МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ ІМЕНІ ГЕРОЇВ КРУТ

ВІСНИК ВІТІ

КОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

ВИПУСК № 1 (3)

Київ – 2022

ББК
Ц4 (4Укр) 39
З – 415

Вісник Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Комунікаційні та інформаційні системи. Київ: ВІТІ, 2022. № 1 (3). 102 с.

РЕДАКЦІЙНА КОЛЕГІЯ

Всі наукові статті, викладені у збірнику, прорецензовані фахівцями з відповідних галузей та отримали позитивний відгук.

Збірник затверджено на засіданні Вченої ради інституту (протокол № 1 від 27.09.2022 року).

З М І С Т

Баканов В. С., Хусаінов П. В., Марчук О. В.
Постановка задачі вибору SIEM-системи на основі методу експертних оцінок 4

Зінченко М. О., Лазута Р. Р., Яковчук О. В., Макарчук В. І.
Аналіз підходів провідних країн світу до ведення кібервійн та кібероперацій 10

Карпенко А. О., Мусієнко В. А., Шугалій О. О., Пономаренко З. М.
Аналіз інструментів збору розвідувальної інформації з відкритих джерел 18

Куцаєв В. В., Головко О. Є., Лазута Р. Г.
Перспективи використання квантових технологій 26

Кузавков В. В., Михайлюк С. С., Погребняк С. В.
Аналіз параметрів надійності об'єктів радіоелектронної техніки з надлишковістю 41

Лазута Р. Р., Зінченко М. О., Яковчук О. В., Шкіцький Д. В.
Пропозиції з організації космічної підтримки Збройних сил України
за стандартами НАТО 48

Радченко М. М., Драглюк О. В., Дикий О. В., Коротков М. М., Павлюк Д. О.
Застосування технологій Virtual Desktop Infrastructure
в інформаційних інфраструктурах учасників сектору безпеки та оборони 60

Сінько В. В.
Аналіз факторів, які впливають на надійність програмного забезпечення
телекомунікаційного обладнання мережі військового зв'язку 73

Шаповал В. М., Радзівілов Г. Д., Османов Р. Н., Сердюк П. Є.
Підвищення рівня захищеності броньованого автомобіля «БАРС-8»
локальним бронюванням 78

Штаненко С. С., Краснобокий А.В.
Підвищення кіберстійкості АСУ технологічними процесами шляхом впровадження інтелектуальних систем кібербезпеки 83

Яровий В. С.
Діагностування та усунення несправностей перемикання
режимів живлення вторинного джерела електроживлення 90

Автори номера 99

Пам'ятка автору 101

УДК 681.35

Баканов В. С. (ВІТІ ім. Героїв Крут)
Хусаінов П. В. (ВІТІ ім. Героїв Крут)
Марчук О. В. (ВІТІ ім. Героїв Крут)

ПОСТАНОВКА ЗАДАЧІ ВИБОРУ SIEM-СИСТЕМИ НА ОСНОВІ МЕТОДУ ЕКСПЕРТНИХ ОЦІНОК

Забезпечення оперативного (кризового) реагування на кіберінциденти в умовах обмеженого часу обумовлює необхідність моніторингу інформаційних систем, здійснення аналізу подій безпеки, що відбуваються на робочих станціях, мережевих пристроях, засобах захисту інформації та інших елементах IT-інфраструктури в режимі реального часу з метою пошуку аномалій, що лишаються непомітними для спеціалізованих засобів захисту, та вимагає пошуку технічних рішень автоматизованого збору, агрегації та обробки даних.

Сучасні SIEM-системи за своїми функціональними можливостями можуть забезпечити або значно спростити виконання вище вказаних завдань. Велика кількість наявних рішень породжує проблему вибору, для вирішення якої потрібен час та експертиза.

Вибір універсального рішення, яке було б оптимальним для будь-якої IT-інфраструктури, не можливий. Аналіз наукових праць та літератури показує, що задача вибору SIEM-системи може бути вирішена шляхом визначення відповідності заданим критеріям (багатокритеріальної оцінки).

Задача багатокритеріальної оцінки на основі якісних показників системи може бути вирішена методом експертних оцінок. Використання спеціалістів як експертів надає ряд переваг. Експерт, який володіє достатньою кількістю інформації, досвідом, знанням суті питання, здатний ефективно вирішувати задачі в області його професіональної діяльності. Інформація, отримана від експертів, у подальшому може оброблюватись за допомогою спеціальних логічних та математичних прийомів і процедур з метою перетворення її в формулу, зручну для вибору кращого рішення.

Ключові слова: *SIEM-система, експертна оцінка, багатокритеріальна оцінка.*

V. Bakanov, P. Khusainov, O. Marchuk Statement of the problem of choosing of SIEM-system on the basis of the method of expert assessments.

Ensuring rapid (crisis) response to cyber incidents in a limited time requires monitoring of information systems, analysis of security events occurring on workstations, network devices, information security tools and other elements of the IT-infrastructure in real time in order to find anomalies that remain invisible to specialized appliance and requires the search for technical solutions for automated data collection, aggregation and processing.

Modern SIEM-systems by their functionality can provide or significantly simplify the mentioned tasks. The large number of available solutions creates the problem of choosing a system that requires time and expertise.

It is not possible to choose a universal solution that would be optimal for any IT infrastructure. Analysis of scientific research shows that the problem of choosing a SIEM-system can be solved by determining compliance with the specified criteria (multi criteria evaluation).

The problem of multicriteria evaluation based on qualitative indicators of the system can be solved by the method of expert evaluations. There are a number of advantages to using specialists as experts. An expert who has sufficient information, experience, knowledge of the essence of the issue is able to effectively solve problems in the area of his professional activity. The information obtained from the experts can be further processed using special logical and mathematical techniques and procedures in order to turn it into a formula that is convenient for choosing the best solution.

Keywords: *SIEM-system, expert assessment, multicriteria assessment.*

Постановка завдання у загальному вигляді

Зміна ландшафту загроз у бік складних багатовекторних атак та ускладнення комплексу засобів захисту ведуть до швидкого зростання популярності систем класу SIEM (англ. *Security Information and Event Management*).

Під поняттям SIEM-система розглядається сукупність технічних, програмних та математичних засобів виявлення кібератак (кіберінцидентів).

Такі рішення (SIEM-системи) дозволяють здійснювати моніторинг інформаційних систем, аналізувати події безпеки в режимі реального часу, наприклад, що відбуваються на робочих станціях, мережевих пристроях, засобах захисту інформації та інших елементах

ІТ-інфраструктури. Зібрані та проаналізовані ними дані допомагають виявляти інциденти кібербезпеки або аномалії, що залишилися непомітними для спеціалізованих засобів захисту.

Практично щодня публікуються факти про успішні кібератаки (у тому числі цілеспрямовані за спонсорством окремих держав). Вище вказане, зі свого боку, веде до необхідності автоматизованого і ретельного аналізу подій, передбачення кібератак, їх розвитку або хоча б вміння локалізувати проблему з меншими втратами. Сучасні SIEM-системи за своїми функціональними можливостями можуть забезпечити виконання вище вказаних завдань.

Попит формує пропозиції. Велика кількість рішень вендорів породжує проблему вибору, для вирішення якої потрібен час та експертиза. На жаль, у публічному просторі практично немає методологій порівняння, які б допомагали потенційним замовникам обрати оптимальну для себе SIEM-систему.

Вибір універсального рішення, яке було б оптимальним для будь-якої ІТ-інфраструктури, не можливий. Існує декілька шляхів вирішення задачі вибору SIEM-системи. Проаналізувавши наукові праці та кращі світові практики, вважаємо, що задачу вибору SIEM-системи доцільно вирішувати шляхом визначення відповідності заданим критеріям (багатокритеріальної оцінки).

Зважаючи на викладене, *метою статті* є постановка завдання щодо обґрунтування раціонального вибору SIEM-системи. Для вирішення поставленої задачі пропонується використання методу експертних оцінок.

Аналіз останніх публікацій за темою дослідження

Аналіз джерел із даної проблематики показує, що значна кількість задач, у тому числі і багатокритеріальної оцінки на основі якісних показників, вирішується на основі методів експертних оцінок. Це пов’язано з тим, що є необхідність враховувати як якісні, так і людські фактори, які завжди фігурують в задачах застосування автоматизованих систем під управлінням оператора [1].

Методи експертних оцінок – це методи організації роботи зі спеціалістами-експертами й обробки їхніх рішень, виражених в кількісній або якісній формі. Використання експертних методів допомагає формалізувати процедури збору, узагальнення і аналізу пропозицій спеціалістів з метою перетворення їх в форму, найбільш зручну для прийняття обґрунтованого рішення [1].

Можливість використання спеціалістів як експертів надає ряд переваг. Мислення спеціаліста опирається на інтуїцію, на підсвідому діяльність, набуті як досвід під час довготривалої практичної діяльності. Існує гіпотеза, що для набуття досвіду до рівня експерта необхідно щонайменше 10 років практичної діяльності в заданій області. Досвід, що базується на накопичених знаннях, допомагає спеціалісту вирішувати складні, комплексні завдання. На практиці не рідко буває, що вирішення складних задач вимагає настільки трудомістких розрахунків, що це призводить до значних затрат засобів та часу. Водночас прості методи, які базуються на певному переліку правил і здоровому глузді, можуть забезпечити вирішення таких задач у короткі строки з достатньою точністю.

Отже, експерт, який володіє достатньою кількістю інформації, досвідом, знанням суті питання, здатний ефективно вирішувати задачі в області його професіональної діяльності.

На нашу думку для вирішення поставленої задачі вибору SIEM-системи можливо використати метод багатокритеріальної оцінки на основі експертного рішення. При цьому інформація, отримана від експертів, в подальшому може оброблюватись за допомогою спеціальних логічних та математичних прийомів і процедур з метою перетворення її в формулу, зручну для вибору кращого рішення.

Виклад основного матеріалу

Для рішення задачі вибору SIEM-системи пропонується визначити перелік якісних показників, за допомогою методу експертних оцінок визначити їхні коефіцієнти важливості (ранжирування) та обрати метод рішення багатокритеріальної задачі.

Припустимо, що $\overline{X}$ – це вектор параметрів SIEM-системи *S* (1).

$$\overline{X} = |x_1, \dots, x_i, \dots, x_n|. \quad (1)$$

Деяка *j*-а властивість SIEM-системи *S* характеризується величиною *j*-го показника (2):

$$q_i = (\bar{X}); j = \overline{1,m}. \quad (2)$$

Тоді SIEM-система в цілому характеризується вектором показників $\bar{Q}$ (3):

$$\bar{Q} = |q_1, \dots, q_j, \dots, q_m|. \quad (3)$$

Задача багатокритеріального вибору зводиться до того, щоб з множини M_s варіантів SIEM-систем вибрати такий варіант S_0, який має найкраще значення вектора $\bar{Q}$. При цьому припускається, що поняття «найкраще значення вектора $\bar{Q}$» попередньо сформовано математично на основі критерію(їв) відповідності.

Пропонуємо такі етапи рішення поставленої задачі.

1 етап. Визначення якісних показників SIEM-системи.

Показник – це якісна або кількісна характеристика для оцінки окремої властивості чи сукупності властивостей об’єкта (процесу), що розглядається [1].

Пропонуються наступні показники:

прогнозована ефективність (X_1) – здатність SIEM-системи до обробки та кореляції подій за заданими критеріями та політиками, встановленими в системі;

наочність інформаційної моделі (X_2) – достатня кількість організованої за певними правилами сукупності інформації про стан функціонування об’єкта управління (кіберзахисту), зовнішнього середовища та їхніх найбільш суттєвих властивостей, на основі яких людина-оператор SIEM-системи аналізує поточну ситуацію, планує та обирає управляючий вплив, а також оцінює його результати;

продуктивність (X_3) – час, який прогнозується на обробку, кореляцію подій та оповіщення людини-оператора SIEM-системи для роботи з інцидентами кібербезпеки;

здатність до навчання (X_4) – можливість SIEM-системи в автоматизованому режимі накопичувати знання в процесі роботи та можливість враховувати нові типи кіберзагроз;

можливість експорту (імпорту) знань (X_5) – здатність бази знань SIEM-системи до модернізації в процесі еволюції експертної системи (підтримка обміну даними про загрози кібербезпеки за стандартами MISP, STIX, MAEC, IODEF, OpenIOC (Cybox), CAPEC, VERIS);

масштабованість (X_6) – можливість нарощування бази знань SIEM-системи або об’єднання декількох баз знань SIEM-систем різних рівнів в єдину ієрархічну систему.

2 етап. Визначення коефіцієнтів важливості якісних показників SIEM-системи або їх ранжирування.

Детальний огляд методів визначення коефіцієнтів важливості наведено в [2]. У сучасній математичній теорії вимірювання виділяють два види вимірювань: в первинних шкалах (найменувань, порядку, інтервалів та ін.) і в похідних шкалах (функцій корисності і частот уподобань). Серед первинних та похідних вимірювань виділяються два підкласи типів вимірювань.

Перший клас – первинні вимірювання: попарні порівняння; точкові оцінки на шкалі. *Другий клас* – похідні вимірювання: функції цінності, частоти уподобань.

Ієрархічна класифікація методів визначення коефіцієнтів важливості відповідно до вищевикладеного підходу приведена в [2].

Для визначення коефіцієнтів важливості пропонується провести експертну оцінку, при цьому рівень компетентності експертів визначити попередньо. Із відомих методів експертних оцінок, на нашу думку, прийнятним може бути метод попарного порівняння Сааті [2].

3 етап. Оброблення результатів експертного опитування.

Успішне проведення експертної оцінки в багатьох випадках залежить від правильної організації опитування експертів. При проведенні опитування необхідно забезпечити однозначність розуміння експертами окремих питань, формування яких може викликати різне тлумачення. Результатом даного етапу є заповнення листа опитування, за допомогою якого і відбувається збір необхідної інформації.

Експертне опитування включає в себе: аналіз індивідуальних експертних висновків, аналіз сукупності зібраних висновків та агрегацію експертних висновків [1].

4 етап. Вибір методу рішення багатокритеріальної задачі вибору SIEM-системи на основі результатів експертної оцінки.

Аналіз літератури показує, що всі численні методи рішення багатокритеріальних задач можна звести до трьох груп: метод головного показника, метод результуючого показника, лексикографічний метод.

Метод головного показника базується на переводі всіх показників якості, крім будь-якого одного, який називається головним, в розряд обмежень типу рівність і нерівність. Головному показнику присвоюється номер $q_1(S)$. У такому разі задача зводиться до однокритеріальної задачі вибору системи $S\epsilon M_s$, що має мінімальне значення показника $q_1(S)$ при наявності обмежень типу рівність і нерівність, тобто має вигляд (4) при обмеженнях (5):

$$\min_{S\epsilon M_s} q_1(S); \tag{4}$$

$$\begin{gathered} q_j(S) = q_{j0}; j = 2, \dots, l; \\ q_k(S) \le q_{k0}; k = l+1, \dots, p; \\ q_r(S) \ge q_{r0}; r = p+1, \dots, m. \end{gathered} \tag{5}$$

Метод результуючого показника базується на формуванні загального показника шляхом інтуїтивних оцінок впливу показників якості $q_1, \dots, q_m$ на результуючу якість виконання системою її функцій. Оцінки такого впливу даються групою спеціалістів, експертів, що мають досвід використання (розробки) таких систем.

Найбільшого застосування серед результуючих показників якості набули адитивний, мультиплікативний та максимінний показники.

Адитивний показник якості являє собою суму зважених нормованих показників та має вигляд (6):

$$Q = \sum_{j=1}^{m} w_j \bar{q}_j, \tag{6}$$

де $\bar{q}_j$ – нормоване значення j-го показника;

w_j – ваговий коефіцієнт j-го показника, величина якого тим більша, чим більше він впливає на якість системи (7).

$$\sum_{j=1}^{m} w_j = 1;\ w_j > 0; j = \overline{1, m}. \tag{7}$$

Мультиплікативний показник формується шляхом перемноження показників з урахуванням їхніх вагових коефіцієнтів та має вигляд (8):

$$Q = \prod_{j=1}^{m} \bar{q}_j^{\ w_j}, \tag{8}$$

де $\bar{q}_j$ та w_j мають один і той же сенс, що і в адитивному показнику.

Найбільш суттєва різниця між мультиплікативним та адитивним показником полягає в тому, що адитивний показник базується на принципі справедливої абсолютної поступки за окремими показниками, а мультиплікативний – на принципі справедливої відносної поступки. Суть мультиплікативного показника полягає в тому, що справедливим вважається такий компроміс, коли сумарний рівень відносного погіршення одного або декількох показників не перевищує сумарного рівня відносного покращення решти показників.

Максимінний показник. У ряді випадків вид результуючої цільової функції достатньо важко обґрунтувати або застосувати. У таких випадках можливим простим шляхом рішення

задачі є застосування максимінного показника. Правило вибору оптимальної системи S_0 в цьому випадку має вигляд (9), якщо вагові коефіцієнти показників відсутні, або (10), якщо вагові коефіцієнти визначені.

$$\max_{S \in M_s} \quad \min_{1 \le j \le m} \quad \left\{\overline{q_1}(S), \dots, \overline{q_j}(S), \dots, \overline{q_m}(S)\right\}, \tag{9}$$

$$\max_{S \in M_s} \quad \min_{1 \le j \le m} \quad \left\{\overline{q_1} \quad {}^{w_1}(S), \dots, \overline{q_j} \quad {}^{w_j}(S), \dots, \overline{q_m} \quad {}^{w_m}(S)\right\}. \tag{10}$$

Максимальний показник забезпечує найкраще (найбільше) значення найгіршого (найменшого) із показників якості.

Лексикографічний метод. Припустимо, що показники упорядковані за важливістю (11).

$$q_1(S) > q_2(S) > \dots > q_m(S). \tag{11}$$

Суть методу полягає у визначенні множини альтернатив з найкращою оцінкою по найбільш вагомому показнику. Якщо така альтернатива одна, то вона вважається найкращою. Якщо альтернатив декілька, то із їх множини виділяються ті, які мають кращу оцінку по другому показнику і т. ін.

Принциповою особливістю задачі вибору рішення, що розглядається в статті, є переважно якісний характер критеріїв. У зв'язку з цим методи багатокритеріальної оцінки, що розглядаються, повинні сформулюватися в нечіткій постановці. В такому випадку критерії якості являють собою функції приналежності варіантів рішення заданому рівню якості.

