ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Виходить 4 рази на рік

№ 64

КИЇВ – 2019

УДК621.43
ББК 32-26.8-68.49
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – № 64. – 172 с.

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень та побажань.

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації - серія КВ № 11541 – 413Р від 21.07.2006 р.

Відповідно до Наказу МОН України від 16.05.2016 № 515 «Збірник наукових праць ВІКНУ імені Тараса Шевченка» внесено до переліку наукових фахових видань із технічних наук, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук.

Затверджено на засіданні вченої ради ВІКНУ від 13.06.2019р., протокол № 14.

Відповідальні за макет:
Ряба Л.О., Солодєєва Л.В.

Адреса редакції: 03189, м. Київ, вул. Ломоносова,81 тел./факс +38 (044) 521 – 33 – 82
Наклад 300 прим.

Ел.адреса редактора: lenkov_s@ukr.net
Офіційний сайт журналу: http://miljournals.knu.ua/

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ЗАГАЛЬНІ ПИТАННЯ

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

INFORMATION TECHNOLOGIES

GENERAL QUESTIONS

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

УДК 629.7

Адамов Ю.І. (ВА, Одеса)
д.т.н., доц. **Боряк К.Ф.** (ОДАТРЯ)
к.ф-м.н., доц. **Завальнюк В.В.** (ВА, Одеса)

ВДОСКОНАЛЕННЯ ПАРАШУТНО-РЕАКТИВНОЇ СИСТЕМИ З ДЕСАНТУВАННЯ БОЙОВОЇ ТЕХНІКИ АБО КРУПНО ГАБАРИТНИХ ОБ'ЄКТІВ

В роботі розглядаються питання вдосконалення парашутно-реактивної системи (ПРС) із застосуванням сучасних радіовисотомірів з метою підвищення відсотку м'яких приземлень та забезпечення можливості коригування положення об'єкту десантування в горизонтальній площині залежно від значення кута ухилу поверхні пересічної місцевості в розрахунковій точці приземлення. Критичні значення кута нахилу об'єкта десантування до горизонту пропонується встановлювати на підставі зазначених виробником тактико-технічних даних або розрахунковим шляхом. Першочерговою задачею є підвищення точності роботи висотоміру, від якого залежить момент спрацювання піропатронів реактивних двигунів ПРС. Автори пропонують заміни механічний висотомір застарілої конструкції сучасним електронним радіовисотоміром на базі скануючої радарної решітки. В статті розглянуто особливості роботи скануючої радарної решітки, методи підвищення точності визначення висоти (відстані до поверхні землі), необхідність та шляхи врахування крену машини в процесі зниження та можливості визначення кута ухилу поверхні землі в місці приземлення. Отримані результати дозволяють підвищити точність роботи радіовисотоміра та істотно зменшити ймовірність помилкового визначення висоти внаслідок розгойдування або статичного крену об'єкту, а також виявити та врахувати особливості рельєфу місцевості.

Ключові слова: парашутно-реактивна система, скануюча радарна решітка, кут ухилу поверхні землі, термінальна швидкість зниження, швидкість зниження.

Постановка проблеми. Десантування важких об'єктів з літаків пов'язано з необхідністю їх доставки у район застосування за призначенням у найкоротші терміни [1-3]. При десантуванні важких об'єктів з літаків найбільшу швидкість, надійність та точність приземлення об'єкту забезпечують парашутно-реактивні системи (ПРС). Для забезпечення безпечного приземлення особливо важливим є питання визначення оптимальної висоти (відстані до поверхні землі) спрацювання піропатрону реактивного двигуна ПРС. Метою роботи є вдосконалення парашутно-реактивної системи в напрямку підвищення надійності, точності та безпечності десантування об'єкту шляхом застосуванню радіолокаційної системи на базі скануючої радарної решітки замість традиційних механічних пристроїв (щупів) та можливості коригування у просторі від 0º до 90º в горизонтальній площині положення об'єкта десантування у залежності від значення кута нахилу поверхні пересічної місцевості в розрахунковому місці приземлення.

Аналіз останніх досліджень та публікацій. На сьогодні для цього використовуються застарілі механічні пристрої у вигляді двох щупів, які ініціюють запуск гальмівної системи (спрацювання піропатронів реактивного двигуна ПРС) у момент механічного контакту з поверхнею землі (або іншою перешкодою).

Довжина щупів виставляється перед десантуванням з урахуванням як маси об'єкту, так і температурних умов, за яких відбувається його десантування, – температури атмосферного повітря та температури пороху реактивної гальмівної системи [4,5]. Проблема визначення необхідної довжини щупів ПРС розглядається у навчальних посібниках з питань забезпечення десантування важкої повітрянодесантної техніки та у останніх публікаціях із визначення впливу похибок на швидкість приземлення об'єкту [6,7].

Ця механічна система має цілий перелік недоліків, основними з яких є неможливість точного передбачення температури повітря в місці десантування, неможливість врахування наявності та потужності висхідних потоків повітря, висока ймовірність похибки у визначенні повної маси об'єктів перед десантуванням, втрата працездатності щупів у разі їх ушкодження чи деформування після десантування [6].

Одним із найбільш перспективних шляхів вдосконалення системи ПРС із одночасним вирішенням значної частини перелічених вище проблем є заміна механічних висотомірів (щупів) дистанційним висотоміром [8]. До потенційних варіантів приладів, що можуть претендувати на дане застосування, відносяться

- оптичні висотоміри[9];

- імпульсні радіовисотоміри (дають малу похибку при роботі на великих висотах, проте, як правило, мають серйозне обмеження мінімальної висоти в діапазоні 30-70 м, що не підходить для даної задачі) [10];

- радіолокатори безперервного випромінювання з частотною модуляцією (добре підходять для вимірювання порівняно малих відстаней та мають похибку вимірювань на рівні до 3%, тобто до 0.6 м на відстані 20 м; задовольняють приведені вище вимоги з максимальної відстані роботи [11,12];

Окрім того, можуть виникнути проблеми із передбаченням рельєфу поверхні землі у місці приземлення при десантуванні (завеликий кут ухилу поверхні або пересічена місцевість), тим самим збільшуючи ймовірність занадто жорсткого приземлення об'єкту (особливо спеціальної техніки) чи втрати його стійкості (перевертання) після приземлення. Ця проблема також може бути вирішена за допомогою інформації, отриманої радіовисотоміром протягом зниження, її комп'ютерної обробки та наступного керування процесом зниження тим чи іншим шляхом. Тому актуальність вирішення питання вдосконалення засобів ПРС для десантування спеціальної техніки й інших об'єктів із метою підвищення її надійності, точності та безпечності десантування не визиває сумніву.

Виклад основного матеріалу. Серед розглянутих варіантів висотомірів найбільш привабливим за своїми технічними характеристиками ми вважаємо дистанційний радіовисотомір на базі скануючої радарної решітки. Розглянемо більш детально схему застосування такого радару в процесі зниження об'єкту та критерії увімкнення двигуна ПРС.

Типова радарна решітка сканує простір уздовж заданої прямої із частотою ν, отримуючи відповідний масив l_i відстаней до землі у заданих напрямках сканування φ_i (де $i = 1 \ldots n$, де n – число вимірювань відстані протягом одного сканування; кути φ_i визначаються приладом відносно перпендикуляру до горизонтальної площини об'єкту).

Внаслідок того, що при кожному вимірюванні відстані до поверхні землі РЛС протягом певного часу очікує на повернення відбитого сигналу, після чого переналаштовується на наступний напрямок вимірювання, то проведення повного сканування займає деякий проміжок часу. Нехай, τ – середня тривалість одного вимірювання, тоді повна тривалість одного сканування дорівнюватиме $(n \cdot \tau)$. Зрозуміло, що максимальна кількість сканувань, що виконуються за одну секунду не може перевищувати числа $\nu = 1/(n \cdot \tau)$. Наявність цих затримок разом із фактом неперервного зниження машини, призводить до того, що відстані до поверхні землі, виміряні протягом одного сканування, відповідають різним значенням поточної висоти (рис. 1).

Необхідність врахування зміни висоти протягом одного сканування залежить від його повної тривалості $(n \cdot \tau)$ та швидкості зниження υ.

Якщо, наприклад, $\upsilon \approx 20$ м/с, $n = 5$, $\tau = 0{,}004$ с, то зміна Δh поточної висоти бойової машини над поверхнею Землі протягом одного сканування становитиме $\Delta h = \upsilon \cdot n \cdot \tau = 20 \cdot 5 \cdot 0{,}004 = 0{,}4$ м, що перевищує верхню межу похибки вимірювання відстані. Відповідно, у такому випадку при визначенні поточної висоти машини необхідно враховувати її вертикальний рух.

Якщо ж $\upsilon \approx 20$ м/с, $n = 5$, $\tau = 0{,}0005$ с, то $\Delta h = 0{,}05$ м, тобто є нехтовно малою, а рухом машини протягом сканування можна знехтувати, вважаючи, що воно виконується миттєво.

Таким чином, врахування похибки вимірювання відстані від об'єкту до поверхні землі, яка виникає під час сканування простору внаслідок неперервного зниження машини, може ви-

явитися необхідним кроком для забезпечення цільової точності роботи вимірювальної системи. Для достатньо точного врахування даного фактору достатньо знати лише часову затримку між послідовними вимірюваннями, поточну швидкість зниження машини та кути θ_i відносно вертикалі, під якими проводилися вимірювання (за відсутності крену машини ці кути визначаються виключно налаштуваннями радару: $\theta_i = \varphi_i$).

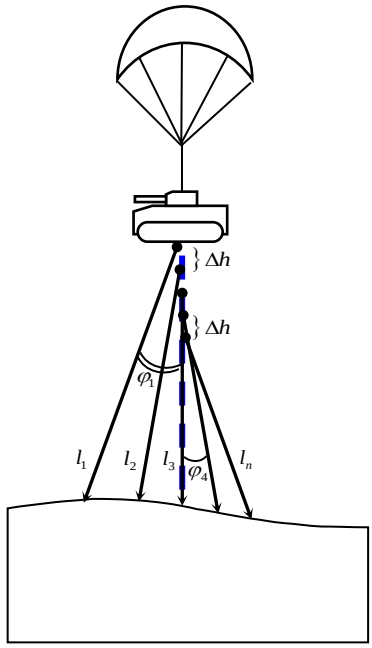


Рисунок 1 – Врахування руху машини протягом сканування

До параметрів руху, точне знання яких є найбільш важливими для забезпечення м'якого приземлення, відносяться поточна висота $h(t)$ знаходження машини над землею та миттєва швидкість $v(t)$ її зниження, які разом із масою та параметрами двигуна ПРС, визначають оптимальну висоту (відстань до поверхні землі) його увімкнення. Як $h(t)$, так і $v(t)$ вимірюються безпосередньо за допомогою радарної системи, однак на точність їх визначення може істотно впливати наявність крену β машини (і, відповідно, радара) внаслідок її розгойдування (або неправильного закріплення парашутної системи тощо), наслідком чого буде вимірювання поточної висоти не уздовж вертикального напрямку, а під деяким кутом до нього, та (у випадку малих значень кутів ухилу поверхні у місці приземлення) отримання завищених значень поточної висоти. В результаті, увімкнення двигуна ПРС відбуватиметься із деяким запізненням, приводячи до швидкості приземлення, більшої за очікувану.

Форма рельєфу поверхні землі у місці приземлення, яка можна бути спрощено описана кутом ухилу α поверхні землі (відносно горизонту), також може відчутно впливати на результат приземлення.

1. Врахування впливу затримки між вимірюваннями на точність визначення висоти. За умови відсутності розгойдування машини її поточна висота h дорівнює відстані до поверхні Землі, отриманій при вимірюванні уздовж вертикального напрямку ($\varphi = 0°$). Похибка визначення висоти радіолокаційною системою може бути зменшена за рахунок статистичного усереднення результатів вимірювань, отриманих протягом одного сканування під різними кутами відносно вертикалі або, навіть, декількох повних сканувань (залежно від їх частоти ν та швидкості зниження v машини). Даний підхід є особливо корисним у тих випадках, коли похибка вимірювання відстані радіолокаційною системою є нормально розподіленою, а також за можливості хибних спрацювань внаслідок наявності поміх (дерев, кущів, птахів, скирт сіна тощо).

При усередненні по вимірюванням одного сканування поточну висоту можна оцінити в тому числі й по значення відстаней l_i, виміряних під кутами φ_i відносно вертикалі, відмінними від нульового ($\varphi_i \neq 0$):

$$h_i = l_i \cos\varphi_i \,.\,, \tag{1}$$

де h_i – відповідні оцінки значення висоти над точкою приземлення за припущення горизонтальності поверхні Землі у цій місці.

У тих випадках, коли зміна Δh поточної висоти знаходження машини протягом одного сканування є відчутною (що визначається частотою ν проведення сканувань РЛС та швидкістю зниження υ), спершу необхідно провести приведення всіх отриманих значень висоти h_i до одного моменту часу (тут пропонується проводити приведення до моменту останнього вимірювання: $i = n$, де n – повне число вимірювань в одному скануванні; $i = 1\ldots n$ – індекс, що нумерує вимірювання; τ – проміжок часу між послідовними вимірюваннями; h_i^* – значення висоти, приведені до моменту проведення останнього вимірювання з урахуванням безперервного зниження машини протягом сканування):

$$h_i^* \approx h_i - (n-i)\upsilon\tau\,, \tag{2}$$

тобто, останнє отримане значення висоти залишається незмінним, передостаннє зменшується на величину $\upsilon\cdot\tau$ – відстань, пройдену машиною за проміжок між вимірюваннями, і так далі. Якщо ж величина зниження машини протягом сканування є малою (складає одиниці сантиметрів), тоді можна вважати, що

$$h_i^* \approx h_i\,. \tag{3}$$

В обох випадках уточнена оцінка поточного значення висоти на момент завершення сканування визначатиметься як середнє арифметичне отриманих значень h_i^*:

$$h(t) = \text{average}\,(h_i^*)\,. \tag{4}$$

2. Врахування крену машини для підвищення точності визначення поточної висоти. Якщо протягом зниження виникнуть відчутні розгойдування або внаслідок невірного закріплення парашутної системи утворюється постійних крен, наведені вище міркування призведуть до виникнення статистичної похибки у визначенні поточної висоти (в бік збільшення значень).

Оптимальним шляхом визначення кута крену, під яким проводилося кожне конкретне вимірювання, є застосування магнітного, механічного, електронного чи гіроскопічного, датчику, наприклад (рис. 2).

Inclinometer

DPG-Series Inclinometer

6160A-2 Analog Tilt Sensor

Рисунок 2 – Сучасні серійні датчики крену

Inclinometer NS-25/DQL2-IXA (вимірює кути нахилу від –25° до 25° відносно двох осей із точністю біля 0.02°);

DPG-Series Inclinometer (вимірює кути нахилу від –30° до 30° відносно двох осей із точністю до 0,2° і частотою вимірювань до 30 Гц);

6160A-2 Analog Tilt Sensor (MEMS-сенсор із діапазоном вимірюваних кутів –15° до 15° та точністю біля 0,01°).

Наведені моделі датчиків і їх аналоги, мають достатньо високу точність стосовно задачі, що розглядається, при цьому їх ціна не перевищує декількох десятків доларів.

За умови відомого значення кута крену β (вимірюється відносно вертикалі) поточна висота розташування машини визначатиметься на базі відстані до перешкоди l_i, отриманій при вимірюванні під кутом $\varphi_{\min}$, найближчим до вертикалі (рис. 3). Більш точно:

$$h = l(\varphi_{\min})\cos\varphi_{\min};\tag{5}$$

$$\varphi_{\min} = \min(|\varphi_i + \beta|). \quad (6)$$

Для підвищення точності оцінки висоти можна скористатися й статистичним усередненням (4), увівши у відповідні формули поправку на крен:

$$h_i = l_i \cos(\varphi_i + \beta); \quad (7)$$

$$h_i^* \approx h_i - (n-i)\upsilon\tau; \quad (8)$$

$$h(t) = \text{average}\,(h_i^*). \quad (9)$$

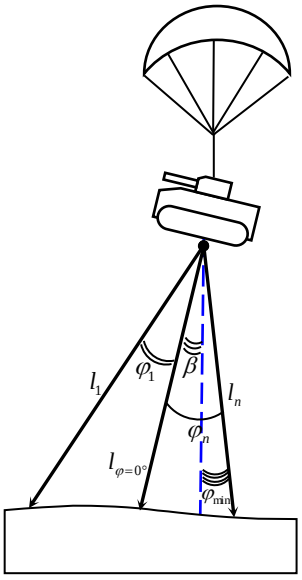


Рисунок 3 – Врахування крену машини

3. Визначення кута ухилу поверхні землі в місці приземлення. Окрім визначення поточних значень висоти та швидкості зниження машини, використання скануючого радару дозволяє оцінити значення кута ухилу поверхні Землі у місці приземлення (в площині сканування радару).

У найпростішому наближенні (вважаючи поверхню біля точки приземлення плоскою) для цього достатньо знати значення однієї відстані до поверхні Землі, виміряної під деяким ненульовим кутом φ_i відносно вертикалі (рис. 4) а також значення поточної висоти h, перераховане відносно даного вимірювання. Застосовуючи теорему косинусів, отримуємо

$$s_i^2 = h^2 + l_i^2 - 2hl_i \cos\varphi_i. \quad (10)$$

Відповідно, кут ухилу α поверхні дорівнює

$$\alpha_i = \arccos(b_i / s) = \arccos(l_i \sin\varphi_i / s). \quad (11)$$

Визначені таким чином кути ухилу поверхні Землі α_i для кожного з вимірювань відстані до землі протягом поточного сканування можна усереднити (враховуючи напрями ухилу, які можна визначити, наприклад, за допомогою теореми синусів, обчислюючи кут між h та s_i), підвищуючи таким чином точність визначення кута α

$$\alpha = \text{average}\,(\alpha_i). \quad (12)$$

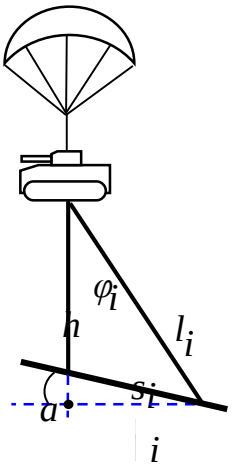


Рисунок 4 – Визначення кута ухилу поверхні Землі

Кут ухилу поверхні землі у напрямку, перпендикулярному до площини сканування радару, можна визначити, встановивши ще один радар із площиною сканування, розташованій перпендикулярно до площини сканування першого. Застосування двох радарів є ще більш доцільним, оскільки воно забезпечує дублювання системи визначення висоти і швидкості зниження, тобто істотно підвищує надійність парашутно-реактивної системи.

Якщо визначений кут ухилу поверхні землі в місці приземлення виявляється завеликим, збільшити ймовірність вдалого приземлення можна шляхом корекції траєкторії зниження об'єкту із урахуванням отриманої інформації. Одним із найпростіших шляхів корегування траєкторії зниження є обладнання об'єкту невеликими аеродинамічними елементами (рулями) та електромеханічними приводами, що забезпечують їх необхідну орієнтацію на основі результатів визначення рельєфу поверхні радіолокатором. Керування цим процесом може виконуватися обчислювальним пристроєм системи ПРС автоматично або, за необхідності, віддаленим оператором за умови надійного захисту каналу передачі даних.

Як один із варіантів, авторами пропонується застосування додаткових реактивних двигунів ПРС, які конструктивно розташовані на протилежних сторонах об'єкту десантування таким чином, щоб утворити крутний момент обертання об'єкта у просторі від 0° до 90° в горизонтальній площині за рахунок кінетичної енергії руху від спрацювання реактивних двигунів. Момент спрацювання піропатронів розраховується на підставі визначення оптимальної відстані об'єкта до поверхні землі, а потреба у спрацюванні піропатронів для розвороту об'єкту (коригування його положення у просторі) залежить від визначеного значення кута ухилу поверхні землі та його порівняння із допустимими критичними значеннями кута нахилу об'єкта (що відповідає втраті об'єктом десантування стійкості під час приземлення).

Висновки. Таким чином в ході проведених досліджень було розглянуто:

- роботу скануючої радарної решітки в процесі зниження об'єкту;
- метод підвищення точності визначення висоти шляхом статистичного усереднення багатьох вимірювань;
- вплив затримки між вимірюваннями протягом сканування на точність визначення поточної, висоти;
- шляхи врахування крену машини (в тому числі і внаслідок її розгойдування) для підвищення точності визначення поточної висоти;
- метод визначення кута ухилу поверхні землі в місці приземлення.

Отримані результати дозволяють підвищити точність роботи радіовисотоміру та істотно зменшити імовірність неправильного визначення поточної висоти знаходження об'єкту внаслідок його розгойдування чи статичного крену, а також складного рельєфу місцевості. Практичний результат полягає в підвищені загальної ефективності системи та забезпеченні заданих умов приземлення об'єкту десантування, а можливість врахування крену об'єкту десантування та оцінки рельєфу місцевості є додатковою (до описаних у роботах [6,7,8]) перевагою

електронного висотоміру на базі скануючої радарної решітки над механічним пристроєм (щупом).

ЛІТЕРАТУРА:

1. Куянов О.Ю., Александров В.Є. Основні напрямки розвитку засобів десантування озброєння та військової техніки . *Наука і техніка Повітряних Сил Збройних Сил України.* 2010. №1(1). С. 49-54.

2. Дмитрієв В.А. Методи випробувань парашутних систем для повітряного десантування. *Наука і техніка Повітряних Сил Збройних Сил України.* 2013. №1(3). С. 41-43.

3. Патент № 111571.Автономна дистанційно керована транспортна модульна платформ супроводження повітряного десанту. Опубл.від 10.05.2016

4. Соломатин И.И., Арабин М.В. Учебное пособие по тяжёлой воздушно-десантной технике. Под общ. ред. Гуськова Н.Н. Часть пятая. *Управление командующего ВДВ. – М. Воениздат*, 1980. С. 152.

5. Соломатин И.И., Арабин М.В. Учебное пособие по тяжёлой воздушнодесантной технике. Под общ. ред. Лисова И.И. Часть третья. *Управление командующего ВДВ. – М. Воениздат*, 1967. С. 168.

6. Адамов Ю.І., Дяченко О.Ф., Завальнюк В.В. Визначення впливу похибок на швидкість приземлення об'єкту, який десантуеться за допомогою парашутно-реактивної системи при розрахунках реальної маси. *Збірник наукових праць.* ВА Одеса. 2016. №1(5) С. 83-90.

7. Адамов Ю.І., Дяченко О.Ф., Завальнюк В.В. Вплив похибок визначення стану атмосфери на швидкість приземлення об'єкту який десантується. *Науково-виробничий журнал ВКФ. Фаворит ЛТД.* Харків.2017. 4(66) – 72. С. 36-41.

8. Адамов Ю.І., Дяченко О.Ф., Завальнюк В.В., Кондратенко О.І., Бондаренко А.В. Шляхи вдосконалення парашутно-реактивної системи. *Теоретичний і науково – практичний журнал*. 2017. №3.2017. С. 25-27.

9. Васильева В.Н. Оптические и лазерные технологии. Учебное издание. Серия Интеграция. Выпуск 1.Санкт – Петербург. 2001. 251с.

Харченко В. П., Барабанов Ю. М., Міхалочкін М. А. Системи зв'язку та навігації. *Навчальний посібник*. Видавництво Національного авіаційного університету. 2009. С. 207.

11. R. Ulrich and A.J. D'Onofrio. An Active Optical Ground Sensor for a Parachute Retrorocket Airdrop System. USAF, February 1973. (USAF Report HDL-TM-73-2 (AD 911 216L).)

12. L. Stanislas, T. Peynot. Characterisation of the Delphi Electronically Scanning Radar for Robotics Applications. Australasian Conference on Robotics and Automation 2015. 2-4 Dec. 2015, Canberra, Australia.

REFERENCES:

1. Kuianov O.Yu., Aleksandrov V.Ye. Osnovni napriamky rozvytku zasobiv desantuvannia ozbroiennia ta viiskovoi tekhniky . Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy. 2010. №1(1). S. 49-54.

2. Dmytriiev V.A. Metody vyprobuvan parashutnykh system dlia povitrianoho desantuvannia. Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy. 2013#1(3).S. 41-43.

3. Patent #111571.Avtonomna dystantsiino kerovana transportna modulna platform suprovodzhennia povitrianoho desantu. Opubl.vid 10.05.2016

4. Solomatyn Y.Y., Arabyn M.V. Uchebnoe posobye po tiazhëloi vozdushno-desantnoi tekhnyke. Pod obshch. red. Huskova N.N. Chast piataia. Upravlenye komanduiushcheho VDV. – M. Voenyzdat, 1980. S. 152.

5. Solomatyn Y.Y., Arabyn M.V. Uchebnoe posobye po tiazhëloi vozdushnodesantnoi tekhnyke. Pod obshch. red. Lysova Y.Y. Chast tretia. Upravlenye komanduiushcheho VDV. – M. Voenyzdat, 1967. S. 168.

6. Adamov Yu.I., Diachenko O.F., Zavalniuk V.V. Vyznachennia vplyvu pokhybok na shvydkist pryzemlennia obektu, yakyi desantuetsia za dopomohoiu parashutno - reaktyvnoi systemy pry rozrakhunkakh realnoi masy. Zbirnyk naukovykh prats. VA Odesa. 2016. №1(5) S. 83-90.

7. Adamov Yu.I., Diachenko O.F., Zavalniuk V.V. Vplyv pokhybok vyznachennia stanu atmosfery na shvydkist pryzemlennia obiektu yakyi desantuietsia. Naukovo-vyrobnychyi zhurnal VKF. Favoryt LTD. Kharkiv, #4(66) – 72. S. 36-41.

8. Adamov Yu.I., Diachenko O.F., Zavalniuk V.V., Kondratenko O.I., Bondarenko A.V. Shliakhy vdoskonalennia parashutno - reaktyvnoi systemy. Teoretychnyi i naukovo – praktychnyi zhurnal. 2017. №3.2017. S. 25-27.

9. Vasyleva V.N. Optycheskye y lazernыe tekhnolohyy. Uchebnoe yzdanye. Seryia Yntehratsyia. #1.Sankt – Peterburh. 2001.-251s.

10. Kharchenko V. P., Barabanov Yu. M., Mikhalochkin M. A. Systemy zviazku ta navihatsii. Navchalnyi posibnyk. Vydavnytstvo Natsionalnoho aviatsiinoho universytetu. 2009. S. 207.

11. R. Ulrich and A.J. D'Onofrio. An Active Optical Ground Sensor for a Parachute Retrorocket Airdrop System. USAF, February 1973. (USAF Report HDL-TM-73-2 (AD 911 216L).)

12. L. Stanislas, T. Peynot. Characterisation of the Delphi Electronically Scanning Radar for Robotics Applications. Australasian Conference on Robotics and Automation 2015. 2-4 Dec 2015, Canberra, Australia.

Адамов Ю.И., д.т.н, доц. Боряк К.Ф., к.ф-м.н., доц. Завальнюк В.В.

УСОВЕРШЕНСТВОВАНИЯ ПАРАШЮТНО-РЕАКТИВНОЙ СИСТЕМЫ ДЛЯ ДЕСАНТИРОВАНИЯ ВОЕННОЙ ТЕХНИКИ ИЛИ КРУПНОГАБАРИТНЫХ ОБЪЕКТОВ

В работе рассматриваются вопросы модернизации парашютно-реактивной системы (ПРС) с применением современных радиовысотомеров с целью повышения доли мягких приземлений и обеспечения возможности корректировки положения объекта десантирования в горизонтальной плоскости в зависимости от значения угла наклона поверхности пересеченной местности в расчетной точке приземления. Критические значения угла наклона объекта десантирования к горизонту предлагается устанавливать на основании указанных производителем тактико-технических данных объекта десантирования или расчетным путем. Первоочередной задачей является повышение точности работы высотомера, от которого зависит момент срабатывания пиропатронов реактивных двигателей ПРС. Авторы предлагают замену механического высотомера устаревшей конструкции современным электронным радиовысотомером на базе сканирующей радарной решетки. В статье рассмотрены особенности работы сканирующей радарной решетки, методы повышения точности определения высоты (расстояния до поверхности земли), необходимость и пути учета крена машины в процессе снижения и возможность определения угла уклона поверхности земли к горизонту в месте приземления. Полученные результаты позволяют повысить точность работы радиовысотомера и существенно уменьшить вероятность ошибочного определения высоты вследствие раскачивания или статического крена объекта, а также выявлять и учитывать особенности рельефа местности.

Кроме определения текущих значений высоты и скорости снижения машины, использование сканирующего радара позволяет оценить значение угла наклона поверхности Земли в месте приземления (в плоскости сканирования радара). Если определенный угол уклона поверхности земли в месте приземления оказывается слишком большим, увеличить вероятность удачного приземления можно путем коррекции траектории снижения объекта с учетом полученной информации. Одним из самых простых путей корректировки траектории снижения есть оборудование объекта небольшими аэродинамическими элементами (рулями) и электромеханическими приводами, обеспечивающими их необходимую ориентацию на основе результатов определения рельефа поверхности радиолокатором. Как один из вариантов, авторами предлагается применение дополнительных реактивных двигателей ПРС, которые конструктивно расположены на противоположных сторонах объекта десантирования таким образом, чтобы образовать крутящий момент вращения объекта в пространстве от 0 ° до 90 ° в горизонтальной плоскости за счет кинетической энергии движения от срабатывания реактивных двигателей. Момент срабатывания пиропатронов рассчитывается на основании определения оптимального расстояния объекта до поверхности земли, а потребность в срабатывании пиропатронов для разворота объекта (корректировка его положения в пространстве) зависит от определенного значения угла уклона поверхности земли и его сравнение с допустимыми критическими значениями угла наклона объекта (что соответствует потере объектом десантирования устойчивости во время приземления).

Ключевые слова: парашютно-реактивная система, сканирующая радарная решетка, угол уклона поверхности земли, терминальная скорость снижения, скорость снижения.

Adamov Yu., prof. Boriak K., PhD. Zavalniuk V.

ON IMPROVEMENT OF PARACHUTE-RETROROCKET AIRDROP SYSTEM

The paper is devoted to the study of the prospects for improving the parachute-retrorocket airdrop system (PRS) in order to increase its reliability and enable the ability to adjust the orientation of a load in the horizontal plane depending on the slope of the earth's surface at the landing site. The primary task is to improve the accuracy of the altimeter, which determines the triggering moment of the PRS jet engines. The replacement of a mechanical altimeter of an outdated design with a modern electronic radio altimeter based on phased array radar is proposed, which allows to improve the accuracy of determining the absolute altitude (distance to the ground) and to take into account a roll of the load during the descent. The ways of determining the slope of earth's surface at the estimated landing site are also discussed. The results obtained make it possible to increase the accuracy of radio altimeter operation and significantly reduce the probability of an error in determining the absolute altitude due to rocking or static roll of the object.

In addition to determining the current values of the height and speed of the descent of the vehicle, the use of a scanning radar makes it possible to estimate the inclination angle of the Earth's surface at the landing site (in the radar scanning plane). If a certain angle of inclination of the earth surface at the landing site turns out to be too large, the probability of a successful landing can be increased by correcting the object's descent path, taking into account the information received. One of the easiest ways to correct a descent trajectory is to equip an object with small aerodynamic elements (rudders) and electromechanical actuators, ensuring their necessary orientation based on the results of determining the surface relief with radar. As one of the options, the authors propose the use of additional jet engines, which are structurally located on opposite sides of the object of landing in such a way as to form a torque of rotation of the object in a space from 0 ° to 90 ° in the horizontal plane due to the kinetic energy of motion from the actuation of jet engines. The triggering moment of the squibs is calculated based on determining the optimal distance of the object to the ground surface, and the need for triggering the squibs to rotate the object (correcting its position in space) depends on a certain value of the slope angle of the earth surface and comparing it with the admissible critical values of the angle, at which the object loses its stability during landing.

Keywords: parachute-retrorocket airdrop system, scanning radar grid, angle of slope of the earth's surface, terminal descent rate, descent rate.

УДК 519.6:534.88+623.746.-51
д.ф.-м.н., проф., чл.-кор. НАНУ **Анісімов А.В.** (КНУ)
с.н.с. **Волков О.Є.** (МННЦ ІТ та С)
к.ф.-м.н. **Ліндер Я.М.** (КНУ)
к.ф.-м.н. **Тарануха В.Ю.** (КНУ)
Волошенюк Д.О. (МННЦ ІТ та С)

МЕТОД АКУСТИЧНОЇ ПЕЛЕНГАЦІЇ ДИНАМІЧНИХ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ

У статті описано спосіб побудови, структуру та роботу методу визначення напрямку на джерело звуку. Метод спирається на прости математичний апараті, що дозволяє реалізувати його на обладнанні мінімальної потужності, наприклад на мікропроцесорах Arduino. Розглянуто ключові елементи методу та умови використання, що впливають на результат. До них належать параметри звучання цілей, перш за все основні частоти та тривалість звучання необхідні для надійного визначення напрямку на джерело звуку. Крім того, в методі передбачено оцінювання параметрів середовища з метою визначення швидкості звуку в залежності від погодних умов, оскільки результати роботи методу сильно залежать від цього параметру. Вироблено рекомендації до БпЛА на який треба буде встановлювати обладнання, та описано спосіб використання для отримання найкращих результатів з визначення напрямків на джерела звуку. Продемонстровано доведення формули, що дозволяє визначати напрямок на джерело звуку з урахуванням того, що платформа де буде змонтовано програмно-апаратний комплекс має рухатися і виконувати визначення напрямку на джерело звуку під час руху або, в найгіршому випадку, коротких зависань на місці. Для цієї формули виконано оцінку помилки кута в градусах, в залежності від того, під яким кутом до напрямку руху і, відповідно, бази між мікрофонами, надходить звукова хвиля.

Виконано прототипування програмних засобів, для подальшої реалізації у вигляді повноцінного програмно-апаратного комплексу для установки на БпЛА. Також представлено графічний інтерфейс програмної реалізації методу. Проведено моделювання роботи системи за умови різних обставин. В ході експериментів визначено порогове значення для ключового критерію, що спирається на співвідношення сигнал/шум, оскільки в надто зашумленому середовищі метод працювати не буде. Проведені експерименти показують високу дієвість методу з урахуванням особливостей реальних джерел звуку.

Ключові слова: програмне забезпечення, безпілотний літальний апарат, визначення напрямку на джерело сигналу, обробка звуку.

Постановка проблеми у загальному вигляді. Розробка систем спостереження, особливо на основі безпілотних літальних апаратів (БпЛА), останнім часом набула високої значимості. Особливо це стосується необхідності вести спостереження в областях, де немає можливості застосувати звичайні засоби спостереження, як то, наприклад, в зоні ведення бойових дій. При цьому, важливим є створення мультисенсорних систем з додаванням засобів звукової розвідки. Саме звукова розвідка потенційно може стати основним засобом фіксації використання та віднаходження розташування замаскованих озброєнь ворожих угрупувань. Крім того, треба враховувати, що на відміну від візуальних зображень, які, зазвичай, не вдається знімати у всіх ракурсах та для розпізнавання яких необхідно передавати їх оператору, звук можна фіксувати з будь-якого напрямку та визначати напрямок на джерело в автоматичному режимі засобами, що розміщені безпосередньо на борту БпЛА. Значна відстань поширення звуку, особливо гарматних пострілів [1,2], також сприяє розробці засобів визначення напрямку на джерело звуку – акустичної пеленгації.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми. Існує ряд робіт, які присвячені цій темі, але вони переважно концентруються на задачах розпізнавання шумів (перш за все пострілів) та визначення координат за умов значних обчислювальних ресурсів та спеціалізованих засобів, як то направлені мікрофони [3,4,5,6,7,8]. На відміну від них, дана робота зосереджується на задачі визначення напрямку на джерело звуку довільної природи за умови обмежених ресурсів ьа мінімальної ваги апаратних компонент.

Також, важливими елементами дослідження є те, що:

очікувані джерела звуку є, переважно, великими, складними за структурою (колона техніки, що пересувається, артилерійська батарея, тощо), та породжують звук протягом значного часу;

платформа з сенсорами є мобільною і може як переорієнтувати себе у просторі відносно джерела звуку, так і переміщуватись ближче до джерела звуку, а також мати різні параметри польоту, в першу чергу різну висоту, швидкість та кутове положення;

платформа може бути реалізована різним чином, як у вигляді квадрокоптеру, так і у вигляді БпЛА літакового типу;

відсутні фізичні ефекти типові для систем, що розробляться для приміщень, перш за все в наслідок відсутності стін, які спричиняють додаткові відбиття звуку [9];

можна вважати що фронт звукової хвилі має просту форму, і немає потреби враховувати складніші варіанти [10].

Виклад основного матеріалу дослідження.

Першим етапом методу визначення напрямку до джерела звуку є фільтрація отриманого сигналу для визначення робочого діапазону частот. Для цього сигнал перетворюється на спектр частот за допомогою швидкого перетворення Фур'є [11]. Для кожної частоти f_n маємо .– комплексну амплітуду синусоїдального сигналу, що разом складають вихідний сигнал. Оскільки амплітуди комплексні, то по ним можна обчислити одночасно і амплітуду, і фазу.

Після чого обчислюються реальні частоти, що відповідають значенням X_n за формулою:

$$f_n = \begin{cases} F_s \dfrac{n}{N}, 0 \le n \le \left[\dfrac{N-1}{2}\right]; \\ F_s \dfrac{N-n}{N}, \left[\dfrac{N-1}{2}\right] \le n \le N-1, \end{cases}$$

де N – кількість компонент розкладу;

F_s – частота сигналу, що одержується з мікрофонів;

Задається два порогових значення, Tr_a та Tr_b – частоти, що задають діапазон, за межами якого сигнал розглядатись не буде. Відповідно, значення X_n, які відповідають частотам $f_n \le Tr_a$, та $f_n \ge Tr_b$ обнуляються. Відфільтрований сигнал отримується після здійснення оберненого перетворення Фур'є.

Другий етап методу – безпосереднє відшукання напрямку до джерела звуку. Для знаходження кута визначається максимальний допустимий зсув сигналів Δ за формулою:

$$\Delta = \left[\frac{F_s D}{V}\right],$$

де *V*– швидкість звуку, у метрах на секунду;

D– відстань між мікрофонами у метрах;

Після чого обчислюється функція крос-кореляції двох сигналів $XCORR_{lr}(k)$ для всіх $k \in [-\Delta, \Delta]$. Функція крос-кореляції вимірює подібність між першим часовим рядом і зсунутими версіями іншого часового ряду як функцію від зсуву. Використання саме цього критерію зумовлено бажанням створити систему, яку можна буде реалізувати з використанням мінімальних апаратних засобів та готових компонент, як то мікропроцесори Arduino.

Відхилення сигналів лівого та правого мікрофонів мають вигляд:

$$\sigma_l = \sqrt{\frac{1}{N}\sum_{t=0}^{N-1}(l_t - \bar{l})^2};$$
$$\sigma_r = \sqrt{\frac{1}{N}\sum_{t=0}^{N-1}(r_t - \bar{r})^2}.$$

Функція коваріації двох сигналів визначається за формулою:

$$COV_{lr}(k) = \begin{cases} \frac{1}{N}\sum_{t=0}^{N-k-1}(l_t - \bar{l})\ (r_{t+k} - \bar{r}), k \geq 0, \\ \frac{1}{N}\sum_{t=0}^{N-k-1}(r_t - \bar{r})\ (l_{t+k} - \bar{l}), k < 0. \end{cases}$$

Тоді шукана крос-кореляція двох сигналів записується за допомогою формули:

$$XCORR_{lr}(k) = \frac{COV_{lr}(k)}{\sigma_l \sigma_r}, k = 0, \pm 1, \pm 2, \ldots N$$

де N – кількість значень сигналу (довжина часового ряду), а також кількість компонент розкладу;

k– індекс частоти; частота, k-го сигналу дорівнює $\frac{k}{T}$, де T- період часу, протягом якого бралися вхідні дані;

l_t – значення сигналу лівого мікрофону під час відлікут;

r_t – значення сигналу правого мікрофону під час відлікут;

$\bar{l} = \frac{1}{N}\sum_{i=0}^{N-1} l_t$ – середнє значення сигналу лівого мікрофону;

$\bar{r} = \frac{1}{N}\sum_{i=0}^{N-1} r_t$ – середнє значення сигналу правого мікрофону.

Після обчислення функції крос-кореляції метод розраховує максимум функції крос-кореляції та зсув S, на якому цей максимум досягається. Якщо $XCORR_{lr}(S)$ менше порогового значення 0.2, робота алгоритму завершується (співвідношення сигнал/шум надто низьке для якісного визначення напрямку до звуку). Значення S>0 означає, що сигнал від джерела звуку першим дійшов до мікрофона на лівому кінці бази, у той час як від'ємне значення сигналізує про те, що правий мікрофон отримав звук першим.

Остаточно кут до джерела звуку визначається за формулою:

$$\alpha(S) = -\arcsin(\frac{S}{\Delta})\frac{180}{\pi}. \quad (1)$$

Кут обчислюється перпендикулярно до бази, і у випадку двох мікрофонів це відповідає повздовжній осі БпЛА. Нульовий кут означає, що джерело шуму прямо по курсу. Додатній кут у 90º означає, що джерело знаходиться у напрямку правого кінця бази, а кут -90º означає, що джерело знаходиться у напрямку лівого кінця бази.

У розрахунках швидкість звуку є одним з ключових параметрів алгоритму, і її точне визначення є важливим для точного обчислення положення джерела звуку. Для обчислення швидкості звуку найчастіше використовується формула:

$$c = \sqrt{\frac{p}{\rho}k} \quad (2)$$

де p– тиск повітря у Паскалях;

ρ – густина повітря;

k– тут показник адіабати, що для повітря дорівнює 1.4.

Проте дана формула розрахунку не враховує вологість повітря та його температуру. У роботі [12] пропонується більш точний метод вимірювання швидкості звуку $c(t, p, x_\omega, x_c)$ з урахуванням вологості та температури:

$$c(t, p, x_\omega, x_c) = 331.5024 + 0.603055t - 0.000528t^2 +$$
$$+ (51.471935 + 0.1495874t - 0.000782t^2)x_\omega +$$
$$+ (-1.82 \cdot 10^{-7} + 3.73 \cdot 10^{-8}t - 2.93 \cdot 10^{-10}t^2)p +$$
$$+ (-85.20931 - 0.228525t + 5.91 \cdot 10^{-5}t^2)x_c -$$
$$- 2.835149x_\omega^2 - 2.15 \cdot 10^{-13}p^2 + 29.179762x_c^2 + 0.000486x_\omega p x_c,$$

де t – температура у градусах Цельсія;

p– тиск повітря;

x_ω – мольна частка водяної пари;

x_c – мольна часткаCO_2, яку приймають на рівні $x_c = 0.0004$.

Мольну ж частку водяної пари обчислюють за формулою:

$$x_\omega = hf\frac{p_{sv}}{p},$$

Де *h* – відносна вологість;

f– фактор підсилення;

p_{sv} – тиск насичених парів водяної пари в повітрі.

Останні дві величини обчислюються за формулами:

$$f = 1.00062 + 3.14 \cdot 10^{-8}p + 5.6 \cdot 10^{-7}t^2,$$
$$p_{sv} = \exp(1.28 \cdot 10^{-5}T^2 - 1.95 \cdot 10^{-2}T + 34.05 - 6.354 \cdot 10^3 / T),$$

де *T* – температура у градусах Кельвіна.

Такий розрахунок дає точне значення швидкості звуку у діапазоні 0ºС – 30ºС. За замовчуванням припускається, що швидкість звуку складає 340 м/с, якщо немає можливості її уточнити. Також ця швидкість використовується у подальших оцінках, які можуть змінитися для іншої швидкості звуку.

Перед програмною реалізацією алгоритму необхідно також визначити його ключові параметри: вікно фільтрування сигналів Tr_a, Tr_b та відстань між мікрофонами (база *B*). У якості джерела звуку для налаштування алгоритму було використано шум квадрокоптеру. Після аналізу спектральних характеристик звуку виявлено, що домінуючі частоти є 1 кГц, 4.5 кГц та близько 8 кГц (рис. 1).

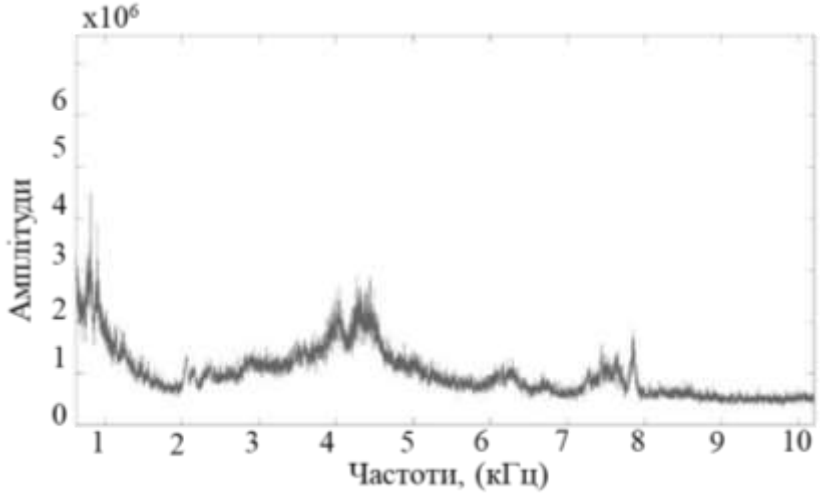


Рис. 1. Аналіз спектральних характеристик

Частоти шуму (у даному випадку вітру) знаходяться у діапазоні нижче 1 кГц. Хоча високі частоти понад 8 кГц мають значно менший вклад у результуючий сигнал (досить мала амплітуда), але шум там теж нижчий. Таким чином, було вирішено взяти вікно фільтрування сигналів $Tr_a = 0.9$ кГц, $Tr_b = +\infty$ кГц.

Довжина звукової хвилі складає:

$$\lambda(\omega) = \frac{c}{\omega},$$

де ω – частота хвилі у Герцах;

c– швидкість звуку.

Таким чином, довжина хвилі на частоті 1кГц складає 0.34 м. для вибраної швидкості звуку. У випадку ідеального гармонічного сигналу алгоритм дозволяє знайти зсув сигналів з точністю до пів довжини хвилі. Отже, незважаючи на те, що збільшення відстані між мікрофонами збільшує точність визначення кута, збільшується також і ймовірність помилки. Тому у якості бази було обрано величину B = 0.3 м.

При такому значенні бази, швидкості звуку і частоті дискретизації сигналу 44100 Гц значення максимального зсуву $\Delta = 40$ відліків, і всього можливо [-40, 40] = 81 варіантів знаходження кута. Проте точність знаходження кута падає зі збільшенням відхилення джерела кута від перпендикуляра до бази. Так, якщо взяти різницю між значеннями за формулою (1), то $|\alpha(1) - \alpha(0)| = 1.43^o$, тоді як, $|\alpha(40) - \alpha(39)| = 12.65^o$.

Метод визначення напрямку на джерело звуку розрахований на політ невеликого та нешвидкого БпЛА на невеликій висоті, тобто для квадрокоптеру. У такому випадку кут до джерела звуку перш за все визначається азимутом і лише незначно – кутом нахилу у сферичній системі координат. Враховуючи, що джерело звуку даватиме сигнал протягом тривалого часу, та те, що БпЛА зможе виконувати виміри по мірі наближення до джерела звуку, то похибкою визначення напрямку на джерело звуку через неврахований кут нахилу можна знехтувати. Крім того, БпЛА має можливість скоригувати своє кутове положення в просторі після того, як буде зафіксовано початок звуку, а отже це дозволить знехтувати помилками, що зумовлені кутами нахилу БпЛА (тангажу і крену).

Використання трьох мікрофонів, розташованих у вершинах рівностороннього трикутника дозволяє утворити три бази та гарантувати, що звукова хвиля, яка набігає на БпЛА, завжди матиме принаймні одну базу, кут до якої складає 30^o або менше. Найближчому значенню $\alpha(S)$ до кута 30^o відповідає 20 відлік. Таким чином, у найгіршому випадку помилка при оцінюванні кута складе не більше, ніж $|\alpha(21) - \alpha(20)| = 1.67^o$, що значно менше за помилки, що породжуються іншими факторами, які виникають під час польоту БпЛА. Передбачається, що

після того, як оператор БпЛА вирішить, що джерело звуку треба дослідити, БпЛА буде зорієнтовано на джерело, що дозволить використовувати дані лише з двох мікрофонів для подальшого супроводження джерела.

Якщо БпЛА не може зависнути для точного визначення звуку (наприклад, БпЛА літакового типу), то це означає, що вибрана база вимірювання рухається відносно звукової хвилі, що набігає і, відповідно, помилка методу може складати значну величину. Проте, навіть така помилка дозволяє віднайти сектор, у якому знаходиться джерело звуку та зорієнтувати БпЛА так, щоб напрямок набігання звуку був якомога ближче до перпендикуляру до вибраної бази вимірювання.

При цьому формула (2) набуває такого вигляду:

$$c = \sqrt{\frac{p}{\rho}k} + V_D. \qquad (3)$$

Для застосування методу на БпЛА літакового типу з притаманними такому типу БпЛА параметрами і характеристиками польоту, розроблений метод набув подальшого розвитку. Він передбачає, що є необхідність відстежувати джерело звуку без того, щоб зорієнтувати напрямок руху БпЛА на джерело звуку та за умови, що БпЛА не може або не повинен зависати на місці (рис.2).

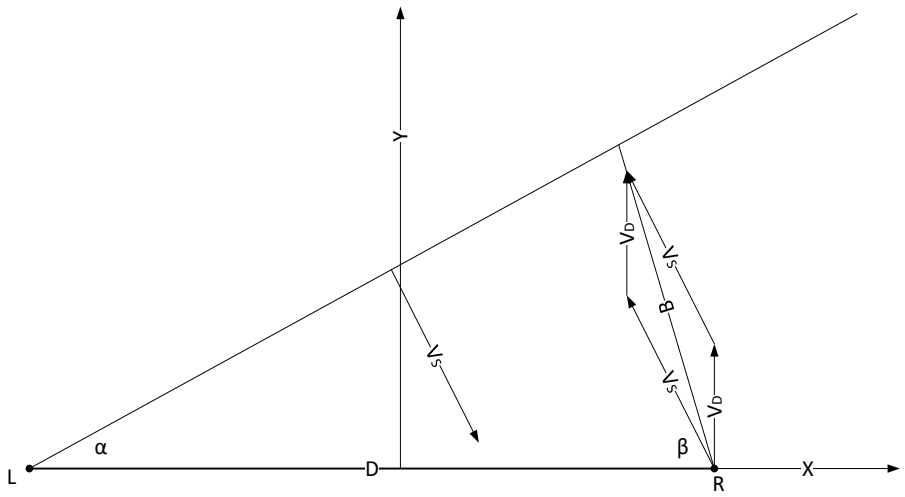


Рис. 2. Набігання звукової хвилі на БпЛА, що рухається

На рис. 2 прийнято такі позначення:*L, R*– лівий та правий мікрофони, які розташовані на крилі БпЛА; *D* – відстань між мікрофонами (база); β – кут між базою (*D*) та відрізком *B*, який у свою чергу паралельний вектору, що є сумою векторів V_S та V_D; V_S - вектор, що задає напрямок руху звукової хвилі; α – кут набігання хвилі; V_D – швидкість БпЛА, що направлена вздовж повздовжньої осі *Y* БпЛА. Тоді:

$$V_S^x = V \sin\alpha,$$
$$V_S^y = V \cos\alpha,$$

де *V* – швидкість звуку (скаляр).

Розглянемо рух БпЛА відносно фронту хвилі. Тоді вектор наближення точки *R* до хвилі запишеться як:

$$V_{tot} = (V \sin\alpha, V \cos\alpha + V_D).$$

За теоремою синусів:

$$B = \frac{D\sin\alpha}{\sin(\alpha+\beta)}.$$

Час до зустрічі точки *R* з фронтом хвилі:

$$\Delta = \frac{B}{\sqrt{(V\sin\alpha)^2 + (V\cos\alpha + V_D)^2}} = \frac{B}{\sqrt{V^2 + 2V\cos\alpha V_D + V_D^2}} =$$

$$= \frac{D\sin\alpha}{(\sin\alpha\cos\beta + \cos\alpha\sin\beta)\sqrt{V^2 + 2V\cos\alpha V_D + V_D^2}}.$$

Кут β можна записати у вигляді:

$$\beta = \arcsin(\frac{V\cos\alpha + V_D}{\sqrt{V^2 + 2V\cos\alpha V_D + V_D^2}}),$$

або:

$$\beta = \arccos(\frac{V\sin\alpha}{\sqrt{V^2 + 2V\cos\alpha V_D + V_D^2}}).$$

Тоді час до зустрічі точки *R* з фронтом хвилі приймає вигляд:

$$\Delta = \frac{D\sin\alpha}{(\sin\alpha(V\sin\alpha) + \cos\alpha(V\cos\alpha + V_D))} = \frac{D\sin\alpha}{V + V_D\cos\alpha}.$$

Виразимо кут α через Δ:

$$(V + V_D\cos\alpha)\Delta = D\sin\alpha,$$
$$D\sin\alpha - \Delta V_D\cos\alpha = \Delta V.$$

Цю формулу можна переписати у вигляді:

$$\sqrt{D^2 + \Delta^2 V_D^2}\sin(\alpha - \phi),$$

де:

$$\phi = \arcsin(\frac{\Delta V_D}{\sqrt{D^2 + \Delta^2 V_D^2}}) = \arccos(\frac{D}{\sqrt{D^2 + \Delta^2 V_D^2}}) = \arctan 2(\Delta V_D, D),$$

де:

$$\arctan 2(y,x) = \begin{cases} \arctan(\frac{y}{x}), x > 0; \\ \arctan(\frac{y}{x}) + \pi, x < 0, y \geq 0; \\ \arctan(\frac{y}{x}) + \pi, x < 0, y < 0; \\ \frac{\pi}{2}, x = 0, y \geq 0; \\ -\frac{\pi}{2}, x = 0, y < 0. \end{cases}$$

Остаточно формула шуканого кута запишеться у вигляді:

$$\alpha = \arcsin\left(\frac{\Delta V}{\sqrt{D^2 + \Delta^2 V_D^2}}\right) + \arctan 2(\Delta V_D, D).$$

Для точнішого визначення напряму на джерело звуку є бажаним, але не обов'язковим, перехід БпЛА в режим планерування на короткий час (0,5-2 с), що даватиме невисоку швидкістю руху БпЛА відносно джерела звуку, і це дозволить зменшити помилку, що зумовлена рухом відносно джерела звуку.

На базі запропонованого методу було створено програмне забезпечення, що реалізує динамічний пошук джерела звуку за даними двох мікрофонів. Вигляд інтерфейсу показано на рис. 3.

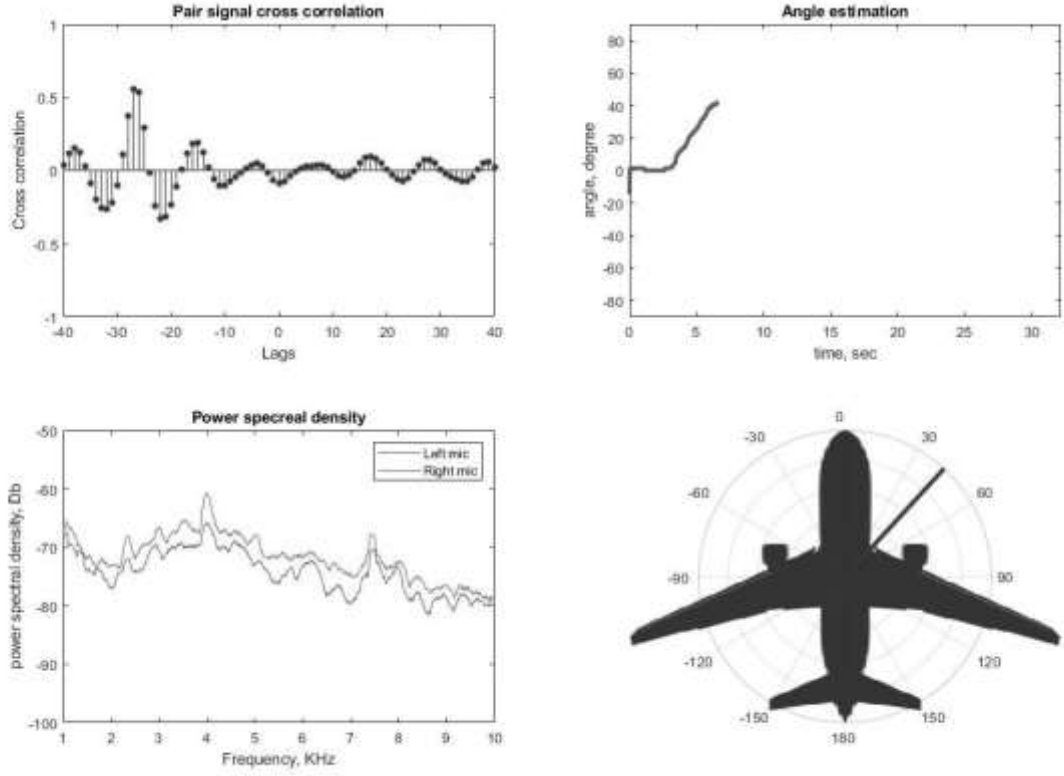


Рис. 3. Графічний інтерфейс розробленого методу

У лівому верхньому вікні (рис. 3) виводиться обчислена крос-кореляція пари сигналів. На рис. 3, максимум досягається при зсуві сигналу з правого мікрофона на -25 відліків. Таким чином, звук на правий мікрофон приходить раніше.

У лівому нижньому вікні виводиться обчислена спектральна густина сигналів. На ілюстрації обидва сигнали мають виражений пік на частоті 4 кГц.

У правому верхньому вікні проводиться візуалізація обчисленого кута у декартовій системі координат зі збереженням попередніх значень кутів.

У правому нижньому вікні відбувається анімація зміни кута у полярній системі координат.

Під час динамічного визначення кута використовувалось плаваюче вікно довжиною 0.5 с (22050 відліків), яке зсувалось на 1000 відліків кожну наступну ітерацію.

Висновки

В роботі було запропоновано та отримано метод, що дозоляє з достатньою надійністю визначати напрямок до джерела складного звуку. На відміну від імпульсного звуку (вибухи, постріли), саме такий звук важче локалізувати, з огляду на відсутність чітко вираженого звукового фронту, який сприймається мікрофонами. Також, значна кількість частот джерела звуку робить використання більш простих методів, як то фазового, неефективними.

Варіант тестової системи з трьома мікрофонами дозволяє визначити напрямок на джерело звуку з точністю до 1.67°.

У подальшому планується підвищити точність локалізації джерела звуку шляхом збільшення кількості мікрофонів та покращення якості записуючого обладнання. Крім того, подальша робота буде спрямована на покращення методу таким чином, щоб за його допомогою можна було визначати напрямки на декілька менших джерел, що звучать одночасно, оскільки зараз метод не передбачає виділення окремих малих джерел у межах одного великого джерела звуку.

ЛІТЕРАТУРА:

1. Луценко В.И., Луценко И.В, Соболяк А.В. Дальность действия систем акустической разведки. *Прикладная радиоэлектроника*. 2015. Т. 14, № 2. С.125-136.
2. Tactical Infrasound /Ch. Stubbs et al. JASON The MITRE Corporation. 2005. 72p.
3. Izabela L. Freire and Jose A. Apolinario Jr. Gunshot detection in noisy environments in *Proceeding of the 7th International Telecommunications Symposium*. Manaus, Brazil. 2010 pp. 1-4 .
4. Talal U. Momin and Abubakr M. Improving efficiency and reliability of gunshot detection systems. in *Proc. of 38th International Conference on Acoustics, Speech and Signal Processing*. 26-31 May 2013. Vancouver, Canada. pp. 513-517
5. Nandwana, M.K., Ziaei A., Hansen J.H.L. *Robust* Unsupervised Detection of Human Screams in Noisy Acoustic Environments. in *Proc. of International Conference on Acoustics, Speech, and Signal Processing*. April 19-24 2015 South Brisbane, Queensland, Australia. pp.161–165.
6. Almaadeed N. Et al. Automatic Detectionand Classification of Audio Events for Road Surveillance Applications. *Sensors* 2018.Vol 18(6). [Електронний ресурс] Режим доступу: https://www.mdpi.com/1424-8220/18/6/1858/pdf (дата звернення: 2.08.2019).
7. Izabela L. Freire and Jose A. Apolinario Jr. GCC-based DoA Estimation of Overlapping Muzzleblast and Shockwave Components of Gunshot Signals in *Proc. of Second IEEE Latin American Symposium on Circuits and Systems,* 23-25 Feb. 2011 Bogotá, Colombia, 2011. pp. 1-4.
8. Valenzise G., Gerosa, L., Tagliasacchi M., Antonacci F. and Sarti A. Scream and gunshot detection and localization for audio-surveillance systems. in *Proc. of IEEE Conference on Advanced Video and Signal Based Surveillance*, 2007, pp. 21–26
9. Абракітов В.Е. Багаторазові відбиття звуку в акустичних розрахунках: [Електронний ресурс] Режим доступу: http://eprints.kname.edu.ua/6053/1/%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F2.pdf (дата звернення: 2.08.2019).
10. Селіванов С. Є., Абракітов В. Е., Нікітченко О. Ю., Чупріна Я. І. Визначення інтенсивності випромінювання на відстані від джерела залежно від форми хвильового фронту. *Коммунальное хозяйство городов*, 2007 №79, С. 356-363.
11. Р. Лайонс, Цифровая обработка сигналов:монография. Москва.: Бином, 2006. 656 с.
12. Cramer, O. The variation of the specific heat ratio and the speed of sound in air with temperature, pressure, humidity and CO2 concentration. *J.Acoust.Soc.Am* 1993 №93. pp. 2510-2516.

REFERNCES:

1. Lutsenko, V.E., Lutsenko, E.V., Sobolyak, A.V. (2015) “Dalnost deystviya sitem akustich-eskoy razvedky” [Acoustic reconnaissance systems range]. *Applied radioelectronics* T. 14, № 2. pp.125-136.
2. Ch. Stubbs et al. (2005) *Tactical Infrasound* JASON, The MITRE Corporation. 72p.
3. Izabela L. Freire and Jose A. Apolinario Jr. (2010) “Gunshot detection in noisy environments” in *Proc. of the 7th International Telecommunications Symposium*. Manaus, Brazil. 2010 pp. 1-4 .
4. Talal, U. Momin and M. Abubakr (2013) “Improving efficiency and reliability of gunshot detection systems” in *Proc. of 38th International Conference on Acoustics, Speech and Signal Processing*. 26-31 May 2013. Vancouver, Canada. pp. 513-517

5. Nandwana, M. K., Ziaei, A., Hansen, J. H. L.(2015) “Robust Unsupervised Detection of Human Screams in Noisy Acoustic Environments.” In *Proc. of International Conference on Acoustics, Speech, and Signal Processing*. April 19-24 2015 South Brisbane, Queensland, Australia. pp.161–165.

6. Almaadeed N. Et al. (2018) “Automatic Detectionand Classification of Audio Events for Road Surveillance Applications”. *Sensors*.Vol 18(6) . www.mdpi.com/1424-8220/18/6/1858/pdf (accessed 2 August 2019)

7. Izabela L. Freire and Jose A. Apolinario Jr. (2011) “GCC-based DoA Estimation of Overlapping Muzzleblast and Shockwave Components of Gunshot Signals” in *Proc. of Second IEEE Latin American Symposium on Circuits and Systems,* 23-25 Feb. 2011 Bogotá, Colombia, 2011. pp. 1-4.

8. Valenzise, G., Gerosa, L., Tagliasacchi, M., Antonacci, F. and Sarti., A (2007). “Scream and gunshot detection and localization for audio-surveillance systems.” In *Proc. of IEEE Conference on Advanced Video and Signal Based Surveillance*, pp. 21–26

9. Abrakitov, V.Ye. (2007) *Bagatorazovi vidbuttya zvuku v akustuchnuh rozrahunkah* [Multiple sound reflections in acustic calculations]: eprints.kname.edu.ua/6053/1/%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F2.pdf (accessed 2 August 2019)

10. Selivanov, S.Ye., Abrakitov, V.Ye., Nikitchenko, O.Yu, Chuprina, Ya.E. (2007) “Vusnachennya intensyvnosty vyprominyuvannya na vidstani vid dzherela zalezhno vid formy hvulyovogo frontu”. [Evaluation of intencity of emission at distance from source in dependance on wave front form] *City utilities*, №79, pp. 356-363.

11. Layons, R. (2006) *Cifrovaya obrabotka signalov* [Digiatal signal processing].Binom Moscow, 656 p.

12. Cramer, O. (1993) “The variation of the specific heat ratio and the speed of sound in air with temperature, pressure, humidity and CO2 concentration”, *J.Acoust.Soc.Am* №93. pp. 2510-2516.

д.ф-м.н., проф., чл.-кор. НАНУ Анисимов А.В., с.н.с. Волков А.Е.,
к.ф.-м.н. Линдер Я.Н., к.ф.-м.н. Тарануха В.Ю., Волошенюк. Д.А.

МЕТОД АКУСТИЧЕСКОЙ ПЕЛЕНГАЦИИ ДИНАМИЧЕСКИХ ОБЪЕКТОВ С ПОМОЩЬЮ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

В статье описывается способ создания, структура и работа метода определения направления на источник звука. Метод опирается на простой математический аппарат, что позволяет реализовать его на оборудовании минимальной мощности, например на микропроцессорах Arduino. Рассмотрены ключевые элементы метода и условия использования, влияющие на результат. К ним относятся параметры звучания целей, прежде всего основные частоты и продолжительность звучания, необходимые для надежного определения направления на источник звука. Кроме того, в методе предусмотрено оценивания параметров среды с целью определения скорости звука в зависимости от погодных условий, поскольку результаты работы метода сильно зависят от этого параметра. Выработаны рекомендации к БпЛА на который надо будет устанавливать оборудование, и описывается использование для получения лучших результатов по определению направлений на источники звука. Продемонстрировано доказательства формулы, позволяющей определять направление на источник звука с учетом того, что платформа, где будет смонтировано программно-аппратный комплекс должна двигаться и выполнять определения направления на источник звука во время движения или, в худшем случае, коротких зависаний на месте. Для этой формулы выполнена оценка ошибки угла в градусах, в зависимости от того, под каким углом к направлению движения и, соответственно, базе между микрофонами, приходит звуковая волна.

Выполнено прототипирование программных средств, для дальнейшей реализации в виде полноценного программно-аппаратного комплекса для установки на БПЛА. Также представлены графический интерфейс программной реализации метода. Проведено моделирование работы системы при различных обстоятельствах. В ходе экспериментов определено пороговое значение для

ключевого критерия, которое опирается на соотношение сигнал/шум, поскольку в слишком зашумленной среде метод работать не будет. Проведенные эксперименты показывают высокую действенность метода с учетом особенностей реальных источников звука.

Ключевые слова: программное обеспечение, беспилотный летательный аппарат, определения направления на источник сигнала, обработка звука.

Prof. Anisimov A.V., Volkov O.E., Ph.D. Linder Ya.M., Ph.D. Taranukha V. Yu., Volosheniuk D. O.

THE METHOD OF ACOUSTIC DIRECTION FINDING OF DYNAMIC OBJECTS USING AN UNMANNED AERIAL VEHICLE

The article describes the method of creation, structure and operation of the method for determining the direction to the sound source. The method relies on a simple mathematical apparatus, which allows it to be implemented on equipment of minimal power, for example, on Arduino microprocessors. The key elements of the method and conditions of use affecting the result are considered. These include the sound parameters of targets, primarily the main frequencies and duration of sound necessary to reliably determine the direction to the sound source. In addition, the method provides means for estimating environmental parameters in order to determine the speed of sound depending on weather conditions, since the results of the method are highly dependent on this parameter. Recommendations have been developed for UAVs on which it will be necessary to install equipment, and the use is described to obtain better results in determining directions to sound sources. Demonstrated proof of the formula that allows one to determine the direction to the sound source, given that the platform where the hardware-software complex will be mounted must move and carry out the determination of the direction to the sound source during movement or, in the worst case, short stops for hovering. For this formula the angle error in degrees is estimated depending on the angle at which the sound wave arrives relatively to direction of movement.

Software prototyping was performed for further implementation in the form of a full-fledged software and hardware complex for installation on UAVs. The graphical interface of the software implementation of the method is also presented. The simulation of the system under various circumstances was performed. During the experiments, a threshold value was determined for the key criterion, it is based on the signal-to-noise ratio since the method will not work in a too noisy environment. The experiments performed shown the high efficiency of the method taking into account the features of real sound sources.

Keywords: Software, Unmanned aerial vehicle, Definition of the Direction to the Source of the Signal, Sound Processing.

УДК 351.746.1

д.т.н., проф. **Боровик О.В.** (НАДПСУ)
Купельський В.В. (НАДПСУ)

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ ВИБОРУ ОПТИМАЛЬНОГО МАРШРУТУ РУХУ КОЛОНИ ТЕХНІКИ ПРИКОРДОННОЇ КОМЕНДАТУРИ ШВИДКОГО РЕАГУВАННЯ

Прикордонна комендатура швидкого реагування є структурним підрозділом прикордонного загону, призначена для захисту та посилення охорони визначеної ділянки Державного кордону й повинна оперативно здійснювати передислокацію власних сил і засобів. Успіх виконання поставлених перед підрозділом завдань значною мірою залежить від своєчасності прибуття у точку призначення. Оперативне перевезення значної кількості озброєння, особового складу та різнорідних вантажів на сухопутній ділянці здійснюється шляхом використання техніки. На підготовчому етапі організації перевезень розв'язується задача формування оптимального складу колони техніки. Паралельно з її вирішенням потребує розв'язування задача вибору маршрутів руху колони техніки.

Існуюча мережа автомобільних доріг забезпечує достатньо велику кількість маршрутів руху між вихідним і кінцевим пунктами. Причому це має місце навіть для незначних відстаней між точками вибуття та призначення. Вказане обумовлює багатоваріантність під час вибору.

Крім того, вибір маршруту руху залежить від багатьох допоміжних умов: навченості водіїв, технічних характеристик та надійності техніки, безпеки руху, дорожніх і природньо-кліматичних умов, відстані та термінів перевезень тощо. Неякісне врахування цих факторів у сукупності може призвести до вибору нераціонального маршруту руху, який не забезпечить своєчасного прибуття підрозділу в пункт призначення, та може призвести до зриву виконання визначених завдань. Тому задача вибору оптимального маршруту руху колони техніки є актуальною. На змістовному рівні задача виглядає як обґрунтування математичної моделі вибору оптимального маршруту руху колони техніки, якщо критерієм оптимальності виступає мінімізація часу руху з вихідної точки в пункт призначення.

Авторами сформовано математичну модель наведеної задачі, запропоновано алгоритм її вирішення для трьох випадків: дискретно-стохастичного, дискретно-детермінованого та неперервно-невизначеного, а також розроблено відповідне програмне забезпечення. Вибір маршрутів здійснюється для трьох варіантів з урахуванням того, що зміна ваг ребер може здійснюватися:

у моменти часу, коли колона знаходиться в певній вершині графа, і оновлення матриці ваг здійснюється саме в ці моменти. Це випадок, коли рішення щодо подальшого маршруту руху формується у точках розгалуження доріг з урахуванням обстановки щодо стану окремих ділянок, що динамічно змінюється і дані щодо якого з'являються періодично;

у моменти часу, коли колона знаходиться в певній вершині графа, і для цих моментів матриці ваг, які матимуть місце при попаданні колони у вершину, наперед відомі. Це випадок, коли рішення щодо маршруту руху може бути сформоване на початку руху з урахуванням відомої обстановки щодо стану доріг, що динамічно змінюватиметься, але дані щодо якого можуть бути враховані завчасно;

довільним чином в залежності від швидкості колони у фіксований момент часу, для якого відомою є функція швидкості колони.

Ключові слова: математична модель, алгоритм, матриця, прикордонна комендатура швидкого реагування, техніка, колона.

Постановка проблеми у загальному вигляді. Успіх виконання поставлених перед прикордонною комендатурою швидкого реагування (ПКШР) завдань значною мірою залежить від своєчасності прибуття підрозділів ПКШР у точку призначення. Оперативне перевезення значної кількості особового складу та різнорідних вантажів ПКШР на сухопутній ділянці здійснюється шляхом використання транспортних засобів. На підготовчому етапі організації перевезень розв'язується задача формування оптимального складу колони техніки [14]. Паралельно з її вирішенням потребує розв'язування задача вибору маршрутів руху колони техніки.

Існуюча мережа автомобільних доріг забезпечує достатньо велику кількість маршрутів руху між вихідним і кінцевим пунктами. Причому це має місце навіть для незначних відстаней між точками вибуття та призначення. Вказане обумовлює багатоваріантність під час вибору.

Крім того, вибір маршруту руху залежить від багатьох допоміжних умов: навченості водіїв, технічних характеристик техніки, економічності, безпеки руху, дорожніх і природно-кліматичних умов, відстані та термінів перевезень тощо. Неякісне врахування цих факторів у сукупності може призвести до вибору нераціонального маршруту руху, який забезпечить несвоєчасність прибуття підрозділу в пункт призначення, та може призвести до зриву виконання визначених завдань. Тому задача вибору оптимального маршруту руху колони техніки прикордонної комендатури швидкого реагування є актуальною.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми. Питанням вибору маршрутів руху колони транспортних засобів для ефективного переміщення вантажів, а також суміжним задачам приділялась увага у ряді робіт, зокрема в роботах [1-14].

Підхід щодо вибору маршруту, який ґрунтується на edgelabels, наведений у праці [1]. Його застосування дозволяє прискорити пошук найкоротшого шляху в 500 разів у порівнянні зі стандартним алгоритмом Дейкстри над великим графом. У роботі [2] наведено алгоритм для вибору оптимальних маршрутів у мультимодальному режимі мережі громадського транспорту. За результатами цього дослідження підхід щодо маршрутизації транзитних вузлів був адаптований для планування переміщення громадським транспортом. У науковій праці [3] для пошуку найкоротшого шляху застосовано метод ієрархії контракції. У дослідженні [4] на основі застосування алгоритму SHARC наведено можливості з відшукання найкоротших шляхів для довільних засобів переміщення у транспортній мережі континентального масштабу. У науковій праці [5] досліджено проблему планування мультимодальних маршрутів. У роботі [6] наведено модель для оцінки трафіку затримки транспортних засобів з урахуванням довільних навантажень у процесі руху. У дослідженні [7] наведене планування маршрутів для військових наземних транспортних засобів на полі бою. У роботі проведено моделювання невизначеностей, що мають місце на дорожній мережі, за допомогою набору дискретних сценаріїв. Запропоновано метод відшукання найкоротшого шляху для кожного окремого транспортного засобу. Результати розрахунків свідчать про те, що запропонований метод може забезпечити якісне рішення лише для мереж з невеликою кількістю вузлів. У науковій праці [8] розроблено алгоритм розв'язування задачі пошуку найкоротших за часом шляхів у міських маршрутних мережах транспорту загального користування з урахуванням тривалості пересадок методом віток і меж.

У джерелах [9-11] описуються можливості застосування геоінформаційних програмних продуктів ArcGIS для відшукання раціональних маршрутів руху. Маршрутний аналіз ArcGIS дозволяє здійснювати пошук найшвидшого за часом, найкоротшого за відстанню або навіть найбільш живописного маршруту з вихідної до кінцевої точки. До параметрів аналізу маршруту можуть входити час початку руху, час доби, точна дата, день тижня тощо. При виборі маршруту руху враховуються бар'єри – об'єкти, які обмежують, ускладнюють чи змінюють маршрут руху. За результатами обчислення з урахуванням вихідних параметрів та обмежень програмним продуктом формується певний маршрут руху.

