторам не повертаються.

Редакційна колегія залишає за собою право вносити зміни в рукопис редакційного характеру.

Телефон для довідок: 256-22-37, 256-22-73, внутрішній 442-37, 442-73.

Електронна адреса для надання статей: naukaviti@gmail.com, naukaviti@viti.edu.ua.