Вибір методу рішення багатокритеріальної задачі визначається тим, у якому вигляді представлена експертна інформація про важливість показників. В таблиці 1 показано залежність вибору методу рішення багатокритеріальної задачі залежно від експертної інформації.

Таблиця 1

Вибір методу рішення багатокритеріальної задачі

Експертна інформація про важливість показників	Метод рішення багатокритеріальної задачі
Відсутня	Максимінний показник
Показники впорядковані по важливості	Лексикографічний метод
Визначені вагові коефіцієнти показників	1. Адитивний показник. 2. Мультиплікативний показник. 3. Максимінний показник

Висновки

Задача раціонального вибору SIEM-системи є комплексною та містить визначення вихідних умов: середовище функціонування, об'єми даних, які підлягають аналізу, вимоги до швидкості обробки даних, вимоги до інформаційної моделі системи, рівень навченості людини-оператора та ін. Відповідно до вихідних умов можуть бути сформовані кількісні та якісні показники системи, що задовольняють завчасно визначеним критеріям, які отримані шляхом експертних оцінок.

Задачу багатокритеріального вибору пропонується вирішувати шляхом обрання з множини варіантів прийнятного (кращого) на основі попередньо сформованих критеріїв відповідності, що формуються з використанням методу експертних оцінок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Самохвалов Ю. Я., Науменко Е. М. Экспертное оценивание. Методический аспект. Киев, 2007. 262 с.

2. Герасимов Б. М., Дивизинюк М. М., Субач И. Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. Севастополь: СНИЯЭиП, 2004. 319 с.

3. S. Toliupa, P. Khusainov, V. Bakanov, S. Shtanenko. Substantial formulation of the task of improving the information model of decision-making in the prompt (crisis) response to cyber incidents // International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). 2022. № 16. С. 281–286.

4. Искусственный интеллект. правочник: в 3-х кн. / Под ред. Д. А. Поспелова. Москва: Радио и связь, 1990. Кн. 2. Модели и методы. 304 с.

5. Толковый словарь по искусственному интеллекту / Авторы-составители А. Н. Аверкин, М. Г. Гаазе-Рапопорт, Д. А. Поспелов. Москва: Радио и связь, 1992. 256 с.

6. Орлов А. І. Теорія прийняття рішень. Москва: Видавництво «Март», 2004. 656 с.

УДК 341:004

Зінченко М. О. (ВІТІ ім. Героїв Крут)
Лазута Р. Р. (ВІТІ ім. Героїв Крут)
Яковчук О. В. (ВІТІ ім. Героїв Крут)
Макарчук В. І. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ПІДХОДІВ ПРОВІДНИХ КРАЇН СВІТУ ДО ВЕДЕННЯ КІБЕРВІЙН ТА КІБЕРОПЕРАЦІЙ

У статті розглянуті аналізи підходів провідних країн світу та країн-членів НАТО до ведення кібервійн та кібероперацій та застосування, впровадження і заміна цих підходів у нашій державі в цілому.

У війнах і збройних конфліктах минулого століття, у класичному їх розумінні, з «нематеріальних» технологій протиборства застосовувалися, як відомо, переважно лише методи інформаційно-психологічної боротьби як механізм впливу на свідомість людини, а також дезінформації населення і Збройних сил супротивника.

Саме такий стан справ, по-перше, обумовив нові завдання для Збройних сил і компетентних державних правоохоронних органів провідних країн світу, які мають спрямовуватися на забезпечення протидії або на повну нейтралізацію різного роду кіберзагроз; по-друге, підняв на беззаперечно вищий щабель вагу досліджень, спрямованих на розроблення методології кібервоєн та прогнозування довгострокових тенденцій їхнього розвитку, вироблення актуальних моделей проведення атакуючих дій у кіберпросторі, а також створення систем ефективної протидії останнім.

Тобто, як бачимо, тема кібервійни останнім часом доволі активно досліджується представниками більшості провідних країн світу. Увагу цьому питанню приділяють також і військові блоки. Так, у керівних документах НАТО та країн-членів НАТО кібервійна розглядається в одному ряду з протиракетною обороною та боротьбою з тероризмом.

Під кібероперацією, за аналогією з методами звичайної війни, розуміють сукупність узгоджених за часом, глибиною та завданнями відносно короткочасних кібератак, спрямованих на один або декілька об'єктів впливу протиборчої сторони з наміром одержання незаконного доступу до їх інформаційних ресурсів, порушення роботи їхніх інформаційних систем або взагалі повного виведення обраних об'єктів з функціонування.

Тобто, якщо взяти до уваги головні характеристики майбутніх кібервоєн, а саме: можливість здійснення нападу будь-ким; географічну досяжність; невідворотність; потенціал і легкість поширення, а також вплив на «електронно готові» цілі, – можна припустити, що їхній початок може стати революцією у військовій справі, а їх результати взагалі можуть виявитися непередбачуваними.

Отже, пропонується змінити прийняті в нашій державі підходи до визначень та термінологічних взаємозв'язків між кіберопераціями та кібердіями, розробити та впровадити відповідні документи та закупити новітні засоби зв'язку для розвитку новітніх ІТ-технологій країни.

Ключові слова: *НАТО, кібервійна, кібероперація, кіберзагроза.*

M. Zinchenko, R. Lazuta, O. Yakovchuk, V. Makarchuk Of approaches of leading countries of the world to cyberwins and cyberoperations.

The article examines the approaches of the world's leading countries and NATO member states to the conduct of cyber wars and cyber operations and the application, implementation and replacement of these approaches in our country as a whole.

In the wars and armed conflicts of the last century, in their classical sense, with «intangible» technologies of confrontation were used, as is known, mainly only methods of information and psychological struggle as a mechanism to influence human consciousness and misinformation of the population and armed forces.

It is this state of affairs that has, firstly, set new challenges for the Armed Forces and the competent state law enforcement agencies of the world's leading countries, which must be aimed at ensuring the counteraction or complete neutralization of various types of cyber threats; secondly, it raised to an unequivocally higher level the weight of research aimed at developing cyber warfare methodologies and forecasting long-term trends in their development, developing current models of attacking actions in cyberspace, and creating systems to effectively counter the latter.

That is, as we see, the topic of cyber warfare has recently been quite actively studied by representatives of most leading countries in the world. Military blocs are also paying attention to this issue. Thus, in the guiding documents of NATO and NATO member countries, cyber warfare is considered on a par with missile defense and the fight against terrorism.

Under cyber operation, by analogy with the methods of conventional warfare, is a set of agreed on time, depth and objectives for short-term cyberattacks aimed at one or more objects of influence of the opposing side with the

intention of gaining illegal access to their information resources, disruption of their information systems or complete withdrawal of selected objects from operation.

That is, given the main characteristics of future cyber wars, namely: the possibility of an attack by someone; geographical reach; inevitability; the potential and ease of dissemination, as well as the impact on «electronically prepared» targets, suggest that their onset may be a military revolution, and their results may be unpredictable.

Thus, it is proposed to change the approaches adopted in our country to the definition and terminological relationships between cyber operations and cyberdia, to develop and implement relevant documents and purchase the latest communications for the development of the latest IT technologies in the country.

Keywords: *NATO, cyber war, cyber operation, cyber threat.*

Постановка завдання

Більшість аспектів військових операцій Збройних сил України частково покладаються на використання кіберпростору, який в нашому сьогоденні є водночас як невід'ємною сферою інформаційного середовища, так і тією субстанцією, яка, з аналогію будь-якого визначення «системи», є одночасно й елементом цієї системи та тією прихованою «силою» («відношенням»), що зумовлює взаємодію елементів інформаційного середовища між собою.

Якщо розглянути підходи до визначення «кіберпростір», наведені в керівних документах більшості країн-членів НАТО, зокрема США, кіберпростір являє собою (в буквальному перекладі різних організацій): «Глобальний домен в інформаційному середовищі, що складається із взаємозалежних мереж інфраструктур інформаційних технологій та даних резидентів, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори і контролери» (документи JP 3-12 та FM 3-12).

Виходячи із викладеного, стає зрозумілим численне обговорення тем, пов'язаних з кіберпростором та так званими «кібердіями» (визначення яких відсутнє на загальнодержавному рівні, і навіть якщо з'явиться, то буде періодично змінюватись). Але все ж таки, у зв'язку із їх «віртуальною» наявністю, ця робота спрямована саме на їх розгляд та удосконалення в інтересах нашої держави.

Розвиток інформаційного суспільства дозволяє використовувати кіберпростір для вирішення політичних, соціокультурних та воєнних завдань (прості приклади: Крим, Донбас), можливості прихованого впливу на підсвідомість людей і масштабного маніпулювання суспільною думкою за рахунок використання інформаційних технологій та засобів масових комунікацій, не кажучи вже при цьому про ще ряд аспектів, пов'язаних, наприклад, з дистанційним ураженням як військових, так і цивільних об'єктів, особливо в мирний час. Це постійно призводить до появи нових форм і методів кібердій, завдяки яким провідні держави намагаються досягти своїх зовнішньополітичних цілей і владнати міждержавні розбіжності.

У сучасному світі зазначене відбувається через використання (звичайно приховано) кібердій у кіберпросторі, форми і способи яких постійно удосконалюють спеціальні (визначені) підрозділи провідних країн світу.

У цих умовах підрозділи кібербезпеки Збройних сил України повинні постійно вживати зусилля для удосконалення форм і способів кібердій в рамках готовності до кібероборони держави.

Аналіз останніх досліджень і публікацій

Розвиток подій на міжнародній арені наприкінці XX – на початку XXI століття свідчить, що, попри потужні зусилля світової спільноти з урегулювання міждержавних суперечностей мирним шляхом, кількість і гострота збройних конфліктів сучасності практично не зменшуються. Більше того, нині вони охоплюють не тільки традиційні сфери збройної боротьби (землю, море, повітря), а й поступово просуваються в новітні сфери, наприклад, у віртуальний комп'ютерний світ, який практично є основою життя сучасної людини.

У війнах і збройних конфліктах минулого століття, у класичному їх розумінні, з «нематеріальних» технологій протиборства застосовувалися, як відомо [1], переважно лише методи інформаційно-психологічної боротьби як механізм впливу на свідомість людини, а також дезінформації населення і Збройних сил супротивника. При цьому обладнання зв'язку та засоби масової інформації розглядалися тоді переважно як середовище для перенесення думки, потрібної передусім атакуючій стороні.

З появою феномена глобальних комп'ютерних мереж з'явився так званий новий театр воєнних дій – кіберпростір, де поступово почали:

використовуватися принципово нові, специфічні засоби й методи ураження – інформаційна і кіберзброя, та формуватися тактика і стратегія їх застосування;

розгортатися угруповання сил і спеціальних програмно-апаратних засобів для проведення активних операцій (дій);

розвиватися засоби й методи захисту тощо.

На думку колишнього заступника міністра оборони США Елвіна Бернштейна, кібервійну в нинішніх умовах можна розглядати як складову загального театру воєнних дій, «як технологічний крок уперед у розвитку сучасних засобів і методів ведення війни та завдання ударів по системах командування і контролю противника». При цьому «комп'ютеризація даної сфери» та поява «нових засобів зв'язку й комунікацій», у розумінні екзаміністра, неминуче зробить саме такі засоби «об'єктами військового нападу». Американський журнал «The Economist», крім того, описує кібервійну як «п'яту область війни, – після землі, моря, повітря й космосу» [3]. Інший американський експерт з безпеки Річард А. Кларк у своїй книзі «Cyber War» (перша редакція якої вийшла у травні 2010 р.) визначає кібервійну як «дії однієї національної держави з проникнення в комп'ютерні мережі іншої національної держави для досягнення цілей щодо завдання збитку або руйнування» [4]. Державний секретар США Гіларі Клінтон, представляючи у травні 2011 р. «Національну стратегію в кіберпросторі», зробила заяву про можливість відповіді держави на будь-які прояви кіберагресії збройними засобами, якщо інші способи виявилися неефективними. Український вчений О. О. Мережко вважає кібервійну сукупністю заходів з «використанням Інтернету і пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці, а також суверенітету іншої держави» [5].

Метою статті є аналіз підходів провідних країн світу до ведення кібервійн та кібероперацій, застосування, впровадження і заміна цих підходів в нашій державі в цілому.

Виклад основного матеріалу

Досвід війн і воєнних конфліктів підтверджує, що успіх ведення бойових дій, поряд з іншими факторами, буде у тієї сторони, яка більш оперативно приймає рішення та своєчасно організовує їх виконання. Більш-менш чітке тлумачення поняття кіберпростір вперше було надано в директиві президента США «Національна стратегія гарантування безпеки кіберпростору США» (NSPD 54, 2004), кіберпростір визначений як взаємозалежна мережа комп'ютерних технологій, на яку спираються ведення бізнесу, дії уряду, керівництво національною обороною тощо [2].

Саме такий стан справ, по-перше, обумовив нові завдання для Збройних сил і компетентних державних правоохоронних органів провідних країн світу, які мають спрямовуватися на забезпечення протидії або на повну нейтралізацію різного роду кіберзагроз; по-друге, підняв на беззаперечно вищий щабель вагу досліджень, спрямованих на розроблення методології кібервоєн та прогнозування довгострокових тенденцій їхнього розвитку, вироблення актуальних моделей проведення атакуючих дій у кіберпросторі, а також створення систем ефективної протидії останнім.

Тобто, як бачимо, тема кібервійни останнім часом доволі активно досліджується представниками більшості провідних країн світу. Увагу цьому питанню приділяють також і

військові блоки. Так, у керівних документах НАТО кібервійна розглядається в одному ряду з протиракетною обороною та боротьбою з тероризмом.

НАТО сьогодні має три лінії кібероборони (а саме: службу NATO Computer Incidents Response Capabilities Centre; Гаазький дослідницький центр перевірки діючих систем і вироблення новітніх стандартів захисту та Програму розробки захищених систем зв'язку) з метою підвищення ефективності ведення воєнних дій саме в кіберпросторі та додатково розробляє:

спеціальну структуру для захисту країн-членів Альянсу від кібератак, яка займатиметься збиранням розвідувальних даних і координуватиме дії членів НАТО в боротьбі з кіберзлочинністю;

концепцію майбутніх кібервійн, в основу якої покладено насамперед військово-технічну концепцію C4I (Command, Control, Computer, Communications and Intelligence) та C4IFTW (Command, Control, Computer, Communications and Intelligence for the Warrior), а також доктрину кіберманевру, що передбачає поділ усього театру воєнних дій на дві складові – традиційний та кіберпростори (ідея запропонована ще у 1996 р. експертом Пентагону Р. Банкером).

Отож, у світі вже передбачається проведення як оборонних (захист власних ІТ-систем від деструктивного впливу), так і наступальних дій (встановлення контролю над ІТ-системами супротивника або взагалі їх знищення). При цьому основною формою таких дій, з урахуванням пропозицій [6], на тактичному рівні слід вважати кібератаки, на стратегічному та спеціальному рівнях – кібероперації, основні методи яких наведено в таблиці 1.

Таблиця 1

Основні методики кібератак, тактичних, стратегічних та спеціальних кібероперацій

Рівень операцій	**Основні методики проведення**
Тактичний	Ускладнення чи вибіркове зупинення діяльності телекомпаній, операторів стільникового зв'язку, провайдерів Інтернет, відомчих локальних обчислювальних мереж тощо. Тимчасове призупинення, дезорганізація чи ускладнення діяльності систем управління транспортом, енерго- й газопостачанням тощо. Вибіркове призупинення та порушення діяльності систем управління об'єктами критичної інфраструктури, включно з банківською сферою, підприємствами атомної, хімічної, нафтопереробної промисловості тощо
Стратегічний	Розкриття таємних кодів і шифрів, перехоплення й розшифрування листування високопосадовців. Неправомірний доступ до державних баз даних, у яких зберігається інформація з обмеженим доступом, крадіжка, редагування або знищення інформації в базах даних органів державного управління. Завдання програмної або апаратної шкоди інформаційним системам на атомних електростанціях, підприємствах хімічної, нафто- і газопереробної сфери тощо. Знищення, редагування баз даних операторів стільникового зв'язку, провайдерів Інтернет, відомчих комп'ютерних мереж, систем централізованого управління енерго- і газопостачанням, зв'язком тощо
Спеціальний	Несанкціонований доступ до систем управління стратегічною зброєю та імітація примусового запуску окремих елементів ракетної чи іншої зброї. Блокування систем управління військами, передача у війська хибних наказів і директив. Дезорганізація космічного угруповання супротивника, ураження систем управління й орієнтації супутників різного призначення, переведення їх на нестабільні орбіти.

Рівень операцій	Основні методики проведення
	Блокування запуску стратегічних та тактичних ракет, зміна їхнього польотного завдання й навіть перенацілювання їх на інші об’єкти в суміжних країнах тощо

У цьому випадку під кібератакою доцільно розуміти сукупність узгоджених за ціллю, змістом і часом дій (кібердій), які реалізуються в кіберпросторі та призводять або можуть призвести до порушення конфіденційності, цілісності, доступності, спостережності та/або авторства інформації, а також порушення роботи ІТ-систем.

Під кібероперацією, за аналогією з методами звичайної війни, розуміють сукупність узгоджених за часом, глибиною та завданнями відносно короткочасних кібератак, спрямованих на один або декілька об’єктів впливу протиборчої сторони з наміром одержання незаконного доступу до їхніх інформаційних ресурсів, порушення роботи їхніх інформаційних систем або взагалі повного виведення обраних об’єктів з функціонування.

Кібероперації можуть проводитися за допомогою спеціальних засобів ураження (спеціально організованої інформації та інформаційних технологій), що становлять зміст поняття «кіберзброя» і надають змогу конкретно редагувати, копіювати, видаляти та блокувати інформацію, проникати крізь системи захисту, блокувати доступ законних користувачів, порушувати роботу носіїв інформації для дезорганізації роботи технічних засобів комп’ютерних систем та інформаційно-обчислювальних мереж. При цьому до спеціальних оборонних засобів слід віднести засоби, призначені для захисту й виявлення атак противника, а також протидію атакам.

Спеціальні оборонні засоби можуть бути поділені на такі групи:

засоби захисту інформації (засоби захисту каналів зв’язку, території, приміщень, пристроїв; засоби захисту операційних систем, баз даних і програмного забезпечення; засоби шифрування; засоби контролю й керування доступом і т. ін.);

розвідувальні засоби в кіберпросторі (радіоелектронна, кіберрозвідка та інші види розвідки).