У дослідженні [12] сформовано та досліджено варіант моделі планування вантажоперевезень, представлено прикладну програму для знаходження у транспортній мережі оптимального маршруту перевезення вантажів від одного постачальника до кількох споживачів.

У праці [13] задача вибору найкоротшого маршруту розв'язувалась за критерієм максимізації рівня готовності транспортних засобів та мінімізації марочного складу й кількості транспортних засобів у колоні. Обмеження моделі стосувалися забезпечення нормативно встановлених часу на перевезення та коефіцієнта готовності техніки, перевезення колоною особового складу заданої кількості та вантажу, заданої маси і об'єму, витрат різних видів пального, що не перевищують встановлених значень, не зниження запасу ходу по моторесурсу кожним транспортним засобом зі складу колони.

В авторській роботі [14] було здійснено формалізацію постановки задачі розмічення графа з неоднорідними ребрами та обґрунтовано метод її вирішення у двох різних випадках: у випадку, коли можливим є розбиття довільного ребра досліджуваного графа точками, що відповідають моментам часу, коли швидкість колони дискретно змінює своє значення, а також у

випадку, коли розбиття ребра точками, що відповідають моментам часу, коли швидкість колони дискретно змінює своє значення, є проблемним, але при цьому швидкість колони у кожен фіксований момент часу є відомою.

З наведеного випливає, що у проаналізованих працях залишилися поза увагою наступні аспекти, які потребують урахування при виборі оптимального маршруту руху колони техніки:

- перевезення військових підрозділів вимагає дотримання вимог режимності, тому застосування загальнодоступного програмного забезпечення з великою ймовірністю може створювати передумови для прогнозування вибору маршруту руху ймовірним противником або порушником;

- перевезення військових підрозділів потребує прогнозування зміни дорожньої обстановки з урахуванням комплексної статистичної інформації щодо проблемних ситуацій (аналіз ДТП на маршруті руху за минулий рік, інформації щодо проведення ремонтних робіт, врахування прогнозу погоди та ін.) на усьому маршруті руху з метою своєчасного виходу у визначений район;

- військові перевезення передбачають переміщення значної кількості особового складу та специфічних вантажів як на невеликі, так і на значні відстані;

- у зв'язку зі специфікою військових завдань під час перевезення військових підрозділів сумісно застосовується не тільки різномарочна, але і достатньо різнотипна техніка;

- виконання перевезень передбачає широке застосування будь-яких доріг, в тому числі ґрунтових, а іноді і бездоріжжя.

Отже, підходи та методи, які проаналізовані у наведених вище роботах, не можуть бути застосовні для розв'язування досліджуваної задачі безпосередньо. Разом з тим, запропонований у праці [14] метод є базовим і таким, що дозволяє впритул наблизитися до вирішення задачі вибору оптимального маршруту руху колони техніки прикордонної комендатури швидкого реагування. Особливість досліджуваної задачі полягає в нефіксованості ваг ребер, які описують окремі ділянки мережі доріг, у процесі руху колони.

Мета статті. Таким чином, метою даної роботи є формалізація задачі вибору оптимального маршруту руху колони техніки прикордонної комендатури швидкого реагування з урахуванням особливостей, пов'язаних із забезпеченням достовірності початкових даних, та алгоритмізація методу її розв'язування.

Виклад основного матеріалу дослідження. Для досягнення сформульованої мети вбачається за доцільне насамперед здійснити постановку задачі, що адекватна реальному процесу, формалізувати її, а далі запропонувати алгоритми її вирішення.

Постановка задачі, що адекватна реальному процесу. Нехай задано колону техніки, яка повинна вибути з пункту відправлення (точки А) та прибути в пункт призначення (точку В). Умови формування складу колони аналогічні визначеним у роботі [2]. Нехай також задано мережу доріг, що зв'язують точки А та В. Математична модель мережі доріг являє собою розмічений граф, вага ребер якого являє час руху колони вздовж них.

Необхідно знайти оптимальний маршрут руху, якщо критерієм оптимальності виступає мінімізація часу руху з точки А в точку В.

При цьому слід врахувати, що в процесі руху колони час руху вздовж окремих ребер може бути змінним. Така умова визначається впливом на час руху вздовж окремого ребра різних умов, наприклад, кліматичних (дощ, ожеледь, туман тощо), техногенних (завали дорожнього полотна, його пошкодження внаслідок підтоплення ділянки місцевості тощо), зміни періоду доби (день, ніч) тощо.

Також слід врахувати, що зміна ваг ребер може здійснюватись:

1. У моменти часу, коли колона знаходиться в певній вершині графа, і оновлення матриці ваг здійснюється саме в ці моменти. Це випадок, коли рішення щодо подальшого маршруту руху формується у точках розгалуження доріг з урахуванням обстановки щодо стану окремих ділянок, що динамічно змінюється і дані щодо якого з'являються періодично. Цей випадок у подальшому називатимемо дискретно-стохастичним;

2. У моменти часу, коли колона знаходиться в певній вершині графа, і для цих моментів матриці ваг, які матимуть місце при попаданні колони у вершину, наперед відомі. Це випадок,

коли рішення щодо маршруту руху може бути сформоване на початку руху з урахуванням відомої обстановки щодо стану доріг, що динамічно змінюватиметься, але дані щодо якого можуть бути враховані завчасно. Цей випадок у подальшому називатимемо дискретно-детермінованим;

3. Довільним чином в залежності від швидкості колони у фіксований момент часу, для якого відомою є функція швидкості колони. Цей випадок у подальшому називатимемо неперервно-невизначеним.

Формалізація задачі, що адекватна реальному процесу. Зважаючи на те, що задача, яка адекватна реальному процесу, може мати місце у трьох постановках, необхідним є формування математичної моделі для кожної з них.

Випадок 1 - дискретно-стохастичний.

Нехай задано розмічений граф, кількість вершин якого рівна n.

І нехай v_i - деяка вершина графа.

Матриця ваг графа має вигляд $W^{(i)} = \left(w_{ij}^{(i)}\right)_{n\times n}$. Тут $w_{ij}^{(i)}$ - вага ребра $\{v_i, v_j\}$ у момент перебування у вершині v_i.

Необхідно знайти найкоротший шлях від заданої початкової вершини a до заданої вершини z, якщо величини $w_{ij}^{(i)}$ наперед невідомі і стають відомими лише в момент перебування у вершині v_i.

Випадок 2 - дискретно-детермінований.

Нехай задано розмічений граф, кількість вершин якого рівна n.

І нехай v_i - деяка вершина графа.

Матриця ваг графа має вигляд $W^{(i)} = \left(w_{ij}^{(i)}\right)_{n\times n}$. Тут $w_{ij}^{(i)}$ - вага ребра $\{v_i, v_j\}$ у момент перебування у вершині v_i.

Необхідно знайти найкоротший шлях від заданої початкової вершини a до заданої вершини z, якщо величини $w_{ij}^{(i)}$ наперед відомі.

Випадок 3 – неперервно-невизначений.

Нехай задано розмічений граф, кількість вершин якого рівна n.

І нехай v_i - деяка вершина графа.

Матриця швидкостей руху вздовж ребер графа має вигляд $V = \left(v_{ij}\right)_{n\times n}$. Тут v_{ij} - швидкість руху вздовж ребра $\{v_i, v_j\}$ у фіксований момент t, тобто $v_{ij} = f_{ij}(t)$. Функції $f_{ij}(t)$ можуть бути різними в залежності від того, вздовж якого ребра здійснюється рух.

Необхідно знайти найкоротший шлях від заданої початкової вершини a до заданої вершини z, якщо величина шляху визначається часом руху вздовж нього.

Алгоритмізація методу розв'язування досліджуваної задачі. З урахуванням фізичного змісту задачі можна стверджувати, що матриця ваг $W^{(i)} = \left(w_{ij}^{(i)}\right)_{n\times n}$ може бути різною в залежності від часу, коли колона перебуває у вершині v_i. Тому природно, що матрицю ваг слід диференціювати в залежності від часу перебування колони у певній вершині.

Цей процес реалізуємо так. Початковий момент часу вважатимемо нульовим етапом. Момент часу, коли колона перемістилася вздовж одного ребра і знаходиться у деякій вершині графа, вважатимемо першим етапом. Момент часу, коли колона перемістилася вздовж двох ребер і знаходиться у деякій вершині графа, вважатимемо другим етапом і т.д.

З урахуванням цього, матрицю ваг у подальшому позначатимемо $W^{(i.k)} = \left(w_{ij}^{(i.k)}\right)_{n\times n}$. Тут k визначає етап реалізації руху колони.

Отже, у розгорнутому вигляді початкові умови задачі можна представити у вигляді даних табл. 1.

Таблиця 1

Початкові умови досліджуваної задачі для випадків 1, 2 щодо матриці ваг графа в залежності

від вершини, в якій перебуває колона, та етапу її руху

Вершина, в якій знаходиться колона	Етапи руху колони			
	0	1	2	…
v_1	$W^{(1.0)} = \left(w_{ij}^{(1.0)}\right)_{n\times n}$	$W^{(1.1)} = \left(w_{ij}^{(1.1)}\right)_{n\times n}$	$W^{(1.2)} = \left(w_{ij}^{(1.2)}\right)_{n\times n}$	…
v_2	$W^{(2.0)} = \left(w_{ij}^{(2.0)}\right)_{n\times n}$	$W^{(2.1)} = \left(w_{ij}^{(2.1)}\right)_{n\times n}$	$W^{(2.2)} = \left(w_{ij}^{(2.2)}\right)_{n\times n}$	…
…	…	…	…	…
v_n	$W^{(n.0)} = \left(w_{ij}^{(n.0)}\right)_{n\times n}$	$W^{(n.1)} = \left(w_{ij}^{(n.1)}\right)_{n\times n}$	$W^{(n.2)} = \left(w_{ij}^{(n.2)}\right)_{n\times n}$	…

При цьому слід зазначити, що для формування матриць ваг табл. 1 може бути застосований підхід, який описаний у роботі [9] і вибір складових якого залежить від початкових умов задачі, що проаналізовані у цій праці, та фізичного змісту досліджуваної задачі.

Випадок 1 - дискретно-стохастичний.

Наведена математична модель досліджуваної задачі у випадку 1 дозволяє зробити висновок, що для її розв'язування можна скористатися методом Дейкстри [10] пошуку найкоротшої відстані між заданими вершинами графа a і z. При цьому матриця ваг графа матиме вигляд однієї з матриць, що наведений у першому стовпці початкових умов табл. 1. Якою саме буде матриця ваг, залежатиме від того, з якої вершини розпочинається рух. Позначимо цю вершину як $v^{(0)}$. Тобто, для досліджуваної задачі $a = v^{(0)}$.

Таким чином, застосування алгоритму Дейкстри дозволяє встановити оптимальний маршрут руху для етапу 0. Однак цей маршрут не буде оптимальним в цілому для задачі, оскільки матриця ваг у момент перебування колони у наступній вершині після вершини $v^{(0)}$ зміниться.

З урахуванням цього, для етапу 1 відомою буде кінцева вершина графа, яка залишається незмінною (вершина z), а також початкова вершина, яка визначатиметься з оптимального маршруту, отриманого для етапу 0, як його друга вершина. Позначимо її через $v^{(1)}$.

З урахуванням того, що в момент перебування колони у першій вершині етапу 1, тобто в вершині $v^{(1)}$, матриця ваг зміниться і матиме вигляд однієї з матриць, що наведений у другому стовпці початкових умов табл. 1 (якою саме буде матриця ваг, залежатиме від того, з якої вершини розпочинається рух), задачу визначення оптимального маршруту можна далі розглядати як задачу пошуку найкоротшої відстані між вершинами $v^{(1)}$ і z.

Для її розв'язування знову можна скористатися алгоритмом Дейкстри, як і на попередньому етапі. Застосування цього алгоритму дозволяє встановити оптимальний маршрут руху для етапу 1.

Таким чином, для етапу 2 відомою буде не лише кінцева вершина графа, яка залишається незмінною (вершина z), а й початкова вершина, яка визначатиметься з оптимального маршруту, отриманого для етапу 1, як його друга вершина. Позначимо її через $v^{(2)}$.

З урахуванням того, що в момент перебування колони у першій вершині етапу 2, тобто в вершині $v^{(2)}$, матриця ваг зміниться і матиме вигляд однієї з матриць, що наведений у третьому стовпці початкових умов табл. 1 (якою саме буде матриця ваг, залежатиме від того, з якої вершини розпочинається рух), задачу визначення оптимального маршруту можна далі розглядати як задачу пошуку найкоротшої відстані між вершинами $v^{(2)}$ і z.

З наведеного можна зробити висновок, що метод розв'язування задачі для випадку 1 полягає в ітераційному застосуванні алгоритму Дейкстри із змінною першою вершиною та різними матрицями ваг на окремих етапах його застосування.

Якщо ввести позначення, що $z = v^{(g)}$, то ознакою зупинки запропонованого алгоритму є суміжність вершин $v^{(g-1)}$ і $v^{(g)}$ в оптимальному маршруті $(g-1)$-го етапу.

Наглядне представлення наведеного алгоритму можна оцінити з табл. 2.

Таблиця 2

Етапи реалізації ітераційного застосування алгоритму Дейкстри із змінною першою вершиною та різними матрицями ваг на окремих етапах його застосування

Етап	Вершини оптимального маршруту руху в залежності від етапу						
	a						z
0	$v^{(0)}$	$v^{(1)}$					
1		$v^{(1)}$	$v^{(2)}$				
2			$v^{(2)}$	$v^{(3)}$			
…					…		
$g-1$						$v^{(g-1)}$	$v^{(g)}$

Таким чином, оптимальний маршрут руху колони у випадку 1 являтиме собою наступну послідовність вершин: $a = v^{(0)}$, $v^{(1)}$, $v^{(2)}$,…, $v^{(g-1)}$, $v^{(g)} = z$.

А отже, оптимальна тривалість руху колони у досліджуваному випадку становить $T = \sum_{i=0}^{g-1} w^{(v^{(i)}.i)}_{v^{(i)}v^{(i+1)}}$, де $w^{(v^{(i)}.i)}_{v^{(i)}v^{(i+1)}}$ - вага ребра між вершинами $v^{(i)}$ і $v^{(i+1)}$ матриці ваг $W^{(v^{(i)}.i)}$.

Випадок 2 - дискретно-детермінований.

Наведена математична модель досліджуваної задачі у випадку 2 дозволяє зробити висновок, що для її розв'язування можна скористатися методом, алгоритм якого полягає у побудові на початковому етапі усіх можливих шляхів між заданими вершинами графа a і z, встановленні сукупностей матриць ваг для кожного знайденого шляху, що відповідають кожній вершині на відповідному етапі, подальшому визначенні тривалості реалізації кожного шляху та вибору найкоротшого з шляхів на основі порівняння знайдених тривалостей.

Ідею методу можна оцінити з прикладу, що стосується випадку, коли $a = v_1$ і який наведений у табл. 3-5.

Таблиця 3

Приклад можливих альтернативних шляхів між вершинами графа a і z

Номер альтернативного шляху між вершинами графа a і z	Етапи руху колони							
	0	1	2	3	4	5	6	…
1	v_1	v_2	v_4	z				…
2	v_1	v_3	v_4	v_6	z			…
3	v_1	v_2	v_3	v_5	v_7	v_6	z	…
…	…	…	…	…	…	…	…	…

Слід звернути увагу на те, що при побудові альтернативних варіантів можливих шляхів між вершинами графа не варто розглядати ті з них, які містять повтори вершин, у яких колона вже побувала.

Таблиця 4

Послідовності матриць ваг, що відповідають кожній вершині на відповідному етапі для кожного знайденого шляху і стосуються прикладу, що наведений у табл. 3

Номер альтернативного шляху між вершинами графа a і z	Етапи руху колони							
	0	1	2	3	4	5	6	…
1	$W^{(1.0)}$	$W^{(2.1)}$	$W^{(4.2)}$	z				…
2	$W^{(1.0)}$	$W^{(3.1)}$	$W^{(4.2)}$	$W^{(6.3)}$	z			…
3	$W^{(1.0)}$	$W^{(2.1)}$	$W^{(3.2)}$	$W^{(5.3)}$	$W^{(7.4)}$	$W^{(6.5)}$	z	…
…	…	…	…	…	…	…	…	…

Нехай $T^{(i)}$ - це тривалість реалізації i-го альтернативного шляху між вершинами графа

a і z.

Тоді тривалість реалізації кожного шляху для прикладу, що наведений у табл. 3, можна оцінити з табл. 5.

Таблиця 5

Тривалість реалізації кожного шляху для прикладу, що наведений у табл. 3

Номер альтернативного шляху між вершинами графа a і z	Тривалість реалізації альтернативного шляху між вершинами графа a і z	Складові (доданки) тривалості реалізації альтернативного шляху між вершинами графа a і z, що пов'язані з етапами руху колони							
		0	1	2	3	4	5	6	…
1	$T^{(1)}$	$w_{1.2}^{(1.0)}$	$w_{2.4}^{(2.1)}$	$w_{4.z}^{(4.2)}$					…
2	$T^{(2)}$	$w_{1.3}^{(1.0)}$	$w_{3.4}^{(3.1)}$	$w_{4.6}^{(4.2)}$	$w_{6.z}^{(6.3)}$				…
3	$T^{(3)}$	$w_{1.2}^{(1.0)}$	$w_{2.3}^{(2.1)}$	$w_{3.5}^{(3.2)}$	$w_{5.7}^{(5.3)}$	$w_{7.6}^{(7.4)}$	$w_{6.z}^{(6.5)}$		…
…		…	…	…	…	…	…	…	…

З табл. 5 випливає, що

$$T^{(1)} = w_{1.2}^{(1.0)} + w_{2.4}^{(2.1)} + w_{4.z}^{(4.2)},$$

$$T^{(2)} = w_{1.3}^{(1.0)} + w_{3.4}^{(3.1)} + w_{4.6}^{(4.2)} + w_{6.z}^{(6.3)},$$

$$T^{(3)} = w_{1.2}^{(1.0)} + w_{2.3}^{(2.1)} + w_{3.5}^{(3.2)} + w_{5.7}^{(5.3)} + w_{7.6}^{(7.4)} + w_{6.z}^{(6.5)},$$

……

А отже, мінімальний час руху колони між заданими вершинами графа a і z рівна

$$T = \min\left\{T^{(1)};\ T^{(2)};\ T^{(3)};\ \ldots\right\}.$$

Тоді, якщо $T = T^{(i)}$, то i-й маршрут є оптимальним.

Випадок 3 – неперервно-невизначений.

Наведена математична модель досліджуваної задачі у випадку 3 дозволяє зробити висновок, що для її розв'язування можна скористатися методами, запропонованими для випадків 1 або 2 з урахуванням підходу до розмічення графа, що наведений у роботі [9].

Застосування одного з методів, що запропоновані для випадків 1 або 2, залежить від того, відомими чи невідомими є моменти перебування колони у вершинах графа.

У разі, якщо завчасно відомі можливі моменти перебування колони у кожній вершині графа, то застосовуючи метод, що описаний у роботі [9], можна завчасно встановити матриці ваг графа, сформувавши табл. 1 до початку руху колони. А отже, в цьому випадку для відшукання оптимального шляху руху колони можна скористатися методом, що запропонований у даній роботі для випадку 2.

Якщо ж можливі моменти перебування колони у кожній вершині графа завчасно невідомі, то застосування методу розмічення графа, що описаний у роботі [9], можливе на етапі перебування колони у певній вершині. А отже, в цьому випадку для відшукання оптимального

шляху руху колони можна скористатися методом, що запропонований у даній роботі для випадку 1.

Таким чином, метод розв'язування досліджуваної задачі у випадку 3 полягає в комплексуванні алгоритмів розмічення графа та безпосередньо визначення оптимального шляху в залежності від часу формування матриці ваг графа.

Висновки. Отже, у результаті проведеного дослідження: здійснено постановку задачі вибору оптимального маршруту руху колони техніки прикордонної комендатури швидкого реагування з урахуванням особливостей, пов'язаних із попереднім встановленням і забезпеченням достовірності початкових даних; побудовано математичні моделі досліджуваної задачі для трьох випадків (дискретно-стохастичного, дискретно-детермінованого та неперервно-невизначеного), які залежать від особливостей реалізації руху колони; запропоновано алгоритми вибору оптимального маршруту руху колони техніки прикордонної комендатури швидкого реагування для кожного з можливих випадків, що проаналізовані в роботі.

Напрямами подальших досліджень авторам вбачається автоматизація запропонованих алгоритмів та їх апробація на типових прикладах.

ЛІТЕРАТУРА:

1. Fast point-to-point shortest path computations with arc-flags / M.Hilger, E. Kohler, R. H. Mohring, H. Schilling // The Shortest Path Problem / M.Hilger, E. Kohler, R. H. Mohring, H. Schilling. – Rhode Island: American Society, 2009. – (DIMACS). – (Discrete Mathematics and Theoretical Computer Science; vol. 74). – pp. 41–72.
2. Antsfeld L. Finding Multi-criteria Optimal Paths in Multi-modal Public Transportation Networks using the Transit Algorithm / L. Antsfeld, T. Walsh // Artificial Intelligence and Logistics AILog 2012 Workshop Proceedings. – 2012. – №1. – pp. 7–11.
3. Contraction Hierarchies: Faster and Simpler Hierarchical Routing in Road Networks / [R. Geisberger, P. Sanders, D. Schultes та ін.] // Experimental Algorithms / – Berlin: Springer-Verlag Berlin Heidelberg, 2008. – (Springer-Verlag Berlin Heidelberg). – (Theoretical informatics and general questions; vol. 5038). – pp. 319–333.
4. Delling D. Time-dependent SHARC-routing / Daniel Delling // Algorithmica / – Cham: Springer International Publishing AG, 2011. – (Springer-Verlag). – (Special Issue: European Symposium on Algorithms; vol. 60). – pp. 60–94.
5. Route Planning in Transportation Networks / [H. Bast, D. Delling, A. Goldberg та ін.] // Algorithm Engineering / [H. Bast, D. Delling, A. Goldberg та ін.]. – Cham: Springer International Publishing AG, 2016. – (Springer Nature). – (Theoretical informatics and general questions; vol. 9220). – pp. 19–80.
6. Resilience and efficiency in transportation networks / [A. A. Ganin, M. Kitsak, D. Marchese та ін.]. // Science Advances. – 2017. – №3. – pp. 1–8.
7. Route Planning for Military Ground Vehicles in Road Networks under Uncertain Battlefield Environment / [T. Zhao, J. Huang, J. Shi та ін.]. // Journal of Advanced Transportation Received. – 2018. – №1. – pp. 1–10.
8. Кузькін О. Ф. Пошук шляхів у маршрутних мережах міст методом відгалужень і меж / О. Ф. Кузькін. // Комунальне господарство міст. – 2012. – №103. – С. 378–388.
9. Лейс Т. Г. ArcGIS. ArcMap. Руководство пользователя / Т. Г. Лейс. – Москва: МГУ, 2005. – 558 с.
10. Crosier S. ArcGIS 9: Getting started with ArcGIS / Scott Crosier. – Redlands, Calif.: ESRI, 2004. – 256 с. – (ESRI).
11. ArcGIS 9 ArcMap Руководство пользователя [Електронний ресурс] // ESRI. – 2004. – Режим доступу до ресурсу: https://www.rulit.me/books/arcgis-9-arcmap-rukovodstvo-polzovatelya.
12. Матвейчук Т. А. Моделювання та програмна реалізація процесу планування вантажоперевезень у військовій логістиці / Т. А. Матвейчук. // Військово-технічний збірник АСВУ. – 2016. – №14. – С. 18–25.
13. Математична модель задачі формування складу транспортної колони прикордонної комендатури швидкого реагування та її програмно-алгоритмічна реалізація / О. В. Боровик, Л. В. Рачок, Л. В. Боровик, В. В. Купельський. // Збірник наукових праць ВІКНУ. – 2017. – №55. – С. 17–30.
14. Боровик О. В. Розмічення графа мережі доріг при розв'язуванні задачі вибору оптимального маршруту руху колони техніки прикордонної комендатури швидкого реагування / О. В. Боровик, В. В. Купельський. // Збірник наукових праць НАДПСУ. – 2018. – №76. – С. 244–255.

15.Нікольський Ю. В. Дискретна математика / Ю. В. Нікольський, В. В. Пасічник, Ю. М. Щербина. – Київ: Видавнича група BHV, 2007. – 368 с.

REFERENCES:

1. Hilger, M., Kohler, E., Mohring, R. and Schilling, H. (2009), ”Fast point-to-point shortest path computations with arc-flags”, DIMACS, Vol. 74, pp. 41–72.

2. Antsfeld, L. and Walsh T. (2012), ”Finding Multi-criteria Optimal Paths in Multi-modal Public Transportation Networks using the Transit Algorithm”, Artificial Intelligence and Logistics AILog 2012 Workshop Proceedings, No 1. – pp. 7–11.

3. Geisberger, R., Sanders, P., Schultes, D. and Delling, D. (2008), ”Contraction Hierarchies: Faster and Simpler Hierarchical Routing in Road Networks”, Springer-Verlag Berlin Heidelberg, Vol. 5038, pp. 319–333.

4. Delling, D. (2008), ”Time-dependent SHARC-routing”, Springer International Publishing AG, Vol. 60, pp. 60–94.

5. Bast, H., Delling, D., Goldberg, A., Müller-Hannemann, M., Pajor, T., Sanders, P., Wagner, D. and Werneck, R.F. (2016), ”Route Planning in Transportation Networks”, Springer International Publishing AG, Vol. 9220, pp. 19–80.

6. Ganin, A.A., Kitsak, M., Marchese, D., Keisler, J.M., Seager, T. and Linkov, I. (2017), ”Resilience and efficiency in transportation networks”, *Science Advances*, No 3, pp. 1–8.

7. Zhao, T., Huang, J., Shi , J. and Chen, C. (2018), ”Route Planning for Military Ground Vehicles in Road Networks under Uncertain Battlefield Environment”, *Journal of Advanced Transportation Received*, No 1, pp. 1–10.

8. Kuz′kin, O.F. (2012), ”Poshuk shlyakhiv u marshrutnykh merezhakh mist metodom vidhaluzhen′ i mezh” [The search of ways in the route networks of cities by the method of branches and boundaries], *Communal economy of cities*, No 103, pp. 378–388.

9. Leys, T.G. (2005), ”ArcGIS. ArcMap. Rukovodstvo pol'zovatelya”, [ArcGIS. ArcMap. User Manual], MSU, Moskva, 558 p.

10.Crosier, S. (2005), ”ArcGIS 9: Getting started with ArcGIS”, Redlands, Calif., 256 p.

11.”ArcGIS 9 ArcMap Rukovodstvo pol'zovatelya”, [ArcGIS 9 ArcMap User Guide], Access mode to the resource: https://www.rulit.me/books/arcgis-9-arcmap-rukovodstvo-polzovatelya.

12.Matveychuk, T.A. (2016), ”Modelyuvannya ta prohramna realizatsiya protsesu planuvannya vantazhoperevezen′ u viys′koviy lohistytsi” [Modeling and programme of the planning process cargo transportation in military logistics], *Military-technical collection*, No 14, pp. 18–25.

13. Borovik, O.V., Rachok, R.V., Borovik, L.V. and Kupelskiy, V.V. (2017), ”Математична модель задачі формування складу транспортної колони прикордонної комендатури швидкого реагування та її програмно-алгоритмічна реалізація”, [The mathematical model of the problem of formation of the convoy of frontier commandant rapid response and its software-algorithmic implementation], *Military-technical collection*, No 55, pp. 17–30.

14. Borovik, O.V. and Kupelskiy, V.V. (2018), ”Rozmichennya hrafa merezhi dorih pry rozv″yazuvanni zadachi vyboru optymal′noho marshrutu rukhu kolony tekhniky prykordonnoyi komendatury shvydkoho reahuvannya”, [Graph labelling of road network while solving the problem of selecting optimal traffic route for motor convoy of rapid mobility border command post], *Military-technical collection*, No 76, pp. 244–255.

15.Nikol′s′kyy, YU.V., Pasichnyk, V.V. and Shcherbyna, YU.M. (2012), ”Dyskretna matematyka”, [Discrete mathematics], Publishing group BHV, Kyiv, 368 p.

д.т.н., проф. Боровик О.В., Купельський В.В.

АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ВЫБОРА ОПТИМАЛЬНОГО МАРШРУТУ ПЕРЕМЕЩЕНИЯ КОЛОННЫ ТЕХНИКИ ПОГРАНИЧНОЙ КОМЕНДАТУРЫ БЫСТРОГО РЕАГИРОВАНИЯ

Пограничная комендатура быстрого реагирования является структурным подразделением пограничного отряда, предназначена для защиты и усиления охраны определенного участка государственной границы и должна оперативно осуществлять передислокацию своих сил и средств. Успех выполнения поставленных перед подразделением задач во многом зависит от своевременности прибытия в точку назначения. Оперативные перевозки значительного количества воору-

жения, личного состава и разнородных грузов на сухопутном участке осуществляется путем использования техники. На подготовительном этапе организации перевозок решается задача формирования оптимального состава колонны техники.

Существующая сеть автомобильных дорог обеспечивает достаточно большое количество маршрутов движения между исходным и конечным пунктами. Причем это имеет место даже для незначительных расстояний между точками выбытия и назначения. Указаное обусловливает многовариантность при выборе.

Кроме того, выбор маршрута движения зависит от многих вспомогательных условий: обученности водителей, технических характеристик и надежности техники, безопасности движения, дорожных и природно-климатических условий, расстояния и сроков перевозок и тому подобное.

Не качественное учета этих факторов в совокупности может привести к выбору нерационального маршрута движения, не обеспечит своевременного прибытия подразделения в пункт назначения, и может привести к срыву выполнения определенных задач. Поэтому задача выбора оптимального маршрута движения колонны техники является актуальной.

На содержательном уровне задача выглядит как обоснование математической модели выбора оптимального маршрута движения колонны техники, если критерием оптимальности выступает минимизация времени движения с исходной точки в пункт назначения.

Авторами сформирован математическую модель приведенной задачи, предложен алгоритм ее решения для трех случаев: дискретно-стохастического, дискретно-детерминированного и непрерывно-неопределенного, а также разработано соответствующее программное обеспечение. Выбор маршрутов осуществляется для трех вариантов с учетом того, что изменение весов ребер может осуществляться:

в моменты времени, когда колонна находится в определенной вершине графа, и обновление матрицы весов осуществляется именно в эти моменты. Это случай, когда решение о дальнейшем маршрута движения формируется в точках разветвления дорог с учетом обстановки по состоянию отдельных участков динамично меняется и данные по которому появляются периодически;

в моменты времени, когда колонна находится в определенной вершине графа, и для этих моментов матрицы весов, которые будут иметь место при попадании колонны в вершину, заранее известны. Это случай, когда решение о маршруте движения может быть сформировано в начале движения с учетом известной обстановки по состоянию дорог, динамично меняться, но данные по которому могут быть учтены заранее;

произвольным образом в зависимости от скорости колонны в фиксированный момент времени, для которого известна функция скорости колонны.

Ключевые слова: математическая модель, алгоритм, матрица, пограничная комендатура быстрого реагирования, техника, колонна.

Dr.Sc. Borovyk O.V., Kupelskiy V.V.

ALGORITHMIC SUPPORT FOR SELECTING OPTIMAL TRAFFIC ROUTE OF MOTOR CONVOY OF RAPID REACTION BORDER COMMAND POST

The rapid response border commandant's office is a structural unit of the border detachment, designed to protect and strengthen the protection of a certain section of the state border, and must quickly redeploy its forces and assets. The success of the tasks assigned to the unit depends largely on the timeliness of arrival at the destination. Operational transportation of a significant amount of weapons, personnel and dissimilar cargoes on land is carried out using equipment. At the preparatory stage of the organization of transportation, the problem of forming the optimal composition of the convoy of equipment is solved.

The existing road network provides a sufficiently large number of traffic routes between the starting and ending points. Moreover, this takes place even for insignificant distances between points of departure and destination. The specified conditions for multivariance in the selection.

In addition, the choice of the route of movement depends on many auxiliary conditions: driver training, technical characteristics and reliability of vehicles, traffic safety, road and environmental conditions, distance and timing of transportation, and the like.

Poor accounting of these factors in the aggregate may lead to the choice of an irrational route of movement, will not ensure the timely arrival of the unit at the destination, and may lead to the failure to fulfill certain tasks. Therefore, the task of choosing the optimal route of movement of the column of equipment is relevant.

At the substantive level, the task looks like the justification of the mathematical model for choosing the optimal route for the column of equipment, if the criterion of optimality is minimizing the time it takes to move from the starting point to the destination.

The authors formed a mathematical model of the given problem, proposed an algorithm for its solution for three cases: discrete-stochastic, discretely-determined and continuously-indefinite, and the corresponding software was developed. The choice of routes is carried out for three options, taking into account the fact that the change in the weights of the ribs can be carried out:

at times when the column is at a certain vertex of the graph, and the update of the matrix of weights is carried out precisely at these moments. This is the case when a decision on the further route of movement is formed at the road branching points, taking into account the situation, the status of individual sections changes dynamically and data for which appears periodically;

at times when the column is at a certain vertex of the graph, and for these moments, the matrix of weights that will occur when the column hits the vertex are known in advance. This is the case when a decision on the route of movement can be formed at the beginning of the movement, taking into account the known situation on the state of the roads, dynamically change, but data on which can be taken into account in advance;

randomly depending on the speed of the column at a fixed point in time for which the column speed function is known.

Key words: mathematical model, algorithm, matrix, border commandant of quick reaction, equipment, column.

УДК 629.7.083

д.т.н., проф. **Шишанов М.О.** (ЦНДІ ОВТ ЗСУ)
к.т.н., с.н.с. **Зубарєв О.В.** (ЦНДІ ОВТ ЗСУ)
Гурба О.В. (ДержККБ «Луч»)
Крижанівський Є.С. (ДержККБ «Луч»)

ОЦІНКА ЕФЕКТИВНОСТІ РЕМОНТУ КЕРОВАНИХ АВІАЦІЙНИХ ЗАСОБІВ УРАЖЕННЯ

У статті наведено загальні вимоги до рівня надійності керованих авіаційних засобів ураження (КАЗУ), які можуть бути пред'явлені на основі вимог до показників ефективності функціонування в процесі експлуатації, що в свою чергу залежать від сукупності тактико-технічних та експлуатаційних характеристик КАЗУ, які визначають рівень їх технічної досконалості, а також методику оцінки ефективності керованих авіаційних засобів ураження, в основу якої покладено метод прогресуючого еталону.

Розглянуто оцінку коефіцієнта технічної досконалості зразка ОВТ, яка полягає в оцінці їх рівня розвитку і здійснюється стосовно їх класифікації. Під час проведення аналізу головним чином розглядають найважливіші ТТХ зразків, які визначають основний обрис даного виду (типу) озброєння і найбільшим чином впливають на характер виконання завдань з бойовою використання. Основи їх функціонування та порядок їх використання за призначенням більш повно розглянуто в ряді джерел. Розроблена методика порівняльної оцінки КАЗУ призначена для порівняння можливих варіантів та дозволяє визначити комплексні показники якості, що найбільшою мірою враховують усі існуючі властивості КАЗУ, оцінити відповідність різнорідних за типом виробів КАЗУ тактико-технічним вимогам, кількісним вимогам технічних умов і державних стандартів та провести порівняльну оцінку вітчизняних та іноземних зразків. Наведені основні тактико-технічні характеристики авіаційних керованих ракет класу «Повітря-Повітря» малої дальності з інфрачервоними голівками самонаведення та їх закордонні аналоги. Метою даної статті є проведення попереднього розрахунку рівня технічної досконалості та аналізу пріоритетних напрямків розвитку авіаційних керованих ракет класу «Повітря-Повітря».

Ключові слова: експертна оцінка, керовані авіаційні засоби ураження, коефіцієнт технічної досконалості, метод прогресуючого еталону, метод ранжування, показники ефективності, тактико-технічні характеристики.

Постановка проблеми. Сучасні КАЗУ представляють собою складні технічні системи, елементами яких є механічні, електричні, радіоелектронні, лазерні та інші складові частини. В основі методології їх досліджень, доцільно використовувати системний підхід, який передбачає врахування взаємозв'язків і взаємодій елементів системи. При чому об'єкти системи розглядаються не як самостійні, а як ті, що складаються з підсистем, які, у свою чергу, складаються з окремих складових частин [1, 2]. В основу досліджень КАЗУ був покладений принцип функціонально-морфологічної декомпозиції, яка знайшла широке розповсюдження завдяки своїй наочності, оскільки співпадає з фізичною реалізацією КАЗУ та рекомендується використовувати при оцінці ефективності [3].

Аналіз останніх досліджень і публікацій. Аналіз світового досвіду підтримання справності засобів ураження (ЗУ) засвідчує, що на озброєнні провідних країн продовжують знаходитися ЗУ, які виготовлені ще до початку 90-х років минулого сторіччя. Такий підхід, направлений на зменшення витрат військових відомств, притаманний багатьом країнам світу. Так, Міноборони США виділяє 46,7 мільйони доларів на проведення повторної сертифікації і модернізації ракет для зенітно-ракетних комплексів (ЗРК) "Патріот", які також знаходяться на озброєнні армій 12 держав Європи і Азії. Крім того, на сьогодні основу парку авіаційних ЗУ провідних країн складають вироби, виготовлені ще до початку 90-х років минулого сторіччя. При цьому їх частка у загальному парку приблизно складає 43 % у Сполучених Штатів Америки і майже 100% у країнах Європи. Винятком на загальному тренді є закупівля нових зразків авіаційних керованих ракет класу "повітря-повітря": AIM-120A (Сполучені Штати Америки), РВВ-АЕ (Російська Федерація) та МІКАІЯ (Франція) тощо, яка здійснюється невеликими партіями у зв'язку з їх високою вартістю. Таким чином, переважна більшість країн світу, максимально використовує ресурсний потенціал існуючого парку ЗУ до досягнення ними гранично

допустимих меж експлуатації, дуже поступово замінюючи старіючий парк новими зразками. При цьому підтримання справності цих ЗУ забезпечується їх розробниками та виробниками, які володіють відповідною конструкторською, технологічною і ремонтною документацією, технологічним обладнанням, даними по надійності ЗУ за весь період експлуатації, даними по результатах бойового застосування тощо. Такого потужного конструкторського, технологічного та інформаційного забезпечення в Україні на початок 90-х років минулого сторіччя не було [1-3].

Саме це викликало необхідність створення в Україні системи підтримання справності ЗУ без участі їх розробників та виробників, шляхом максимального використання науково-технічного потенціалу вітчизняних підприємств та науково-дослідних установ, розробки та узаконення на законодавчому рівні правил їх взаємодії.

Мета роботи – проведення попереднього розрахунку рівня технічної досконалості та аналізу пріоритетних напрямків розвитку авіаційних керованих ракет класу «Повітря-Повітря».

Основний матеріал досліджень. Загальні вимоги до рівня надійності КАЗУ можуть бути пред'явлені на основі вимог до показників ефективності функціонування в процесі експлуатації. В свою чергу, показники ефективності залежать від сукупності тактико-технічних та експлуатаційних характеристик КАЗУ, що визначають рівень їх технічної досконалості. Для оцінки рівня технічної досконалості КАЗУ використовують коефіцієнт технічної досконалості $K_{ТД}$ [4-6].

Розрахунок $K_{ТД}$ визначається за формулою

$$K_{ТД} = \sum_{i=1}^{N} Q_i \times \beta_i \ , \qquad (1)$$

де Q_i – показник ефективності i-го зразка КАЗУ; β_i – узагальнене за результатами експертного опитування значення вагового коефіцієнта i-го зразка КАЗУ; N – кількість КАЗУ, що аналізується.

Для вибірки варіантів були обрані КАЗУ, які за функціональними ознаками розділені на однотипні вироби (подальші процедури проводилися тільки між однотипними виробами).

Структурно-логічна схема методики представлена на рис.1 та реалізується в наступній послідовності.

1) Визначення вихідних даних. В якості вихідних даних для проведення розрахунків та порівняння КАЗУ будемо використовувати відомі показники ефективності (наприклад, ймовірність безвідмовної роботи, точність попадання в ціль, дальність бойового застосування, радіус ураження бойової частини тощо).

Для однотипних КАЗУ встановлюється певний перелік показників, що відображають їх властивості, та узагальнюються чисельні значення $\{A_{ij}\}$ – характеристики для кожного КАЗУ.

2) Оцінка пріоритетності j-ої характеристики. Для визначення пріоритетності характеристик β_j застосовується метод ранжирування. Під ранжируванням розуміється процедура встановлення значущості характеристик КАЗУ на підставі їх упорядкування [7].

Для цього проводиться опитування групи із G експертів. Кожен g-й експерт визначає набір чисел C_{jg}, $j = \overline{1, J}$, які відображають його погляд про пріоритетність технічних характеристик КАЗУ, розташовує їх у порядку значимості (важливості) та приписує кожному з них числа натурального ряду: 1, 2, 3 тощо. Ранг показника визначається його номером, якщо на його місці в ряду відсутні будь-які інші. Коли на одному місці маємо декілька показників, що не розрізняються (мають зв'язані ранги), то ранг кожного з них дорівнює середньоарифметичному їх нових номерів. При цьому кількість рангів показників дорівнює R .

Рисунок 1 – Структурно-логічна схема методики порівняльної оцінки КАЗУ

При визначенні коефіцієнтів C_{jg} приймемо, що між рангом і важливістю характеристики КАЗУ існує лінійна залежність. Тоді визначення коефіцієнтів C_{jg} можна визначити за формулою [7-9]

$$C_{jg} = 1 - \frac{r_{jg} - 1}{R}, \tag{2}$$

де r_{jg} – ранг відповідної j -ої характеристики КАЗУ за думкою g -го експерта; R – кількість рангів [10].

Після цього значення C_{jg} нормуються

$$\beta_{jg} = \frac{C_{jg}}{\sum_{j=1}^{J} C_{jg}}, \qquad \sum_{j=1}^{J} \beta_{jg} = 1. \tag{3}$$

Остаточно значення коефіцієнтів важливості β_j за відомостями обчислюються шляхом усереднення значень β_{jg}, які надходять від усіх експертів. Якщо компетентність експертів у групі вважається однаковою, то справедливий вираз [11]:

$$\beta_j = \frac{1}{G} \cdot \sum_{g}^{G} \beta_{jg} \;\; ; \quad g = \overline{1,G} \, . \tag{4}$$

Достовірність результатів експертної оцінки за відомостями характеризується ступенем узгодженості оцінок, які надаються експертами. Для цього використовується коефіцієнт конкордації (W), який визначається за формулою [7]

$$W = \frac{12B}{G^2 \cdot (R^3 - R) - G \cdot \sum_{g=1}^{G} T_g}, \qquad g = \overline{1,G}, \tag{5}$$

де G – кількість експертів; R – кількість рангів; T_g – показник зв'язаних рангів у g-му ранжируванні, що визначається як

$$T_g = \sum_{\varphi=1}^{H_g} (h_{\varphi g}^3 - h_{\varphi g}), \tag{6}$$

де H_g – кількість груп рівних рангів у g-му ранжируванні; $h_{\varphi g}$ – кількість рівних рангів у φ-й групі ранжирування зв'язаних рангів при ранжируванні g-м експертом.

Якщо ранги, що збігаються (зв'язані), відсутні, тоді $T_g = 0$. Сума квадратів відхилення рангів від середньої суми рангів B визначається за формулою

$$B = \sum_{l=1}^{R} \left(\sum_{g=1}^{G} r_{\mathrm{lg}} - \frac{1}{R} \sum_{l=1}^{R} \sum_{g=1}^{G} r_{\mathrm{lg}} \right)^2, \qquad l = \overline{1,R}, \tag{7}$$

де r_{lg} – ранг відповідної l-ої характеристики КАЗУ за оцінкою g-го експерта.

Значення коефіцієнта конкордації знаходиться в діапазоні $0 < W < 1$. При $W = 0$ маємо повну протилежність ранжирувань, а при $W = 1$ – повне збігання ранжирувань.

Якщо характеристики за важливістю вважаються рівними між собою, то показник пріоритетності кожної з них визначається співвідношенням типу $\frac{1}{J}$, де J – загальна чисельність характеристик оцінюваних КАЗУ.

3) Покрокове порівняння КАЗУ з умовно-еталонним. Для кожної характеристики встановлюється критеріальне правило, за яким зі всієї вибірки покроково обирається найкращий (умовно-еталонний) КАЗУ за кожною з характеристик

$$A_{ej} = \max A_{ij}, i = \overline{1...N}, \tag{8}$$

або

$$A_{ej} = \min A_{ij}, i = \overline{1...N}, \tag{9}$$

де A_{ij} – абсолютне значення j-ї властивості у i-ого КАЗУ, що порівнюється; A_{ej} – абсолютне значення цієї властивості у еталона.

4) Визначання відносних персональних показників кожного КАЗУ для кожної характеристики. Для властивостей "більше-краще" відносний показник має вид

$$q_{ij} = \frac{A_{ij} - A_{\min}}{A_{\max} - A_{\min}}, \tag{10}$$

а для властивостей "більше-гірше"

$$q_{ij} = \frac{A_{\max} - A_{ij}}{A_{\max} - A_{\min}} \, . \tag{11}$$

Для властивостей, які виражаються у вигляді "є" чи "немає" відносний показник має вид

$$q_{ij} = \begin{cases} 1, A_{ij} - \text{"є"}, \\ 0, A_{ij} - \text{"немає"}. \end{cases} \quad (12)$$

Для будь-яких властивостей $q_{ij} = 1$, якщо $A_{1j} = A_{2j} = ... = A_{nj} = A_{ej} \neq 0$.

5) Розрахунок середньозваженого комплексного показника ефективності кожного КАЗУ. Комплексний показник i-го КАЗУ Q_i визначається як

$$Q_i = \sum_{j=1}^{J} \beta_j q_{ij}, \quad (13)$$

де β_j – коефіцієнт вагомості j-ої властивості (параметра, технічної характеристики); q_{ij} – відносний одиничний показник j-ої властивості i-го КАЗУ.

6) Нормування значення комплексного показника Q_i. Отримані значення комплексного показника ефективності кожного КАЗУ по відношенню до найбільшого значення нормуються наступним чином [12]:

$$K_i = \frac{Q_i}{\max Q_i}. \quad (14)$$

В результаті проведеного розрахунку визначається рівень технічної досконалості КАЗУ, робиться висновок про пріоритетність оцінюваних варіантів, визначаються переваги та вимоги до характеристик, що потребують покращення.

Розроблена методика порівняльної оцінки КАЗУ призначена для порівняння можливих варіантів та дозволяє:

- визначити комплексні показники якості, що найбільшою мірою враховують усі існуючі властивості КАЗУ;
- оцінити відповідність різнорідних за типом виробів КАЗУ тактико-технічним вимогам, кількісним вимогам технічних умов і державних стандартів;
- провести порівняльну оцінку вітчизняних та іноземних зразків.

В якості прикладу, для оцінки технічної досконалості КАЗУ були відібрані авіаційні керовані ракети (АКР) класу «Повітря-Повітря» малої дальності з інфрачервоними голівками самонаведення (ІЧ ГСН) та їх закордонні аналоги. Основні тактико-технічні характеристики цих ракет наведено у таблиці 1 [13]. Основні тактико-технічних характеристик КАЗУ були розподілені таким чином: поражаюча дія, дальність дії, точність наведення, маневреність, надійність.

Таблиця 1

Основні тактико-технічні характеристики КАЗУ класу «Повітря – Повітря» малої дальності

Основні характеристики	**Р-73** (на озброєнні ЗС України)	**AIM-9X «Сайдуіндер»** (США)	**ASRAAM AIM-132** (Англія)	**A-DARTER** (ЮАР)	**IRIS-T** (Німеччина)	**“Питон-5”** (Ізраїль)
Аеродинамічна схема	Качка	Нормальна	Нормальна	Нормальна	Нормальна	Качка
Маса, кг: стартова бойової частини	105 8	85 10,15	87 7	89 11	87 11,4	105 11
Довжина, м	2.9	2.9	2.9	2.98	3	3
Діаметр, мм	170	127	166	166	127	160
Швидкість, М	3	2.5	3	2	3	4
Тип бойової частини	Стержнева	Стержнева	Осколочно-фугасна	Осколочно-фугасна	Осколочна-фугасна	Стержнева
Система наведення	ІЧ ГСН	Інерціальна + матрична ІЧ ГСН (128x128)	Інерціальна + матрична ІЧ ГСН (128x128)	Інерціальна + ІЧ ГСН (біспектральна матриця)	Інерціальна + матрична ІЧ ГСН (128x128)	Інерціальна + двохспектральна матрична ІЧ ГСН (320x240)

Основні характеристики	**Р-73** (на озброєнні ЗС України)	**AIM-9X «Сайдуіндер»** (США)	**ASRAAM AIM-132** (Англія)	**A-DARTER** (ЮАР)	**IRIS-T** (Німеччина)	**“Питон-5”** (Ізраїль)
Кути відхилення координатора, град.	±45°	±90°	±80°	±90°	±90°	±100°
Максимальна дальність захвату цілі, км	12…20	14…18,5	14...18	20	25	20
Максимальна дальність пуску, км	20	18,5	18	20	25	20
Захват цілі під носієм	Є	Є	Є	Є	Є	Є
Захват цілі на траєкторії	Не має	Є	Є	Є	Є	Є

Згідно із співвідношеннями (2) – (14) методики для обраних ракет визначено $K_{ТД}$, що показано на рис. 2.

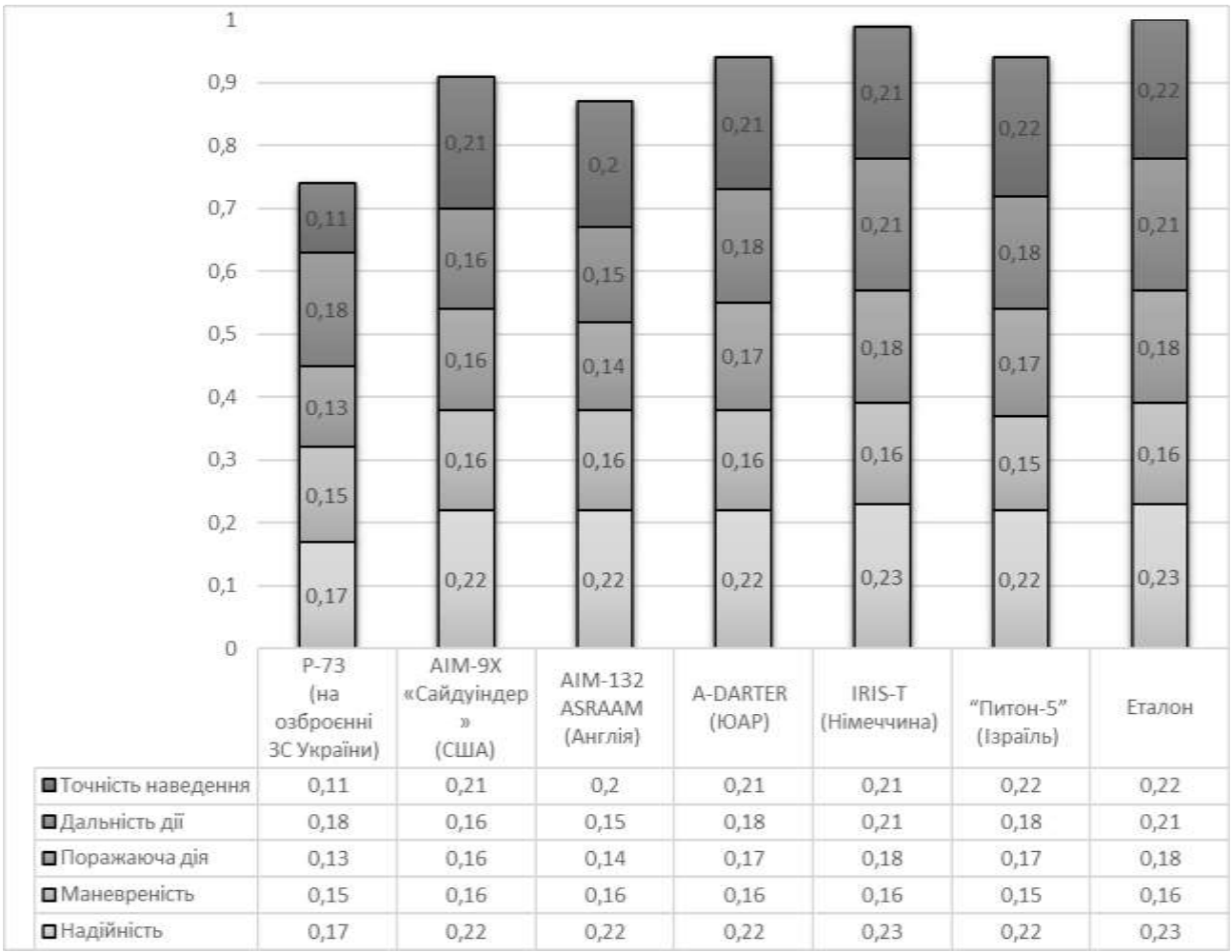


Рисунок 2 – Розрахункові значення $K_{ТД}$ обраних КАЗУ

Аналіз результатів розрахунків $K_{ТД}$ показав, що пріоритетними напрямами розвитку АКР Р-73 класу «Повітря-Повітря» малої дальності, що знаходяться на озброєнні ЗС України є:

- збільшення максимальної дальності пуску (більше 20 км);
- використання сучасних інфрачервоних голівок самонаведення з матричними фотоприймальними пристроями та цифровою обробкою сигналу для розпізнавання цілі та підвищення точності її наведення;

- захват цілі на траєкторії за рахунок застосування високоточних інерціальних систем та сучасних алгоритмів наведення;

- підвищення потужності бойових частин;

- оптимізація масо-габаритних характеристик за рахунок інтеграції елементів апаратури і використання сучасної елементної бази.

Висновки. Таким чином, запропонована методика при проведенні робіт з відновлення справності КАЗУ дає можливість об'єктивно встановити пріоритетність і альтернативи можливих варіантів покращення їх тактико-технічних характеристик та визначити вимоги до них, відпрацювати технічні рішення і технології, що можуть бути застосовані при розробці нових КАЗУ.

ЛІТЕРАТУРА:

1. Ковтуненко А.П., Зубарев В.В. Основы анализа сложных технических систем. Теория и приложения: Монография. – К.: НАУ, 2009. – 483 с.

2. Дедков В.К. Основные вопросы эксплуатации сложных систем / В.К. Дедков, Н.А. Северцев. – М.: Высшая школа, 1976. – 348 с.

3. Зубарев В.В., Любарець А.А., Шатров А.М., Шишанов М.О. Методичні рекомендації щодо декомпозиції керованих авіаційних засобів ураження при рішенні завдань продовження строку їх експлуатації. // Зб. наук. праць ЦНДІ ОВТ ЗС України. – К.: ЦНДІ ОВТ ЗСУ, 2015. – Вип. 2(57). - С. 244-252.

4. Зубарев В.В. Математические методы оценки и прогнозирования технических показателей эксплуатационных свойств радиоэлектронных систем / Монография // В.В. Зубарев, А.П. Ковтуненко, Л.Г. Раскин. – К.: Изд-во НАУ, 2005. – 210 с.

5. Ковтуненко А.П. Основы анализа сложных технических систем / Теория и приложения // А.П. Ковтуненко, В.В. Зубарев. – К.: Изд-во НАУ, 2009. – 483 с.

6. Каменев А.Ф. Технические системы – закономерности развития. – Л.: Машиностроение, 1985. – 186 с.

7. Пирумов В.С. Системный подход в современных исследованиях. Введение в теорию систем / В.С. Пирумов, Е.Б. Лена, А.В. Ефтефеева. – М.: изд. ВМОПА, 1973. – 213 с.

8. Кузнецов В.И. Надежность и эффективность в технике / Справочник // В.И. Кузнецов, Е.Ю. Барзилович, М.: Машиностроение, 1990. – 278 с.

9. Дергачев А.С. Основы экономики авторемонтного производства. – М.: Автотрансиздат, 1978. – 326 с.

10. Моррис де Гроот. Оптимальные статистические решения. -М.: Издательство Мир,1974.- 492 с.

11. Маньшин Г.Г. Управление режимами профилактики сложных систем. – М.: Наука и техника, 1976. – 289 с.

12. Растригин Л.А. Случайный поиск в задачах оптимизации многопараметрических систем. – М.: Знание, 1975. – 310 с.

13. Давыдов А.Н., Черных Л.Г., Панкратов О.Н., Чабанов В.А. Состояние и перспективы развития оружия класса «воздух-воздух» для самолетов 5-го поколения // Научно-информационный центр ГосНИИАС, 2004 – С. 92.

REFERENCES:

1. Kovtunenko A.P., Zubarev V.V. Basics of analysis of complex technical systems. Theory and Applications: Monograph – K.: NAU, 2009. – 483 c.

2. Dedkov V.K. Basic issues of operation of complex systems / V.K. Dedkov, N.A. Severcev. – M.: Высшая школа, 1976. – 348 c.

3. Zubarev V.V., Luberec A.A., Shatrov A.M., Shishanov M.O. Methodical recommendations for the decomposition of controlled aviation means of destruction in solving the tasks of extending terms their use. // Зб. наук. праць CRI WME AFU. – К.: CRI WME AFU, 2015. – Вип. 2(57). - С. 244-252.

4. Zubarev V.V. Mathematical methods of estimation and forecasting of technical indicators of operational performances of radio electronic systems / Monograph // V.V. Zubarev, A.P. Kovtunenko, L.G. Raskin. – K.: Изд-во NAU, 2005. – 210 c.

5. Kovtunenko A.P. Basics of the analysis of complex technical systems / Theory and Applications // A.P. Kovtunenko, V.V. Zubarev. – K.: Изд-во NAU, 2009. – 483 c.

6. Kamenev A.F. Technical systems - patterns of development. - L .: Mechanical Engineering, 1985. – 186 c.
7. Pirumov V.S. A systematic approach to modern research. Introduction to systems theory / V.S. Pirumov, E.B. Lena, A.V. Evtefeeva. – M.: изд. ВМОПА, 1973. – 213 c.
8. Kuznecov V.I. Reliability and efficiency in technology / Handbook // V.I. Kuznecov, E.U. Barzilovich, M.: Машиностроение, 1990. – 278 c.
9. Dergachev A.S. Fundamentals of auto repair production economy. - M .: Avtotransizdat, 1978. – 326 c.
10. Morris de Groot. Optimal statistical solutions. -M .: Mir Publishing, 1974.- C.492.
11. Manshin G.G. Management of modes of preventive measure of complex systems. - M .: Science and technology, 1976. – 289 c.
12. Rastrigin L.A. Random search in optimization problems of multiparameter systems. - M .: Knowledge, 1975. – 310 c.
13. Davudov A.N., Chernuh L.G., Pankratov O.N., Chabanov V.A. State and prospects of development of air-to-air weapons for 5th generation aircrafts // Scientific and Information Center GosNIIAS, 2004 – C. 92.

д.т.н., проф. Шишанов М.А., к.т.н., с.н.с. Зубарев О.В., Гурба О.В., Крижанівський Є.С.

ОЦЕНКА ЭФФЕКТИВНОСТИ РЕМОНТА УПРАВЛЯЕМЫХ АВИАЦИОННЫХ СРЕДСТВ ПОРАЖЕНИЯ

В статье приведены общие требования к уровню надежности управляемых авиационных средств поражения (УАСП), которые могут быть предъявлены на основании требований к показателям эффективности функционирования в процессе эксплуатации, что в свою очередь зависит от совокупности тактико-технических и эксплуатационных характеристик УАСП, которые определяют уровень их технического совершенства, а также методику оценки эффективности управляемых авиационных средств поражения, в основу которой положено метод прогрессирующего эталона.

Рассмотрена оценка коэффициента технического совершенства образца ВВТ, которая заключается в оценке их уровня развития и осуществляется согласно их классификации. Во время проведения анализа главным образом рассматривают важнейшие ТТХ образцов, которые определяют основной обрис данного вида (типа) вооружения и крупнейшим образом влияют на характер выполнения задания по боевому использованию. Основы их функционирования и порядок их использования по назначению более полно рассмотрено в ряде источников. Разработанная методика сравнительной оценки УАСП предназначена для сравнения возможных вариантов и позволяет определить комплексные показатели качества, которые большей мерой учитывают все существующие свойства УАСП, оценить соответствие разнородных по типу изделий УАСП тактико-техническим требованиям, количественным требованиям технических условий и государственных стандартов и провести сравнительную оценку отечественных и иностранных образцов. Наведены основные тактико-технические характеристики авиационных управляемых ракет класса «Воздух-Воздух» малой дальности с инфракрасными головками самонаведения и их иностранные аналоги. Целью данной статьи есть проведение предварительного расчёта уровня технического совершенства и анализа приоритетных направлений развития авиационных управляемых ракет класса «Воздух-Воздух».

Ключевые слова: экспортная оценка, управляемые авиационные средства поражения, коэффициент технического совершенства, метод прогрессирующего совершенства, метод ранжирования, показатели эффективности, тактико-технические характеристики.

Prof. Shyshanov M.O., PhD, Zubariev O.V., Hurba O.V., Kryzhanivskyi Y.S.

ASSESSING THE EFFECTIVENESS OF REPAIR GUIDED AVIATION MEANS OF DESTRUCTION

The article presents the general requirements for the level of reliability of guided aviation means of destruction (GAMD), which can be applied based on the requirements for performance indicators of operation. This depends on the set of tactical, technical and operational characteristics of GAMD, which determine their level technical excellence, as well as a method for assessing the effectiveness of guided aviation means of destruction, based on the progressive standard method. The estimation of the coefficient of technical excellence of samples of armaments, which reveal their level of development and is carried out in relation to their classification, has been considered. During the analysis, the most important performance

characteristics are considered. They define the basic architecture and design of this type of armaments and have the greatest influence on their combat missions.

The basics of their functioning and the order of their intended using are more fully considered in a number of sources. The developed method of comparative estimation of GAMD is intended for comparison of possible variants and allows to define complex indicators of quality that take into account most of all existing properties of GAMD, to assess its conformity to tactical and technical requirements, quantitative requirements and state standards. Moreover, it allows conducting a comparative assessment of domestic and foreign samples of armaments. The basic performance characteristics of short-range guided aviation missiles of the Air-to-Air class with infrared heads and their foreign analogues are given. The purpose of this article is to conduct a preliminary calculation of the level of technical excellence and analysis of the priority directions of development of air guided missiles of the Air-to-Air class.

Keywords: expert assessment, guided aviation means of destruction, coefficient of technical excellence, progressive standard method, ranking method, performance indicators, tactical and technical characteristics.

UDC 681.3

Prof. **Lienkov S.V.** (MIKNU)
Ph.D. **Banzak G.V.** (OSATRQ)
Ph.D. **Zhyrov G.B.** (MIKNU)
Ph.D. **Okhramovych M.M.** (MIKNU)
Ph.D. **Protsenko Ya.N.** (MIKNU)

OPTIMIZATION OF MAINTENANCE COMPLEX OBJECTS OF RADIO ELECTRONIC EQUIPMENT

The article discusses models for optimizing the maintenance eservice process (MS) of complex objects of radio-electronic technics (RET). The statement of the problem determining optimal parameters of objects MS is formulated for the case if the state maintenance strategy MS (MSS strategy) is used.

As a criterion of optimization, the requirement minimum unit cost of operating an object for a given period of its operation is used, provided that the required level of failure-free operation of the object is estimated as estimated by "mean time on failures". The objective functions of the optimization task are determined by modeling the process of MS and repair (MSandR) of the object. This circumstance explains the choice of a search method for an approximately optimal solution to the problem: simplest relaxation method of direct enumeration is used, controlled by a human expert who solves this problem in the interactive dialogue mode between the user and the computer.

The methodology for determining approximately optimal parameters of strategy MSS described in this article is intended for use in the development of object RET. The methodology allows the early stages of development to pre-evaluate possibility of increasing level reliability of the facility due MS. At later stages of development, when all technical solutions have already become known, elements for which there are measurable determining parameters become known, preliminary estimates of the necessary parameters MSS can be refined and corrected design decisions. Corresponding refinement of calculations should be made every time when accurate data on the reliability of component parts appear.

Software (SW) was developed for computer support of the solution search process. SW developed by Delphi programming tools.

Key words: object of radio-electronic technics, maintenance, mean time on failures, unit cost of operation, simulation statistical modeling.

Introduction and statement of the problem. A complex object of radio-electronic technics (RET) is understood to mean a technical device consisting of a large number (tens, hundreds of thousands) of various types components (mechanical, electromechanical, radio and optoelectronic, hydraulic, etc.). Examples of complex RET objects include radar stations, elements of anti-aircraft missile systems, electronic warfare stations, etc. The operation of various components of such objects is based on different physical principles, have significantly different reliability indicators and, therefore, require different terms and volumes of work for their maintenance.

Maintenance (MS) of complex RET facilities is intended to ensure the required level of their failure-free operation. Carrying out maintenance always requires certain costs (time, cost, electricity, etc.), so the task of minimizing these costs naturally arises. To solve this problem, it is necessary to build a mathematical model in which the goals of the optimization problem (objective functions) and the parameters of these functions should be optimized in a formalized form.

With this in mind, we will use the following indicators as objective functions in the problem under consideration:

T_0 - average time between failures of an object [1];

$c_э$ - unit cost of operating RET object at a given time interval.

Using these notations, the problem of optimizing the parameters of the selected MS strategy in a formal form can be written as follows:

$$T_0(\mathrm{P}^*_{\text{то}}) \geq T_0^{\text{тр}};$$
$$c_э(\mathrm{P}^*_{\text{то}}) \to \min, \qquad (1)$$

where $\mathrm{P}_{\text{то}}$ - is the designation of the generalized parameter of the maintenance strategy, the specific content of which is determined by the selected maintenance strategy;

$T_0^{тр}$ – required value of the mean time between failures of the facility.

$P_{то}^{*}$ – is the optimal value for the parameter.

The most common in practice are two fundamentally different MS strategies: the maintenance-by-status strategy (MSS strategy) and the maintenance-by-resource strategy (MSR). The strategy MSS is more effective than strategy MSR (in terms of influencing the facility's failure-free level). However, strategy MSS, as a rule, requires significantly greater economic costs, since it requires the presence of additional hardware necessary to determine the actual technical condition of object during its operation.

In this article we will consider only strategy MSS. Let us denote the set of all structural elements objects, by the state of which the TC of the object is determined $E_{о}$ ($E_{о}$ – these are the elements included in the structural diagram of the reliability objects). We assume that only a part of them undergo maintenance during operation. The set of serviced elements is denoted by $E_{то}$ ($E_{то} \subseteq E_{о}$).

Analysis of recent research. Recently, more and more attention has been paid to improving the technical operation of complex equipment. A special “niche” is the issues of optimizing the maintenance parameters long-term use of electronic equipment. For the developer of these processes, it is important to have methodologies for a qualitative assessment of the mechanism influence of individual processes on the degradation and failure of RET.

A lot of research has been devoted to questions of calculating and predicting reliability, as well as creating models (including simulation ones). In work [2], a method has been proposed for developing modern methods for assessing reliability based on numerical modeling. In work [3], a method for calculating reliability based on graphs was proposed. In work [4], MEMS structural reliability modeling method is presented and the FORM method is described for obtaining the reliability index and its sensitivity with respect to input random variables and their parameters, which can not only be used to assess the reliability of an object, but can also help determine key factors for additional structural improvements. In work [5], Weibull – Corrosion extended covariance model is proposed for assessing the reliability of a system that faces operational stresses. A combination method for analyzing the reliability of a multivariate system was proposed in work [6]. The method is based on a combination of BDD and MMDD models. In work [7], it is proposed to use a semi-parametric bayesian approach to obtain reliability indicators of multilevel hierarchical systems, both with parallel and serial connection of components.

In these works, the methodology for determining reliability indicators of system for given set of failing elements and their characteristics is described in detail, but the problem of choosing this set and its effect on reliability indicators is practically not addressed.

где $\{E_{то}\}$ - множество всех множеств $E_{то}$;

The main results of study. By *determining parameter* (DP) we mean the physical or functional parameter, value of which determines the operability of element [8].

The normalized DP value of the *i*-th element is denoted by $u_i(t)$ ($u_i(t) \in [0,1], i = \overline{1, |E_{то}|}$). The value 0 corresponds to the nominal (required) value of the parameter, the value 1 is the boundary value, upon reaching which the element is considered to be failed (inoperative). Random DP values $u_i(t)$ describe the physical process of element degradation. All values $u_i(t) < 1$ correspond to the healthy state of element.

We introduce the concept of a maintenance *level* as $u_{i\,то}$ follows ($u_{i\,то} < 1$). If the value at a certain point in time (operating time) t reaches a level (level of maintenance), then at this point in time, maintenance (replacement) of this element is required.

Taking into account the introduced concepts and notation, the generalized parameter of the strategy MSS $P_{тос}$ is represented by the following set [9]:

$$P_{то} = P_{тос} = \{E_{то}, U_{то}, T_{к}\}, \quad (2)$$

where $E_{то}$ – is the set of serviced elements; $U_{то} = \{u_{i\,то}; i = \overline{1, |E_{то}|}\}$ $T_{к}$ – a vector of normalized values determining parameters of the serviced elements (vector of MS levels), upon reaching which

element MS is required; $T_к$ – frequency of monitoring the vehicle. When monitoring the vehicle's vehicle, the values of all serviced TC elements are measured and, based on the measurement results $u_i(t)$, a decision is made about the need for maintenance.

Taking into account definition (2), the statement of optimization problem (1) can now be written as follows:

$$T_0(E^*_{то}, U^*_{то}, T^*_к) \geq T_0^{тр};$$
$$c_э(E^*_{то}, U^*_{то}, T^*_к) \to \min, \quad (3)$$

where, $E^*_{то}$, $U^*_{то}$ and $T^*_к$ - are the sought optimal values parameters of strategy MSS.

The main features of problem (3) are two: firstly, there are no analytical expressions for the objective functions that would associate their values with the parameters of the functions, and secondly, this is a complex structure of the space optimized parameters $P_{тос}$ (according to (3) this space is three-dimensional and heterogeneous). These features do not allow the use of standard classical optimization methods to solve problem (3).

The space in which the search for optimal values $E^*_{то}$, $U^*_{то}$ and $T^*_к$ should be carried out is a cartesian product of the following form (Fig. 1)

$$\{E_{то}\} \times [0,1]^{|E_{то}|} \times [0,\infty), \quad (4)$$

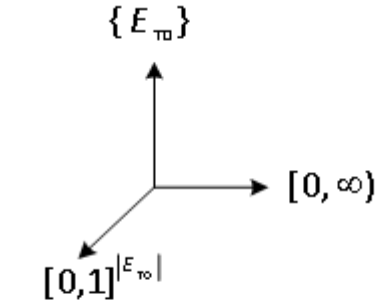


Fig .1. The search space for optimal solution

where $\{E_{то}\}$ - is the set of all sets $E_{то}$;

$[0,1]^{|E_{то}|}$ - hypercube, each point in which is a vector of dimension $|E_{то}|$, elements of the vector are numbers belonging to a segment;

$[0,\infty)$ - numerical axis containing all positive numbers.

Searching in such a space for a "point" representing an optimal solution $P^*_{тос} = \{E^*_{то}, U^*_{то}, T^*_{то}\}$ is a difficult task requiring use of non-standard approaches.

The article discusses the methodology for approximate solution of problem (3), based on the application of the ISM, which is implemented in the ISMPN program [10]. With the help of the ISM, the estimates of the objective functions T_0 and $c_э$ taking into account the maintenance are determined by modeling. The problem is solved in the mode of interactive user dialogue with a personal computer (PC).

The idea of the methodology consists in the sequential (step-by-step) formation of set $E^*_{то}$ by including in it at each step one element taken from the base set $E^*_{то}$ of all potentially serviced elements. The set $E^*_{то}$ is set by the user ($E'_{то} \subseteq E_о$) [11,12]. It is assumed that before starting to solve the problem, a database (DB) was created (using the ISMPN program), into which all the necessary information about object RET for which this problem is solved is entered. The content of the methodology is most conveniently stated by presenting it in the form of an algorithm (Fig. 2). Let us briefly consider the operation of this algorithm.

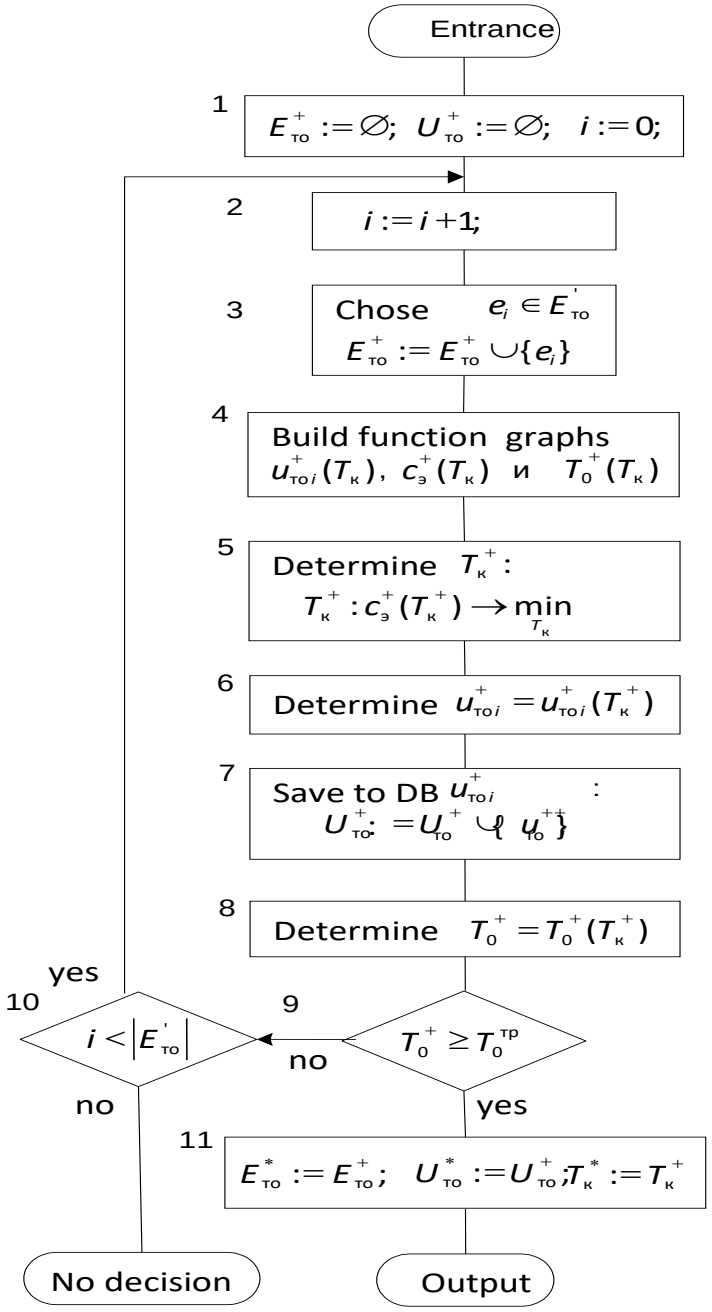


Figura 2. Algorithm for determining pameters with a constant freguency of control

Operator 1 indicates preparatory operations: auxiliary sets $E^+_{\text{то}}$ и $U^+_{\text{то}}$ are created (in the PC memory) and in which the corresponding elements of the future solution $E^+_{\text{то}}$ и $U^+_{\text{то}}$ will be formed and. At first they are empty. The variable i is initiated, with the help of which the number of completed steps in the process of solving the problem will be calculated. Operator 2 generates number of the next step.