Як одну з можливостей протистояти сучасним загрозам у сфері інформаційної та кібербезпеки британські програмісти запропонували нову оборонну кіберзброю – «Інтернет-телескоп». Він відстежує проблемні зони мережі Інтернет й автоматично припиняє кібератаки [7]. Проникаючи в «глибини» мережі, «телескоп» аналізує вміст трафіку (переданих даних) на предмет наявності злоякісних програмних кодів, які призводять до перетворення окремих зон мережі на ботнети, що складаються з уражених машин – «комп’ютерів-зомбі». Уражені машини, найчастіше без відома їхніх користувачів і власників, віддалено керуються зловмисниками та втягуються у виконання масованих дій на кшталт розсилання спаму, навмисного створення надмірного числа запитів на ті чи інші сервери (DDoS-атаки) з метою спровокувати їхню відмову тощо.

Виявивши заражені вузли мережі, «телескоп» встановлює фізичне місце перебування окремих «зомбованих» комп’ютерів і складає карту загроз, яка, за бажанням, може бути проаналізована фахівцями. У подальшому «телескоп» без зайвого втручання обслуговуючого персоналу визначає тип шкідливої програми й переводить її подальші дії під свій контроль.

Як заявили представники британського уряду [7], відсутність таких та подібних, «більш реалістичних» рішень, у сфері протидії кібератакам на критично важливу інфраструктуру (фінансові ринки, банківські мережі, об’єкти енергетики, телекомунікації тощо) може суттєво «підштовхнути міждержавні кібервійни в майбутньому». Аналогічну позицію висловлено в доповіді генерального секретаря Міжнародного союзу телекомунікацій Хамадуна Турі на виставці ITU Telecom World у Женеві, в якій він визначив, що «третя світова війна може початися як наслідок інформаційного протиборства саме в кіберпросторі»

[8]. І тоді, за його ж словами, майже будь-яка людина «за допомогою армії заражених комп'ютерів («ботів») зможе мати велику владу у такій віртуальній битві».

Наступальна зброя кібероперацій охоплює засоби активного комп'ютерного впливу, здатні порушити функціонування інформаційних систем органів управління державних і військових об'єктів, промисловості, транспорту, зв'язку, енергетики, банків та інших установ шляхом безпосереднього інформаційного втручання в роботу комп'ютерних систем. Найчисленнішою й найнебезпечнішою для ІТ-систем противника серед наступальних засобів є група активного впливу, тобто атакуюча кіберзброя. До її арсеналу можна віднести: комп'ютерні віруси; програмні закладки й логічні бомби; електромагнітні гармати (портативні генератори електромагнітних випромінювань великої потужності); різноманітні пристрої постановки активних комунікаційних перешкод; засоби знищення, перекручування та розкрадання інформаційних масивів; спеціальні апаратні закладні пристрої; спеціальні мікроорганізми, здатні руйнувати ізоляційний матеріал та радіоелектронні елементи.

Зазначені засоби найбільшою мірою здатні вразити найважливіші АСУ супротивника, які діють у реальному часі, наприклад системи спостереження й попередження про ракетний напад, системи наведення зброї тощо.

Одним з доволі показових прикладів застосування атакуючої кіберзброї слід вважати події 2010 р., спричинені мережевим хробаком Win32/Stuxnet. Проникнувши в систему іранської АЕС у Бушері, вірус, розроблений групою експертів, які, найімовірніше, володіли сучасною технічною базою, загальмував ядерну програму Ірану практично без будь-якого насильства.

Перш ніж потрапити до АЕС у Бушері, вірус протягом тривалого часу поширювався світом через флеш-накопичувачі за допомогою невідомої раніше уразливості ОС Windows. Як з'ясувалося, він був вузько цілеспрямованим і, згідно з опублікованими у засобах масової інформації на кшталт [9] та іншими даними, мав на меті впровадження шкідливого функціонала до промислових інформаційних систем контролю над виробничими процесами класу SCADA, що працюють під керуванням SIMATIC WinCC корпорації Siemens, проведення їх подальшого моніторингу, а також крадіжку з них інформації та змінювання реєстрів.

Як видно з наведених вище прикладів, оборонна й наступальна кіберзброя може застосовуватися переважно двома способами. Перший з них передбачає впровадження програмних та апаратних закладок у технічні засоби обробки інформації на етапі їхнього виробництва з подальшим постачанням у визначені країни (активуються ці закладки, як правило, за спеціальною командою). Другий передбачає застосування кіберзброї шляхом фізичного проникнення на об'єкт або використання спеціальних технічних засобів уже в процесі ведення кіберборотьби – комплексу заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на автоматизовані ІТ-системи супротивника й захисту від такого впливу власних інформаційно-обчислювальних ресурсів шляхом використання спеціально розроблених програмно-апаратних засобів. Як стверджує директор Лондонського міжнародного інституту стратегічних досліджень Джон Чіпмен [7], імовірність застосування оборонної та наступальної кіберзброї дуже зросла, але вона й досі залишається «серйозно недооціненою» загрозою міжнародній безпеці. Як один з можливих прикладів ведення кібервоєн доцільно навести акт публікації величезної кількості конфіденційної інформації на сайті Wikileaks. Тобто в цьому випадку США виявилась, як і практично всі інші провідні країни світу, абсолютно неготовою до кібервійни, уразливою для такого роду атак і такою, що не в змозі забезпечити належний рівень захисту власних конфіденційних даних.

Отже, стрімкі темпи розвитку світової науково-технічної думки та подальшого вдосконалювання ІТ-систем і технологій фактично призвели до створення єдиного

глобального інформаційного й кіберпросторів, у яких у перспективі будуть акумульовані всі засоби збору, накопичення, обробки, обміну та зберігання інформації.

Це, у свою чергу, формує передумови для:

упровадження нових та розвитку існуючих форм і способів інформаційного протиборства за володіння світовим інформаційним ресурсом;

зростання ймовірності виникнення конфліктів у боротьбі за досягнення й утримання інформаційної переваги одних суб'єктів над іншими тощо.

Основною формою таких дій у недалекому майбутньому стануть, скоріш за все, кібервійни, які відрізнятимуться від звичайних бойових дій і слугуватимуть лише приводом до їх розв'язання. Їхні основні цілі, скоріш за все, полягатимуть передусім у здійсненні кіберрозвідки в органах державного та військового управління, порушенні цілісності й доступності інформації та прозорості процесів, руйнуванні інфраструктури мереж або їхніх окремих елементів, блокуванні або виведенні з ладу автоматизованих систем управління тощо.

Основними об'єктами негативного впливу кібервійн (об'єктами критичної інформаційної інфраструктури) при цьому можуть бути:

комп'ютерні мережі державних урядових органів, фінансових установ, енергетичного сектору;

системи керування повітряним рухом, рухом залізничного транспорту та важливих підприємств, критичних для життєдіяльності;

автоматизовані системи управління військами та зброєю;

інші мережі, що призначаються для збору, обробки, збереження та видачі інформації, виведення з ладу яких також може вплинути на досягнення поставлених цілей тощо.

Тобто, якщо взяти до уваги головні характеристики майбутніх кібервоєн, а саме: можливість здійснення нападу будь-ким; географічну досяжність; невідворотність; потенціал і легкість поширення, а також вплив на «електронно готові» цілі, – можна припустити, що їхній початок може стати революцією у військовій справі, а їхні результати взагалі можуть виявитися непередбачуваними. Здебільшого це пояснюється тим, що:

кібервійна дає можливість здійснювати атаки безпрецедентній кількості аматорів, яким достатньо мати з'єднання з мережею Інтернет (вплив таких атак зростатиме з посиленням ролі глобальної мережі в щоденному політичному, соціальному й економічному житті);

кібервійна не передбачає тих витрат і зусиль, яких потребують напади на цілі, розташовані на далекій відстані (її поширення не обмежується засобами комунікації, як це було раніше);

кібервійна – це відносно легкий спосіб скористатись дедалі сильнішою залежністю від упровадження сучасних ІТ-технологій;

кібервійна не заміщає собою війну звичайну. Фактично вона є іншою ареною ведення більш масштабної війни. І ті країни, які першими оволодіють мистецтвом кібервійни, зможуть отримати фундаментальну перевагу вже на її початкових стадіях.

Висновки

За результатами викладеного матеріалу пропонується змінити прийняті в нашій державі підходи до визначень та термінологічних взаємозв'язків між кібероперaціями та кібердіями, розробити та впровадити відповідні документи та закупити новітні засоби зв'язку для розвитку новітніх ІТ-технологій країни.

Напрямки подальших досліджень

Аналіз та розробка подальших рекомендацій із удосконалення форм та способів кібердій в оборонній операції сил оборони на основі найкращих світових практик, зокрема, ґрунтуючись на керівних документах провідних країн світу та країн-членів НАТО з організації та ведення кібервійн та кібероперацій.

ЛІТЕРАТУРА

1. Национальная стратегия обеспечения безопасности киберпространства США: Неофиц. перевод / Смирнов А. // Информационная глобализация и Россия: вызовы и возможности. Москва, 2005. С. 363–370.

2. Cyberwar: War in the Fifth Domain // The Economist. 2010. Jul 1st.

3. Clarke R. A. Cyber War // Harper Collins. 2010.

4. Мережко А. А. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете) // Електронний ресурс. URL: http://www.politik.org.ua/vid/publcontent.php3.

5. Ляшенко І. О., Кириленко В. А. Кібернетичні операції – майбутня форма збройної боротьби // Електронний ресурс. URL: http://www.nbuv.gov.ua/portal/soc_gum/znpnapv_vtn/2010_53/10liofzb.pdf.

6. СМИ внезапно вспомнили о черве WIN32/Stuxnet // Електронний ресурс. URL: http://purogok.ucoz.ua/news/smi_vnezapno_vspomnili_o_cherve_win32_stuxnet/2011/09/30/501.

7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. С. 403.

8. JP 3-12, Cyberspace Operations, 08 June 2018.

9. FM 3-12, Cyberspace and Electronic Warfare Operations, 11 April 2017.

10. NATO Standard Ajp-3.10.2 Allied Joint Doctrine For Operations Security And Deception, Edition A Version 2, January 2020.

11. NATO Standard Ajp-3.20 Allied Joint Doctrine For Cyberspace Operations, Edition A Version 1, January 2020.

12. STANAG 6514 Allied Joint Doctrine For Cyberspace Operations, Edition 1, 29 January 2020.

УДК 004.062(045)

Карпенко А. О. (ВІТІ ім. Героїв Крут)
Мусієнко В. А. (ВІТІ ім. Героїв Крут)
Шугалій О. О. (ВІТІ ім. Героїв Крут)
Пономаренко З. М. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ІНСТРУМЕНТІВ ЗБОРУ РОЗВІДУВАЛЬНОЇ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ

Російсько-українська війна дуже відрізняється від попередніх відомих конфліктів тим, що завдяки сучасним технологіям вона є значно відкритою для суспільства. Зараз кожен має мобільний телефон, за допомогою якого можна поділитися свіжою інформацією з місця подій в мережі Інтернет. Саме тому сьогодні набирає великої популярності метод розвідки на основі аналізу інформації з відкритих джерел (OSINT – Open Source Intelligence). Для того, щоб розвідати необхідну інформацію, потрібно знати де шукати і мати необхідні для цього програмні інструменти. Зважаючи на вищевикладене, метою даної статті є дослідження основ розвідки інформації з відкритих джерел та порівняльний аналіз існуючих інструментів для збору розвідувальної інформації.

Під терміном OSINT зазвичай мають на увазі збір інформації з відкритих джерел, її аналіз, підготовку та передачу кінцевому замовнику для вирішення певних завдань. Відкрите джерело інформації (ВДІ) – це особа чи група, яка надає інформацію без вимоги збереження її конфіденційності. До ВДІ відносять мережу Інтернет, засоби масової інформації, академічну сферу, публічні організації, бібліотеки (архіви), інформаційні служби, загальнодоступні документи, сіру літературу та ін. Збір розвідувальної інформації можна поділити на такі етапи, як визначення мети, вибір інструментів, пошук та збір інформації, аналіз інформації, формування звіту. Існує два методи збору інформації – пасивний та активний. Пасивний метод полягає у зборі даних із загальнодоступних джерел, при використанні активного здійснюється безпосередній вплив на досліджуваний об'єкт.

У статті було проведено порівняльний аналіз інструментів збору розвідувальної інформації, як-от Maltego, OWASP Maryam, TheHarvester, SpiderFoot, Shodan, Google Dork Queries. Було досліджено їхні функціональні можливості, виявлено переваги та недоліки. Визначено перспективні напрямки подальших досліджень.

Ключові слова: *OSINT, відкрите джерело, Інтернет, пошукова система, фреймворк.*

A. Karpenko, V. Musiienko, O. Shuhalii, Z. Ponomarenko Analysis of open source intelligence gathering tools.

The Russian-Ukrainian war is very different from the previous known conflicts in that, thanks to modern technology, it is much more open to society. Now everyone has a mobile phone with which they can share the latest information from the scene on the Internet. That is why today the method of intelligence based on the analysis of information from open sources (OSINT) is gaining popularity. In order to find the necessary information, you need to know where to look and have the necessary software tools. Based on the above, the purpose of this article is to study the basics of intelligence from open sources and a comparative analysis of existing tools for gathering intelligence.

The term OSINT usually refers to the collection of information from open sources, its analysis, preparation and transmission to the end customer to solve certain tasks. An open source information (OS) is a person or group that provides information without requiring it to be kept confidential. OS includes the Internet, mass media, academia, public organizations, libraries (archives), information services, public documents, gray literature, etc. The collection of intelligence can be divided into such stages as goal setting, selection of tools, search and collection of information, analysis of information, reporting. There are two methods of collecting information – passive and active. The passive method is to collect data from publicly available sources, when using the active is a direct impact on the object under study.

The article conducted a comparative analysis of intelligence gathering tools such as Maltego, OWASP Maryam, TheHarvester, SpiderFoot, Shodan, Google Dork Queries. Their functionality was investigated, the advantages and disadvantages were identified. Perspective directions of further researches are defined.

Keywords: *OSINT, open source, Internet, search engine, framework.*

Постановка завдання

Через стрімкий розвиток технологій та зростання кількості інформації мережа Інтернет нині є основним джерелом для OSINT. Головними її перевагами є швидкість отримання даних, включаючи кількість, якість та прозорість, різноманітність, простоту використання та низьку вартість аналізу [1].

Розвідану інформацію можна використовувати в багатьох сферах, зокрема й для забезпечення національної оборони та безпеки. Наприклад, в країнах НАТО існують спеціальні центри, що займаються розвідкою OSINT і на основі зібраної інформації потім приймають відповідні рішення [2]. З початком гібридної російсько-української війни 2014 року в Україні активно почали застосовувати технології OSINT. В той час активістами були створені ресурси «InformNapalm» та «Миротворець». У своїй діяльності вони користувалися методами розвідки із відкритих джерел для проведення розслідувань та збору інформації про ворогів. Після початку російської збройної агресії 2022 року за допомогою технології OSINT вдалось розвіяти туман війни, спростовувати російські заяви та пропаганду, протидіяти ворожим інформаційним операціям, розвінчувати фейки, фіксувати численні військові злочини та ін. Загалом важко переоцінити роль OSINT в сучасній війні.

В умовах зростання популярності технології OSINT виникає проблема у виборі необхідних інструментів для ведення розвідки з ВДІ, тому доцільно приділити цьому увагу в цій статті.

Аналіз останніх досліджень і публікацій

Дослідженням проблематики отримання розвідувальної інформації OSINT на сьогодні займаються як вітчизняні, так і закордонні вчені. В цій роботі було використано напрацювання таких авторів, як Д. В. Ланде, А. Г. Додонов, В. В. Циганок, О. В. Андрійчук, С. В. Каденко, А. Н. Грайворонська, К. В. Власов, О. Ю. Іохов, О. В. Минько та ін.

У праці [3] автори розглянули використання технології OSINT як одного із способів отримання розвідувальної інформації та визначили їхні перспективи у процесі службово-бойової діяльності Національної гвардії України. У роботі [4] були проаналізовані методології та інструменти в аналітичній діяльності OSINT, приведено перелік сервісів та програмних рішень. Однак досліджень щодо аналізу інструментів збору розвідувальної інформації з відкритих джерел не проводилось.

Отже, **метою статті** є дослідження теоретичних основ розвідки OSINT та аналіз інструментів збору розвідувальної інформації з ВДІ із застосуванням порівняльного аналізу.

Основна частина

Під терміном OSINT зазвичай мають на увазі збір інформації з відкритих джерел, її аналіз, підготовку та передачу кінцевому замовнику для вирішення певних завдань. OSINT є методом ведення розвідки на основі збору та аналізу загальнодоступної інформації.

ВДІ – це особа чи група, яка надає інформацію без вимоги збереження її конфіденційності, тобто інформація чи відносини незахищені від публічного розкриття. ВДІ може бути загальнодоступним, але не вся публічно доступна інформація є відкритим джерелом [5].

До основних ВДІ можна віднести: мережу Інтернет (соціальні мережі, форуми, блоги, чати, сайти обміну відео, пошукові системи, дошки оголошень, бази даних, сервіси геолокації та супутникові знімки), засоби масової інформації (телебачення, радіомовлення, газети, журнали, наукові видання), спостереження (радіомоніторинг, дані дистанційного зондування землі), загальнодоступні документи, публічні заходи (конференції, форуми), сіра література (технічні звіти, патенти, робочі документи) та будь-які інші, що не мають обмежень допуску. У зв’язку з поширеністю засобів обміну інформацією нові джерела з’являються швидко, тому потрібно постійно підтримувати актуальність даних, щоб збільшити їхню цінність під час використання. Зокрема, постійне оновлення в режимі онлайн є перевагою ВДІ, яка не дає можливості викривлення інформації.

Загалом збір розвідувальної інформації в OSINT можна поділити на такі етапи:

1. Визначення мети.
2. Підготовка інструментів для досягнення мети.
3. Пошук та збір інформації.

4. Аналіз отриманих даних.
5. Формування звітних матеріалів.

На першому етапі потрібно визначити всі вимоги, які повинні виконуватися протягом всього процесу розвідки. Необхідно чітко сформулювати цілі та задачі. Далі варто підібрати необхідний набір інструментів для збору інформації. Потім потрібно провести дослідження на основі кожного з ВДІ, які можуть надати більше даних або інформації для вашого дослідження. З них потрібно виокремити найбільш цінні джерела, які будуть збиратися відповідно до поставленого завдання. Далі йде збір інформації з визначених джерел. На наступному етапі проводиться аналіз отриманих даних – виявляють зв'язки між інформацією з різних джерел, шукають закономірності, щоб робити відповідні висновки. У такий спосіб аналіз дає можливість класифікувати отриману інформацію за рівнем цінності. Останнім етапом є оформлення результатів у вигляді звіту для подальшого використання кінцевим замовником.

Існує два методи розвідки OSINT з ВДІ – пасивний та активний. Вибір залежить від типу інформації та складності її отримання. Пасивний метод використовують найчастіше, він полягає у зборі даних із загальнодоступних джерел. Інформація збирається вручну або за допомогою спеціальних сервісів та інструментів, що спрощують збирання, систематизацію та аналіз даних. Прикладом може бути пошук у соціальних мережах, пошукових системах, перегляд витоків баз даних, вилучення метаданих із публічних файлів та ін. При використанні активного методу здійснюється безпосередній вплив на досліджуваний об'єкт, застосовуються спеціалізовані засоби отримання даних або порядок дій, що потребують певних зусиль. Прикладом даного підходу є сканування портів, визначення доменних імен серверу, збір даних на закритих платних ресурсах, використання сервісів сканування сайтів та ін.

Збір інформації з ВДІ – це трудомістка робота, тому для цього були розроблені спеціальні технології, які дозволяють спростити збір розвідданих. Далі в роботі будуть проаналізовані найбільш популярні комплексні інструменти OSINT.

Порівняльний аналіз інструментів збору розвідувальної інформації на основі відкритих джерел [6–11]. Метою даного аналізу є дослідження інструментів розвідки OSINT на предмет визначення їхніх функціональних можливостей. Для досягнення мети передбачено виконання таких завдань, як виявлення особливостей застосування інструментів та їх порівняльний аналіз. У таблиці 1 наведено коротку інформативну довідку про дані засоби.

Таблиця 1

Комплексні інструменти розвідки OSINT

Назва	Розробник	Офіційний сайт
Maltego	Maltego Technologies	https://www.maltego.com/
OWASP Maryam	Saeed Dehqan	https://owasp.org/www-project-maryam/
TheHarvester	Christian Martorella	https://github.com/laramies/theHarvester
SpiderFoot	Steve Micallef	https://www.spiderfoot.net/
Shodan	John Matherly	https://www.shodan.io/
Google Dork Queries	Google Inc	https://www.google.com/

Maltego – один з найвідоміших OSINT-фреймворків для персональної та корпоративної розвідки. Це інструмент із графічним інтерфейсом, який забезпечує можливість збору інформації про будь-яких осіб шляхом отримання загальнодоступної інформації в Інтернеті різними методами. Maltego також здатний складати списки DNS і збирати дані із соціальних мереж у зручному форматі. Одним з найпоширеніших варіантів використання Maltego є дослідження та отримання інформації про вебсайти.

Модулі в Maltego мають назву transforms. Transforms вбудовані в інструмент і визначаються як сценарії коду, які виконують певні завдання. Maltego також має безліч плагінів, таких як набір інструментів SensePost, Shodan, VirusTotal, ThreatMiner і т. д.

Дослідимо основні модулі:

CaseFile Entities – цей модуль включає всі сутності з версії CaseFile.

Blockchain.info – відстежує та візуалізує зв'язки та транзакції між гаманцями у блокчейн мережі bitcoin та у мережі Ethereum.

CipherTrace – модуль для відстеження транзакцій у криптовалюті та побудови ланцюжків зв'язків між різними криптогаманцями. Може бути корисним для спроб визначення власника гаманця.

Have I been Pwned? – перевіряє чи зламаний цільовий сайт, електронна пошта або акаунт, шукає у витоках баз даних скомпрометований пароль.

Hybrid-Analysis – дозволяє взаємодіяти з ресурсом Hybrid-Analysis, що дозволяє перевіряти підозрілі файли на віруси.

PassiveTotal – додає додаткові трансформації для вивчення доменів, даних організацій, електронної пошти за допомогою RiskIQ.

PeopleMon – дозволяє шукати дані користувачів по базах InGrav PeopleMon.

Shodan – дозволяє використовувати можливості пошукача Shodan.

Social Links CE – дозволяє шукати дані людей та компаній, використовуючи бази ZoomEye, Shodan, SecurityTrails, Censys, Rosette, Skype, Documentcloud, Social Links. А також додає можливості пошуку реєстраційних даних компаній з відкритих баз Євросоюзу та офшорних зон.

ThreatMiner – додає трансформації, що дозволяють аналізувати та збирати інформацію про домени, IP, DNS, e-mail, а також виявляти шкідливе програмне забезпечення (ПЗ).

ZETAlytics Massive Passive – дозволяє знаходити історію зміни IP-адрес, шукати зв'язки між IP та доменами, електронними поштами та доменами, NS та доменами, а також шукати реєстраційні дані, враховуючи історію змін.

Програма може бути використана для виявлення відносин та реальних зв'язків між: людьми, групами людей (соціальні мережі), компаніями, організаціями, вебсайтами, доменами, DNS-іменами, сутностями NetBlocks, IP-адресами, фразами, документами та файлами, а також сутностями, пов'язаними між собою за допомогою відкритих джерел.

Даний інструмент написаний на мові JAVA, що дозволяє користуватися ним на більшості операційних систем (ОС). Він має гнучку структуру, яка формується завдяки налаштуванням і може бути легко адаптована під власні вимоги. До недоліків можна віднести умовну безоплатність, так щоб отримати додаткові функції, необхідно оформлювати підписку.

OWASP Maryam – OSINT-фреймворк з відкритим кодом, що містить в собі велику кількість модулів, за допомогою яких можна вирішувати великий спектр задач з пошуку та збору інформації. Написаний на мові програмування Python і має сумісність з ОС Linux та MacOS. У програмі відсутній графічний інтерфейс.

Модулі інструменту розділені на три категорії:

Footprint – містить в собі модулі для збирання та аналізу інформації про вебдодатки. Можна шукати файли, папки, піддомени, визначати ОС, збирати інформацію на сторінках (форми, пошти, ніки тощо);

Search – містить в собі модулі для роботи з соціальними мережами та пошуковими системами. Кожен модуль відповідає соціальній мережі та пошуковій системі;

OSINT – містить в собі модулі для розширеного пошуку електронних листів, документів, імен DNS, соціальних мереж та сканування сайтів.

Дослідимо основні модулі категорії OSINT:

reddit_search – пошук по Reddit. Находить відповідні пости і теми;

crawler – сканує сайт, щоб знайти посилання, пошту, телефони, коментарі, усі файли CSS та іншу цінну інформацію;

username_search –пошук за іменем користувача;

social_nets – пошук соціальних мереж за нікнеймом;

article_search – пошук наукових статей;

dark_web_crawler – сканер мережі DarkWeb;

phone_number_search – шукає телефон по ENUM (відображає країну, оператора, локальний і міжнародний формати номера);

tweet_search – шукає твіти в Твітері;

onion_search – пошукова система для мережі Tor;

domain_reputation – перевіряє репутацію цілого домену;

email_pwned – перевіряє адресу електронної пошти в базах витоку інформації;

email_search – шукає електронні пошти;

cloud_storage – шукає файли в загальному доступі в онлайн-сховищах GoogleDrive, OneDrive, Dropbox, Amazon;

dns_search – шукає піддомени через пошукові системи;

slavna_person – шукає за іменем та/або прізвищем в Google, Wikipedia, Wikileaks та Twitter;

offer – на основі вихідного запиту генерує варіанти ключових слів для використання в пошукових системах;

docs_search – шукає документи в пошукових системах.

OWASP Maryam – це потужний багатофункціональний інструмент для OSINT та збору даних, а також для автоматизації завдань розвідки. Недоліками є відсутність підтримки пошукової системи Shodan та інтерфейс командного рядка.

TheHarvester – OSINT-фреймворк для збору адрес електронної пошти, імен піддоменів, віртуальних хостів, відкритих портів та імен співробітників компаній з різних відкритих джерел.

Дослідимо основні модулі:

google – розширений пошук в Google;

googleCSE – пошук Google-користувача;

google-profiles – специфічний пошук за профілями Google;

bing – розширений пошук в Microsoft Bing;

bingapi – розширений пошук в Microsoft Bing через API;

dogpile – розширений пошук в Dogpile;

pgp – сервер ключів pgp – mit.edu;

linkedin – специфічний пошук за користувачами Linkedin;

vhost – пошук Bing за віртуальними хостами;

twitter – специфічний пошук за Twitter-акаунтами;

yahoo – пошук в системі Yahoo;

baidu – пошук в системі Baidu;

shodan – пошук в системі Shodan;

brutforceDNS – цей плагін запустить перебір доменів за словником;

resolveDNS – зворотне перетворення виявлених IP для пошуку хостів;

DNS_TDL – перебір за словником TLD.

Цей інструмент створений мовою Python та має відкритий програмний код. З недоліків – це інтерфейс командного рядка та підтримка лише ОС Linux.

SpiderFoot – це інструмент автоматизації розвідки OSINT з відкритим вихідним кодом. Він інтегрується майже з кожним доступним джерелом даних і використовує цілий ряд методів для аналізу даних, що полегшує навігацію в цих даних. Інструмент має вбудований

вебсервер для забезпечення інтуїтивно зрозумілого вебінтерфейсу, але його також можна повністю використовувати через командний рядок.

Інструмент містить в собі близько 200 модулів, що забезпечують збір даних для таких речей, як:

- індексація/вилучення хосту/піддомену/TLD;
- адреса електронної пошти, номер телефона та вилучення людського імені;
- вилучення адрес Bitcoin та Ethereum;
- розвідка про загрози та запити в чорний список;
- інтеграція API з SHODAN, HaveIBeenPwned, GreyNoise, AlienVault, SecurityTrails тощо;
- індексація акаунтів у соціальних мережах;
- IP-геолокація;
- вебскрапінг, аналіз вебконтенту;
- аналіз метаданих зображень, документів і бінарних файлів;
- пошук в DarkNet;
- сканування портів і захоплення банерів;
- пошук у витоках баз даних.

Основною перевагою є автоматизація процесу збору OSINT, що дає змогу знайти що-небудь про вашу ціль централізовано одним інструментом. Для розвідки необхідно вказати ціль, обрати модулі для запуску, після чого Spiderfoot збере всі дані, щоб створити повний профіль досліджуваного об’єкта.

Shodan – це пошукова система, яка дозволяє користувачеві за допомогою різноманітних фільтрів знаходити певні типи пристроїв (вебкамери, маршрутизатори, сервери тощо), підключених до Інтернету. Окрім виявлення пристроїв, Shodan також можна використовувати для моніторингу баз даних щодо витоку даних на загальнодоступних сайтах і навіть для пошуку прихованих серверів у корпоративних мережах. Дана пошукова система застосовується спеціалістами у багатьох сферах – безпека мережі, дослідження ринку, кібербезпека, інтернет речей, відстеження шкідливого ПЗ та ін.

Дослідимо основні фільтри Shodan для OSINT:

country – пошук пристроїв в межах певної країни;

product – пошук пристроїв на основі продуктів (Tomcat, Kafka);

port – пошук пристроїв на основі певних портів;

server – пошук серверів (Apache, Nginx);

os – пошук на основі операційної системи (Windows XP, Windows 7);

org – пошук за певними організаціями (Google, Facebook);

vuln – пошук на основі CVE.

До недоліків даного інструменту можна віднести умовну безоплатність, так як повний функціонал доступний за оплату. Перевагами є зручний вебінтерфейс та сумісність з усіма ОС, що мають встановлений веббраузер з доступом до Інтернету.

Google Dork Queries (GDQ) – техніка, що використовується спеціалістами OSINT для створення запитів у пошукових системах з використанням розширених параметрів для виявлення прихованої інформації та вразливостей, які можна знайти на загальнодоступних серверах.

Dorking можна використовувати в різних пошукових системах, не лише в Google. У повсякденному використанні пошукові системи, такі як Google, Bing, Yahoo та DuckDuckGo, приймають пошуковий запит або рядок пошукових запитів та повертають відповідні результати. Також ці системи запрограмовані приймати більш просунуті і складніші оператори, які значно звужують ці умови пошуку. Оператор – це ключове слово або фраза, що має особливе значення для пошукової системи. Ось приклади операторів, що

часто використовуються: «inurl», «intext», «site», «feed», «language». За кожним оператором слідує двокрапка, далі за якою – відповідна ключова фраза або фрази.

Ці оператори дозволяють шукати більш конкретну інформацію, наприклад: певні рядки тексту всередині сторінок вебсайту або файли, розміщені за конкретною URL-адресою. Крім того, Google Dorking може також знаходити приховані сторінки для входу в систему, повідомлення про помилки, що видають інформацію про доступні вразливості та файли загального доступу.

Найбільш практичним сервісом Google є можливість пошуку видалених або архівних сторінок. Це можна зробити за допомогою оператора cache. Оператор працює так, що показує збережену в кеші Google версію вебсторінки.

Дослідимо основні оператори Google Dorking:

site – даний оператор обмежує пошук одним вебсайтом;

title – визначає будь-яку згадку запиту в заголовку вебсторінки;

allintitle – ідентифікує лише сторінки з усім пошуковим текстом у заголовку;

inurl – ідентифікує будь-яку згадку пошукового запиту в URL-адресі;

intext – ідентифікує лише сторінки з усім текстом пошукового запиту в URL-адресі;

filetype – обмежує результати лише вказаним типом файлу;

cache – показує останній кеш вказаного сайту.

Комбінуючи різним чином команди для пошуку, можна знайти практично все, аж до логіну/паролю адміністратора.

Для порівняння розглянутих інструментів здійснимо аналіз за низкою критеріїв, поданих нижче у таблиці 2.

Таблиця 2

Порівняльний аналіз інструментів розвідки OSINT

Інструмент	Функціональні можливості	Зручність інтерфейсу	Сумісність	Підтримка оновлень	Доступність
Maltego	пасивний та активний збір; аналіз	графічний інтерфейс	Windows, MacOS, Linux	версія 4.3.0 від 24.01.22	умовно безкоштовна
OWASP Maryam	пасивний та активний збір; аналіз	інтерфейс командного рядка	MacOS, Linux	версія 2.5.1 від 24.05.22	безкоштовна
TheHarvester	пасивний та активний збір	інтерфейс командного рядка	Linux	версія 4.0.3 від 25.11.21	безкоштовна
SpiderFoot	пасивний та активний збір; аналіз	вебінтерфейс або інтерфейс командного рядка	Windows, MacOS, Linux	версія 4 від 07.04.22	безкоштовна
Shodan	пасивний збір	вебінтерфейс	пристрої з веббраузером	постійна	умовно безкоштовна
Google Dork Queries	пасивний збір	вебінтерфейс	пристрої з веббраузером	постійна	безкоштовна

Проведений порівняльний аналіз інструментів розвідки інформації з відкритих джерел показав, що найбільш універсальним засобом OSINT є SpiderFoot, так як він володіє необхідними функціональними можливостями, зручним інтерфейсом, сумісний з більшістю ОС, є безкоштовним та з підтримкою розробником оновлень. Поряд з цим виявлено, що кожний інструмент має свої особливості та в деяких випадках краще використати той, що більше підходить для знаходження потрібної інформації.

Висновок

Як показало дослідження, OSINT є актуальною технологією інформаційної розвідки в сучасному світі. Даний метод широко використовується в багатьох сферах людської діяльності. З метою спрощення процесу аналізу інформації з відкритих джерел використовують програмне забезпечення та сервіси.

Порівняльний аналіз таких застосунків показав, що для того, щоб покрити більшість завдань розвідки, доцільно використовувати універсальний інструмент SpiderFoot. Цей програмний засіб не поступається іншим за функціональними можливостями, має відкритий вихідний код, підтримує автоматизацію, розповсюджується безкоштовно, володіє зручним інтерфейсом і сумісний з більшістю платформ. Потрібно розуміти, що не існує ідеальних застосунків і залежно від типу розвідувальної інформації, для максимально точного результату, потрібно використовувати вузько спеціалізовані інструменти.

Перспективними напрямками подальших наукових досліджень є розробка методичних рекомендацій щодо впровадження технологій OSINT у Збройні сили України.

ЛІТЕРАТУРА

1. Agata Ziółkowska Open source intelligence (OSINT) as an element of military recon // Електронний ресурс. URL: https://doi.org/10.5604/01.3001.0012.1474.

2. Пащенко Т. П. Гібридна війна та соціальні мережі // Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 62–65.

3. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації // Системи управління, навігації та зв'язку. 2016. Вип. 4. С. 81–84. URL: http://nbuv.gov.ua/UJRN/suntz2016422.

4. Додонов А. Г., Ландэ Д. В., Путятин В. Г. Применение OSINT в аналитической деятельности // URL: http://dwl.kiev.ua/art/ipri2018-3/dlp.pdf.

5. Open-Source Intelligence: ATP 2-22.9 June 2017 // URL: https://irp.fas.org/doddir/army/atp2-22-9-2017.pdf.

6. Maltego: website. URL: https://www.maltego.com/.

7. Maryam: website. URL: https://owasp.org/www-project-maryam/.

8. TheHarvester // GitHub. URL: https://github.com/laramies/theHarvester.

9. SpiderFoot: website. URL: https://www.spiderfoot.net/.

10. Shodan: website. URL: https://www.shodan.io/.

11. Google Dork Queris // Cylab. URL: https://cylab.be/blog/116/osint-simple-tips-3-google-dorks.

УДК 004.056(075.8)

Куцаєв В. В. (ВІТІ ім. Героїв Крут)
Головко О. Є. (ВІТІ ім. Героїв Крут)
Лазута Р. Г. (ВІТІ ім. Героїв Крут)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ КВАНТОВИХ ТЕХНОЛОГІЙ

Метою статті є ознайомлення науковців з надпотужними можливостями квантових технологій, надання основ квантових обчислень та квантового зв'язку.

Розглянуто основи квантових обчислень, які стрімко розвиваються у світі. Автори підкреслюють великі досягнення у практичній реалізації квантових технологій, які нададуть прорив у дослідженнях в усіх сферах наукової діяльності, пов'язаної з обробкою, збереженням та передачею інформації. Очікується, що квантові комп'ютери зможуть вирішувати математичні проблеми, які неможливо вирішити за допомогою звичайних комп'ютерів. Завданням статті є ознайомлення з механізмами квантових обчислень, основними квантовими логічними елементами, квантовими помилками та їх виправленнями. Представлені базові квантові алгоритми та їхні переваги над класичними.

Надаються основи побудови квантового зв'язку, Інтернету та телепортації.

Пояснено перспективи використання фотону як кубіта, його переваги та недоліки над іншими фізичними реалізаціями кубітів.