At the beginning of each step, one element e_i must be added to the set $E^+_{\text{то}}$, taken from the set $E'_{\text{то}}$ (operator 3). These actions are performed by the user "manually" in the **Database** mode of the ISMPN program. The choice of elements to include them in the set is recommended to be made in order of increasing level of reliability.

After adding a new element to set $E'_{\text{то}}$, calculations are carried out using the ISMPN program (in **Optimization TO | TO "by state"** mode). In fig. 2, these actions are presented by operator 4. As a result of the calculations, function $u^+_{\text{то}i}(T_к)$, $c^+_э(T_к)$ and $T_0^+(T_к)$ schedules are generated, and in a given range of control $D(T_к)$ periodicity values.

The results obtained during the modeling process always contain a random component, therefore, these graphs are formed as average estimates accumulated by the results repeated repetitions of calculations. The user monitors calculation process and interrupts calculations as soon as he considers achieved accuracy of the graphs sufficient for practical solutions. The form of obtained graphs for example considered below is shown in Fig.3.

Each point on the graphs $u^+_{\text{то}i}(T_к)$, $c^+_э(T_к)$ and $T_0^+(T_к)$, and it turns out as the accumulated average, obtained by varying parameter $u_{\text{то}i}$ (level of MS element e_i), added in $E^+_{\text{то}}$ in current step. As a conditionally optimal value of MS $u^+_{\text{то}i}$ level, value corresponding to minimum of indicator is selected $c_э(E^+_{\text{то}\,i}, U^+_{\text{то}\,i}, T_к)$:

$$u^+_{\text{то}\,i}(T_к) : c_э(E^+_{\text{то}\,i}, U^+_{\text{то}\,i}, T_к) \to \min_{u_{\text{то}\,i} \in [0,1]}, \qquad (5)$$

where $U^{+}_{\text{то}i} = \{u^{+}_{\text{то}1}, ..., u^{+}_{\text{то}i-1}, u_{\text{то}i}\}$ – is vector in which $u^{+}_{\text{то}1}, ..., u^{+}_{\text{то}i-1}$ – are conditionally optimal values of MS $u_{\text{то}i}$ – levels found in the previous steps and stored in database, is value of MS level of *i*-th element varied in the current step.

On graphs $c^{+}_{\text{э}}(T_{\text{к}})$ and $T^{+}_{0}(T_{\text{к}})$ displays estimates of the corresponding indicators and found as a result of modeling are displayed $c_{\text{э}}(E^{+}_{\text{то}i}, U^{+}_{\text{то}i}, T_{\text{к}})$ and $T_{0}(E^{+}_{\text{то}i}, U^{+}_{\text{то}i}, T_{\text{к}})$. Varying frequency of control $T_{\text{к}}$ is carried out in a user-defined range of values $D(T_{\text{к}})$. The range of variation $D(T_{\text{к}})$ is selected by the user in such a way as to ensure that a minimum of function $c^{+}_{\text{э}}(T_{\text{к}})$ (if one exists) falls within him and an acceptable accuracy of solution.

Based on obtained schedule $c^{+}_{\text{э}}(T_{\text{к}})$, conditionally optimal value of the monitoring periodicity is determined $T^{+}_{\text{к}}$ (operator 5):

$$T^{+}_{\text{к}} : c^{+}_{\text{э}}(T^{+}_{\text{к}}) = \min_{T_{\text{к}} \in D(T_{\text{к}})} c^{+}_{\text{э}}(T_{\text{к}}). \qquad (6)$$

For the found value $T^{+}_{\text{к}}$ from graph $u^{+}_{\text{то}i}(T_{\text{к}})$, determine the conditionally optimal value of level MS $u^{+}_{\text{то}i} = u^{+}_{\text{то}i}(T^{+}_{\text{к}})$ (operator 6). Save obtained value $u^{+}_{\text{то}i}$ in database (operator 7). This operation is performed by the user "manually" in **Database** mode [10]. After that, value $u^{+}_{\text{то}i}$ is stored as *i*-th element of vector $U^{+}_{\text{то}i}$.

Then, according to schedule $T^{+}_{0}(T_{\text{к}})$, determine value T^{+}_{0} - mean time between failures achieved in current step (operator 8).

Check compliance with the requirement $T^{+}_{0} \geq T^{\text{тр}}_{0}$ (operator 9). If this requirement is fulfilled, process of solving problem is completed, conditionally optimal parameter values are obtained, $E^{+}_{\text{то}}$, $U^{+}_{\text{то}}$ and $T^{+}_{\text{к}}$ are accepted as approximately optimal values $E^{+}_{\text{то}}$, $U^{+}_{\text{то}}$ and $T^{+}_{\text{к}}$ (operator 11), an approximate solution is obtained $\text{P}^{*}_{\text{тос}} = \left\{E^{*}_{\text{то}}, U^{*}_{\text{то}}, T^{*}_{\text{то}}\right\}$.

If condition $T^{+}_{0} \geq T^{\text{тр}}_{0}$ is not fulfilled, it is necessary to check if there are more elements that can be included in set $E^{+}_{\text{то}}$ (operator 10). If there are any, it is necessary to continue the process of searching (forming) a solution to the problem, proceed to the next step of solving the problem (operator 10 transfers control to operator 2). Otherwise, if all potentially serviced elements $E^{+}_{\text{то}}$ have been exhausted, it is concluded that there is no solution to problem (3) under given conditions.

In fig. 3 shows the view of the PC screen after completion of the simulation at the next step of solving the problem (after executing operator 4).

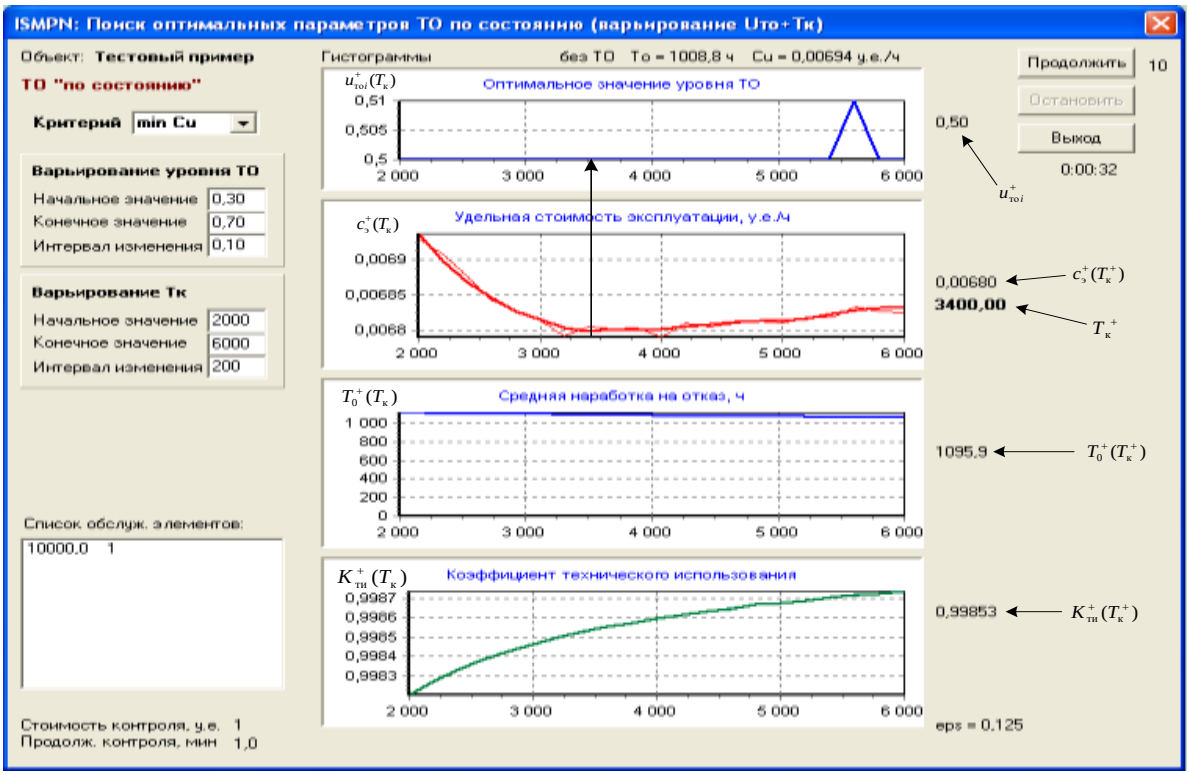


Figure 3 - The view of PC screen after completing calculations in the 1-st step

Findings. The methodology for determining approximately optimal parameters of strategy MSS described in this article is intended for use in the development process of RET object. The technique allows the early stages of development to pre-evaluate the possibility of increasing the level of reliability of an object due to maintenance. At later stages of development, when all technical solutions have already become known, elements for which there are measurable determinative parameters become known, preliminary estimates of the necessary parameters of MSS can be refined and corrected design decisions. Corresponding refinements to calculations should be made each time when accurate data on the reliability of component parts appear. Thus, the developed technique and its supporting software can be an effective means of reliable analysis of the RET object at all stages of its creation.

LITERATURE:

1. SOST 27.002-89. Reliability in technics. The basic concepts. Terms and definitions. It is entered from 01.07.1990.

2. Jason Brown, Lucas Mol. (2017). On the roots of all-terminal reliability polinomials. Discrete Matehematics, 340(6), P. 1287-1299.

3. Xiao Feng Liang, Hong Dong Wang, Hong Yi, Dan Li. (2017)/ Warship reliability evaluation based on dynamic Bayesian networks and numerical simulation/ Ocean Engineering, 136, P. 129-140.

4. Hongmao Tu, Wenzhong Lou, Zhili Sun, Yunpeng Qian. (2017). Structural reliability simulation for the latching mechanism in MEMS-based Safety and Arming device. Advances in Engineering Softvare, 108, PP. 48-56.

5. Jianing Wu, Shaoze Yan, Junlan Li, Yongxia Gu. (2016). Mechanism reliability of bistable compliant mechanisms considering degradation and uncertainties: Modeling and evaluation metod. Applied Mathematical Modelling, 40(23-24), P. 10377-10388.

6. Ying Yi Li, Ying Chen, Zeng Hui Yuan, Ning Tang, Rui Kang. (2016). Reliability analysis of multistate systems subject to failure mechanism dependence based on a combination method. Reliability Engineering & System Safety, Available online 18 November 2016.

7. Li, M., Q. Hu, and J. Liu (2014). Proportional hazard modeling for hierarchical systems with multilevel information aggregation. He Transactions, 46(2), P. 149-163/

8. SOST 27.005-97. Reliability in technics. Models of refusals. Substantive provisions. - It is entered from 01.01.99. - 45 p.

9. Lienkov S.V., Tsytsarev V.N., Zajtsev D.V., Proczenko Ja.N. Modelling of process of maintenance service on a condition of objects of radio-electronic technics with that are reserved elements // Magazine Kharkov university of Air forces of Kharkov «Systems of processing information». - Kharkov, 2016. . - №7(144). – P. 61-65.

10. Forecasting reliability of complex objects of radio-electronic technics and optimization of parameters of their technical operation with use of imitating statistical models. The monography / S.V. Lienkov, K.F. Borjak, G.V.Banzak, V.O.Brown [and, etc.]: under edition S.V.Lienkov. - Odessa: Publishing house " BMB ", 2014. - 256 p.

11. For, R., Kofman, A. & Deni-Papen, M. (1966). Sovremennaja matematika. M/: Mir. – 276 p.

12. Strelnikov V.P. & Feduhin A.V. (2002). Otsenka I prognozirovanie nadezhnosti elektronnyh elementov I system. K.: Logos. 486 p.

д.т.н., проф. Лєнков С.В., к.т.н Банзак Г.В., к.т.н., с.н.с. Жиров Г.Б., к.т.н., с.н.с. Охрамович М.М., к.т.н. Проценко Я.М.

ОПТИМІЗАЦІЯ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ СКЛАДНИХ ОБ'ЄКТІВ РАДІОЕЛЕКТРОННОЇ ТЕХНІКИ

У статті розглянуті моделі оптимізації процесу технічного обслуговування (ТО) складних об'єктів радіоелектронної техніки (РЕТ). Сформульовано постановку задачі визначення оптимальних параметрів системи ТО об'єкта для випадку, якщо застосовується стратегія ТО за станом (стратегія ТОС).

В якості критерію оптимізації використовується вимога мінімуму питомої вартості експлуатації об'єкта на заданому періоді його експлуатації за умови забезпечення необхідного рівня безвідмовності об'єкта, що оцінюється показником «середнє напрацювання на відмову». Цільові функції задачі оптимізації визначаються шляхом моделювання процесу ТО і ремонту (ТОіР) об'єкта. Цією обставиною пояснюється вибір методу пошуку наближено оптимального рішення задачі: використовується найпростіший релаксаційний метод прямого перебору, керований людиною-експертом, вирішальним це завдання в режимі інтерактивного діалогу користувача з комп'ютером.

Викладена в даній статті методика визначення наближено оптимальних параметрів стратегії ТОС призначена для застосування в процесі розробки об'єкта РЕТ. Методика дозволяє на ранніх стадіях розробки попередньо оцінити можливості підвищення рівня безвідмовності об'єкта за рахунок проведення ТО. На більш пізніх стадіях розробки, коли вже стають відомими все технічні рішення, стають відомими елементи, для яких є вимірювані визначають параметри, попередні оцінки необхідних параметрів ТОС можна уточнювати і коректувати конструкторські рішення. Відповідні уточнення розрахунків слід проводити кожен раз при появі уточнених даних про надійність комплектуючих елементів.

Розроблено програмне забезпечення (ПО) для комп'ютерної підтримки процесу пошуку рішення. ПО розроблено засобами програмування Delphi.

Ключові слова: об'єкт радіоелектронної техніки, технічне обслуговування, середнє напрацювання на відмову, питома вартість експлуатації, імітаційне статистичне моделювання.

д.т.н., проф. Ленков С.В., к.т.н Банзак Г.В., к.т.н., с.н.с. Жиров Г.Б., к.т.н., с.н.с. Охрамович М.Н., к.т.н. Проценко Я.Н.

ОПТИМИЗАЦИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ СЛОЖНЫХ ОБЪЕКТОВ РАДИОЭЛЕКТРОННОЙ ТЕХНИКИ

В статье рассмотрены модели оптимизации процесса технического обслуживания (ТО) сложных объектов радиоэлектронной техники (РЭТ). Сформулирована постановка задачи определения оптимальных параметров системы ТО объекта для случая, если применяется стратегия, ТО по состоянию (стратегия ТОС).

В качестве критерия оптимизации используется требование минимума удельной стоимости эксплуатации объекта на заданном периоде его эксплуатации при условии обеспечения требуемого уровня безотказности объекта, оцениваемый показателем «средняя наработка на отказ». Целевые функции задачи оптимизации определяются путем моделирования процесса ТО и ремонта (ТОиР) объекта. Этим обстоятельством объясняется выбор метода поиска приближенно оптимального решения задачи: используется простейший релаксационный метод прямого

перебора, управляемый человеком-экспертом, решающим данную задачу в режиме интерактивного диалога пользователя с компьютером.

Изложенная в данной статье методика определения приближенно оптимальных параметров стратегии ТОС предназначена для применения в процессе разработки объекта РЭТ. Методика позволяет на ранних стадиях разработки предварительно оценить возможности повышения уровня безотказности объекта за счет проведения ТО. На более поздних стадиях разработки, когда уже становятся известными все технические решения, становятся известными элементы, для которых имеются измеряемые определяющие параметры, предварительные оценки необходимых параметров ТОС можно уточнять и корректировать конструкторские решения. Соответствующие уточнения расчетов следует производить каждый раз при появлении уточненных данных о надежности комплектующих элементов.

Разработано программное обеспечение (ПО) для компьютерной поддержки процесса поиска решения. ПО разработано средствами программирования Delphi.

Ключевые слова: объект радиоэлектронной техники, техническое обслуживание, средняя наработка на отказ, удельная стоимость эксплуатации, имитационное статистическое моделирование.

UDC 531:535

Prof. **Mokritskij V.A** (ONPU)
Dr. Sci. Tech. **Maslov O.V.** (ONPU)
Dr. Sci. Tech. **Banzak O.V.** (OSATRQ)
PhD. **Leshchenko O.I.** (OSATRQ)

MODELING OF HARDWARE SPECTRUMS OF CdZnTe- DETECTORS

This article has developed a technique for modeling the instrumental spectrum obtained by measuring the intrinsic gamma radiation of spent nuclear fuel with different burnup depths and the degree of leakage fuel cladding. The spectrum model of the studied fuel assembly made it possible to determine the sensitivity of measurements and choose the optimal algorithm for processing the spectra. Due to this, costs of developing hardware and software components of the nuclear fuel condition monitoring system have been reduced.

The difference between this technique and the known ones is that they did not use the simulation of the distribution of electric field strength in the volume of the sensor crystal and did not use the Monte Carlo method to simulate electric charge induced during the initial interaction of gamma radiation with the crystal. An experimental verification of the technique using the example of modeling the radiation spectrum of ^{137}Cs source confirmed the effectiveness of the use of the spectrometer based on the CdZnTe detector created in this work: compliance with the requirements for monitoring the state of nuclear fuel in real time; identification of fuel assemblies containing fuel elements with an unpressurized cladding; determination of fuel burnup based on the activity of fission products.

For the first time, a method has been proposed for processing large packets of the spectra of the own gamma radiation of spent nuclear fuel. A distinctive feature of the method is the two-stage processing of the spectra: at the first stage, parameters are determined that describe the measured spectra and are necessary for the operation of the algorithms for their processing by methods of numerical differentiation; at the second stage, using these methods, large arrays of spectra are automatically processed in real time.This method increases the accuracy of measurements and the completeness of the distribution pattern of burnup over the fuel assembly volume. This is the technological basis of the tomography method created in this work.

Keywords: parametric reliability, photodetectors, performance criterion, ionizing radiation, crystal structure

Formulation of the problem. The aim of this work is to develop new improved methods and means of controlling nuclear materials and the state protective barriers at nuclear power plants. Creation of new generation radiation sensors and measuring systems based on them.

Analysis of recent research. Methods for tomographic analysis objects of different physical nature, i.e. the restoration of the physical structure an object from physical fields measured outside the object, as a rule, on a closed surface, originated in the 70s of the 20th century. in connection with the construction of x-ray tomographic images of human organs [1]. In the 80s tomographic methods were widely used in industry for flaw detection [2, 3]. Most of the methods developed to date, as a rule, use active tomography, which assumes the presence of a radiation source passing through the object being examined, and a receiver (or group of receivers) recording the radiation transmitted through the object. To analyze the state of nuclear fuel (NF), in particular, fuel assemblies, it is advisable to use passive emission tomography, based on the registration of its own gamma radiation from fission products (FP) NF, followed by determination of their activity inside the studied fuel assembly.

A rather limited number of papers are devoted to the actual tasks passive emission tomography of nuclear fuel. All of them are made at Uppsala University (Department of Radiation Sciences, Uppsala, Sweden). In particular, in the most thorough pioneering work, as in the subsequent works of Swedish researchers, task was to substantiate theoretically passive emission tomography of the BWR fuel assembly produced by ABB Atom, Sweden of a square form containing 8x8 = 64 round fuel rods [4]. The goal of this work was to establish the absence of one or more fuel rods in the fuel assembly, since the task of nuclear fuel imaging was solved within the framework program for ensuring the nonproliferation of nuclear materials.

The analysis of state questions led to the following conclusions:

– there is a fundamental possibility of using emission gamma tomography of nuclear fuel in order to restore the distribution of fission products by the example of a fuel assembly of a BWR reactor with 64 fuel rods;

– for a fuel assembly of WWPR-1000 reactor containing much more structural elements, development of a new, more efficient tomography algorithm is required;

– from point view of real-time tomography implementation when performing routine operations with nuclear fuel, in particular, overloading, is required sufficiently high computational efficiency of the algorithm.

Main part. In this work, the main principle of constructing a spent nuclear fuel (SNF) control system was chosen to increase the efficiency of measuring the spectra of our own gamma radiation from the spent fuel assembly (SFA). At the same time, from the point of view of minimizing the time spent, it is optimal to carry out such a measurement directly in the process of SNF overload: during vertical movement from the rack of the holding pool [5-7].

This choice is due to the significantly higher information content measurements of the own gamma radiation of SFA. Such measurements make it possible to determine the burnup, holding time and initial enrichment of a controlled SFA without using additional information. In contrast, the data obtained using the existing methodology — measuring the total neutron count rate — make it possible to estimate SNF burnup with the use of additional information on the exposure time and initial enrichment [8, 9]. However, since the overload time is strictly regulated, operations to control burnup depth of nuclear fuel, the exposure time and the initial enrichment should be coordinated in time with the schedule of overload process. Therefore, the main criterion in determining the structure of burnup depth control system should be chosen to work in real time.

As a result of passage gamma radiations through the detector and subsequent processing of the received signal, it is possible to obtain an instrumental spectrum, which is a direct reflection of the interactions of gamma rays with a detecting medium. It provides the primary information used for further analysis of gamma radiation.

The hardware spectrum is complex due to the peculiarities of registering gamma radiation with proportional detectors. In addition, there are both natural and technological limitations on how accurately a detecting system can detect gamma radiation energy. A natural limitation arises mainly due to statistical fluctuations associated with the processes of charge formation in the detector. The positions of the total absorption peaks can also be distorted by such electronic effects as noise, pulse superposition, incorrect installation of the pole-zero circuit, etc. In addition, the real spectrum of gamma radiation of the sample can differ significantly from the spectra obtained in laboratory conditions.

Therefore, in this work, to analyze the possibility of using the manufactured spectrometer in a radiation-technological monitoring system for the state of nuclear fuel, to refine and debug algorithms and programs for processing the measured spectra, we developed a technique for modeling instrument spectra when measuring the own gamma radiation of spent nuclear fuel at various burnup depths and leaks fuel cladding [10]. This significantly reduced the development of hardware and software components of the radiation technology control system, since the theoretical spectrum model of fuel assembly under study allows one to determine measurement sensitivity and select the optimal spectral processing algorithm.

When developing the methodology, the statement was used that the changes in the measurement conditions correspond to linear irreversible transformations of the space of the instrument spectra, and the spectrum of *i*-th component under arbitrary measurement conditions can be represented as:

$$\varphi(a) = \sum_{i=0}^{L} a_i \varphi_i(a), \quad \sum a_i = 1, \tag{1}$$

where $\varphi_i(a)$ – linearly independent spectrum obtained by preliminary measurements, and the coefficients a_i are ame for all components.

The technique for simulating instrumental spectra is based on the following procedures:

1. The spectrum of isotopes with a large number lines is represented as a linear combination of monoenergetic spectra taking into account the quantum yield in geometry of the "narrow beam"; for each isotope, self-absorption in fuel assemblies is not taken into account.

2. The change in the monoenergetic spectrum is simulated due to interaction with the material of surrounding technological environment and the fuel matrix.

3. The first and second procedures are used to form the instrumental spectrum of a mixture isotopes.

The instrumental spectrum of monoenergetic gamma radiation in the “narrow beam” geometry consists of three main components — the peak of total absorption, the peak of emission, and the continuous distribution on the left side due to Compton scattering.

The peculiarity of the detector used is that the analogous representation of the total absorption peak is not a simple Gaussian due to the physics of the process of collecting charge arising from the interaction of the gamma quantum with the detector material.

There are several methods for modeling the hardware gamma-ray detection spectra with detectors based on CdZnTe and CdTe [11, 12]. This method differs from the known methods in that it did not use the simulation of the distribution of electric field strength in the detector volume and did not use the Monte Carlo method to simulate electric charge induced during initial interaction of gamma radiation with detector material [10]. This is due to the fact that applied system of electrodes uses an electrode system that creates spherical geometry of the electric field. Verification of the fulfillment of the quasisphericity conditions for the collection of charge carriers is a key link in the manufacture of the detector. In addition, the peak of departure is modeled, and this does not provide for any of the mentioned methods.

Common to all techniques for modeling the total absorption peak in CdZnTe-based detectors are taking into account the “pulling” of left half total absorption peak due to the contribution of the slower “hole” component, as well as the use of experimental parameters. This is due to poor knowledge processes of growing homogeneous defect-free single crystals of CdZnTe and CdTe and, as a result, the inability to describe band structure of a specific sample from which the detector will be made from generalized electrophysical characteristics. In addition, presence and quantitative characteristics of defects, differences in the mobility and configuration of electric field, and influence of the site primary interaction gamma quantum with the crystal cannot be foreseen. At the same time, general view of the hardware spectrum for detectors made using the same technology is same.

When modeling the spectrum in this work, we used the analytical representation of the peak of total absorption:

$$n(E_i) = n_0 \exp\left[-\frac{(E_i - E_0)^2}{2\sigma^2}\right] + n_0 F_t(E_i), \qquad (2)$$

where $F_t(E_i) = \{A \cdot \exp[B(E_i - E_0)]\}\left\{1 - \exp\left[\frac{C(E_i - E_0)^2}{2\sigma^2}\right]\right\}\delta$ is a function describing the left “tail” of peak total absorption formed due to later collection of charge by holes (F_t – symbol *t* from “tail” – remainder); $n(E_i)$ – number of samples in the channel corresponding to energy of gamma rays E_i; n_0 – peak amplitude; E_0 – centroid peak; σ^2 – dispersion of the Gaussian distribution; $FWHM = 2\sigma\sqrt{\ln 2}$ – full width of photopeak at half its height; A – parameter determining amplitude of the function F_t; B – parameter that determines decline of the function F_t; C – parameter defining “cutoff” of the function F_t; $\delta = 1$ at $E_i < E_0$ and $\delta = 0$ at $E_i > E_0$.

In this case, the peak of emission is described by a Gaussian distribution similar to the first term of equation 2, shifted by the value of the experimentally determined parameter [11].

The dependences of the values of parameters A and B obtained from laboratory energy with exemplary sources are shown in Figures 1 and 2, respectively. The values for the two types of radiation detectors based on CdZnTe and CdTe are given. The parameters were determined by comparing the experimentally measured spectrum with the calculated model spectrum for various values of the studied parameters. The obtained dependences are in good agreement with the data presented in [12]. This is because the detectors are made from raw materials produced by eV PRODUCTS. The literature indicates that the value of the parameter *C*, which determines "cutoff" of the function F_t, is 0.7 for a large set of investigated detectors [12].

To represent Compton distribution $\mu(E, E_i)$, we used the statistical test method (Monte Carlo method), the most effective when considering radiation transfer in matter due to the statistical nature of this process. This is explained by the fact that elementary scattering events occur on a free electron, and therefore the properties of the crystal are not significant. In addition, scattering has a continuous spectrum of secondary particles, and more statistics are needed for its correct presentation. Therefore, it is optimal to use the Monte Carlo method, in which random motion of a particle is considered as a certain trajectory, and its state at each nodal point is played using random numbers from the corresponding distributions. It has been shown that modern implementation algorithms for this method make it possible to achieve modeling accuracy of up to 1-2% [6, 11].

The distribution $\mu(E, E_i)$ is the probability of scattering secondary electrons in the energy interval and is determined by the Klein-Nishina formula:

$$W(\alpha_1)d\alpha_1 = A(\alpha)f(\alpha,\alpha_1)d\alpha_1, \quad \frac{\alpha}{1+2\alpha} \le \alpha_1 \le \alpha, \qquad f(\alpha,\alpha_1) = \frac{\alpha_1}{\alpha} + \frac{\alpha}{\alpha_1} + \left(\frac{1}{\alpha} - \frac{1}{\alpha_1}\right)\left(2 + \frac{1}{\alpha} - \frac{1}{\alpha_1}\right), \tag{3}$$

where α, α_1 – energy before and after scattering in units of electron mass; $A(\alpha)$ – normalization constant.

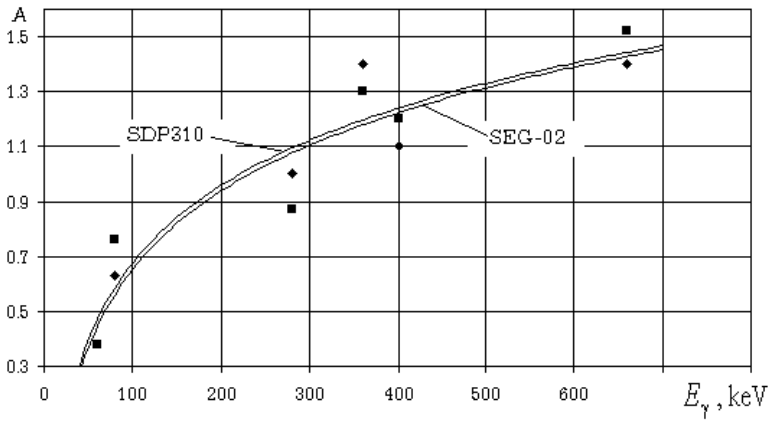


Figure 1 – The dependence of parameter *A*, which determines the amplitude of the function F_t, on the energy of detected radiation: 1 – prototype crystal with a quasispherical contact design; 2 – prototype crystal with planar contact design

In this case, maximum energy of a Compton electron is determined by the formula:

$$E_{k\max} = \frac{E}{1 + \frac{mc^2}{2 \cdot E}}. \tag{4}$$

For monoenergetic gamma radiation, the maximum energy E of the Compton electron is calculated by the formula (4), and then the Monte Carlo model is used to construct a model of the Compton distribution. When simulating the required portion of the instrument spectrum, the resulting distribution is multiplied by a correction factor, which is the detector constant and determines its characteristic as “compton / peak” ratio.

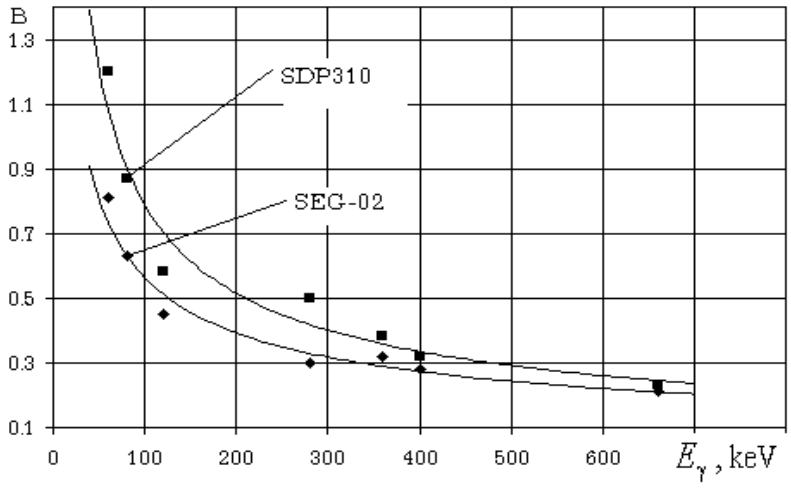


Figure 2 – The dependence of parameter *B*, which determines the decay of the function F_t, on the energy of detected radiation: 1 – prototype crystal with a quasispherical contact design; 2 – prototype crystal with planar contact design

Then differential energy spectrum $d\varphi(E)/dE$ for a large number of gamma rays in the decay scheme has the form:

$$d\varphi(E)/dE = \sum_{i=1}^{M}\left[n_i(E)+n_{esc}(E)+\mu(E,E_i)\right], \quad (5)$$

where *M* is the number of gamma lines in the decay scheme of the studied isotope.

The experimental spectrum $S_э(E)$ has a discrete character, therefore, the theoretical spectrum is converted into a discrete form with a given energy window ΔE:

$$\varphi(E) = (d\varphi(E)/dE)\Delta E\,. \quad (6)$$

A model of instrumental spectrum obtained by measuring the intrinsic radiation of a fuel assembly can be obtained using expression (5) based on simulation results of the instrumental spectra for each isotope present under the cladding of a fuel rod. In addition, in order to take into account influence of isotopes present in small quantities, a correction in the form of a continuous distribution was introduced during modeling. In order to ensure that the spectrum obtained on the basis of (5) corresponds to the instrumental spectrum when measuring gamma radiation of spent nuclear fuel, contribution of scattering in the fuel matrix and environment was additionally taken into account. The resulting distribution is normalized to determine the absolute values; therefore, reference data on differential cross sections for the interaction of gamma radiation with matter are used [10].

Based on the developed methodology and experimentally determined characteristics of spectrometer, instrumental spectrum were simulated under various measurement conditions with subsequent processing of obtained model spectra.

To verify the correct implementation, the spectrum of a ^{137}Cs point source with random noise was superimposed (Fig. 3). For comparison, Figure 4 shows the measured 137Cs spectrum from a set of gamma-ray spectra. A characteristic feature of model is a more pronounced peak in the region of maximum energy of Compton electrons.

In addition, a peak in region of 210 keV and peaks in the X-ray region should be noted in the experimentally obtained spectrum. The peak in the region of 210 keV is due to gamma rays, which were subjected to Compton scattering in one of the materials surrounding the detector. Gamma rays scattered by more than 110-120 °, will have almost the same energy values in the range from 200 to 250 keV. Consequently, the contribution of the monoenergetic source will be represented by many scattered gamma rays whose energy is close to this minimum value.

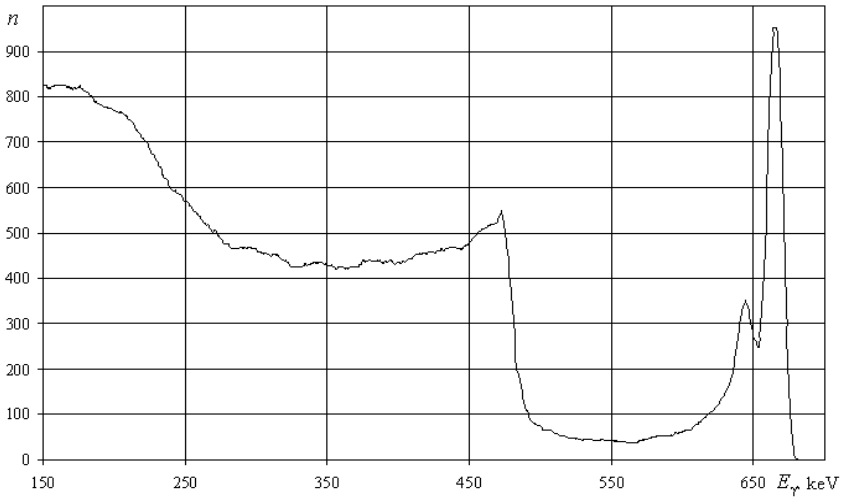


Figure 3 – Model of instrumental spectrum when measuring ^{137}Cs point source

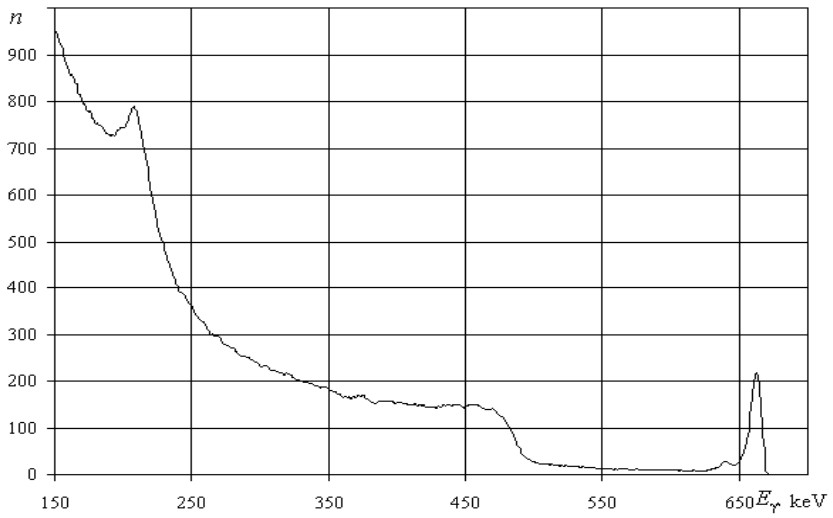


Figure 4 – Hardware spectrum for measuring ^{137}Cs point source

Conclusion. X-ray peaks are associated with the peculiarity of the organization of measurements – location of the source, detector and protection, and are caused by the characteristic radiation of lead from which the protection is made. Unfortunately, such peaks are rather difficult to model, but this is not necessary, since in real conditions a collimator is used and these peaks are absent.

The results of modeling the instrumental spectra during measurements of intrinsic gamma radiation of SNF are close to those obtained previously. This confirms the conclusion that the CdZnTe-based spectrometer made in this work satisfies the requirements for monitoring the state of SNF in real time, identifying fuel assemblies containing fuel elements with an unpressurized cladding, and determining the burnup of nuclear fuel using analysis of the activity of fission products.

LITERATURE:

1. Vavilov V.S. The effect of radiation on semiconductors / V.S. Vavilov, N.P. Kekelidze, L.S. Smirnov. - M .: Nauka, 1988 .-- 192 p.

2. Lienkov S.V. Physicotechnical fundamentals of radiation technology of semiconductors / S.V. Lenkov, V.A. Mokritsky, D.A. Peregudov, G.T. Tarielashvili. - Monograph. - Odessa: Astroprint, 2002 .-- 297 p.

3. Garkavenko A.C. Radiation modification of the physical properties of wide-gap semiconductors and the creation of high-power lasers on their basis / Lviv: ZUKZ, 2012. - 258 p.

4. Bansak O.V. Semiconductor detectors of a new generation for radiation monitoring and dosimetry of ionizing radiation / O.V. Bansak, O.V. Maslov, V.A. Mokritsky: Ed. V.A. Mokritsky, O.V. Maslova. - Monograph. - Odessa, 2013. - Publishing House "BMB". - 220 p.

5. Bouchet J.M. PWR primary flow masurements by correlation analysis of nitrogen-16 fluctuations / J.M. Bouchet, et al. – Progress in Nuclear Energy. – 1982. – Vol. 9.

6. Awadalla S.A. Characterization of detector-grade CdZnTe crystals grown by traveling heater method (THM) / S.A. Awadalla, J. Mackenzie, H. Chen, eds. // Journal of Crystal Growth. – Vol. 312, issue 4. – 2010. – P. 507-513/

7. Grybos P. Front-end Electronics for Multichannel Semiconductor Detector Systems; EuCARD Editorial Series on Accelerator Science and Technology, Vol.08 / Institute of Electronic Systems Warsaw University of Technology . – Warsaw: 2010. – 201 p.

8. Dumitrescu A. Comparison of a digital and an analogical gamma spectrometer at low count rates / A. Dumitrescu // U.P.B. Sci. Bull., Series A. – Vol. 73. – Iss. 4, 2011. – P. 127-138.

9. Maslov O. Passive Computer Gamma- Tomography of Nuclear Fuel / O. Maslov, V. Mokritsky, O. Banzak, // ANIMMA. Third International Conference on Advancements in Nuclear Instrumentation Measurement Methods and their Applications – Marseille, June 23-27, 2013. – Book of Abstracts – P. 51.

10. Maslov O.V. The Improved CdZnTe Dose Rate Probe / O.V. Maslov, M.V. Maksimov, L.L. Kalnev // 2008 IEEE Nuclear Science Symposium, Medical Imaging Conference and 16th Room Temperature Semiconductor Detector Workshop – Dresden: 19–25 Oct. 2008. – P. 12-87.

11. Masuruk K. Dopant incorporation during liquid phase epitaxy / K. Masuruk, T.Bryskewicz // J. Appl. Phys., 1981. – V. 52. – N3. – part 1. – P. 1347–1350.

12. Maslov O. Multiple energies passive computer tomography of nuclear fuel / O. Maslov // Proceedings of the International Ukrainian-Japanese Conference on Scientific and Industrial Cooperation – Odesa 24 – 25 October 2013. – P. 114-116.

д.т.н., проф. Мокрицький В.А., д.т.н., доц. Маслов О.В.,
д.т.н., доц. Банзак О.В., к.т.н., доц. Лещенко О.І.

МОДЕЛЮВАННЯ АПАРАТУРНИХ СПЕКТРІВ CdZnTe-ДЕТЕКТОРІВ

У даній статті розроблена методика моделювання апаратурних спектрів, одержуваних при вимірюванні власного гамма-випромінювання відпрацьованого ядерного палива з різною глибиною вигоряння і ступенем негерметичності оболонки твела. Модель спектру досліджуваної тепловиділяючої збірки дозволила визначити чутливість вимірювань і вибрати оптимальний алгоритм обробки спектрів. За рахунок цього скорочені витрати на розробку апаратної і програмної складових системи контролю стану ядерного палива.

Відмінність даної методики від відомих сотоит в тому, що не використовувалося моделювання розподілу напруженості електричного поля в об'ємі кристала датчика і не застосовувався метод Монте-Карло для моделювання електричного заряду, індукованого при первинному взаємодії гамма-випромінювання з кристалом.

Експериментальна перевірка методики на прикладі моделювання спектра випромінювання джерела ^{137}Cs підтвердила ефективність застосування створеного в даній роботі спектрометра на основі CdZnTe-детектора: відповідність вимогам контролю стану ядерного палива в режимі реального часу; ідентифікації ТВС, що містить ТВЕЛ з негерметичной оболонкою; визначення вигоряння палива на основі активності продуктів поділу.

Вперше запропоновано метод обробки великих пакетів спектрів власного гамма-випромінювання відпрацьованого ядерного палива. Відмінною особливістю методу є двоетапна обробка спектрів: на першому етапі визначаються параметри, що описують виміряні спектри і необхідні для роботи алгоритмів їх обробки методами чисельного диференціювання; на другому етапі за допомогою цих методів автоматизовано обробляються великі масиви спектрів в режимі реального часу.

Даний метод збільшує точність вимірювань і повноту картини розподілу вигоряння за обсягом ТВС. Це є технологічною основою створеного в даній роботі методу томографії.

Ключові слова: параметрична надійність, фотоприймальні пристрої, критерій працездатності, іонізуюче випромінювання, кристалічна структура

д.т.н., проф. Мокрицкий В.А., д.т.н., доц. Маслов О.В.,
д.т.н., доц. Банзак О.В., к.т.н., доц. Лещенко О.И.

МОДЕЛИРОВАНИЕ АППАРАТУРНЫХ СПЕКТРОВ CDZNTE-ДЕТЕКТОРОВ

В данной статье разработана методика моделирования аппаратурных спектров, получаемых при измерении собственного гамма-излучения отработавшего ядерного топлива с разной глубиной выгорания и степенью негерметичности оболочки твэла. Модель спектра исследуемой тепловыделяющей сборки позволила определить чувствительность измерений и выбрать оптимальный алгоритм обработки спектров. За счет этого сокращены затраты на разработку аппаратной и программной составляющих системы контроля состояния ядерного топлива.

Отличие данной методики от известных сотоит в том, что не использовалось моделирование распределения напряженности электрического поля в объеме кристалла датчика и не применялся метод Монте-Карло для моделирования электрического заряда, индуцированного при первичном взаимодействии гамма-излучения с кристаллом.

Экспериментальная проверка методики на примере моделирования спектра излучения источника ^{137}Cs подтвердила эффективность применения, созданного в данной работе спектрометра на основе CdZnTe-детектора: соответствие требованиям контроля состояния ядерного топлива в режиме реального времени; идентификации ТВС, содержащей твэл с негерметичной оболочкой; определения выгорания топлива на основе активности продуктов деления.

Впервые предложен метод обработки больших пакетов спектров собственного гамма-излучения отработавшего ядерного топлива. Отличительной особенностью метода является двухэтапная обработка спектров: на первом этапе определяются параметры, описывающие измеренные спектры и необходимые для работы алгоритмов их обработки методами чисельного дифференцирования; на втором этапе с помощью этих методов автоматизировано обрабатываются большие массивы спектров в режиме реального времени.

Данный метод увеличивает точность измерений и полноту картины распределения выгорания по объему ТВС. Это является технологической основой созданного в данной работе метода томографии.

Ключевые слова: параметрическая надежность, фотоприемные устройства, критерий работоспособности, ионизирующее излучение, кристаллическая структура.

UDC 681.3 PhD. **Tolok I.V.** (VIKNU)
PhD. **Lienkov Ye.S.** (CRI Armed Forces of Ukraine IWT)

ALGORITHMS FOR MODELING PROCESS SPENDING AND REPLENISHMENT OF RESOURCE GROUPING TECHNOLOGY

This article explores the basic initial steps for constructing an enlarged structural diagram of an algorithm for modeling the processes of spending and replenishing resource of a grouping military objects in normative planning mode.

The organizations responsible for operating the groupings have an important task of timely planning for repair of weapons and military equipment (WME) and military equipment and supplies to the grouping of new objects. Obviously, solution of such a problem is possible only on the basis of applying a mathematical model process of expenditure and replenishment of resource (PERR) of grouping objects, with which you can predict the composition and resource of the grouping, and taking into account the forecast obtained, find (calculate) optimal plans for replenishing its resource.

The article shows the results of studies various groups in terms of elucidating patterns of the occurrence of PERR in them. To do this, using the model, various grouping options can be generated with the specified characteristics, as well as calculating the optimal plans for replenishing resource for a specific group of military equipment (user groups), save these plans in a database, and then make refinement calculations taking into account current changes in grouping.

It is assumed that by the time this algorithm is launched, all the necessary data structures have already been created in random access memory of the personal computer, user has already selected an implementation option for the grouping for which simulation is performed. Also, the number of implementations of modeling process and coefficient specifying range of variation limit on the consumption of resource objects (in percent) are given. In each iteration, process of PERR objects the i-th type is simulated at a given forecast interval

Key words: complex objects of military equipment, process of expenditure and replenishment of resource, regime of normative planning.

Introduction and statement of problems. Complex objects of weapons and military equipment (WME) are used for their intended purpose, usually as part of groups (military units, formations, associations). Examples of such objects are radar stations, anti-aircraft missile systems, electronic warfare stations, and others. Groups are created temporarily or on an ongoing basis to solve certain problems in a certain territory. In order for the group to satisfy the requirements for its quantitative and qualitative composition established for it. Quantitative composition (hereinafter simply composition). Groupings are determined by the number of objects various types that are available in the group at a given time and are ready for immediate completion of tasks for their intended purpose. In this case, the number of types objects and the distribution of the number objects by types must correspond to specified grouping requirement. The qualitative composition of the group is determined by residual resource of the objects available in the group. The larger average residual resource of grouping objects, more qualitative is its composition, the greater will be the duration of group's existence in a state in which all tasks will be performed with required efficiency.

During operation of grouping, resource of individual objects is spent randomly, as a result of this, qualitative composition of group deteriorates over time (“safety margin” of group decreases). After exhaustion of resource by individual objects, their operation should be stopped, objects that have exhausted the resource should be repaired, restoring resource, or decommissioned (irrevocably removed from the group). To maintain required efficiency of functioning of the grouping, it is necessary, instead of decommissioned objects, to put in the grouping new objects of corresponding types.

Thus, for higher bodies (headquarters) responsible for operation of group, an important task arises of timely planning of repair military equipment and supplies to the group of new facilities. Obviously, solution of such a problem is possible only on the basis of applying a mathematical model process of expenditure and replenishment of resource (PERR) of grouping objects, with the help of which it would be possible to predict composition and resource of the grouping, and taking into account forecast obtained, find (calculate) optimal plans for replenishing its resource.

Therefore, an important problem is the modeling of processes for determining and replenishing the technical resource of grouping objects. To do this, it is necessary to solve two problems.

1. To explore various groups in terms of elucidating the patterns of the occurrence of PERR in them. To do this, using the model, various grouping options with specified characteristics can be generated.

2. Calculate the optimal plans for replenishing resource for a specific group of OME objects (user groupings), save these plans in database (DB), and then make refinement calculations taking into account current changes in the grouping.

Analysis of recent research. Recently, research in Ukraine aimed at improving the processes technical maintenance of military equipment, its restoration and modernization is being restored in Ukraine [1-8]. So, in [1, 4, 5], models process of research and replenishment of resource objects of complex radio engineering were investigated. In [2], new technologies for determining the reliability of objects were proposed. In [3], optimal system of scheduled repairs for individual objects was proposed. In [6], maintenance was offered "as-is" with an adaptive change in the frequency of control.

In [7–9], the authors have come close to studying the grouping of objects to optimize the number of repair bodies and evaluate effectiveness of maintenance military equipment. This is all the basis for development of an algorithm for modeling PERR of grouping objects.

The basic results of research

The integrated structural diagram of modeling algorithm. In figure 1 shows an enlarged structural diagram of the algorithm that explains structure of computation process that is implemented when modeling PERR grouping. In fact, this is an algorithm that is implemented by operator 8 ("Modeling") of the algorithm circuit shown in [1].

It is assumed that by time this algorithm is launched, all the necessary data structures have already been created in the PC's RAM, the user has already selected implementation of *GR* grouping for which simulation is performed. Also, the number implementations of modeling process $N_{\text{І}}$ and coefficient KV_{Lim} specifying range of variation limits on the expenditure of resource objects (in percent) are given. In each iteration, process of PERR objects of *i*-th type is simulated at a given forecast interval $T_{\text{п}}$. As a result of the simulation, functions $T_{\text{п}}$ of average values $\overline{R}_{\Sigma i}(t)$, $\overline{N}_{\Sigma i}(t)$, $\overline{N}_{\text{р}\Sigma i}(t)$, $\overline{N}_{\text{сп}\Sigma i}(t)$ and $\overline{N}_{\text{нС}\Sigma i}(t)$ ($\forall t \in T_{\text{п}}$) predicted on the interval are formed, which are displayed on PC screen in form of graphs. Corresponding averages are accumulated according to results of implementation of the real-time simulation of real-time simulation. The operation of the algorithm briefly consists in following.

Operator 1 sets the initial value of *iter* variable, which is used to count the number of completed simulation implementations.

Operator 2 creates a copy of List_O list, which contains information about the objects of GR grouping. Operator 3 increments value of iter variable by 1, thus forming the number of current iteration. Operator 4 restores the initial state of List_O data from the copy. Operator 5 generates random values of resource consumption limit by individual objects that are part of the grouping. This is done by executing the following statement for each object:

$\texttt{O.Lim} := \texttt{O.Lim0} \cdot (1 - KV_{\text{Lim}} / 100 / 2) + \texttt{R}$,

where $\texttt{O.Lim0}$ – is the initial value of the resource spending limit specified for object O (h / year);

– user-specified value of the coefficient of variation of the limit of spending the re-source of objects (in%);

R – is a random variable uniformly distributed in the interval .

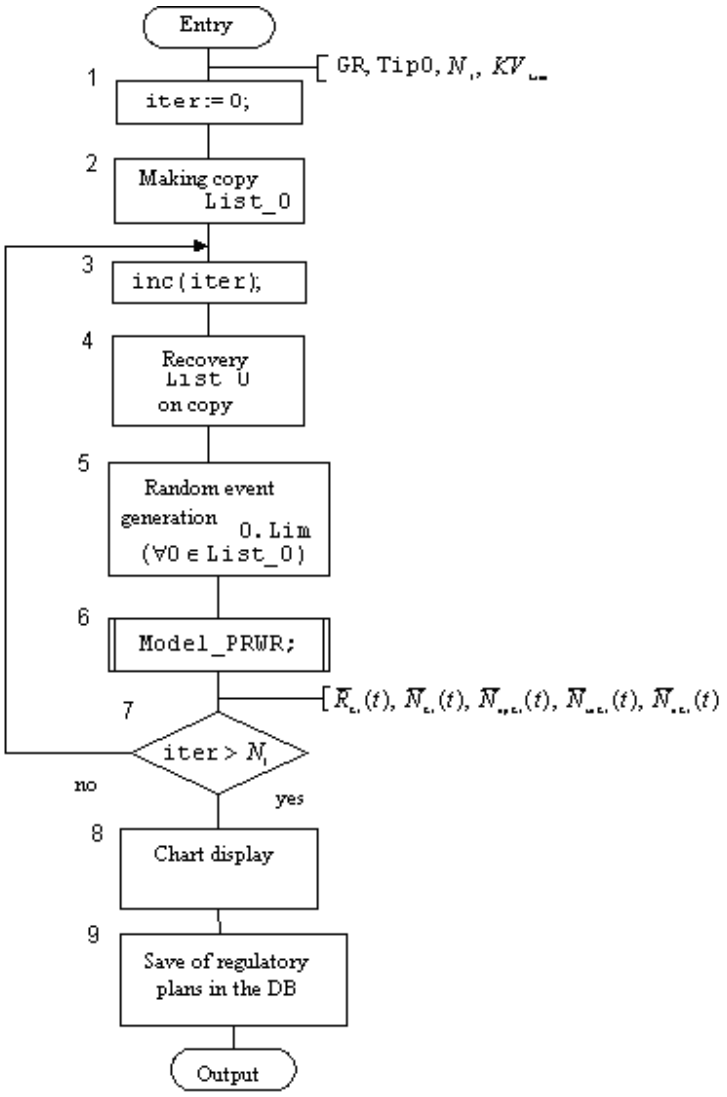


Figure 1 - An enlarged block diagram of modeling algorithm

Operator 6 (procedure Model_PERR) imitates ERR process with objects of GR grouping. Inside this procedure, information is accumulated necessary for constructing function schedules, and regulatory plans for repairing, decommissioning and delivering new objects to the group are also formed. An algorithm that implements this procedure is discussed in detail below.

Operator 7 checks the condition for a given number of iterations. If not all iterations have been completed, control is transferred to operator 3 and the simulation process continues. If all iterations are completed, the simulation process is interrupted, and operators 8 and 9 are executed. Operator 8 displays function graphs on PC screen, operator 9 saves the generated normative plans for repairs, write-offs, and deliveries of new objects to database. This completes work of the algorithm.

The modeling algorithms implemented by the Model_PERR procedure are slightly different, depending on program mode selected by the user. Let's consider these algorithms separately.

Regulatory planning mode. Consider structural diagram of the simulation model algorithm (SM) of PERR (procedure Model_PERR) in the standard planning mode without delivery of new objects. The block diagram of the algorithm in this mode is shown in Fig. 2.

The initial information for the algorithm is GR and TipO data structures created in the main memory at time the algorithm started to execute. The output of the algorithm are functions $\overline{R}_{\Sigma i}(t)$, $\overline{N}_{\Sigma i}(t)$, $\overline{N}_{\text{р}\Sigma i}(t)$ and $\overline{N}_{\text{сп}\Sigma i}(t)$, as well as the standard repair $\Pi^{\text{н}}_{\text{р}i}$ and decommissioning $\Pi^{\text{н}}_{\text{с}i}$ plans stored in the arrays of simulation results.

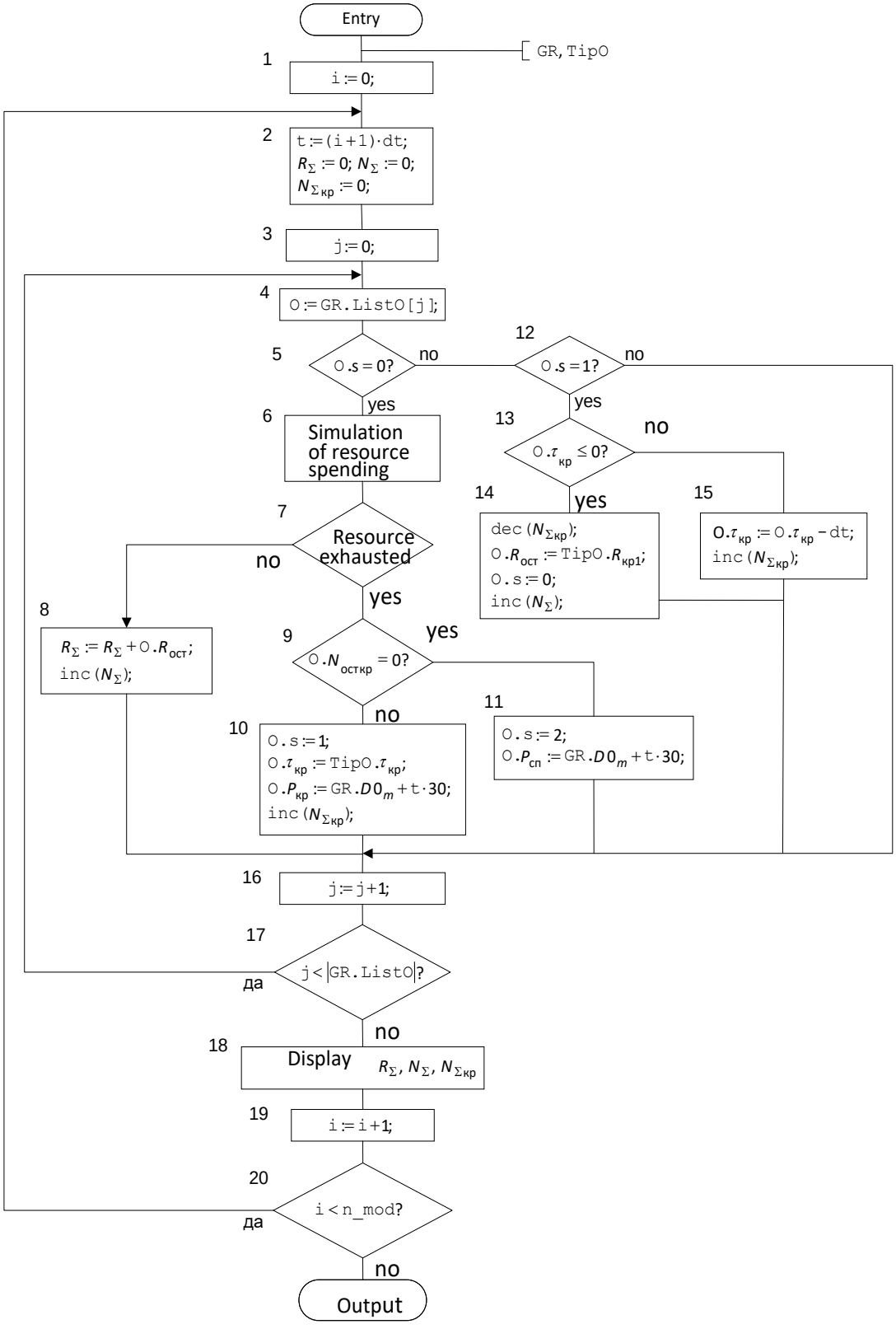


Figure 2 - Block diagram of the algorithm for modeling PERR in regulatory planning mode

Simulation parameters (in addition to the selected Reg_p forecasting mode) are:

- type of objects for which calculations are performed (data on the type are available through TipO pointer);
- duration of operation period of the grouping DT_MOD;
- date corresponding to the beginning of specified period of operation D0_MOD;

- interval discreteness modeling RWR DT.

These parameters are entered by the user from PC screen immediately before starting simulation.

The idea of the algorithm is very simple - it consists of two cycles: the external (by i), in which the operation time intervals of group are sorted, and the internal (by j), in which the group objects of a given type are sorted.

The external cycle is implemented by operators 1, 19, and 20. Operator 2 generates the current model time t and initializes variables R_{Σ}, N_{Σ} and $N_{\Sigma кр}$ in which total resource, total number of workable objects in the group, and total number of objects that are currently under repair will be accumulated.

The inner loop (operators 3, 16, and 17) is re-executed for each value of the model time t. In this cycle, all elements of the GR.List_O list are enumerated - a list of pointers to objects that are part of grouping. Operator 4 selects a pointer to the j-th object from this list.

Operator 5 checks the current state of object $O.s$. If $O.s = 0$, then the object is currently in a healthy state and performs the task as part of grouping. Operator 6 simulates consumption of an object's resource over a period of time $dt = [t - dt, t]$ by executing the following instructions:

$O.R_{ост} := O.R_{ост} - dt \cdot O.Lim0/12;$

$O.T_{ост} := O.T_{ост} - dt,$

где $O.R_{ост}$ и $O.T_{ост}$ –

where $O.R_{ост}$ and $O.T_{ост}$ – value of the residual resource and residual life of object at time t;

$O.Lim0$ – annual limit of the resource consumption of the object;

dt – is the value of the discrete interval (dt = DT).

Operator 7 checks condition of exhaustion resource of object at time t:

$(O.R_{ост} < 0) \vee (O.T_{ост} < 0)$.

If this condition is not met, then operator 8 is executed, in which the current total resource R_{Σ} and number of objects in grouping are calculated N_{Σ}.

If the resource of the object is not exhausted, operators 9-11 are executed. The operator 9 checks whether the set number of scheduled repairs has been completed. If "no" (remaining number of repairs $O.N_{ост кр} > 0$), then operator 10 is executed, which simulates the transfer of an object to a repair state. In this case, following actions are performed:

$O.s := 1;$ – sets a new value for the state variable of object;

$O.\tau_{кр} := TipO.\tau_{кр};$ – value of duration stay object in repair;

$O.P_{кр} := GR.D0_{m} + t \cdot 30;$ – planned (normative) time of sending the object for repair is formed:

$inc(N_{\Sigma кр});$ – current number of objects under repair is calculated.

If all the set (normative) number of scheduled repairs the facility O ($O.N_{ост кр} = 0$) is completed, then operator 11 is executed, which imitates conversion of the facility to a decommissioned state. In this case, following actions are performed:

$O.s := 2;$ – value of the state variable is set to the state "object decommissioned";

$O.P_{сп} := GR.D0_{m} + t \cdot 30;$ – value of planned time to write off the object is formed.

If during execution of operator 12 it is discovered that the object is in a repair state ($O.s = 1$), then operators 13-15 are executed that simulate the object being in repair. The operator 13 checks condition for completion of the repair. If the repair has not yet been completed ($O.\tau_{кр} > 0$), then operator 15 is executed, simulating the continuation of the repair:

$O.\tau_{кр} := O.\tau_{кр} - dt;$ – residence time of the object in the repair is reduced by dt;

inc ($N_{\Sigma кр}$); – current total number of objects under repair is calculated.

If the repair is completed ($O.\tau_{кр} \le 0$), then following actions are performed:

dec ($N_{ост\ кр}$); – unit decreases the residual number of scheduled repairs of the facility O;

$O.R_{ост} := TipO.R_{кр1}$; – simulated replenishment resource of the object as a result of repairs;

$O.s := 0$; – simulates the restoration of operational state of the object;

inc (N_{Σ}); – total number of workable objects in the group is calculated.

Next, operator 16 counts the number of objects j for which simulated actions were taken to expend and replenish the resource in current interval dt. If these actions ($j < |GR.ListO|$) have not yet been performed for all objects, then operator 17 transfers control to operator 2 and then execution of operators 2-17 is repeated as described above. The cyclic execution of operators 2-17 ends after condition is met $j = |GR.ListO|$. In variables R_{Σ}, N_{Σ} and $N_{\Sigma кр}$, values corresponding to the grouping state at the current time t will be generated.

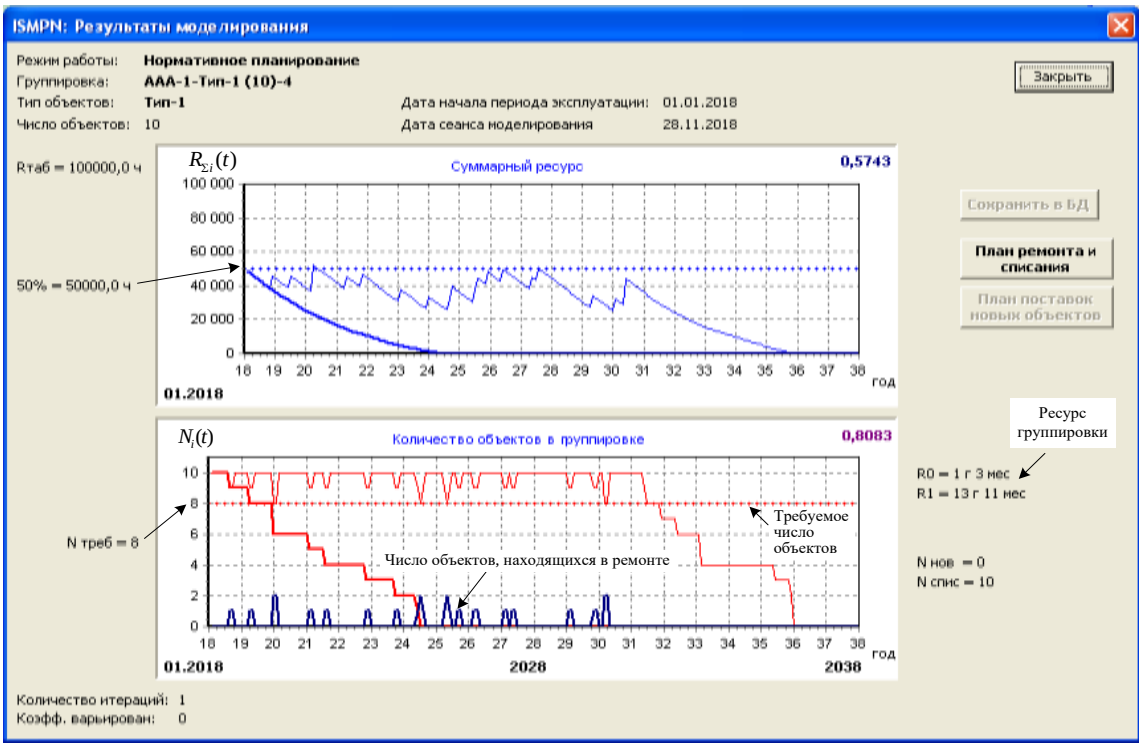
The operator 18 displays obtained values on the PC screen R_{Σ}, N_{Σ} and $N_{\Sigma кр}$ in the form of points on the function graphs, and. Next, operator 19 provides a transition to next time section t (forms the number i of the next point on the time axis). Operator 20 checks the condition for completing the graphing. If all points of graphs ($i = n\_max$) are formed and displayed, then operation of the algorithm ends here.

As an example in fig.3 shows graphs of functions $\overline{R}_{\Sigma i}(t)$, $\overline{N}_{\Sigma i}(t)$ and $\overline{N}_{кр\,\Sigma i}(t)$ obtained as a result of execution of considered algorithm. The graphs are given for the case when the group contains 10 objects of type **Type-1** (**Type-1** is the name of type objects in TipO structure). The maximum number of repairs after which the object must be written off is set to 2.

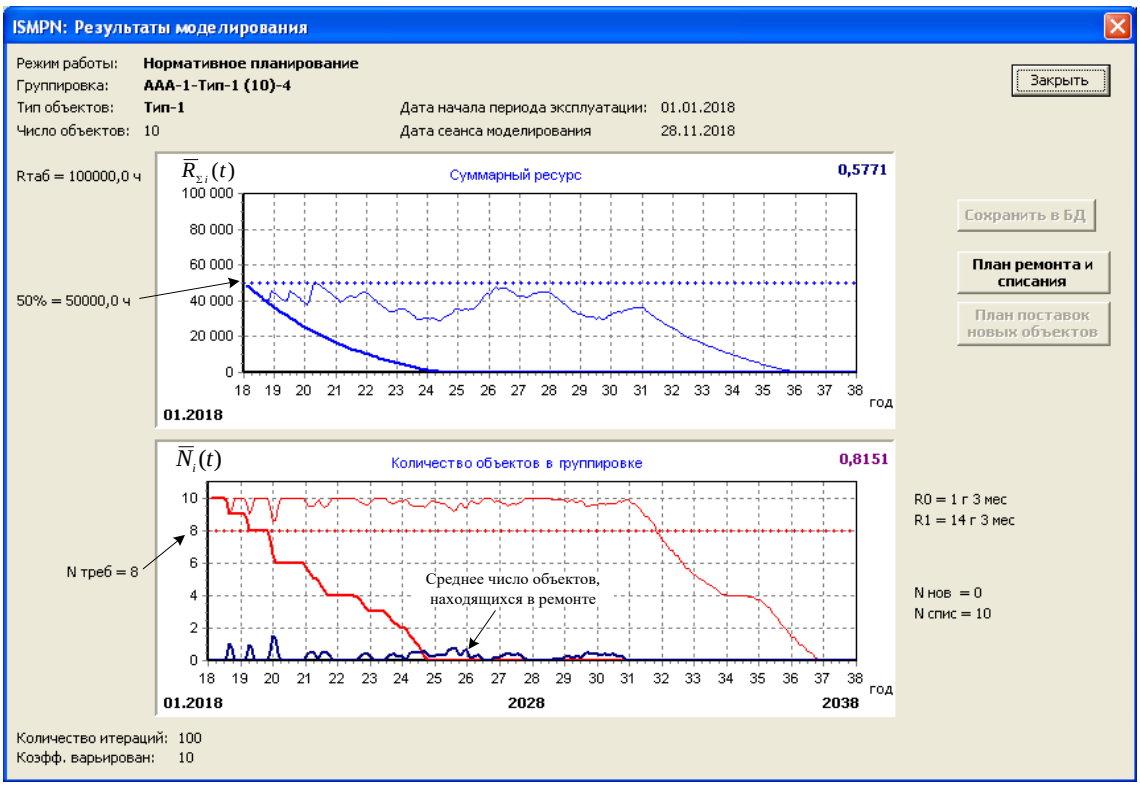
In the upper graph in fig.3 shows function of total resource $\overline{R}_{\Sigma i}(t)$ (for objects of type **Type-1**). The bold line shows the initial part of function, which displays the forecast for the case if no planned repairs (PR) are carried out. With a thinner line, this same function represents the forecast, provided that PR are carried out within the standard time frames established for this type of object. The lower graph (in red) shows the graph of the function $\overline{N}_{\Sigma i}(t)$. Also, the bold line shows the initial part of the graph for the case if PR had not been carried out, a thinner red line shows the continuation of same function, provided that all PR are carried out within the established regulatory periods. The lower graph in the same coordinates shows a graph of the function, which displays the number objects that are in a state of repair at each moment of time (currently missing in the group).

In fig. 3a shows results for the case of performing 1 implementation of modeling process, in fig. 3b - for 100 implementations. Comparing the graphs in these figures, we can see that with a large number of implementations, average time for sending to the 2-nd repair and the time for writing off objects become more “blurred”, stretched over time. This is consistent with the physical meaning of average indicators (average number of objects under repair $\overline{N}_{кр\,\Sigma i}(t)$ and the average number of objects remaining in the group $\overline{N}_{\Sigma i}(t)$).

The graphs (in the upper right corner) show the values of quality indicators Q_{Ri} and Q_{Ni} (Q_{Ri} - in upper graph, Q_{Ni} - in lower).



a) one implementation ($N_I = 1, KV_{\text{Lim}} = 0$)



b) 100 implementations ($N_I = 100, KV_{\text{Lim}} = 10\%$)

Figure 3 - Example of simulation results (**Normative planning** mode)

On the form of simulation results (to the right of graph $\overline{N}_{\Sigma i}(t)$), value of the grouping resource $R^1_{\text{групп}i}$ (duration of grouping with the required composition) is displayed. In this example, the required number of objects $N_i^{\text{тр}} = 8$. Under this condition, the group's resource is 13 years 11 months. (one

implementation) and 14 years 3 months. (according to the predicted average composition). The discrepancy between corresponding values at 1 and at 100 implementations is quite understandable, since the predicted functions are different.

The initial grouping resource $R^{0}_{\text{груп}i}$ is also displayed, defined as the grouping resource, provided that no repairs are made to restore the resource of the objects. The initial grouping resource in this example is 1 year 3 months. (with 1 and with 100 implementations).

The graphs corresponding to the initial resource are shown in bold lines in figures.

Along with the functions $\overline{R}_{\Sigma i}(t)$, $\overline{N}_{\Sigma i}(t)$ and $\overline{N}_{\text{кр}\,\Sigma i}(t)$ as a result of the simulation, a plan of repair and decommissioning of grouping objects is also formed, corresponding to the specified intensities (limit) of the resource consumption of objects `O.Lim0` and the established standards for replenishing the resource `TipO`$.R_{\text{кр1}}$, `TipO`$.T_{\text{кр1}}$ and `TipO`$.N_{\text{кр}}$.

The plan of repair and decommissioning of objects is displayed in a separate form when you click the **Plan of repair and decommissioning** button (fig. 3). The form in which this plan is displayed is shown in fig 4.

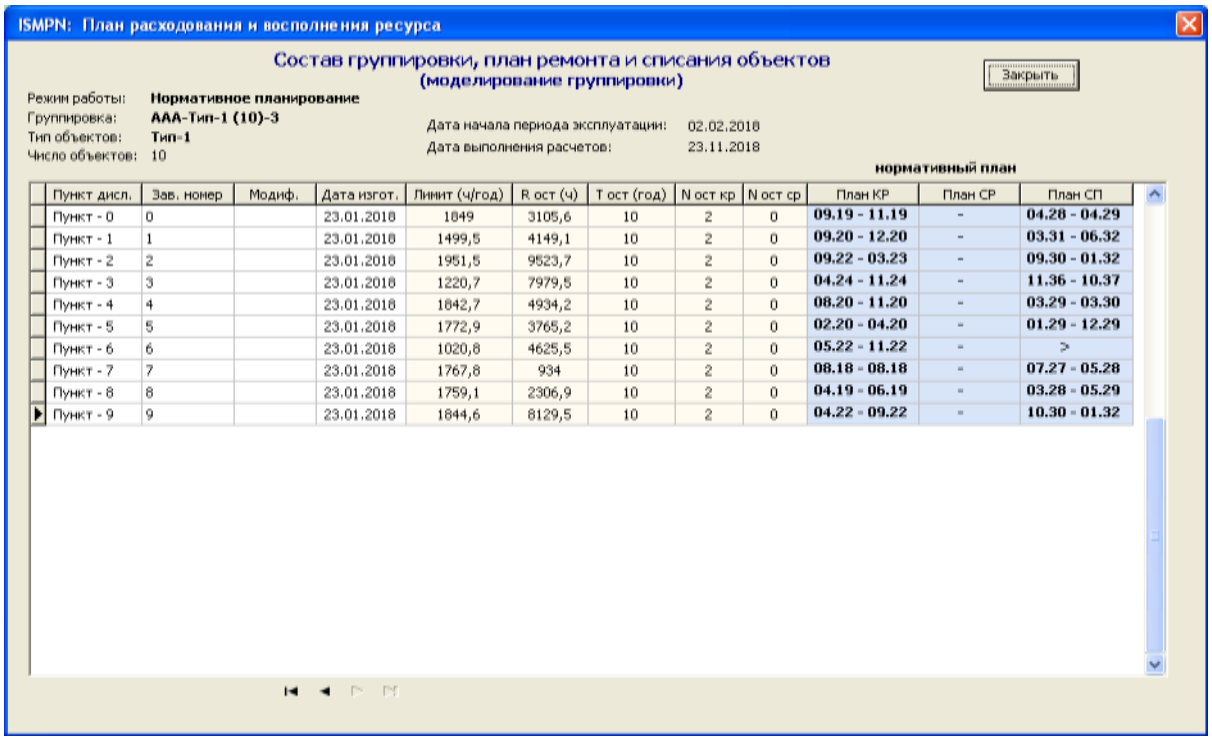


Figure 4 - PC screen view when displaying form of the repair plan and decommissioning of grouping objects (**Regulatory planning** mode)

Planned dates for repair and decommissioning of objects are displayed in the three right columns of the table. The minimum and maximum values of the planned repair and write-off period, obtained as a result of forecast calculations, are displayed.

The table also displays additional information about the characteristics of facilities: location, serial number, production date, etc. In the case of a virtual grouping, this information is automatically generated when it is created. In the case of user grouping, all this information is set by the user.

Conclusions. This article explores the basic initial steps for constructing an enlarged structural diagram of an algorithm for modeling the processes of spending and replenishing the resource of a grouping of military objects in normative planning mode.

In the future, a regulatory planning regime will be developed taking into account the supply of new objects to the grouping.

LITERATURE:

1. Boryak, K. F. Models of processes expenditures and replenishment resource of complex restored objects and systems of electronic equipment: monograph / K. F. Boryak, V. A. Braun, S. V. Lienkov, A. V. Selyukov, V. M. Tsitsarev. - M.: Knowledge of Ukraine, 2008. - 267 p.