Підкреслено важливість вивчення та використання можливостей квантових обчислень та фрагментів квантового захищеного зв'язку. Це надасть можливість забезпечення безпеки інформаційно-телекомунікаційних систем в постквантовий період та позбавить противника можливості використовувати квантову перевагу.

Ключові слова: *постквантовий період, квантові розрахунки, квантовий зв'язок, квантова перевага, кубіт, зв'язаність кубітів, квантові помилки, корекція квантових помилок, фотон, квантовий паралелізм.*

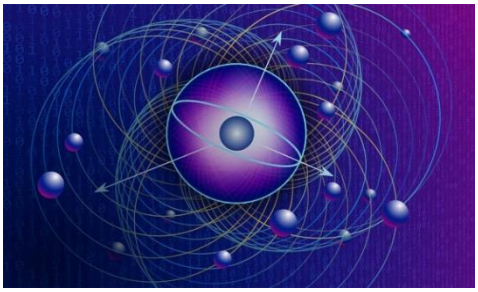
V. Kutsaiev, O. Golovko, R. Lazuta Prospects of using quantum technologies.

The purpose of the article is to acquaint scientists with the powerful capabilities of quantum technologies, to provide the basics of quantum computing and quantum communication. The basics of quantum computing, which are rapidly developing in the world, are considered. The authors emphasize great achievements in the practical implementation of quantum technologies, which will provide a breakthrough in research in all areas of scientific activity related to the processing, storage and transmission of information. Quantum computers are expected to be able to solve mathematical problems that cannot be solved by conventional computers. The task of the article is to get acquainted with the mechanisms of quantum calculations, the main quantum logical elements, quantum errors and their corrections. Basic quantum algorithms and their advantages over classical ones are presented. The basics of building quantum communication, the Internet, and teleportation are provided. The prospects of using a photon as a qubit, its advantages and disadvantages over other physical implementations of qubits are explained. The importance of studying and using the possibilities of quantum computing and fragments of quantum secure communication is emphasized. This will provide an opportunity to ensure the security of information and telecommunication systems in the post-quantum period and prevent the enemy from using the quantum advantage.

Keywords: *post quantum period, quantum calculations, quantum communication, quantum superiority, qubit, qubit connectivity, quantum errors, correction of quantum errors, photon, quantum parallelism.*

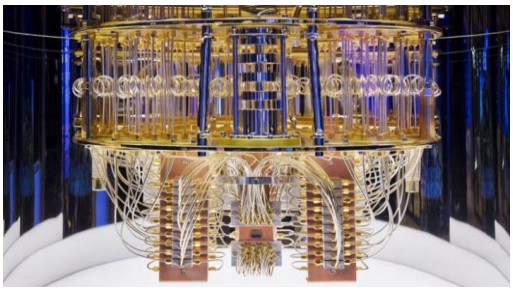
Постановка завдання в загальному виді

Актуальність. *Квантові розрахунки.* Сучасна теорія стверджує, що застосування квантових технологій (далі – КТ) призведе до стрибка у швидкості розрахунків для спеціальних завдань від 100 000 000 до 10 000 000 000 разів [1]. До таких спеціальних завдань можуть належати такі:



створення квантового закритого зв'язку, Інтернету та телепортації [2; 6; 10];
злам існуючих криптошрифтів квантовим алгоритмом Шора [6; 10];
проведення досліджень з ДНК [3];
розробки універсального штучного інтелекту [4];
створення нових складних матеріалів [4];
реалізація проєктів клінічних досліджень [5];

моделювання кліматичних умов [6];
моделювання складних систем [7];
створення каталізатора для абсорбування вуглекислого газу з атмосфери [8];
надпровідники, які здатні працювати при кімнатній температурі;
створення нових ліків від хвороб [9] та багато інших досліджень.



За останні 15 років у світі відбувається стрімкий розвиток засобів для реалізації КТ. В основу КТ покладено заміну послідовного перемикання носія біту зі стану «0» на «1» за час $\Delta t_{біт} > 0$ на квантовий кубіт, побудований *на основі квантових часток, де* стани «0» та «1» існують одночасно на різних енергетичних рівнях або спінах квантової частки, при цьому час перемикання «0» на «1» прагне до *0*, $\Delta t_{кубіту} \rightarrow 0$. Зі зростанням кількості зв'язаних кубітів, потужність розрахунків зростає в геометричній прогресії [6; 10].

Кубіти та їхня зв'язаність дозволяють квантовим комп'ютерам досягнути квантової переваги над сучасними розрахунковими комплексами орієнтовно на 50-кубітовому квантовому комп'ютері (далі – КК), що потенційно призводить до неймовірного збільшення ефективності обчислень на відміну від класичних комп'ютерів. Є цілий ряд застосувань, де КК принесуть особливі зміни.

Автори вважають, що слід інтенсивно готуватися до дій в постквантовий період. Також визначається прискорення, **надзвичайна масовість та інтенсивність досліджень КТ у світі.** Масові дослідження пояснюються надзвичайною перспективністю застосування КТ та квантового зв'язку. Найімовірніше, це призведе до технологічного прориву у КТ в найкоротші терміни. КТ інтенсивно досліджують США, Канада, Великобританія, Німеччина, Франція, Китай, Австралія, Японія та рф) [1–9].

Розробки КТ успішно ведуть приватні компанії IBM, Intel, Швейцарська Quantique, Google, Microsoft, Amazon, Alibaba, Rigetti, IonQ, Toshiba канадська D-Wav, американська ВПК Northropp Grumman та ін.

Саме тому користувачам інформаційних технологій слід вживати заходів щодо готовності працювати в постквантовий період.

Квантова перевага – означає момент, коли КК будуть вміти робити речі, на які не здатні звичайні комп'ютери. Концепція квантової переваги передбачає наявність унікальних особливостей КК, таких як квантова *заплутаність і суперпозиція.*

В таблиці 1 вказані високі темпи побудови зв'язаності кубітів та досягнення квантової переваги [1–12].

Таблиця 1

Держава / Компанія	**Рік презентації КК**	**Кількість кубітів**
США	2014 рік	5 кубіт
Intel	2017 рік	17 кубіт
Microsoft	2019 рік	50 кубіт
Досягнення стану квантової переваги над звичайним комп'ютером > 50 кубіт		
США / рф	2020 рік	51 кубіт
UMD / NIST	2017–2021 роки	53 кубіт
Rigetti Computing	2021 рік	80 кубіт (2 блоки*40 біт)
IBM	2021 рік	127 кубіт
IBM	**2022–2025 роки**	**400–1 000 кубіт**
компанія випустила КК *D-Wave One*	**2011 рік**	**з 128-кубітовим процесором**
D-Wave One	**2025 рік**	**Планується створення комп'ютера з 1024-кубітовим процесором**
перспектива	**2030 рік**	**1 000 000 кубіт**

Квантовий зв'язок (далі – КЗ). На сьогодні вже розроблено протокол квантового Інтернету. Наприклад, протокол квантового розподілу ключа на основі заплутаності BB84 та B92 [6; 10].

Квантове розподілення ключа – це теоретично абсолютно безпечний спосіб обміну таємними ключами між віддаленими користувачами. Метод заснований на фундаментальних законах квантової фізики, коли процес виміру квантової системи змінює її стан. Зловмисник, який спробує вкрасти ключ, має якимось чином виміряти його, але вимір вводить аномалії, які бачать і легітимні учасники протоколу. Отже, користувачі можуть розкрити та перевірити частину отриманого ключа та переконатися, що ніхто, крім них самих, його не виміряв.

Для реалізації подібних протоколів зв'язку необхідно налагодити квантову комунікацію між відправником та одержувачем. У випадку міських мереж, це можна зробити за допомогою оптоволоконних ліній. Також розподіл ключа між нерухомими об'єктами можна організувати «по повітрю», за допомогою лазера та детектора. Ці підходи вже були реалізовані – граничні відстані становлять близько кількох сотень кілометрів в обох випадках [1–12].

Потенціал КЗ визначається його обіцянкою забезпечити ультразахищене передавання даних, потенційно навіть повністю недоступне для хакерів. Нині наш обмін даними залежить від потоків електричних сигналів, які являють собою одиниці (1) і нулі (0), що біжать по оптоволоконних кабелях. Хакер, якому вдається підключитись до такого кабелю, може читати і копіювати ці біти в міру їхнього руху по кабелю. З іншого боку, у КЗ інформація, що передається, закодована в квантову частку у суперпозиції 1 і 0, так званій «кубіт». Завдяки чуттєвості квантових станів до зовнішніх подразників щоразу, коли хакер намагається захопити інформацію, що передається, кубіт «згортається» або до 1, або до 0, – таким способом знищуючи квантову інформацію і залишаючи підозрілий слід [16].

Першим застосуванням КЗ стало так зване «Квантове поширення ключів» (QKD), в якому квантові частки використовуються для обміну криптографічними ключами. В QKD самі дані передаються традиційною інфраструктурою зв'язку, в той час як необхідні для розшифрування даних криптографічні ключі передаються окремо за допомогою квантових часток. Вже ведуться широкомасштабні експерименти з QKD із застосуванням як наземних ліній зв'язку, так і космічного зв'язку. У 2016 році Китай запустив перший у світі квантовий супутник «Міціус», який вже продемонстрував міжконтинентальне QKD «Земля – супутник» та «супутник – Земля», забезпечивши захищену відеоконференцію між Пекіном і Віднем.

Квантова телепортація може стати наступним кроком у КЗ. Якщо у QKD криптографічні ключі поширюються із застосуванням КТ, при квантовій телепортації сама інформація передається із застосуванням зчеплених квантових пар. Найбільша відстань, на яку досі була здійснена телепортація за допомогою оптоволоконного кабелю, становить 50 км, і на найближчі роки стоїть завдання розвитку квантової телепортації задля забезпечення захищеного зв'язку на більші відстані.

Кінцевою метою КЗ є створення «квантового Інтернету»: мережі зчеплених між собою КК, підключених до ультразахищеного КЗ, гарантованого фундаментальними законами фізики. Проте квантовому Інтернету потрібна не лише квантова телепортація на дуже великі відстані, йому також буде потрібний подальший розвиток інших важливих допоміжних технологій, таких як квантові процесори, комплексний квантовий стек Інтернету, який передбачає Інтернет-протоколи і програмне забезпечення квантового Інтернету. В таблиці 2 вказані темпи досягнень щодо КЗ [1–10].

Таблиця 2

Відомості про квантові телекомунікаційні події	**Відстань**
2021 р. вчені НПЛ Fermi ME США здійснили квантову телепортацію	44 км
Експериментальне розподілення ключа було продемонстровано за допомогою оптоволокна	421 км

Відомості про квантові телекомунікаційні події	Відстань
2020 р. китайським вченим вдалося передати ключ від супутника	1200 км
У Китаї відбувся сеанс квантового зв'язку на відстані	1120 км
2016 р. у Китаї відкрилася найдовша у світі квантова комунікаційна лінія. На лінії розташовано 11 наземних станцій. Вона є частиною проєкту квантової комунікаційної лінії завдовжки 2 тис. км	712 км В планах 2000…4000 км
2019 р. у Британії було запущено першу у світі комерційну квантову мережу. Безпечна мережа буде застосовувати квантове розподілення ключів (QKD)	100…700 км
Квантовий інтернет. Експерименти проводяться і на Східному узбережжі США, де дослідники посилають заплутані фотони волоконно-оптичними кабелями	між Брукхейвенскую НЛ у Нью-Йорку та Університетом шт. Нью-Йорк на **18** км
Toshiba створила несприйнятливу до зламу квантову мережу	100 км
У січні 2009 р. вченим вперше вдалося телепортувати квантовий стан іона на один метр, а у травні 2010 р. дослідниками з університету Сіньхуа виконано передавання квантового стану на 16 км. На сьогодні рекорд телепортації належить вченим Китайського університету науки і технологій	2017 р. здійснили передавання квантового стану на відстані 1200 км

Очікується, що найближчим часом квантовий інтернет може стати окремим відгалуженням звичайного Інтернету. Квантова телепортація передбачає передачу квантового стану частинки з одного місця в інше за допомогою квантової заплутаності явища, у якому квантові стани кількох об'єктів виявляються взаємозалежними. Телепортація потрібна не тільки для квантових комунікацій, вона є основою для оптичних квантових обчислень.

Аналіз останніх досліджень та публікацій

В роботі [6] викладені навчальні матеріали до курсу «Основи квантової інформатики», які дають базові знання для підготовки до використання КТ на практиці. Недолік полягає в тому, що ця робота не поспіває за новими здобутками, розробками та відкриттями у квантовій сфері.

В роботі [10] висвітлюються сучасні квантові обчислення, квантові вентилі та принцип використання фотону як кубіту в КК. Вдало освітлено нинішній стан використання фотону як кубіту, його недоліки та переваги над іншими фізичними об'єктами, які використовуються як кубіти. Зазначимо, що у зв'язку з масованістю та інтенсивністю розробок інших реалізацій кубіту цього не достатньо.

Метою роботи є висвітлення наступних проблем:

обґрунтування загрози від швидкого наступу постквантового періоду, обґрунтування важливості своєчасного опанування КТ та обрис шляхів подолання очікуваних загроз використання КТ противником;

ознайомлення з сучасними визначеннями, термінами та методами, які використовуються у КТ та КЗ.

Першочергово науковців повинні зацікавити методи прикладного використання квантових алгоритмів, методів постквантового шифрування та удосконалення атак на криптографію, а також основ використання КЗ, квантового Інтернету та квантової телепортації.

Виклад основного матеріалу

Кубіт – квантовий біт, основний об'єкт інформації у квантових обчисленнях. Звичайний класичний біт, який є основним об'єктом інформації у класичних обчисленнях, може мати одне з двох значень: 0 або 1. Принципова відмінність кубітів полягає у тому, що вони не обмежуються лише 0 та 1, кубіт може мати значення, яке є або одним із них, або

будь-яке інше значення, яке знаходиться між 0 та 1. Дане явище називається квантовою *суперпозицією* та, відповідно, може відбуватись лише в квантах – дуже маленьких об'єктах. Кубітом може виступати будь-який об'єкт, який має квантову поведінку, наприклад, фотон.

Суперпозиція станів – кубіт, що знаходиться в суперпозиції, при вимірюванні колапсує в одне з двох детермінованих станів (0 або 1). Імовірність стану 1 або 0 визначається суперпозицією кубіта. Якщо кубіт знаходиться в рівній суперпозиції, то він знаходиться наполовину в стані 0, наполовину в стані 1.

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle. \quad (1)$$

Суперпозицію станів кубіта зображують графічно у вигляді координатної сітки на сфері, де кожний вузол відповідає певному стану (рис. 1).

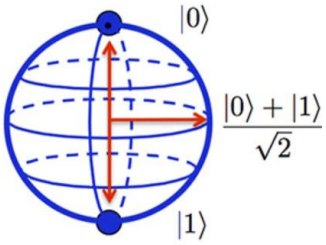


Рис. 1. Представлення кубіта

Стани $|0\rangle$ та $|1\rangle$ називають спеціальними станами обчислювального базису, які утворюють ортонормований базис цього векторного простору. Можна виміряти біт, щоб визначити стан, в якому він знаходиться [10; 12].

Сфера Блоха. Сфера Блоха існує для графічного представлення кубітів. Стан кубіта (1) можна переписати у такому вигляді:

$$|\psi\rangle=\cos\theta/2|0\rangle+e^{i\varphi}\sin\theta/2|1\rangle. \quad (2)$$

Числа θ та φ задають точку на одиничній тривимірній сфері, як зображено на рисунку 2. Сфера, зображена на рисунку, називається сферою Блоха. Вона існує для наочного представлення стану одиничного кубіту [10; 12].

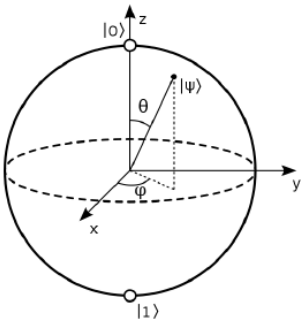


Рис. 2. Представлення стану кубіта на сфері Блоха

Вимірювання кубіту. Вимірювання відповідає неформальній ідеї «дивитись» на кубіт, який негайно згортає квантовий стан до одного з двох класичних станів 0/1 та 1/0.

Квантові обчислення. Фундаментальна модель квантових обчислень – квантові схеми. КК будується з квантових схем, що складаються з дротів та елементарних квантових елементів, які дозволяють передавати квантову інформацію та маніпулювати нею. Будь-яка квантова схема відображає перетворення квантової системи [12]. Квантова схема є квантовою обчислювальною моделлю, побудованою з квантових логічних ґейтів, в яких обчислювальні кроки синхронізовано по часу. Входи квантових ґейтів зв'язані з входами

схеми або виходами інших ґейтів. Складна унітарна операція може бути представлена у вигляді схеми, яка складається з кількох квантових ґейтів.

Вентилі Паулі. Вентилі Паулі – це одні з найпростіших квантових вентилів. Вентилі діють на один кубіт за раз.

Вентиль Паулі X. Вентиль Паулі X відповідає класичному вентилю NOT. Саме з цих міркувань, вентиль-X також часто називається квантовим NOT-вентилем. На рисунку 3 наведено приклад графічного зображення вентиля NOT.

Рис. 3. Графічне зображення вентиля Паулі X

Вентиль Паулі Z. Елемент Z займає важливе місце в квантових схемах, він залишає стан $|0\rangle$ без змін, а $|1\rangle$ переводить в стан $-|1\rangle$.

Вентиль Паулі Y. Елемент Y є комбінацією елементів X та Z. Даний елемент здійснює наступні перетворення: $|0\rangle \rightarrow |1\rangle$, $|1\rangle \rightarrow |0\rangle$

Елемент Адамара. Елемент Адамара є фундаментальним квантовим вентилем. Елемент дозволяє нам відійти від полюсів сфери Блоха і створити суперпозицію. Елемент Адамара являє собою перетворення, які описуються матрицею:

$$H=1/\sqrt{2}* \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (3)$$

Відіграє ключову роль в багатьох квантових схемах, здійснюючи наступні перетворення:

$$|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2};$$
$$|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}.$$

Елемент Адамара є одним з найбільш корисних квантових елементів, тому розглянемо його роботу в представленні на сфері Блоха. Виявляється, тут дії однокубітних елементів відповідають обертанню сфери. Операція Адамара – це обертання сфери навколо осі *y* на 90° з наступним обертанням навколо площини *xy* на кут 180°, як показано на рисунку 4.

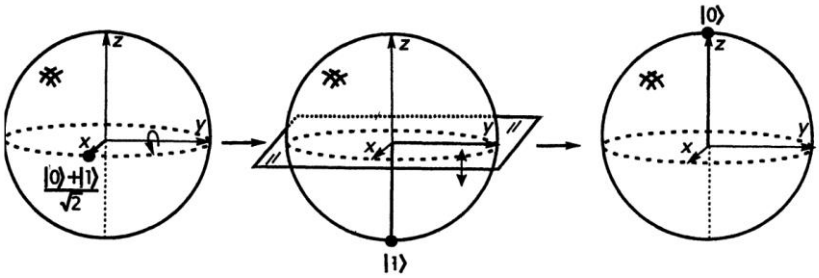


Рис. 4. Наглядне представлення елемента Адамара за допомогою сфери Блоха

На рисунку 5 зображено однокубітні квантові елементи.

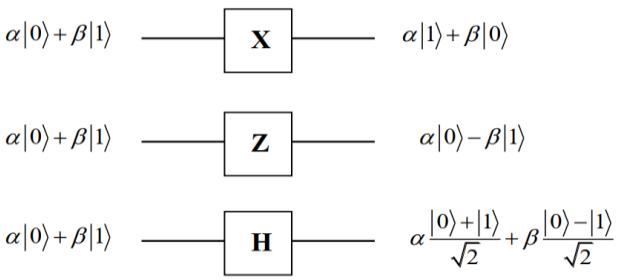


Рис. 5. Однокубітні квантові елементи та їхня дія на квантовий стан

Фотон як кубіт. Різні фізичні сутності можуть бути використані як кубіти, включаючи іони, надпровідні заряди, спін атомного ядра тощо. Фотони мають деякі властивості, які роблять їх надзвичайно привабливими для використання в КК та для створення квантових каналів зв'язку. Існують різні властивості фотонів, які дозволяють їх використовувати як кубіти.

1) Двоканальні кубіти (dual-rail qubits). Фотони рухаються по прямій. Отже, якщо обрано два шляхи руху і покладено фотон на будь-який з них, залежно від того, на якому шляху виявлений фотон, ми можемо сказати стосовно квантового стану фотону $|0\rangle$ або $|1\rangle$ відповідно. На рисунку 6 зображено двоканальний кубіт [6; 10].

Двоканальний фотонний кубіт на рисунку 6. Залежно від того, в якому каналі знаходиться фотон, стан кубіту є $|0\rangle$ або $|1\rangle$.

Рис. 6. Однокубітні квантові елементи та їхня дія на квантовий стан

Поляризаційний кубіт. Виходить, що площина вібрації електричного поля може бути під будь-яким кутом, незалежним від напрямку поширення світла (якщо воно перпендикулярне напрямку розповсюдження у 3 вимірах). Отже, електричне поле може приймати будь-який напрямок у двовимірному просторі. Цей двовимірний простір може бути представлений основою, що складається з горизонтальної поляризації $\langle HH|$ та вертикальної поляризації $\langle VV|$. Тоді будь-який інший напрямок можна записати як суперпозицію цих двох.

Виявлення фотону. Життя фотона в квантовому експерименті починається з його генерації і закінчується його виявленням. Обидва процеси повинні бути ефективними, а їхні продуктивність та властивості відіграють важливу роль у фотонних квантових обчисленнях.

Генерування фотонів. Наявність виняткових детекторів малокорисна, якщо неможливо ефективно зробити високоякісні фотони, на яких можна кодувати кубіти. Однак справді детерміновані високоякісні джерела фотонів розробляються з використанням різноманітних фізичних систем, таких як захоплені іони та атоми, кольорові центри в діамантах, напівпровідники, квантові точки та інші, більш екзотичні методи. Деякі з них покладаються на використання єдиного випромінювача, який, в принципі, природно забезпечує однофотонну емісію на вимогу, тоді як інші, такі як атомний ансамбль та параметричні нелінійні процеси, вимагають сигналів попередження та перемикання, щоб зробити їх такими.

Керування фотоном. Існує точний та детальний контроль поляризації фотона, траєкторії або статичного значення часу, що завжди був силою ФКО. Сучасні електрооптичні елементи, такі як Покелс-комірки або інтегровані електрооптичні модулятори, дозволяють швидко переключати поляризацію, достатньо чітко виконувати тести Белла з локалізацією та закритими лазівками свободи вибору або перемикати просторовий режим для цілей мультиплексування джерел. Ефективні способи для маніпулювання, такі як частота або поперечні просторові режими, також є в розробці, включаючи методи, що передають інформацію від одного ступеня свободи до іншого, наприклад, поляризацію до просторового поперечного режиму, дискретних змінних до безперервної змінної, перетворення частоти тощо.

Квантові помилки. Реальні системи страждають від небажаної взаємодії з зовнішнім світом. Ці небажані взаємодії виявляються як шум в квантовій системі обробки інформації. Потрібно розуміти та контролювати такі шумові процеси та квантові помилки при побудові квантових систем обробки інформації.

*Квантова декогерентність***.** Здається, що квантові обчислення з кожним днем стають дедалі прогресивнішими. Кубіти стають чистішими, ворота покращуються, а алгоритми ускладняються. Очевидно, лише питання часу, коли квантові обчислення стануть основною технологією. Однак залишається велика перешкода, яка потребуватиме величезних зусиль для подолання, – декогерентність.

Квантова корекція помилок. Протоколи квантової корекції помилок відіграють центральну роль у реалізації квантових обчислень; вибір коду виправлення помилок вплине на весь стек квантових обчислень, починаючи з макета кубітів на фізичному рівні для створення стратегій компіляції на програмному рівні. Як такий, знайомство з квантовим кодуванням є важливою передумовою розуміння поточної та майбутньої архітектур квантових обчислень.

Від класичної до квантової корекції помилок. Наприклад, припустимо, ми хочемо передати біт з одного місця в інше через шумний класичний канал зв'язку. Ефект шуму в каналі полягає в перевертанні біт, що передається з імовірністю p>0, тоді як з імовірністю 1 – p біт передається без помилок. Такий канал відомий як двійковий симетричний канал (рис. 7). Простий засіб захисту від впливу шуму у двійковому симетричному каналі має замінити біт, який ми хочемо захистити, трьома копіями себе [6; 10].

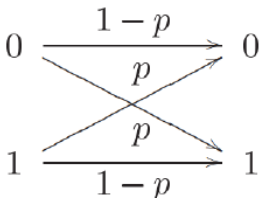


Рис. 7. Бінарний симетричний канал

Припустимо, ми кодуємо єдиний кубітовий стан $\alpha|0\rangle + \beta|1\rangle$ в три кубіти таким способом: $\alpha|000\rangle + \beta|111\rangle$. Зручний шлях запису цього шифрування є таким:

$$|0\rangle \rightarrow |0LL\rangle \equiv |000\rangle,$$
$$|1\rangle \rightarrow |1LL\rangle \equiv |111\rangle,$$

де розуміється, що суперпозиції базових станів беруться за відповідні суперпозиції закодованих станів. Позначення $|0LL\rangle$ та $|1LL\rangle$ вказують на те, що це логічний $|0\rangle$ та логічний $|1\rangle$ стани, а не фізичний нуль та один стан. Схема виконання цього кодування показано на рисунку 8.

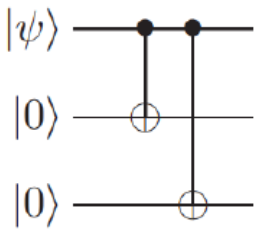


Рис. 8. Схема кодування для трикубітного бітового фліп-коду

Дані, що кодуються, надходять у схему на верхню лінію.

Види квантових помилок. Внаслідок оцифрування помилки існує два основні типи квантових помилок, які потрібно враховувати квантовими кодами. Помилки типу Паулі X

можна вважати квантовими біт-фліпс (bit-flips), які мають наступну відповідність $X|0\rangle=|1\rangle$ та $X|1\rangle=|0\rangle$. Дія X-помилки на загальний стан кубіта є:

$$X|\varphi\rangle=\alpha X|0\rangle+ \beta X|1\rangle= \alpha|1\rangle+ \beta|0\rangle.$$

Другий тип квантової помилки, Z-помилку, часто називають фазовим відхиленням і який не має класичного аналога. Фазове відхилення відображення базису кубітів $Z|0\rangle=|0\rangle$ та $Z|1\rangle=-|1\rangle$, а отже, має наступну дію на загальний стан кубіта:

$$Z|\varphi\rangle=\alpha Z|0\rangle+ \beta Z|1\rangle= \alpha|0\rangle-\beta|1\rangle.$$

Наразі для простоти я обмежив обговорення когерентними помилками, що діють на одиничні кубіти. Однак, оцифровка результату помилки узагальнює до довільних процесів квантових помилок, включаючи ті, які описують некогерентну еволюцію квантового стану в результаті взаємодії кубітів з оточуючим їх середовищем.

Квантові алгоритми.

Будь-яку класичну схему можна замінити еквівалентною схемою, що містить лише оборотні (реверсивні) елементи, використовуючи реверсивні ворота, відомі як ворота Тоффолі. Ворота Тоффолі має три вхідні біти та три вихідні біти, як показано на рисунку 9 [6; 10].

Входи			Виходи		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

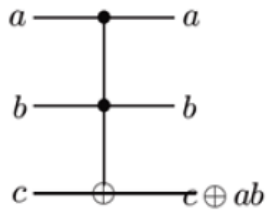


Рис. 9. Таблиця істинності для елемента Тоффолі та його схемна реалізація

Два біти є контрольними бітами, на які не впливає дія воріт Тоффолі. Третій біт – ціль біт, який перевертається, якщо для обох контрольних бітів встановлено значення 1, а в іншому випадку залишається в спокої. Зауважте, що застосування два рази Тоффолі двічі до набору бітів має ефект (a, b, c) → (a, b, c ⊕ ab) → (a, b, c), і, отже, ворота Тоффолі є реверсивними воротами.

Ворота Тоффолі можна використовувати для імітації NAND-воріт, як показано на рисунку 10.

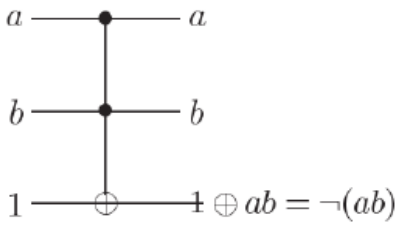


Рис. 10. Таблиця істинності для елемента Тоффолі та його схемна реалізація

Другий біт є вхідним сигналом до FANOUT (і два інших біти стандартних станів допоміжних елементів), а вихід FANOUT з’являється на другому і третьому бітах, що відображено на рисунку 11.

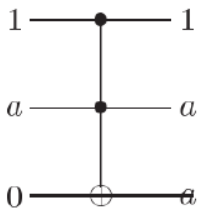


Рис. 11. FANOUT на основі воріт Тоффолі

Перевага квантових обчислень полягає в тому, що можуть бути обчисленими набагато потужніші функції за допомогою кубітів і квантових воріт.

Квантовий паралелізм. Квантовий паралелізм є фундаментальною особливістю багатьох квантових алгоритмів. Квантовий паралелізм дозволяє КК оцінити функцію *f (x)* для багатьох різних значень *x* одночасно.

Припустимо, *f (x)*: {0, 1} → {0, 1} – це функція з однобітовим доменом та діапазоном. Зручним способом обчислення цієї функції на КК є розгляд двокубітового КК, який запускається у стані $|x,y\rangle$. З відповідною послідовністю логічних воріт можна перетворити цей стан в $|x,y \oplus f(x)\rangle$, де $\oplus$ вказує додавання за модулем 2; перший регістр називається регістром даних, а другий – цільовим регістром. Дамо перетворення, визначене відображенням $|x,y\rangle \rightarrow |x,y \oplus f(x)\rangle$ а ім'я, Uf, і зауважте, що це легко виявляється унітарним. Якщо $y = 0$, то кінцевий стан другого кубіта – це лише значення *f (x)*. Для наших цілей це можна вважати таким чорний ящик, як зображено на рисунку 12.

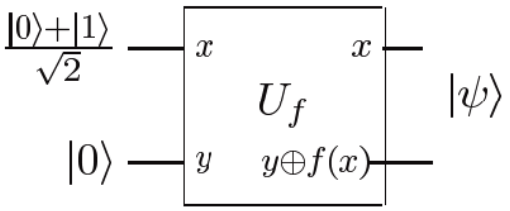


Рис. 12. Квантова схема для розрахунку *f(0), f(1)* одночасно. Uf квантова схема, яка трансформує входи, такі як $|x,y\rangle$ до $|x,y \oplus f(x)\rangle$

Як вихід, $HH\otimes 2$ слугує для позначення паралельної дії двох воріт Адамара і '$\otimes$' читається як тензор. Більш загальним результатом виконання перетворення Адамара над *n* кубітами спочатку у всіх станах $|0\rangle$ є

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle,$$

де сума перевищує всі можливі значення *x*, і для позначення цієї дії ми пишемо $HH\otimes$n. Тобто перетворення Адамара виробляє рівну суперпозицію всіх обчислювальних базових станів. Більше того, він робить це надзвичайно ефективно, створюючи суперпозицію 2^n станів, використовуючи лише *n* воріт.

На рисунку 13 зображена квантова схема для перетворення Адамара $HH\otimes 2$ на двох кубітах.

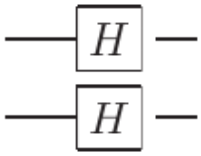


Рис. 13. Перетворення Адамара $HH\otimes 2$ на двох кубітах

Пошук в базі даних. Прикладом ефективного квантового алгоритму є алгоритм пошуку інформації в невпорядкованій базі даних, іноді ще названий алгоритмом перебору. Алгоритм вирішення наступної достатньо простої задачі: даний неупорядкований набір з N предметів, знайти номер предмету, який співпадає з даним зразком. Класичний метод послідовного порівняння зразку зі всіма предметами потребує в середньому $N/2$ порівнянь. Запропонований Гровером квантово-механічний алгоритм потребує порядку $\sqrt{N}$ кроків [6; 10].

Ми повинні якось розрізняти потрібний елемент за номером j від усіх інших. Використовуємо сконструйований унітарний оператор порівняння S, котрий діє як тотожній на непотрібні елементи та міняє фазу у потрібного:

$$S|i\rangle = |i\rangle \text{ при } i \neq j \text{ та } S|j\rangle = -|j\rangle.$$

Візьмемо квантовий регістр, достатньо довгий, щоб число його станів перевищувало N. Переведемо його в «універсальний» стан, в котрому всі можливі стани регістра присутні з рівними амплітудами. Позначимо амплітуду виділеного стану a, звичайного – b. Якщо стан регістру для стислості позначити парою цих амплітуд, можна описати первісний стан як

$$|a, b\rangle = a|j\rangle + b\sum_{i \neq j}|j\rangle,$$

де за умовою нормування $a2+(N-1)b2=1$. У первісному стані $a=b=1/\sqrt{N}$. Застосуємо до цього стану складне перетворення UG, котре визначене наступним способом: спочатку перетворення S, потім перетворення Фурьє, зміна знака у всіх компонент за виключенням $|0\rangle$, зворотне перетворення Фурьє. Можна показати, що це перетворення призводить до наступного результату:

$$U_G|a, b\rangle = |\frac{2N-2}{N}b + \frac{N-2}{N}a, \frac{N-2}{N}b - \frac{2}{N}a\rangle.$$

Коефіцієнт при виділеному елементі став дещо більше, ніж при інших. Фактично виконаний певний поворот у просторі в направленні чистого стану $|j\rangle$. Далі ми застосовуємо перетворення UG m разів, де $m \approx (\pi/4)\sqrt{N}$. При цьому первісний стан наближується до чистого $|j$. Залишається тільки заміряти його.

Але практична користь даного методу велика. Це насправді є універсальний алгоритм перебору. Існує багато задач, у котрих знайти відповідь не просто, а перевірити, що рішення правильне – просто. Яскравим прикладом є підбір пароля до зашифрованих даних. Будь-яку таку задачу можна вирішувати повним перебором методу Гровера – перевірку правильності рішення можна вставити в алгоритм порівняння S.

Розробка програм та запуск на КК. В якості практичної частини була розроблена програма, яка демонструє принцип дії елемента Адамара, логічного вентиля Паулі X та операції порівняння. У ході програми задіяно два кубіти: до одного з котрих задіяний елемент Адамара, а до іншого – вентиль Паулі X, який спрацьовує при істинному значенні (квантовий стан $|1\rangle$) першого кубіту, який завдяки дії елемента Адамара знаходиться в суперпозиції. У такий спосіб утворюється квантова заплутаність, коли квантовий стан одного кубіта впливає на стан іншого [10].

Програма була запущена на класичному комп’ютері, використовуючи спеціальне програмне забезпечення, яке імітує КК. Також відбувся запуск програми на справжньому КК компанії IBM, який територіально знаходиться в Мельбурні. Цікавим фактом сьогодення дійсного КК є те, що для запуску програми потрібно зайняти чергу [10].

Програмне забезпечення. В якості програмного забезпечення використовувалось Qiskit. Qiskit – це програмне забезпечення з відкритим кодом для роботи з КК на рівні схем, імпульсів та алгоритмів. Крім того, поверх цього основного модуля існує кілька API додатків для конкретного домену [10].

Основна мета Qiskit – створити стек програмного забезпечення, який дає змогу користування КК кожному, незалежно від рівня їхньої кваліфікації або сфери інтересів. Qiskit дозволяє легко розробляти експерименти та програми та запускати їх на реальних КК або класичних тренажерах. Qiskit підтримує Python 3.6 або новіші версії.

Використовувалась Qiskit версії 0.26.2. Офіційний сайт: https://qiskit.org.

Код програми. Першим кроком є підключення необхідних модулів з бібліотеки qiskit:

```
from qiskit import *
```

Далі необхідно вказати необхідну кількість кубітів, яка буде використовуватись в системі, в нашому випадку це два кубіти. Робиться так:

```
qr = QuantumRegister(2) ,
```

де змінна qr – це змінна, яка є масивом, що містить два об’єкти класу кубітів. Наступним кроком є вказання необхідної кількості класичних бітів, оскільки вимір стану кубіта – це є процес перенесення стану кубіта на класичний біт. Відповідно, в нашому випадку необхідною кількістю класичних бітів є два:

```
cr = ClassicalRegister(2)
```

Далі треба «зібрати» квантову схему:

```
circ = QuantumCircuit(qr, cr)
```

Для того, щоб впевнитись, що ми маємо необхідну кількість кубітів та бітів в схемі, ми можемо скористатись наступними командами:

```
%matplotlib inline
circ.draw()
```

Результатом роботи функції draw() є вивід в консоль поточної схеми (рис. 14). Як можна побачити зі схеми, наразі ми маємо два кубіти та два класичних біти, що відповідає дійсності.

```
q0_0:

q0_1:

c0: 2/
```

Рис. 14. Результат в консолі після команди circ.draw()

Наступним кроком є створення елемента Адамара, який буде діяти на перший кубіт:

```
circ.h(qr[0])
circ.draw(output='mpl')
```

На рисунку 15 можна побачити поточний стан схем з елементом Адамара.