2. Strelnikov, V. P. A new technology for studying reliability of machines and equipment / V. P. Strelnikov // Mathematical machines and systems. - M., 2007. - No. 3, 4. - P. 227-238.

3. Lienkov, S. V. Determination of the optimal system of scheduled repairs for high-risk PET objects / S. V. Lienkov, K. F. Boryak, V. N. Tsytsarev, A. G. Zinchik // Sb. scientific tr East ukrainian national university. V. Dahl. - Lugansk, 2009. - No. 5 (135). - P. 26-32.

4. Lienkov, S. V. Estimates of reliability complex technical objects taking into account their hierarchical structural structure / S. V. Lienkov, V. N. Tsytsarev, Yu. A. Gunchenko, K. F. Boryak, R. Yu. Koltsov / / Collection of Odessa state academy of technical regulation and quality. - Odessa, 2012. - No. 1. - P. 65-70.

5. Lienkov, S.V. Simulation statistical model of adaptive maintenance of complex technical objects / S.V. Lienkov, V.N. Tsytsarev, G.V. Banzak // Collection of Central scientific research institute of arms and military equipment. - M., 2011. - No. 19. - P. 145-154.

6. Bansak, G.V. Methodology for determining optimal parameters of maintenance strategy "according to state" with an adaptive configuration of frequency monitoring the facility / G.V. Bansak, A. V. Selyukov, V. N. Tsytsarev // Bulletin of state university of information and communication technology. - M., 2011. - T. 9, No. 4. - P. 342-349.

7. Brown, V. A. Determination of optimal number repair bodies in the grouping of electronic equipment / A. Brown, K. F. Boryak, S. V. Lienkov, S. A. Pashkov, V. N. Tsytsarev // Collection of scientific proceedings of Military institute of Taras Shevchenko national university of Kyiv. - K., 2013. - No. 44. - P. 23-26.

8. S. Lienkov, G. Zhyrov, D. Zaytsev, I. Tolok, E. Lienkov, T. Bondarenko, Y. Gunchenko, V. Zagrebnyuk, O. Antonenko / Features of modeling failures of Recoverable complex technical objects with a hierarchical constructive structure / East European journal of advanced technology. - Kharkov, 2017.-№4 / 4 (88) - P. 34-42.

9. Lienkov S.V., Tolok I.V., Lienkov E.S. Prognostication of composition and resource of groupment of objects of technigue. Collection of scientific proceedings of Military institute of Taras Shevchenko national university of Kyiv. K.: 2019. - P. 54-65.

к.пед.н., доц. Толок І.В., к.т.н. Лєнков Є.С.

АЛГОРИТМИ МОДЕЛЮВАННЯ ПРОЦЕСУ ВИТРАТ І ЗАПОВНЕННЯ РЕСУРСНОЇ ГРУПОВОЇ ТЕХНОЛОГІЇ

В даній статті досліджено основні початкові дії з побудови укрупненої структурної схеми алгоритму моделювання процесів витрачання та поповнення ресурсу угруповання військових об'єктів в режимі нормативного планування.

В організаціях, відповідальних за експлуатацію угруповань, виникає важливе завдання своєчасного планування ремонту об'єктів озброєння і військової техніки (ОВТ) і поставок в угруповання нових об'єктів. Очевидно, що рішення такого завдання можливе лише на основі застосування математичної моделі процесу витрачання та поповнення ресурсу (ПВВР) об'єктів угруповання, за допомогою якої можна прогнозувати склад і ресурс угруповання, і з урахуванням отриманого прогнозу знаходити (розраховувати) оптимальні плани заповнення її ресурсу.

У статті показані результати досліджень різних угруповань з точки зору з'ясування закономірностей протікання в них ПВВР. Для цього за допомогою моделі можуть генеруватися різні варіанти угруповань із заданими характеристиками, а також здійснюються розрахунки оптимальних планів поповнення ресурсу для конкретного угруповання об'єктів військової техніки (угруповання користувача), зберігати ці плани в базі даних, а потім проводити уточнюючі розрахунки з урахуванням поточних змін в угрупованні.

Передбачається, що до моменту запуску цього алгоритму в оперативній пам'яті персонального комп'ютера вже створено всі необхідні структури даних, користувачем вже обраний варіант реалізації угруповання, для якої проводиться моделювання. Також задано число реалізацій процесу моделювання і коефіцієнт, що задає діапазон варіювання ліміту витрачання ресурсу об'єктів (у відсотках). У кожній ітерації імітується процес ПВВР об'єктів і-го типу на заданому інтервалі прогнозування

Ключові слова: складні об'єкти військової техніки, процес витрачання та поповнення ресурсу, режим нормативного планування.

к.пед.н., доц. Толок И.В., к.т.н. Ленков Е.С.

АЛГОРИТМЫ МОДЕЛИРОВАНИЯ ПРОЦЕССА РАСХОДА И ЗАПОЛНЕНИЯ РЕСУРСНОЙ ГРУППОВОЙ ТЕХНОЛОГИИ

В данной статье исследованы основные начальные действия по построению укрупненной структурной схемы алгоритма моделирования процессов расходования и восполнения ресурса группировки военных объектов в режиме нормативного планирования.

В организациях, ответственных за эксплуатацию группировок, возникает важная задача своевременного планирования ремонта объектов вооружения и военной техники (ВВТ) и поставок в группировку новых объектов. Очевидно, что решение такой задачи возможно только на основе применения математической модели процесса расходования и восполнения ресурса (ПРВР) объектов группировки, с помощью которой можно прогнозировать состав и ресурс группировки, и с учетом полученного прогноза находить (рассчитывать) оптимальные планы восполнения ее ресурса.

В статье показаны результаты исследований различных группировок с точки зрения выяснения закономерностей протекания в них ПРВР. Для этого с помощью модели могут генерироваться различные варианты группировок с заданными характеристиками, а также производятся расчеты оптимальных планов восполнения ресурса для конкретной группировки объектов военной техники (группировки пользователя), сохранять эти планы в базе данных, а затем производить уточняющие расчеты с учетом текущих изменений в группировке.

Предполагается, что к моменту запуска этого алгоритма в оперативной памяти персонального компьютера уже созданы все необходимые структуры данных, пользователем уже выбран вариант реализации группировки, для которой производится моделирование. Также задано число реализаций процесса моделирования и коэффициент, задающий диапазон варьирования лимита расходования ресурса объектов (в процентах). В каждой итерации имитируется процесс ПРВР объектов i-го типа на заданном интервале прогнозирования

Ключевые слова: сложные объекты военной техники, процесс расходования и восполнения ресурса, режим нормативного планирования.

УДК 004.413.4

д.т.н., проф. **Даник Ю.Г**. (НУОУ)
Вдовенко С.Г. (НУОУ)

ЛАНЦЮГОВІ ЕФЕКТИ В КІБЕРДІЯХ

У статті представлені результати досліджень особливостей гібридної війни, яка відбувається в Україні та інших державах в кіберпросторі. Встановлені роль і місце ланцюгових ефектів та асиметричних деструктивних дій у сфері інформаційної та кібербезпеки. У зв'язку з тим, що на цей час енергетика є базовою галуззю національної економіки та національної безпеки будь-якої держави, особливості комплексних деструктивних кібер-, інформаційних та когнітивних дій та впливів в кіберпросторі та через кіберпростір розглянуті на прикладі енергетичної сфери з урахуванням загроз, ризиків та особливостей кібервпливів на системи і об'єкти критичної інфраструктури паливо-енергетичного комплексу. Актуальність забезпечення енергобезпеки держав світу зростає, про що свідчить перегляд енергетичних стратегій розвитку Євросоюзу, США, та інших країн. За поглядами ряду вітчизняних та іноземних фахівців, енергетика з галузі економіки перетворилася на інструмент геополітики. Від її ефективного, надійного й сталого функціонування значною мірою залежать рівень національної безпеки держави в цілому, темпи структурних перетворень в економіці, забезпечення потреб населення, суспільного виробництва та оборони. Застосування на об'єктах критичної інфраструктури держави сучасних комп'ютерних, інформаційно-телекомунікаційних та кібертехнологій вимагає впровадження та здійснення заходів із кібербезпеки, протидії кібертероризму та забезпечення кібероборони. Визначені найбільш важливі аспекти цих впливів, запропоновані підходи щодо розробки обґрунтованих організаційних та технічних заходів щодо забезпечення кібербезпеки суспільства і держави в сучасних умовах.

Ключові слова: кібербезпека, кібероборона, комплексний інформаційно-кібернетичний вплив, об'єкти енергетики, розподілено-зосереджений кібервплив, кібервплив з ланцюговим ефектом

Вступ та постановка проблеми. Розвиток інформаційних та кібертехнологій та глобальна інформатизація призвели до того, що інформаційна та кіберсфери стали об'єктом різноманітних деструктивних впливів на усі сфери діяльності суспільства через кіберпростір, який доповнив існуючи: сухопутний, морський, повітряний, космічний, та став сферою конфліктів і можливих бойових дій [1,2]. При цьому відбувається зміна традиційних форм і способів ведення протиборства. Більше того, майбутня війна може бути спровокована в кіберпросторі. Сучасне суспільство практично повністю залежить від стану безпеки інформаційної інфраструктури. Не лише урядові структури держав, але й злочинні та терористичні організації отримали можливість використання глобальної мережі для досягнення своїх цілей. Через це забезпечення безпеки кібер- та інформаційної інфраструктури об'єктів управління є надважливою умовою забезпечення обороноздатності держави, її економічного та соціального розвитку.

Виходячи з цього, необхідність побудови ефективної кібероборони слід розглядати через призму ризиків та загроз, що притаманні світові та насамперед для України у першій чверті XXI століття. Гібридна війна, яка йде на території України, фактично охоплює все більше учасників у всьому світі. Це конфлікт, в якому стираються відмінності між безпосередньо війною в її класичному розумінні, і політикою та економікою, між військовими й іншими її учасниками та мирним населенням. **Гібридна війна** є високотехнологічним конфліктом, продовженням політики держав (коаліцій, політичних угруповань, транснаціональних корпорацій тощо) з метою нав'язування опонентам своєї волі за допомогою комплексних адаптивних і асиметричних синхронізованих впливів на них у різних просторах та сферах з поєднанням конвенційної і неконвенційної складових, забезпеченням багатовимірності, мультиплікативності та синергетичності результатів і високого рівня невизначеності для опонентів щодо кінцевих цілей і шляхів їх досягнення. Гібридна війна не оголошується і тому не може бути завершена в класичному розумінні завершення воєн і воєнних конфліктів. Це перманентна війна змінної

інтенсивності. Деструктивні впливи в ній супроводжуються, як правило, ланцюговими ефектами і синергетичними наслідками. У гібридних війнах в тій чи іншій мірі свідомо чи несвідомо задіяне не тільки все населення країни, яка стала об'єктом агресії, а й міжнародне співтовариство. У гібридних конфліктах військові дії поєднуються з іншими, головним чином економічними, політичними, дипломатичними, інформаційними, психологічними, кібернетичними, когнітивними й іншими діями, які комплексно призводять до системної дестабілізації в усіх сферах життя і діяльності держави, яка є об'єктом агресії.

Кібервійна (війна у кіберпросторі) – складне суспільно-політичне явище, що відбивається в протиборстві непримиренних сторін в кіберпросторі з використанням кіберзброї, засобів кіберрозвідки, захисту або впливу для завдання матеріальних втрат (збитків) супротивнику і мінімізації особистих втрат (збитків) в економічній, військовій, політичній та ідеологічних сферах. На відміну від інших деструктивних впливів, або війни, воєнних чи бойових дій та конфліктів, кібервійна не оголошується, а якщо починається – то не закінчується. Вона може бути закінчена лише у випадку зникнення (знищення) кіберпростору.

Кіберзброя – сукупність технічних, програмних та інших засобів, призначених для здійснення деструктивних впливів на визначені елементи кіберпростору противника з метою виведення їх з ладу, або - на елементи управління через кіберпростір з метою порушення процесів управління [3]. З асоби кібервпливу це перші в історії людства засоби боротьби, які реально існують і застосовуються, але без повного розуміння і контролю [3]. В класичному розумінні кіберзброю під контроль та на облік за номерами та комплектністю взяти не можливо.

Кібервплив – сукупність реалізованих підрозділами кібероборони за єдиним замислом та під єдиним керівництвом одночасних або послідовних взаємопов’язаних за метою і завданнями кібератак та/або кіберударів, спрямованих на визначені елементи кіберпростору противника з метою порушення їх функціонування (стану), або - на елементи управління через кіберпростір з метою порушення процесів управління [4]. Його складові: програмно-комп’ютерний вплив; фізичний вплив на органи і системи управління; радіоелектронне подавлення (ураження); інформаційно-психологічний вплив тощо. Кібератаки та кіберудари – розосереджені в кіберпросторі та часі, та зосереджені на досягненні кінцевої мети

В січні 2018 року в Сенаті США здійснено доповідь [5], в якій відзначено, що з 2014 року Росія невпинне й різноманітно використовує кіберпростір України в якості театру кібердій та полігону для випробовування російської кіберзброї, а кібератаки, як головний інструмент гібридної війни в російській операції в Україні направлені на всі сектори суспільства та економіки, зокрема такі як медіа, фінанси, транспорт, політика, енергетика і військова справа. Принаймні у двох випадках, у грудні 2015 року та грудні 2016 року, російські кібератаки були спрямовані на українську систему розподілу електроенергії, знеструмлюючи на тривалий час об’єкти економіки, інфраструктури та оселі. Після нападу на українську енергетичну мережу, американські чиновники Департаменту енергетики, Департаменту внутрішньої безпеки, ФБР і Корпорації Північноамериканської електричної надійності активізували свою діяльність, визнавши необхідність використання такої ситуації для розуміння тактики й практики дій російського уряду, прогнозування типів майбутніх кіберударів та відпрацювання ефективних заходів захисту від них, з одночасним наданням допомоги Україні в побудові оборонних сил. Співпраця з Україною щодо протидії цим загрозам вважається також критично важливим елементом створення кібероборони Сполучених Штатів [5].

Аналіз останніх досліджень. Концептуальні проблемні питання щодо загроз національній безпеці, зокрема у сфері інформаційної безпеки, соціальні аспекти кіберконфліктів, окремі організаційно-правові засади протидії кіберзлочинності та боротьби з кібертероризмом, дефініційні, правові та технічні аспекти проблем захисту військової інфраструктури від деструктивних, в тому числі кібервпливів досліджували О.А.Баранов, В.Л.Бурячок, Ю.І.Грицюк, Р.В.Грищук, Ю.Г.Даник, Д.В.Дубов, Р.В.Лук'янчук, В.В.Петров, В.П.Шеломенцев, М.Ю.Яцишин та інші [4, 6-23]. Проблеми кібероборони, з точки зору воєнно-політичного та воєнно-стратегічного аналізу розглядаються здебільш іноземними фахівцями, публікуються в офіційних виданнях самітів НАТО, але не мають юридичної сили альянсу та є лише поглядами фахівців [24, 25].

Питання виявлення та протидії комплексним інформаційно-кібернетичним впливам з ланцюговим ефектом на всі сфери діяльності держави та суспільства національними та іноземними фахівцями не розглядалися. Недостатньо також досліджені проблеми, пов'язані із кіберзагрозами енергетичній сфері, що безпосередньо впливає на стан національної безпеки України. Таким чином, на сьогодні існує об'єктивна необхідність дослідження та аналізу питань теорії та практики забезпечення кібербезпеки людини, громадянина, суспільства і держави в умовах кібервпливів з ланцюговим ефектом, зокрема розглядаючи кіберзагрози в енергетичній сфері. **Під ланцюговим ефектом кібервпливу** слід розуміти ефект виникнення, в результаті його здійснення на певний об'єкт впливу, великої кількості (ланцюга) негативних наслідків на інші об'єкти, взаємопов'язані з ним, в тому числі в інших взаємопов'язаних сферах, які у свою чергу породжують свої вторинні хвилі деструктивних ефектів, що призводять до ще більш системно руйнівних наслідків такого впливу.

Викладення основних результатів. Законами та нормативно-правовими актами [26-28] визначено, що найбільш актуальними для України у середньостроковій перспективі загрозами визнані: агресивні дії Росії, розвідувально-підривна і диверсійна діяльність Російської Федерації та інших держав та наголошено на уразливості об'єктів критичної інфраструктури та їх систем управління, а саме: урядових структур; установ сектору безпеки і оборони; науково-дослідного сектору; кредитно-фінансової і банківської системи, сфер соціального захисту, цивільної оборони, енергетики, хімічної та харчової промисловості, транспорту, комунального господарства, водопостачання, телекомунікацій, сільського господарства, закладів охорони здоров'я, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв.

Глибоке проникнення енергетики в усі галузі економіки та в соціальну сферу визначає її особливу роль у забезпеченні безпеки розвитку сучасного суспільства. Енергетична безпека характеризує міру виконання енергетикою її функцій перед суспільством, державою як у звичайних, так і в критичних умовах, зокрема в умовах надзвичайного чи воєнного стану, особливий період тощо.

Підприємства та установи енергетичної сфери відіграють провідну роль в розвитку держави. Основним споживачем електроенергії залишається промисловість, хоча її питома вага у загальному споживанні електроенергії в усьому світі дещо зменшується. Електрична енергія у промисловості застосовується для приведення в дію різних механізмів і безпосередньо в технологічних процесах. Зараз коефіцієнт електрифікації силового приводу у промисловості становить 80%. При цьому близько 1/3 електроенергії витрачається безпосередньо на технологічні потреби. Об'єкти енергетичної сфери є стратегічно важливими об'єктами і повинні функціонувати безперервно та якісно. На території України в кожній області присутні об'єкти енергетики, які відносяться до критичної інфраструктури, і на кожному з них є так звані «критичні точки», елементи порушення нормального функціонування яких призводить до порушення їх функціональної придатності, а у ряді випадків викликає ланцюгові деструктивні ефекти. Всі вони пов'язані певною ієрархією, системою управління та системою захисту. Основу електроенергетики становить об'єднана енергетична система України, яка централізовано забезпечує електроенергією внутрішніх споживачів, а також здійснює її експорт та імпорт. Дана система об'єднує 8 регіональних електроенергетичних систем, пов'язаних між собою системоутворюючими та міждержавними високовольтними лініями електропередач. За даними Держкомстату України, найбільша частка електроенергії виробляється на теплових електростанціях - приблизно 50%, на АЕС - 45%, на гідроелектростанціях – до 5%, відновлювальні джерела електроенергії – до 1%.

Загрози в енергетичній сфері. Вся сукупність загроз, які можуть впливати на функціонування систем енергетики умовно можливо поділити на ординарні загрози (ймовірні відмови та аварії) та неординарні (унікальні за причиною виникнення, характером розвитку та наслідками). Для протидії неординарним загрозам в системах енергетики передбачені різноманітні форми резервування потужностей, по виробленню та транспортуванню паливно-енергетичних

ресурсів, систем забезпечення гарантованого енергопостачання та створення запасів паливно-енергетичних ресурсів. За умов розвитку та функціонування національної економіки подібні ординарні явища майже не становлять загроз енергетичній безпеці, на відміну від неординарних впливів, які здатні негативно впливати на енергетичний комплекс в цілому. Серед неординарних загроз провідне місце займають кіберзагрози, які здатні спровокувати такі проблеми, як порушення забезпечення енергоресурсами, так і надзвичайні ситуації в енергетичному комплексі (ЕК) держави.

Такі кіберзагрози можуть бути реалізовані шляхом впливу на весь ЕК в цілому, або на його окремі елементи, як без так і з досягненням синергетичності результатів. Вплив може бути проведений комплексно, одночасно, послідовно або змішано на автоматизовану систему управління (АСУ), апаратно-програмний комплекс, персонал, фінансову систему енергетики. Найбільш уразливим місцем об'єднаної енергетичної системи (ОЕС) є АСУ.

Система управління ОЕС відіграє провідну роль у функціонуванні всього ЕК України. Саме на АСУ ОЕС може бути здійснений потужний кібервплив, який може призвести до порушення управління певним об'єктом енергетики або ЕК в цілому. За допомогою шкідливого програмного забезпечення кіберзловмисник може контролювати, а в окремих випадках, керувати частиною або всією АСУ. АСУ ОЕС має бути стійкою до кібервпливів та мати відповідну комплексну систему реагування на кібератаки.

У грудні 2015 року здійснені розосереджені синхронні кібератаки типу «розвинена стійка загроза» (*Advanced Persistent Threat* – APT) на АСУ енергосистемами компаній ПАТ «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго». Внаслідок кібератак виникли збої в роботі систем віддаленого доступу, протягом однієї-шести годин повністю або частково відключено понад 100 населених пунктів, вимкнено близько 60 підстанцій, в тому числі такі, від яких живляться стратегічні об'єкти, велика кількість користувачів залишилися без енергопостачання. Наслідки такої атаки можливо були здійсненні з метою перевірки функціонування системи захисту енергокомпаній та системи реагування на критичні ситуації. Кібератаки були комплексними та системно організованими, в ході яких було здійснено:

попереднє зараження мереж за допомогою підроблених листів електронної пошти;

захоплення управління АСУ з виконанням операцій вимикань на підстанціях;

виведення з ладу елементів АСУ;

видалення за допомогою утиліти KillDisk інформації на серверах та робочих станціях;

атака на телефону мережу кол-центрів, з метою забезпечення відмов в обслуговуванні знеструмлених абонентів.

Система управління виявилася вразливою до кібератак такого роду. Реагування на таку кібератаку не було своєчасним, система захисту не виконала свої функції.

У грудні 2016 року була проведена менш масштабна за наслідками кібератака енергокомпанії «Укренерго», яка призвела до виведення з ладу підстанції «Північна» та знеструмлення північної частини м. Києва та прилеглих районів. Атака мала за мету «демонстрацію сили» та була частиною операції проти державних установ України.

Кібератаки проведені на енергетичні підприємства у 2015 році були не в повній мірі самостійно організованими. В 2016 році дії стали більш оперативними, а шкідливе програмне забезпечення (ПЗ) «Crash Override» забезпечувало проведення спланованих атак на декілька «критичних точок» ЕК, передбачало самоорганізацію дій в процесі атак, було спроможним надсилати команди обладнанню енергетичної мережі щодо включення або відключення живлення. Що могло призвести до віяльного відключення електроенергії по всій державі. Аналіз кібервпливів на енергосистеми України представлено в таблиці 1.

Таблиця 1

Аналіз кібервпливів на енергосистеми України.

	Засіб впливу	Шлях проникнення	Ефект впливу	Наслідки
2015 рік				
«Прикарпаттяобленерго»	1. DoS-атака «відмова від обслуговування» на кол-центр обленерго.	Мережа Інтернет	Перенасичення мережевого устаткування великою кількістю зовнішніх запитів	Неможливість споживачів повідомити про відключення електроенергії.
	2. APT- атака.	Мережа SCADA, встановлення шкідливого ПЗ «Black Energy».	Перехоплення системи управління в мережі SCADA через викрадені облікові записи, команда на вимкнення систем безперебійного живлення та запобіжних систем	Відключення протягом 1-6 годин близько 30 підстанцій, залишення без світла близько 230 тисяч мешканців.
«Чернівціобленерго»	1. DoS-атака «відмова від обслуговування» на кол-центр обленерго.	Мережа Інтернет	Перенасичення мережевого устаткування великою кількістю зовнішніх запитів	Неможливість споживачів повідомити про відключення електроенергії.
	2.Утиліта KillDisk.	Мережа Інтернет	Знищення інформації на серверах та робочих станція	Виведення з ладу елементів IT інфраструктури
	3. APT-атака.	Мережа SCADA, встановлення шкідливого ПЗ «Black Energy»	Захоплення управління SCADA з виконанням операцій вимикань на підстанціях	Перерва електропостачання на 1-3,5 год. Зменшення обсягу споживання на 73 МВт/год (0.015% добового обсягу України).
«Київобле-	1. APT-атака.	Система віддаленого доступу.	Несанкціоноване втручання в АСУ	Відключення від електропостачання протягом 1-3 годин 30 вузлових підстанцій стратегічних об'єктів, близько 80 тис. споживачів
2016 рік				
«Укренерго»	Шкідливе ПЗ «Crash Override». (повністю автоматизована атака)	Мережа Інтернет	Перехоплення управління енергетичною системою, автоматизоване знеструмлення підстанцій	Повне знеструмлення підстанції із втратою живлення власних потреб. Зниження постачання від Київської ГАЭС до: ПАО «Київенерго» 144,9 МВт/год, ОАО «Київобленерго» - 58 МВт/год.

У червні 2017 року зловмисниками проведена масштабна деструктивна хакерська атака, яка була націлена на порушення роботи web-сайтів компаній та на систему клієнтської підт-

римки, яка отримала назву «Petya». Під деструктивним впливом опинились й «критичні точки» енергетичної галузі України. У травні 2018 року фахівці компанії Cisco повідомили про зараження більш ніж 500000 маршрутизаторів та роутерів в 54 державах. Для проведення такої атаки було використане деструктивне шкідливе ПЗ «VPNFilter», що дозволило зловмисникам здійснювати моніторинг протоколів Modbus, які використовуються в АСУ системи диспетчерського управління (СДУ) і збору даних (*Supervisory Control And Data Acquisition,* SCADA), перехоплювати весь трафік, що проходить через уражений пристрій, збирати інформацію (включно дані авторизації та персональні дані платіжних систем), віддалено керувати інфікованим пристроєм та виводити його з ладу.

На фоні довготривалої політичної кризи у Венесуелі 7 березня 2019 року, внаслідок кібератак на АСУ СДУ гідроелектростанції «Ель-Гурі», відбулася аварія, що спричинила широкомасштабне відключення електрики. Без енергопостачання залишилися 23 з 25 штатів, або 80% території країни. а також її столиця - Каракас. Системи управління енергопостачанням розбалансовані. У столиці обмежена подача води, виникли проблеми з каналізацією, магазини зачинені або працюють в умовах обмежень, гостро не вистачає продовольства та медикаментів. Платіжні банківські системи не працюють, телекомунікації, зокрема мобільний зв'язок, порушені. Припинив роботу міжнародний аеропорт Майкетія, знеструмлені лінії метро. За три місяці у лікарнях Венесуели з причин пов’язаних із відсутністю електрики померло 79 осіб. Уряд закликав до жорсткої економії пального. Жителі декількох районів Каракаса вийшли на вулиці, вимагаючи від влади відновити електропостачання. У країні проходять масові протести опозиції і зіткнення з поліцією. 10 березня 2019 року тимчасовий президент Венесуели Х. Гуайдо, який є головою парламенту країни - Національної асамблеї, запропонував оголосити надзвичайний стан у зв'язку з масштабними відключеннями електроенергії, що дозволяє запросити міжнародної допомоги, та закликав військових країни перейти на бік опозиції. Уряд США ввів санкції проти посадовців урядових силових структур, під керівництвом яких здійснювалися акції насильства та спалення гуманітарних вантажів продовольства та медикаментів, а також проти 35 нафтових танкерів декількох кампаній, в тому числі найбільшого державного нафтового концерну PDVSA [29-31].

Основні особливості APT-атак:

спрямованість на елементи критичної інфраструктури;

проведення групою висококваліфікованих зловмисників «хакерів»;

залишення невідомими (невиявленими) протягом тривалого часу;

ретельне маскування з використанням спеціально розроблених програмних засобів (спеціалізовані Shell-коди, RootKit та ін.);

належність до розвідувально-підривних операцій і підкріплення розвідувальними або руйнівними акціями.

АСУ ЕК є вразливими перед кібератаками. В результаті проведеного аналізу виокремлюються категорії можливих кібератак, які можуть бути націлені на:

елементи систем управління, наприклад віддалені термінали зв’язку з об’єктом (*Remote Terminal Unit*), або людино-машинного інтерфейсу (*Human Machine Interface* - ЛМІ), які зазвичай мають можливість віддаленого налаштування або управління;

протоколи передачі даних, які добре задокументовані та їх опис знаходиться у відкритому доступі.

Через віддалений доступ зловмисник може перехопити управління системою та спричинити повне або часткове виведення елементів системи з ладу; пошкодити обладнання, внести зміни в інформацію та передані оператору дані. Що може призвести до значних матеріальних та фінансових витрат через пошкодження обладнання, вимкнення ліній електропередач, аварії під час роботи працівників, перевиробництво електричної енергії, перенавантаження систем тощо.

На підставі проведеного аналізу кібератак на підприємства енергетичної галузі України, можемо спрогнозувати один з варіантів проведення типової кібератаки на АСУ. Розділимо її на фази: доступ, розвідка, перехоплення управління.

Для здійснення атаки на АСУ СДУ ЕК зловмисник спочатку має отримати до них доступ. Для нормальної роботи АСУ СДУ необхідний обмін інформацією. Зазвичай, інформація з АСУ СДУ потрапляє до тих чи інших баз даних, включно термінали операторів, долаючи мережеві шлюзи між комерційною та промисловою підмережами. Системи захисту операторського терміналу та комунікації обміну інформацією можуть бути вразливим до атак та використані зловмисником для проникнення до мережі АСУ СДУ ЕК.

Вразливим до атак може бути і віддалений доступ операторів або інших інженерів до систем АСУ СДУ ЕК через віртуальну мережу (*Virtual Private Network*), особливо у випадку невірного налаштування. Вразливість можуть становити сторонні сервери (архівування даних, розробників, аналітиків, тощо) та їхнє підключення до системи промислового управління.

Після здобуття доступу до мережі промислового управління, зловмисник має здійснити розвідку з метою вивчення схеми роботи АСУ СДУ. Складність систем АСУ СДУ примушує зловмисника витрачати час та сили на її вивчення. Одразу після вторгнення зловмисник, швидше за все, матиме дуже обмежений доступ до решти мережі. Серед доступних йому джерел інформації можуть бути внутрішні web-сервери, робочі станції операторів, мережеві диски, інші інтерфейси до керованих систем. Ці джерела інформації можуть бути доступними всім терміналам у мережі, інколи навіть без автентифікації користувача.

Іншим джерелом інформації може стати пасивна розвідка комп'ютерної мережі. Успіх цього методи істотно залежить від знаходження скомпрометованої системи в мережі та вимагає від операторів виконувати якісь дії (аби генерувати потоки даних). На відміну від попереднього підходу, може надати інформацію про облікові дані користувачів, використані ними протоколи, налаштування, тощо. Також пасивна розвідка мережі не потребує відправки пакетів даних і тому непомітна системам виявлення вторгнень. Якщо скомпрометована система знаходиться в одній мережі з основними складовими АСУ СДУ, зловмисник матиме можливість розвідки використаних протоколів та команд.

Зловмисник може вдатись і до активної розвідки мережі. Для цього йому знадобиться доступ до скомпрометованої системи з правами адміністратора, оскільки й цей метод передбачає можливість відправляти мережею спеціально сформовані пакети даних. Однак, ці пакети можуть бути помічені системою виявлення вторгнень, внаслідок чого системні адміністратори дізнаються про існування в мережі скомпрометованої системи. На противагу попереднім методам, цей метод дозволяє зловмисникові дізнатись про доступні зі скомпрометованої системи пристрої та інші термінали в мережі.

Нарешті, для розуміння та відтворення промислового процесу зловмисникові доведеться ретельно вивчити отриману ним інформацію.

Після вивчення промислового процесу, зловмисник може перейти до перехоплення управління ним. Різні методи можуть надавати різний рівень контролю, а відповідно, і результати атаки.

Серед найважливіших об'єктів для атаки є головний диспетчерський блок (*Front-End Processor*), який відповідає за взаємодію між програмованими логічними контролерами та іншими компонентами системи АСУ СДУ, зокрема, ЛМІ з оператором.

Однією з важливих цілей для зловмисника може бути ЛМІ, оскільки він доступно представляє стан всієї системи та надає можливість оператору керувати нею. Однак, можливості для атаки будуть обмежені можливостями ЛМІ і тому зловмисникові може не вдатись вивести систему з ладу або завдати більш істотної шкоди. Атака на ЛМІ є атакою націленою на часткове або повне перехоплення управління. З її переваг можна назвати те, що вона може бути здійснена із використанням звичайних підходів та інструментів, не пов'язаних з промисловими системами управління. Також атака на ЛМІ дозволить зловмисникові приховати свою діяльність під виглядом звичайної роботи оператора.

Схожою на атаку на ЛМІ може бути атака на робочі станції персоналу (РСП - *Engineering workstation*), залучених в розробці програмного забезпечення для ЛМІ та іншого системного ПЗ. Перевага атаки на РСП полягає в тому, що вони можуть не мати обмежень, які накладає

ЛМІ. Зловмисник, після вивчення протоколу між ЛМІ і контролерами, може здійснити спуфінгову атаку – відправляти підроблені команди контролерам або спотворювати дані, передані оператору.

Кіберзловмисники продовжують розвивати та нарощувати спроможності щодо здійснення кібервпливу на різні об'єкти та системи, продовжують створювати й застосовувати нові способи та форми існуючих і модернізованих кібератак. Виходячи з проведеного аналізу проведення кібератак на об'єкти критичної інфраструктури енергетичної сфери, встановлено, що кожна кібератака має свою форму застосування, свій ефект та наслідки після її проведення.

Стійкість системи – це здатність витримати різноманітні деструктивні впливи та відновлюватись у разі пошкоджень. Головне забезпечити функціонування, хоча б і в обмеженому обсязі [22]. Функціональна стійкість може бути оцінена кількістю і потужністю впливів, які може витримати система зі збереженням своєї функціональної спроможності.

Рівень стійкості та стан ОЕС буде впливати на інші галузі з можливістю проявів ланцюгових ефектів. То б то, від ЕК держави залежить функціонування інших об'єктів критичної інфраструктури, які впливають на економіку та обороноздатність держави.

Зниження стійкості та нестабільна робота ЕК держави нанесе колосальні збитки державі та населенню. Довгострокове відключення електроенергії призведе до хаосу у великих містах. Всі галузі та об'єкти пов'язані між собою, тобто створений так званий «ланцюг» і енергетична галузь знаходиться на ключовому місці. Руйнування системи енергетики або порушення її функціонування призведе до створення надзвичайних ситуацій, аварій, катастроф. Збої функціонування систем: транспортної, телекомунікаційної, фінансової, життєзабезпечення, безпеки населення можуть призвести до глобальних екологічних та техногенних наслідків.

Управління паливно-енергетичним комплексом (ПЕК) є автоматизованим, кожний цикл функціонування супроводжується роботою АСУ, тому на кожному етапі управління будь якою складовою ПЕК, може бути здійснений кібервплив на АСУ. Кібератаки можуть бути направлені як на об'єкти генерації енергоресурсів, так і на об'єкти їх транспортування та споживання. Кібервплив на складові ПЕК може бути проведено як асинхронно, так і синхронно. Найбільш уразливою ланкою є СДУ ЕК. Крім того, одночасно може бути проведений психологічний вплив, який буде спрямований на цільову аудиторію таку як управлінській та/або обслуговуючий персонал, споживачів тощо. Існує велика ймовірність проведення кібератак на всі об'єкти та системи одночасно. Метою проведення такого кібервпливу є створення ланцюгового ефекту, який розповсюджується на взаємодіючі об'єкти та системи. Характер та метод їх здійснення може мати гібридний розподільно-зосереджений вплив з ланцюговим ефектом, що передбачає здійснення зосереджених ефективних кібератак на найбільш вразливі елементи об'єкту (системи) і одночасно – інших розподілених кібератак на всі елементи системи, які здатні впливати синхронно, комплексно, одночасно або послідовно і наносити ураження елементам системи та/або виводити її з ладу. Методика здійснення гібридного розподільно-зосередженого кібервпливу з ланцюговим ефектом на прикладі АСУ об'єкту енергетичної сфери представлена в таблиці 2.

Таблиця 2

Методика можливого здійснення гібридних розподільно-зосереджених кібервпливів з ланцюговим ефектом

Об'єкти впливу	**Уразливість**	**Засоби впливу**	**Результат**	**Наслідки**	**Втрати**
Система управління видобуванням сировини	Людино-машинний комплекс	Зосереджена кібератака	Зупинка комплексу добутку сировини	Пошкодження програмного комплексу АСУ	Порушення безперервності функціонування
Система управління транспортом	АСУ транспортної галузі	Зосереджена кібератака на АСУ транспортування сировини	Затримка або припинення доставки сировини та готової продукції	Пошкодження програмного комплексу АСУ, фінансові втрати	Порушення функціонування інших складових транспортної системи
Переробні підприємства	АСУ переробної (нафто, газопереробної) галузі	Зосереджена кібератака на АСУ переробної промисловості	Зупинка переробних підприємств	Фінансові втрати	Зупинка постачання переробленої продукції
Енергетичні підприємства	АСУ, кол-центри	Організована комплексна асинхронна або синхронна кібератака на АСУ електростанціями	Відключення електроенергії, відмова роботи АСУ	Перехоплення управління	Припинення забезпечення електроенергією
Системи життєзабезпечення	Кол-центри, системи диспетчеризації		Збої у функціонуванні систем водопостачання та очищення	Фінансові втрати	Створення хаосу серед населення
Транспортна система регіону	АСУ, система диспетчеризації, системи оповіщення	Розподілено-зосереджені кібервпливи на транспортну та енергетичну галузі	Одночасна відмова функціонування АСУ транспортної системи та АСУ ЕК	Відмова в управлінні повітряним, водним та залізничним рухом, фінансові втрати	Створення хаосу серед населення в аеропортах, залізничних вокзалах
Системи довгострокового зберігання продовольства	АСУ енергетичного комплексу та транспортної галузі	Синхронні кібервпливи на АСУ транспортної установи та електростанції	Виведення з ладу систем, забезпечення довгострокового зберігання продовольства	Фінансові втрати підприємств, установ торговельної сфери	Порушення систем забезпечення потреб населення. Створення хаосу
Сектор безпеки та оборони (СБіО)	АСУ електростанцій, АСУ установ і організацій СБіО	Гібридні розподілено - зосереджені кібервпливи на АСУ установ та організацій	Відключення від електроенергії військових частин, установ і організацій	Втрата функцій контролю, управління, втрата інформації	Зниження бойової готовності, матеріальні та бойові втрати

Об'єкти впливу	Уразливість	Засоби впливу	Результат	Наслідки	Втрати
		СБіО та АСУ електростанцій, які забезпечують їх життєдіяльність та бойову готовність	ЗСУ, МВС, СБУ, ДПСУ, ДСНС, ДССЗЗІ. Знищення або вилучення інформації в ІТС військових частин, установ і організацій СБіО		
Підприємства важкої промисловості	АСУ електростанцій та транспортних установ	Синхронні кібервпливи на АСУ транспортних установ та електростанції, які забезпечують функціонування підприємств важкої промисловості	Повне відключення від електропостачання одного або декількох підприємств важкої промисловості	Фінансові втрати	Зупинка промисловості. Порушення систем забезпечення потреб держави, населення, СБіО.
Фінансова система (банки, фінансово-розрахункові установи)	АСУ електростанцій та АСУ фінансових установ та організацій	Гібридні розподілено- зосереджені кібервпливи на АСУ електростанцій, що забезпечують функціонування фінансивих установ і організацій та на АСУ фінустанов	Відключення від електроенергії фінустанов і організацій та одночасне проникнення в АСУ фінустанов	Фінансові втрати, втрата інформації	Фінансові втрати фізичних та юридичних осіб, державних підприємств, установ та організацій

Виходячи з проведеного нами аналізу проведення кібератак на об'єкти критичної інфраструктури та соціальні компоненти кіберпростіру, встановлено, що кожна кібератака має свої мету, зміст, організацію, тактику реалізації, основні та супутні ефекти і результати, наслідки після її здійснення тощо.

Кібердії можуть здійснюватися послідовно, паралельно та послідовно-паралельно, з використанням методів розподільно-зосереджених дій та/або сукупності одночасних та/або послідовних впливів, які полягають в зосередженні кібервпливів на найбільш вразливі елементи об'єкта (системи), які забезпечують отримання синергетичного ефекту в апріорі непередбачуваних місцях (елементах, системах, сферах), на які не обов'язково спрямовується безпосередній вплив.

Результат виникає за рахунок системи розосереджених впливів на не завжди безпосередньо взаємопов'язані елементи. Цей метод передбачає створення так званих гібридних кібератаки, які діють комплексно і взаємоузгоджено та охоплюють технічну, соціотехнічну та соціальну сфери. Вони здатні впливати синхронно, комплексно, одночасно або послідовно, наносити ураження елементам системи та/або виводити її з ладу. Метою проведення кібервпливу

на АСУ СДУ ЕК може бути створення ланцюгових ефектів, які розповсюджують деструктивну хвилю на взаємодіючі об’єкти та системи.

До складу АСУ можуть входити різноманітні технічні системи та засоби: системи і засоби координатно-часового, метеорологічного і інших видів забезпечення; системи, засоби, лінії та мережі зв'язку і передачі даних; системи і засоби дистанційного моніторингу; системи і засоби збору, накопичення та обробки інформації; автоматизовані системи і засоби управління; системи і засоби відображення і доведення інформації; інші технічні та програмно-технічні засоби. Значна частина систем і засобів використовується для формування каналу зворотного зв'язку як з людиною-оператором, так і з керованими технічними компонентами ОЕС.

Для протидії таким кібервпливам, що несуть в собі тяжкі наслідки для населення та держави в цілому, необхідно розробити методику виявлення таких особливих кібервпливів. Розглянемо розроблену методику щодо можливого здійснення гібридних розподілено-зосереджених кібервпливів з ланцюговим ефектом.

Критичність виходу з ладу об’єкта енергетики вимагає опрацювання питань захисту АСУ з акцентом на доступність та стійкість системи, а також цілісність інформації. Наприклад, можливі два підходи до побудови зон забезпечення кібербезпеки єдиного центру кіберзахисту (ЄЦК) енергетичної галузі – на основі рівнів або вимог безпеки і на основі загроз кібербезпеки. У першому випадку зони кібербезпеки визначаються як умовні кордони, що розділяються необхідними рівнями безпеки. На практиці зони утворюються шляхом виділення деяких функціональних областей АСУ.

В іншому випадку зони утворюються на основі можливих загроз кібербезпеки [22]. Для ЄЦК пропонуються наступні зони: зона ЄЦК (I), зона управління (II), зона доступу користувачів (III), зона мережевого обладнання (IV), зовнішня зона (V).

Для побудови ефективної системи захисту автоматизованої системи управління від кібервпливів, вибору і впровадженню адекватних організаційно-технічних заходів та засобів повинен передувати аналіз, опис і моделювання загроз й вразливості систем, розроблення методики виявлення кібервпливів. Отже, очевидним є те, що спочатку кожна загроза повинна бути розпізнана та ідентифікована. Зазначимо, що використовувані в сучасних системах виявлення й протидії кібератакам, методи є досить ефективними в тому разі, якщо відомі точні характеристики кібератак. Незалежно від використовуваних методів виявлення кібератак на автоматизовану систему управління енергетичної галузі зустрічаються з однаковою проблемою – постійно змінювані характеристики кібератак вимагають гнучкої системи захисту, яка здатна залишатися ефективною, навіть якщо не відомі точні характеристики кібератаки [21]. Методику виявлення та запобігання кібератакам представлено схематично на рисунку 1.

Реальність високого ризику практичної реалізації розглянутих кіберзагроз вимагає формування такої системи кібербезпеки та кібероборони, яка забезпечить скоординоване управління всіма її складовими. Така система потребує наявності відповідного єдиного органу управління, подібного за структурою, завданнями і функціями до аналогічних органів управління в цій сфері країн-членів НАТО, призначеного для реалізації єдиної політики та стратегії дій Міністерства оборони України та Збройних Сил України в інформаційному та кіберпросторі; організації та координації заходів щодо кібербезпеки та захисту критичної інформаційної інфраструктури держави; управління силами кібербезпеки та кібероборони під час кризових ситуацій, в умовах особливого періоду та правового режиму воєнного стану.

Цей орган управління інформаційної та кібербезпеки повинен вирішувати такі основні задачі:

участь у формуванні та реалізації державної політики з питань інформаційної, кібер- безпеки та кібероборони;

формування та реалізація політики Міністерства оборони України та Збройних Сил України щодо дій у кіберпросторі;

ЗОНА ЄЦК (I)	ЗОНА УПРАВЛІННЯ (II)	ЗОНА ДОСТУПУ КОРИСТУВАЧІВ (III)	ЗОНА МЕРЕЖЕВОГО ОБЛАДНАННЯ (IV)	ЗОВНІШНЯ ЗОНА (V)

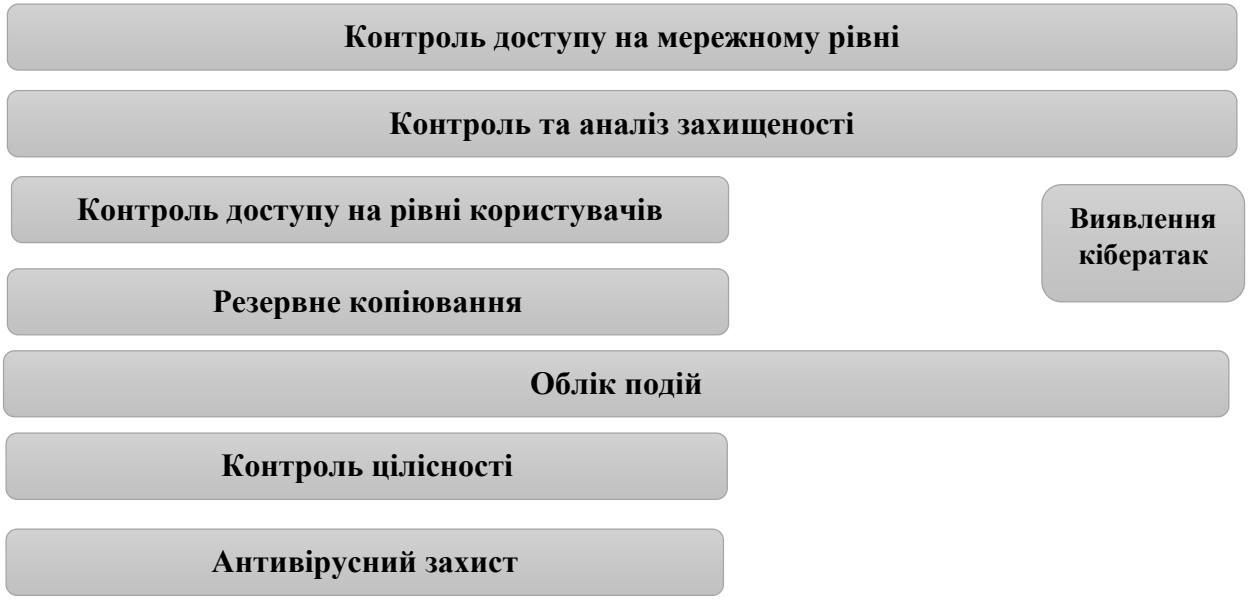


Рисунок 1 – Методика виявлення кібератак

участь у виконанні заходів зі створення та розвитку інформаційних систем та ресурсів у Збройних Силах України;

координації дій суб'єктів інформаційної, кібер- безпеки та кібероборони Міністерства оборони та Збройних Сил України;

участь у формуванні стандартів підготовки та держзамовлення на підготовку фахівців з інформаційної, кібер- безпеки та кібероборони;

організації взаємодії та проведення заходів (в т.ч. щодо підготовки держави до кібероборони) зі структурними підрозділами інших центральних органів виконавчої влади та міжнародними партнерами з питань кібербезпеки;

підтримання взаємодії з системою відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT);

планування та узгоджене управління діяльністю суб'єктів у кіберпросторі за єдиним замислом і планом. Контроль та координація їх дій;

моніторинг та аналіз кіберінцидентів, деструктивних інформаційних та когнітивних дій у кіберпросторі та ефективності дій системи кібербезпеки, виявлення уразливостей в інформаційних та кібер системах своїх і противника;

планування, організація та координація розвідувальних (Cyber Warfare Intelligence), оборонних (Defensive Cyber Warfare) і наступальних (Offensive Cyber Warfare) операцій в кіберпросторі (Cyberspace Operation) та кібероперацій (Cyber Operation);

організація та координація інформаційних дій у кіберпросторі (включаючи соціальні мережі).

З цією метою у складі органу управління інформаційної та кібербезпеки повинні бути підрозділи: моніторингу кіберпростору, захисту кіберпростору, активних дій у кіберпросторі,

Наявність ефективної системи управління силами і засобами які діють в кіберпросторі забезпечить інформаційну, кібернетичну та когнітивну перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції "смарт-оборони", ключовими елементами якої є високотехнологічна підготовка персоналу та збалансоване поєднання найбільш ефективних аспектів стратегій "жорсткої сили" та "м'якої сили", шляхом зваженого і узгодженого використання інструментарію стратегічних комунікацій, санкцій, переконання і застосування сили та інших впливів способом, який є найбільш рентабельним та має політичну і соціальну легітимність. Особливістю стратегії "м'якої сили" є об'єднання

трьох когнітивних компонентів: культури держави (у тому, чим вона цікавить інші держави), її політичних цінностей (чи дотримується вона їх у внутрішній і зовнішній політиці) та зовнішніх відносин (чи сприймаються вони як легітимні і морально обґрунтовані).

За досвідом провідних країн світу до найбільш ефективних та результативних дій сил спеціальних операцій у сучасних гібридних війнах відносяться впливи спрямовані на порушення систем управління державою та її сектором безпеки та оборони шляхом комплексного ведення різноманітних, але в першу чергу, інформаційних і кібернетичних дій спрямованих на дискредитацію військово-політичного керівництва держави у сприйнятті особового складу збройних сил, населення та світової спільноти.

Аналіз деструктивних дій, які ведуться з використанням спеціальних технологій в інформаційному та кібернетичному просторах України, дозволив виявити комплексні узгоджені за метою, замислом, місцем і часом інформаційно-кібернетичні впливи на всі верстви населення, соціальні і демографічні групи, керівництво держави, Міністерство оборони України та командування Збройних Сил України.

Для їх реалізації використовуються засоби телерадіомовлення, Інтернет ресурси (інформаційні сайти, соціальні мережі, спеціалізовані форуми тощо). Серед усіх деструктивних інформаційно-психологічних, інформаційно-кібернетичних дій, що проводяться, найбільш ефективними є ті, що спрямовані проти керівного складу держави та командування збройних сил.

Дослідження показали, що, як правило, такі дії є комплексними і включають елементи «непрямих впливів», маніпуляцію репутацією, сугестивний вплив. В рамках такої загальносистемної дії визначаються керівники, ті особи, вплив на яких забезпечує досягнення мети найкращим чином. Надалі обираються способи та форми впливу і проводиться інформаційна операція.

Вирішальним є те, що достатньо запустити інформацію, а далі, зважаючи на особливості соціуму, він сам буде продукувати плітки, будувати домисли та поширювати інформацію далі.

Таким чином, у кіберсфері уже є сформований спеціальний контент, активізація якого у визначений момент може блокувати дії будь-якого керівника і тим самим заблокувати дії структури, яку він очолює, або зробити її функціонування не ефективним, або примусити її працювати так як потрібно стороні, що проводить інформаційну операцію. Крім того такі дії створюють передумови до паніки, непокори, дезорієнтації, дезертирства тощо.

Завдяки використанню інноваційних технологій у конвенційній складовій сучасних війн став можливим перехід від дій загальноруйнівного характеру до дій із перевагою функціонально-структурного впливу на супротивника, а найголовніше – досягнення над ним когнітивної переваги.

Проведені дослідження показали, що когнітивне протиборство стало невід'ємною складовою сучасних і майбутніх війн і воєнних конфліктів як міждержавних і внутрішньодержавних, так і між будь-якими геополітичними та регіональними акторами. Когнітивній складовій належить виняткова роль в сукупності факторів, що формують і викликають воєнний конфлікт, впливають на його хід та результат, інтенсивність і наслідки. Тому, сучасні війни, а особливо війни майбутнього ведуться за когнітивну сферу соціуму (суспільства, соціальних груп, людини, населення) і керування ним (нею).

Когнітивні впливи можуть бути навмисними і випадковими, багатовекторними і комплексними, загальної спрямованості або цільовими (цілеспрямованими), спрямованими на суспільство в цілому чи на конкретні спільноти або індивідів, на досягнення короткотривалого або довготривалого ефекту, негайно або після латентної фази, з варіацією значень або без.

В сучасних умовах всі сторони конфлікту прагнуть взяти під контроль саме когнітивний простір, який охоплює сприйняття, усвідомлення, переконання, розуміння і цінності, інтелектуальне середовище, як індивідів, так і соціальних груп і суспільства в цілому, в якому власне і відбувається ухвалення ними рішень. Тому головний результат успішних когнітивних впливів – це зміна моделі світу та його сприйняття в людині, соціальних групах суспільства, та суспільстві в цілому, що забезпечує можливість взяття їх під контроль і здійснювати зовнішнє управління ними на емоційному, моральному, культурному, світоглядному і ментальному рівнях, з формуванням стійких стереотипів для сприйняття дійсності через їх призму. Особливе

значення мають при цьому нав'язування та просування хибних наукових, суспільних, економічних, державних, військових теорій, парадигм, концепцій, стратегій, наративів, які найбільш ефективно просуваються та впроваджуються через заклади освіти та наукові установи, електронні, соціальні мережі та блогосферу. З цією метою використовуються всі можливості стратегічних комунікацій, ведуться інформаційні, психологічні, кібернетичні та інші дії (акції, операції тощо), які спрямовані як на безпосередніх учасників конфлікту, так і на населення країн, що беруть в ньому участь, міжнародне співтовариство. Особливістю є те, що навіть при проведенні державними акторами дій планово та узгоджено, вони проходять на тлі хаотичних цільових і випадкових подібних впливів всіх інших акторів. Це трансформується в інформаційно-кібернетичний і когнітивний варіант війни "всіх проти всіх" (в кібернетичному, інформаційному та когнітивному просторах). У результаті, як показують проведені дослідження, об'єкти, на які спрямовані когнітивні дії можуть бути не просто введені в стан когнітивного резонансу, дисонансу або дисбалансу, але і отримати інформаційні та когнітивні травми, дійти до когнітивної межі сприйняття (неможливості подальшого безпечного сприйняття когнітивних впливів), часткової або повної когнітивної дезорієнтації і навіть до когнітивного колапсу, з подальшим переходом у стан когнітивної агресії або розчарування у всьому апатії і депресії.

Взагалі в сучасних конфліктах досягнення мети агресії здебільшого починається з несилових методів, головним чином економічних, політичних, дипломатичних, інформаційних, психологічних, кібернетичних, когнітивних тощо. Але, при цьому значну роль відіграють демонстраційні заходи військового попередження і стримування. Вони, найчастіше, виступають не просто демонстрацією сили, а мають за мету спровокувати дії, які сприятимуть економічному і морально-психологічному виснаженню противника, тощо. В цілому, у гібридних конфліктах будь-якої інтенсивності бойові дії (операції) є складовою взаємоузгоджених за єдиним замислом і планом інших (несилових) дій, які превалюють на всіх їх стадіях (зародження, ескалація, інтенсифікація, затухання, залагодження). Цим створюються дестабілізуючі внутрішні і зовнішні процеси в державі, яка є об'єктом агресії (стурбованість і невдоволеність населення, міграції, акції громадської непокори тощо). Надалі для досягнення стратегічних цілей застосовуються силові методи ведення дій з широкомасштабним залученням сил і засобів розвідки, оперативного управління військами (силами) і засобами, а також традиційних засобів ураження, державних збройних формувань, некомбатантів та інших учасників (терористів, радикальних озброєних груп, рухів опору, найманців, партизан), сил спеціальних операцій і т.і.

Перспективи подальших досліджень полягають у тому, щоб визначити найбільш критичні об'єкти інфраструктури держави, що підлягають захисту, а також дослідити запропонований метод інтелектуального розпізнавання загроз на більш широкому класі задач кількісного і якісного розпізнавання кібернападів.

Для ефективного кіберзахисту критичної інфраструктури держави, установ та підприємств оборонного комплексу необхідно впроваджувати комплексні організаційні та технічні заходи, щодо запобігання (зниження ризику реалізації) та протидії кіберзагрозам. Підсистеми захисту, зокрема, реалізовані в АСУ, мають вирішувати наступні організаційно-технічні завдання:

забезпечення безпеки санкціонованого доступу персоналу до системи та її складових;

запобігання цілеспрямованих злочинів та ненавмисних помилкових дій персоналу та сторонніх осіб, направлених на НСД до системи та її складових;

захист АСУ та її складових від деструктивного кібервпливу та інші [22].

Завдання ідентифікації загроз полягає у визначенні типів загроз, їх властивостей та можливостей в умовах апріорної невизначеності про об'єкт, надмірності іншої зовнішньої інформації, в т.ч. й хибної, зовнішнього деструктивного впливу на АСУ, тощо. Вирішення задачі можливе лише за рахунок оптимізації підходів до реалізації АСУ, в тому числі – до побудови систем комплексного захисту від кіберзагроз. [22].

Такий підхід дозволить побудувати систему захисту АСУ, що виконує завдання в умовах апріорної невизначеності, на принципах доцільності, раціональності та розумної достатності. В результаті декомпозиції складних систем управління, які виконують завдання в кризових

умовах, з'ясовано, що для забезпечення функціональної стійкості складні системи мають створюватися з урахуванням наступних основних вимог [22]:

безперервність функціонування;

гнучкість та адаптивність до загроз (атак);

забезпечення захисту від загроз;

багаторівневість захисту відповідно до рівнів загроз;

комплексність (реалізація організаційних, організаційно-технічних й інженерно-технічних засобів та заходів);

уніфікація програмно-апаратних та алгоритмічних рішень систем захисту;

варіативність функціональної логіки (адаптивність підсистеми захисту ІКС до інших подібних складних систем);

автономність функціонування технічної компоненти системи захисту;

реалізація багаторівневої системи контролю безпеки та захисту від помилок персоналу;

гарантоване кореговане забезпечення обмежень кола службових осіб щодо виконання ними повноважних функцій;

дотримання розумного балансу між завданням швидкої обробки великих заданих обсягів інформації в АСУ за мінімальний наявний проміжок часу та необхідністю витрачання значного часового ресурсу на досягнення мети функціонування систем захисту. [22].

Висновки. У статті розглянуті шляхи й напрями до вибору та реалізації раціональних підходів при вирішенні питання комплексного захисту від деструктивних кібервпливів з ланцюговими ефектами критичної інфраструктури держави та отримані такі основні результати:

1. Проаналізовано всі основні кібератаки, які впливали на функціонування об'єктів критичної інфраструктури на прикладі енергетичної сфери. В ході дослідження кібератак, було встановлено, що атаки не були одиночні, а проводилась синхронно, всі вони мали деструктивний вплив на АСУ об'єктами енергетики. Встановлено, що основний синхронний деструктивний кібервплив здійснювався зосереджено на вразливі елементи АСУ. Перед проведенням основної кібератаки, проводилась кібератака на систему обслуговування і диспетчеризації, з метою відмови в обслуговуванні споживачів. Застосування декількох деструктивних зосереджених кібератак на ЕК проводились в рамках масштабної кібероперації, яка була направлена на порушення одночасно декількох об'єктів енергетичної галузі.

2. Встановлено, що в залежності від рівня стійкості залежить результат функціонування системи вироблення та постачання електроенергії. Аналіз проведення кібератак показав, що мінімальне значення рівня стійкості може призвести до руйнування енергетичної системи (об'єкта, мережі).

3. Описано (змодельовано) методику здійснення гібридних розподільно-зосереджених кібервпливів з ланцюговим ефектом на об'єкти критичної інфраструктури. Визначені уразливості об'єктів. Визначені уразливості АСУ. Встановлено, що кібератаки здатні проникати через електронну пошту, отримувати доступ до головних серверів, отримувати інформацію про стан функціонування системи, здійснювати перехоплення управління АСУ та об'єктом в цілому, здійснювати зміну параметрів функціонування об'єктів (особливо критичним є зміна частоти реактора на атомній електростанції).

4. Розроблено методику виявлення гібридних розподілено-зосереджених кібервпливів з ланцюговим ефектом за допомогою моделі інтелектуального розпізнавання кіберзагроз .

5. Запропоновані організаційні та технічні заходи щодо забезпечення кібербезпеки на об'єктах критичної інфраструктури. Визначено, що технічні заходи мають бути реалізовані за допомогою комплексу засобів захисту, який буде забезпечувати своєчасне виявлення кібератак та протидію ним.

Запропоновані методика оцінки функціональної стійкості складних систем до деструктивних впливів та виявлення критичних елементів, вузлів та зв'язків системи, а також диференційний підхід до класифікації, розпізнання та визначення рівня загроз для складних АСУ, дозволяють обґрунтувати та створити комплексну організаційно-технічну підсистему захисту

критичної інфраструктури держави, яка гарантовано забезпечить адекватне реагування на реальні та потенційні загрози, раціонально використовуючи наявні у держави можливості і ресурси

ЛІТЕРАТУРА:

1. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 - Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

2. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

3. Alexander Kosenkov. Cyber Conflicts as a New Global Threat file: Режим доступу: //C:/Users/Downloads/futureinternet-08-00045.pdf

4. С.Вдовенко, Ю.Даник, С.Фараон, "Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення". Електронний журнал політики відкритого доступу "Комп'ютерні науки та кібербезпека" Харківського національного університету імені В.Н.Каразіна. SSN 2519-2310 (Online) №1 (12) 2019

5. Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018 Available: Режим доступу: http://www.gpoaccess.gov/congress/index.html

6. О.А.Баранов, Про тлумачення та визначення поняття "кібербезпека" "Правова інформатика", № 2(42)/2014 – С. 54-62.

7. В. Л. Бурячок. Основи формуваннядержавної системи кібернетичної безпеки: монографія / В. Л. Бурячок. – К.: НАУ, 2013. – 432 с.

8. В.Л. Бурячок. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / А.Л. Бурячок // Сучасна спеціальна техніка : зб. наук. праць. – 2011. – № 3 (26). – С. 104-114.

9. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа (2015). В. Б. Толубко (загальна редакція). Інформаційна на кіберберзпека: соціотехнічний аспект / В. Л. Бурячок, . – К.: ДУТ, 2015. – 288 с.

10. В. Л.Бурячок, Г. М. Гулак, В. О. Дорошко. Завдання, форми та способи ведення воєн у кібернетичному просторі. Наука і оборона, № 3 2011. – С .35-42.

11.Ю.І. Грицюк. Кіберінтервенція та кібербезпека україни: проблеми та перспективи їх подолання, Науковий вісник НЛТУ України. – 2016. – Вип. 26.8 Національний лісотехнічний університет України http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf

12.Р.В. Грищук , Ю.Г.Даник. Основи кібернетичної безпеки. Монографія. вид. трете перероблене Житомир. ЖНАЕУ, 2016. – 636 с.

13.Д.В.Дубов. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К.: Вид-во НІСД, 2011. – 30 с.

14. Д.В. Дубов. Стратегічні аспекти кібербезпеки України / Д.В. Дубов // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К.: Вид-во НІСД. – 2013. – № 4 (29). – С. 119-126.

15. Д. В. Дубов. Кіберпростір як новий вимір геополітичного суперництва : монографія /– К. : НІСД, 2014. – 328 с. Режим доступу: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

16. Р.В. Лук'янчук. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук'янчук // Вісник НАДУ: зб. наук. праць. – 2015. – Вип. 3. – С. 110-116.

17. Р. В. Лук'янчук. Деякі питання реформування системи державного управління у сфері забезпечення кібернетичної безпеки: сучасний погляд / Р.В. Лук'янчук // Вісник НАДУ : зб. наук. праць. – 2013. – Вип. 2. – С. 81 -92.

18. В.В. Петров. Щодо формування національної системи кібербезпеки України / В.В. Петров // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К. : Вид-во НІСД. – 2013. – № 4 (29). – С. 127-130.

19. В.П. Шеломенцев. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : зб. наук. праць. – 2012. – № 1(27). – С. 312-320.

20. М. Ю. Яцишин. Міжнародно-правова протидія кібервійнам / Яцишин М. Ю. //Збірник праць Національного авіаційного університету – 2015 – № 1 – С. 67-71

21. С.Г. Вдовенко, Ю.Г.Даник. Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління Збройних сил / Сучасні інформаційні технології у сфері безпеки та оборони № 2(29), 2017. С. 98-106.

22. С.Г.Вдовенко, Ю.Г.Даник. Концептуальні напрямки комплексного вирішення проблеми захисту від несанкціонованого доступу в складних системах спеціального призначення. Тези доповідей Шостої Міжнародної науково-технічної конференції, Вінниця 24-25.10.2017. С. 61-64

23. О.М.Гук, О.Ю.Чередниченко, Р.М.Штонда, І.О.Диба. Дії в кіберпросторі під час підготовки та ведення мережецентричної війни / Сучасні інформаційні технології у сфері безпеки та оборони № 2(29), 2017. С. 107-110.

24. J. Andress Cyber warfare: Techniques, tactics and tools for security practitioners / Andress J., Winterfeld S., Rogers R. – Amsterdam: Syngress/Elsevier, 2011. – 289 p

25. The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0. Tallinn 2016. Режим доступу – http://csef.ru/media/articles/3990/3990.pdf

26. Закон України Про основні засади забезпечення кібербезпеки України № 2163-VIII від 5 жовтня 2017 року.[Електронний ресурс] – Режим доступу:http://zakon.rada.gov.ua/laws/show/2163-19

27. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96 // Офіц. вісн. України. – 2016. – № 23.

28. Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14.03.2016 №92/2016

29. [Електронний ресурс] – Режим доступу: https://glavcom.ua/world/observe/venesuela-zalishilasya-bez-elektriki-575648.html

30. [Електронний ресурс] – Режим доступу: https://vesti-ukr.com/mir/328311-blekaut-v-venesuele-khuan-huajdo-reshil-vvesti-rezhim-chp

31. [Електронний ресурс] – Режим доступу: https://www.facenews.ua/news/2019/443568/

REFERENCES:

1. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 -Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

2. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

3. Kosenkov,A Cyber Conflicts as a New Global Threat file, Available:///C:/Users/Downloads/futureinternet-08-00045.pdf.

4. Vdovenko, S Danik,Y and Faraon, S (2019), "Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення." [Definitive problems of the Terms of the Sphere of Cyber security and Cyber Defense and the Ways of their solution], International electronic scientific journal Computer Science and Cybersecurity Issue 1(12) 2019 ISSN 2519-2310 (Online). – Available:https://periodicals.karazin.ua/cscs/issue/view/80

5. Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018 Available: Режим доступу: http://www.gpoaccess.gov/congress/index.html

6.Baranov,A (2014) "Pro tlumachennya ta vyznachennya ponyattya kiberbezpeka", [*On the interpretation and definition of cyber security*], "Pravova informatyka", [*Legal Informatics*], No. 2 (42) / 2014 - p. 54-62.

7. Buryachok,V (2013) "Osnovy formuvannya derzhavnoyi systemy kibernetychnoyi bezpeky",[*Fundamentals of the formation of the state system of cybernetic security*], a monograph , Kyiv: NAU, 432 pp.

8. Buryachok,V (2011) "Kibernetychna bezpeka – holovnyy faktor staloho rozvytku suchasnoho informatsiynoho suspilstva", [*Cybernetic security - the main factor for the sustainable development of a modern information society*],"Suchasna spetsialna tekhnika ",[*Modern special technique*] sciences works, No. 3 (26), p. 104-114.

9. Buryachok,V, Tolubko,V, Khoroshko,V and Tolyupa,S. (2015) "Informatsiyna na kiberberzpeka: sotsiotekhnichnyy aspekt",[*Information on cyber-security: the sociotechnical aspect*], Kyiv, DUT, 288 p.p.

10.Buryachok,V, Gulak,G and Doroshko,V. (2011) "Zavdannya, formy ta sposoby vedennya voyen u kibernetychnomu prostori", [*Tasks, forms and methods of conducting wars in cybernetic spacious*], "Nauka i oborona", [*Science and Defense*], № 3, p. 35-42.

11.Grytsuk, Yu. (2016) "Kiberinterventsiya ta kiberbezpeka Ukrayiny: problemy ta perspektyvy yikh podolannya" [*Ciber iintervention and cyber security of Ukraine: problems and prospects for their overcoming*], Naukovyy visnyk NLTU Ukrayiny, [*Scientific Bulletin of NLTU of Ukraine*], vol. 26.8 National Forestry University of Ukraine http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf

12.Grishchuk, R and. Danyk Yu. (2016) "Osnovy kibernetychnoyi bezpeky"[*The basics of cybernetic security*], Monograph., Zhytomyr. ZHNAEU, 636 pp.

13.Dubov, D and Ozhevan,M (2011) "Kiberbezpeka : svitovi tendentsiyi ta vyklyky dlya Ukrayiny", [*Cybersecurity. World Trends and Challenges for Ukraine*], Kyiv,View NISD, 2011, 30 p.p.

14.Dubov,D (2013) "Stratehichni aspekty kiberbezpeky Ukrayiny" [*Strategic Aspects of Cyber security of Ukraine*], "Stratehichni priorytety" [*Strategic Priorities: Sciences*], Kyiv,View NISD, № 4 (29), p. 119-126.

15.Dubov,D (2014) "Kiberprostir yak novyy vymir heopolitychnoho supernytstva", [Cyberspace as a new dimension of geopolitical rivalry], Monograph, Kyiv, View NISD, 328 p.p, Access Mode: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

16.Lukyanchuk,R. (2015) "Derzhavna polityka u sferi zabezpechennya kibernetychnoyi bezpeky v umovakh provedennya antyterorystychnoyi operatsiyi" [*State policy in the field of providing cybernetic security in the context of anti-terrorist operation*], "Visnyk NADU" zb. nauk. prats, [*Visnyk NADU*] sciences works p. 110-116

17.Lukyanchuk, R (2013) "Deyaki pytannya reformuvannya systemy derzhavnoho upravlinnya u sferi zabezpechennya kibernetychnoyi bezpeky: suchasnyy pohlyad" [*Some issues of reforming the system of public administration in the field of cybernetic security: modern view*], "Visnyk NADU" zb. nauk. prats, [*Visnyk NADU*] sciences works, Issue 2. - p. 81 -92.

18.Petrov,V (2013) "Shchodo formuvannya natsionalnoyi systemy kiberbezpeky Ukrayiny" [*Concerning the National Cybersecurity System of Ukraine*], nauk.-analit. zb. "Stratehichni priorytety", [*Strategic Priorities*] Science-analyst. every quarter save, Kyiv, View of NISS, No. 4 (29), p. 127-130.

19.Shelomentsev,V (2012) "Pravove zabezpechennya systemy kibernetychnoyi bezpeky Ukrayiny ta osnovni napryamy yiyi udoskonalennya" [*Legal support of the system of cybernetic security of Ukraine and the main directions of its improvement*], "Borotba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka)" zb. nauk. prats, [*Fighting organized crime and corruption (theory and practice)*] sciences works save. No. 1 (27). - P. 312-320.

20.Yatsyshyn,M. (2015) "Mizhnarodno-pravova protydiya kiberviynam" [*International legal counteraction to cyberwarfaces*], zbirnyk prats Natsionalnoho aviatsiynoho universytetu [*The National Aviation University publication collection*] № 1, p. 67-71.

21.Vdovenko,S and Danyk,Y (2017) "Kontseptualni napryamy kompleksnoho vyrishennya problemy zakhystu informatsiyi v systemi skrytoho upravlinnya Zbroynykh syl" [*Conceptual approaches for complex solution of information security in the code c2 of the armed forces*], *Modern Information Technologies in the Sphere of Security and Defence № 2 (29)/2017*

22.Vdovenko,S and Danyk,Y (2017) "Kontseptualni napryamky kompleksnoho vyrishennya problemy zakhystu vid nesanktsionovanoho dostupu v skladnykh systemakh spetsialnoho pryznachennya." [*Conceptual directions of the complex solution of the problem of protection against unauthorized access in complex systems of special purpose*], Abstracts of the 6th International Scientific and Technical Conference, Vinnytsia, 24-25.10.2017, p. 61-64.

23. Guk O., Cherednychenko O,, Shtonda R. and, Duba I. (2017) "Dii v kiberprostori pid chas pidgotovki ta vedennia merezhecentrychnoi vijny" [*Action in cyberspace during the preparation and conduct of network centric war*], *Modern Information Technologies in the Sphere of Security and Defence № 2 (29)/2017*

24. Andress,J., Winterfeld,S. and Rogers,R. (2011) "Cyber warfare: Techniques, tactics and tools for security practitioners" , – Amsterdam: Syngress/Elsevier, 2011. – 289 p

25.The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0. Tallinn 2016. Режим доступу - http://csef.ru/media/articles/3990/3990.pdf

26.Zakon Ukrayiny "Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny" № 2163-VIII 10/05/2017, [*Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine*] No. 2163-VIII of October 5, 2017. Available: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi

27.Stratehiia kiberbezpeky Ukrainy [*The strategy cyber security of Ukraine*.], of was approved by the Decree of the President of Ukraine dated March 15, 2016, No. 96/2016

28.Kontseptsiia rozvytku sektoru bezpeky i oborony Ukrainy [*Concept of development of the security and defense sector of Ukraine*], put into effect by the Decree of the President of Ukraine dated March 14, 2016, No. 92/2016.

29. Available: https://glavcom.ua/world/observe/venesuela-zalishilasya-bez-elektriki-575648.html

30. Available: https://vesti-ukr.com/mir/328311-blekaut-v-venesuele-khuan-huajdo-reshil-vvesti-rezhim-chp

31. Available:https://www.facenews.ua/news/2019/443568/

д.т.н., проф. Даник Ю.Г, Вдовенко С.Г.

ЭФФЕКТ ЦЕПНЫХ РЕАКЦИЙ В КИБЕРДЕЙСТВИЯХ

В статье представлены результаты исследований особенностей гибридной войны, которая происходит в Украине и других государствах в киберпространстве. Установлены роль и место цепных эффектов и асимметричных деструктивных действий в сфере информационной и кибербезопасности. В связи с тем, что в настоящее время энергетика является базовой отраслью национальной экономики и национальной безопасности любого государства, особенности комплексных деструктивных кибер, информационных и когнитивных действий и влияний в киберпространстве и через киберпространство рассмотрены на примере энергетической сферы с учетом угроз, рисков и особенностей кибервоздействий на системы и объекты критической инфраструктуры топливно-энергетического комплекса. Актуальность обеспечения энергобезопасности стран мира растет, о чем свидетельствует обзор энергетических стратегий развития Евросоюза, США и других стран. По взглядам ряда отечественных и иностранных специалистов, энергетика в области экономики превратилась в инструмент геополитики. От ее эффективного, надежного и устойчивого функционирования в значительной степени зависят уровень национальной безопасности государства в целом, темпы структурных преобразований в экономике, обеспечение потребностей населения, общественного производства и обороны. Применение на объектах критической инфраструктуры государства современных компьютерных, информационно-телекоммуникационных и кибертехнологий требует внедрения и осуществления мероприятий по кибербезопасности, противодействия кибертерроризму и обеспечения кибероборонь. Определены наиболее важные аспекты защиты от этих воздействий, предложенные подходы по разработке обоснованных организационных и технических мероприятий по обеспечению кибербезопасности общества и государства в современных условиях.