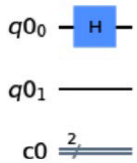


Рис. 15. Проміжна схема, застосування елемента Адамара

Наступним кроком є застосування вентиля Паулі X на другому кубіті та логічне порівняння, яке застосовує вентиль Паулі X тільки в тому випадку, коли перший кубіт знаходиться в істинному логічному стані. Відповідно створюємо квантову заплутаність.

```
circ.cx(qr[0], qr[1])
circ.draw(output='mpl')
```

Проміжна схема виглядає так (рис. 16):

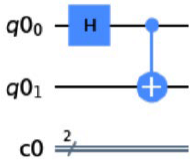


Рис. 16. Проміжна схема, застосування вентиля Паулі X

Передостаннім важливим кроком є вимірювання квантових станів. Реалізується це наступним способом. По суті, це процес копіювання квантового стану кубіту у класичний стан біту.

```
circ.measure(qr, cr)
circ.draw(output='mpl')
```

На рисунку 17 можна побачити кінцеву схему.

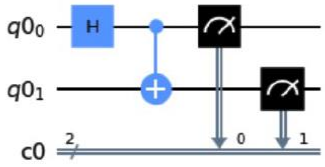


Рис. 17. Кінцева схема програми

Фінальним кроком є запуск програми. Для початку запустимо програму на симуляторі КК:

```
simulator = Aer.get_backend('qasm_simulator')
result = execute(circ, backend = simulator).result()
```

Щоб графічно побачити результати, підключаємо необхідну бібліотеку та виводимо результати:

```
from qiskit.tools.visualization import plot_histogram
plot_histogram(result.get_counts(circ))
```

На рисунку 18 можна побачити результат програми.

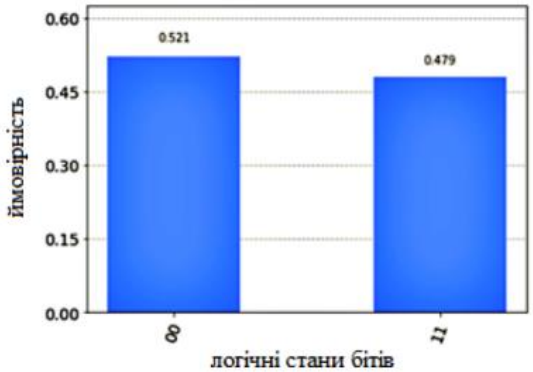


Рис. 18. Результат програми на класичному комп’ютері

Тепер запустимо програму на дійсному КК IBM. Для цього, в першу чергу, необхідно загрузити дані свого акаунта, який був попередньо створений на IBM Quantum (офіційний сайт: https://quantum-computing.ibm.com), та вказати, на якому конкретному комп’ютері ми хочемо запустити програму.

```
IBMQ.load_account()
provider = IBMQ.get_provider('ibm-q')
qcomp = provider.get_backend('ibmq_16_melbourne')
job = execute(circ, backend=qcomp)
```

Для того щоб відслідковувати стан своєї черги, підключаємо наступну бібліотеку та виведемо наш номер в черзі.

```
from qiskit.tools.monitor import job_monitor
job_monitor(job)
```

Отримуємо повідомлення в консолі, що наша програма є під 36-м номером у черзі.

```
Job Status: job is queued (36)
```

Почекавши в черзі 4 години, отримуємо результат виконання програми, як зображено на рисунку 19.

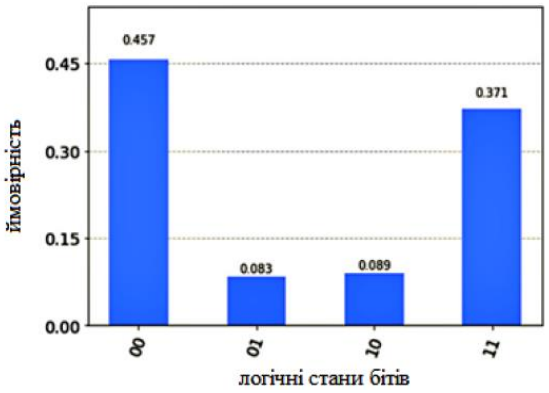


Рис.19. Результат програми на справжньому КК

Аналіз отриманих результатів. Отримані результати підтверджують, що нинішній КК (запуск відбувався на комп'ютері IBM, який використовує електрони як кубіти) має певні погрішності, пов'язані з квантовими помилками та декогерентністю. Комп'ютер, який буде розроблений на фотонній системі, матиме меншу погрішність та стане більш доступним у використанні.

Нами вивчено основні логічні квантові елементи, проблеми декогерентності та квантових помилок, основні квантові алгоритми та зроблено їх порівняння з класичними. Проаналізовано та досліджено особливості використання фотону як кубіта, його переваги та недоліки.

Однак переваги, які має фотон, дають йому дуже велику перспективу бути використаним як кубіт в КК [10].

Висновки

1. Логічно припустити, що величезний стрибок в КТ призведе до вагомих наслідків, а саме:

створення КК з величезною кубітовою обчислювальною перевагою над звичайними бітовими;

найближчим часом здійсниться практична реалізації КЗ та квантової телепортації, квантового (захищеного) Інтернету та реалізація алгоритмів квантового розподілення ключів;

створення КТ загрожує сучасним стандартам шифрування даних.

2. Революційний розвиток КТ може призвести до ситуації типу «Енігма», коли Британія таємно зламала «надійну» систему шифрування зв'язку німецького командування та таємно використовувала цю інформацію, не повідомляючи про це навіть союзникам.

3. Використання КТ призведе до надзвичайної інформаційної переваги того, хто першим ними оволодіє. Тому підрозділам ВЗ та КБ доцільно будувати відповідні засоби, алгоритми та сценарії дій з урахуванням тактики постквантового періоду [11].

4. Наразі відомі компанії починають надавати в аренду робочий час на квантових системах. Це відкриває шляхи для застосування КТ у різноманітних наукових дослідженнях. Відповідно виникає необхідність вирішити наступні питання:

завчасно перейти до постквантових алгоритмів;

здійснити серію тестових перевірок існуючих кодів;

створити або взяти участь у використанні фрагментів КЗ.

У подальшому автори планують приступити до вивчення інструментарію, необхідного при створенні алгоритмів і методів квантових обчислень для їх практичного використання на квантових машинах.

5. У подальшому можливо проведення складних розрахунків в інтересах військових досліджень, які можливо запускати на КК, час роботи на яких можливо орендувати в компаніях IBM, Intel, Google та ін.

6. Необхідно поступово долучатись до використання захищеного КЗ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Китай створив квантові комп'ютери у 10 млн разів потужніше суперкомп'ютера // URL: https://https://focus.ua/digital/496363-v-kitae-sozdali-kvantovye-kompyutery-v-10-mln-raz-moshchnee-lyubogo-superkompyuter (дата звернення: 16.09.2022).

2. Це справжня телепортація. Вченим вперше вдалося передати інформацію квантовою мережею // URL: https://techno.nv.ua/ukr/innovations/kvantoviy-internet-50246228.html (дата звернення: 10.09.2022).

3. Квантові комп'ютери // URL: https://phm.cuspu.edu.ua/nauka/naukovo-populiarni-publikatsii/1026-kvantovi-kompyutery-mriya-chy-realnist (дата звернення: 14.09.2022).

4. Квантовий комп'ютер – нова ера на порозі // URL: https://nrfu.org.ua/news/kvantovyj-kompyuter-nova-era-na-porozi (дата звернення: 15.09.2022).

5. Квантово-фармакологічні дослідження властивостей антиоксидантів як лікарських засобів // URL: https://www.umj.com.ua/article/75175/kvantovo-farmakologichni-doslidzhennya-vlastivostej-antioksidantiv-yak-likarskix-zasobiv (дата звернення: 15.09.2022).

6. Остапов С. Е., Добровольський Ю. Г. Квантова інформатика та квантові обчислення: навч. посіб. Чернівці: ЧНУ, 2021. 99 с.

7. Квантово-фармакологічні дослідження властивостей антиоксидантів як лікарських засобів // URL: https://comsys.kpi.ua/upload/Комп'ютерне_моделювання (дата звернення: 10.09.2022).

8. Комп'ютерне моделювання // URL: https://www.umj.com.ua/article/75175/kvantovo-farmakologichni-doslidzhennya-vlastivostej-antioksidantiv-yak-likarskix-zasobiv (дата звернення: 15.09.2022).

8. П'ять технологічних трендів, які врятують людство // URL: https://techno.nv.ua/ukr/ technoblogs/novi-tehnologiji-50127580.html (дата звернення: 15.09.2022).

9. Квантові комп'ютери: що це, як працюють, які перспективи // URL: https://blog.allo.ua/
ua/kvantovi-komp-yuteri-shho-tse-yak-pratsyuyut-yaki-perspektivi_2018-07-39/ (дата звернення: 15.09.2022).

10. Філоненко Є. О. Фотонні системи з однокубітними квантовими обчисленнями. Київ: Кафедра мікроелектроніки НТУ України «КПІ імені Ігоря Сікорського». Факультет електроніки, 2021.

11. Горбенко І. Д., Качко О. Г., Кузнєцов О. О., Потій О. В., Горбенко Ю. І., Пономар В. А., Єсіна М. В. Проблеми створення стандартів перспективних криптографічних перетворень та хід їх вирішення // Доповідь на конференції ВІТІ, 2018 р. URL: https://iit.com.ua.

12. Карлаш Г. Ю. Квантові інформаційні системи: навч. посіб. для спеціальності «Прикладна фізика та наноматеріали». Київ: факультет радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, 2018. 77 с.

УДК 621.3

д-р техн. наук Кузавков В. В. (ВІТІ ім. Героїв Крут)
Михайлюк С. С. (ВІТІ ім. Героїв Крут)
Погребняк С. В. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ПАРАМЕТРІВ НАДІЙНОСТІ ОБ'ЄКТІВ РАДІОЕЛЕКТРОННОЇ ТЕХНІКИ З НАДЛИШКОВІСТЮ

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

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

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

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

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

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

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

Постановка завдання

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

Аналіз останніх публікацій

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

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

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

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

Виклад основного матеріалу

Найбільш повною характеристикою будь-якої складної технічної системи є її якість – сукупність властивостей, які обумовлюють її придатність задовольняти певні потреби

відповідно до свого призначення протягом установленого часу. Цю сукупність властивостей можна умовно розбити на дві групи характеристик:

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

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

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

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

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

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

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

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

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

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

У поняття складної системи зазвичай вкладають такий зміст:

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

елементи складної системи функціонують у взаємодії один з одним;

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

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

Забезпечення надійності складних технічних систем являє собою єдиний процес, що охоплює всі основні етапи їхнього життєвого циклу. Отже, забезпечення високої надійності

складних технічних систем – це комплексна проблема, що охоплює широке коло наукових (математичних, фізико-технічних, біологічних), інженерних (проєктно-конструкторських, експлуатаційних) й економічних аспектів. Рішення цієї проблеми пов'язане з реалізацією численних організаційних і технічних, а часто і фундаментальних наукових досліджень, що вимагають великих витрат часу та коштів і дотичних різних галузей науки, техніки та народного господарства.

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

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

Резервування – спосіб забезпечення надійності об'єкта завдяки використанню надмірності.

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

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

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

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

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

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

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

Для того щоб властивості надійності можна було «вимірювати» (оцінювати), введено кількісні показники надійності – кількісні характеристики одного або декількох властивостей, які визначають надійність. Розрізняють одиничні показники надійності, які

характеризують одну із властивостей, і комплексні показники, які характеризують кілька властивостей, що визначають надійність об'єкта.

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

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

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

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

Імовірність протилежної події є *імовірність відмови*

$$F(t) = Імов\{t_н < t\}.$$

Очевидно, що $P(t) + F(t) = 1$, де $F(t)$ – інтегральна функція розподілу випадкової величини $t_н$.

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

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

звідки знаходимо:

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

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

Відповідно до визначення:

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

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

$$T_0 = \int_0^\infty t f(t)\,dt. \qquad (1)$$

Провівши інтегрування в (1) за частинами, отримаємо:

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

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

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

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

n – математичне сподівання числа відмов протягом сумарного напрацювання.

Властивість ремонтопридатності об'єктів прийнято «вимірювати» часом приведення об'єкта в працездатний стан – часом відновлення $t_в$, що є випадковою величиною. Тому

показники ремонтопридатності використовують такі самі імовірнісні характеристики, як і у випадку безвідмовності, а саме: $F_{в}(t)$ – імовірність відновлення у заданий час; $f_{в}(t)$ – щільність розподілу часу відновлення; $\mu(t)$ – інтенсивність відновлення; $T_{в}$ – середній час відновлення.

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

$$F_{в}(t) = Імов\{t_{в} \le t\}.$$

Так само як і $F(t)$, $F_{в}(t)$ – це функція розподілу випадкової величини $t_{в}$. Імовірність невідновлення в заданий час:

$$Імов\{t_{в} > t\} = 1 - F_{в}(t).$$

За аналогією зі щільністю $f(t)$ щільність розподілу часу відновлення $F_{в}(t)$ виражається формулою:

$$f_{в}(t) = \frac{dF_{в}(t)}{dt}.$$

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

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

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

$$T_{в} = \int_{0}^{\infty} t f_{в}(t) dt = \int_{0}^{\infty} [1 - F_{в}(t)]\, dt.$$

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

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

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

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

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

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

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

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

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

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

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

Розглянуті вище комплексні показники $K_{\text{г}}$ і $K_{\text{тв}}$ є характеристиками надійності, усередненими для тривалого періоду експлуатації. У багатьох випадках цього виявляється недостатньо, тому що виникає необхідність оцінки можливості виконання об'єктом деякої задачі (функції), що вимагає безперервної безвідмовної роботи об'єкта протягом заданого часу. Для оцінки такої можливості введено показник – коефіцієнт оперативної готовності.

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

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

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

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

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

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

Висновки

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

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

ЛІТЕРАТУРА

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

УДК 621.396.981

Лазута Р. Р. (ВІТІ ім. Героїв Крут)
Зінченко М. О. (ВІТІ ім. Героїв Крут)
Руденко В. І. (ВІТІ ім. Героїв Крут)
Шкіцький Д. В. (УІТ МОУ)

ПРОПОЗИЦІЇ З ОРГАНІЗАЦІЇ КОСМІЧНОЇ ПІДТРИМКИ ЗБРОЙНИХ СИЛ УКРАЇНИ ЗА СТАНДАРТАМИ НАТО

У країнах-членах НАТО функція космічної підтримки полягає у забезпеченні виконання завдань особовим складом штабу, який буде виконувати функції радників командувачів з питань космічної підтримки операцій на стратегічному та оперативному рівнях.

Головним напрямком створення системи космічної підтримки у Збройних силах України є удосконалення системи й оптимізація структури космічної діяльності у Міністерстві оборони України та Збройних силах України, розвиток організаційно-технічних структур (систем), застосування (використання) космічної техніки та технологій відповідно до стандартів НАТО.

Реалізація запропонованого передбачає розроблення, впровадження та розвиток нової моделі космічної діяльності в сфері безпеки і оборони, особливо в Міністерстві оборони України та Збройних силах України відповідно до сучасних умов та національних інтересів, шляхом формування інфраструктури космічної підтримки операцій (бойових дій) угруповань військ (сил) Збройних сил України на основі розподілу відповідальності підрозділів Міністерства оборони України та Збройних сил України за космічну діяльність у сфері безпеки і оборони та космічну підтримку, а також порядку їх взаємодії під час запровадження в органах військового управління (військового командування) стандартних процедур космічної підтримки операцій (бойових дій) з урахуванням вітчизняного досвіду космічної діяльності у сфері оборони, досвіду проведення Антитерористичної операції та Операції об'єднаних сил.

Отже, впровадження розглянутих пропозицій надасть змогу побудувати єдину адаптовану систему використання спроможностей космосу у сфері безпеки і оборони України, що збільшить область використання продуктів та послуг космічної діяльності у повсякденній діяльності та під час планування операцій (бойових) дій.

Ключові слова: *космічна діяльність, космічна підтримка, космічна техніка.*

R. Lazuta, M. Zinchenko, V. Rudenko, D. Shkitskyi Proposals for the organization of space support of the Armed Forces of Ukraine according to NATO standards.

In NATO member countries, the space support function is to provide mission support to the staff of the headquarters, which will act as advisers to commanders on matters of space support for operations at the strategic and operational levels.

The main direction of creating a space support system in the Armed Forces of Ukraine is the improvement of the system and optimization of the structure of space activities in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, the development of organizational and technical structures (systems), the use (use) of space technology and technologies in accordance with NATO standards.

The implementation of the proposed provides for the development, implementation and development of a new model of space activities in the field of security and defense, especially in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine in accordance with modern conditions and national interests, by forming the infrastructure for space support of operations (combat operations) of groupings of troops (forces) of the Armed Forces of Ukraine on the basis of the distribution of responsibility of the units of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine for space activities in the field of security and defense and space support, as well as the procedure for their interaction when introducing standard procedures for space support of operations (combat) actions) on the basis of domestic experience in space activities in the field of defense, the experience of conducting the Anti-Terrorist Operation and the Joint Forces Operation.

Thus, the implementation of the considered proposals will make it possible to build a single adapted system for using space capabilities in the field of security and defense of Ukraine, which will increase the area of using products and services of space activities in daily activities and in planning operations (combat) actions.

Keywords: *space activities, space support, space technology.*

Постановка завдання

Основою досягнення переваги над противником у сучасних збройних конфліктах є технологічна перевага та збільшення інформаційної складової забезпечення операцій

(бойових дій). Тому у збройних силах багатьох країн світу значний акцент робиться на розвиток та застосування космічних систем і засобів.