Ключевые слова: кибербезопасность, кибероборона, комплексные информационно-кибернетические воздействия, объекты энергетики, распределенно-сосредоточенные кибервоздействия, кибервоздействия с эффектом цепных реакций.

prof. Y. Danyk, S.Vdovenko

A CHAIN EFFECTS IN THE CYBER-ACTIONS

The article presents the results of research on the features of the hybrid war that occurs in Ukraine and other states in cyberspace. Established role and place of chain effects and asymmetric destructive actions in the field of information and cyber security. Due to the fact that at present energy is the basic industry of national economy and national security of any state, the features of complex destructive cyber-, informational and cognitive actions and influences in cyberspace and through cyberspace are considered on the example of the energy sphere taking into account threats. , risks and features of cyber-impacts on systems and objects of the critical infrastructure of the fuel and energy complex. The urgency of ensuring energy security of the countries of the world is increasing, as evidenced by the revision of energy development strategies of the European Union, the United States, and other countries. According to the views of a number of domestic and foreign specialists, energy in the field of economics has become an instrument of geopolitics. The level of national security in general, the pace of structural transformation in the economy, the provision of the needs of the population, social production and defense depend to a large extent on its effective, reliable and sustainable functioning. The use of state-of-the-art computer, information-telecommunication and cyber-tech equipment in state critical infrastructure objects requires the implementation and implementation of measures on cyber security, countering cyberterrorism and providing cyber defense. The most important aspects of these influences are identified, approaches are offered for the development of sound organizational and technical measures to ensure the cyber security of society and the state in modern conditions.

Keywords: cybersecurity, cyber defense, integrated information-cybernetic influence, energy objects, distributed-concentrated cyber impact, cyber impact with chain effect.

УДК.355.91

к.т.н., с.н.с. **Жиров Г.Б.** (КНУ)
к.т.н., с.н.с. **Литвиненко Н.І.** (ВІКНУ)
к.військ.н., с.н.с. **Федченко О.П.** (ВІКНУ)

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ СТРУКТУРИ ПРОСТОРОВОЇ БАЗИ ЦИФРОВИХ КАРТОГРАФІЧНИХ ДАНИХ МАСШТАБІВ 1:500 000, 1:1 000 000, СТВОРЕНОЇ ТОПОГРАФІЧНОЮ СЛУЖБОЮ ЗБРОЙНИХ СИЛ УКРАЇНИ

В останні роки потреба у відомостях про місцевість вже не задовольняється використанням тільки топографічних карт у паперовому вигляді. Недостатня інформативність карти, відсутність у працівників різних відомств, які не мають відповідної освіти, вміння читати карту ускладнюють її використання, а в окремих випадках, навіть, обмежують її застосування. Для вирішення ряду задач, які включають автоматизований аналіз стану території, потрібна детальна інформація про просторове положення об'єктів саме в цифровій формі

На сьогоднішній час велика частина інформації містить географічні дані, які є важливою інформацією в структурі національної безпеки держави. Відповідно до особливостей сучасних інформаційних технологій геодані повинні бути організовані в бази даних. Створюючи бази даних, користувач прагне впорядкувати інформацію за різними ознаками, щоб за необхідності здійснювати швидкий пошук, аналіз та її обробку. Допомогу в цьому можуть надати геоінформаційні системи (ГІС), які застосовуються в різних галузях і можуть функціонувати на різних рівнях. Сфера використання ГІС дуже широка. Сьогодні важко уявити без використання ГІС просторове моделювання та аналіз планування, управління, оцінки результатів багатьох сучасних інформаційних технологій, дослідження природних ресурсів, управління арміями і зброєю тощо. Так, за допомогою ГІС створюються і використовуються цифрові бази даних, які є основою цифрових та електронних карт місцевості різних масштабів.

У даній статті розглядається інформаційна структура просторової бази цифрових картографічних даних масштабів 1 :500 000, 1 :1 000 000, створеної Топографічною службою Збройних Сил України, та визначаються її особливості з метою подальшої розробки технології створення топографічних карт масштабів 1 : 500 000, 1 :1 000 000 у відповідності до стандартів НАТО (ТРС, ОNС) із застосуванням програмного забезпечення ArcGIS.

Ключеві слова: цифрові картографічні дані, геоінформаційні системи, геоінформаційні технології, цифрова карта, електронна карта, топографічна карта.

Вступ та аналіз останніх досліджень. В останні роки потреба у відомостях про місцевість вже не задовольняється використанням тільки топографічних карт у паперовому вигляді. Недостатня інформативність карти, відсутність у працівників різних відомств, які не мають відповідної освіти, вміння читати карту ускладнюють її використання, а в окремих випадках, навіть, обмежують її застосування. Для вирішення ряду задач, які включають автоматизований аналіз стану території, потрібна детальна інформація про просторове положення об'єктів саме в цифровій формі [1, 2].

Як свідчать проведені дослідження [3-5], 75–90 % усієї інформації, яку використовують спеціалісти різного рівня, містять у собі географічні (геопросторові) дані, тобто різні відомості про розподіл у просторі або за територіями об’єктів, явищ, процесів, подій. Це означає, що геоінформаційні системи (ГІС) обробляють велику частину інформації. Вони відрізняються від інших інформаційних систем саме тим, що володіють ефективними можливостями інтеграції різнопланової просторової інформації, пов'язаної з реальним земним простором. Таким чином, будь-які дані можуть бути інтегровані в одну систему, якщо ці дані мають або можуть мати просторову прив'язку в реальному земному просторі. Сучасні ГІС розширюють методи дослідження нашого світу, надаючи цифрові інструменти для організації й оперування просторовими даними, моделювання процесів, що відбуваються в просторі, візуалізації цих даних, моделей і процесів за допомогою розвинених комп'ютерних засобів, спеціалізованих інструментів обробки й аналізу геоданих.

Сфера використання ГІС дуже широка [6]. Сьогодні важко уявити без використання ГІС просторове моделювання та аналіз планування, управління, оцінки результатів багатьох сучасних інформаційних технологій, дослідження природних ресурсів, управління арміями і зброєю тощо [3,7].

ГІС охоплюють усі просторові рівні: глобальний, регіональний, національний, локальний, муніципальний; інтегрують різноманітну інформацію про нашу планету: картографічну, ДДЗ, статистику, кадастрові відомості, гідрометеорологічні дані, матеріали польових топогеодезичних знімань тощо. За їх допомогою вирішуються завдання розвитку територій, використання природних ресурсів, охорони довкілля, забезпечення суспільної безпеки.

Навіть миттєвий погляд на карту дає змогу оцінити особливості й закономірності просторово-розподілених подій і явищ. Розроблені в ГІС автоматизовані методи просторового аналізу вже сьогодні є потужною зброєю в руках дослідника, керівника будь-якого рівня та, навіть, простого споживача. Ідеї, закладені в ГІС, стають каталізатором процесів інтеграції геоінформаційних технологій (ГІТ), надаючи їм новий вимір. При цьому, геопросторові дані стають важливою інформацією в структурі національної безпеки держави. ГІС виконує функції введення, інтеграції, зберігання, обробки, аналізу, моделювання і візуалізації геопросторової інформації, яка за допомогою ГІС впорядковується в цифрові бази даних з метою швидкого пошуку, аналізу та обробки необхідної інформації.

Процес введення даних у ГІС передбачає наступні три етапи:

– введення просторових даних (цифрування або дігіталізація);

– введення непросторових (атрибутивних) даних;

– встановлення зв’язку між просторовими та непросторовими даними.

Два останніх етапи являють собою попередню обробку даних. У процесі такої обробки нагромаджується новий клас даних – метадані (дані про дані). Метадані зазвичай містять інформацію про дату одержання, точність позиціонування, точність класифікації, ступінь повноти, метод, який використовується для одержання та кодування даних.

Ядром ГІС є база даних, під якою розуміють поіменовану сукупність даних, які відбивають стан об’єкта, його властивості та взаємовідношення з іншими об’єктами, а також комплекс технічних і програмних засобів для ведення цих баз даних.

Формування структури ГІС починається з формування баз даних, які ґрунтуються на територіальній (географічній) прив’язці даних [3].

Таким чином, тематика статті, яка спрямована на аналіз особливостей інформаційної структури просторової бази цифрових картографічних даних масштабів 1 : 500 000 та 1:1 000 000, створеної Топографічною службою ЗС України, є актуальною.

Постановка завдання. В даній статті розглядається інформаційна структура просторової бази цифрових картографічних даних масштабів 1 :500 000, 1 :1 000 000, створеної Топографічною службою Збройних Сил України, та визначаються її особливості з метою подальшої розробки технології створення топографічних карт масштабів 1 : 500 000, 1 :1 000 000 у відповідності до стандартів НАТО (TPC, ONC) із застосуванням програмного забезпечення ArcGIS.

Основні результати дослідження. Цифрова карта місцевості (ЦКМ) являє собою цифрову модель місцевості, яка записана на магнітний носій у встановленій структурі та кодах відповідно до визначеної математичної основи, проекції і розграфлення, прийнятих для карт, і відповідає встановленим для конкретного використання вимогам за точністю і змістом.

Електронна карта місцевості (ЕКМ) – це цифрова модель місцевості, яка візуалізована з використанням програмних та технічних засобів у заданій проекції, системі координат та умовних знаків, і призначена для автоматизації картографічного відображення та аналізу об’єктів, процесів і явищ з урахуванням динаміки їх розвитку.

Цифрові карти місцевості призначені для використання в інформаційно-аналітичних системах за допомогою геоінформаційних технологій з метою вивчення та оцінки місцевості, орієнтування на ній, виконання вимірювань, розрахунків, побудови моделей ситуацій і процесів, які відбуваються на місцевості.

ЦКМ повинні відповідати таким основним вимогам:

1) створюватися на вибрану територію цілком без розподілу інформації на номенклатурні листи топографічних карт чи будь-якої іншої нарізки;

2) створюватися у світових координатах (довгота, широта);

3) забезпечувати можливість програмного визначення даних про розташування об’єктів та їх характеристики;

4) включати значення кількісних, якісних характеристик та кодів об'єктів у системі класифікації та кодування картографічної інформації (відповідно до класифікатора топографічної інформації для топографічних карт масштабів 1:10 000, 1:25 000, 1:50 000, 1:100 000, 1:200 000, 1:500 000, 1:1 000 000, який затверджений начальником Головного управління геодезії, картографії та кадастру при Кабінеті Міністрів України в 1998 р. і погоджений з начальником Центрального топографічного управління Генерального штабу Збройних Сил України);

5) точність зображення об'єктів на ЦКМ повинна відповідати точності вихідного картографічного матеріалу;

6) мати структуру подання інформації, яка забезпечить можливість внесення змін та доповнень;

7) мати структуру подання інформації, яка забезпечить можливість конвертації як у топологічні (такі, що підтримують просторові відношення перетину, сусідства, суміщення, об’єднання, виключення тощо), так і в нетопологічні формати геоінформаційних систем.

Зміст електронної карти повинен відповідати змісту карти певного виду та масштабу. При цьому система умовних знаків електронної карти включає спеціальні шрифти, а класифікація електронних карт відповідає загальній класифікації карт, наприклад, електронна топографічна карта, електронна авіаційна карта, електронна геологічна карта, електронна кадастрова карта та інші.

Для обміну цифровими картами між різними інформаційними системами використовуються спеціальні обмінні формати. Це можуть бути або популярні формати будь-яких виробників програмного забезпечення (наприклад, DXF, MIF, SHP та інші), що стали стандартом “де-факто”, або міжнародні стандарти (наприклад, такий стандарт Open Geospatial Consortium (OGC), як GML). Цифрові карти, що створюються Топографічною службою Збройних Сил України можуть зберігатися і використовуватися як у вигляді закритих даних (формат F20S), так і у відкритих поширених форматах: MIF, SHP, MDB, GDB. Перехід між форматами здійснюється за допомогою конверторів без втрати інформації. За необхідності можлива конвертація в будь-який формат, оскільки структура даних є уніфікованою.

Структура ЦКМ побудована на принципах об’єктно-орієнтованих систем і складається з елементів, об’єктів, узагальнюючих об’єктів, підсегментів та сегментів. Топографічні об’єкти можуть бути елементами та об’єктами ЦКМ. Основою ЦКМ є об’єкт, який може мати множину елементів та входити до складу узагальнюючого об’єкта. Узагальнюючі об’єкти або самостійні об’єкти, які не входять до їх складу, поєднуються в підсегменти і сегменти.

За типом просторової локалізації всі топографічні та узагальнюючі об’єкти ЦКМ поділяються на точкові, лінійні та площинні. Змістовні властивості топографічних та узагальнюючих об’єктів відображаються в семантичній інформації ЦКМ. Семантичну інформацію складає множина якісних і кількісних характеристик, які є атрибутами цих об’єктів.

Кожний топографічний та узагальнюючий об’єкт ЦКМ має унікальний ідентифікаційний код. За систему кодування приймається, в першу чергу, державна система (наприклад, для населених пунктів, об’єктів адміністративно-політичного поділу областей, районів – коди Класифікатора об'єктів адміністративно-територіального устрою України), за її відсутності – відомча, а за відсутності обох – система кодів, яка традиційно використовується в існуючих інформаційних системах, і лише у разі відсутності таких – довільне кодування.

Усі елементи ЦКМ, які відносяться до окремого об’єкта ЦКМ, повинні мати у відповідному атрибуті ідентифікаційний код цього об’єкта, а всі об’єкти, які відносяться до певного узагальнюючого об’єкта, – ідентифікаційний код цього узагальнюючого об’єкта.

Кожний топографічний об’єкт ЦКМ має топографічний код згідно з Класифікатором топографічної інформації для топографічних карт масштабів 1:10 000, 1:25 000, 1:50 000, 1:100 000, 1:200 000, 1:500 000, 1:1 000 000. Об’єкти ЦКМ, які не мають коду Класифікатора,

позначені додатковими кодами. Сама електронна карта місцевості складається з восьми базових сегментів, які показані на рис.1.

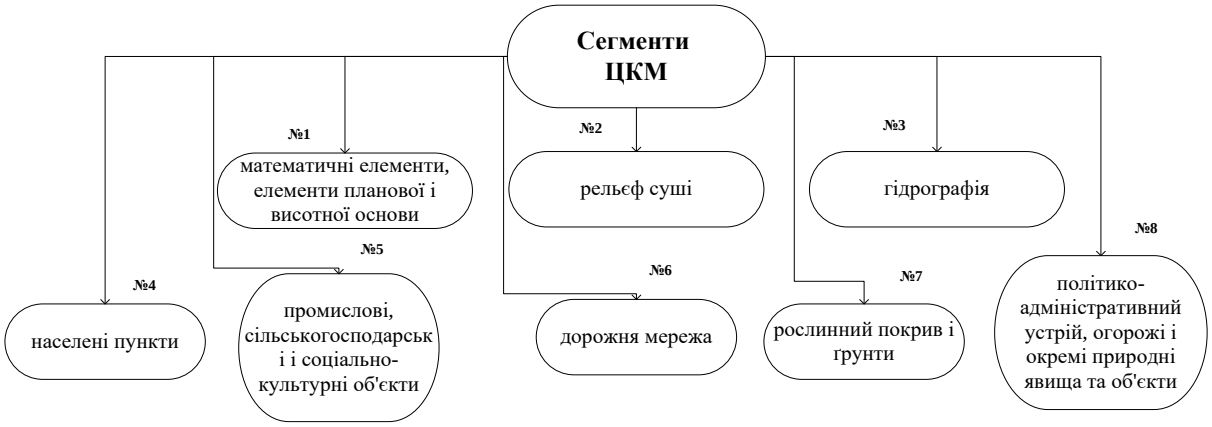


Рисунок 1 – Базові сегменти цифрової карти місцевості

Включення додаткових сегментів необхідно обгрунтовувати в технічному завданні на виготовлення ЦКМ.

Відповідно до вимог [8], основним програмним продуктом для застосування в Збройних Силах України визначено геоінформаційний продукт ArcGIS компанії ESRI (США).

До складу ArcGIS входять інтегровані програмні продукти, призначені як для розробки та експлуатації геоінформаційних систем різного рівня складності, так і для геоінформаційного забезпечення розв'язання завдань, пов'язаних з використанням просторової інформації, включаючи польову зйомку і роботу в комп'ютерних мережах, у тому числі і в системі Інтернет.

Основними модулями програмного забезпечення ArcGIS для використання в інтересах Збройних Сил України є: ArcMap – призначений для перегляду, редагування, створення та аналізу геопросторових даних; ArcCatalog – для керування та конвертації геопросторових даних; ArcScene і ArcGlobe – для тривимірного моделювання і відображення; ArcGIS 3D Analyst – для вирішення прикладних задач з використанням тривимірних даних; ArcGIS Spatial Analyst дозволяє працювати з растровими даними; ArcGIS Network Analyst призначений для роботи з геометричними мережами та дозволяє знаходити оптимальні маршрути; ArcGIS Survey Analyst призначений для урівнювання та відображення геодезичних знімань [9].

Створення цифрової карти місцевості включає наступні кроки.

1. Визначення вихідних матеріалів для створення ЦКМ.

Вихідними картографічними матеріалами для складання ЦКМ є:

а) цифрові карти місцевості;

б) видавничі (складальні) оригінали топографічних карт або їх копії;

в) тиражні відбитки топографічних карт;

г) ортофотоплани та матеріали космічної зйомки.

2. Вихідні картографічні матеріали повинні забезпечити точність, достовірність та повноту відображення стану місцевості по метричній і семантичній інформації, яка відповідала би вимогам, висунутим до ЦКМ.

3. Для одержання необхідних відомостей як додатковий матеріал при створенні ЦКМ повинні використовуватися:

а) каталоги та списки кодів об'єктів (КОАТУУ, відомчі коди та ін.);

б) списки населених пунктів з відомостями про кількість мешканців;

в) списки координат об'єктів з їх висотами;

г) дані про висоти будівель в населених пунктах;

е) дані про склад та стан рослинного покриву;

є) каталоги (списки) координат геодезичних пунктів та інші документи.

4. Загальні особливості відображення топографічних об'єктів на ЦКМ.

Об’єкти, нанесені на карту, поділяються на точкові, лінійні та площинні.

До точкових відносяться об’єкти, які мають розміри 1 мм^2 і менше у масштабі карти. Положенню точкового об’єкта на місцевості відповідає головна точка позамасштабного умовного знаку, яка зображує його на карті.

До лінійних об’єктів відносяться лінійно-протяжні об’єкти, які мають ширину 1 мм і менше у масштабі карти. Положенню лінійного об’єкта на місцевості відповідає осьова лінія умовного знаку.

До площинних відносяться об’єкти, які мають розміри більше 1 мм^2 у масштабі карти. Якщо зображення площинного об’єкта перетинає рамка обрізу ЦКМ, то за його межу приймається відрізок рамки на цій ділянці.

На ЦКМ базові сегменти відображуються наступним чином:

Сегмент №1. Математичні елементи, елементи планової і висотної основи. Відображаються всі пункти планової та висотної основи (астрономічні, геодезичні, зйомочної і нівелірної мереж), які мають підпис абсолютної висоти та підписи відміток висот. Узагальнюючі об'єкти в цьому сегменті відсутні.

Сегмент №2. Рельєф суші. Як правило, відображаються всі горизонталі в поєднанні з умовними знаками обривів, скель, ярів, вимоїн, зсувів, сухих русел, карстових воронок, кам'яних рік, лавових потоків, фірнових полів та ін.

Рельєф на ЦКМ може бути відображений відмітками висот як на рівномірній сітці у будь-якому GRID форматі, текстовому форматі, форматі електронних таблиць чи у форматі растрового файлу (TIFF, BMP, PCX та ін.), так і на нерівномірній сітці при умові надання програмних засобів перетворення цього формату в інші формати.

Сегмент №3. Гідрографія і гідротехнічні споруди. Відображаються водойми (океани, моря, озера водосховища та ін.), водотоки (ріки, канали, струмки, канави), об'єкти прибережної смуги (берегові обмілини і мілини, береги обривисті та ін.), рельєф дна (ізобати, позначки глибин), об'єкти навігаційної небезпеки (рифи, скелі, камені, банки), характеристики гідрографії, що виділяються на карті як самостійні об'єкти (урізи води на ріках, напрямки течії та ін.), джерела води та гідротехнічні споруди (греблі, шлюзи, портові і причальні споруди, водопровідні та водорозподільні споруди та ін.).

Сегмент №4. Населені пункти. Відображаються населені пункти всіх типів, окремі будівлі та елементи внутрішньої структури населених пунктів.

Сегмент №5. Промислові, сільськогосподарські та соціально-культурні об'єкти. Відображаються промислові об'єкти, місця видобутку корисних копалин, комунікації, споруди при промислових об'єктах, споруди і об'єкти соціального призначення, культові споруди та ін.

Сегмент №6. Дорожня мережа і дорожні споруди. Відображаються автомобільні шляхи всіх класів, залізниці, ґрунтові дороги, стежки, характерні ділянки дорожньої мережі, споруди на залізницях та автомобільних дорогах та ін.

Сегмент №7. Рослинний покрив та ґрунти. Відображається деревна рослинність природного та штучного походження, інша рослинність, всі види ґрунтів.

Сегмент №8. Політико-адміністративний устрій, огорожі і окремі природні явища та об'єкти. Відображаються кордони, межі, огорожі, аеронавігаційні дані, окремі природні явища та об'єкти.

Вимоги до додаткових (тематичних) сегментів ЦКМ полягають у наступному:

- додаткові (тематичні) сегменти повинні мати таку ж геометричну, інформаційну та об'єктну структуру, як і базові сегменти ЦКМ;
- кожен сегмент може включати в себе декілька підсегментів, об'єкти яких поєднуються за просторовими чи іншими тематичними принципами;
- атрибути об'єктів повинні мати українські та англійські скорочення для назв полів. Назви полів не можуть мати більше 8 символів;
- структура тематичних сегментів повинна бути описана в формулярі ЦКМ окремим підрозділом.

Вимоги до електронної бібліотеки умовних знаків та кодових сторінок полягають у наступному:

- ЦКМ як віртуальна сукупність структурованої інформації не має свого відображення в екранній або надрукованій формі, тобто не може мати своєї системи умовних знаків;
- відображення інформації ЦКМ відбувається за допомогою програмних засобів геоінформаційних технологій, які використовують свої бібліотеки умовних знаків, достатні для відображення всіх суттєвостей, які мають топографічні та додаткові до них коди;
- семантична інформація ЦКМ повинна заноситися в єдину кодовану сторінку. Ця сторінка повинна містити в собі повний набір символів української абетки та символів ASCII. В формулярі ЦКМ повинна бути приведена повна назва кодової сторінки з посиланням на державний або міжнародний стандарт, яким вона прийнята [8].

Вимоги до оформлення ЦКМ полягають у наступному: ЦКМ видається у вигляді файлової структури, яка записана на магнітний або оптичний носій. Крім змістовних файлів, в комплекті повинен бути текстовий файл формуляру ЦКМ (ім'я файлу - formular.*) та спеціальна директорія, що містить файли бази метаданих (ім'я директорії – metadata).

Висновки. Таким чином, у статті розглянуто інформаційну структуру просторової бази цифрових картографічних даних масштабів 1 :500 000, 1 :1 000 000, створеної Топографічною службою Збройних Сил України, та визначено її особливості з метою подальшої розробки технології створення топографічних карт масштабів 1:500 000, 1:1000 000 у відповідності до стандартів НАТО (TPC, ONC) із застосуванням програмного забезпечення ArcGIS.

ЛІТЕРАТУРА:

1. Журкин И.Г., Хлебникова Т.А. Цифровое моделирование измерительных трехмерных видеосцен: монография. Новосибирск: СГГА, - 2012. 246 с.

2. Руденко Л.Г., Козаченко Т.І., Ляшенко Д.О. та ін. Геоінформаційне картографування в Україні. Концептуальні основи і напрями розвитку. Київ: Наук. думка, 2011. - 104 с.

3. Зацерковний В.І., Бурачек В.Г., Железняк О.О., Терещенко А.О. Геоінформаційні системи і бази даних: монографія. Ніжин: НДУ ім. М. Гоголя, 2014. - 492 с.

4. Капралов Е.Г., Коновалова Н.В. Введение в ГИС: учебн. пособие. Москва: ООО “Библион”, 1997. - 160 с.

5. Геоинформатика / Е.Г. Капралов, А.В. Кошкарев, В.С. Тикунов и др. – Москва: Академия, 2005. - 480 с.

6. Шипулін В.Д. Основні принципи геоінформаційних систем: навч. посібник. Харків: ХНАМГ, 2010. - 313 с.

7. Пересадько В.А. Проектування картографічної бази даних для створення регіональної еколого-природоохоронної ГІС. Збірник наукових праць “Проблеми безперервної географічної освіти і картографії” Харківського національного університету імені В.Н. Каразіна. 2013. Вип. 17. С.34–40.

8. ВСТ 01.110.001 – 2011 (01). Топогеодезичне забезпечення. База даних картографічної інформації для створення та використання в геоінформаційних системах ArcGIS, 2011. 112 с.

9. Інструкція з використання топографічних, спеціальних, цифрових (електронних) карт у Збройних Силах України: затв. наказом Начальника Генерального штабу Збройних Сил України від 17.09.2016 № 354.

REFERENCES:

1. Zhurkin I.G., Hlebnikova T.A. (2012), “Cifrovoe modelirovanie izmeritel'nyh trehmernyh videoscen: monografija” [Digital modeling of measuring three-dimensional video scenes], Novosibirsk: SGGA,. 246 p.

2. Rudenko L.H., Kozachenko T.I., Liashenko D.O. and other (2011), “Heoinformatsiine kartohrafuvannia v Ukraini. Kontseptualni osnovy i napriamy rozvytku” [Geographic information map mapping in Ukraine. Conceptual basis and direct development], Kyiv: Nauk. dumka,. 104 p.

3. Zatserkovnyi V.I., Burachek V.H., Zhelezniak O.O., Tereshchenko A.O. (2014), “Heoinformatsiini systemy i bazy danykh: monohrafiia” [Geographic information systems and databases], Nizhyn: NDU im. M. Hoholia,. 492 p.

4. Kapralov E.G., Konovalova N.V. (1997), “Vvedenie v GIS: uchebn. posobie” [Introduction to GIS], Moscow: OOO “Biblion”, 160 p.

5. Kapralov E.G., Koshkarev A.V., Tikunov V.S. and other. (2005), “Geoinformatika” [Geoinformatics], Moscow: Akademija, 480 p.

6. Shypulin V.D. (2010), “Osnovni pryntsypy heoinformatsiinykh system: navch. posibnyk” [The Basic Principles of Geographic Information Systems], Kharkiv: KhNAMH,. 313 p.

7. Peresadko V.A. (2013), “Proektuvannia kartohrafichnoi bazy danykh dlia stvorennia rehionalnoi ekoloho-pryrodookhoronnoi HIS” [Designing a mapping database for the creation of a regional ecological and environmental GIS], Collection of scientific works “Problems of Continuous Geographical Education and Cartography” of Kharkiv National University of V.N. Karazin, No. 17, pp. 34–40.

8. VST 01.110.001 – 2011 (01) (2011), “Topoheodezychne zabezpechennia. Baza danykh kartohrafichnoi informatsii dlia stvorennia ta vykorystannia v heoinformatsiinykh systemakh ArcGIS” [Topogeodetic support. Map data map database for creation and using in ArcGIS Geoinformation Systems], 112 p.

9. “Instrukcija z vykorystannja topografichnyh, special'nyh, cyfrovyh (elektronnyh) kart u Zbrojnyh Sylah Ukrai'ny” [Instruction on the use of topographic, special, digital (electronic) maps in the Armed Forces of Ukraine], Zatverdzheno Nakaz Nachal'nyka General'nogo shtabu Zbrojnyh Syl Ukrai'ny vid 17.09.2016 № 354.

к.т.н., с.н.с. Жиров Г.Б., к.т.н., с.н.с. Литвиненко Н.І.,
к.військ.н., с.н.с. Федченко О.П.

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ СТРУКТУРЫ ПРОСТРАНСТВЕННОЙ БАЗЫ ЦИФРОВЫХ КАРТОГРАФИЧЕСКИХ ДАННЫХ МАСШТАБОВ 1 : 500 000 И 1 : 1000 000, СОЗДАННЫХ ТОПОГРАФИЧЕСКОЙ СЛУЖБОЙ ВОРУЖЕННЫХ СИЛ УКРАИНЫ

В нынешнее время большая часть информации содержит данные о географическом расположении объектов. В соответствии с особенностями современных информационных технологий все данные должны быть организованы в базы данных с целью адекватного отражения объектов определенной предметной области (которые имеют тенденцию постоянно изменяться). Создавая базу данных, пользователь стремится упорядочить информацию по различным признакам, осуществлять при необходимости быстрый поиск, анализ и обработку. Таким образом, ГИС занимают лидирующие позиции среди других информационных систем.

ГИС применяются во всех отраслях хозяйственного комплекса и могут функционировать на разных уровнях. При использовании ГИС пространственные данные становятся стратегически важной информацией как для корпоративной деятельности, так и в структуре национальной безопасности государства, при этом, одной из задач является задача создания цифровой базы данных, от которой напрямую зависит полезность ГИС и, которая представляет собой ее ядро. На основе базы геоданных создаются цифровые карты местности различных масштабов.

Таким образом, в статье решается задача по определению требований, предъявляемых к цифровой карте местности, ее структуре и этапов создания с целью дальнейшей разработки технологии создания топографических карт масштабов 1 : 500 000 и 1 : 1000 000 в соответствии со стандартами НАТО (ТРС, ОNC) с применением программного обеспечения ArcGIS.

Ключевые слова: цифровая картографическая база данных, геоинформационные системы, геоинформационные технологии, цифровая карта, электронная карта, топографическая карта.

Ph.D. Zhyrov G.B., Ph.D. Lytvynenko N.I., Ph.D. Fedchenko O.P.

FEATURES OF THE INFORMATION STRUCTURE OF THE SPACIOUS BASIS OF DIGITAL CARDOGRAPHIC DATA SHEETS 1 : 500 000 AND 1 : 1 000 000, CREATED BY THE TOPOGRAPHIC SERVICE OF THE ARMED FORCES OF UKRAINE

In recent years, the need for information about the terrain is no longer satisfied with the using of only topographic maps in paper form. The lack of informativeness of the map, the lack of employees from different departments who dom't has the appropriate education, the ability to read the map complicate its use, and in some cases, even limit its use. For solving a number of the problems, that the automated analysis of the territory state is included, the detailed information about the spatial position of objects in a digital form requires.

To date, the most of the information contains the geographic data that is the important information in the structure of the national security. According to the features of the modern information technology, the location data must be organized in databases. When creating databases, the user seeks to arrange the information by various features, so that if necessary, they can quickly search, analyze and process it. Geographic Information Systems (GIS) that can be used in different fields and can operate at different levels can help in this. The scope of GIS using is very wide. Today it is difficult to imagine the spatial modeling

and analysis of the planning, management, evaluation of the results of many modern information technologies, the study of natural resources, the management of the armed forces and weapons, without the GIS using. Thus, with the helping of GIS, the digital databases are created and used, which are the basis of the digital and electronic terrain maps of different scales.

In this article the information structure of the spatial database of digital map data of scale 1: 500 000, 1: 1 000 000, created by the Topographic Service of the Armed Forces of Ukraine is considered, and its features are determined with the purpose for the further development of the technology for the creation of topographic maps of scale 1: 500 000, 1: 1000,000 according to NATO standards (TPC, ONC) using ArcGIS software.

Keywords: the digital cartographic data, the geoinformation systems, the geoinformation technologies, the digital map, the electronic map, the topographic map.

УДК 004.522

д.т.н., проф. **Мясищев А.А**. (ХмНУ)
д.т.н., с.н.с. **Комарова Л.А.** (НАС им. С.. Попова Одесса)
Грицкий Р.В. (А 3990 Полтава)
Кулик К.В. (А 0796 Ровно)

WEB-SERVER НА ARDUINO С АВТОРИЗАЦИЕЙ И ГРАФИЧЕСКИМ ПРЕДСТАВЛЕНИЕМ ИНФОРМАЦИИ С ДАТЧИКОВ

В работе на базе Arduino Mega и контроллера W5100 построен web-сервер для графического отображения данных удаленного клиента, полученных с датчиков температуры, давления, влажности. Программа сервера написана в среде разработки Arduino IDE. Откорректирована библиотека Ethernet для W5100, которая для Arduino IDE ver. 1.0.3, 1.0.5-r2 приводила к зависанию сервера. Показана возможность использования библиотеки Dygraphs для графической визуализации данных, полученных с помощью датчиков. Написаны скрипты для прорисовки графиков для спроектированного web-сервера. Проанализирована скорость передачи данных с web-сервера Arduino для различных сетевых контроллеров ENC28J60, W5100, W5500 для среды программирования Arduino IDE и библиотек UIPEthernet, Ethernet, Ethernet2. Показано, что с наименьшей скоростью данные передаются web-сервером с контроллером ENC28J60 - 3.3КБайт/с, с наибольшим контроллером W5500 - 23.4Кбайт/с. Отмечено, что эти сервера не поддерживают многопоточную работу. Поэтому они не могут быть использованы для создания миниатюрных универсальных web-серверов для обработки нескольких запросов одновременно. Рассмотренный в работе сервер может обслуживать только один запрос от одного удаленного клиента. Проанализированы скоростные параметры передачи данных для сервера на микроконтроллере ATmega328p(Arduino UNO) с контроллером сети ENC28J60. Программа сервера реализована на языке Си в среде программирования AVR Studio. Отмечена высокая скорость передачи данных - 140КБайт/с и возможность многопоточной работы. Установлено, что при одновременной передачи трех файлов разным клиентам суммарная скорость передачи достигает 120-130КБайт/с, а для каждого клиента 40-50КБайт/с. Показано, что использование такого сервера для решения задачи графического представления данных с датчиков затруднено вследствие сложности переноса программного обеспечения на другие микроконтроллеры и ограниченностью библиотеки для работы с картой microSD. Эксплуатация разработанного здесь сервера в течении трех лет показала высокую надежность его работы.

В работе рассмотрено создание web-сервера на Arduino, который имеет модернизированную HTTP basic authentication. Модернизация состоит в том, что для авторизации используется пароль из списка паролей, который выбирается пользователем на основании ключа, пересылаемого сервером. При каждом новом входе на сервер предыдущий пароль становиться недействительным. Представлен практический пример web-сервера на Arduino Mega, контроллерами Ethernet: enc28j60 и w5500.

Ключевые слова: микроконтроллер, ENC28J60, W5100, W5500, Arduino Mega, Arduino UNO, ATmega2560, библиотека Dygraphs, AVR Studio, base64-encoded, basic authentication.

Постановка проблеми. Для управления удаленными объектами часто требуется не только получать детальную информацию с множества датчиков, но и отслеживать текущее состояние системы, динамику изменения состояния системы в течении заданного промежутка времени. Для решения такой задачи удобно использовать графическое представление величин, снимаемых с различных датчиков. Поскольку датчики находятся на удаленных объектах, наиболее дешевым решением является использование web-сервера на Arduino, к которому подключены необходимые датчики и который имеет доступ к сети Интернет. Со стороны клиента удобно использование браузера, который формирует графическое представление массива полученных данных с удаленного датчика. Для формирования графиков с сервера требуется пересылать достаточно большой объем информации. Т.е. кроме массива данных, накопленных с датчиков, пересылается программное обеспечение для браузера, которое позволяет браузеру формировать графики. Это требует, чтобы сервер Ардуино мог пересылать через Интернет не один пакет данных, а множество с приемлемой скоростью. Например, для формирования месячного графика температуры с интервалом 5 минут необходимо передать браузеру массив

данных размером примерно 200КБайт. Программа для формирования графика имеет размер примерно 125КБайт, которая должна быть передана с массивом данных. Таким образом для построения одного месячного графика web-серверу Ардуино требуется передать примерно 325КБайт информации.

С появлением технологий удаленного управления оборудованием через сеть Интернет с помощью микроконтроллеров (Ардуино) актуальной также стала задача авторизации на управляющих серверах. Однако в отличие от современных компьютеров Ардуино имеют скромные вычислительные ресурсы в связи с чем не в состоянии поддерживать полноценные сетевые протоколы, не говоря уже о программном обеспечении, обеспечивающих шифрование данных в пакетах. Несмотря на это рассмотрим возможность упрощенной удаленной авторизации на сервере Arduino. Для этого воспользуемся технологией HTTP authentication, описанной в стандартах HTTP 1.0/1.1.

Анализ последних исследований и публикаций. Решению задачи построения web-сервера на микроконтроллерах уделялось много внимания особенно с появлением первого аппаратного контроллера сети Ethernet 10Base-T - микросхемы enc28j60 [1-9]. Первая практическая работа по созданию такого сервера представлена в работе [8]. Однако этот сервер мог пересылать только один пакет, выполняя удаленное включение, выключение нескольких устройств. В этом проекте использовались микроконтроллеры avr - atmega88, atmega168 со скромными ресурсами. В 2011г. появилась работа [2] в которой был представлен модернизированный протокол tcp/ip, позволяющий с использованием микросхемы enc28j60 и микроконтроллера atmega328p создать web-сервер с многопотоковым режимом работы, пересылающий множество пакетов с высокой скоростью (до 140кбайт/с). Подключение карты microSD позволяло использовать этот микроконтроллер для создания web-сервера, содержащего достаточно большой объем статических html станиц с фотографиями. Дальнейшее развитие получил web-сервер на базе микроконтроллера atmega2560 и контроллера сети w5100(w5500) [10-14]. Однако эти сервера до настоящего времени не в состоянии были отображать графическое представление показаний датчиков. С появлением библиотеки Dygraphs[3,7], эффективных библиотек Ethernet.h, Ethernet2.h[10-12] среды Arduino IDE позволили создать web-сервер на базе atmega2560 для формирования графического представления. Однако малые ресурсы микроконтроллеров не позволяют создать авторизированный вход на web-сервер. В работе [16] рассматривалась попытка создания доступа по паролю с использованием GET, POST запросов. А в работе [15-19] - авторизация с использованием схемы basic. Однако использование нешифрованного протокола HTTP позволяло легко перехватить используемые логин и пароль с помощью программ - снифферов.

Цель работы - разработка аппаратных и программных средств, реализующих web-сервер на базе микроконтроллеров avr с авторизацией доступа по циклически меняющимся паролям и графическим представлением информации с датчиков через сеть Интернет.

Основной материал исследований. Предположим, что канал Интернет имеет пропускную способность 4Мбит/с - 500КБайт/с (например, самая низкая скорость подключенного к телефонной линии цифрового модема). Рассмотрим скорость передачи данных web-серверами Ардуино, построенные на наиболее распространенных и доступных сетевых контроллерах и библиотеках к ним.

На рисунке 1 представлены фото контроллеров Ethernet с микросхемами: ENC28J60, W5100, W5500.

Рисунок 1 – Контроллеры Ethernet ENC28J60, W5100, W5500

На рис. 2 представлены стенды исследуемых web-серверов Arduino Mega с установленными, показанными выше, контроллерами сети.

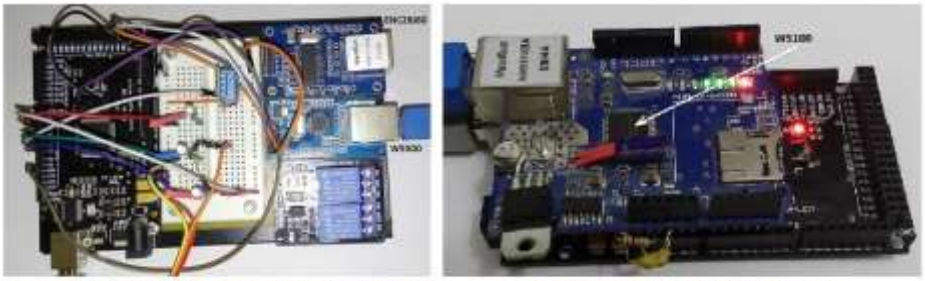


Рисунок 2 – Web-сервера Arduino Mega с сетевыми контроллерами ENC28J60, W5100, W5500

Для определения скоростей передачи данных использовалась программа универсального web-сервера, представленная в источнике [1]. Эта программа по запросу браузера считывает html документы с карты microSD и передает их клиенту. Причем сервер корректно работает как с текстовыми документами, так и с изображениями и исполняемыми файлами. На рисунке 3 показаны скоростные диаграммы работы серверов. Для работы с сетевыми контроллерами в среде Arduino IDE использовались популярные библиотеки UIPEthernet (ENC28J60), Ethernet (W5100) и Ethernet2 (W5500).

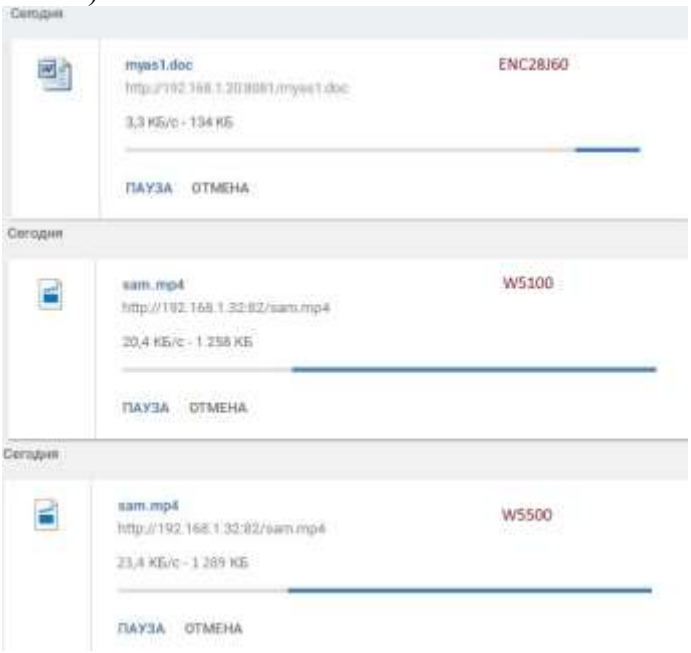


Рисунок 3 – Скоростные диаграммы работы серверов для разных контроллеров сети

Из рис. 3 видно, что максимальная скорость передачи данных 23.4Кбайт/с соответствует контроллеру W5500, минимальная 3.3Кбайт/с - контроллеру ENC28J60. Сервер Arduino с контроллером W5500 на передачу данных для формирования месячного графика потратит 325/23.4 = 13.9 секунд. Недостатком серверов с указанными библиотеками является то, что они работают только с одним потоком данных. Т.е. одновременно копировать с них два файла (например, текст и рисунок) не получиться. Второй файл будет ожидать очереди, пока первый полностью не будет скопирован. Также опыт показал, что библиотека Ethernet для W5100, поставляемая с Arduino IDE ver. 1.0.5-r2 работает некорректно, сервер зависает, поэтому в работе ниже будет дана корректировка этой библиотеки. В последних версиях Arduino IDE (например, ver. 1.8.6.) ошибка исправлена и сервер работает устойчиво, но также не поддерживает многопоточной работы, а скорость передачи данных несколько ниже, чем в исправленной библиотеки Ethernet.

Рассмотрим еще один проект web-сервера на Arduino. Он реализован в среде программирования AVR Studio на языке С. Здесь используется микроконтроллер ATmega328p (Arduino UNO, Arduino Nano) и контроллер сети ENC28J60. Технология его работы и программное обеспечение подробно описаны в работе [2]. На рисунке 4 показана фотография воспроизведенного из источника [2] сервера, который использует контроллер Arduino UNO.

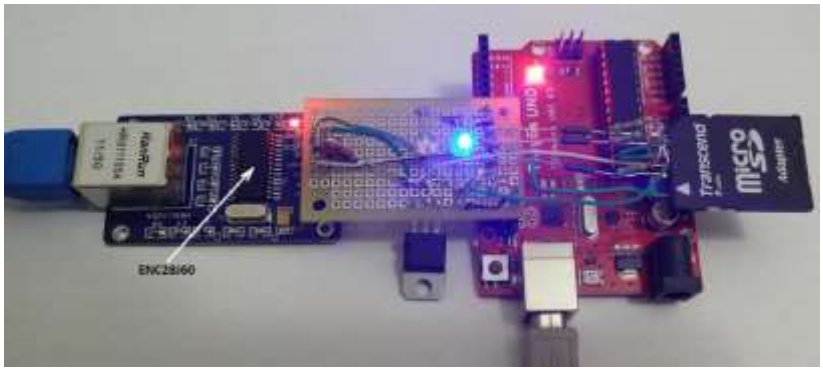


Рисунок 4 – Web - сервер на базе Arduino UNO и ENC28J60

На рис. 5 показаны скоростные диаграммы работы этого сервера. Видно, что он допускает многопоточную обработку, а скорость одного потока достигает 140Кбайт/с. Причем, максимальное количество потоков устанавливается программным путем. Поэтому этот сервер является наиболее подходящим для решения задачи графического представления массива данных, накопленного на карте microSD. Может также быть использован в качестве универсального миниатюрного web-сервера для пересылки html документов с карты microSD и управления оборудованием.

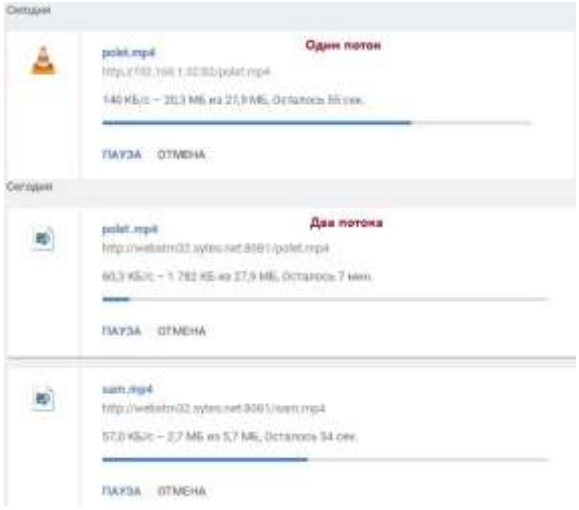


Рисунок 5 – Скоростные диаграммы работы многопоточного сервера Arduino UNO

В данной работе для построения сервера для графического представления данных будут использоваться Arduino Mega с контроллером ATmega2560, контроллер сети W5100, среда разработки Arduino IDE ver. 1.0.3, 1.0.5-r2 с модернизированной библиотекой Ethernet для W5100. Такой сервер позволит формировать недельные графики с временем ожидания примерно 15-20 секунд. Более предпочтительным является сервер, представленный на рисунке 4, однако программирование его для задач с дополнительными серверными функциями является более сложно задачей, чем создание сервера на основе библиотек, включенных в состав среды программирования Arduino IDE. Дополнительно к этому сервер на рис. 4 написан под конкретный микроконтроллер и переход к другой модели требует изменения кода, а библиотека для работы с картами microSD поддерживает только формат карт SD (до 2Гбайт), которые в настоящее время не выпускаются. Например, microSD карты формата SDHC, имеющие емкость 8 и более Гбайт, не поддерживаются.

Использование сервера с контроллером сети W5100 связана с тем, что используется простая и отработанная универсальная среда разработки Arduino IDE, встроенная библиотека для работы с картами microSD (поддерживает формат SDHC), откорректированная устойчиво работающая библиотека Ethernet, относительно небольшой объем пересылаемых данных. В случае необходимости пересылки большого объема информации целесообразно использовать сервер, представленный на рис. 4 и описанный в работе [2].

На рис. 6 представлен экспериментальный стенд работающего сервера, который получает данные с датчиков температуры DS18B20, давления и температуры MS5611, влажности и температуры DHT11, записывает данные на карту microSD каждые 300 сек. и пересылает все записанные данные при запросе конкретного массива данных браузеру клиента вместе с программой dygraph (java-скрипт), которая запускается браузером и формирует график.

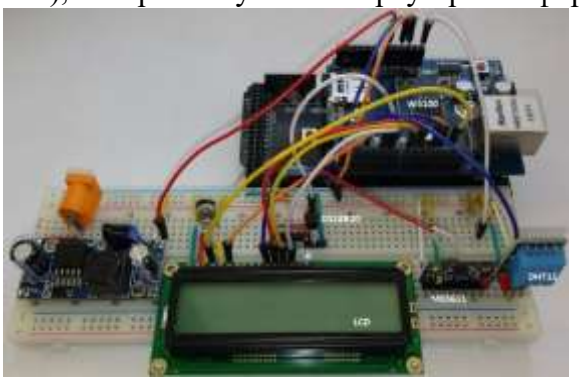


Рисунок 6 – Экспериментальный стенд web-сервера для формирования графиков

Рассмотренный сервер использует библиотеку dygraph [3], и формирует графики температуры вне помещения (DS18B20), внутри помещения (MS5611), атмосферного давления (MS5611) и влажности воздуха (DHT11). Web - server позволяет формировать графики в течении 3-х суток. Для этого существует страничка "текущие показания датчиков, настройки" в которой устанавливается время и 3-и последовательные даты, для которых требуются графики. После 3-х суток в файлы данных информация с датчиков заноситься не будет. Так как данные с датчиков добавляются в файлы, то после перегрузки сервера можно внести следующие последовательные 3-и даты. Таким образом на графиках будет отображено еще дополнительно трое суток. Для построения новых графиков необходимо карту microSD переставить на компьютер и удалить данные с файлов datat.txt, datata.txt, datap.txt, datah.txt, содержимое которых будет рассмотрено ниже. На рис. 7 представлены интерфейсы главной страницы сервера, график температуры вне помещения и текущие показания датчиков с установкой времени и даты.

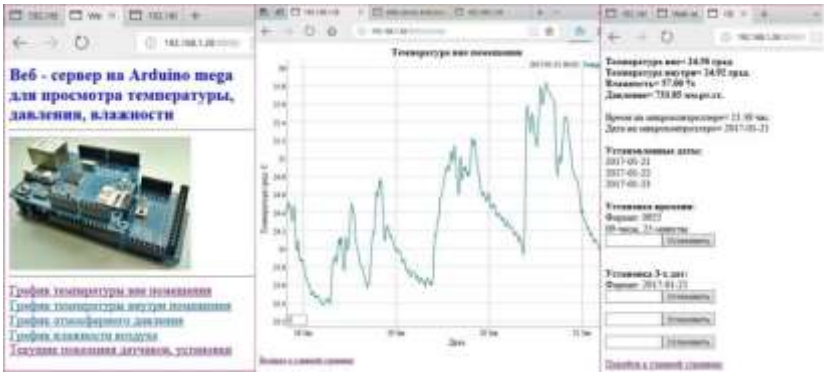


Рисунок 7 – Интерфейсы главной страницы сервера, график температуры вне помещения и текущие показания датчиков с установкой времени и даты

Рассмотрим принцип работы сервера, выполняющего визуализацию графиков. При запросе клиента по адресу сервера(http://192.168.1.38:9000), сервер обращается к microSD карте и считывает файл index.htm, который пересылается браузеру. При переходе по ссылке, например http://192.168.1.38:9000/in0.htm, сервер считывает файл in0.htm с microSD и пересылает

этот html документ браузеру, который его исполняет. Исключение составляет переход по ссылке http://192.168.1.38:9000/temp. В этом случае открывается страничка, которая представляет текущие показания датчиков с установкой времени и даты (рис.7). Данные с microSD для этой ссылки не считываются.

Dygraphs - это библиотека, подключаемая к любой программе (скрипту), написанной на языке JavaScript. Таким образом HTML-документ превращается в инструмент графической визуализации. Для этого необходимо подключить библиотеку к скрипту и создать объект Dygraph в соответствии с правилами языка. Каждый такой объект в общем случае представляет собой диаграмму, обладающую соответствующими признаками – легендой, наименованиями осей и т.д. Скрипт с библиотекой, которые находятся на браузере, запрашивают набор данных в виде файла в формате CSV с сервера при помощи запроса XHR. Обозначение параметров на графике выбирается со скрипта. Если прорисовывается несколько кривых на графике, то цвет линий выбирается библиотекой автоматически так, чтобы визуально кривые отличались друг от друга. Обозначения по оси X будут меняться при масштабировании - например, если по умолчанию по оси аргументов идут месяцы года, то при увеличении диаграммы будут появляться сначала недели месяца, а затем дни и потом часы. Для правильного функционирования библиотеки Dygraphs на карте microSD сервера должны присутствовать следующие файлы:

1. index.htm

```
<HTML>
<HEAD>
 <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
 <TITLE>Web server Arduino w5100</TITLE>
</HEAD>
<BODY>
<B><FONT color=blue size="5">Веб - сервер на Arduino mega<br> для просмотра температуры,<br> давления, влажности</FONT></B>
<hr>
<a href="web_gr.jpg"><img src="web3.JPG"/></a>
<hr>
<FONT  size="4"><A href="in0.htm">График температуры вне помещения</A></FONT>
<br><FONT  size="4"><A  href="in1.htm">График температуры внутри помещения</A></FONT>
<br><FONT  size="4"><A href="in2.htm">График атмосферного давления</A></FONT>
<br><FONT  size="4"><A href="in3.htm">График влажности воздуха</A></FONT>
<br><FONT  size="4"><A  href="temp">Текущие показания датчиков, установки</A></FONT>
</body>
</html>
```

2. in0.htm

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
<script type="text/javascript"
 src="dygm.js"></script>
```

```
<link rel="stylesheet" href="dygraph.css">
</head>
<body>
<div id="graphdiv2"
  style="width:800px; height:600px;"></div>
<script type="text/javascript">
  g2 = new Dygraph(
    document.getElementById("graphdiv2"),
    "DATAT.TXT", // path to CSV file
    {
title: 'Температура вне помещения',
xlabel: 'Дата',
ylabel: 'Температура град. С',
showRoller: true,
rollPeriod: 5,
//color: "#0000ff",
labels: [ "Date", "Temp" ],
strokeWidth: 1.5
}
  );
</script>
<br>
<A href="/">Возврат к главной странице</A>
</body>
</html>
```

3. in1.htm - скрипт для формирования графика температуры внутри помещения, аналогичный in0.htm

4. in2.htm - скрипт для формирования графика атмосферного давления, аналогичный in0.htm

5. in3.htm - скрипт для формирования графика относительной влажности воздуха, аналогичный in0.htm

6. dygraph.min.js - файл библиотеки dygraphs (переименован в dygm.js, так как имя файла должно быть не более 8 символов, расширение - не более 3-х символов в файловой системе FAT)

7. dygraph.css - файл библиотеки dygraphs

8. Файлы данных показаний датчиков, представленных в таблице 1. Эти файлы при первом включении сервера создаются автоматически. В них могут дописываться данные при повторном включении сервера, поэтому график будет продолжаться. Например, если сервер возобновит работу через 10 дней, то эти дни будут отображены графиком в виде прямой линии, соединяющей конец предыдущей кривой с началом следующей.

При включении сервера и последующей его работе каждые 5 минут в файлы datat.txt, datata.txt, datap.txt, datah.txt записываются построчно данные, как представлено в таблице 1.

Таблица 1

DATAT.TXT	DATATA.TXT	DATAP.TXT	DATAH.TXT
2017-01-17 20: 4, 24.56	2017-01-17 20: 4, 24.92	2017-01-17 20: 5, 722.4	2017-01-17 20: 5, 40
2017-01-17 20: 9, 24.56	2017-01-17 20: 9, 24.89	2017-01-17 20: 9, 722.4	2017-01-17 20:10, 40
2017-01-17 20:14, 24.44	2017-01-17 20:14, 24.84	2017-01-17 20:14, 722.3	2017-01-17 20:15, 40
2017-01-17 20:19, 24.50	2017-01-17 20:19, 24.87	2017-01-17 20:19, 722.3	2017-01-17 20:20, 41
2017-01-17 20:24, 24.44	2017-01-17 20:24, 24.86	2017-01-17 20:24, 722.3	2017-01-17 20:25, 41
2017-01-17 20:29, 24.44	2017-01-17 20:29, 24.82	2017-01-17 20:29, 722.3	2017-01-17 20:30, 41
...	...	...	...

В эти файлы пишутся дата вдоль оси X, температура вне помещения(datat.txt), температура внутри помещения(datata.txt), атмосферное давление в мм.рт.ст.(datap.txt), относительная влажность в %(datah.txt) по оси Y.

Программа сервера с подключенным к нему LCD индикатором для отображения текущего состояния датчиков, представлена в источнике [4].

Программа работает следующим образом.

1. Каждую секунде идет обращение к функции прерывания ISR (TIMER5_COMPA_vect), реализующую работу часов. Она вычисляет минуты, часы, дни и рассчитывает дополнительные параметры, которые позволяют корректно отрабатывать некоторые временные фрагменты программы.

2. В цикле loop() выполняются следующие действия:

2.1.Выполняется запись данных на карту microSD. Например для датчика температуры вне помещения запись на microSD выполняется следующими операторами:

```
if( time==299 && endn==0 && endgraf==0 ) // При совпадении времени пишем в файл каждые 300 сек. и так до достижении 24 часов 3-го дня
 { endn=1; // Чтобы была только 1 запись при time=299
   myFile1 = SD.open("datat.txt", FILE_WRITE);
   if (myFile1) {  sensors.requestTemperatures(); cel=sensors.getTempCByIndex(0);
    dtostrf(cel,6,2,celbuf);  dtostrf(ho,2,0,hobuf);  dtostrf(mi,2,0,mibuf);
      if(day==0) myFile1.print(fd0);  else if(day==1) myFile1.print(fd1);
       else if(day==2) myFile1.print(fd2);  myFile1.print(" ");
        myFile1.print(hobuf); myFile1.print(":"); myFile1.print(mibuf);
        myFile1.print(","); myFile1.println(celbuf);
    myFile1.close();  } ...  }
```

2.2. Открывается сетевое соединение (socket) и прослушивается. Если соединение установлено (ESTABLISHMENT), определяется длина поля данных пакета TCP. Если длина равна нулю и так 25 раз подряд, срочно принудительно на сервере закрывается соединение, иначе контроллер W5100 "зависнет" (вероятно аппаратная ошибка). После этого опять открывается соединение и так до тех пор, пока длина поля данных не будет больше нуля. Далее идет считывание заголовка, посылаемого браузером до достижения пустой строки, которая определяет конец заголовка при запросе GET. Если первой строкой заголовка является строка

GET / HTTP/1.1

то данные считываются с карты microSD с файла index.htm и пересылаются браузеру в виде html документа.

Если первой строкой являются строки

GET /temp?c= HTTP/1.1, GET /temp?d= HTTP/1.1

то выполняется распознавание времени и 1-й даты при их вводе в форму следующими операторами:

```
   if(strstr(clientline, "GET /temp?c=") !=0) {  // Распознаем время
  fh[0]=clientline[12]; fh[1]=clientline[13]; fh[2]=0;
  fm[0]=clientline[14]; fm[1]=clientline[15]; fm[2]=0;  ho=atoi(fh); mi=atoi(fm);
 }
    if(strstr(clientline, "GET /temp?d=") !=0) {  // Распознаем 1-ю дату
  fd0[0]=clientline[12]; fd0[1]=clientline[13]; fd0[2]=clientline[14];fd0[3]=clientline[15];
```

fd0[4]=clientline[16]; fd0[5]=clientline[17]; fd0[6]=clientline[18];fd0[7]=clientline[19];
fd0[8]=clientline[20]; fd0[9]=clientline[21];fd0[10]=0; }

Если первой строкой является строка

GET /temp HTTP/1.1

то на в окне браузера распечатываются текущие показания датчиков, формы ввода времени и даты (рис. 7). Программа содержит также функцию meter(), которая распечатывает на экране LCD сервера текущие показания датчиков, обновляемые каждые 18 секунд.

Для предотвращения "зависания" сервера стандартная библиотека Ethernet в Arduino IDE ver. 1.0.3, 1.0.5-r2 была откорректирована. В источнике [5] подробно рассматривается содержимое измененных файлов:

socket.cpp, EthernetClient.cpp, EthernetClient.h.

Внесены изменение в функцию *void EthernetClient::stop() - (client.stop())* для файла *EthernetClient.c*.

Рассмотрим HTTP authentication. Применительно к web-сайтам он работает следующим образом:

1. Сервер, при обращении неавторизованного клиента к защищенному ресурсу, отсылает HTTP статус “401 Unauthorized” и добавляет заголовок “WWW-Authenticate” с указанием схемы и параметров аутентификации.

2. Браузер, при получении такого ответа, автоматически показывает диалог ввода username и password. Пользователь вводит детали своей учетной записи.

3. Сервер аутентифицирует пользователя по данным из этого заголовка.

Весь процесс стандартизирован и поддерживается всеми браузерами и web-серверами. Существует несколько схем аутентификации. Для случая сервера на Ардуино рассмотрим Basic. Здесь username и password пользователя передаются в заголовке Authorization в незашифрованном виде (base64-encoded).

Рассмотрим схему аутентификации basic, и впоследствии модифицируем ее для веб-сервера Arduino. Механизм авторизации выглядит следующим образом. Сначала при запросе на подключение к серверу Arduino браузер посылает заголовок без запроса авторизации:

GET / HTTP/1.1
Host: 192.168.1.18:81
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/*;q=0.8*
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/44.4.2403.3 Amigo/44.4.2403.3 MRCHROME SOC Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4

Сервер Ардуино отвечает браузеру заголовком на необходимость запроса с авторизацией:

HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="Arduino - HOME"

Браузер Amigo посылает серверу запрос но уже с авторизацией:

GET / HTTP/1.1
Host: 192.168.1.18:81
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic ***YWxleDoxMzY=***
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/*;q=0.8*

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/44.4.2403.3 Amigo/44.4.2403.3 MRCHROME SOC Safari/537.36

Accept-Encoding: gzip, deflate, sdch

Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4

Сервер Arduino посылает ответ и после пустой строки html документ

HTTP/1.0 200 OK

Content-Type: text/html

<Здесь идет передача браузеру html документа>

YWxleDoxMzY= -это закодированный в Base64 набор символов alex:136 (alex - это login, 136 - password, которые вводятся в выскакивающем у браузере окне авторизации). На рисунке 8 представлены интерфейсы ввода логина и пароля и ответа сервера Arduino. Программа сервера Ардуино с описанной авторизацией представлена в источнике [3]. В этой программе работа сервера по представленной схеме реализуется с помощью операторов:

```
if (readString.lastIndexOf("YWxleDoxMzY=")>-1) {
 if (readString.lastIndexOf("GET /favicon.ico")>-1) {
  client.println("HTTP/1.0 404 Not Found");
 } else html_doc(client); }
else { client.println("HTTP/1.0 401 Unauthorized");
 client.println("WWW-Authenticate: Basic realm=\"Arduino - HOME\"");}
```

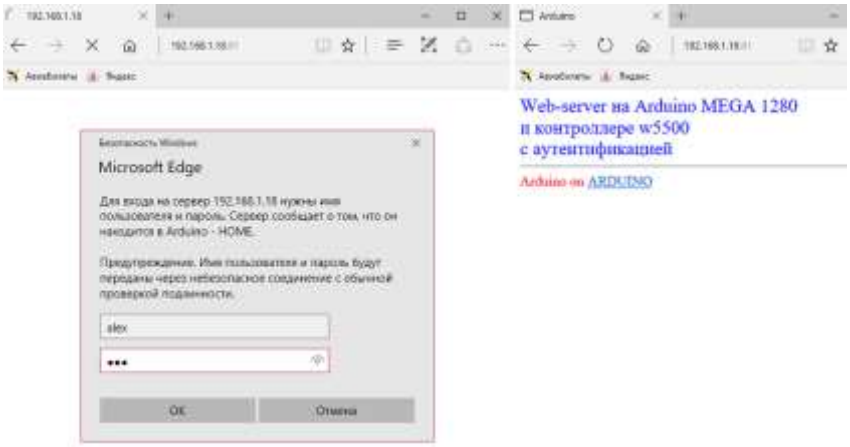


Рисунок 8 – Интерфейса ввода логина и пароля и ответа сервера Arduino

Однако безопасность при этой схеме весьма низкая. Пакеты по Интернет передаются в открытом виде, поэтому закодированный логин и пароль (YWxleDoxMzY=) можно легко выловить с помощью программ снифферов и раскодировать с помощью Base64 decode. Модернизируем программу, чтобы в большей степени защитить сервер Ардуино для предотвращения несанкционированного управления им. Для этого создадим список паролей, которые известны пользователю сервера. Причем при каждом новом входе на сервер пароль доступа должен меняться на следующий по списку. Поэтому, если предыдущий пароль будет расшифрован, то он становиться недействительный и злоумышленник не сможет зайти по нему. В источнике [14] представлена программа web-сервера Ардуино, на котором установлены три светодиода, имитирующие включение-выключение 3-х силовых источников питания(например электро-розеток), датчик температуры DS18B20(температура улицы) и датчик влажности и температуры DHT 11 (делает измерения в помещении) или датчик давления и температуры BMP280. Программа использует 3 пары логин: пароль:

1. alex:136; 2. alex:138; 3. alex:140

При каждом новом обращении к серверу пароль циклически меняется на следующий в списке. Для того, чтобы знать следующий номер пароля в браузере выводится параметр index. Его пользователь должен запомнить или определить с помощью открытого входа по адресу http://192.168.1.18:81/index. Таким образом, чем больше паролей в списке, тем более защищенным должен выглядеть сервер. На рисунке 9 представлен интерфейс управления сервером на Arduino Mega.

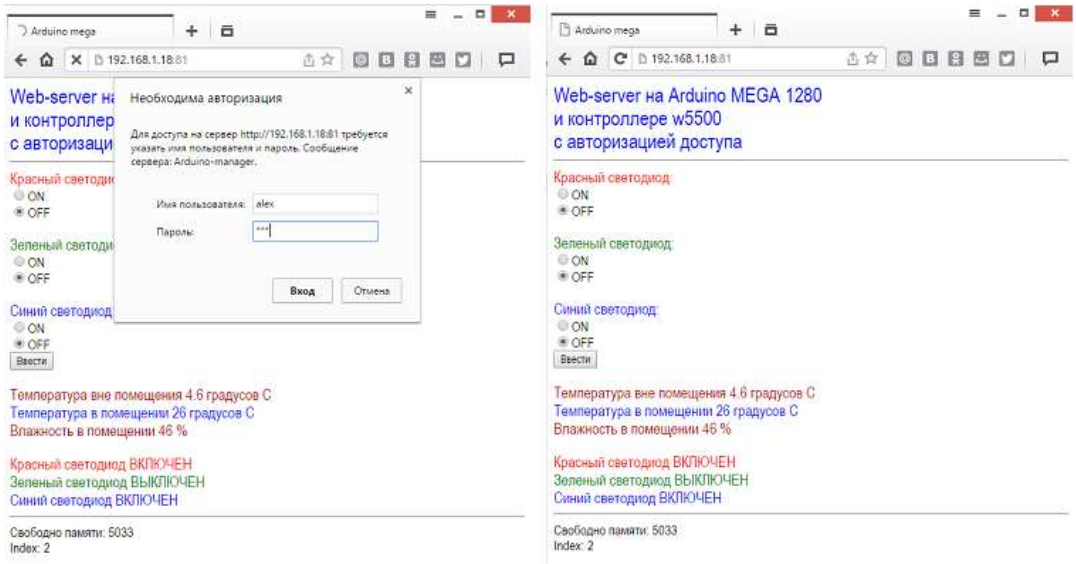


Рисунок 9 – Интерфейс управления web-сервером на Arduino Mega

В представленном интерфейсе Index:2 обозначает то, что при следующем входе на сервер необходимо для авторизации использовать пару alex:138.

Выводы

1. Проанализирована скорость передачи с web-сервера Arduino для различных сетевых контроллеров ENC28J60, W5100, W5500 для среды программирования Arduino IDE[6] и библиотек UIPEthernet, Ethernet, Ethernet2. С наименьшей скоростью данные передаются сервером с контроллером ENC28J60 - 3.3КБайт/с, с наибольшей контроллером W5500 - 23.4Кбайт/с. Отмечено, что эти сервера не поддерживают многопоточную работу.

2. Проанализированы скоростные параметры передачи данных для сервера на микроконтроллере ATmega328p(Arduino UNO) с контроллером сети ENC28J60. Программа сервера реализована на языке Си в среде программирования AVR Studio[2]. Отмечена высокая скорость передачи данных - 140КБайт/с и возможность многопоточной работы.

3. Показана возможность использования библиотеки Dygraphs[3] для графической визуализации данных, полученных с помощью датчиков. Написаны скрипты для прорисовки графиков для спроектированного сервера.

4. На базе Arduino Mega и контроллере W5100 построен web-сервер для графического отображения данных удаленного клиента, полученных с датчиков температуры, давления, влажности. Программа сервера написана в среде разработки Arduino IDE на языке Wiring (C++).

5. Откорректирована библиотека Ethernet для W5100, которая для Arduino IDE ver. 1.0.3, 1.0.5-r2 приводила к зависанию сервера.

6. Показано, что HTTP авторизация Basic передает username и password пользователя в незашифрованном виде (base64-encoded). И если не используется протокол HTTPS (HTTP over SSL), является относительно небезопасной.

7. Представленная в работе модернизация схемы авторизации Basic позволяет относительно безопасно управлять сервером Ардуино, но требует использования нескольких паролей, каждый из которых сообщается сервером пользователю через специальный параметр index.

ЛИТЕРАТУРА:

1. Мясищев А.А. Универсальный web - сервер на Arduino. [Electronic resource]. - Mode of access: http://webstm32.sytes.net/web_1.htm, 2013.

2. Подключение микроконтроллера к локальной сети. [Electronic resource]. - Mode of access: http://we.easyelectronics.ru/electro-and-pc/podklyuchenie-mikrokontrollera-k-lokalnoy-seti.html, 2011.

3. Dan Vanderkam. Dygraphs library. [Electronic resource]. - Mode of access: http://dygraphs.com, 2017.

4. Мясищев А.А. Web-server на Arduino для представления графиков температуры, давления, влажности. [Electronic resource]. - Mode of access: https://sites.google.com/site/webstm32/web_graph, 2018.

5. Мясищев А.А. Управление через Интернет голосовыми командами Web - сервером на Arduino Mega и контроллере W5100 с файлами на SD. [Electronic resource]. - Mode of access: https://sites.google.com/site/webstm32/web_server_speech, 2015.

6. Arduino. Официальный сайт. [Electronic resource]. - Mode of access: https://www.arduino.cc/, 2018.

7. Филлипова Е. Инструменты визуализации данных: Dygraphs. [Electronic resource]. - Mode of access: http://datareview.info/article/instrumentyi-vizualizatsii-dannyih-dygraphs, 2014.

8. Мясищев А.А. Создание надежного http-сервера для удаленного управления по TCP/IP сети на основе ATmega1280 и Wiznet W5100 //Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. - К.ВІКНУ, 2014. - Вип. №46 - С. 59 - 70.

9. ENC28J60 Stand-Alone Ethernet Controller with SPI Interface. [Electronic resource]. - Mode of access: http://ww1.microchip.com/downloads/en/DeviceDoc/39662e.pdf, 2012.

10. W5100 Datasheet. [Electronic resource]. - Mode of access: http://www.hobbytronics.co.uk/datasheets/W5100_Datasheet_v1_1_6.pdf, 2008.

11. W5500 Datasheet Version 1.0.7. [Electronic resource]. - Mode of access: http://wizwiki.net/wiki/lib/exe/fetch.php?media=products:w5500:w5500_ds_v108e.pdf, 2013.

12. Web Server. [Electronic resource]. - Mode of access: https://www.arduino.cc/en/Tutorial/WebServer, 2015.

13. Arduino SD Card Web Server. [Electronic resource]. - Mode of access: https://startingelectronics.org/tutorials/arduino/ethernet-shield-web-server-tutorial/SD-card-web-server/, 2013.

14. Мясищев А.А. Web-server на Arduino MEGA и контроллере сети w5500 с авторизацией доступа для удаленного управления. [Electronic resource]. - Mode of access: https://sites.google.com/site/webstm32/web-server-avtorizaciej, 2018.

15. Анисимов В.В. Криптографические методы защиты информации. [Electronic resource]. - Mode of access: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture, 2012.

16. Мясищев А.А. Авторизация на web-сервере Arduino с помощью GET и POST запросов. Materials of the XIII International scientific and practical Conference Modern scientific potential - 2018 , February 28 - March 7 , 2018 Construction and architecture. Mathematics. Modern information technology. Technical science. Physics. : Sheffield. Science and education LTD c. 36-42

17. Мясищев А.А. WEB-SERVER НА ARDUINO ДЛЯ ГРАФИЧЕСКОГО ПРЕДСТАВЛЕНИЯ ДАННЫХ С ДАТЧИКОВ ЧЕРЕЗ ИНТЕРНЕТ. [Electronic resource]. - Mode of access: https://www.researchgate.net/publication/332257299_WEB-SERVER_NA_ARDUINO_DLA_GRAFICESKOGO_PREDSTAVLENIA_DANNYH_S_DATCIKOV_CEREZ_INTERNET, 2019.

18. HTTP/TCP with an atmega88 microcontroller (AVR web server). Guido Socher. [Electronic resource]. - Mode of access: http://www.tuxgraphics.org/electronics/200611/article06111.shtml, 2006

19. Kitsum. Авторизация на Web сервере микроконтроллера. [Electronic resource]. - Mode of access: https://it4it.club/topic/13-авторизация-на-web-сервере-микроконтроллера/, 2015

REFERENCES:

1. Myasishchev A.A. Universal'nyj web - server na Arduino. [Electronic resource]. - Mode of access: http://webstm32.sytes.net/web_1.htm, 2013.

2. Podklyuchenie mikrokontrollera k lokal'noj seti. [Electronic resource]. - Mode of access: http://we.easyelectronics.ru/electro-and-pc/podklyuchenie-mikrokontrollera-k-lokalnoy-seti.html, 2011.

3. Dan Vanderkam. Dygraphs library. [Electronic resource]. - Mode of access: http://dygraphs.com, 2017.

4. Myasishchev A.A. Web-server na Arduino dlya predstavleniya grafikov temperatury, davleniya, vlazhnosti. [Electronic resource]. - Mode of access: https://sites.google.com/site/webstm32/web_graph, 2018.

5. Myasishchev A.A. Upravlenie cherez Internet golosovymi komandami Web - serverom na Arduino Mega i kontrollere W5100 c fajlami na SD. [Electronic resource]. - Mode of access: https://sites.google.com/site/webstm32/web_server_speech, 2015.

6. Arduino. Oficial'nyj sajt. [Electronic resource]. - Mode of access: https://www.arduino.cc/, 2018.

7. Fillipova E. Instrumenty vizualizacii dannyh: Dygraphs. [Electronic resource]. - Mode of access: http://datareview.info/article/instrumentyi-vizualizatsii-dannyih-dygraphs, 2014.

8. Myasishchev A.A. Sozdanie nadezhnogo http-servera dlya udalennogo upravleniya po TCP/IP seti na osnove ATmega1280 i Wiznet W5100 //Zbirnik naukovih prac' Vijs'kovogo institutu Kiïvs'kogo nacional'nogo universitetu imeni Tarasa SHevchenka. - K.VIKNU, 2014. - Vip. №46 - S. 59 - 70.

9. ENC28J60 Stand-Alone Ethernet Controller with SPI Interface. [Electronic resource]. - Mode of access: http://ww1.microchip.com/downloads/en/DeviceDoc/39662e.pdf, 2012.

10. W5100 Datasheet. [Electronic resource]. - Mode of access: http://www.hobbytronics.co.uk/datasheets/W5100_Datasheet_v1_1_6.pdf, 2008.

11. W5500 Datasheet Version 1.0.7. [Electronic resource]. - Mode of access: http://wizwiki.net/wiki/lib/exe/fetch.php?media=products:w5500:w5500_ds_v108e.pdf, 2013.

12. Web Server. [Electronic resource]. - Mode of access: https://www.arduino.cc/en/Tutorial/WebServer, 2015.

13. Arduino SD Card Web Server. [Electronic resource]. - Mode of access: https://startingelectronics.org/tutorials/arduino/ethernet-shield-web-server-tutorial/SD-card-web-server/, 2013.

14. Myasischev A.A. Web-server na Arduino MEGA i kontrollere seti w5500 s avtorizatsiey dostupa dlya udalennogo upravleniya. [Electronic resource]. - Mode of access: https://sites.google.com/site/webstm32/web-server-avtorizaciej, 2018.

15. Anisimov V.V. Kriptograficheskie metodyi zaschityi informatsii. [Electronic resource]. - Mode of access: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture, 2012.

16. Myasischev A.A. Avtorizatsiya na web-servere Arduino s pomoschyu GET i POST zaprosov. Materials of the XIII International scientific and practical Conference Modern scientific potential - 2018 , February 28 - March 7 , 2018 Construction and architecture. Mathematics. Modern information technology. Technical science. Physics. : Sheffield. Science and education LTD s. 36-42

17. Myasischev A.A. WEB-server na ARDUINO dlya graficheskogo predstavleniya dannyih s datchikov cherez internet. [Electronic resource]. - Mode of access: https://www.researchgate.net/publication/332257299_WEB-server_na_ARDUINO_dla_graficeskogo_predstavlenia_dannyh_s_datcikov_cerez_internet, 2019.

18. HTTP/TCP with an atmega88 microcontroller (AVR web server). Guido Socher. [Electronic resource]. - Mode of access: http://www.tuxgraphics.org/electronics/200611/article06111.shtml, 2006

19. Kitsum. Avtorizatsiya na Web servere mikrokontrollera. [Electronic resource]. - Mode of access: https://it4it.club/topic/13-avtorizatsiya-na-web-servere-mikrokontrollera/, 2015

д.т.н., проф. Мясіщев О.А., д.т.н., с.н.с. Комарова Л.О., Грицький Р.В., Кулік К.В.

WEB-SERVER НА ARDUINO З АВТОРИЗАЦІЄЮ І ГРАФІЧНИМ ПРЕДСТАВЛЕННЯМ ІНФОРМАЦІЇ З ДАТЧИКІВ

У роботі на базі Arduino Mega і контролера W5100 побудований web-сервер для графічного відображення даних віддаленого клієнта, отриманих з датчиків температури, тиску, вологості. Програма сервера написана в середовищі розробки Arduino IDE. Відкоригована бібліотека Ethernet для W5100, яка для Arduino IDE ver. 1.0.3, 1.0.5-r2 приводила до зависання сервера. Показана можливість використання бібліотеки Dygraphs для графічної візуалізації даних, отриманих за допомогою датчиків. Написані скрипти для промальовування графіків для спроектованого web-сервера. Проаналізовано швидкість передачі даних з web-сервера Arduino для різних мережевих контролерів ENC28J60, W5100, W5500 для середовища програмування Arduino IDE і бібліотек UIPEthernet, Ethernet, Ethernet2. Показано, що з найменшою швидкістю дані передаються web-сервером з контролером ENC28J60 - 3.3КБайт/с, з найбільшою контролером W5500 - 23.4Кбайт / с. Відзначено, що ці сервера не підтримують багатопотокову роботу. Тому вони не можуть бути використані для створення мініатюрних універсальних web-серверів для обробки декількох запитів одночасно. Розглянутий в роботі сервер може обслуговувати тільки один запит від одного віддаленого клієнта. Проаналізовано швидкісні параметри передачі даних для сервера на мікроконтролері

ATmega328p (Arduino UNO) з контролером мережі ENC28J60. Програма сервера реалізована на мові Сі в середовищі програмування AVR Studio. Відзначено високу швидкість передачі даних - 140КБайт/с і можливість багатопотокового режиму роботи. Встановлено, що при одночасній передачі трьох файлів різним клієнтам сумарна швидкість передачі досягає 120-130КБайт / с, а для кожного клієнта 40-50КБайт/с. Показано, що використання такого сервера для вирішення завдання графічного представлення даних з датчиків ускладнено внаслідок складності перенесення програмного забезпечення на інші мікроконтролери і обмеженістю бібліотеки для роботи з картою microSD. Експлуатація розробленого тут сервера в перебігу трьох років показала високу надійність його роботи.

В роботі розглянуто створення web-сервера на Arduino, який має модернізовану HTTP basic authentication. Модернізація полягає в тому, що для авторизації використовується пароль зі списку паролів, який вибирається користувачем на підставі ключа, який пересилається сервером. При кожному новому вході на сервер попередній пароль ставати недійсним. Представлений практичний приклад web-сервера на Arduino Mega, контролерами Ethernet: enc28j60 і w5500.

Ключові слова: мікроконтролер, ENC28J60, W5100, W5500, Arduino Mega, Arduino UNO, ATmega2560, бібліотека Dygraphs, AVR Studio, base64-encoded, basic authentication.

Prof. Myasischev A.A., Prof Komarova L.O., Gritsky R.V., Kulik K.V.

WEB SERVER ON ARDUINO WITH AUTHORIZATION AND GRAPHIC REPRESENTATION OF INFORMATION FROM SENSORS

In the work on the basis of Arduino Mega and the W5100 controller, a web server is built for graphical display of remote client data obtained from temperature, pressure, humidity sensors. The server program is written in the Arduino IDE development environment. The Ethernet library for the W5100 has been updated, which for Arduino IDE ver. 1.0.3, 1.0.5-r2 caused the server to hang. The possibility of using the Dygraphs library for graphical visualization of data obtained with sensors is shown. Written scripts for drawing graphics for the projected web server. The data transfer rate from the Arduino web server for various network controllers ENC28J60, W5100, W5500 for the Arduino IDE programming environment and UIPEthernet, Ethernet, Ethernet2 libraries was analyzed. It is shown that with the lowest speed the data is transmitted by the web server with the ENC28J60 controller - 3.3Kb/s, with the largest controller W5500 - 23.4Kbytes/s. It is noted that these servers do not support multithreaded work. Therefore, they can not be used to create miniature universal web servers for processing multiple requests simultaneously. The server considered in the work can serve only one request from one remote client. The speed parameters of data transfer for the server on the ATmega328p microcontroller (Arduino UNO) with the network controller ENC28J60 are analyzed. The server program is implemented in C language in the AVR Studio programming environment. A high data transfer rate of 140Kb/s and a possibility of multithreading are noted. It is established that with simultaneous transmission of three files to different clients, the total transmission speed reaches 120-130Kb/s, and for each client 40-50Kb/s. It is shown that the use of such a server to solve the problem of graphical representation of data from sensors is difficult due to the complexity of transferring software to other microcontrollers and the limited library for working with a microSD card. The operation of the server developed here for three years has shown high reliability of its operation.

The paper discusses the creation of a web server on the Arduino, which is a modernized HTTP basic authentication. The upgrade consists in the fact that for authorization a password is used from the list of passwords that is selected by the user on the basis of the key sent by the server. With each new login to the server, the previous password becomes invalid. Presents a practical example of a web server on Arduino Mega, Ethernet controllers: enc28j60 and w5500.

Keywords: microcontroller, ENC28J60, W5100, W5500, Arduino Mega, Arduino UNO, ATmega2560, Dygraphs library, AVR Studio, base64-encoded, basic authentication.

УДК 004.891

д.т.н., с.н.с. **Сєлюков О.В.** (ТОВ «Укрспецконсалтинг»)
к.т.н., доц. **Хмельницький Ю.В.** (ХмНУ)
Ковпа Д.М. (ХмНУ)
Лісовський О.С. (ХмНУ)

АНАЛІЗ МОДЕЛЕЙ ТА ПРОГНОЗУВАННЯ РИЗИКІВ ФУНКЦІОНУВАННЯ СИСТЕМИ УПРАВЛІННЯ SDN АРХІТЕКТУРИ

У статті розглянуто питання аналізу моделей та алгоритмів функціонування системи управління SDN архітектури для забезпечення більш якісної роботи мережі. Велика різнорідність самої апаратної реалізації пристроїв передачі даних SDN архітектури призводить до того, що різні комутатори можуть не підтримувати деякі функції чи підтримувати їх із обмеженою продуктивністю. У процесі роботи мережі це може суттєво вплинути на пропускну здатність окремих потоків передачі даних чи цілих доменів мережі. Маршрутизація потоків передачі здійснюється за критерієм якості обслуговування та за критерієм рівномірного завантаження мережевих ресурсів мережі. Підвищення якості обслуговування здійснюється із врахуванням класифікації потоку передачі, що досить обмежує можливість управління потоком даних. Більшість моделей таких мереж не враховують характеристик мультисервісного потоку даних, що призводить до погіршення якості обслуговування та підвищення ймовірності блокування каналів передачі мережі. Відсутність можливості здійснювати диференційоване управління для окремих потоків даних окремих клієнтів мережі та врахувати їхні вимоги щодо якості, призводить до низької ефективності каналу маршрутизації, неоптимального розподілу навантаження мережі, погіршення якості обслуговування високо пріоритетних потоків даних. Засоби контролю за процесом передачі окремих потоків передачі даних відсутні, внаслідок чого система управління не має змогу визначити погіршення обслуговування для цих потоків даних, а тому не зможе гарантувати необхідний рівень управління. Застосування нових моделей та алгоритмів забезпечення функціонування програмно – керованою мережею дозволить проводити маршрутизацію потоків даних мережі, диференціюючи їх за чутливістю до перемішування порядку пакетів та розриву з'єднання.

Метою даної статті є проведення аналізу моделей та алгоритмів функціонування системи управління архітектури SDN для більш надійної роботи мережі. Це надає можливість користувачам отримувати послуги із необхідною якістю, достовірністю та дозволить подолати виникаючі проблеми, пов'язані із складнощами міграції від традиційних мереж до архітектури SDN.

Ключові слова: програмно керовані мережі SDN, управління мережевими пристроями, архітектура SDN, моделі та алгоритми системи управління, рівень функціонування мережі.

Постановка проблеми. Основна ідея розвитку SDN-підходу при побудові мереж полягає у тому, щоб відділити керування мережевим обладнанням від управління передачею даних за рахунок розроблення спеціального програмного забезпечення, яке може працювати на окремому обладнанні під контролем адміністратора мережі. Допоможе перейти від управління окремими екземплярами мережевого обладнання до керування мережею у цілому та створити інтелектуальний програмно – керований інтерфейс між мережним додатком та транспортним середовищем мережі. У стандартній архітектурі програмно керованих мереж виділяють три основних рівні – інфраструктурний рівень тобто рівень передачі даних, на якому функціонують мережеві комутатори та канали передачі даних, рівень керування - набір програмних засобів, логічно відділених від рівня передачі даних, що забезпечують реалізацію механізмів керування пристроями інфраструктурного рівня та рівень мережевих додатків – не уніфікований та незалежний від виробника рівень для простішого керування мережею і внесення додаткових функцій та елементів, які потрібні самому власнику мережі.

Протокол Open-Flow – це протокол управління процесом обробки даних, що передаються по мережі маршрутизаторами та комутаторами. Використовується для керування мережевими елементами із центрального пристрою - контролера мережі, яким може слугувати звичайний комп'ютер чи сервер. Протокол Open-Flow, що реалізує незалежний від виробника інтерфейс між логічним контролером мережі та мережевим транспортом, є однією з реалізацій концепції програмно - керованої мережі. Ядром рівня керування програмно - керованої мережі є мережева операційна система - програмний засіб, що забезпечує інтерфейс засобами рівня

передачі даних та прикладний програмний інтерфейс для рівня мережевих додатків, сформульований в термінах більш високого рівня абстракції порівняно з тим, який використовується в параметрах конфігурації мережевих пристроїв. На відміну від традиційного застосування мережевої операційної системи як операційної системи інтегрованої зі стеком мережевих протоколів, в даному випадку будемо розуміти програмну система, що забезпечує моніторинг, доступ, керування ресурсами всієї мережі, а не конкретного вузла. Об'єктом керування мережевої операційної системи є один або кілька комутаторів. Контролер забезпечує набір інтерфейсів для створення, редагування, видалення, керування конфігурацією таблиць потоків у комутаторах. Комутатором керує програмний процес, який виконується на контролері. Контролер повинен володіти інформацією про топологію мережі в будь - який момент часу. Інформація про топологію мережі також містить інформацію про розміщення користувачів та серверів, інших елементів та сервісів мережі, а крім того, прив'язку між іменами та адресами. Тому однією з найважливіших задач, що розв'язуються мережевою операційною системою, є постійний моніторинг мережі та побудова топології мережі. Використання стандартизованого відкритого інтерфейсу площини передачі даних дає можливість впроваджувати інновації набагато оперативніше, ніж це відбувається сьогодні. Власники мережі та оператори можуть додавати нові функціональні можливості та послуги в таку програмно - керовану мережу. Нова функціональність та послуги впроваджуються за допомогою створення мережевих сервісів на мережевій операційній системі чи контролері з використанням стандартизованого API. Це суттєво прискорює розвиток мережі, наприклад, впровадження нових методів контролю доступу.

Аналіз останніх досліджень і публікацій. Проведений аналіз методів та моделей управління програмно - керованими мережами показав, що проблема забезпечення якості обслуговування займає досить важливе місце у наукових працях закордонних і вітчизняних дослідників. Значна увага науковців приділяється до адаптивності програмно - керованої мережі в умовах обслуговування мультисервісного потоку даних. Особливе місце тут займає забезпечення достовірності передачі інформації та сервісних послуг управління для мереж [1] де враховуються і програмно - конфігуровані мережі [2]. Система моніторингу пакетної затримки в програмно - конфігурованих телекомунікаційних мережах [3] покращує управління мережами із застосуванням сучасних технологій. Багатокритеріальна оптимізація параметрів програмно - конфігурованих мереж [4] дозволяє забезпечити задану стабільність та безперервність управління. Управління телекомунікаціями із застосуванням новітніх технологій [5] дозволяє забезпечити задану стабільність та безперервність управління. Визначення доступності програмних комплексів у системах з сервісно-орієнтованою архітектурою [6] забезпечується застосуванням інтелектуальних технологій для підвищення якості роботи мереж при невизначеності [7]. Метод автоматизації побудови програмно – керованих мереж [8] забезпечує оптимальну систему управління при проектовані мереж [9], а метод балансування навантаження на основі інтегрованої архітектури управління[10] допомагає забезпечити достовірність передачі інформації. Знання сучасних сервісних послуг архітектури LTE для високошвидкісних мереж [11] допомагає в забезпечені відмово стійкості при використанні хмарних обчислень [12], багаторівневої ієрархії управління у програмно -конфігурованих мережах [13]. Враховуючи проведений аналіз, можна дійти до висновку, що існуючі моделі управління інформаційним потоком у програмно - конфігуруємо мережах не завжди враховують вимоги окремого клієнта, а диференціюють потоки лише за класами інформації та не завжди використовують актуальні параметри управління та обслуговування як окремих каналів, так й індивідуальних потоків окремого клієнта мережі.

Мета роботи – провести аналіз моделей та алгоритмів функціонування системи управління архітектурою SDN для більш надійної роботи мережі. Це надає можливість користувачам отримувати послуги із необхідною якістю, достовірністю та дозволить подолати виникаючі проблеми.

Основний матеріал досліджень. В рамках аналізу складових елементів системи управління SDN архітектури, що забезпечують якість обслуговування потоків у програмно - керованими мережах є деякі недоліки. Це, незважаючи на вищий рівень оперативності обчислення

маршрутів та аналіз топології мережі, сама маршрутизація здійснюється за допомогою традиційних алгоритмів, що використовуються існуючими протоколами - OSPF та EIGRP. Різнорідність самої апаратної реалізації пристроїв передачі даних мережі призводить до того, що різні види комутаторів можуть не підтримувати деякі функції чи підтримувати їх із обмеженою продуктивністю. У процесі роботи мережі це може суттєво вплинути на пропускну здатність окремих потоків передачі даних чи цілих доменів мережі. Сама маршрутизація потоків передачі здійснюється за критерієм якості обслуговування чи за критерієм рівномірного завантаження мережевих ресурсів мережі. Підвищення якості обслуговування здійснюється із врахуванням класифікації потоку передачі згідно ITU-T, що досить суттєво обмежує можливість управління потоком даних. Більшість моделей не враховують характеристик мультисервісного потоку даних, що призводить до погіршення якості обслуговування та підвищення ймовірності блокування каналів передачі мережі. Ще одна категорія методів базується на потокових аналітичних моделях для оптимізації мережі. Ці методи використовують моделі балансування навантаження потоків передачі даних, які не враховують чутливості потоку даних до перемішування порядку пакетів, погіршення затримки та тимчасового розриву з'єднання [1].

Розглянемо архітектуру SDN (рис. 1), що складається із рівня програми, рівня мережевого устаткування та рівня даних. Мережеві комутатори стають простими пристроями пере адресації, а логіка управління в архітектурі SDN реалізована в логічно централізованому контролері.

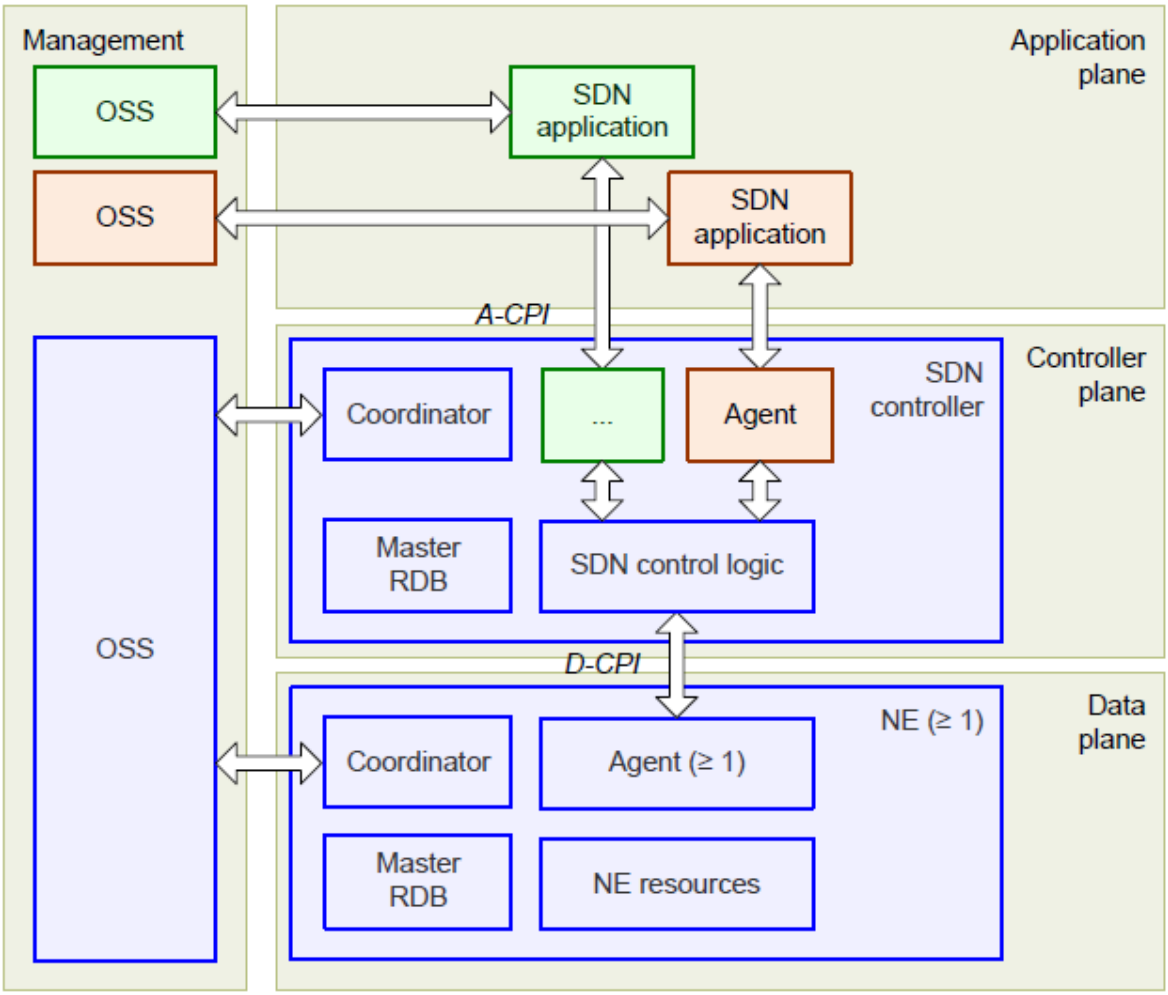


Рисунок 1 – Класична модель архітектура SDN мережі

SDN контролер управляє ресурсами даних через D-CPI інтерфейс. A-CPI інтерфейс використовується для реалізації зв'язку між додатками та контролером тому функція управління відбувається через інтерфейс управління. Така конфігурація може підтримувати різні

мережеві додатки. На відміну від традиційних мереж у мережах SDN маршрутизатор виконує лише функції передачі. Відмінність передачі пакетів у традиційних мережах та мережах SDN представлено на рис. 2 [3].

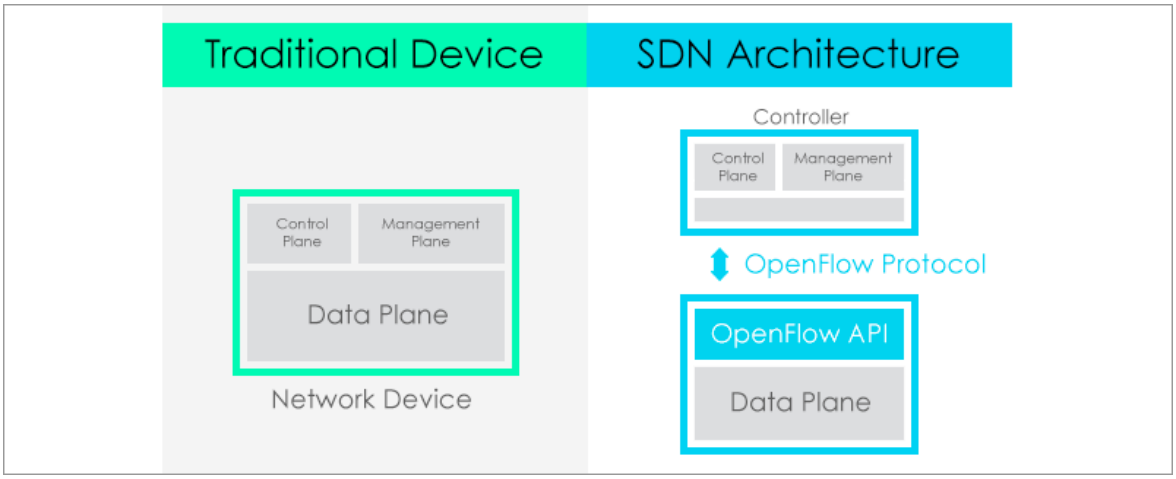


Рисунок 2 – Порівняння традиційної та SDN архітектури

При аналізі моделей та алгоритмів функціонування системи управління SDN архітектури розглянемо співвідношення до її традиційних мереж. Усі сучасні інформаційні технології висувають досить великі вимоги до гнучкості та масштабованості комп'ютерних мереж і очікується, що SDN мережі допоможуть вирішити цілий ряд наявних проблем, сприятимуть створенню автоматизованих, програмованих, гнучких та економічних мережевих інфраструктур, однак ця стратегія у різних провідних виробників помітно розрізняється. За оцінками GARTNER[3], на мережеву інфраструктуру припадає приблизно 17% IT - бюджету. При цьому вона далеко не завжди може адаптуватися до змін потреб бізнесу. Тому нові тенденції - віртуалізація, хмарні обчислення, мобільність користувачів, зростання обсягів передачі - змінюють вимоги до мережевих інфраструктур. Будуть виникати питання чи зможуть сьогодні мережеві продукти забезпечити підтримку майбутніх додатків і сервісів, якою мірою розвиток мережі буде прив'язаний до продуктів обраного виробника тощо. Пріоритетність рішень, архітектура традиційного мережевого обладнання робить цю прив'язку дуже міцною. Деякі виробники навіть характеризують поточну ситуацію у мережевий галузі як революційну. Ряд експертів [4] в якості рецепту усунення розкритих в мережах проблем називають перехід до архітектури програмно-керованих мереж (Software-Defined-Networking, SDN). Архітектура SDN обіцяє істотно послабити залежність від замовників технологій конкретного виробника. В архітектурі SDN вся логіка управління мережевими пристроями виноситься в так звану «площину управління», яка реалізується програмним чином. Конструктивно контролери в архітектурі SDN можуть будуватися на базі фізичних або віртуальних вузлів. В архітектурі SDN управління мережевими пристроями, як правило, здійснюється по протоколу Open-Flow. Головна ідея архітектури SDN - відділення функцій передачі даних від функцій управління. У традиційних комутаторах та маршрутизаторах ці процеси зв’язані. У архітектурі SDN мережа, що складається із безлічі пристроїв різних виробників, постає для застосування як один логічний комутатор. Архітектура SDN дозволяє адміністраторам програмувати мережу як єдине ціле, а не займатися окремими комутаторами, які можуть просто виконувати інструкції контролера. Реалізація такої концепції значно спрощує експлуатацію та функціонування мережі, її конфігурацію. Комутатори можуть бути простими та дешевими. Характеристики мережі можна оперативно змінювати у режимі реального часу, скорочуються терміни впровадження нових додатків та сервісів. Програмні інтерфейси (API), контролери дозволяють розробникам створювати додатки для управління такою мережею. Ці програми можуть виконувати найрізноманітніші функції, причому для цього не потрібно знати особливості роботи конкретних мережевих пристроїв. З

точки зору виробників, такий підхід не повинен викликати ентузіазму у розробників мережевого устаткування, які багато років удосконалювали унікальні функції своїх комутаторів та маршрутизаторів. Можливість використання простих та дешевих комутаторів, створення додатків сторонніми розробниками за рахунок відкритих API підриває бізнес таких компаній, позбавляє їх джерела додаткової вартості. Проте великі замовники, включаючи провідних операторів зв'язку та провайдерів, вже перейнялися ідеями архітектури SDN, а виробники мікросхем комутаторів оголосили про підтримку Open-Flow, тому поставники не можуть залишатися осторонь. Структура Open-Flow маршрутизатора представлена на рис. 3. Open-Flow маршрутизатор складається із однієї або декількох таблиць потоків. Маршрутизатор обмінюється повідомленнями з контролером за допомогою протоколу Open-Flow. За допомогою протоколу Open-Flow, контролер виконує такі дії з записами потоків в таблицях як додавати, оновлювати, видаляти.

У таблицях потоків маршрутизатора містяться набори записів, а усі записи визначаються полями порівнянь, лічильниками та набором інструкцій, які застосовуються до пакету та співпали із полями. При передачі, заголовки пакетів порівнюються із полями порівнянь записів в порядку пріоритету, а це одне із полів порівняння. Якщо знайдені відповідні записи, то до пакету застосовуються інструкції, асоційовані із цим записом. Якщо не знайдено жодного запису, то пакет скидається або передається для аналізу прийняття рішення контролеру.

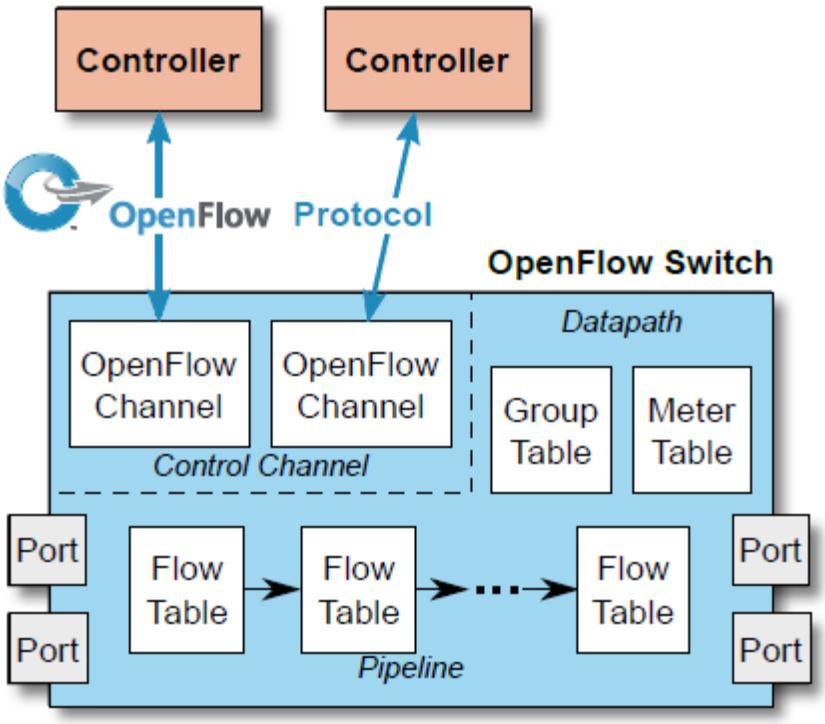


Рисунок 3 – Стандартний алгоритм функціонування Open-Flow маршрутизатора

Інструкції у відповідних записах Open-Flow маршрутизатора містять дії, які застосовуються до пакету та визначають безпосередньо самі правила пересилання, чи визначають подальшу обробку пакета, у наступних таблицях потоків - конвеєрна обробка. Конвеєрна обробка дозволяє передавати аналіз пакета із однієї таблиці в іншу, додатково пересилаючи спеціальні метадані. Обробка закінчується, коли відповідні інструкції не містять команд пересилання в наступну таблицю у цей момент виконується модифікація пакету, виконання "накопичених" дій. Завдяки такій моделі, Open-Flow комутатор може функціонувати як простий комутатор, маршрутизатор, мережевий екран чи як інше мережевий пристрій. Все визначається за таблицею передачі. Така модель обробки пакета відкриває унікальні можливості. Пристрій може використовуватися в ролі як комутатора, так і маршрутизатора чи мережевого екрану. Групова таблиця містить записи груп, а кожен запис містить також список інструкцій зі специфічною

семантикою, що залежить від типу групи. Дії в одній застосовуються для всіх пакетів, що посилаються до цієї групи. Збір статистики реалізується за допомогою лічильників. Лічильники можуть бути призначені для кожної таблиці, потоку, порту, черги, групи чи набори лічильників, визначені спеціалізацією Open-Flow. Всі Open-Flow сумісні лічильники можуть бути реалізовані в програмному забезпеченні та відображають інформацію на основі опитування апаратних лічильників, які мають обмежений діапазон значень. Любий потоковий запис містить набір інструкцій, які виконуються в тому разі, коли пакет відповідає правилу. Усі інструкції діляться на наступні типи: для негайного виконання, для очищення списку інструкцій, для додавання нової інструкції, для запису метаданих, для переходу до наступної таблиці. Інструкції для негайного виконання дають вказівку застосувати певні дії негайно, без будь - яких змін у наборі дій. Така інструкція може бути використана для модифікації пакета при передачі його до іншої таблиці. Інструкції для очищення видаляють всі інструкції з набору інструкцій для окремого потоку. Інструкції для додавання нової інструкції доповнюють наявний набір інструкцій для окремого правила новими інструкціями. Інструкція переходу до наступної таблиці містить номер таблиці, в яку пакет буде переданий після обробки в поточній таблиці. Номер наступної таблиці обов'язково повинен бути більшим від номера поточної таблиці.

Дослідження та аналіз моделей і алгоритмів забезпечення функціонування й процесів управління мережею, побудованою за принципами SDN, показує, що спочатку необхідно здійснити модернізацію механізмів моніторингу стану її ресурсів, по скільки при використанні стандартного механізму спостерігається генерація надлишкової службової інформації для елементів, що простоюють. Це може мати досить негативний вплив на ефективність роботи через завантаженість каналів передачі. Тому при аналізі моделей та алгоритмів функціонування системи управління SDN архітектури, у зв'язку із недоліками існуючих систем моніторингу, у багатьох публікаціях [7] пропонується використовувати метод динамічної адаптації параметрів системи моніторингу, наприклад, зміну інтенсивності моніторингу стану мережевого елемента залежно від його поточної завантаженості. Інтелектуальний моніторинг в мережі на основі SDN реалізується шляхом встановлення головного додатку моніторингу на контролер та відповідних підконтрольних йому агентів на кожен комутатор. Загалом процес моніторингу ґрунтується на двох основних підходах:

• зміна інтенсивності моніторингу залежно від попередньо накопиченої статистичної інформації про стан завантаженості у пам'яті керуючого пристрою мережі. На основі аналізу можна визначати характеристики потоку інформації в певний період часу та змінювати інтенсивність відповідно до визначених потреб. В години пікового навантаження, наприклад, слід збільшувати інтенсивність моніторингу, а вночі можна зменшити;

• динамічна зміна інтенсивності моніторингу, залежно від завантаженості елементів мереж на основі зібраних у режимі реального часу. У випадку наближення завантаженості мережі до критичного рівня, збільшується частота опитування мережевих вузлів і таким чином здійснюється перехід у стан пильного моніторингу відповідних елементів мережі.

Тому аналіз моніторингу виконує додаток, встановлений на контролері, а підконтрольні йому агенти виконують функції збору інформації, модифікацію та відправлення на контролер. Розподіл інтенсивності моніторингу окремих сегментів мережі дає можливість усунути надлишкові процеси моніторингу та обробки даних про стан мережі, виконуючи необхідну інтенсивність лише на тих вузлах, де все це необхідно робити. На основі інтенсивності моніторингу можна збільшувати гнучкість управління елементами мережі на основі SDN, та ефективніше використовувати обчислювальні ресурси пристроїв рівня управління. Володіючи поточною службовою інформацією, можна здійснювати оптимальний розподіл навантаження на мережі, попереджуючи таким чином негативні явища перевантаження мережевих вузлів. Також можна переводити елементи, що простоюють, у режим очікування, зберігаючи при цьому можливість надійного та швидкого їх відновлення до нормального режиму роботи. Це значно зменшить витрати та збільшує час «життя» мережевих пристроїв. Повністю відключати обладнання не завжди доцільно, по скільки його ввімкнення потребує певного часу для відновлення таблиць комутації, запуску усіх апаратних та програмних процесів комутатора, що впли-

ває на час перебудови топології мережі та спричиняє стрибок службової інформації між контролером та комутатором. Особливістю розглянутого механізму є зміна інтенсивності моніторингу лише конкретного мережевого вузла, який цього потребує, однак це не впливає на інтенсивність моніторингу інших вузлів. Такий алгоритм [7] функціонування системи управління SDN архітектури та пропонований механізм є адаптованим до сучасного динамічного потоку даних та забезпечує хорошу базу для подальшого процесу балансування навантаження. Чим вище миттєве значення завантаження каналу, тим швидше відбудеться наступне опитування, тому чим більше завантаження каналу, тим частіше система моніторингу здійснює опитування щодо кількості переданої інформації. Такий метод можна використовувати стосовно усіх параметрів комутатора у випадку, коли підвищення інтенсивності їхнього опитування не впливає негативно на характеристики продуктивності та якості функціонування мережі. Ще важливим параметром процесу моніторингу є кількість інформації, що генерується цим процесом. При роботі мережі, у випадку підвищення інтенсивності моніторингу кількість службової інформації, навантаження на інформаційний канал зростає, що загалом призводить до часткового зниження ефективності використання інформаційного каналу. Функція зміни інтенсивності моніторингу буде різною для кожного окремого параметру мережі, а її максимальне значення залежатиме від рівня навантаження процесу моніторингу на мережеві елементи. Обмеження щодо частоти моніторингу деяких параметрів часто встановлюють виробники, вказуючи критичне значення у документації до пристроїв.

Спрощені підходи до аналізу потоків даних і спроби отримання інформації про мережеві додатки на підставі легкодоступних атрибутів та характеристик потоків найчастіше виявляються непродуктивними. У більшості програм обміну файлами активно використовуються прийоми, що ускладнює достовірну ідентифікацію таких додатків – динамічне призначення портів, децентралізовані сховища, використання поширених прикладних протоколів як транспортних, а також криптографічні методи приховування та маскування потоку даних. Тому для виявлення мережевих аномалій необхідний ретельний аналіз. Ці обставини вимагають використання додаткових технічних, програмних та алгоритмічних засобів і математичних моделей досліджуваних процесів. Характеристики функціонування програмно-керованої мережі, що складається з різнорідних Open-Flow комутаторів, залежать від апаратних характеристик кожного комутатора. З метою зменшення складності та вартості комутатора постачальники можуть обмежити функціональні можливості Open-Flow, наприклад, розмір апаратної таблиці потоків чи можливостей цієї таблиці щодо пошуку за певними полями, виконання певних дій над пакетами. Додатки, що встановлюються на контролері, повинні враховувати ці обмеження, щоб уникнути можливих проблем, пов’язаних із погіршенням продуктивності мережі в процесі її роботи. Використання нових моделей та алгоритмів дозволяє забезпечити централізований моніторинг параметрів мережевих пристроїв та формувати характеристики функціонування програмно-керованої мережі на виході. Результати моніторингу можуть бути додатково використані при плануванні роботи мережі чи для динамічної оптимізації мережі - встановлення правил із врахуванням апаратних характеристик комутатора та передачі потоку даних через різні шляхи для уникнення вузьких місць у такій мережі. Специфікація Open-Flow визначає необхідну функціональність, яка повинна бути реалізована у кожному комутаторі Open-Flow. Основною метою цієї специфікації є забезпечення уніфікованих процесів контролю та управління програмно-керованою мережею, що складається із пристроїв різних моделей від різних виробників. Реалізація необхідної функціональності є індивідуальною та змінюється від одного виробника до іншого [7] та може привести до змін продуктивності у реальній мережі. Проблеми виникають уже тоді, коли програмно-керована мережа налаштована та окремі комутатори починають створювати вузькі місця, погіршуючи продуктивність та якість обслуговування мережі. Такі недоліки можна врахувати на стадії проектування програмно-керованої мережі та розробки програмного забезпечення для контролера. Тому необхідно, щоб розробники додатків для програмно-керованих мереж змогли отримати інформацію про обмеження продуктивності конкретного комутатора із метою забезпечення стабільної та надійної роботи мережі. Завдяки такій системі розробники зможуть отримати необхідні дані та можливість охарактеризувати продуктивність конкретного комутатора. Комутатор, залежно

від апаратної реалізації, може надавати доступ до окремих параметрів. Специфікація Open-Flow містить загальний алгоритм роботи та список параметрів доступних для моніторингу:

- статистика потоків передачі - тривалість існування, пріоритет, кількість оброблених пакетів, байт;

- статистика таблиць потоків даних - кількість правил, кількість оброблених пакетів, байт;

- статистика портів передачі - кількість переданих чи відкинутих пакетів, байт, помилок передачі та колізій);

- статистика черг передачі - довжина черги, кількість переданих пакетів, байт, кількість відкинутих пакетів через переповнення;

- інші специфікації - STP, збірка сегментів IP пакетів тощо.

Розглянута система дозволяє здійснювати моніторинг як Open-Flow параметрів, так і параметрів Q o S, пов'язаних із роботою комутатора. Параметри Open-Flow - максимальна кількість правил із конкретною структурою, тривалість встановлення правил, тривалість опитування статистики таблиці потоків, тривалість обробки пакетів із використанням програмних таблиць потоків даних, тривалість зчитування інформації із лічильників, а також завантаження центрального процесора пристрою [9]. Основним компонентом розглянутої системи моніторингу є додаток моніторингу, який встановлюється на фізичному сервері. Цей додаток виконує ключову роль збору, форматування та представлення інформації у форматі, зручному для користувача і для подальшої обробки цієї інформації іншими додатками. База даних зберігає інформацію, необхідну для роботи додатка, наприклад, для налаштування комутаторів, моделі та технічні особливостей того чи іншого комутатора. Ці дані заносяться в базу даних адміністратор програмно-керованої мережі. У базі даних зберігаються зібрані дані моніторингу та оброблені статистичні характеристики поведінки мережі в певні періоди.

Прогнозування ризиків та стабільності якості функціонування системи управління SDN архітектури. Ступінь очікуваних ризиків функціонування можна подати як добуток імовірності небажаних наслідків на відповідну величину втрат аналогічно як у працях [11]:

$$R = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} p_i \cdot Z_i \,, \tag{1}$$

де R – величина ризику;

p_i – ймовірності небажаних впливів каналу передачі;

Z_i – величини втрат каналу.

Для оцінювання ризику якості функціонування мережі SDN також використовують величину середньозваженого модуля відхилення ΔZ (тут n=12) [11]:

$$\Delta Z = \sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z}) \quad \overline{Z} = \frac{1}{n} \sum_{i=1}^{n} Z_i \,. \tag{2}$$

Також визначають середньоквадратичне відхилення [11]:

$$\sigma = \sqrt{\sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z})^2} \,, \tag{3}$$

Якщо взяти до уваги негативні відхилення від запланованих параметрів від параметра $\overline{Z}$, то ступінь ризику якості функціонування оцінюється показником варіації S_Z і його значення визначається з допомогою співвідношення [11]:

$$S_Z = \sqrt{\sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z})^2 \cdot I_{vi}} \Big/ \sum_{i=1}^{n} p_i \cdot I_{vi} \,, \tag{4}$$

де $I_i = \{I_{vi}\}$ – індикатор несприятливих відхилень якості роботи, якому відповідають:

0, для сприятливого відхилення $I_{vi} = 0$,

1, для несприятливого відхилення $I_{vi} = 1$.

Висновки. Аналіз моделей та алгоритмів функціонування SDN мереж показує, що більшість моделей не враховують характеристик мультисервісного потоку даних і це призводить до погіршення якості функціонування та підвищення ймовірності блокування каналів передачі мережі. Відсутність можливості здійснювати диференційоване управління для окремих потоків даних окремих клієнтів мережі та врахувати їхні вимоги щодо якості, призводить до низької ефективності каналу маршрутизації, неоптимального розподілу навантаження мережі, погіршення якості обслуговування високо пріоритетних потоків даних. Засоби контролю за процесом передачі окремих потоків передачі даних відсутні, внаслідок чого система управління мережею не має змогу визначити погіршення якості функціонування для цих потоків даних, а тому не зможе гарантувати рівень якості, узгоджений у сервісі. Враховуючи проведений аналіз, можна дійти до висновку, що існуючі моделі управління інформаційним потоком у програмно - конфігуруємо мережах не завжди враховують вимоги окремого клієнта, а диференціюють потоки лише за класами потоку інформації. Розглянута схема розробки мереж SDN показує, що різні організації при створені мереж SDN, ставлять за мету формування такої архітектури мережі та устаткування, що припускає відділення площини управління від площини передачі та докладають значних зусиль до подолання виникаючих проблем, пов'язаних із складнощами міграції від традиційних мереж до архітектури SDN. Це в подальшому надасть можливість користувачам отримувати послуги із необхідною якістю, надійністю, достовірністю та прогнозувати ризики і стабільність якості функціонування системи управління такої архітектури.

ЛІТЕРАТУРА:

1. Хмельницький Ю.В. Забезпечення достовірності передачі інформації та сервісних послуг для високошвидкісних мереж при завадах / Ю.В Хмельницький, Д.П. Яковлєв // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 57. – С. 111-119.

2. Орлов Є. В. Програмно - конфігуровані мережі (SDN): архітектура, міжнародна стандартизація / Є. В. Орлов // – К.: Наукові записки УНДІЗ, 2014. - №4(32). - С. 85-91.

3. Климаш М.М. Система моніторингу пакетної затримки в програмно - конфігурованих телекомунікаційних мережах / М.М.Климаш, М.О.Селюченко, О.М.Панченко // X Міжнародна науково -технічна конференція «Проблеми телекомунікацій» ПТ-2016: Збірник матеріалів конференції (м. Київ, 19-22 квітня 2016 р.). - К.: НТТУ «КПІ», 2016. - С.345-347.

4. Толубко В. Б. Багатокритеріальна оптимізація параметрів програмно - конфігурованих мереж (SDN) / В. Б. Толубко, Л. Н. Беркман, Л. О. Комарова, Є. В. Орлов // – К.: Телекомунікаційні та інформаційні технології, 2014. - №4. - С. 5-11

5. Кривуца В.Г. Управління телекомунікаціями із застосуванням новітніх технологій / В.Г. Кривуца, В.К. Стеклов, Л.Н. Беркман, Б.Я. Костік, В.Ф. Олійник, С.М. Скляренко // Підручник для ВНЗ. – К.: Техніка, 2007. – 384 с.

6. Стрихалюк Б.М. Визначення доступності програмних комплексів у системах з сервісно-орієнтованою архітектурою / Б.М.Стрихалюк, О.М.Шпур, М.О.Селюченко // Наукові праці ДонНТУ. Серія: Обчислювальна техніка та автоматизація. - Донецьк, 2014. - .№2 (27). - С.109-120.

7. Селюков О. В. Застосування інтелектуальних технологій для підвищення якості роботи телекомунікаційних мереж при невизначеності / О. В. Селюков, Ю. В. Хмельницький, І. В. Обертюк, Л. В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, – К.: 2017. - Вип. 56. - С. 146-153.

8. Олизарович Е. В. Метод автоматизации построения программно- конфигурируемых сетей / Е. В. Олизарович, А. И. Бражук // Вестник Гродзенского государственного университета им. Я. Купалы, 2013. - №3(159) - С. 128-134.

9. Стєклов В.І. Проектування телекомунікаційних мереж. Підручник для студ. вищ. навч. закл. за напрямком "Телекомунікації"/ В.І. Стєклов, Л.Н.Беркман //-К.: Техніка, 2002.-792 с.

10. Стрихалюк Б.М. Метод балансування навантаження на основі інтегрованої архітектури управління з використанням функції NVF / Б.М.Стрихалюк, О.М.Шпур, М.О.Селюченко // IX Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2015: Збірник матеріалів конференції (м. Київ, 21-24 квітня 2015 р.). - К.: НТТУ «КПІ», 2015. - С.322-325

11. Хмельницький Ю.В. Сервісні послуги архітектури LTE для високошвидкісних мереж / Ю. В. Хмельницький, С.Ю. Гунченко, О.С. Лєнков, Д.П. Яковлєв // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, – К.: 2017. - Вип. 56. - С. 177-185.

12. Муляр І.В. Захист від прихованих загроз в середовищі хмарних обчислень / І.В. Муляр, О. В. Мірошниченко, А.В. Краснік, Л.В. Солодєва// Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2018. – Вип. № 59. – С. 115-126.

13. Климаш М.М. Забезпечення відмовостійкості багаторівневої ієрархії управління у програмно -конфігурованих мережах / М.М.Климаш, М.О.Селюченко, О.А.Лаврів // Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій: Матеріали конференції (м. Львів, 30 жовтня - 2 листопада 2014 р.). - Львів, 2014. - С.225-228.

REFERENCES:

1. Xmel"nyc"kyj, Yu.V. and Yakovlyev, D.P. (2017), "Zabezpechennya dostovirnosti peredachi informaciyi ta servisnyx posluh dlya vysokoshvydkisnyx merezh pry zavadax" [Ensuring the reliability of data transmission and services for high-speed networks at hindrances], VIKNU, Zbirnyk naukovyx prac" Vijs"kovoho instytutu Kyyivs"koho nacional"noho universytetu imeni Tarasa Shevchenka, Kyyiv, No.57, pp. 111-119.

2. Orlov, Ye. V. (2014),"Prohramno - konfihurovani merezhi (SDN): arxitektura, mizhnarodna standartyzaciya" [Software - defined networking (SDN): architecture, international standardization], Naukovi zapysky UNDIZ, Kyyiv, No. 4(32), pp. 85-91.

3. Klymash, M.M., Selyuchenko, M.O. and Panchenko, O.M. (2016), "Systema monitorynhu paketnoyi zatrymky v prohramno - konfihurovanyx telekomunikacijnyx merezhax" [System of monitoring packet delay in software - defined networks], NTTU «KPI», Kyyiv, X Mizhnarodna naukovo -texnichna konferenciya «Problemy telekomunikacij» PT-2016: Zbirnyk materialiv konferenciyi, pp.345-347.

4. Tolubko V. B. , Berkman, L. N., Komarova L. O. and Orlov Ye. V. (2014), "Bahatokryterial"na optymizaciya parametriv prohramno - konfihurovanyx merezh (SDN) "[Multi-criteria optimization of the parameters of software defined networking (SDN)], Telekomunikacijni ta informacijni texnolohiyi, Kyyiv, No.4, pp. 5-11.

5. Kryvuca, V.H., Steklov, V.K., Berkman, L.N., Kostik, B.Ya., Olijnyk, B.F. and Sklyarenko, S.M. (2007), "Upravlinnya telekomunikaciyamy iz zastosuvannyam novitnix texnolohij" [Management of telecommunication with latest technology], Texnika, Kyyiv, Pidruchnyk dlya VNZ, 384p.

6. Stryxalyuk, B.M., Shpur, O.M. and Selyuchenko, M.O. (2014), "Vyznachennya dostupnosti prohramnyx kompleksiv u systemax z servisno-oriyentovanoyu arxitekturoyu" [Determining availability of software systems in the systems with service-oriented architecture], Naukovi praci DonNTU. Seriya: Obchyslyuval"na texnika ta avtomatyzaciya, Donec"k, No.2(27), pp.109-120.

7. Selyukov, O.V., Xmel"nyc"kyj, Yu. V., Obertyuk, I.V. and Solodyeyeva, L.V. (2017), "Zastosuvannya intelektual"nyx texnolohij dlya pidvyshhennya yakosti roboty telekomunikacijnyx merezh pry nevyznachenosti" [Application of intelligent technologies to improve the quality of work of telecommunication networks under uncertainty], Zbirnyk naukovyx prac" Vijs"kovoho instytutu Kyyivs"koho nacional"noho universytetu imeni Tarasa Shevchenka, Kyyiv, No.56, pp. 146-153.

8. Olyzarovych, E. V. and Brazhuk, A. Y. (2013), "Metod avtomatyzacyy postroenyya prohrammno-konfyhuryruemыx setej" [Method of automated build software - defined networks], Vestnyk Hrodzenskoho hosudarstvennoho unyversyteta ym. Ya. Kupaly, Bilorus", No. 3(159), pp. 128-134.

9. Styeklov, V.I. and Berkman, L.N. (2002), "Proektuvannya telekomunikacijnyx merezh. Pidruchnyk dlya stud. vyshh. navch. zakl. za napryamkom "Telekomunikaciyi" " [Design of telecommunication networks. The textbook for the stud. visch. proc. zakl. in the field of telecommunications], Texnika, Kyyiv, 792p.

10. Stryxalyuk, B.M., Shpur, O.M. and Selyuchenko, M.O. (2015), "Metod balansuvannya navantazhennya na osnovi intehrovanoyi arxitektury upravlinnya z vykorystannyam funkciyi NVF" [Load balancing based on integrated control architecture using NVF], IX Mizhnarodna naukovo-texnichna konferenciya «Problemy telekomunikacij» PT-2015: Zbirnyk materialiv konferenciyi, NTTU «KPI», Kyyiv, pp.322-325.

11. Xmel"nyc"kyj, Yu.V., Hunchenko, S.Yu., Lyenkov, O.S. and Yakovlyev, D.P. (2017), "Servisni posluhy arxitektury LTE dlya vysokoshvydkisnyx merezh" [Fault tolerance for multi-level control hierarchy in software-defined networks], Zbirnyk naukovyx prac" Vijs"kovoho instytutu Kyyivs"koho nacional"noho universytetu imeni Tarasa Shevchenka, Kyyiv, No.56, pp.177-185.

12. Muliar I.V., Miroshnychenko O.V, Krasnik A.V. and Solodyeyeva, L. V. (2018) "Zakhyst vid prykhovanykh zahroz v seredovyshchi khmarnykh obchyslen" [Protection from hidden threats in the cloud

computing environment], Zbirnyk naukovyx prac" Vijs"kovoho instytutu Kyyivs"koho nacional"noho universytetu imeni Tarasa Shevchenka, Kyyiv, No.59, pp.115-126.

13. Klymash, M.M., Selyuchenko, M.O. and Lavriv, O.A. (2014), "Zabezpechennya vidmovostijkosti bahatorivnevoyi iyerarxiyi upravlinnya u prohramno -konfihurovanyx merezhax" [Service architecture LTE for high-speed networks], Suchasni problemy telekomunikacij i pidhotovka faxivciv v haluzi telekomunikacij: Materialy konferenciyi, L"viv, pp.225-228.

д.т.н., с.н.с. Сєлюков О.В., к.т.н., доц. Хмельницкий Ю.В.,
Ковпа Д.М., Лісовський О.С.

АНАЛИЗ МОДЕЛЕЙ И ПРОГНОЗИРОВАНИЕ РИСКОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ SDN АРХИТЕКТУРЫ

В статье рассмотрены вопросы анализа моделей и алгоритмов функционирования системы управления SDN архитектуры для обеспечения более качественной работы сети. Большая разнородность самой аппаратной реализации устройств передачи данных SDN архитектуры приводит к тому, что разные коммутаторы могут не поддерживать некоторые функции или поддерживать их с ограниченной производительностью. В процессе работы сети – это может существенно повлиять на пропускную способность отдельных потоков передачи данных или целых доменов сети. Маршрутизация потоков передачи осуществляется по критерию качества обслуживания и по критерию равномерной загрузки сетевых ресурсов сети. Повышение качества обслуживания осуществляется с учетом классификации потока передачи, что весьма ограничивает возможность управления потоком данных. Большинство моделей таких сетей не учитывают характеристик мульти сервисного потока данных, что приводит к ухудшению качества обслуживания и повышение вероятности блокирования каналов передачи. Отсутствие возможности осуществлять дифференцированное управление для отдельных потоков данных отдельных клиентов сети и учесть их требования относительно качества, приводит к низкой эффективности канала маршрутизации, неоптимального распределения нагрузки сети, ухудшение качества обслуживания высоко приоритетных потоков данных. Средства контроля над процессом передачи отдельных потоков передачи данных отсутствуют, вследствие чего система управления не имеет возможность определить ухудшение обслуживания для этих потоков данных, а потому не сможет гарантировать необходимый уровень управления. Применение новых моделей и алгоритмов обеспечения функционирования программно – управляемой сетью позволит проводить маршрутизацию потоков данных сети, дифференцируя их по чувствительности к перемешиванию порядка пакетов и разрыва соединения.

Целью данной статьи является проведение анализа моделей и алгоритмов функционирования системы управления архитектуры SDN для более надежной работы сети. Это предоставляет возможность пользователям получать услуги с необходимым качеством, достоверностью и позволит преодолеть возникающие проблемы, связанные со сложностями миграции от традиционных сетей к архитектуре SDN.

Ключевые слова: программно управляемые сети SDN, управление сетевыми устройствами, архитектура SDN, модели и алгоритмы системы управления, уровень функционирования сети.

УДК 004.65

к.ф-м.н., доц. **Собчук В.В.** (СНУ)
к.т.н., с.н.с. **Лаптєв О.А** (ДУТ)
к.т.н. **Саланда І.П.** (КОГПА)
к.ф-м.н. **Сачук Ю.В.** (СНУ)

МАТЕМАТИЧНА МОДЕЛЬ СТРУКТУРИ ІНФОРАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ НЕСТАЦІОНАРНОЇ ІЄРАРХІЧНОЇ ТА СТАЦІОНАРНОЇ ГІПЕРМЕРЕЖІ

У статті розроблена модель структури інтегральної інформаційної мережі на основі нестаціонарної ієрархічної та стаціонарної гіпермережі, з врахуванням руйнівних впливів різного характеру. Під функціональною стійкістю інтегральної інформаційної мережі в роботі розуміється можливість функціонування системи, нехай із зменшенням якості, протягом заданого часу під впливом зовнішніх та внутрішніх дестабілізуючих факторів. Під зовнішніми та внутрішніми дестабілізуючими факторами розуміються відмови, збої елементів системи, навмисні пошкодження, бойові ураження, електромагнітні завади, помилки обслуговуючого персоналу. Забезпечення властивості функціональної стійкості будь-якої складної технічної системи здійснюється в три етапи: ідентифікація нештатної ситуації, локалізація нештатної ситуації, відновлення функціонування за рахунок перерозподілу ресурсів. При розгляді інтегральних інформаційних мереж з точки зору функціональної стійкості, вихід з ладу вузла комутації чи лінії зв'язку тягне за собою руйнування каналів передачі вторинних мереж, які в графах цих мереж є несуміжними. Тому моделювати структуру такої мережі графом недоцільно. У зв'язку з цим, введено нові поняття і визначення в теорію функціональної стійкості та розроблено відповідний методичний апарат. Дана модель враховує усі необхідні основні з точки зору функціональної стійкості параметри мережі, їх властивості та відношення, які здійснюють значний вплив на синтез оптимальної структури мережі. Відмінність гіпермереж від інших структурних моделей полягає в тому, що в створені структури гіпермережі бере участь більше двох твірних множин, що дозволяє врахувати вплив можливих позаштатних ситуацій, які обумовлені внутрішніми і зовнішніми чинниками.

Ключові слова: гіпермережа, нестаціонарна гіпермережа, інформаційні мережі, функціональна стійкість, руйнівні впливи.

Вступ. За останні декілька десятиліть в житті сучасного суспільства різко зросла роль інформаційно-технічної сфери. Однак з розвитком інформаційно-технічних систем, підвищується їх чутливість до зовнішніх впливів різного характеру. Ці дії можуть порушувати нормальний режим роботи цих систем і навіть призводити до повної зупинки їх роботи. У той же час стан інформаційно-технічних систем активно впливає на стан політичної, економічної, оборонної та інших складових безпеки нашої країни.

Основою цих систем є інтегральні інформаційні мережі (ІІМ). Здатність ІІМ протистояти руйнівним діям (РД) і продовжувати виконувати певний обсяг функцій, можливо з погіршенням якості, є їх властивістю, яку називають функціональною стійкістю.

Постановка проблеми. Реалізація функціональної стійкості досягається застосуванням в складній технічній системі різних уже існуючих видів надмірності (структурної, часової, інформаційної, функціональної та ін.) шляхом перерозподілу ресурсів з метою парирування наслідків позаштатних ситуацій. Разом з тим, нечисленні роботи в галузі забезпечення функціональної стійкості складних технічних систем не дають змоги виробити єдині підходи та започаткувати теоретичні основи забезпечення функціональної стійкості для ІІМ. Проблема полягає у відсутності підходу та відповідних моделей щодо опису структури сучасної інтегральної інформаційної мережі, параметрів її елементів та зв'язків, а також відсутністю можливості врахувати руйнуючі впливи різного характеру.

Аналіз останніх публікацій. Математична формалізація функціональної стійкості ІІМ є першим науково-обґрунтованим кроком створення методологічних основ забезпечення функціональної стійкості ІІМ [1 – 6]. Аналіз теорії функціональної стійкості щодо методів моделювання складних технічних систем показав, що існують відповідні наукові праці для динамічних систем, які базуються на використані теорії графів [7 – 9]. Зокрема, у роботі [3]

запропоновано математичну модель структури інформаційної мережі 5 покоління (5*G*) на основі теорії випадкових графів, а в статті [10] розглянуто модель складної ієрархічної системи, що ґрунтується на представленні у вигляді *k*-гіпермережі. Особливості принципу роботи сучасних ІІМ дозволяють зробити висновок про те, що незважаючи на серйозні наукові результати теорії функціональної стійкості досліджувані в ній математичні моделі складних систем не здатні адекватно описати процес функціонування ІІМ.

Метою статті є розробка моделі структури інтегральної інформаційної мережі на основі нестаціонарної ієрархічної та стаціонарної гіпермережі, з врахуванням руйнівних впливів різного характеру.

Виклад основного матеріалу. Для того щоб проводити всебічний аналіз функціональної стійкості інформаційних мереж, необхідно розглядати окремо не тільки первинні або вторинні мережі, але і всі мережі передачі даних в сукупності. Такі об'єднані мережі будемо називати інтегральними інформаційними мережами.

При розгляді інтегральних інформаційних мереж з точки зору функціональної стійкості, вихід з ладу вузла комутації чи лінії зв'язку тягне за собою руйнування каналів передачі вторинних мереж, які в графах цих мереж є несуміжними. Тому моделювати структуру такої мережі графом недоцільно.

Таким чином виникає необхідність ввести нові поняття в теорію функціональної стійкості інформаційних мереж. Екзотерична мережа – це така теоретична модель мережі зв'язку, в якій просторове положення каналів передачі не впливає на розв'язання поставлених перед дослідником завдань. Езотерична мережа – теоретична модель мережі зв'язку, в якій явно розглядається реалізація вторинної мережі в первинній інформаційній мережі.

Першій теоретичній моделі інформаційної мережі відповідає поняття «граф» як моделі структури, а другій – поняття «гіпермережа», яке вперше було запропоновано в роботі [11].

Принципова відмінність гіпермереж від інших структурних моделей полягає в тому, що в створені структури гіпермережі бере участь більше двох твірних множин [12].

Так як методи відомих теорій не завжди дозволяють досліджувати гіпермережі, то потрібно розробити відповідний методологічний апарат і створити нові поняття і визначення.

Гіпермережеві моделі. Формально абстрактну гіпермережу можна описати шісткою $AS = (X, V, R; P, F, W)$, яка включає наступні об'єкти: $X = \left(x_1, x_2, \ \ldots, x_n\right)$ – множина вершин; $V = \left(\nu_1, \nu_2, \ ..., \nu_g\right)$ – множина гілок; $R = \left(r_1, r_2, \ ..., r_m\right)$ – множина ребер; $P : V \to 2^X$ – відображення, яке кожному елементу $\nu \in V$ ставить у відповідність множину $P(\nu)$ з X його вершин. Тим самим відображення P визначає гіперграф $PS = \left(X, V; P\right)$; $F : R \to 2^V_{PS}$ – відображення, яке кожному елементу $r \in R$ ставить у відповідність множину $F(r)$ його гілок, причому сімейство підмножин гілок 2^V_{PS} містить такі підмножини, гілки яких складають зв'язну частину гіперграфа PS; відображення F визначає гіперграф $FS = (V, R; F)$; $W : r \to 2^{P(F(r))} \ \forall \ r \in R$ – відображення, яке зіставляє кожному елементу $r \in R$ підмножину $W(r)$ з $P(F(r))$ його вершинами, де $P(F(r))$ – множина вершин в PS, інцидентних гілкам $F(r)$ із V. Таким чином, відображення W визначає гіперграф $WS = (X, R; W)$.

Гіперграф PS назвемо первинною мережею гіпермережі, а гіперграф WS – вторинною.

Неважко помітити, що відображення *P, F, W* є відношеннями інцидентності у відповідних гіперграфах *PS, FS, WS* і, відповідно, вони визначають інцидентність елементів в абстрактній гіпермережі *AS*. На рис. 1 наведена діаграма відношення інцидентності.

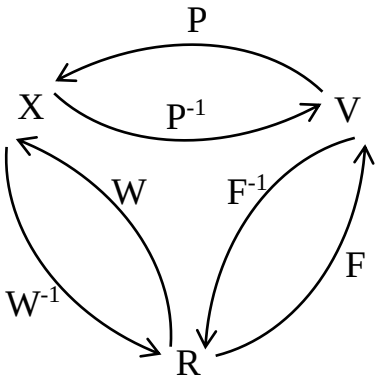


Рисунок 1 – Діаграма відношення інцидентності гіпермережі
інтегральної інформаційної мережі

Іншими словами вершина $x \in X$ інцидентна гілці $v \in V$ тоді і тільки тоді, коли $x \in P(v)$; гілка $v \in V$ інцидентна ребру $r \in R$ тоді і лише тоді, коли $v \in F(r)$; ребро $r \in R$ інцидентне вершині $x \in X$ тоді і лише тоді, коли $x \in W(r)$.

Важливим поняттям є також відношення слабкої інцидентності елементів абстрактної гіпермережі. А саме, два елементи із різних множин слабо інцидентні, якщо знайдеться елемент із третьої множини, інцидентний їм обом. Наприклад, вершина $x \in X$ слабо інцидентна ребру $r \in R$, якщо і тільки якщо існує елемент $v \in V$, такий, що $x \in P(v)$ і $v \in F(r)$, тобто $x \in P(F(r))$. Зрозуміло, що слабо інцидентні елементи можуть бути також інцидентними, навпаки невірно.

З рис. 1 видно, що для елементів гіпермереж можна визначити шість понять суміжності елементів. Дійсно, аналогічно з графами і гіперграфами два елементи із однієї множини суміжні тоді і лише тоді, коли знайдеться елемент із другої множини, інцидентний їм обом. Але так як в гіпермережах для елемента із будь-якої множини можуть бути знайдені інцидентні елементи з двох різних множин, то відповідно маємо два поняття суміжності. Наприклад, вершини x_1 і x_2 із X *v*-суміжні, якщо $\exists v \in V$: $x_1 \in P(v)$ і $x_2 \in P(v)$, і ці вершини *r*-суміжні, якщо $\exists r \in R$: $x_1 \in W(r)$ і $x_2 \in W(r)$. Аналогічним чином визначається суміжність інших елементів *AS*.

Абстрактна гіпермережа $S = (X, V, R; P, F, W)$ називається гіпермережею, якщо:

1) $|P(v)| = 2 \; \forall v \in V, |W(r)| = 2 \; \forall r \in R,$

2) множина $F(r)$ із V складає маршрут в графі $PS = (X, V) \; \forall \; r \in R$.

Таким чином, первинна *PS* і вторинна *WS* мережі гіпермережі *S* є графами, а *F* відображає ребра $WS = (X, R)$ в маршрути графа $PS = (X, V)$.

На рис. 2 зображена гіпермережа та всі її складові частини.

Для кожного значення $x_i \in X$ визначені функція $\beta_i(t)$, яка в подальшому буде трактуватися як ємність буфера на відповідний момент часу, функція $\gamma_i(t) = 1$, якщо вершина x_i знаходиться в робочому стані (тобто справний її прообраз в мережі) в момент *t*, і функція $\gamma_i(t) = 0$ в іншому випадку.

Для кожної гілки $v_j \in V$ поставимо у відповідність функції $\alpha_j(t) \geq 0$ (пропускна здатність відповідної інформаційної мережі) і $\delta_k(t) \geq 0$ (пропускна здатність каналу зв'язку між двома терміналами в мережі), причому $\delta_k(t)$ відповідає ребру $r_k \in R$.

Очевидно, що у випадку $v_j \in V \;\; \forall t \geq 0$

$$\sum_{r_k \in F^{-1}(v)} \delta_k(t) \le \alpha_i(t),$$

тобто пропускна здатність інформаційної мережі в будь-який момент часу не менша, ніж сумарна пропускна здатність каналів, реалізованих в даній мережі. Таким чином, визначена нестаціонарна гіпермережа $AS(t) = (X, V, R; P, F, W)$, в якій між вершинами *x* та *y* можна знайти максимальний потік за час *T* починаючи з t_0.

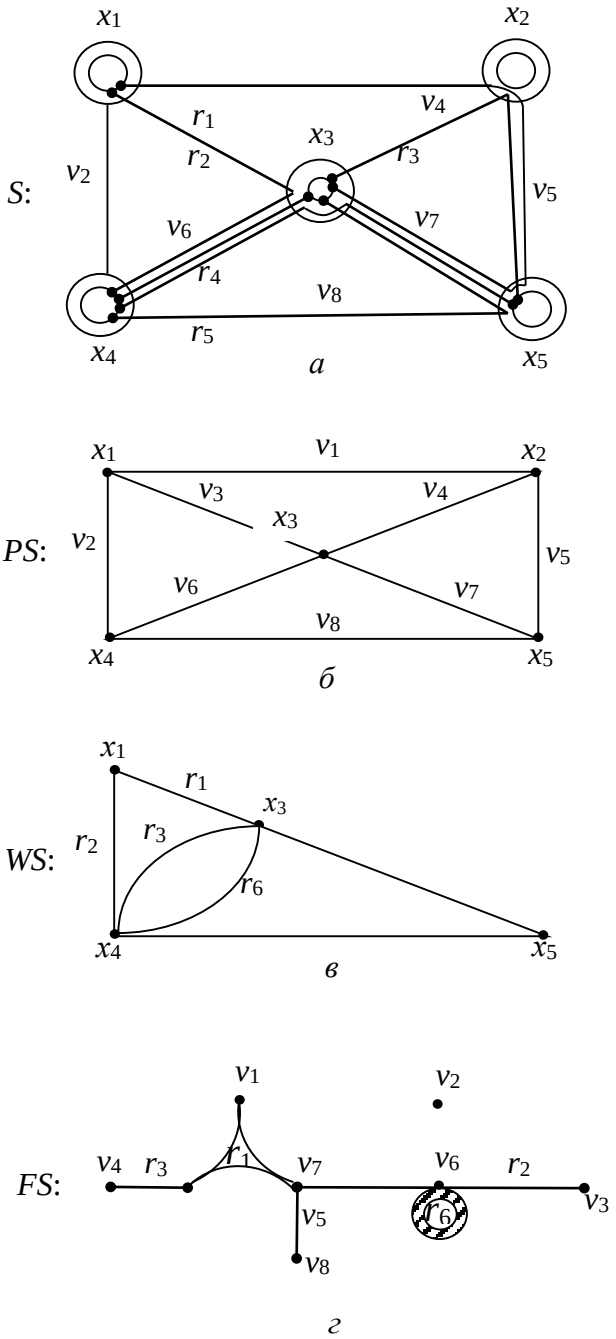


Рисунок 2 – Гіпермережа і її складові:
а – гіпермережа; *б* – первинна мережа *PS*; *в* – вторинна мережа *WS*; *г* – гіпермережа *FS*

Ієрархічні гіпермережі. Найчастіше гіпермережі буває недостатньо для того, щоб описати ієрархічну структуру, яка має більш ніж два рівня. Для цього можуть бути використані ієрархічні гіпермережі.

Ієрархічна гіпермережа – впорядкована множина графів, сусідні елементи якої утворюють гіпермережу [5]:

$$HS = \left(PS, WS_1, WS_2, \ \ldots, WS_h\right).$$

Іншими словами, якщо взяти гіпермережу $Sp\left(X, R_{p-1}, R_p\right)$, утворену WS_{p-1} і WS_p, то WS_{p-1} – первинна мережа S_p, WS_p – вторинна, R_{p-1} – множина ребер WS_{p-1}, R_p – множина ребер WS_p.

Можна говорити про гіпермережі *p*-го рівня, де WS_{p-1} – первинна мережа, якщо $p > 1$, *PS* – первинна мережа, якщо $p = 1$.

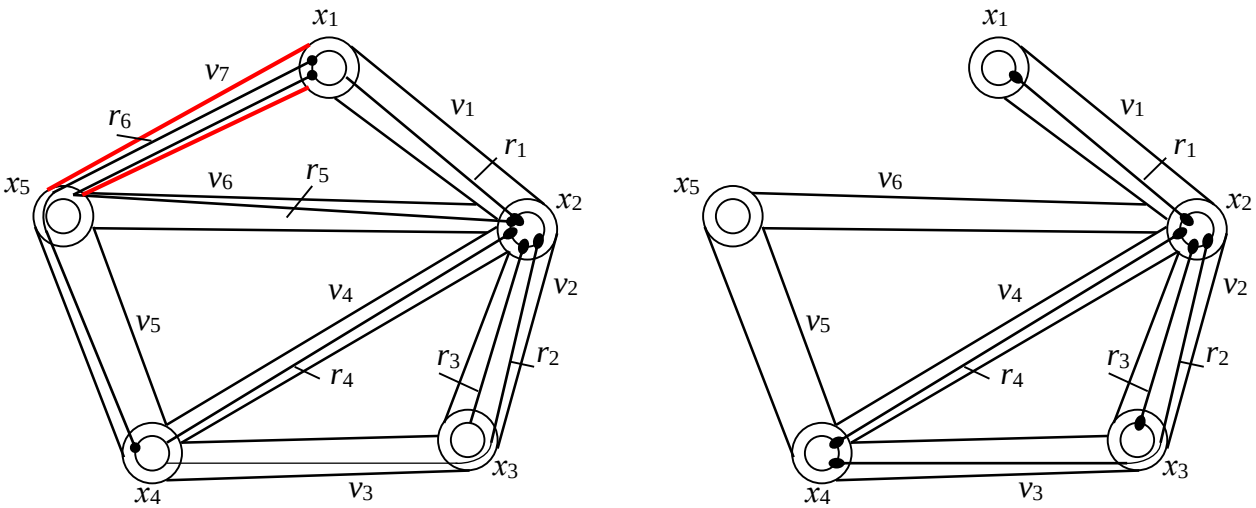
Сформулюємо поняття видалення *p*-го рівня. Внутрішнє (зовнішнє) видалення *p*-го рівня – це видалення вершини гіпермережі рівня *p*, при якому видаляються інцидентні ребра, строго слабо інцидентні ребра, а також сама вершина і гілки гіпермережі *p*-го рівня.

Очевидно, що видалення *p*-го рівня вплине на всі гіпермережі, рівень яких вище *p*. Таким чином, якщо розглянути графи WS_{p-1}, WS_p і WS_{p+1}, то видалення будь-якого ребра *r* з WS_p, спричинене будь-яким видом видалення вершини з гіпермережі S_p, призведе до видалення всіх ребер WS_{p+1}, інцидентних ребру *r* в гіпермережі S_{p+1}. Якщо параметри ієрархічної гіпермережі залежать від часу, то вона називається нестаціонарною.

Види видалення елементів. Для того, щоб проводити всебічний аналіз функціональної стійкості та оцінювати вплив руйнівних факторів на інформаційну мережу, потрібно також описати поняття видалення елементів гіпермережевих моделей:

1) видалення ребер: ребро *r* буде видалено, якщо з графа *WS* буде видалено ребро *r*;

2) видалення гілок: гілка *v* буде видалена, якщо вона буде видалена з графа первинної мережі *PS*, а з графа вторинної мережі будуть видалені всі інцидентні цій гілці ребра (рис. 3).



а *б*

Рисунок 3 – Приклад видалення гілки v_7 із гіпермережі:
а – до видалення гілки; *б* – після видалення

Для гіпермережі розрізняють три способи видалення вершин (рис. 4):

1. Вершина *x* буде внутрішньо видалена, якщо будуть видалені всі інцидентні їй ребра, тобто в графі *WS* вершина *x* виявиться ізольованою.

2. Вершина *x* буде зовні видалена, якщо будуть видалені всі слабо інцидентні (але не інцидентні) їй ребра. На графі *WS* це відповідає видаленню деякої підмножини ребер, а на гіперграфі *FS* – слабкому видаленню підмножини ребер.

3. Вершина *x* буде видалена, якщо будуть видалені всі інцідентні їй гілки і вона сама.

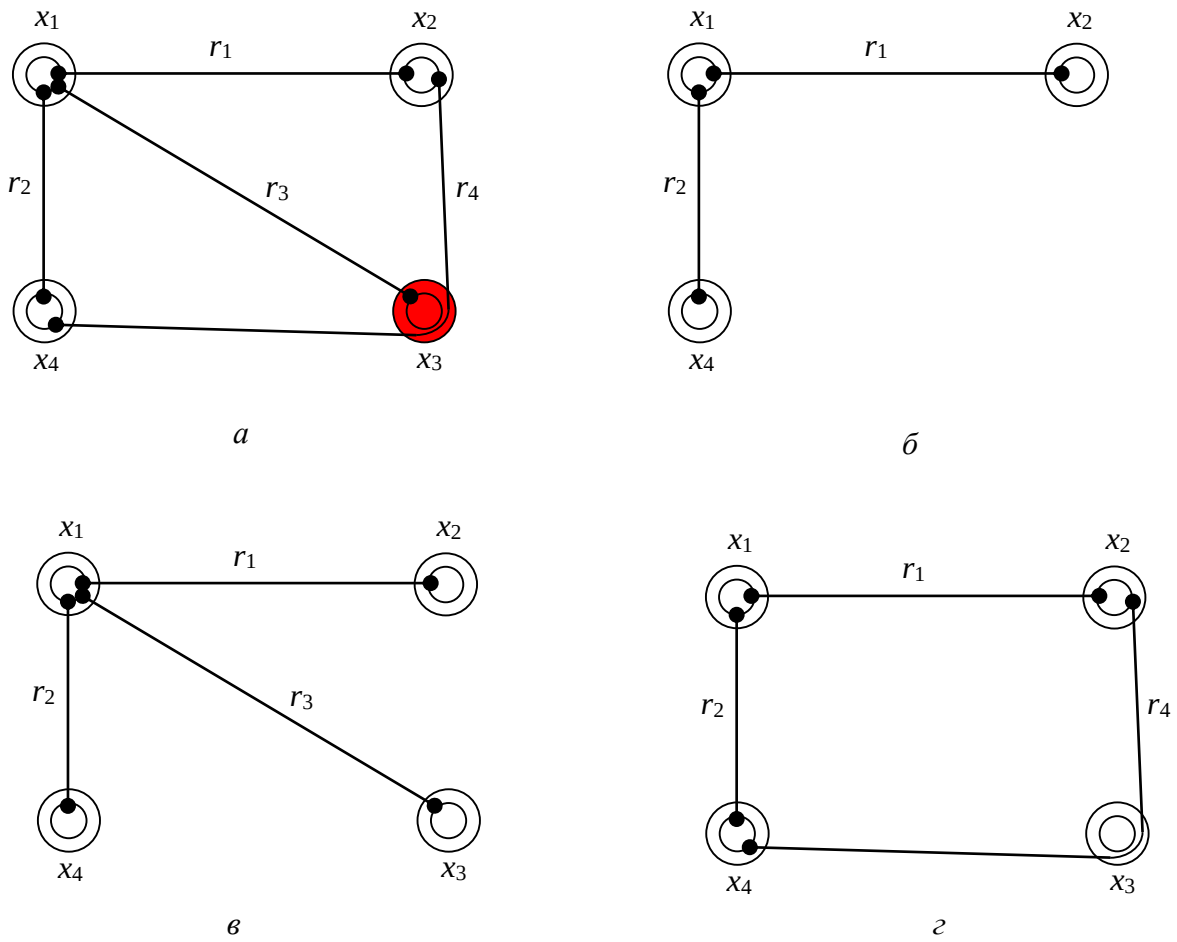


Рисунок 4 – Різні види видалення вершини x_3 із гіпермережі:
а – вихідна гіпермережа; *б* – гіперсеть після видалення вершини; *в* – гіпермережа після зовнішнього видалення вершини;
г – гіпермережа після внутрішнього видалення вершини

Висновки. Дослідження процесу функціонування сучасних інформаційних мереж надали можливість розробити математичну модель ІІМ на основі нестаціонарної гіпермережі. Методи відомих теорій не завжди дозволяють досліджувати гіпермережі. Тому дана модель враховує усі необхідні основні з точки зору функціональної стійкості параметри мережі, їх властивості та відношення, які здійснюють значний вплив на синтез оптимальної структури мережі.

Відмінність гіпермереж від інших структурних моделей полягає в тому, що в створені структури гіпермережі бере участь більше двох твірних множин, що дозволяє врахувати вплив можливих позаштатних ситуацій, які обумовлені внутрішніми і зовнішніми чинниками. Таким чином, забезпечення ІІМ властивості функціональної стійкості стикається з новою теоретичною проблемою, що вимагає для її рішення розробки адекватного математичного апарату синтезу системи.

Перспективними шляхами подальших досліджень у зазначеному напрямку може бути широке коло питань щодо розробки нових та удосконалення існуючих методик підвищення рівня функціональної стійкості інформаційних мереж, які мають автономно функціонувати в умовах впливу зовнішніх та внутрішніх дестабілізуючих факторів.

ЛІТЕРАТУРА:

1. Построение функционально устойчивых распределенных информационных систем: монография / О.В. Барабаш. К.: НАОУ, 2004. 226 с.

2. Саланда І.П., Барабаш О.В., Мусієнко А.П. Система показників та критеріїв формалізації процесів забезпечення локальної функціональної стійкості розгалужених інформаційних мереж. Наукове періодичне видання «Системи управління, навігації та зв'язку». Полтава: ПНТУ, 2017. Вип. 1 (41). С. 122 – 126.

3. Саланда І.П., Барабаш О.В., Мусієнко А.П., Лукова-Чуйко Н.В. Математична модель структури розгалуженої інформаційної мережі 5 покоління (5G) на основі випадкових графів. Наукове періодичне видання «Системи управління, навігації та зв'язку». Полтава: ПНТУ, 2017. Вип. 6 (46). С. 118 – 121.

4. Мусієнко А.П. Неділько С.М., Арделян В.В. Математична формалізація функціональної стійкості пілотажно-навігаційного комплексу повітряного судна під час горизонтального польоту. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2017. Вип. 58. С. 48 – 53.

5. Musienko A.P., Barabash O.V., Lukova-Chuiko N.V., Salanda I.P. Diagnostic model of wireless sensor network based on the random test of checks. Science and Education a New Dimension. Natural and Technical Sciences, 2018. VI (18), Issue 158, Budapest, Hungary, P. 25 – 28.

6. Musienko A., Barabash O., Shevchenko G., Dakhno N., Neshcheret O. Information Technology of Targeting: Optimization of Decision Making Process in a Competitive Environment. International Journal of Intelligent Systems and Applications. Vol. 9. № 12. Hong Kong: MECS Publisher, 2017. P. 1 – 9.

7. Zhang H., Shen H. Balancing Energy Consumption to Maximize Network Lifetime in Data-Gathering Sensor Networks. IEEE Trans. Parallel Distrib. Syst. 2009. Vol. 20, № 10. P. 1526 – 1539.

8. Musienko A., Pashynska N., Snytyuk V., Putrenko V. A decision tree in a classification of fire hazard factors. Eastern-European Journal of Enterprise Technologies. Kharkov, 2016. № 5/10(83). P. 32 – 37.

9. Xie L., Shi Y., Hou Y.T., Sherali H.D. Making sensor networks immortal: An energyrenewal approach with wireless power transfer .IEEE/ACM Trans. on Networking. Dec. 2012. V. 20. № 6. P. 174 – 1761.

10. Пампуха І.В., Самолов І.В., Толюпа С.В., Берназ Н.М. Інтелектуальний підхід до управління мережними відмовами систем передачі даних. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К: ВІКНУ, 2008. №20. С. 18 – 21.

11. Математические модели живучести сетей связи: монография / В.К. Попков. – Новосибирск: Вычислительный центр СО АН СССР, 1990. – 235 с.

12. Akkaya K., Younis M. A Survey on Routing Protocols for Wireless Sensor Networks, Elsevier Ad Hoc Network Journal, 2005 vol. 3, №.3, P. 325 –349.

REFERENCES:

1. Postroenye funktsyonalno ustoichyvыkh raspredelennыkh ynformatsyonnыkh system: monohrafyia / O.V. Barabash. K.: NAOU, 2004. 226 p.

2. Salanda, I.P., Barabash, O.V., Musiienko, A.P. (2017), “Systema pokaznykiv ta kryteriiv formalizatsii protsesiv zabezpechennia lokalnoi funktsionalnoi stiikosti rozghaluzhenykh informatsiinykh merezh”. [Naukove periodychne vydannia «Systemy upravlinnia, navihatsii ta zviazku».] Poltava: PNTU, Vyp. 1 (41). pp. 122 – 126.

3. Salanda, I.P., Barabash, O.V., Musiienko, A.P., Lukova-Chuiko, N.V. (2017), “Matematychna model struktury rozghaluzhenoi informatsiinoi merezhi 5 pokolinnia (5G) na osnovi vypadkovykh hrafiv”. [Naukove periodychne vydannia «Systemy upravlinnia, navihatsii ta zviazku»]. Poltava: PNTU, Vyp. 6 (46). pp. 118 – 121.

4. Musiienko, A.P. Nedilko, S.M., Ardelian, V.V. (2017), “Matematychna formalizatsiia funktsionalnoi stiikosti pilotazhno-navihatsiinoho kompleksu povitrianoho sudna pid chas horyzontalnoho polotu”. [Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka]. K.: VIKNU, 2017. Vyp. 58. pp. 48 – 53.

5. Musienko, A.P., Barabash, O.V., Lukova-Chuiko, N.V., Salanda, I.P. (2018), “Diagnostic model of wireless sensor network based on the random test of checks”. [Science and Education a New Dimension. Natural and Technical Sciences]. VI (18), Issue 158, Budapest, Hungary, pp. 25 – 28.

6. Musienko, A., Barabash, O., Shevchenko, G., Dakhno, N., Neshcheret, O. (2017), “Information Technology of Targeting: Optimization of Decision Making Process in a Competitive Environment”. [International Journal of Intelligent Systems and Applications.] Vol. 9. № 12. Hong Kong: MECS Publisher, P. 1 – 9.

7. Zhang, H., Shen, H. “Balancing Energy Consumption to Maximize Network Lifetime in Data-Gathering Sensor Networks”. (2009), [IEEE Trans. Parallel Distrib. Syst]. Vol. 20, № 10. pp. 1526 – 1539.

8. Musienko, A., Pashynska, N., Snytyuk, V., Putrenko, V. (2016), “A decision tree in a classification of fire hazard factors”. [Eastern-European Journal of Enterprise Technologies]. Kharkov, № 5/10(83). pp. 32 – 37.

9. Xie, L., Shi, Y., Hou, Y.T., Sherali, H.D. (2012), “Making sensor networks immortal: An energyrenewal approach with wireless power transfer” . [IEEE/ACM Trans. on Networking. Dec.] V. 20. № 6. pp. 174 – 1761.

10. Pampukha, I.V., Samolov, I.V., Toliupa, S.V., Bernaz, N.M. (2008), “Intelektualnyi pidkhid do upravlinnia merezhnymy vidmovamy system peredachi danykh”. [Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka]. K: VIKNU, 2008. №20. pp. 18 – 21.

11. Matematycheskye modely zhyvuchesty setei sviazy: monohrafyia / V.K. Popkov. – Novosybyrsk: Vыchyslytelnыi tsentr SO AN SSSR, 1990. – 235 p.

12. Akkaya, K., Younis, M. “A Survey on Routing Protocols for Wireless Sensor Networks”, [Elsevier Ad Hoc Network Journal], 2005 vol. 3, №.3, pp. 325 – 349.

к.ф.-м.н., доц. Собчук В.В., к.т.н., с.н.с. Лаптев А.А.,
к.т.н. Саланда И.П., к.ф.-м.н. Сачук Ю.В.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СТРУКТУРЫ ИНФОРАЦИЙНОИ СЕТИ НА ОСНОВЕ НЕСТАЦИОНАРНОЙ ИЕРАРХИЧЕСКОЙ И СТАЦИОНАРНОЙ ГИПЕРСЕТИ

В статье разработана модель структуры интегральной информационной сети на основе нестационарной иерархической и стационарной гиперсеть, с учетом разрушительных воздействий различного характера. Под функциональной устойчивостью интегральной информационной сети в работе понимается возможность функционирования системы, пусть с уменьшением качества, в течение заданного времени под влиянием внешних и внутренних дестабилизирующих факторов. Под внешними и внутренними дестабилизирующими факторами понимаются отказа, сбои элементов системы, умышленные повреждения, боевые поражения, электромагнитные помехи, ошибки обслуживающего персонала. Обеспечение свойства функциональной устойчивости любой сложной технической системы осуществляется в три этапа: идентификация нештатной ситуации, локализация нештатной ситуации, восстановления функционирования за счет перераспределения ресурсов. При рассмотрении интегральных информационных сетей с точки зрения функциональной устойчивости, выход из строя узла коммутации или линии связи влечет за собой разрушение каналов передачи вторичных сетей, в графах этих сетей является несмежными. Поэтому моделировать структуру такой сети графом нецелесообразно. В связи с этим, введены новые понятия и определения в теорию функциональной устойчивости и разработан соответствующий методический аппарат. Данная модель учитывает все необходимые основные с точки зрения функциональной устойчивости параметры сети, их свойства и отношения, которые осуществляют значительное влияние на синтез оптимальной структуры сети. Отличие гиперсеть от других структурных моделей заключается в том, что в создании структуры гиперсеть участвует более двух образующих множеств, позволяет учесть влияние возможных внештатных ситуаций, обусловленных внутренними и внешними факторами.

Ключевые слова: гиперсеть, нестационарная гиперсеть, информационные сети, функциональная устойчивость, разрушительные воздействия.

Ph.D. Sobchuk VV, Ph.D. Laptev A.A., Ph.D. Salanda I.P., Ph.D. Sachuk Yu.V.

MATHEMATICAL MODEL OF INFORMATION NETWORK STRUCTURE ON THE BASIS OF NON-STATIONARY HIERARCHICAL AND STATIONARY HYPERSLETS

The article developed a model of the structure of an integrated information network based on a non-stationary hierarchical and stationary hypernetwork, taking into account the destructive effects of various kinds. The functional stability of the integrated information network in the work is understood as the ability of the system to function, albeit with a decrease in quality, for a given time under the influence of external and internal destabilizing factors. External and internal destabilizing factors are understood as failures, malfunctions of system elements, deliberate damages, combat defeats, electromagnetic interferences, maintenance personnel errors. Ensuring the functional stability of any complex technical system is carried out in three stages: identifying abnormal situations, localizing abnormal situations, restoring operation due to the redistribution of resources. When considering integrated information networks from the point of view

of functional stability, the failure of a switching node or communication line entails the destruction of the transmission channels of secondary networks, in the graphs of these networks are non-adjacent. Therefore, it is impractical to model the structure of such a network by a graph. In this regard, introduced new concepts and definitions in the theory of functional stability and developed an appropriate methodological apparatus. This model takes into account all the necessary basic parameters from the point of view of functional stability of the network, their properties and relations, which have a significant impact on the synthesis of the optimal network structure. The difference between a hypernetwork and other structural models is that the creation of a hypernetwork structure involves more than two generating sets, allows you to take into account the influence of possible emergency situations caused by internal and external factors.

Keywords: hyper-network, non-stationary hyper-network, information networks, functional stability, destructive effects.

Ph.D. Khmelnitsky Y.V., prof. Selyukov A.V., Kovpa D.M.

ANALYSIS OF MODELS AND PROGNOSTICATION OF RISKS OF FUNCTIONING OF CONTROL SYSTEM OF SDN OF ARCHITECTURE

The article deals with the analysis of models and algorithms of the system control SDN of architecture for providing of more quality work of network. Great diversity of most hardware implementation of the data devices SDN architecture leads to the fact that different switches may not support some features or support them with limited performance. In the process network, this can significantly affect the throughput of an individual data flow or whole network domains. Routing flow transfer is carried out by criterion of quality of service and the criterion of balanced loads of network resources the network. Improving the quality of service is subject to the classification of the flow that greatly restricts the ability of flow control. Most models of such networks do not take into account the characteristics of multi-service data flow, which leads to deterioration in the quality of service and increase the likelihood of blocking the channels of transmission network. The inability to implement differentiated management for individual data streams for individual clients and take them into account quality requirements, leads to low efficiency of channel routing, suboptimal distribution of network load, the deterioration of the quality of service high-priority data streams. Tools control over the process of transmission of individual data flow do not exist, whereby the control system has the ability to determine service degradation for these data streams, and therefore will not be able to guarantee the necessary level of control. New models and algorithms of functioning of a software – managed network will allow for routing data streams of network, differentiating them according to the sensitivity to mixing of packet and connection drops. At created networks try to dissociate C-plane from the plane of transmission and put considerable efforts to overcoming of the nascent problems related to complications of migration from traditional networks to architecture of SDN.

The aim of this article is realization of analysis of models and algorithms of functioning of control system of architecture of SDN for more reliable work of network. It gives possibility to the users to get services with necessary quality, by authenticity and will allow overcoming the nascent problems related to complications of migration from traditional networks to architecture of SDN.

Keywords: software driven networks SDN control of network devices, SDN architecture, models and algorithms of the control system, the level of functioning of the network.

УДК 004.891

к.т.н., доц. **Хмельницький Ю.В.** (ХмНУ)
Каблуков О.А. (ЦНДІ ЗСУ)
Ряба Л.О. (ВІКНУ)
Солодєєва Л.В. (ВІКНУ)
Ткач А.О. (ХмНУ)

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЗАВАДОСТІЙКОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

У статті проведено аналіз методів та засобів забезпечення завадостійкої передачі інформації в телекомунікаційних мережах які застосовують технології, що дозволяють у режимі реального часу гарантувати якісну, надійну та вірогідну передачу даних в умовах впливу завад. Для телекомунікаційних мереж завдання оптимального та якісного прийому інформації полягає у використанні властивостей корисного сигналу, завади та каналу передачі для збільшення ймовірності правильного прийому. Для збільшення ймовірності правильного прийому має бути проведене попереднє оброблення прийнятого сигналу, що забезпечує збільшення відношення сигнал та завада. Канали передачі даних, що застосовують технології, які дозволяють у режимі реального часу гарантувати якісну, надійну та вірогідну передачу даних в умовах впливу завад, краще забезпечують заданих значень показників вірогідної передачі інформації здійснюється за рахунок використання необхідного кодування. Під час передачі такими каналами виникає багато труднощів, пов'язаних із впливом природних, промислових, навмисних та ненавмисних завад. Всі способи завадостійкості загалом ведуть до часової та апаратурної надмірності як із боку джерела інформації, так і з боку адресата. Якщо розглядати завадостійкість телекомунікаційної мережі як здатність системи протидіяти завадам, то треба знати, чим протидіяти і на що протидіяти, тобто для боротьби із завадами потрібні апріорні відомості про властивості носія інформації та про самі завади. Знаючи всі ці властивості сигналу та завади, можна встановити певні відмінності між ними і використати їх для розроблення способів, засобів та методів забезпечення завадостійкості.

Метою даної статті є проведення аналізу методів та засобів забезпечення завадостійкої передачі інформації в телекомунікаційних мережах, що дозволить у режимі реального часу гарантувати якісну, надійну та вірогідну передачу даних в умовах впливу завад. На відміну від спотворень завади носять випадковий характер. Вони заздалегідь невідомі і тому не можуть бути повністю усунені. Знання методів та засобів побудови сучасних каналів передачі телекомунікаційною мережею в умовах дії завад, дозволить будувати надійні канали передачі інформації для таких мереж.

Ключові слова: завади, завадостійкість, канали передачі, телекомунікаційна мережа, спотворення, вірогідність передачі інформації, надійність, невизначеність.

Постановка проблеми. Сучасні телекомунікаційні мережі визначаються значною кількістю параметрів, функціональними можливостями, конкурентоспроможністю, вимогами до забезпечення захисту інформації, високою надійністю, точністю, вірогідністю, розгалуженою інфраструктурою. Велика кількість службової інформації у таких системах значно зросла разом із ростом об'ємів надання послуг, тому потрібно реорганізувати такі мережі для можливості впровадження нових технологій у майбутньому. Для якісної та надійної передачі даних у телекомунікаційних мережах задача забезпечення завадостійкості є однією із головних задач. Мережа має бути запроектована та експлуатуватись так, щоб у разі наявності завад вона забезпечила задану якість передавання інформаційних сигналів. Розрахунки впливу завад на передавання сигналів та розробка способів зменшення цього впливу є основними задачами, що вирішуються при проектуванні завадостійкості телекомунікаційних мереж. Загалом під завадостійкістю каналу передачі розуміють здатність мережі розрізняти та відновлювати сигнали із заданою достовірністю за наявності зовнішніх та внутрішніх завад. В ряді витоків визначення поняття завадостійкості це здатність системи протистояти шкідливій дії завад, хоча воно більше наближається до розуміння фізичної суті завадостійкості - тут мається на увазі не просто стійкість системи передачі до завад, а її спроможність правильно функціонувати за їх

наявності. Завдання визначення завадостійкості всієї телекомунікаційної мережі досить складне, тому досить часто визначають завадостійкість окремих ланок мережі, наприклад приймача, перетворювача для заданих способів передачі, системи кодування, модуляції тощо. В загальному випадку завадостійкість телекомунікаційної мережі залежить від виду повідомлень, рівня та характеристик завад, параметрів окремих складових частин мережі. В умовах динамічних завад збільшується ймовірність помилки, стає неможливим забезпечення заданого рівня надійності та вірогідності інформації за допомогою простого використання відомих методів кодування. Сучасні методи управління, які застосовуються для забезпечення заданої надійності інформації на основі завадостійких кодів, носять розрізнений характер. У процесі функціонування на сучасні телекомунікаційні мережі та її елементи можуть впливати різні фактори, що порушують її нормальну роботу. Тому вони призводять до порушення роботи каналів та ліній передачі у мережі, фізичного виходу з ладу елементів телекомунікаційної мережі, інших негативних наслідків, у результаті чого вони переходить до стану, за якого вона не може забезпечувати процес доставки необхідної інформації. Тому телекомунікаційна мережа повинна мати здатність протистояти завадам, впливам та перешкодам, які порушують її роботу. Маючи необхідну надійність та завадостійкість телекомунікаційної мережі можливо забезпечити задану стабільність та безперервність управління.

Аналіз останніх досліджень і публікацій. Теорія та техніка передачі інформації в телекомунікаційних мережах складалися протягом багатьох років і сьогодні продовжують швидко розвиватися. Особливе місце канали передачі інформації займають у системах управління де враховуються завадостійкість каналів зв'язку, основи побудови телекомунікаційних мереж, застосування імітаційних завад в радіоканалах [1 - 3]. Управління сучасними телекомунікаціями із застосуванням новітніх технологій [4] дозволяє забезпечити задану стабільність та безперервність управління, а математична модель оцінки достовірності передачі інформації в мережах за умов впливу структурних завад [5] дозволяє забезпечити задану стабільність та безперервність управління. Імітаційна модель системи передачі забезпечує підвищення достовірності передачі [6], а роботи Шеннона К.Є. [7] покращують сучасну математичну теорію передачі інформації. Дослідження характеристик захищеності мереж [8] з сигналами OFDM забезпечує перебудову під несущих частот в умовах оптимальних перешкод за допомогою теорії кодів, що виправляють помилки [9]. Аналіз методів виявлення вторгнень у мобільні радіо мережі [10] допомагає забезпечити достовірність передачі інформації та сервісних послуг для мереж при завадах [11]. Аналіз принципів функціонування, технології, протоколи [12] та методи передачі показує, що вони мають як переваги, так і недоліки. Тому проблема підвищення ефективності роботи каналів передачі телекомунікаційних мереж в умовах невизначеності вирішується за рахунок забезпечення вірогідності інформації та за рахунок створення нової інформаційної технології, моделей і методів. Для досягнення поставленої мети необхідно вирішити проблему, яка полягає в забезпеченні завадостійкої передачі інформації в умовах невизначеності за рахунок методів, що використовують послідовність процесів багаторівневої адаптації та додаткових показників розкриття невизначеності при впливі різних завад.

Мета роботи – провести аналіз методів та засобів забезпечення завадостійкої передачі інформації у телекомунікаційних мережах, що дозволяють у режимі реального часу гарантувати якісну, надійну та вірогідну передачу даних в умовах впливу завад. Це дозволить будувати сучасні надійні канали передачі телекомунікаційною мережею в умовах дії завад.

Основний матеріал досліджень. Проаналізуємо властивості телекомунікаційних мереж, які є найбільш істотними з погляду користувача і з погляду забезпечення заданого рівня вимог до завадостійкості, надійності та вірогідності каналів зв'язку як процесу доставки інформації. В процесі функціонування на телекомунікаційні мережі та її елементи впливають різні фактори, що порушують нормальну роботу. Вони призводять до порушення роботи каналів та ліній зв'язку, фізичного виходу з ладу елементів мереж, інших негативних наслідків, у результаті чого вони переходить до такого стану, при якому не може забезпечувати процес доставки необхідної інформації. Таким чином, сучасна мережа повинна мати здатність протистояти впливам, які порушують її роботу, що забезпечується стійкості її роботи. Під час функціону-

вання доставки інформації може порушуватися не тільки факторами, що безпосередньо впливають на роботу каналу передачі в цілому але і бути готовою до елементів потенційної та реальної завадостійкості. В даному випадку під потенційною завадостійкістю розуміють максимальну завадостійкість для заданих сигналів та завад. Потенційна завадостійкість визначає таку граничну якість, яку можна дістати у заданій телекомунікаційній мережі, проте неможливо перевищити ніяким обробленням для існуючої завади. Загалом реальна завадостійкість - це завадостійкість телекомунікаційній мережі чи окремих її вузлів із урахуванням реального виконання та настройки окремих блоків каналу передачі. Теоретично та технологічно не всі блоки каналу передачі можна виготовити ідеальними із заздалегідь визначеними параметрами. також завжди є похибки установлення параметрів тих чи інших вузлів під час експлуатації мережі. Реальна завадостійкість практично залежить від великої кількості факторів та параметрів окремих ланок телекомунікаційної мережі та завжди менша за теоретичну потенційну завадостійкість. В таких умовах телекомунікаційна мережа повинна мати здатність адаптації до всіх можливих змін. Зробимо висновок, що тільки у разі забезпечення усіх властивостей, телекомунікаційна мережа може виконувати своє функціональне призначення - забезпечувати доставку всієї інформації у необхідному обсязі, із заданою якістю та вірогідністю. Дослідження та аналіз існуючого стану та методів забезпечення завадостійкої доставки інформації мереж передачі показав, що перспективним напрямком вирішення проблеми забезпечення вірогідності інформації в умовах значної невизначеності та завад є застосування необхідних видів кодування та багаторівневої структурної та параметричної адаптації із врахуванням розкриття невизначеності. Сьогодні виникає протиріччя між обмеженими можливостями традиційних підходів щодо завадостійкого контролю, класифікації та кодування інформації, методами та моделями забезпечення вірогідності мультимедійної інформації, що ґрунтуються на надлишкових критеріях та потребами створення організованої послідовності процесів адаптації багаторівневих систем із урахуванням невизначеності.

При розгляді методів та засобів забезпечення завадостійкої передачі інформації в телекомунікаційних мережах необхідно розглянути, що в широкому розумінні являє собою передачу різного роду повідомлень із декількох пунктів в ряд пунктів. В технологіях та засобах передачі інформації семантична особливість повідомлень не враховується, і тому задачею системи передачі інформації в телекомунікаційній мережі є лише транспортування даних у визначене місце, так як оцінка змісту отриманих повідомлень це справа самого одержувача інформації. Сама теорія і техніка передачі інформації в телекомунікаційних мережах складалися протягом багатьох років і сьогодні продовжують швидко та якісно розвиватися. Особливе місце канали передачі інформації займають у системах управління, у яких необхідно забезпечувати передачу досить великих обсягів потоків інформації із високою швидкістю, достовірністю та надійністю. У процесі функціонування на телекомунікаційні мережі та її елементи впливають багато різних факторів, що порушують нормальну роботу каналу передачі. Ці фактори призводять до порушення роботи каналів передачі, фізичного виходу з ладу елементів та компонентів мереж, інших негативних наслідків. Саму основу теорії потенційної завадостійкості розробив ще у 1946 р. академік В.О. Котельников. У ній вирішуються три такі основні задачі:

- синтез оптимального приймача - знаходження правила його роботи та структурної схеми, що забезпечують найкращу в тому чи іншому розумінні якість приймання;

- аналіз роботи оптимального приймача - обчислення якості приймання сигналів, яка забезпечується цим приймачем;

- порівняння потенційної та реальної завадостійкості.

Для практичного використання останнє завдання має особливе значення. Адже порівнювати реальну завадостійкість різних систем, схем, пристроїв, методів оброблення, видів модуляції не має ніякого сенсу. Таких схем та методів існують сотні та зростання їх числа триває, а мала завадостійкість якоїсь системи чи схеми ще не означає, що вона невдала та неякісна. За таких завад кращої якості й неможливо досягти. Тому порівняння реальної та потенційної завадостійкості дає можливість оцінювати якість реальної системи знайти ще не використані

резерви. Якщо знати потенційну завадостійкість приймача каналу передачі, можна завжди оцінити, наскільки близька до неї реальна завадостійкість існуючих способів приймання та наскільки доцільне їх подальше удосконалення для заданого методу передавання по каналах передачі. Знання про потенційну завадостійкість за різних методів передавання інформації дають змогу порівнювати ці методи між собою та знайти, які із них у цьому відношенні є найбільш оптимальними. Розглянемо кількісну міру завадостійкості. Для теоретичних розрахунків як потенційної, так і реальної завадостійкості застосовуються прямі методи оцінки якості. У разі передавання дискретних первинних сигналів для обчислень використовують ймовірність помилки. Розглянемо деякі принципи та засоби побудови систем передачі інформації по каналам з шумами та перешкодами. На рис. 1 наведена узагальнена схема системи зв'язку із завадами [2]. У загальному вигляді вимоги до системи зв'язку включає: систему передачі інформації - лінії передачі і відповідна апаратура, пристрої чи системи комутації, кінцеві пристрої.

Рисунок 1 – Узагальнена схема системи зв'язку з завадами

В іншому випадку структурна схема системи передачі інформації із завадами складається із джерела та одержувача повідомлень, перетворювачів повідомлення в сигнал та сигналу в повідомлення, каналу зв'язку. На рис. 2 зображена типова структурна схема найпростішої одно канальної системи зв'язку. Джерелом повідомлень та одержувачем в одних системах зв'язку може бути людина, в інших різного роду пристрої - автомат, комп'ютер тощо. Перетворення повідомлення у сигнал повинне бути оборотним. В цьому випадку по вихідному сигналу можна відновити вхідний первинний сигнал, тобто одержати усю інформацію, що є в переданому повідомленні. В противному випадку частина інформації буде загублена при передачі.

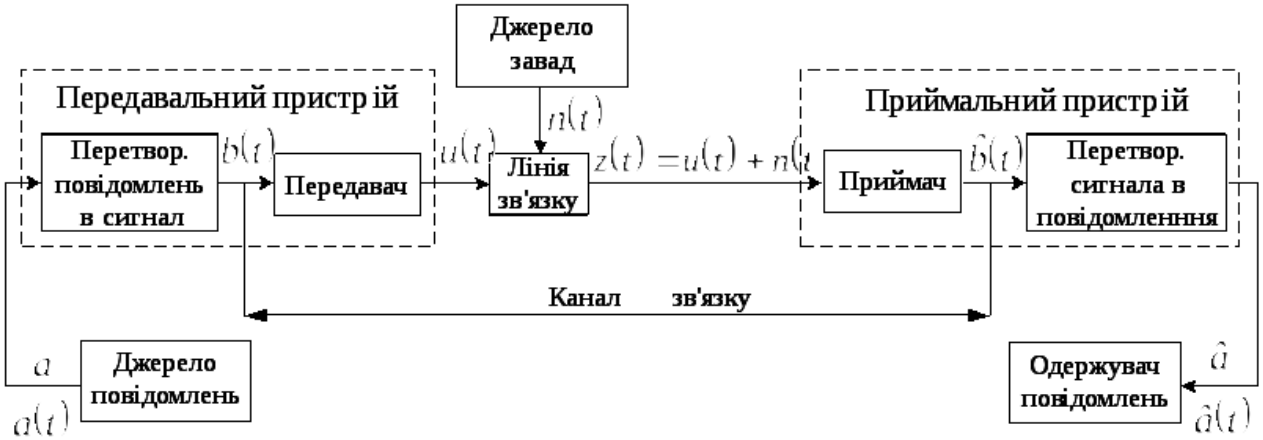


Рисунок 2 – Типова структурна схема системи передачі інформації із завадами

При передачі канальний сигнал $u(t)$ може спотворюватися та на нього можуть накладатися завади $n(t)$. Приймальний пристрій обробляє прийняте коливання $z(t) = x(t) + n(t)$,

яке є сумою перекрученого сигналу $x(t)$ і завади $n(t)$, відновлює по ньому повідомлення a, що з деякою похибкою відображає передане повідомлення a. Тобто приймач повинен на основі аналізу коливання $z(t)$ визначити, яке із можливих повідомлень передавалось. Тому приймний пристрій є одним із найбільш відповідальних та складних елементів системи зв'язку.

У системі телекомунікацій фізична величина, що підлягає виміру - температура, тиск, швидкість, за допомогою необхідних датчиків перетвориться у первинний електричний сигнал, що надходить на передавач. На прийомному кінці передану фізичну величину чи її зміни виділяють із сигналу та спостерігають чи реєструють за допомогою записуючих пристроїв. Впровадження високоефективних комп'ютерних систем привело до необхідності швидкого розвитку нових систем передачі даних, що забезпечують обмін інформацією між обчислювальними засобами та об'єктами автоматизованих систем керування. Цей вид відрізняється більше високими вимогами до швидкості та вірності передачі інформації.

На рис. 3 наведена узагальнена схема системи передачі інформації в мережі [4]. Прийнявши необхідне повідомлення від джерела повідомлень, сам кодер генерує та видає на модулятор вхідну двійкову послідовність із визначеною довжиною - кодове слово. Модулятор перетворює кожен символ на один із двох сигналів, що подаються на вхід каналу передачі інформації у телекомунікаційній мережі. Демодулятор, який підключений до виходу каналу, видає необхідний сигнал. Детектор тут обробляє сигнал та видає елемент інформації, який в двійковому випадку являє собою дійсний скаляр. Декодер перетворює послідовність у розв'язок задачі кодування, що вказує, яке із усієї сукупності кодових слів було передано. Під каналом передачі в даному випадку мається на увазі середовище, за допомогою якого здійснюється передача сигналів від передавача до приймача. Одноразове використання каналу передачі полягає у тому, що передавач певним чином впливає на канал передачі, а приймач спостерігає деякі характеристики каналу, що відображають цей вплив. Якщо ж канал передачі дискретний, то для передавача існує кінцеве число впливів, які називаються вхідними сигналами. Приймач розрізняє тільки визначене число класів результатів спостереження, що називаються загалом вихідними сигналами. Співвідношення між вхідними та вихідними сигналами у загальному випадку має імовірнісний характер. Канал визначається встановленням умовних ймовірностей p_n для кожної вхідної та вихідної послідовності.

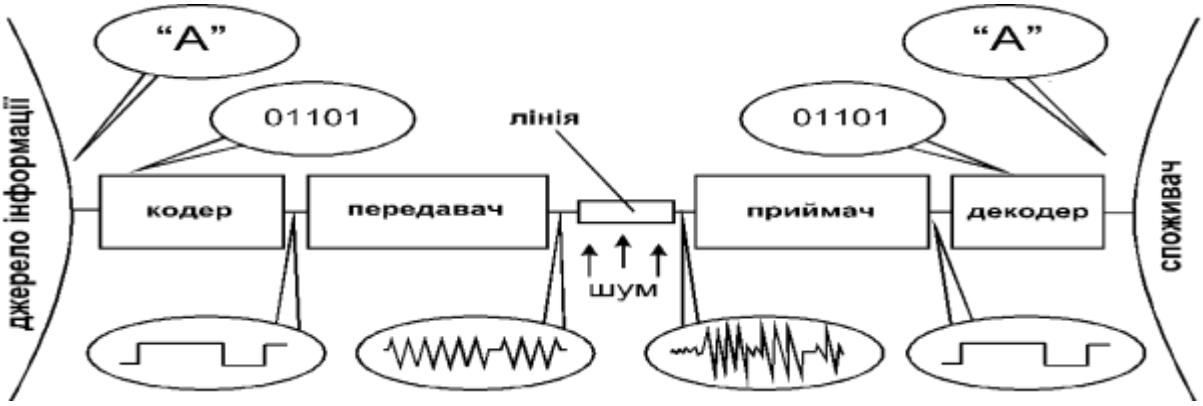


Рисунок 3 – Узагальнена система передачі інформації в мережах

Дослідивши основні взаємовпливи перешкод на основні елементи каналів передачі мережі із позиції теорії імовірності, можливо оцінити коефіцієнти за «технічною надійністю» основних компонентів та елементів телекомунікаційної мережі за допомогою відомого співвідношення [11]:

$$p_n = \exp\left(- \sum_{i=1}^{n} \frac{\tau}{\lambda_i} \right), \qquad (1)$$

де n – кількість основних компонентів телекомунікаційної мережі;

λi – напрацювання на відмову *i*-го компонента відповідного елемента мережі;

τ – час роботи каналу передачі телекомунікаційної мережі.

Загалом кодер - пристрій, який, приймаючи одне з повідомлень від джерела повідомлень, створює відповідну послідовність сигналів, що подається на вхід каналу передачі телекомунікаційної мережі. Джерело повідомлень генерує безперервний потік двійкових символів, при цьому кожні N двійкових символів перетворюються кодером у відповідне кодове слово. Декодер – це пристрій, який, приймаючи вихідну послідовність визначеної довжини, обробляє її та видає результат оброблення споживачу повідомлень у зручному для сприйняття нього вигляді. Головна мета споживача полягає в тому, щоб дізнатися, яке із кодових слів було передано. Якщо ж на вхід кодера надійшли N двійкових символів, то на виході декодера буде отримана сукупність із такого ж числа N двійкових символів, яка називається рішенням. Якщо ж рішення не збігається із вхідним кодовим словом, то має місце помилка передачі. Імовірність помилки залежить від коду та методу оброблення інформації у декодері. Якщо ж застосовується детермінований декодер, то метод оброблення інформації може бути описаний як відображення безлічі усіх прийнятих послідовностей у множину кодових слів, а відображення задається як список послідовностей які перетворюються в декодоване слово. Ступінь ризику передачі невірогідної інформації в завадостійкій системі можна подати як добуток імовірності небажаних наслідків на відповідну величину втрат аналогічно як у працях [11]:

$$R = \sum_{i=1}^{9} R_i = \sum_{i=1}^{9} p_i \cdot Z_i \,, \tag{2}$$

де R – величина ризику;

p_i – ймовірності небажаних наслідків передачі невірогідної інформації;

Zi – величини втрат інформації в каналі передачі.

Для оцінювання ризику в завадостійкій системі використовують величину середньозваженого модуля відхилення ΔZ [11]:

$$\Delta Z = \sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z}) \,. \quad \overline{Z} = \frac{1}{n} \sum_{i=1}^{n} Z_i \,. \tag{3}$$

Визначимо середньоквадратичне відхилення в завадостійкій системі:

$$\sigma = \sqrt{\sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z})^2} \,, \tag{4}$$

У відносному вираженні ризик передачі невірогідної інформації в завадостійкій системі оцінюють за допомогою коефіцієнта варіації δ_Z [11]:

$$\delta_Z = \sigma \frac{1}{\overline{Z}} = \frac{1}{\overline{Z}} \sqrt{\sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z})^2} \,. \tag{5}$$

Виходячи із величини коефіцієнта варіації δ_Z використовують таку шкалу для оцінювання рівня ризику та відповідних зон ризику передачі невірогідної інформації в завадостійких системах. Для ряду завадостійких телекомунікаційних мереж, використовують також коефіцієнт варіації [11]:

$$S_{ZV} = \sqrt{\sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z})^2 \cdot I_{vi}} \Big/ \left(\overline{Z} \cdot \sum_{i=1}^{n} p_i \cdot I_{vi} \right). \tag{6}$$

Також показником оцінювання ризику передачі невірогідної інформації може бути також коефіцієнт можливих втрат каналу передачі, який враховує обсяг втрат по відношенню до суми абсолютних значень ймовірних втрат в завадостійких системах [11]:

$$K_Z = M_{ZV} /(M_{ZV} + M_{ZP}). \quad (7)$$

де M_{ZV}, M_{ZP} – відповідно ймовірні величини сприятливих та несприятливих відхилень відносно значень показників θ_V, θ_P при розгляді запланованих рівнів втрат при передачі інформації Z і позитивних результатів Ω як це виражено у співвідношенні (8) та (9).

Як показує детальний аналіз критичних ситуацій, M_{ZV}, M_{ZP} – умовні математичні сподівання відхилень щодо вірогідної передачі по каналу завадостійкої телекомунікаційної мережі:

$$M_{ZV} = \sqrt{\sum_{i=1}^{n} p_i \cdot (Z_i - \overline{Z})^2 \cdot I_{vi}} \Big/ \left(\sum_{i=1}^{n} p_i \cdot I_{vi} \right) - \theta_V, \quad (8)$$

$$M_{ZP} = \sqrt{\sum_{i=1}^{n} P_i \cdot (\Omega_i - \Omega)^2 \cdot I_{vi}} \Big/ \left(\sum_{i=1}^{n} P_i \cdot I_{vi} \right) - \theta_P. \quad (9)$$

Коефіцієнт ймовірних втрат набуває значень $K_Z \in [0;1]$, причому $K_Z = 0$, якщо відсутні втрати передачі, і $K_Z = 1$, якщо не будуть досягнуті необхідні ймовірні показники доставки інформації в завадостійкій телекомунікаційній мережі.

Якщо розглядати завадостійкість телекомунікаційної мережі як здатність системи протидіяти завадам, для цього треба знати, чим протидіяти і на що протидіяти, тобто для боротьби із завадами потрібні апріорні відомості про властивості носія інформації та про самі завади. До таких властивостей належать [12]:

– величина струму чи напруги вхідного сигналу та завади в каналі передачі;

– середні потужності сигналу Pc та завади $Pз$;

– вид та структура переносника інформації;

– закон розподілу сигналу передачі тощо.

Знаючи всі ці властивості сигналу та завади, можна встановити певні відмінності між ними і використати їх для розроблення способів, засобів та методів забезпечення завадостійкості. Всі способи завадостійкості ведуть до часової та апаратурної надмірності як із боку джерела інформації, так і з боку адресата. Одна група способів підвищення завадостійкості базується на виборі методу передачі інформації. Друга група способів пов'язана із побудовою завадостійких приймачів. Способи підвищення завадостійкості в телекомунікаційній мережі:

1) методи оптимального приймання сигналів;

2) заглушення завад у місцях їх виникнення;

3) використання спеціальних кодів;

4) використання в системах каналу зворотного зв'язку;

5) багаторазового повторення інформації, що передається;

6) збільшення спів відношення сигнал та завада;

7) компенсація завади;

8) раціональній вибір виду оптимальної модуляції сигналів;

9) екранування системи чи її окремих елементів.

Досить простим і часто застосовуваним засобом підвищення завадостійкості є збільшення відношення сигнал та завада за рахунок збільшення потужності передавача. Хоча цей

спосіб, може виявитись економічно недоцільним, по скільки він пов'язаний із значним збільшенням складності та вартості обладнання телекомунікаційної мережі. Важливим засобом підвищення завадостійкості передачі інформації шляхом використання неперервних сигналів є раціональний вибір виду модуляції сигналів. Різні види модуляції мають неоднакову завадостійкість. Тому застосовуючи різні види модуляції, які забезпечують значне розширення смуги частот сигналу, можна досягти істотного підвищення завадостійкості передачі інформації в телекомунікаційній мережі. Ще одним радикальним способом підвищення завадостійкості дискретних систем є використання спеціального кодування інформації - використання завадостійких кодів. Підвищення завадостійкості передачі та оброблення інформації може бути досягнуто шляхом багаторазового повторення передачі інформації. Отримані результати передачі порівнюються і як дійсні беруться ті результати, що мають найбільшу кількість збігів. Щоб виключити чи змінити невизначеність під час оброблення інформації та забезпечити відбір за критерієм більшості, передача має повторюватись не менше трьох разів. Цей спосіб підвищення завадостійкості пов'язаний зі збільшенням часу передачі та ускладненням апаратури. Різновидом телекомунікаційних систем, у яких підвищення завадостійкості досягається за рахунок збільшення часу передачі, є системи із зворотним зв'язком. Завадостійке приймання інформації полягає у використанні надмірності отриманої інформації, апріорних відомостей про сигнали та завади. На сьогодні для побудови систем із оптимальним прийомом широко використовується апарат теорії статистичних рішень. Помилки систем передачі зменшуються із збільшенням відношення сигнал та завада на вході приймача. У зв'язку із цим часто проводять попереднє оброблення прийнятого сигналу із метою збільшення відношення корисної складової до завади.

Розгляд методів, способів та засобів забезпечення завадостійкої передачі інформації в телекомунікаційних мережах показав, що завдання оптимального прийому полягає у використанні властивостей корисного сигналу, завади та каналу передачі для збільшення ймовірності правильного прийому. Для збільшення ймовірності правильного прийому має бути проведене попереднє оброблення прийнятого сигналу, яке забезпечує збільшення відношення сигнал та завада. Для цього на приймальній стороні системи необхідна наявність фільтра та розв´язувального пристрою. Фільтр поліпшує відношення сигнал та завада. Розв´язувальний пристрій виконує функції виявлення, виокремлення та відновлення корисного сигналу. Ідея частотної фільтрації базується на різниці спектрів корисного сигналу та завади. При цьому використовуються лінійні частотні фільтри, які заглушують завади та поліпшують тим самим відношення сигнал та завада. Метод накопичення застосовується у тому випадку, коли корисний сигнал протягом часу прийому є постійним та являє собою періодичну функцію. Він полягає у багаторазовому повторенні сигналу та підсумовуванні окремих його реалізацій в приймальному пристрої системи. Позитивний результат досягається за рахунок збільшення часу роботи, тобто зменшення швидкодії телекомунікаційної мережі. Величину відношення сигнал та завада можна підвищити, якщо використати різницю між кореляційними функціями сигналу та завади. Цей метод є ефективним лише у випадку застосування в системах періодичних та квазіперіодичних сигналів в каналі передачі телекомунікаційної мережі.

Висновки. На основі досліджень та аналізу методів, способів та засобів забезпечення завадостійкої передачі інформації в телекомунікаційних мережах можливо зробити висновок, що завдання оптимального та якісного прийому інформації полягає у використанні властивостей корисного сигналу, завади та каналу передачі для збільшення ймовірності правильного прийому. Для збільшення ймовірності правильного прийому має бути проведене попереднє оброблення прийнятого сигналу, яке забезпечує збільшення відношення сигнал та завада. Канали передачі даних, що застосовують технології, які дозволяють у режимі реального часу гарантувати якісну, надійну та вірогідну передачу даних в умовах впливу завад, краще забезпечують заданих значень показників вірогідної передачі інформації здійснюється за рахунок використання необхідного кодування. Під час передачі такими каналами виникає багато труднощів, пов'язаних із впливом природних, промислових, навмисних та ненавмисних завад. Всі способи завадостійкості ведуть до часової та апаратурної надмірності як із боку джерела інформації, так і з боку адресата. Знаючи всі ці властивості сигналу та завади, можна встановити

певні відмінності між ними і використати їх для розроблення способів, засобів та методів забезпечення завадостійкості. На відміну від спотворень завади носять випадковий характер. Вони заздалегідь невідомі і тому не можуть бути повністю усунені. Таким чином, можна зробити висновок про те, що знання методів та засобів побудови сучасних каналів передачі телекомунікаційною мережею в умовах дії завад, дозволить будувати надійні канали передачі інформації для таких мереж.

ЛІТЕРАТУРА:

1. Бабич В. Д. Завадостійкість каналів зв'язку : навч. посібн. / В.Д. Бабич, О.Д. Кувшинов, О.П. Лежнюк, С.П. Лівенцев // К. : КВІУЗ, 2001. - 150 с.

2. Казимир В. В. Інформаційні основи побудови телекомунікаційних мереж / В. В. Казимир, В.В. Литвинов, С.М. Шкарлет, С.В. Зайцев // Вісник Чернігівського державного технологічного університету. - Чернігів : ЧДТУ, 2013. – 340 с.

3. Бортнік Л. Л. Аналіз варіантів застосування імітаційних завад в радіоканалах з OFDM / Л. Л. Бортнік, О. В. Кувшинов, О. Г. Жук // Сучасний захист інформації. – К.: 2012. – Вип. 5. – С. 45 – 52.

4. Кривуца В.Г. Управління телекомунікаціями із застосуванням новітніх технологій / В.Г. Кривуца, В.К. Стеклов, Л.Н. Беркман, Б.Я.Костік, В.Ф.Олійник, С.М.Скляренко // Підручник для ВНЗ. – К.: Техніка, 2007. – 384 с.

5. Зайцев С. В. Математична модель оцінки достовірності передачі інформації в безпровідних мережах за умов впливу структурних завад / С.В. Зайцев // Молода наука України. Перспективи та пріоритети розвитку : матеріали XIV Всеукр. наук.-практ. конф. з міжнар. участю, (Київ, 26–27 грудня 2013 р.). – К.:, 2014. – С. 174 – 175.

6. Доля А.Е. Имитационная модель беспроводной системы передачи информации с использованием технологии HARQ и дополнительной априорной информации для повышения достоверности передачи / А.Е. Доля, С. В. Зайцев // Матеріали Всеукр. наук.-практ. конф. молодих учених і студентів «Новітні технології у науковій діяльності і навчальному процесі», (Чернігів, 28 квітня 2014 р.). – Чернігів : Черніг. нац. технол. ун-т, 2015. – С. 70 – 71.

7. Шеннон К.Э. Математическая теория связи / К.Э. Шеннон // Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963. – С. 243-332.

8. Приступа В. В. Исследование характеристик помехозащищенности беспроводных сетей с сигналами OFDM с внутрибитовой псевдослучайной перестройкой поднесущих частот в условиях установки оптимальных помех / В. В. Приступа, С. В. Зайцев // Математичні машини і системи. — К.:, 2015. – № 1. – С. 84 – 95.

9. Мак-Вильямс Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. Слоэн. – М. : Связь, 1979. – 744 с.

10. Сальник С.В. Аналіз методів виявлення вторгнень у мобільні радіомережі класу MANET / С.В. Сальник, О.Я. Сова, Д.А. Міночкін // Сучасні інформаційні технології у сфері безпеки. – К.: НУОУ, 2015. – № 1(22). –С. 103-112.

11. Хмельницький Ю.В. Забезпечення достовірності передачі інформації та сервісних послуг для високошвидкісних мереж при завадах / Ю.В Хмельницький, Д.П. Яковлєв // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 57. – С. 111-119.

12. Горбатий І. В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи : навч. посібник / І.В. Горбатий, А.П. Бондарєв // – Львів : Видавництво Львівської політехніки, 2016. – 336 с.

REFERENCES:

1. Babych, V. D., Kuvshynov, O.D., Lezhnyuk, O.P. and Livencev, S.P. (2001), "Zavadostijkist" kanaliv zv'yazku : navch. Posibn" [Noise Immunity of communication channels : proc. porn.], KVIUZ, Kyyiv, 150p.

2. Kazymyr V. V., Lytvynov, V.V., Shkarlet, S.M. and Zajcev, S.V. (2013) "Informacijni osnovy pobudovy telekomunikacijnyx merezh" [Information basis for the design of telecommunication networks], ChDTU, Visnyk Chernihivs"koho derzhavnoho texnolohichnoho universytetu, Chernihiv, 340p.

3. Bortnik, L. L., Kuvshynov, O. V. and Zhuk, O. H. (2012), "Analiz variantiv zastosuvannya imitacijnyx zavad v radiokanalax z OFDM" [Analysis applications simulation of interference in radio channels with OFDM], Suchasnyj zaxyst informaciyi, Kyyiv, No.5. pp 45–52.

4. Kryvuca, V.H., Steklov, V.K., Berkman, L.N., Kostik, B.Ya., Olijnyk, B.F. and Sklyarenko, S.M. (2007), "Upravlinnya telekomunikaciyamy iz zastosuvannyam novitnix texnolohij" [Management of telecommunication with latest technology], Texnika, Kyyiv, 384p.

5. Zajcev, S. V. (2014), "Matematychna model" ocinky dostovirnosti peredachi informaciyi v bezprovidnyx merezhax za umov vplyvu strukturnyx zavad" [Mathematical model of an estimation of reliability of data transmission in wireless networks in terms of the effects of structural interference], Moloda nauka Ukrayiny. Perspektyvy ta priorytety rozvytku: materialy XIV Vseukr. nauk.-prakt. konf. z mizhnar. uchastyu, Kyyiv, pp.174–175.

6. Dolya, A.E. and Zajcev, S. V. (2015), "Ymytacyonnaya model" besprovodnoj systemy peredachy ynformacyy s yspol"zovanyem texnolohyy HARQ y dopolnytel"noj apryornoj ynformacyy dlya povyshenyya dostovernosty peredachy" [Simulation model of a wireless information transmission system using HARQ technology, and additional a priori information to improve the reliability of transfer], Materialy Vseukr. nauk.-prakt. konf. molodyx uchenyx i studentiv «Novitni texnolohiyi u naukovij diyal"nosti i navchal"nomu procesi», Chernih. nac. texnol. un-t, Chernihiv, pp.70–71.

7. Shennon, K.Э. (1963), "Matematycheskaya teoryya svyazy" [Mathematical theory of communication], Ynostrannaya lyteratura, Raboty po teoryy ynformacyy y kybernetyke, Moskva, pp.243-332.

8. Prystupa, V. V. and Zajc, S. V. (2015), "Yssledovanye xarakterystyk pomexozashhyshhennosty besprovodnyx setej s syhnalamy OFDM s vnutrybytovoj psevdosluchajnoj perestrojkoj podnesushhyx chastot v uslovyyax ustanovky optymal"nyx pomex " [Study of the characteristics of noise immunity of wireless networks with OFDM, vnutrividovoi pseudo-random rearrangement of carrier frequencies in terms of setting the optimum interference], Matematychni mashyny i systemy, Kyyiv, No.1, pp.84-95.

9. Mak-Vyl"yams, F. Dzh and Sloэn, N. Dzh (1979) "Teoryya kodov, yspravlyayushhyx oshybky" [The theory of error-correcting codes], Svyaz", Moskva, 744p.

10. Sal"nyk, S.V., Sova, O.Ya. and Minochkin, D.A. (2015), "Analiz metodiv vyyavlennya vtorhnen" u mobil"ni radiomerezhi klasu MANET" [Analysis of methods of intrusion detection in the mobile radio network of the class MANET], NUOU, Suchasni informacijni texnolohiyi u sferi bezpeky, Kyyiv, No. 1(22), pp.103-112.

11. Xmel"nyc"kyj, Yu.V. and Yakovlyev, D.P. (2017), "Zabezpechennya dostovirnosti peredachi informaciyi ta servisnyx posluh dlya vysokoshvydkisnyx merezh pry zavadax" [Ensuring the reliability of data transmission and services for high-speed networks in zavady], VIKNU, Zbirnyk naukovyx prac" Vijs"kovoho instytutu Kyyivs"koho nacional"noho universytetu imeni Tarasa Shevchenka, Kyyiv, No.57, pp.111-119.

12. Horbatyj, I. V. and Bondaryev, A.P. (2016), "Telekomunikacijni systemy ta merezhi. Pryncypy funkcionuvannya, texnolohiyi ta protokoly : navch. posibnyk" [Telecommunication systems and networks. The principles of operation, technology and protocols : proc. a manual], Vydavnyctvo L"vivs"koyipolitexniky, L"viv, 336p.

к.т.н. Хмельницкий Ю.В., Каблуков О.А., Рябая Л.А., Солодеева Л.В., Ткач А.А.

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ПОМЕХОУСТОЙЧИВОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В статье проведен анализ методов и средств обеспечения помехоустойчивости передачи информации в телекоммуникационных сетях, которые применяют технологии, позволяющие в режиме реального времени гарантировать качественную, надежную и достоверную передачу данных в условиях воздействия помех. Для телекоммуникационных сетей задачи оптимального и качественного приема информации заключается в использовании свойств полезного сигнала, помехи и канала передачи для увеличения вероятности правильного приема. Для увеличения вероятности правильного приема должна быть проведена предварительная обработка принятого

сигнала, что обеспечивает увеличение отношения сигнал помеха. Каналы передачи данных, что применяют технологии, которые позволяют в режиме реального времени гарантировать качественную, надежную и достоверную передачу данных в условиях воздействия помех, лучше обеспечивают заданных значений показателей достоверной передачи информации, которая осуществляется за счет использования необходимого кодирования. Во время передачи по таким каналам возникает много трудностей, связанных с влиянием природных, промышленных, преднамеренных и непреднамеренных помех. Все способы помехоустойчивости в целом ведут к временной и аппаратурной избыточности, как со стороны источника информации, так и со стороны адресата. Если рассматривать помехоустойчивость телекоммуникационной сети как способность системы противодействовать помехам, то надо знать, чем противодействовать и на что противодействовать, то есть для борьбы с помехами нужны априорные сведения о свойствах носителя информации и о самих помехах. Зная все эти свойства сигнала и помехи, можно установить определенные различия между ними и использовать их для разработки способов, средств и методов обеспечения помехоустойчивости.

Целью данной статьи является проведение анализа методов и средств обеспечения помехоустойчивой передачи информации в телекоммуникационных сетях, что позволит в режиме реального времени гарантировать качественную, надежную и достоверную передачу данных в условиях влияния помех. В отличие от искажений помехи носят случайный характер. Они загодя неизвестны и потому не могут быть полностью устранены. Знание методов и средств построения современных каналов передачи телекоммуникационной сетью в условиях действия помех, позволит строить надежные каналы передачи информации для таких сетей.

Ключевые слова: помехи, помехоустойчивость, каналы передачи, телекоммуникационная сеть, искажения, достоверность передачи информации, надежность, неопределенность.

Ph.D. Khmelnitsky, Yu.V., Kablukov O.A., Riaba L.O., Solodeeva L.V.,Tkach A.O.

METHODS AND MEANS OF ENSURING THE NOISE IMMUNITY OF TRANSMISSION IN TELECOMMUNICATION NETWORKS

In the article the analysis of methods and means of ensuring the noise immunity transmission in telecommunication networks that use technologies in real time to ensure quality, valid and reliable data transmission under conditions of interference. For telecommunication networks the problem of optimal quality reception of information is to use the properties of the useful signal, interference, and transmission channel to increase the probability of correct reception. To increase the probability of correct reception needs to be pre-processed received signal that increases the signal interference. Transmission channels that use technologies that allow real-time to ensure quality, valid and reliable data transmission under conditions of interference provide better instruction indicators reliable transmission of information is carried out through the use of the necessary coding. During transmission on such channels, there are many difficulties associated with the impact of natural, industrial, intentional and unintentional interference. All methods of a noise stability in General lead to temporal and hardware redundancy as part of the source of information and of the addressee. Examine noise immunity of TCN as ability of the system to counteract to the hindrances, then it is necessary to know, what to counteract and on what to counteract, for a fight against hindrances a priori information is needed about properties of transmitter of information and about hindrances. Knowing all these properties of the signal and noise, it is possible to establish certain differences between them and use them to develop ways, means and methods to provide noise immunity.

The aim of this article is realization of analysis of methods and backer-ups of interference immunity information transfer in TCNS, which will allow real-time to guarantee the quality, reliable and reliable transmission of the hindrances given in the conditions of influence. Unlike distortions hindrances carry casual character. They in are good time unknown and that is why cannot be fully removed. Knowledge of methods and facilities of construction of modern channels of transmission TCN in the conditions of action of hindrances, will allow building the reliable channels of information transfer for such networks.

Keywords: interference, interference immunity, transmission channels, telecommunication network, distortion, reliability of information transmission, reliability, uncertainty.

УДК 004.522

Prof. **Myasishchev A.A.** (KhNU)
Prof. **Lienkov S.V.** (VIKNU)
PhD. **Dzhulii V.M.** (KhNU)
PhD. **Muliar I.V.** (KhNU)

USING GPU NVIDIA FOR LINEAR ALGEBRA PROLEMS

Research goals and objectives: the purpose of the article is to study the feasibility of graphics processors using in solving linear equations systems and calculating matrix multiplication as compared with conventional multi-core processors. The peculiarities of the MAGMA and CUBLAS libraries use for various graphics processors are considered. A performance comparison is made between the Tesla C2075 and GeForce GTX 480 GPUs and a six-core AMD processor.

Subject of research: the software is developed basing on the MAGMA and CUBLAS libraries for the purpose of the NVIDIA Tesla C2075 and GeForce GTX 480 GPUs performance study for linear equation systems solving and matrix multiplication calculating.

Research methods used: libraries were used to parallelize the linear algebra problems solution. For GPUs, these are MAGMA and CUBLAS, for multi-core processors, the ScaLAPACK and ATLAS libraries. To study the operational speed there are used methods and algorithms of computational procedures parallelization similar to these libraries. A software module has been developed for linear equations systems solving and matrix multiplication calculating by parallel systems.

Results of the research: it has been determined that for double-precision numbers the GPU GeForce GTX 480 and the GPU Tesla C2075 performance is approximately 3.5 and 6.3 times higher than that of the AMD CPU. And the GPU GeForce GTX 480 performance is 1.3 times higher than the GPU Tesla C2075 performance for single precision numbers. To achieve maximum performance of the NVIDIA CUDA GPU, you need to use the MAGMA or CUBLAS libraries, which accelerate the calculations by about 6.4 times as compared to the traditional programming method. It has been determined that in equations systems solving on a 6-core CPU, it is possible to achieve a maximum acceleration of 3.24 times as compared to calculations on the 1st core using the ScaLAPACK and ATLAS libraries instead of 6-fold theoretical acceleration. Therefore, it is impossible to efficiently use processors with a large number of cores with considered libraries. It is demonstrated that the advantage of the GPU over the CPU increases with the number of equations.

Key words. GPU Tesla C2075, MAGMA, CUBLAS, CUDA, graphics processor, NVIDIA Tesla V100, SMP system, MPI, ScaLAPACK, ATLAS.

Introduction. A large amount of computational mathematical problems are those solving linear algebraic equations systems. Many managerial and economic, technological problems are either constructed as linear algebraic equations, or are reduced to them. The widely used finite element method, which is used for solving almost all problems that are reduced to systems of partial differential equations, is reduced to solving linear equations systems as well.

Matrix methods are very popular in economic practice. They are used for statistical calculations, labor rationing, reduction of workflow, organization of internal production cost accounting, as well as for economic analysis. Solving linear equations systems is also reduced to matrix transformations, thus the development of efficient hardware and software is an important task.

Such tasks require high performance computing systems. Nowadays, computers with multi-core processors are widely used; they are in fact a parallel computing system with shared memory (SMP-system). With the occurrence of G80, the NVIDIA's chip of the eighth generation (2007), there has emerged CUDA, a software and hardware architecture, which allows performing calculations using NVIDIA GPUs. This technology is, just as in the case of the processor, a parallel computing system, which includes hundreds of processor cores. The problem is to parallelize the matrix multiplication and solve linear equation systems to get the maximum load of the multi-core CPU and GPU processor cores, and then to compare how much the GPU performance differs from that of the CPU for solving such problems with single and double precision numbers.

The purpose and objectives of the paper to study the graphics processors feasibility in solving, in particular, linear equations systems and matrix multiplication as compared to conventional multi-core processors. Peculiarities of the use and installation problems of the MAGMA library are considered.

To achieve the goal, two computing systems were used:

- the first one has an AMD Phenom II X6 1090T processor (CPU) with a 3.2 GHz frequency and a NVIDIA's Tesla C2075 graphics processor (GPU),

- the second one also has an AMD Phenom II X6 1090T processor (CPU) with a 3.2 GHz frequency, but a NVIDIA's GeForce GTX 480 GPU.

Analysis of recent research and publications and problem statement. There are numerous works devoted to the study of parallel systems performance, basing both on cluster systems, and multi-core processors [1-7]. For example, [3,4,8] present a number of tasks solutions using NVIDIA GPU. However, they didn't provide a detailed analysis of NVIDIA GPU's potential for both simple programming methods and programming methods based on cuBLAS (CUDA Basic Linear Algebra Subroutines), and MAGMA (Matrix Algebra on GPU and Multicore Architectures) program libraries [6,9] for solving linear equations systems and matrix multiplication with single and double precision numbers.

Currently, NVIDIA has introduced an accelerator Tesla V100 based on the Volta architecture [10]. This device has a high level of computing power, amounting to about 15 TFLOPS in single precision and 7.5 TFLOPS in double precision operations, which allows using it in modern super-computer systems [11]. NVIDIA also introduced a new family of GeForce RTX 20 Series GPUs [12] based on a new Turing architecture. Its computational capabilities for single-precision operations are about 12 teraflops and 0.37 teraflops for double precision ones. However, at present, budget GPUs based on NVIDIA Tesla C2075 and NVIDIA GeForce GTX 480 video cards, which are installed on many workstations used for high-performance computing, are still important. Therefore, we will focus on computational experiments for these GPUs, and a computer with an AMD Phenom II X6 1090T processor (CPU, 3.2 GHz) will be considered as a multi-core processor with SMP architecture.

Research methods to determine the considered computing systems performance. To solve the problems, a computational experiment was carried out to determine performance in GFLOP/s and calculation time on the two above mentioned computational systems for the matrix multiplication problems and linear equation systems solving. We used test examples from the ScaLAPACK, ATLAS, MAGMA, CUBLAS libraries [6]. We also used our own programs based on the considered libraries and traditional programming methods.

The results of the computing systems performance assessing. As indicated, two systems are considered for performing computational experiments. Moreover, in these systems, GPUs will act as computational accelerators for linear equations systems solving and matrix multiplication. In the first case, the calculation will be performed taking into account parallelization across the 6 cores of the processor using the MPI, ScaLAPACK and ATLAS libraries [1,2,7]. In the second and third cases parallelization is across the cores of the Tesla C2075 GPU and GeForce GTX 480 using the CUDA technology [3]. Computing systems are working on Linux Ubuntu. They have compilers Fortran F77, gfortran with the above mentioned libraries for a 6-core processor. For programming on the Tesla C2075 GPU and GeForce GTX 480, the NVIDIA's video driver and the CUDA Toolkit software are installed from http://developer.nvidia.com/cuda-toolkit-archive. The software installation sequence for the GPU is presented in the source [13]. Installing the MPI, ScaLAPACK, ATLAS libraries on Linux Ubuntu OS is presented in [6] for a system with a 4-core processor CORE 2 QUAD PENTIUM Q6600 2.4GHZ, therefore it is not considered here. Let us take a closer look at the MAGMA library installation and solution of arising problems.

The installation is similar for 32-bit and 64-bit Linux Ubuntu operating systems. For the Tesla C2075 GPU, it is advisable to use a 64-bit system, since the amount of global memory here is 6 GB. Before compiling MAGMA, you need to install the lapack library:

```
sudo apt-get install --yes --force-yes liblapack-dev
```

After copying the source magma_1.0.0.tar.gz from the website
http://www.cs.utk.edu/~tomov/magma_1.0.0.tar.gz unarchiving is performed

```
$gzip –d magma_1.0.0.tag.gz
$tar xf magma_1.0.0.tar
$cd magma_1.0.0
```

Using the nano editor, create the make.inc file with the following contents:

```
GPU_TARGET = 1
CC        = gcc
NVCC      = nvcc
FORT      = gfortran
ARCH      = ar
ARCHFLAGS = cr
RANLIB    = ranlib
OPTS      = -O3 -DADD_
FOPTS     = -O3 -DADD_ -x f95-cpp-input
NVOPTS    = --compiler-options -fno-strict-aliasing -DUNIX -O3 -DADD_
LDOPTS    = -fPIC -Xlinker -zmuldefs
LIB       = -lcblas  -llapack -lpthread -lcublas -lcudart  -lm
CUDADIR   = /usr/local/cuda
LIBDIR    =  -L/usr/local/cuda/lib -L/usr/lib
INC       = -I$(CUDADIR)/include
LIBMAGMA     = ../lib/libmagma.a
LIBMAGMABLAS = ../lib/libmagmablas.a
```

Here you need to pay attention to the value of the GPU_TARGET parameter. If you equate it to zero, the library is built for the GPU Tesla family, if you equate it to one, then this corresponds to Fermi family. GPU NVIDIA GeForce GTX 480 corresponds to Fermi family. For the Tesla C2075 GPU, let us build the Magma libraries with GPU_TARGET = 1 and GPU_TARGET = 0 and compare the speed of calculations.

Run the compile command make all. In this case, the libraries libmagma, libmagmablas will be created and the test cases will be compiled. However, there are problems.

1. For 32-bit system.

gfortran -O3 -DADD_ -x f95-cpp-input -Dmagma_devptr_t="integer(kind=../control/sizeptr.c: In function ‘main’: ../control/sizeptr.c:6: warning: format ‘%lu’ expects type …

Here you need to run the control / sizeptr.c program and bring it to the form

```
#include <stdlib.h>
#include <stdio.h>
int main (){  printf("%d", sizeof(void *));  return EXIT_SUCCESS;}
```

That means you need to change format % lu to format % d. The gfortran compiler does not issue errors FOR the 64-bit system.

2. When compiling test cases.

First problem:

```
../lib/libmagma.a(zlatrd.o): In function `magma_zlatrd':
zlatrd.cpp:(.text+0x332): undefined reference to `zdotc'
zlatrd.cpp:(.text+0xbe2): undefined reference to `zdotc'
```

You must run the src / zlatrd.cpp program and make changes.

```
   cblas_zdotc_sub(i_n, W(i +1, i), ione, A(i +1, i), ione, &value);
  //   blasf77_zdotc(&value, &i_n, W(i+1,i), &ione, A(i+1, i), &ione);
```

and

```
  cblas_zdotc_sub(i, W(0, iw), ione, A(0, i), ione, &value);
  //      blasf77_zdotc(&value, &i, W(0, iw), &ione, A(0, i), &ione);
```

Second problem:

```
../lib/libmagma.a(clatrd.o): In function `magma_clatrd':
clatrd.cpp:(.text+0x321): undefined reference to `cdotc'
clatrd.cpp:(.text+0xb30): undefined reference to `cdotc'
```

Similarly, you need to run the src / clatrd.cpp program and make changes

```
//          blasf77_cdotc(&value, &i, W(0, iw), &ione, A(0, i), &ione);
          cblas_cdotc_sub(i, W(0, iw), ione, A(0, i), ione, &value);
```

and

```
                cblas_cdotc_sub(i_n, W(i +1, i), ione, A(i +1, i), ione, &value);
```

// blasf77_cdotc(&value, &i_n, W(i+1,i), &ione, A(i+1, i), &ione);

It is evident that for the correct connection with the fortran libraries, the library libcblas is needed instead of libblasf77. The libcblas.so library is installed with liblapack installation and therefore it is described in the make.inc file in the LIB parameter.

The compilation of testing programs testing_sgemm.cpp and testing_dgemm.cpp of matrix multiplication with single and double precision numbers, is correspondingly performed by the command lines:

gcc -O3 -DADD_ -DGPUSHMEM=200 -I/usr/local/cuda/include -I../include -I../quark/include -c testing_dgemm.cpp -o testing_dgemm.o

gcc -O3 -DADD_ -DGPUSHMEM=200 -fPIC -Xlinker -zmuldefs -DGPUSHMEM=200 testing_dgemm.o -o testing_dgemm lin/liblapacktest.a -L../lib -lcuda -lmagma -lmagmablas -lmagma -L/usr/local/cuda/lib -L/usr/lib -lcblas -llapack -lpthread -lcublas -lcudart -lm

When running these programs, a calculation performance comparison is performed for cuBLAS and MAGMA libraries. Performance is fixed in GFlop/s. Before compiling these test programs, it is necessary to adjust the parameters istart = 1024 and iend = 10240, which specify the initial and final values of the matrices 1024 and 10240 dimensions. Too large values may not fit in the global memory of the GPU. Let us consider the results of the programs testing_sgemm.cpp and testing_dgemm.cpp for the GPU GeForce GTX 480:

```
./testing_sgemm
device 0: GeForce GTX 480, 1401.0 MHz clock, 1535.2 MB memory
Testing transA = N  transB = N
    M     N     K    MAGMA GFLop/s     CUBLAS GFlop/s       error
=================================================================
1024  1024  1024       670.04                649.38       0.000000e+00
1280  1280  1280       685.46                696.84       0.000000e+00
1600  1600  1600       756.35                698.86       0.000000e+00
2000  2000  2000       792.98                688.97       0.000000e+00
2500  2500  2500       763.24                779.94       0.000000e+00
3125  3125  3125       803.20                776.03       0.000000e+00
3906  3906  3906       812.69                776.12       0.000000e+00
4882  4882  4882       825.38                791.58       0.000000e+00...
6102  6102  6102       820.70                818.51       0.000000e+00
7627  7627  7627       824.92                826.61       0.000000e+00
9533  9533  9533       825.42                844.12       0.000000e+00

./testing_dgemm
device 0: GeForce GTX 480, 1401.0 MHz clock, 1535.2 MB memory
Testing transA = N  transB = N
    M     N     K    MAGMA GFLop/s     CUBLAS GFlop/s       error
=================================================================
1024  1024  1024       154.26                154.56       0.000000e+00
1280  1280  1280       161.57                161.80       0.000000e+00
1600  1600  1600       162.78                162.97       0.000000e+00
2000  2000  2000       155.17                160.45       0.000000e+00
2500  2500  2500       155.78                162.03       0.000000e+00
3125  3125  3125       162.14                161.00       0.000000e+00
3906  3906  3906       158.81                163.31       0.000000e+00
4882  4882  4882       161.21                163.45       0.000000e+00
6102  6102  6102       162.44                164.08       0.000000e+00
```

Comparing the results, we see that the larger the matrix size, the faster the CUBLAS library works. However, the difference in performance is not significant. The performance drops sharply

when moving from single to double precision numbers (approximately 5.1 times). Calculations for GPU GeForce GTX 480 were performed for the GPU_TARGET = 1 parameter (Fermi family).

Let us consider the similar calculation results for the GPU Tesla C2075 for the GPU_TARGET = 0 parameter (Tesla family) and GPU_TARGET=1 parameter (Fermi family).

1. Tesla family

```
./testing_sgemm
device 0: Tesla C2075, 1147.0 MHz clock, 5375.2 MB memory
Testing transA = N  transB = N
   M       N       K     MAGMA GFLop/s    CUBLAS GFlop/s       error
=================================================================
 1024  1024  1024      428.98                433.40        0.000000e+00
 1280  1280  1280      516.29                516.35        0.000000e+00
 1600  1600  1600      514.25                514.83        0.000000e+00
 2000  2000  2000      389.18                525.71        1.525879e-05
 2500  2500  2500      396.82                604.98        1.525879e-05
 3125  3125  3125      405.15                573.97        1.525879e-05
 3906  3906  3906      401.76                579.76        3.051758e-05
 4882  4882  4882      404.92                586.02        3.051758e-05
 6102  6102  6102      402.93                613.92        3.051758e-05
 9533  9533  9533      409.14                639.26        6.103516e-05

./testing_dgemm
device 0: Tesla C2075, 1147.0 MHz clock, 5375.2 MB memory
Testing transA = N  transB = N
   M       N       K     MAGMA GFLop/s    CUBLAS GFlop/s       error
=================================================================
 1024  1024  1024      169.47                280.13        0.000000e+00
 1280  1280  1280      172.29                290.61        0.000000e+00
 1600  1600  1600      173.52                294.22        0.000000e+00
 2000  2000  2000      162.38                287.59        2.842171e-14
 2500  2500  2500      163.30                285.84        2.842171e-14
 3125  3125  3125      165.76                278.25        2.842171e-14
 3906  3906  3906      163.75                291.70        5.684342e-14
 4882  4882  4882      164.99                291.50        5.684342e-14
 6102  6102  6102      162.18                293.82        5.684342e-14
 6102  6102  6102      162.18                293.82        5.684342e-14
 9533  9533  9533      166.24                293.68        1.136868e-13
```

In this case, the MAGMA library has significantly lower performance than the CUBLAS library for both single-precision numbers (about 1.6 times) and double-precision numbers (about 1.8 times)

2. Fermi family

```
./testing_sgemm
device 0: Tesla C2075, 1147.0 MHz clock, 5375.2 MB memory
Testing transA = N  transB = N
   M       N       K     MAGMA GFLop/s    CUBLAS GFlop/s       error
=================================================================
 1024  1024  1024      551.34                431.39        7.629395e-06
 1280  1280  1280      566.34                516.79        7.629395e-06
 1600  1600  1600      600.45                514.57        7.629395e-06
 2000  2000  2000      617.14                525.37        1.525879e-05
 2500  2500  2500      585.90                605.09        1.525879e-05
 3125  3125  3125      622.99                573.94        1.525879e-05
```

3906	3906	3906	629.77	579.80	3.051758e-05
4882	4882	4882	640.83	585.94	3.051758e-05
6102	6102	6102	637.69	613.76	3.051758e-05
9533	9533	9533	639.57	639.24	6.103516e-05

./testing_dgemm
device 0: Tesla C2075, 1147.0 MHz clock, 5375.2 MB memory
Testing transA = N transB = N

M	N	K	MAGMA GFLop/s	CUBLAS GFlop/s	error
1024	1024	1024	279.11	280.61	0.000000e+00
1280	1280	1280	290.00	290.87	0.000000e+00
1600	1600	1600	294.01	294.44	0.000000e+00
2000	2000	2000	281.17	287.59	2.842171e-14
2500	2500	2500	282.24	285.60	2.842171e-14
3125	3125	3125	295.79	278.13	2.842171e-14
3906	3906	3906	289.47	291.83	5.684342e-14
4882	4882	4882	293.89	291.59	5.684342e-14
6102	6102	6102	295.99	293.87	5.684342e-14
9533	9533	9533	300.77	293.83	1.136868e-13

In this case, the MAGMA library has a performance slightly higher than CUBLAS. Therefore, for the GPU Tesla C2075, the compilation of the MAGMA libraries with the GPU_TARGET = 1 parameter (the make.inc file) is necessary.

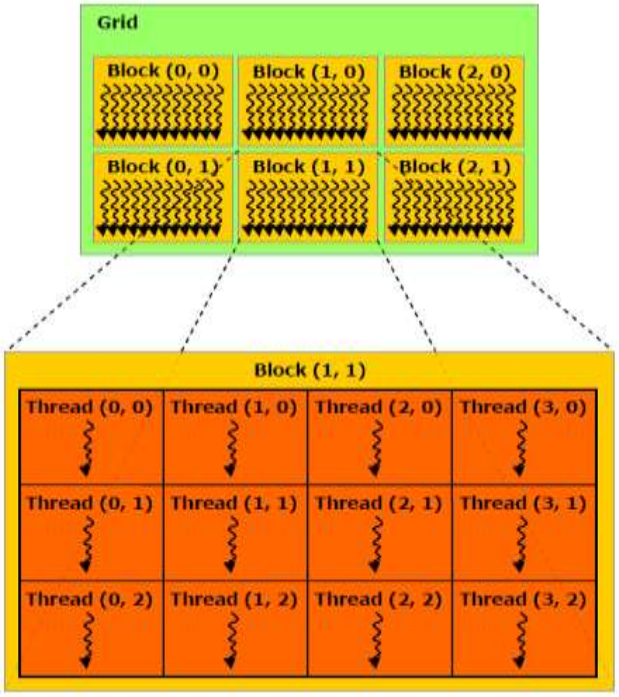


Figure 1 – The GPU program model

Let us analyze how much higher is the GPU's efficiency with NVIDIA's CUDA technology as compared to traditional way of writing parallel programs. To do this, we compare the efficiency of the matrix multiplication program using the global GPU memory (the first program), which is compiled according to the method described in [3, 4] with the program using the MAGMA and CUBLAS libraries (the second program).

To compile a program using global GPU memory, let us consider the GPU program model for the C compiler [4]. The top level of the core, the grid, consists of blocks. The blocks are either one-

dimensional or two-dimensional network of threads. This can be illustrated by Fig.1. The thread number in the block or the block number in the grid can be a variable of int or dim3 type.

The number of threads included in a block is determined by the blockDim built-in variable. The thread index inside the block is determined by the threadIdx variable, and the block index inside the grid is defined by the blockIdx variable. The threads in the block are directly performing of calculations. The thread is a 3-component vector, i.e. it can be identified using one-, two- and three-dimensional index of the thread, forming in turn a one-, two- and three-dimensional block of threads. There is a limit on the number of threads per block, which cannot exceed 1024 threads. The CUDA C extension allows you to call a function called the core so that it will execute in parallel N different CUDA threads. Such a function is declared with the __global__ specifier. Below is the first program compiled in accordance with the GPU's program model.

First program:

```
#include <stdio.h>
#define BLOCK 16 // Set the block size
// Multiplication function of two matrices
__global__ void mulMatr(float* a, float* b, float* c, int n)
{ // Get the id of the current thread.
  int i = threadIdx.y+blockIdx.y*blockDim.y; int j = threadIdx.x+blockIdx.x*blockDim.x;
  // Calculate the result.
     float sum=0.0f;
     for(int p = 0; p < n; p++){ sum+=  a[i*n + p] * b[p*n + j];}  c[i*n+j] = sum;}
__host__ int main()
{int N; int M; float mf=0.0f; printf ( "Input N->");  scanf ( "%d",&N);
 printf ( "Matrix = %dx%d elements\n", N,N );  M=N*N;
// Allocate memory for vectors
  float* a = new float[M]; float* b = new float[M]; float* c = new float[M];
// Initialize the values of the vectors
  for (int i = 0; i < N; i++){
   for (int j = 0; j < N; j++) { a[i*N+j] = 1.0f*((i+1)+2*(j+1)); b[i*N+j] = 1.0f/a[i*N+j];}}
// Video Memory Pointers
  float* deva;float* devb;float* devc;
// Allocate memory for vectors on the video card
  cudaMalloc((void**)&deva, sizeof(float) * M);cudaMalloc((void**)&devb, sizeof(float) * M);
  cudaMalloc((void**)&devc, sizeof(float) * M);
// create cuda event handle
cudaEvent_t start, stop;float gpuTime=0.0f;cudaEventCreate ( &start );cudaEventCreate ( &stop );
// Copy the data to the video card
  cudaMemcpy(deva, a, sizeof(float) * M, cudaMemcpyHostToDevice);
  cudaMemcpy(devb, b, sizeof(float) * M, cudaMemcpyHostToDevice);
// Execute the core function call
dim3 threads = dim3(BLOCK,BLOCK); // The number of threads in the block
dim3 blocks  = dim3(N/BLOCK,N/BLOCK); // The number of blocks in the grid
cudaEventRecord(start, 0); // connect the event to the core execution start
mulMatr<<<blocks, threads>>>(deva, devb, devc,N);
cudaEventRecord(stop, 0); // connect the event to the core execution ending. We get the result of
the calculation
 cudaMemcpy(c, devc, sizeof(float) * M, cudaMemcpyDeviceToHost);
cudaEventSynchronize(stop); // Wait for the core to execute, synchronizing on the stop event.
cudaEventElapsedTime (&gpuTime,start,stop);// Request time between start, stop
  // Calculation results
 gpuTime=gpuTime/1000;  mf=((2.0*N-1)*N*N)/(gpuTime*1000000.0);
 printf("time=%.4fsec\nspeed=%0.2fMFlops\n",gpuTime,mf);
 printf("i=%d\tj=%d\tC=%.5f\n",N/256,N/128,c[(N/256)*N+(N/128)]);
```

```
 printf("i=%d\tj=%d\tC=%.5f\n",3*N/4,5*N/16,c[(3*N/4)*N+(5*N/16)]);
 printf("i=%d\tj=%d\tC=%.5f\n",N-4,N-2,c[(N-4)*N+(N-2)]);
  // Releasing resources
  cudaEventDestroy(start); cudaEventDestroy(stop); cudaFree(deva);cudaFree(devb);cudaF-
ree(devc);
  delete[] a; a = 0;delete[] b; b = 0;delete[] c; c = 0; }
```

This program is compiled by the command:

```
nvcc -arch=sm_20 matrmul_g.cu -o matrmul_g
```

Here matrmul_g.cu is the name of the program source code.

The second program presents a simplified version of the testing_sgemm.cpp and testing_dgemm.cpp test cases, when the dimension of the matrices is a multiple of 16.

Second program:

```
#include <stdio.h>
#include <cuda.h>
#include <cublas.h>
#include "magma.h"
#include "magma_lapack.h"
int main ( int argc, char** argv )
{float time_seconds=0.0f; float mf=0.0f;
cudaEvent_t start, stop;cudaEventCreate ( &start );cudaEventCreate ( &stop );
int N=6144; printf ( "Input N->");if (scanf ( "%d",&N)==1);{printf ( "Matrix = %dx%d ele-
ments\n", N,N );}
int M=N*N; float *d_A, *d_B, *d_C;float* A = new float[M]; float* B = new float[M];
float* C = new float[M];
for (int j = 0; j < N; j++){for (int i = 0; i < N; i++){A[i+j*N] = 1.0*((i+1)+2*(j+1));B[i+j*N] =
1.0/A[i+j*N];}}
cublasInit(); cublasAlloc ( N * N, sizeof(float), (void**)&d_A);
cublasAlloc ( N * N, sizeof(float), (void**)&d_B);cublasAlloc ( N * N, sizeof(float),
(void**)&d_C);
cublasSetMatrix ( N, N, sizeof(float), (void *) A, N, (void *) d_A, N);
cublasSetMatrix ( N, N, sizeof(float), (void *) B, N, (void *) d_B, N);
cudaEventRecord(start, 0); magmablas_sgemm( 'n', 'n', N, N, N, 1.0f, d_A, N, d_B, N, 0.0f, d_C, N
);
cudaEventRecord(stop, 0); cublasGetMatrix ( N, N, sizeof(float), (void *) d_C, N, (void *) C, N );
 cudaEventElapsedTime (&time_seconds,start,stop);
 cublasFree (d_A);cublasFree (d_B); cublasFree (d_C); cublasShutdown();
 time_seconds=time_seconds/1000; mf=((2.0*N-1)*N*N)/(time_seconds*1000000.0);
 printf("time=%.4fsec\nspeed=%0.2fMFlops\n",time_seconds,mf);
 printf("i=%d\tj=%d\tC=%.5f\n",N/256,N/128,C[(N/256)+(N/128)*N]);
 printf("i=%d\tj=%d\tC=%.5f\n",3*N/4,5*N/16,C[(3*N/4)+(5*N/16)*N]);
 printf("i=%d\tj=%d\tC=%.5f\n",N-4,N-2,C[(N-4)+(N-2)*N]); }
```

These two programs are written for single-precision numbers. For double-precision numbers it is necessary to change the float to double data type. Also in the second program, the magmablas_sgemm function must be replaced by magmablas_dgemm one. The second program uses the library MAGMA. To use CUBLAS, instead of the magmablas_sgemm function, you must enter the cublasSgemm function in the program. The program is compiled by commands:

```
gcc -O3 -DADD_ -DGPUSHMEM=200 -I/usr/local/cuda/include -I../include -I../quark/in-
clude -c mb.cpp -o mb.o
gcc -O3 -DADD_ -DGPUSHMEM=200 -fPIC -Xlinker -zmuldefs -DGPUSHMEM=200 mb.o
-o mb -L../lib -lcuda -lmagma -lmagmablas -lmagma -L/usr/local/cuda/lib64 -L/usr/lib -lcblas -
llapack -lpthread -lcublas -lcudart -lm
```

Here mb.cpp is the name of the second program.

Table 1 presents the results of above mentioned programs performance estimates for the double-precision numbers for the Tesla C2075 GPUs and those of the programs presented in [14] using the ScaLAPACK and ATLAS libraries for the AMD Phenom II X6 1090T CPUs. In table 1, the numerator is the counting time in seconds, the denominator is the performance in Gigaflops per second. Performance was defined as the ratio of the floating-point operations number in the matrix product to the elapsed time. The number of operations in programs is determined by the expression: op = N * N (2 * N-1), where N is the number of rows or columns of a square matrix.

Table 1

Results of performance evaluations for the Tesla C2075 GPU and for AMD Phenom II X6 1090T CPU

Matrix NxN	AMD processor Phenom II X6 1090T (6 cores)	GPU Tesla C2075				
		Global memory	Tesla Compilation		Fermi Compilation	
			CUBLAS	MAGMA	CUBLAS	MAGMA
1024	0,062/34,6	0,045/47,3	0,008/284,4	0,013/170,2	0,008/284,8	0,008/282,4
2048	0,407/42,2	0,375/45,9	0,058/295,9	0,099/173,8	0,058/295,9	0,058/295,2
3072	1,234/47,0	1,233/47,0	0,194/299,3	0,333/174,1	0,194/299,4	0,194/298,9
4096	2,870/47,9	2,963/46,4	0,458/300,3	0,792/173,5	0,458/300,2	0,458/299,9
5120	5,687/47,2	5,715/47,0	0,893/300,6	1,536/174,7	0,893/300,5	0,894/300,2
6144	- / -	10,025/46,3	1,542/300,8	2,654/174,7	1,543/300,6	1,543/300,6

Comparison of the data in Table 1 with the results of test programs showed their close similarity. The performance of the processor is comparable with the performance of the program for the Tesla C2075 GPU, written using global memory [3] and about 6.3 times lower for the Tesla C2075 GPU for programs using the CUBLAS and MAGMA libraries.

Solving linear equation systems. Let us consider linear equation systems solving. In the test program on FORTRAN the calculation is made for double-precision numbers. Solution of the equations system for AMD CPU is divided into two stages:

- system matrix factorization (A) [15];
- the system solving using the results obtained at the first stage.

Each stage is performed by referring to the corresponding subroutines of the ScaLAPACK, BLACS, ATLAS libraries. The first stage uses the PDGETRF subroutine, the second uses the PDGETRS subroutine [7]. The program counts for each subroutine the time of its execution. The number of operations for the first (ops) and second stage (ops1) is calculated, and the system performance is calculated for LU factorization and the solution of the system as a whole.

Let us consider the procedure for solving the same problem on the GPU. To ensure maximum performance, we will also use ready-made libraries for solving equations systems using the LU factorization method. For this purpose, lapack-3.4.0 and MAGMA libraries (Matrix Algebra on GPU and Multicore Architectures) were installed on the computing system [9].

Below there is the ur_f1.f90 program, written on FORTRAN 90 for the GPU, for equations system solving using the LU factorization method:

```
program testing_dgetrf_gpu_f
use magma
external cublas_init, cublas_set_matrix, cublas_get_matrix
external cublas_shutdown, cublas_alloc
integer cublas_alloc
double precision, allocatable :: h_A(:), h_B(:), h_X(:)
magma_devptr_t              :: devptrA, devptrB
integer,  allocatable       :: ipiv(:)
integer                     :: i, n, info, stat, lda, size_of_elt, nrhs
real(kind=8)                :: ops,ops1, t, t1
integer                     :: tstart(2), tend(2), tstart1(2), tend1(2)
```

```
      call cublas_init()
      write (*,*) "Input n"
      read (*,*) n
      nrhs = 1
      lda  = n
      ldda = ((n+31)/32)*32
      size_of_elt = sizeof_double
      allocate(h_A(lda*n))
      allocate(h_B(lda*nrhs))
      allocate(h_X(lda*nrhs))
      allocate(ipiv(n))
      stat = cublas_alloc(ldda*n, size_of_elt, devPtrA)
      stat = cublas_alloc(ldda*nrhs, size_of_elt, devPtrB)
      do 10 i=1,n
      do 10 j=1,n
      h_A(i+(j-1)*n)=(sqrt(i/1.0d0))/11.0d0+(sqrt(j/1.0d0))/12.0d0
      if(i.eq.j) h_A(i+(j-1)*n)=10.0d0
10    continue
      do 11 i=1,n
      h_B(i)=(sqrt(i/1.0d0))/20.0d0 - 1.0d0
11    continue
      h_X(:) = h_B(:)
      call cublas_set_matrix(n, n, size_of_elt, h_A, lda, devptrA, ldda)
      call cublas_set_matrix(n, nrhs, size_of_elt, h_B, lda, devptrB, ldda)
      call magma_gettime_f(tstart)
      call magmaf_dgetrf_gpu(n, n, devptrA, ldda, ipiv, info)
      call magma_gettime_f(tend)
      call magma_gettimervalue_f(tstart, tend, t)
      write(*,*) "time LU =", t
      call magma_gettime_f(tstart1)
      call magmaf_dgetrs_gpu('n', n, nrhs, devptrA, ldda, ipiv, devptrB, ldda, info)
      call magma_gettime_f(tend1)
      call magma_gettimervalue_f(tstart1, tend1, t1)
      write(*,*) "time solve =", t1
      call cublas_get_matrix (n, nrhs, size_of_elt, devptrB, ldda, h_X, lda)
      write(*,*) "X(1)=",h_X(1),"X(",n,")=",h_X(n)
      ops = 2.0d0 * (dfloat(n))**3 / 3.0d0
      ops1 = 2.0d0 * (dfloat(n))**3 / 3.0d0 + 2.0d0*(dfloat(n))**2
      write(*,*)   '  Gflops LU  = ', ops /(t*1e6)
      write(*,*)   '  Gflops summa solve  = ', ops1 /(1e6*(t+t1))
      deallocate(h_A, h_X, h_B, ipiv)
      call cublas_free(devPtrA)
      call cublas_free(devPtrB)
      call cublas_shutdown()
      end
```

Here, the subroutine magmaf_dgetrf_gpu is used for LU factorization, and magmaf_dgetrs_gpu is used to solve the equations system [9,16]. The execution time and computational performance for them are also considered separately for LU factorization and the solution of the system as a whole.

Let us consider the results of computational experiments. Table 2 summarizes the results of calculations for the programs presented above for the AMD CPU and the Tesla C2075 GPU with double precision calculations. Two options are given for the processor: the calculation is performed by one core and 6 cores. The presented acceleration value does not reach the sixfold value anywhere. The results are presented as a fraction where the numerator is the counting time in seconds, and the

denominator is the performance in Gigaflops per second. Separate columns present calculations for LU factorization and system solutions. The "solution" column numerator gives the working time of the PDGETRS subroutine, i.e. return trace, and the denominator shows the total performance of system solving. It is ovious that the main complexity of the calculations is associated with LU-factorization. For a CPU, it is 26.491 / 0.121 = 219 times longer than the return trace time, and for a GPU it is 3.718 / 0.071 = 52 times longer for a 11008x11008 matrix. The ratio increases with the equations size. Thus, performance evaluation can only be performed by LU factorization.

Table 2

Calculation results for AMD CPU and Tesla C2075 GPU

Matrix NxN	CPU AMD Phenom II X6 1090T					GPU Tesla C2075	
	6 cores		1 core		Acceleration	LU-factor.	Solution
	LU-fact.	Solution	LU-fact.	Solution			
1920	0.31/15.4	0.01/14.9	0.60/7.89	0.01/7.77	1.92	0.076/61.7	0.010/54.4
3072	0.91/21.1	0.02/20.7	2.38/8.11	0.03/8.03	2.58	0.230/84.0	0.017/78.4
4992	2.62/31.7	0.03/31.3	8.51/9.75	0.06/9.68	3.24	0.518/160.0	0.029/151.7
7104	7.61/31.4	0.05/31.2	23.52/10.2	0.12/10.1	3.09	1.180/202.6	0.043/195.6
8064	10.88/32.1	0.07/31.9	33.92/10.3	0.15/10.3	3.10	1.684/207.6	0.050/201.7
9984	20.23/32.8	0.10/32.6	61.90/10.7	0.24/10.7	3.05	2.882/230.2	0.063/225.3
11008	26.49/33.6	0.12/33.4	82.28/10.8	0.28/10.8	3.09	3.718/239.2	0.071/234.7
25344	-	-	-	-	-	38.665/280.7	0.204/279.2

Table 3 shows the results of performance calculations of LU factorization in GFlop / s for the GPU Tesla C2075, GeForce GTX 480 and AMD Phenom II X6 1090T CPU for single (real) and double (double) precisions. It can be seen that for the equations size up to 3072, the cheaper GPU GeForce 480 overtakes the Tesla C2075 GPU. The Tesla C2075 has advantage for big equations. In general, with double-precision calculations for the 11008 equations size, the GPU Tesla C2075 overtakes the processor by 239.2 / 34.1 = 7.01 times.

Table 3

Results of productivity calculations for LU factorization in GFlop/s

Matrix NxN	GPU Tesla C2075		GPU GeForce 480		CPU AMD	
	real	double	real	double	real	double
1920	77.9	61.7	90.9	66.4	18.3	15.4
3072	**132.3**	**84.2**	**170.1**	**84.2**	**30.8**	**21.1**
4992	150.9	160.3	161.2	128.5	50.0	31.7
7104	221.4	203.3	234.3	143.1	60.9	32.1
8064	251.4	208.1	263.4	145.0	58.5	32.7
9984	317.3	230.2	329.7	150.9	71.6	33.3
11008	351.4	239.2	365.3	153.2	73.9	34.1

Table 4 shows the first argument calculations results of the equations system. Here Xr (1) corresponds to single precision, and Xd (1) corresponds to double precision. It is clear that the smaller the equations size, the less Xr (1) and Xd (1) differ. With a system size of 3000 equations, you can "believe" only the first three significant digits of the first argument, and with a size of 10,000 equations, the error becomes so large that the first significant digits become questionable. Thus, for systems with over 3000 equations, it is advisable to use only double-precision numbers in calculations.

Table 4

The results of the first argument calculations of the equations system

Matrix NxN	Argument Xr(1), Single precision.	Argument Xd(1), Double precision	Difference |Xr(1)-Xd(1)|
100x100	-9.904994E-02	-9.904992E-02	2.0E-06
1000x1000	7.36474E-03	7.36434E-03	4.0E-04
2000x2000	2.50738E-03	2.50710E-03	2.80E-04
3000x3000	**1.16325E-03**	**1.16273E-03**	**4.80E-04**
4000x4000	4.93012E-04	5.01715E-04	8.70E-02
5000x5000	4.92534E-04	5.03876E-04	1.13E-01
10000X10000	7.34304E-04	7.90892E-04	5.66E-01

Solving a system of 11008 equations with double precision numbers for Xd (1) showed the following results:

GPU Tesla C2075 Xd(1)=**9.93926624**47128E-004

CPU AMD Phenom II X6=**9.93926624**52686E-004

Here we can assume that the first nine significant digits are correct.

Conclusions

1. The installation process of the MAGMA libraries is not self-adjusting. Often it is necessary to make manual adjustments to the libraries when compiling and change the program texts. Therefore, the libraries' installation requires sufficient qualifications of a system programmer.

2. The MAGMA and CUBLAS libraries showed approximately the same matrix product performance for both single and double precision numbers. However, performance drops dramatically for the GeForce GTX 480 GPU when moving from single-precision to double-precision numbers (about 5.1 times). For the Tesla C2075 GPU, the performance drop does not exceed 2.1 times. Thus, Tesla C2075 GPU is more suitable for solving complex problems, requiring calculations with double precision. It also has a global memory of 6 GB (GeForce GTX 480 GPU has 1.5 GB).

3. The GPU GeForce GTX 480 and GPU Tesla C2075 performance for double-precision numbers is higher than that of the AMD Phenom II X6 1090T CPU by approximately 3.5 and 6.3 times respectively. And the performance of the GPU GeForce GTX 480 is 1.3 times higher than the performance of the GPU Tesla C2075 for single precision numbers. Therefore, for small tasks that require no more than 1.5 GB of memory and calculations with single precision, it is better to use GeForce GTX 480 GPU as an inexpensive and very efficient solution.

4. To achieve maximum performance of the NVIDIA CUDA GPU, it is necessary to use the MAGMA or CUBLAS libraries, which give an acceleration of the considered calculations about 6.4 times as compared with the use of global memory (the traditional programming method).

5. When solving equations systems, performance can be estimated only by LU factorization.

6. For systems with over 3000 equations, it is advisable to use only double-precision numbers in calculations.

7. When solving systems with up to 3000 equations, it is advisable to use a cheaper GPU GeForce 480 for computing with any precision. It works in this range of equations faster than AMD Phenom II X6 1090T CPU by 4 times for double precision numbers and 5.5 times for single precision numbers.

8. For a system of 11008 equations with double-precision GPU computations, it "excels" the CPU 7 times.

9. When solving systems of equations on a 6-core CPU, it is possible to achieve a maximum acceleration of 3.24 times as compared to calculations on the 1st core for the ScaLAPACK and ATLAS libraries. Sixfold acceleration cannot be obtained. Therefore, the effective use of processors with a large number of cores with the considered libraries is questionable.

10. The advantage of the GPU over the CPU increases with the number of equations. For example, the Tesla C2075 GPU for the 1920 equations in the system is 4 times faster than AMD CPU, and for 11008 equations it is even 7 times faster.

11. The considered methods for linear equations systems solving and matrix multiplication are valid for use in the single GPU computing system. However, it is not known how effective the parallelization of this task is on several GPUs installed in a multi-core system.

д.т.н., проф. Мясищев О.А., д.т.н., проф. Ленков С.В.,
к.т.н., доц. Джулий В.Н., к.т.н., доц. Муляр И.В.

ИСПОЛЬЗОВАНИЯ GPU NVIDIA ПРИ РЕШЕНИИ ЗАДАЧ ЛИНЕЙНОЙ АЛГЕБРЫ

В работе исследуется целесообразность применения графических процессоров при решении систем линейных уравнений и расчета матричного умножения по сравнению с обычными многоядерными процессорами. Рассматриваются особенности использования и проблемы установки библиотеки MAGMA. Для проведения вычислительных экспериментов рассмотрены две системы. В каждой из них установлен шестиядерный процессор (CPU) AMD. В первой системе использован графический процессор (GPU) Tesla C2075, во второй GeForce GTX 480 фирмы NVIDIA. GPU выполняют роль вычислительных ускорителей для решения систем линейных уравнений и матричного умножения. Причем в первом случае расчет выполняется с учетом распараллеливания по 6-ядрам процессора с использованием библиотек MPI, ScaLAPACK и ATLAS. Во втором и третьем случаях – распараллеливанием по ядрам GPU Tesla C2075 и GeForce GTX 480 с использованием технологии CUDA. Вычислительные системы работают под управлением операционной системы теками для 6-и ядерного процессора. Для программирования на GPU Tesla C2075 и GeForce GTX 480 инсталлированы видеодрайвер nvidia и программное обеспечение CUDA Toolkit. Установлено, что производительность GPU GeForce GTX 480 и GPU Tesla C2075 выше производительности тельность GPU GeForce GTX 480 в 1.3 раза выше производительности GPU Tesla C2075 для чисел с одинарной точностью. Показано, что для достижения максимальной производительности ускорение расчетов примерно в 6.4 раза по сравнению с традиционным способом программирования. Установлено, что при решении систем уравнений на 6-и ядерном CPU удается достичь максимального ускорения в 3.24 раза по сравнению с расчетами на 1-м ядре при использовании библиотек ScaLAPACK и ATLAS. Шестикратного ускорения получить не удается. Поэтому эффективное использование процессоров с большим количеством ядер с рассмотренными библиотеками стоит под вопросом. Показано, что преимущество GPU по сравнению с CPU возрастает с увеличением числа уравнений. Например, GPU Tesla C2075 для 1920 уравнений в системе работает в 4 раза быстрее CPU AMD, а для 11008 уравнений в 7 раз.

Ключевые слова: GPU Tesla C2075, MAGMA, CUBLAS, CUDA, графический процессор,

д.т.н., проф. Мясіщев О.А., д.т.н., проф. Лєнков С.В.
к.т.н., доц. Джулій В.М., к.т.н., доц. Муляр І.В.

ВИКОРИСТАННЯ GPU NVIDIA ПРИ ВИРІШЕННІ ЗАВДАНЬ ЛІНІЙНОЇ АЛГЕБРИ

В роботі досліджується доцільність застосування графічних процесорів при вирішенні систем лінійних рівнянь і розрахунку матричного множення у порівнянні зі звичайними багатоядерними процесорами. Розглядаються особливості використання і проблеми установки бібліотеки MAGMA. Для проведення обчислювальних експериментів розглянуті дві системи. У кожній з них встановлено шестиядерний процесор (CPU) AMD. У першій системі використаний графічний процесор (GPU) Tesla C2075, в другій GeForce GTX 480 фірми NVIDIA. GPU виконують роль обчислювальних прискорювачів для вирішення систем лінійних рівнянь і матричного множення. Причому в першому випадку розрахунок виконується з урахуванням розпаралелювання по 6-ядер процесора з використанням бібліотек MPI, ScaLAPACK і ATLAS. У другому і третьому випадках - розпаралелюванням по ядрах GPU Tesla C2075 і GeForce GTX 480 з використанням технології CUDA. Обчислювальні системи працюють під управлінням операційної системи Linux Ubuntu. На них встановлені компілятори фортран і C ++ з перерахованими вище бібліотеками для 6-и ядер-

ного процесора. Для програмування на GPU Tesla C2075 і GeForce GTX 480 інстальовані відеодрайвер nvidia і програмне забезпечення CUDA Toolkit. Встановлено, що продуктивність GPU GeForce GTX 480 і GPU Tesla C2075 вище продуктивності CPU AMD приблизно в 3.5 і 6.3 разів відповідно для чисел з подвійною точністю. А продуктивність GPU GeForce GTX 480 в 1.3 рази вище продуктивності GPU Tesla C2075 для чисел з одинарної точністю. Показано, що для досягнення максимальної продуктивності GPU NVIDIA CUDA необхідно використання бібліотек MAGMA або CUBLAS, які дають прискорення розрахунків приблизно в 6.4 рази в порівнянні з традиційним способом програмування. Встановлено, що при вирішенні систем рівнянь на 6-й ядерному CPU вдається досягти максимального прискорення в 3.24 рази в порівнянні з розрахунками на 1-му ядрі при використанні бібліотек ScaLAPACK і ATLAS. Шестиразового прискорення отримати не вдається. Тому ефективне використання процесорів з великою кількістю ядер з розглянутими бібліотеками стоїть під питанням. Показано, що перевага GPU у порівнянні з CPU зростає зі збільшенням числа рівнянь. Наприклад, GPU Tesla C2075 для 1920 рівнянь в системі працює в 4 рази швидше CPU AMD, а для 11008 рівнянь в 7 разів.

Ключові слова: GPU Tesla C2075, MAGMA, CUBLAS, CUDA, графічний процесор, NVIDIA Tesla V100, SMP система, MPI, ScaLAPACK, ATLAS.

УДК 35.082.37

к.військ.н. **Думенко М.П.** (ГУП ГШ ЗСУ)
Гуляк У.М. (Кадровий центр ЗСУ)

ОЦІНКА ЕФЕКТИВНОСТІ РОБОТИ СЛУЖБ (ПІДРОЗДІЛІВ) ПЕРСОНАЛУ ЗБРОЙНИХ СИЛ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ (ОСОБЛИВОГО ПЕРІОДУ)

У статті описано взаємозалежність ефективного виконання завдань за призначенням службами (підрозділами) персоналу від їх структури та чисельності. Зосереджено увагу на особливостях виконання задач службами (підрозділами) персоналу в умовах особливого періоду. Крім того, розглянуто які зміни відбулися в структурі, чисельності та функціях служб (підрозділів) персоналу при їх переході на функціонування в умовах особливого періоду. Наведено рекомендації щодо раціональної структури системи кадрового забезпечення, спрямовані на оптимальне виконання завдань щодо забезпечення потреб ЗС України в людських ресурсах та індивідуального підходу до кожної особи, її розвитку, кар'єрного зростання та використання відповідно до призначення. Зроблено висновки щодо необхідності подальшого вдосконалення існуючої системи кадрового менеджменту, а також приведення структури та чисельності служб (підрозділів) персоналу Збройних Сил України у відповідність до перспективної системи, структури і чисельності "J-структури" (J-1), прийнятої за основу в штабах збройних сил країн – членів НАТО. Описано поняття "ефективність" з наукової точки зору, у контексті дослідження результативності функціонування будь-якої системи або процесів, як основну властивість будь-якої системи, у тому числі і системи управління. Здійснено короткий огляд декількох варіантів оцінки ефективності професійної діяльності служб (підрозділів) персоналу Збройних Сил України під чим розуміється процес визначення ефективності діяльності працівників служб (підрозділів) персоналу в реалізації стратегічних завдань Збройних Сил України з метою послідовного накопичення інформації, необхідної для прийняття подальших управлінських рішень. Запропоновано напрямок і перспективи подальших досліджень у сфері діяльності служб (підрозділів) персоналу.

Ключові слова: військова кадрова політика, служба (підрозділ) персоналу, гібридна війна, особливий період, ефективність.

Вступ. Сучасні перетворення в державі вимагають надійного захисту від зовнішньої агресії та потребують консолідації суспільства, При цьому Збройні Сили України (далі – ЗС України) відіграють провідну роль у забезпеченні національної безпеки. Одним із пріоритетних напрямів підвищення ефективності формування та реалізації державної політики забезпечення національної безпеки є удосконалення науково-методичного та інформаційно-аналітичного забезпечення всіх систем управління, у тому числі служб (підрозділів) персоналу.

З огляду на те, що наша країна перебуває в умовах гібридної війни, зважаючи на значне розширення спектру викликів та загроз національній безпеці України постає питання наукового обґрунтування системи функціонування органів державної влади та забезпечення функціонування ЗС України.

У цьому контексті зростає потреба в запровадженні нових підходів у військовій кадровій політиці, як державного кадрового менеджменту у військовій сфері. А кадрова політика, безумовно, реалізується в управлінні персоналом через діяльність кадрових органів, їх кадрову роботу.

Постановка проблеми. Аналіз різноманітних досліджень, присвячених проблемам підвищення ефективності комплектування особовим складом, оцінюванню ефективності роботи служб (підрозділів) персоналу ЗС України та системи комплектування взагалі, показують, що ці питання активно досліджуються. Особливої уваги вони набувають сьогодні, коли країна переходить від тенденцій скорочування ЗС України до нарощування кадрових та бойових потенціалів військових формувань з метою підвищення рівня обороноздатності. Стан, у якому перебувають ЗС України не відповідає вимогам сьогодення, тобто умовам їх функціонування в

стані підвищеної бойової готовності. Однією із головних причин такого стану є неефективне реформування протягом останніх років служб (підрозділів) персоналу ЗС України, що вже призвела до невідповідності кадрового потенціалу ЗС України сучасним вимогам. Існуючі підходи щодо оцінювання ефективності роботи служб (підрозділів) персоналу ЗС України не дозволяють отримати повністю об'єктивну оцінку їх функціонування, а тим більше не дозволяють оцінити різні варіанти пропозицій щодо удосконалення служб (підрозділів) персоналу ЗС України, та прийняти рішення щодо вибору найбільш оптимального із них.

Виходячи із зазначеного розгляд питання функціонування служб (підрозділів) персоналу та визначення варіанту оцінювання ефективності їх роботи є актуальним питанням сьогодення.

Аналіз останніх досліджень і публікацій. Питанням функціонування служб (підрозділів) персоналу з урахуванням перспектив розвитку збройних сил та з урахуванням попереднього досвіду в умовах дії особливого періоду займаються різні науковці та спеціалісти. Серед останніх, дослідження фахівців Науково-дослідного інституту ЗС України, які опрацювали рекомендації щодо раціональної структури системи кадрового забезпечення з урахуванням перспектив розвитку ЗС України, а саме: рекомендації загального характеру щодо удосконалення системи кадрового забезпечення ЗС України; рекомендації щодо удосконалення структури системи кадрового забезпечення ЗС України; рекомендації щодо удосконалення системи кадрового забезпечення за напрямом "залучення на військову службу"; рекомендації щодо удосконалення системи кадрового забезпечення за напрямом "підготовка кадрів"; рекомендації щодо розвитку системи кадрового забезпечення за напрямом "кадровий менеджмент". Наведено рекомендації щодо раціональної структури системи кадрового забезпечення, спрямовані на оптимальне виконання завдань щодо забезпечення потреб ЗС України в людських ресурсах та індивідуального підходу до кожної особи, її розвитку, кар'єрного зростання та використання відповідно до призначення.

Проблемами розробки критеріїв ефективності управлінських процесів розглядалися такими науковцями, як: Р. Беллман, Р. Калаба, Н. Красовський, Н. Мойсеєв, С. Поленіна, А. Файнстейн та інші. Сучасна наука розглядає достатньо широкий спектр критеріїв, які застосовуються в різних областях знань, управлінських та інформаційних системах, такі як: байєсовський критерій, критерій Гурвіца, критерій "ідеального спостерігача", критерій якості, критерій максимально швидкодії, критерій мінімаксний, критерій мінімуму вірогідності помилки, критерій мінімуму середнього ризику, критерій Найквіста, критерій Неймана – Пірсона та ін. [1, 2].

Вітчизняні науковці О. Водчиць, О. Семененко, Ю. Добровольський, А. Бердочник у своїх наукових роботах запропонували методики оцінки ефективності функціонування систем (органів) комплектування ЗС України особовим складом [3].

С. Богунов, Ю. Герман, О. Сакун, Б. Шупель у своїх дослідженнях висвітлили такі достатні умови ефективної роботи кадрових органів: кількісна та якісна укомплектованість особовим складом відповідає діючим нормативам; ефективне планування та прогнозування кадрової ситуації; висування на вищі посади та направлення на навчання здійснюється виключно з кадрового резерву; не допускаються випадки формалізму та протекціоналізму під час роботи з кадрами; якісно та своєчасно опрацьовується звітно-облікова статистична документація, подаються документи на присвоєння військових звань та переміщення по службі; систематично аналізується якісний склад військовослужбовців та готуються пропозиції щодо їх подальшого службового використання; своєчасно та ефективно використовуються всі методи морального та матеріального стимулювання за досягнуті результати у службі; якісно і своєчасно здійснюється відбір та розстановка кадрів на підставі чинного законодавства; застосовуються сучасні методи кадрового менеджменту під час роботи з особовим складом для запобігання плинності кадрів; відсутні скарги на працівників кадрових органів [4].

У статті увага зосереджена на діяльності служб (підрозділів) персоналу під час ведення гібридної війни (в умовах особливого періоду).

Мета статті полягає у визначенні варіанту оцінки ефективності функціонування служб (підрозділів) персоналу під час ведення гібридної війни (в умовах особливого періоду).

Викладення основного матеріалу. Сучасний процес розвитку ЗС України тісно пов'язаний зі змінами всієї системи управління, передбачає її відхід від принципів адміністративно-командного керівництва одним із елементів якого є система кадрового менеджменту, основна мета якого – задовольнити потреби збройних сил у кваліфікованих кадрах, ефективно використовуючи їх знання і навички з урахуванням можливостей самореалізації. Проведення шести черг часткової мобілізації під час проведення антитерористичної операції на сході України засвідчило, що намагання створити цілісну та ефективну централізовану систему підтримки прийняття рішень в управлінні персоналом пройшли перевірку на дієздатність на практиці і показали свою неефективність у питаннях управління персоналом, зокрема, стосовно військового обліку персоналу, що потребує постійного вдосконалення з питань обліку як військовозобов'язаних громадян, так і особового складу ЗС України, який проходить дійсну військову службу [5]. Відповідно до проведеного аналізу було встановлено, що для вирішення проблем, що впливають на роботу служб (підрозділів) персоналу в умовах особливого періоду необхідно скорегувати завдання та функції служб (підрозділів) персоналу усіх рівнів органів військового управління та військових комісаріатів, визначити та удосконалити їх організаційно-штатну структуру, а також автоматизувати процеси обліку діючого особового складу ЗС України та військовозобов'язаних громадян України.

Добре відомо, що починаючи з 2012 року структура кадрових органів (на той час) постійно змінювалася і проявлялася тенденція скорочення структур та особового складу служб (підрозділів) персоналу. Було розформовано кадрові центри Сухопутних військ та Військово-Морських Сил ЗС України. Кадровий центр Повітряних Сил ЗС України розформувати не встигли. Поступово, протягом 2014-2018 років, кадрові центри було відновлено та укомплектовано кваліфікованими спеціалістами [6]. На теперішній час, порівнюючи з початком ведення гібридної війни, відбулися суттєві зміни у структурі служб (підрозділів) персоналу, зміни в чисельності працівників служб (підрозділів) персоналу, а також відбувається активна автоматизація процесів їх повсякденної діяльності на всіх рівнях військового управління.

На сьогоднішній день у ЗС України розподіл повноважень між кадровими органами військового управління системи кадрового забезпечення в ЗС України та ведення ними військового обліку персоналу здійснюється на трьох рівнях:

вищий рівень управління – стратегічний. Командири цього рівня здійснюють управління у прямому сенсі цього слова. На цьому рівні розробляються довгострокові програми, перспективні цілі кадрової політики (концепції), приймаються рішення щодо найважливіших і найскладніших проблем.

Середній рівень – оперативний рівень управлінської діяльності, на якому органи особового складу здійснюють організацію кадрової професійної діяльності в з'єднаннях. Іде розстановка безпосередніх організаторів і виконавців заходів. Важливим напрямом діяльності органу управління є навчання та допомога командирам й офіцерам у роботі та контроль за виконанням рішень, узагальнення і поширення передового досвіду.

Тактичний рівень управлінської діяльності притаманний ланці "військова частина – військовий комісаріат – підрозділ". На цьому рівні здійснюється безпосередня організація управління персоналом, тобто кадрова робота.

Таким чином, цілі та рішення, які розробляються на стратегічному рівні управління, уточнюються й конкретизуються на оперативному рівні, після чого виконуються безпосередньо на тактичному рівні.

Результати досліджень Центрального науково-дослідного інституту ЗС України свідчать, що структура служб (підрозділів) персоналу, чисельність їх персоналу та розподіл завдань між ними повинні забезпечувати повноту та своєчасність виконання покладених на службу (підрозділ) персоналу завдань [7].

Відповідно до керівних документів [8], служба персоналу – структурний підрозділ органу військового управління, з'єднання, військової частини, військового навчального закладу, установи або організації (посадова особа, на яку покладено завдання кадрової роботи, де штатом не передбачено відповідного органу або окремої штатної посади), який призначений

для реалізації державної військової кадрової політики та політики з питань проходження державної служби у ЗС України, комплектування ЗС України особовим складом у мирний час, а також військовозобов'язаними в особливий період, забезпечення проходження військової служби (трудової діяльності) громадянами України відповідно до законодавства.

Таким чином, діяльність служб (підрозділів) персоналу не обмежується лише вирішенням питань прийому, обліку та звільнення з військової служби. А й реалізацією ключових питань військової кадрової політики.

Так, з початком особливого періоду основна робота служб (підрозділів) персоналу була спрямована на розв'язання проблем оперативного комплектування особовим складом частин (підрозділів) ЗС України, у першу чергу військових частин бойового складу, крім того:

удосконалюються нормативно-правові акти та керівні документи, якими врегульовуються питання комплектування ЗС України особовим складом, порядку проходження військової служби, підвищення мотивації та соціального захисту військовослужбовців в особливий період;

виконуються заходи щодо розвитку професійного сержантського та старшинського складу;

делеговано окремі повноваження Міністра оборони України, начальника Генерального штабу – Головнокомандувача ЗС України та їх перших заступників керівникам органів військового управління нижчого рівня та служб персоналу щодо присвоєння військових звань та звільнення з військової служби;

розширено повноваження командирів щодо призначення на посади для підвищення оперативності прийняття кадрових рішень;

сформовано дієвий кадровий резерв з числа учасників антитерористичної операції для комплектування керівних посад військовослужбовців в органах військового управління різного рівня;

запроваджено нову комплексну систему оцінювання військовослужбовців із обов'язковим врахуванням її результатів на етапі підготовки та прийняття кадрових рішень;

проведення щорічного оцінювання службової діяльності військовослужбовців, які виконують завдання в операції об'єднаних сил, зі складанням скороченої оцінної картки військовослужбовця;

запровадження процедури самооцінки військовослужбовців, яка відображається в його оцінній картці;

перегляд та деталізація критеріїв оцінювання службової діяльності військовослужбовців з урахуванням специфіки їх службової діяльності за посадами, як у мирний час, так і на особливий період;

продовжується впровадження єдиної автоматизованої інформаційно-аналітичної системи обліку та управління персоналом тощо.

Поряд з цим залишається невирішеною низка питань, позитивний вплив проведених заходів на якісний стан комплектування ЗС України усіма категоріями особового складу досі недостатній.

Так, не набули системного характеру перепідготовка та підвищення кваліфікації фахівців служб персоналу Міністерства оборони та ЗС України. Система управління кар'єрою не забезпечує на достатньому рівні планування та управління кар'єрою військовослужбовців, не спрямована на оптимальне виконання завдань щодо забезпечення потреб збройних сил у людських ресурсах та застосування індивідуального підходу до кожної особи, її розвитку, кар'єрного зростання та використання відповідно до призначення. Допускається необ'єктивна оцінка службової діяльності підлеглих під час їх атестування. Ротація офіцерського складу використовується не достатньо ефективно через невирішеність соціально-побутових проблем військовослужбовців. Існуюча система комплектування не забезпечує належного рівня укомплектованості офіцерських посад, особливо первинних, через різке збільшення штатної чисельності та звільнення особового складу з військової служби [8].

У цьому контексті слід зробити висновок, що на даному етапі функціонування ЗС України, існуюча система кадрового менеджменту потребує подальшого вдосконалення, а структура та чисельність служб (підрозділів) персоналу ЗС України потребують приведення у відповідність до перспективної системи, структури і чисельності "J-структури" (J1), прийнятої за основу в штабах збройних сил країн – членів НАТО [9].

Разом з тим, існують методи, які дозволяють виміряти ефективність роботи служб (підрозділів) персоналу емпірично.

Ефективність є однією з найважливіших загальнонаукових категорій і через це широко застосовується в різних галузях людської діяльності. Існує кілька визначень цієї важливої категорії, якими розкривається її сутність. Поняття "ефективність" є похідним від поняття "ефект". Ефект (від лат. Effectus) – результат певних дій, заходів. Ефективний, дієвий, який дає бажаний результат. Отже, ефективність це результативність, дії чого-небудь. Поняття "ефективність" з наукової точки зору, як правило, використовується в тих випадках, коли досліджується результативність функціонування, будь-якої системи або процесів, тобто це не що інше, як основна властивість будь-якої системи, у тому числі і системи управління [10].

У сучасній науці під оцінкою персоналу розуміють процес визначення ефективності діяльності працівників служб (підрозділів) персоналу в реалізації стратегічних завдань ЗС України з метою послідовного накопичення інформації, необхідної для прийняття подальших управлінських рішень [11].

Варто відмітити, що ефективність роботи працівників служб (підрозділів) персоналу кількісно достатньо важко виміряти. У цілому це полягає в тому, що її результат не тільки не виражається прибутком, але і не проявляється безпосередньо (наприклад соціально, політично). Таким чином, оцінка ефективності діяльності таких працівників є набагато складнішою, ніж створення аналогічних розрахунків для цивільних працівників виробничої сфери чи сфери послуг [12].

На теперішній час не існує одного сталого методу оцінки ефективності діяльності служб (підрозділів) персоналу, який би дозволяв повністю відобразити ступінь їх пристосованості до свого цільового призначення – головна, цільова властивість служби (підрозділу) персоналу забезпечує досягнення мети кадрового забезпечення з найменшими втратами під час переходу на функціонування в умовах особливого періоду та збільшення потреби в особовому складі. Найбільш ефективною служба (підрозділ) персоналу є в ідеальних умовах (відсутність впливу противника, перешкод, порушень роботи технічних засобів управління, а також повна укомплектованість органів військового управління, військових частин, підрозділів високо підготовленим особовим складом і сучасними боєготовими технічними засобами управління і автоматизації) [13]. Як уже зазначалося на початку статті, у реальних умовах під впливом багатьох об'єктивних і суб'єктивних факторів служби (підрозділи) персоналу функціонують "неідеально", тобто їх ефективність залежить від ступеня пристосованості до умов функціонування з урахуванням багатьох чинників.

Розглянемо деякі з варіантів оцінювання ефективності функціонування служб (підрозділів) персоналу ЗС України в умовах дії особливого періоду.

Варіант 1. Оскільки система комплектування ЗС України є підсистемою більш складної системи управління стратегічного (оперативно-стратегічного) рівня, то її ефективність, безумовно, впливатиме на результати вирішення стратегічних завдань, ступінь реалізації яких буде характеризувати ефективність роботи служб (підрозділів) персоналу на оперативному рівні.

$$E_{SP} = \frac{\sum_{i}^{N} \frac{T_{SRi}}{T_{SPi}}}{N},$$

де E_{SP} – ефективність роботи служби (підрозділу) персоналу;

T_{SRi} – реалізовані стратегічні завдання під час переходу на функціонування в умовах особливого періоду, де $i \in \{1 \ldots N\}$ – множина стратегічних завдань;

T_{SPi} – стратегічні завдання, які заплановані для виконання під час переходу на функціонування в умовах особливого періоду.

Варіант 2. Під ефективністю роботи служб (підрозділів) персоналу можна розуміти їх вклад в реалізацію потенційних оперативних (бойових) можливостей військ, військових частин і підрозділів, на що безпосередньо впливає рівень укомплектованості. Змістом кадрової роботи у цьому випадку є здатність виконувати завдання за призначенням з урахуванням конкретних умов (бойових) обстановки, тоді ефективність роботи служби (підрозділу) персоналу буде визначатися виразом:

$$E_{SP} = \sum_{j=1}^{m} \frac{B_{Rj}}{\sum_{i=1}^{n} B_{Pi}},$$

де E_{SP} – ефективність служби (підрозділу) персоналу;

B_{Rj} – кадрова робота, яка була проведена під час переходу на функціонування в умовах особливого періоду, де $j \in \{1 \ldots m\}$ – множина реалізованих кадрових задач;

B_{Pi} – кадрова робота, яка була спланована до виконання під час переходу на функціонування в умовах особливого періоду, де $i \in \{1 \ldots n\}$ – множина потенційних кадрових задач.

Варіант 3. На служби (підрозділи) персоналу покладається виконання низки завдань, основними з яких є: створення ефективної системи управління кар'єрою військовослужбовців та впровадження прозорої і доброчесної системи підбору, розстановки та призначення особового складу на посади; приведення структури особового складу у відповідність до потреб ЗС України, які зумовлені їх завданнями і структурою та наближені до середніх показників збройних сил країн – членів НАТО; забезпечення розподілу випускників вищих військових навчальних закладів у відповідності з отриманим рівнем освіти та набутою спеціальністю; забезпечення ефективного службового використання військовослужбовців, які мають оперативно-стратегічний (оперативно-тактичний) рівень військової освіти, високий рівень професійної підготовки, науковий ступінь, пройшли навчання за кордоном, є учасниками бойових дій та мають високі досягнення в індивідуальній підготовці; забезпечення укомплектованості первинних офіцерських посад; забезпечення розвитку служби у військовому резерві з поступовим нарощуванням чисельності резервістів для доукомплектування військових частин як у мирний час, так і в особливий період; використання в системі управління персоналом сучасних технологій кадрового менеджменту, впровадження у кадровій роботі прозорих та доброчесних процедур прийняття кадрових рішень, підвищення відповідальності за прийняття кадрових рішень, створення єдиної автоматизованої системи обліку та управління персоналом; здійснення індивідуального планування кар'єри військовослужбовців відповідно до типових алгоритмів управління кар'єрою, визначених вимог до посад та результатів службової діяльності; формування дієвого резерву кандидатів для просування по службі за рейтинговим принципом, на підставі результатів комплексного оцінювання; уточнення кваліфікаційних вимог до посад, переопрацювання паспортів військових посад і типових алгоритмів управління кар'єрою військовослужбовців тощо [8].

Таким чином, у такому аспекті ефективність роботи служб (підрозділів) персоналу можна розглядати як ступінь своєчасного виконання (обсягу виконаних) покладених на них завдань під час переходу на функціонування в умовах особливого періоду.

$$E_{SP} = \frac{\sum_{j=1}^{m} \mathrm{E}_{SRj}}{\sum_{i=1}^{n} T_{Pi}},$$

де E_{SP} – ефективність роботи служби (підрозділу) персоналу;

E_{SRj} – завдання служби (підрозділу) персоналу, яке було реалізоване під час переходу на функціонування в умовах особливого періоду, де $j \in \{1...m\}$ – множина реалізованих кадрових задач;

T_{Pi} – завдання служби (підрозділу) персоналу, які було сплановано до виконання, де $i \in \{1...n\}$ – множина потенційних кадрових задач.

Варіант 4. До служб (підрозділів) персоналу висувається ряд вимог. Для того, щоб вони ефективно функціонували повинні виконуватися всі вимоги, причому в різних умовах ці вимоги можуть зазнавати змін. Ступінь відповідності цим вимогам і буде визначати ефективність їх функціонування. Таким чином, робота служб (підрозділів) персоналу буде ефективна, коли всі показники (які характеризують відповідність вимогам, що пред'являються) будуть відповідати необхідним значенням, або бути близькими до них. Основні вимоги до служб (підрозділів) персоналу в умовах особливого періоду це – високий рівень готовності до функціонування; забезпечення укомплектованості пріоритетних військових частин до визначених показників; оперативність, раціональність використання кадрового потенціалу тощо.

У такому випадку ефективність роботи служби (підрозділу) персоналу буде визначатися виразом:

$$E_{SP} = \sum_{i=1}^{n} \frac{R_{ri}}{R_i},$$

де E_{SP} – ефективність роботи служби (підрозділу) персоналу;

R_{ri} – вимоги, які були реалізовані під час переходу на функціонування в умовах особливого періоду, де $i \in \{1...n\}$ – множина вимог до служби (підрозділу) персоналу;

R_i – вимоги, які пред'являються до служби (підрозділу) персоналу.

Критерії ефективності застосовуються на основі певної концепції формулювання рішень. Розрізняють три таких концепції: придатності, оптимізації, адаптивності [1].

Згідно з концепцією придатності раціональне будь-яке рішення u, при якому обраний показник ефективності приймає значення не нижче деякого припустимого (потрібного) рівня E_0, тобто $E(u) \geq E_0 \quad u \in V$, де V – множина припустимих рішень.

Оптимізація зводиться до визначення рішень $u^* \in V$, які екстремізують (максимізують або мінімізують) обраний показник ефективності при фіксованих обмеженнях, тобто:

$$E(u^*) = \underset{u(t) \in V(t)}{extr} \cdot E(u).$$

Адаптивність передбачає можливість оперативного реагування в процесі функціонування системи на поточну інформацію, яка надходить, щодо змін умов її функціонування. Сутність концепції адаптивності полягає в зміні параметрів, структури і алгоритмів функціонування системи на основі не тільки апріорної інформації, але поточної і прогнозованої для досягнення або збереження певної ефективності системи при змінах умов функціонування останньої.

Множина припустимих рішень може змінюватися в процесі отримання поточної інформації. Згідно з концепцією адаптивності раціональним слід вважати рішення $u^*(t)$ із множини $V(t)$, яка, наприклад, забезпечує виконання умови:

$$E_t(u^*(t), \tau) = \underset{u(t) \in V(t)}{extr} \cdot E_t(u(t), \tau).$$

Виходячи із зазначеного, можна резюмувати, що кожен із запропонованих варіантів заслуговує на увагу і може бути використаний при оцінці ефективності роботи відповідних служб (підрозділів) персоналу. Виходячи з конкретних умов обстановки доцільно обирати один із них. Так, перший варіант доцільно застосовувати для стратегічної ланки, другий дозволяє здійснювати оцінку для оперативно-тактичної ланки, третій варіант – для тактичної ланки. Останній пропонується застосовувати в контексті розвитку теорії та пошуку нових методів і підходів щодо оцінки ефективності роботи служб (підрозділів) персоналу.

Усі перераховані вище варіанти на перший погляд досить прості, складність полягає у визначенні (знаходженні) значень складових ефективності роботи служб (підрозділів) персоналу. Твердження "чим краще функціонують служби (підрозділи) персоналу, тим вище ефективність виконання завдань при переході на функціонування в умовах особливого періоду" в принципі може бути правильним. Але, у ньому міститься велика невизначеність, так як успіх проведення будь-якої військової операції буде залежати великою мірою від оперативних (бойових) можливостей військ, а також їх бойової готовності. Саме тому завдання щодо визначення кількісного внеску служб (підрозділів) персоналу в досягнення кінцевої мети операції є складною і важливою одночасно. Ефективність функціонування будь-якої системи може (повинна) мати кількісну міру і виражатися числом.

У цьому ракурсі оцінювання ефективності служби (підрозділу) персоналу пропонується здійснювати за шкалами у балах, наприклад, двохбальною або п'ятибальною шкалою, дванадцятибальною або стобальною тощо. Заслуговує на увагу оцінка у відсотковому відношенню за методом Харрінгтона [1].

Висновки й перспективи подальших досліджень. Досвід проведення антитерористичної операції на сході України, функціонування ЗС України в умовах особливого періоду показав, що ефективність роботи служб (підрозділів) персоналу безпосередньо впливає на результативність виконання ЗС України завдань за призначенням.

Запропоновані в статті варіанти дозволяють оцінювати результати функціонування існуючих служб (підрозділів) персоналу ЗС України, а також оцінювати можливі удосконалені або нові варіанти структури цих служб з метою прийняття обґрунтованих рішень щодо вибору найбільш ефективних (раціональних) варіантів. Подальші дослідження у цій сфері доцільно спрямувати на обґрунтування чисельності служб (підрозділів) персоналу, необхідної для їх ефективного функціонування в умовах ведення гібридної війни (під час особливого періоду).

ЛІТЕРАТУРА:

1. Агаєва Н.С., Базарний В.Т., Даценко О.П., Критерії та оцінка елементів кадрового потенціалу ЗС / Вісник Національного університету оборони України 3(40)/ 2014. – С. 10-15.

2. Харин В.В., Шишков М. В., Бобринев Е.В., Удавцова Е.Ю. ФГБУ ВНИИПО МЧС России, г. Балашиха "Оценка эффективности служебной деятельности кадровых органов". – 2011. – С. 58-62.

3. Водчиць О.Г. Методика оцінки ефективності функціонування систем (органів) комплектування Збройних Сил України особовим складом/ О.Г. Водчиць, О.М. Семененко, Ю.Б. Добровольський, А.Д. Бердочник // Наука і техніка Повітряних Сил Збройних Сил України. – 2014., № 3. – С. 14-17.

4. Шмелева А.Н. Оценка и повышение операционной эфективности системы менеджмента качества предприятия: теория, методология, практика. Дис. к.э.н. – Тамбов, 2011. – С. 41-42.

5. Гриненко О.І. Деякі проблеми перспективного планування розвитку ЗС України/ О.І. Гриненко, Дєнєжкін М.М. // Наука і оборона. – № 3. – К.,2011. – С. 31-35.

6. Половінкін І.М., Базарний В.Т., Медвідь А.П. Кадрова політика у ЗС України, як система управління людськими ресурсами/ Вісник Національного університету оборони України 3(22)/ 2011. – С. 66-70.

7. Дослідження шляхів оптимізації системи кадрового забезпечення з урахуванням перспектив розвитку ЗС України. Обґрунтування рекомендацій щодо раціональної структури системи кадрового забезпечення з урахуванням перспектив розвитку ЗС України: звіт про НДР шифр "КАДРИ – 2014" (проміжн.) кер. Дідіченко В. П.; викон. Козлов В.В., Пасічник В.П. та ін. Київ, ЦНДІ ЗС України ЦНДІ Київ, 2014. 98 с.

8. Концепція військової кадрової політики у Збройних Силах України на період до 2020 року: наказ Міністерства оборони України від 26.06.2017 № 342.

9. План дій щодо впровадження оборонної реформи у 2016 – 2020 роках (дорожня карта оборонної реформи): затв. Міністром оборони України 15.08.2016.

10. Дамиров Д.Я. Критерии эффективности государственного управления [Електронний ресурс www.lex-pravo.ru/ru-2740.html].

11. Методика оцінювання ефективності використання кадрового потенціалу в Збройних Силах України/ Романченко І.С., Артюх В.М. // Труди академії. – 2008. № 7(87). С. 12-20.

12. Королева С.В. Оценка эффективности деятельности государственного гражданского служащего / Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2013. № 7.

13. Оцінка ефективності системи кадрового менеджменту у Збройних Силах України/ Устименко О.В. // Збірник наукових праць "Труди університету". – 2010. – № 2(95). – С. 281-287.

REFERENCES:

1. Agaeva, N.S., Bazarnyi, V.T and Datsenko, O.P. (2014), "Kryterii ta otsinka elementiv kadrovogo potentsialu ZS" [Criteria and assessment of elements of personnel potential of the Armed Forces] / *Visnyk natsional'nogo universytetu oboronu Ukrainu*, No. 3(40), pp. 10-15.

2. Kharin, V.V., Shishkov, M.V., Bobrinev, E.V. and Udavtsova, E.Yu. (2011), "Otsenka efectivnosti sluzebnoy deyatel'nosti kadrovih organov" [Perfomance appraisal of personnel agencies]. Balashikha: FGBU VNUUPO MCHS Rosii, pp. 58-62.

3. Vodchuts', O.G. (2014), "Metoduka otsinku efectuvnosti funktsionyvannya system (organiv) konplectyvannya Zbroynuh Syl Ukrainy osobovum skladom" [A methodology for evaluating of the effectiveness of the functioning of systems (sections) staffing personnel of the Armed Forces of Ukraine] / Vodchuts' O.G., Semenenko O.M., Dobrovol'skyu Yu.B., Berdochnuk A.D. // *Science and Technology of the Air Force of Ukraine*, No. 3, pp. 14-17.

4. Shmeleva, A.N. (2011), "Otsenka i povishenie operatsionnoy efektivnosti sistemy menedgmenta katchestva predpriyatiya: teoriya, metodologiya, practika" [Evaluation and improvement of the operational efficiency of the enterprise quality management system: theory, methodology, practice] – Tambov, pp. 41-42.

5. Grunenko, O.I. (2011), "Deyaki problemu perspectyvnogo planyvannya rozvutky ZS Ukrainy" [Some problems of forward-looking development of the Armed Forces of Ukraine] / Grunenko O.I., Denezkin M.M. // *Science and defense*, Kyiv, No. 3, pp. 31-35.

6. Polovinkin, I.M., Bazarnuy, V.T. and Medvid', A.P. (2011), "Kadrova polityka y ZS Ukrainy, yak systema upravlinnya lyuds'kymy resursamy" [Personnel policy in the Armed Forces of Ukraine as a human resources management system] / *Visnyk natsional'nogo universytetu oboronu Ukrainu*, No. 3(22), pp. 66-70.

7. "Doslidgennya shlyahiv optumizatsii systemy kadrovogo zabezpechennya z vrakhyvannyam perspectyv rozvutky ZS Ukrainy. Obgryntyvannya recomendatsiy schodo ratsional'noi structury systemy kadrovogo zabespechennya z vrakhyvannyam perspectuv rozvutky ZS Ukrainy": [Studying the ways ov optimizing the personnel supply system taking into account the prospects for the development of the Armed Forces of Ukraine. Justification of recommendations for a rational structure of the personnel supply system taking into account the prospects for the development of the Armed Forces of Ukraine] / Zvit NDR "Kadry" – 2014 / Didichenko V.P., Kozlov V.V., Pasichnyk V.P., Kyiv, p. 98.

8. Kontseptsiya viys'kovoi kadrovoi polituky y Zbroynyh Sylah Ukrainy na period do 2010 roky: nakaz Ministerstva oborony Ukrainy vid 26.06.2017 № 342.

9. Plan diy schodo vprovadjennya oboronnoi reform y 2016-2020 rokah (dorojnya karta oboronnoi reformy): zatv. Ministrom oborony Ukrainy 15.08.2016.

10. Damirov, D.Ya. "Kryterii efectivnosti gosydarstvennogo ypravleniya" [Perfomance criteria of public administration] / www.lex-pravo.ru/ru-2740.html.

11. Romanchenko, I.S. and Artyukh, V.M. (2008), "Metodyka otsinyuvannya efectyvnosti vukorystannya kadrovogo potentsialy v Zbroynuh Sylah Ukrainy" [A methodology for assessing the effectiveness of the use of human resources in the Armed Forces of Ukraine] / *Trudy Academii*, No. 7(87), pp. 12-20.

12. Koroleva, S.V. (2013), "Otsenka efectivnosti deyatel'nosti gosydarstvennogo grajdanskogo slujaschego" [Civil servant performance evaluation] / *Science and education: household and economy; entrepreneurship; law and administration*, No. 7, pp. 18-24.

13. Ustimenko, O.V. (2010), "Otsinka efectyvnosti systemu kadrovogo menedgmenty y Zbroynuh Sylah Ukrainy" [Assessment of the effectiveness of the personnel management system], *Collection of scientific works "University works"*, No. 2(95), pp. 281-287.

к.воен.н. Думенко Н.П., Гуляк У.Н.

ОЦЕНКА ЕФЕКТИВНОСТИ РАБОТЫ СЛУЖБ (ПОДРАЗДЕЛЕНИЙ) ПЕРСОНАЛА ВОРУЖЕННЫХ СИЛ УКРАИНЫ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ (ОСОБОГО ПЕРИОДА)

В статье описана взаимозависимость эффективного выполнения задач по назначению службами (подразделениями) персонала от их структуры и численности. Сосредоточено внимание на особенностях выполнения задач службами (подразделениями) персонала в условиях особого

периода. Кроме того, рассмотрено изменения в структуре, численности и функциях служб (подразделений) персонала при переходе на функционирование в условиях особого периода. Наведены рекомендации касательно рациональной структуры системы кадрового обеспечения, которые нацелены на оптимальное выполнение задач по обеспечению потребностей Вооруженных Сил Украины в человеческом ресурсе и индивидуального подхода к каждой личности, ее развития, карьерного роста и использования по назначению. Сделаны выводы касательно необходимости дальнейшего усовершенствования существующей системы кадрового менеджмента, а также приведения структуры и численности служб (подразделений) персонала Вооруженных Сил Украины в соответствие с перспективной системой, структурой и численностью J-структуры (J-1), которая принята за основу в штабах вооруженных сил стран – членов НАТО. Описано понятие "эффективность" с научной точки зрения, в контексте исследования результативности функционирования любой системы или процессов, как главное качество любой системы, в том числе и системы управления. Осуществлен краткий обзор нескольких вариантов оценки эффективности профессиональной деятельности служб (подразделений) персонала Вооруженных Сил Украины, под чем подразумевается процесс определения эффективности деятельности работников служб (подразделений) персонала во время реализации стратегических задач Вооруженных Сил Украины с целью последовательного накопления информации, которая необходима для принятия последующих управленческих решений. Предложено направление и перспективы последующих исследований в сфере деятельности служб (подразделений) персонала.

Ключевые слова: военная кадровая политика, служба (подразделение) персонала, гибридная война, особый период, эффективность.

Ph.D. Dymenko M.P., Guliak U.M.

ESTIMATION OF EFFECTIVENESS OF THE SERVICES (UNITS) OF PERSONNEL OF THE ARMED FORCES OF UKRAINE IN THE CONDITIONS OF HYBRID WAR (SPECIAL PERIOD)

The article describes the interdependence of the effective execution of tasks by appointment of services (units) of the personnel on their structure and size. The attention is focused on the peculiarities of the tasks performed by the services (units) of personnel in the conditions of a special period. In addition, the changes that took place in the structure, size and functions of the services (units) of personnel during their transition to functioning in a special period were considered. Recommendations on the rational structure of the personnel supply system are given, aimed at optimal fulfillment of tasks related to ensuring the human resource needs of the Armed Forces of Ukraine and individual approach to each person, its development, career growth and intended use. Conclusions are made on the necessity of further improvement of the existing personnel management system, as well as bringing the structure and the number of services (units) of the personnel of the Armed Forces of Ukraine into line with the prospective system, structure and size of the "J-structure" (J-1), which is taken as a base in the headquarters of the armed forces of NATO member states. The concept of "efficiency" is described from the scientific point of view, in the context of the study of the effectiveness of the functioning of any system or processes, as the main property of any system, including the management systems. A brief overview of several options for assessing the effectiveness of the services (units) of personnel of the Armed Forces of Ukraine what is meant the process of determining the effectiveness of the services (units) of personnel during the implementation of the strategic tasks of the Armed Forces of Ukraine with the aim of consistently accumulating information that is necessary for the subsequent management decisions. The direction and prospects of further researches in the field of activity of services (units) of personnel are offered.

Keywords: military personnel policy, service (unit) of personnel, hybrid war, special period, efficiency.

ДАНІ ПРО АВТОРІВ

Адамов Юрій Іванович, старший науковий співробітник науково-дослідного відділу (проблем розвитку та застосування десантно-штурмових частин і підрозділів) наукового центру Військової академії, Одеса, , https://orcid.org/0000-0002-7355-777X.

Анісімов Анатолій Васильович, доктор фізико-математичних наук, професор, член-кореспондент НАН України, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, декан факультету комп`ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-1467-2006.

Банзак Геннадій В'ячеславович, кандидат технічних наук, доцент кафедри метрології та метрологічного забезпечення Одеської державної академії технічного регулювання та якості, https://orcid.org/0000-0003-1684-3785.

Банзак Оксана Вікторівна, доктор технічних наук, доцент, завідувач кафедри електроніки та мікросистемної техніки Одеської державної академії технічного регулювання та якості, https://orcid.org/0000-0003-6649-5013.

Боровик Олег Васильович, доктор технічних наук, професор, Заслужений працівник освіти України, заступник ректора (проректор) Національної академії Державної прикордонної служби України з навчальної роботи, https://orcid.org/0000-0003-3691-662X.

Боряк Костянтин Федорович, доктор технічних наук, доцент, завідувач кафедри метрології та метрологічного забезпечення Одеської державної академії технічного регулювання та якості, https://orcid.org/0000-0002-4226-0102.

Вдовенко Сергій Григорович, доцент кафедри зв'язку та автоматизованих систем управління Інституту інформаційних технологій Національного університету оборони України імені Івана Черняховського, https://orcid.org/0000-0003-5418-6723.

Волков Олександр Євгенович, в.о. завідувача відділу 185 Міжнародного науково-навчального центру інформаційних технологій та систем, orcid.org/0000-0002-5418-0102.

Волошенюк Дмитро Олександрович, науковий співробітник відділу 185 Міжнародного науково-навчального центру інформаційних технологій та систем, orcid.org/0000-0003-3793-7801.

Грицький Роман Володимирович, начальник циклової комісії бойових інформаційно-управляючих систем. Військова частина А 3990, м. Полтава.

Гуляк Уляна Миколаївна, офіцер відділу впровадження технологій кадрового менеджменту Кадрового центру Збройних Сил України, http://orcid.org/0000-0002-0625-7814.

Гурба Олександр Володимирович, начальник сектору відділу експлуатації, надійності і випробувань Державного підприємства "Державне київське конструкторське бюро "Луч".

Даник Юрій Григорович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, професор, начальник інституту інформаційних технологій Національного університету оборони України імені Івана Черняховського, https://orcid.org/0000-0001-6990-8656.

Джулій Володимир Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, http://orcid.org/0000-0003-1878-4301.

Думенко Микола Петрович, кандидат військових наук, перший заступник начальника Головного управління персоналу Генерального штабу Збройних Сил України, http://orcid.org/0000-0001-5633-7700.

Жиров Генадій Борисович, кандидат технічних наук, старший науковий співробітник, доцент кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0001-7648-7992.

Завальнюк Володимир Вікторович, кандидат фізико-математичних наук, доцент кафедри фундаментальних наук Військової академії, Одеса, , https://orcid.org/0000-0002-3193-9569.

Зубарєв Олександр Валерійович, кандидат технічних наук, старший науковий

співробітник, провідний науковий співробітник Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

Каблуков Олег Анатолійович, старшний науковий співробітник наукового центру Центрального науково-дослідного інституту Збройних Сил України.

Ковпа Дмитро Миколайович, магістр кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету,

Комарова Лариса Олексіїіна, доктор технічних наук, старший науковий співробітник, професор кафедри «Телекомунікації» ОНАЗ ім. О.С. Попова, Одеса, https://orcid.org/0000-0002-9776-0879.

Крижанівський Євгеній Сергійович, начальник сектору відділу експлуатації, надійності і випробувань Державного підприємства "Державне київське конструкторське бюро "Луч".

Кулік Костянтин Володимирович, старший офіцер відділу організації зв`язку та інформаційних систем управління зв`язку та інформаційних систем. Військова частина А 0796, м. Рівне.

Купельський Віктор Валерійович, ад'юнкт Національної академії Державної прикордонної служби України, https://orcid.org/0000-0002-7661-1356.

Лаптєв Олександр Анатолійович, кандидат технічних наук, старший науковий співробітник, доцент кафедри систем інформаційного та кібернетичного захисту Державний університет телекомунікацій, https://orcid.org/0000-0002-4194-402X.

Лещенко Олег Іванович, кандидат технічних наук, доцент, доцент кафедри електроніки та мікросистемні техніки Одеської державної академії техничного регулюівання та якості, https://orcid.org/0000-0001-8589-8596.

Лєнков Євген Сергійович, кандидат технічних наук, старший науковий співробітник наукового центру Центрального науково-дослідного інституту Збройних Сил України, http://orcid.org/0000-0001-5819-2656.

Лєнков Сергій Васильович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0001-7689-239X.

Литвиненко Наталія Ігорівна, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідної лабораторії науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-2203-2746.

Ліндер Ярослав Миколайович, кандидат фізико-математичних наук, асистент кафедри інформаційних систем факультету комп`ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0003-1076-9211.

Лісовський Олександр Сергійович, магістр кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, https://orcid.org/0000-0002-6021-5358 .

Маслов Олег Вікторович, доктор технічних наук, доцент, завідувач кафедри Фізики Одеського національного політехнічного університету, https://orcid.org/0000-0002-0288-0289.

Мокрицький Вадим Анатолійович, доктор технічних наук, професор, професор кафедри Інформційних технологій проектування в електроніці та телекомунікаціях Одеського національного політехнічного університету, https://orcid.org/0000-0002-2514-4137.

Муляр Ігор Володимирович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем та мереж Хмельницького національного університету, http://orcid.org/0000-0002-6659-605X.

Мясіщев Олександр Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, https://orcid.org/0000-0003-1269-425X.

Охрамович Михайло Миколайович, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного відділу науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-

0002-8776-3937.

Проценко Ярослав Миколайович, кандидат технічних наук, начальник науково-організаційного відділу Військового інституту Київського національного університету імені Тараса Шевченка.

Ряба Людмила Олександрівна, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-7436-4443.

Саланда Іванна Петрівна, кандидат технічних наук, доцент кафедри теорії і методики трудового навчання та технологій Кременецької обласної гуманітарно-педагогічної академії ім. Тараса Шевченка.

Сачук Юрій Володимирович, кандидат фізико-математичних наук, старший викладач кафедри національної безпеки Східноєвропейського національного університету ім. Лесі Українки.

Селюков Олександр Васильович, доктор технічних наук, старший науковий співробітник, заступник директора ТОВ «Укрспецконсалтинг», https://orcid.org/0000-0001-7979-3434.

Собчук Валентин Володимирович, кандидат фізико-математичних наук, доцент, доцент кафедри диференціальних рівнянь і математичної фізики, факультету інформаційних систем, фізики та математики Східноєвропейський національний університет ім. Лесі Українки, https://orcid.org/0000-0002-4002-8206.

Солодєєва Людмила Василівна, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-7979-8443.

Тарануха Володимир Юрійович, кандидат фізико-математичних наук, асистент кафедри математичної інформатики факультету комп`ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-9888-4144.

Ткач Артем Олександрович, магістр кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, https://orcid.org/0000-0002-4438-2923 .

Толок Ігор Вікторович, кандидат педагогічних наук, доцент, Заслужений працівник освіти України, начальник Військового інституту, Київський національний університет імені Тараса Шевченка, http://orcid.org/0000-0001-6309-9608.

Федченко О.П., кандидат військових наук, старший науковий співробітник, старший науковий співробітник науково-дослідної лабораторії науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-2203-2746.

Хмельницький Юрій Владиславович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету. https://orcid.org/0000-0002-4005-5669 .

Шишанов Михайло Олексійович, доктор технічних наук, професор, провідний науковий співробітник Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

АЛФАВІТНИЙ ПОКАЗЧИК

Наукове видання

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

Київського національного університету імені Тараса Шевченка

№ 64

Усі матеріали надруковані в авторській редакції.
Деякі статті не рецензуються, у зв'язку з пріоритетною кваліфікацією авторів або через сумніви редколегії у змісті.

Підписано до друку 14.06.19 р.
Авт. друк. Арк. 18. Формат 60х90/8
Безкоштовно. Замовлення № 10-2012

Надруковано у навчальному картографічному комплексі ВІКНУ

03189, Київ, вул. Ломоносова 81

т. 521-32-89