Космос є середовищем, яке надає можливості здійснення як глобального видового та радіоелектронного спостереження поверхні Землі й приземного простору, так і глобального передавання різнорідної інформації без порушення норм міжнародного права. Космічні системи розвідки, раннього попередження, навігації, зв'язку і бойового управління військами та зброєю, топогеодезичного і гідрометеорологічного забезпечення є основою створення глобального інформаційного поля, яке рівною мірою ефективно може використовуватись як вищими органами воєнно-політичного керівництва держави, так і командирами безпосередньо на полі бою.

Основними чинниками підвищення ефективності виконання завдань у сфері оборони шляхом застосування космічної техніки є значне посилення основних спроможностей (оперативних, бойових, спеціальних) сил оборони щодо організації керівництва та управління різнорідними силами, підтримки готовності військ, розвідки, розгортання та мобільності військ, їх застосування, забезпечення, захисту та живучості.

Космічна діяльність – це наукові космічні дослідження для використання космічного простору, розроблення, виробництво, ремонт та технічне обслуговування, випробування, експлуатація, управління об'єктами космічної діяльності (у тому числі їхніми агрегатами та складовими частинами), забезпечення запуску, запуск та повернення космічних апаратів, їхніх складових частин із космічного простору на Землю.

Наявна система космічної діяльності та космічної підтримки в Збройних силах України (далі – ЗС України) не повною мірою відповідає сучасності, а також сумісності з системою космічної підтримки НАТО.

Аналіз останніх досліджень і публікацій

Аналіз останніх досліджень і публікацій фахівців України та країн-членів НАТО у сфері космічних систем військового та подвійного призначення говорить про важливість використання космічних систем не тільки у воєнній сфері, а й у сферах безпеки і оборони в цілому, особливо проглядається підвищена увага до можливого застосування космічних систем у військових цілях не тільки у напрямку інформаційного забезпечення, а й у напрямку проведення оборонних та ударних дій [1–4].

Метою статті є розробка пропозицій щодо космічної підтримки ЗС України за стандартами НАТО.

Виклад основного матеріалу

В країнах-членах НАТО функція космічної підтримки полягає у забезпеченні виконання завдань особовим складом штабу, який буде виконувати функції радників командувачів з питань космічної підтримки операцій.

Космічна підтримка здійснює [5]:

планування, впровадження, координацію та організацію реалізації можливостей видів космічного забезпечення (космічної діяльності) під час планування операцій та дій військ;

експертну оцінку з можливості надання видами космічного забезпечення космічних продуктів та послуг штабам та підлеглим військам.

Космічна підтримка не дублює функції видів космічного забезпечення. Вона лише надає та отримує дані щодо можливості видів космічного забезпечення з метою збільшення ефективності планування та проведення операцій за рахунок продуктів та послуг космічної діяльності (рис. 1) [5].

Космічна підтримка в НАТО складається зі стратегічного та оперативного рівнів.

Космічна підтримка стратегічного рівня зосереджена на створенні умов для проведення операцій космічної підтримки [5].

Космічна підтримка стратегічного рівня відповідає за просування пропозицій щодо розподілу ресурсів видів космічного забезпечення військ та визначення необхідного рівня

нарощування спроможностей для забезпечення всього спектру операцій. Ця функція несе відповідальність за встановлення процедур запиту та надання космічних продуктів та послуг, що надаються кожною окремою країною, а також встановлення формальних угод для забезпечення відповідного доступу. Космічна підтримка стратегічного рівня надає загальні керівні вказівки та здійснює координацію щодо планування та проведення операцій завдяки продуктам та послугам космічної діяльності.

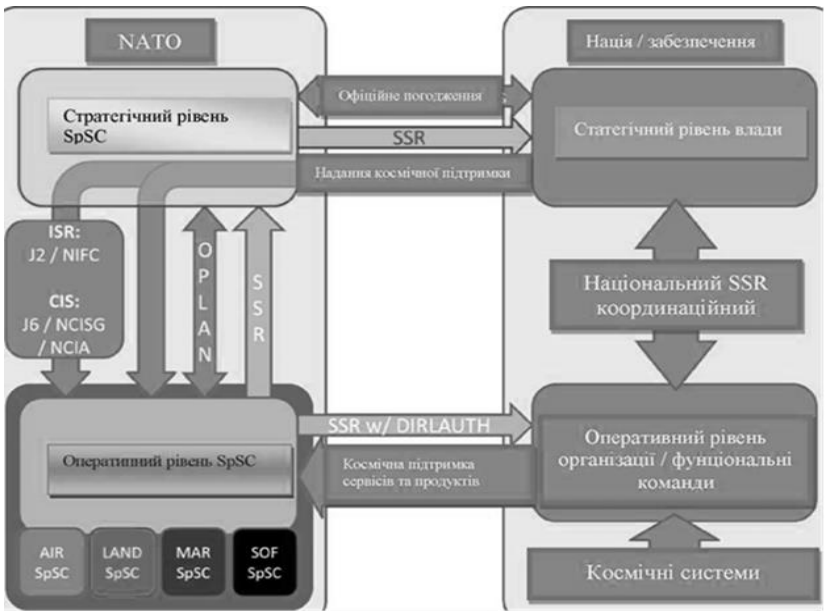


Рис. 1. Організація космічної підтримки у НАТО

Також, космічна підтримка стратегічного рівня забезпечує організацію та координацію з питань навчання, підготовки кадрів та підлеглих органів щодо виконання функцій, завдань та обов'язків, пов'язаних із космосом.

Під час планування операцій космічна підтримка стратегічного рівня залучається до участі в процесі визначення сил і спроможностей, які будуть надаватися постачальниками для залучення в операції, з метою використання необхідних космічних продуктів і послуг.

Космічна підтримка оперативного рівня зосереджується на безпосередній космічній підтримці поточних операцій, користуючись заздалегідь визначеними процесами та наявними космічними спроможностями, продуктами та послугами.

Космічна підтримка оперативного рівня як штабна функція повинна знати та відстежувати спроможності відповідних космічних систем, своєчасно надавати рекомендації щодо можливих варіантів їх застосування.

Функція космічної підтримки оперативного рівня полягає у збиранні, аналізі та обробці запитів на надання космічних продуктів та послуг за допомогою встановлених механізмів. Крім того, космічна підтримка оперативного рівня визначає пріоритет надання космічних продуктів і послуг.

Під час проведення планування операцій аспекти космічної підтримки повинні враховуватись на всіх його етапах.

Визначення вимог до космічної підтримки є частиною розробки стратегічного та оперативного замислу операції. Це реалізується в запитах до космічної підтримки та у створенні відповідного додатку до плану операції, що включає космічну специфіку [6].

Розробка стратегічного плану містить етап формування угруповання сил, де вимоги до космічної підтримки будуть представлені видам космічного забезпечення. Види космічного забезпечення повинні надати плануючу інформацію щодо послуг, продуктів, процедур

доступу та способів налагодження контактів для здійснення планування та проведення операції. Забезпечення космічної підтримки операції та театру воєнних дій вимагає розширеної та активної координації між користувачами та видами космічного забезпечення. Космічна підтримка операцій інтегрована та розгорнута в системи планування операцій. Відповідальний за космічну підтримку бере участь в оперативному плануванні у штабі, як правило, це офіцер з космічної підтримки. Роль офіцера (групи) з космічної підтримки полягає в тому, щоб допомогти командувачу і персоналу оцінити потреби операції у космічних продуктах та послугах з метою організації їх надання. Зазначене включає в себе підтримку операції з точки зору забезпечення космічними продуктами та послугами, на етапі планування та проведення від стратегічного до тактичного рівнів. Завдання офіцера (групи) з космічної підтримки можуть перетинатись із завданнями інших посадових осіб, особливо в J2 (управлінням розвідки), J3 (оперативним управлінням), J5 (управлінням планування) і J6 (управлінням зв'язку), але до функцій офіцера (групи) з космічної підтримки відносяться питання з організації взаємодії джерел космічного забезпечення та споживачів з метою якісного надання та отримання космічних продуктів та послуг.

До основних завдань офіцера (групи) космічної підтримки відносяться:[6].

впровадження та удосконалення підтримки, яка повинна бути своєчасною і оперативною;

забезпечення визначення пріоритетів та надання продуктів і послуг від об'єктів космічної діяльності для досягнення цілей операції;

розуміння координації та взаємодії при здійсненні інформаційного забезпечення даними від об'єктів космічної діяльності;

підтримка ситуаційної обізнаності в межах операції;

надання допомоги персоналу у створенні елементів, пов'язаних з забезпеченням даними від об'єктів космічної діяльності в зоні дій;

координація з планувальниками радіоелектронної боротьби, щоб уникнути негативного впливу на мирне використання космосу;

дослідження впливу електромагнітних перешкод на космічну продукцію та послуги;

координація з J3 і J6;

підтримка заходів щодо відновлення та пошуку персоналу;

розробка заходів з ефективності забезпечення космічними продуктами та послугами планування та проведення операції;

моніторинг використання противником космічних систем та надання пропозицій щодо його обмеження;

визначення критичних космічних продуктів та послуг у проведенні операції та розробка переліку заходів у разі погіршення або втрати зазначених продуктів та послуг;

вивчення особливостей бойового складу та участь у підготовці відповідного особового складу;

налагодження координації з J2, J3, J5 і J6, координація співробітників з питань використання космічних продуктів та послуг;

координація з метеорологічним персоналом щодо впливу космічної/земної погоди на забезпечення даними від об'єктів космічної діяльності;

співпраця з J6 щодо встановлення пріоритетності пропускної здатності супутника на основі пріоритету операції;

консультація персоналу про потенційні негативні впливи, пов'язані з космосом;

розвиток/вдосконалення фахових навичок із забезпечення даними від об'єктів космічної діяльності;

визначення та проведення планових звітів щодо ефективності космічних засобів, а також щодо інших проблем, що виникли під час виконання завдання;

отримання даних про завдання. Визначення, впливу космічних умов на успішне виконання завдання і акцентування уваги на моменти, де можуть виникнути ризики;

участь у розробці стратегій та планів;

здійснення моніторингу поточних операцій;

отримання даних про противника (Як відреагує противник? Яка в нього реакція, сили та засоби? Як він буде досягати своїх цілей? Чи працює ваша розвідка над встановленням способу використання космосу противником і як він може перешкоджати використанню космосу вами?);

отримання даних про загрози: загрози можуть бути природними або антропогенними. Знання загроз сприяє адекватній оцінці успішності операції;

отримання даних про системи озброєння. Потрібно знати склад і кількість наземних сил й те, як вони діють в космосі. Діяти в рамках виконання завдання та знати процедуру запиту на додаткові сили та засоби. Навчитись правильно використовувати космічні сили та засоби в рамках військових угрупувань різних військ та родів військ.

Перелік питань, яких офіцер (група) космічної підтримки повинен уникати, якщо інші члени штабу відповідальні за виконання та здатні виконувати наступні завдання [7]:

не збирати інформацію відповідно до задач космічних засобів, спостереження та розвідки, проте надавати інформацію особі, що є відповідальною за збір розвідувальної інформації щодо наявності та можливості використання об’єктів космічної діяльності для спеціальних цілей;

не використовувати неналежні супутникові частоти, проте допомагати в цьому відділу управління військами (J6). Допомагати J6 у створенні матриці пріоритезації користувача та розробці кризового плану дій в умовах обмеженої кількості наявних частот. Допомагати J6 в оцінці проблем з точки зору оператора космічного засобу, в той час як працівники J6, зазвичай, розглядають проблему з точки зору комунікаторів;

не розробляти звіти з погодної обстановки, проте сприяти діяльності штабних метеорологів. Пересвідчуватись в тому, що штабні метеорологи знають свої обов’язки щодо доведення відомостей про зміни погодних умов та їхній прогноз, а також в тому, що вони мають для цього всі необхідні ресурси;

не координувати ведення боротьби у сфері навігаційних засобів (навігаційна війна), якщо це вже здійснюється за планами РЕБ.

Враховуючи вищезазначене, головними напрямками створення системи космічної підтримки у ЗС України є:

удосконалення системи й оптимізація структури космічної діяльності у Міністерстві оборони України (далі – МО України) та ЗС України;

розвиток організаційно-технічних структур (систем);

застосування (використання) космічної техніки та технологій відповідно до стандартів НАТО.

Реалізація запропонованого передбачає розроблення, впровадження та розвиток нової моделі космічної діяльності в сфері безпеки і оборони, особливо в МО України та ЗС України відповідно до сучасних умов та національних інтересів, шляхом формування інфраструктури космічної підтримки операцій (бойових дій) угруповань військ (сил) ЗС України на основі розподілу відповідальності підрозділів МО України та ЗС України за космічну діяльність в сфері безпеки і оборони та космічну підтримку, а також порядку їх взаємодії під час запровадження в органах військового управління (військового командування) стандартних процедур космічної підтримки операцій (бойових дій) з урахуванням вітчизняного досвіду космічної діяльності у сфері оборони, досвіду проведення Антитерористичної операції та Операції об’єднаних сил.

Для вирішення завдань з організації космічної діяльності та космічної підтримки (управління, контролю, координації, взаємодії, забезпечення тощо) у сфері оборони,

створення та застосування (використання) космічної техніки, формування та використання даних від об'єктів космічної діяльності (космічних продуктів) і космічних послуг, контролю їхньої якості, забезпечення визначених точності, достовірності та оперативності, зазначений варіант передбачає створення (удосконалення) відповідних організаційних структур (визначення посадових осіб), а саме:

у складі МО України – структурного підрозділу, безпосередньо підпорядкованого МО України із функцією відповідальності за космічну діяльність у сфері безпеки і оборони України та космічну підтримку стратегічного рівня з організації та координації космічної діяльності в МО України та ЗС України;

у складі Генерального штабу Збройних сил України (далі – ГШ ЗС України) – системи космічної підтримки частково стратегічного рівня та оперативного рівня для забезпечення космічними послугами з функцією збору, аналізу та обробки потреби (запитів) у космічних послугах структурних підрозділів ЗС України та вживання заходів щодо їх надання за видами космічного забезпечення: дистанційне зондування Землі (космічна розвідка ISR), контроль та аналіз космічної обстановки (космічна ситуаційна обізнаність SSA), супутниковий зв'язок (SATCOM), координато-часове та навігаційне забезпечення (PNT), спеціальний контроль та сейсмічний моніторинг (метеорологія та океанографія METOC);

у визначених органах військового управління та командуваннях ЗС України – фахівців з космічної підтримки оперативного рівня для виконання завдань із організації з забезпечення космічними послугами та продуктами (офіцерів з космічної підтримки).

Відповідно може передбачатись:

створення структурного підрозділу, безпосередньо підпорядкованого МО України із функцією космічної підтримки стратегічного рівня, організації та координації космічної діяльності в МО України та ЗС України;

створення структурного підрозділу (групи) космічної підтримки стратегічного рівня у складі ГШ ЗС України;

розроблення проєктів нормативно-правових актів держави, що формують єдину нормативну базу космічної діяльності у сфері оборони України;

обґрунтування місця, ролі та змісту космічної підтримки та діяльності при формуванні концептуальних засад оперативних стандартів підготовки, розробленні (уточненні) настанов, керівництв, бойових статутів та інших документів системи стандартів для ЗС України та інших складових сил оборони відповідно до процедур та стандартів НАТО;

розроблення нормативних правових актів, які визначають цілі, завдання, повноваження та відповідальність суб'єктів космічної діяльності у сфері оборони України з організації та/або проведення наукових космічних досліджень, порядок, процедури створення та застосування (використання) об'єктів космічної діяльності, використання космічного простору;

планування формування заходів із провадження космічної діяльності у сфері оборони України;

розвиток (впровадження) у вищих військових навчальних закладах (підрозділах), навчальних центрах ЗС України відповідних навчальних дисциплін (курсів) із питань космічної діяльності (відповідно до потреб МО України та ЗС України);

наукові дослідження в області космічної підтримки (діяльності) у МО України та ЗС України;

розвиток системи підготовки фахівців тактичного і оперативного рівнів за спеціалізаціями, що відносяться до космічної діяльності;

формування державного замовлення на підготовку та підвищення кваліфікації фахівців космічної діяльності у МО України та ЗС України;

визначення спеціальностей, спеціалізацій, освітніх (освітньо-професійних, освітньо-наукових) стандартів вищої освіти і стандартів підготовки, що формують цілісну освітню систему в області космічної діяльності МО України та ЗС України;

визначення базових вищих військових навчальних закладів, що здійснюють підготовку та підвищення кваліфікації фахівців за пріоритетними функціональними областями використання космічної техніки (технологій), забезпечення даними від об'єктів космічної діяльності МО України та ЗС України (за замовленням від зацікавлених структурних підрозділів).

До основних заходів зі створення системи космічної підтримки стратегічного рівня можуть відноситись:

створення структурного підрозділу із функцією космічної підтримки стратегічного рівня з організації та координації космічної діяльності в МО України;

удосконалення координації космічної діяльності в інтересах МО України та ЗС України, удосконалення нормативно-правової бази з космічної діяльності у МО України та ЗС України;

розвиток наукових досліджень в області космічної діяльності щодо створення космічної техніки і технологій, її оперативного впровадження у зразки ОВТ, розвиток форм і способів її застосування в МО України та ЗС України;

створення у складі ГШ ЗС України системи космічної підтримки стратегічного рівня;

організація підготовки військових фахівців із космічної підтримки.

Враховуючи зазначене, доцільно створити відділ космічної діяльності з функцією космічної підтримки стратегічного рівня у складі МО України, на реалізацію завдань (9.3.3) Каталогу спроможностей МО України.

До організаційно-штатної структури відділу космічної діяльності з функцією космічної підтримки стратегічного рівня доцільно включити:

начальника відділу;

заступника начальника відділу;

старшого офіцера (за напрямком ДЗЗ та КСО);

старшого офіцера (за напрямком супутникового зв'язку, координато-часового та навігаційного забезпечення, спеціального контролю та сейсмічного моніторингу);

офіцера (за напрямком ДЗЗ та КСО);

офіцера (за напрямком супутникового зв'язку, координато-часового та навігаційного забезпечення, спеціального контролю та сейсмічного моніторингу).

До основних завдань відділу космічної діяльності з функцією космічної підтримки стратегічного рівня доцільно віднести:

здійснення космічної діяльності у сфері оборони та національної безпеки України;

розробку концептуальних основ державної космічної політики та Загальнодержавної цільової науково-технічної космічної програми України в частині, пов'язаній зі створенням та використанням космічної техніки військового призначення, а також разом із центральним органом виконавчої влади, що забезпечує формування державної політики у сфері космічної діяльності – космічної техніки подвійного призначення;

виконання, разом з відповідними міністерствами та іншими центральними органами виконавчої влади, Загальнодержавної цільової науково-технічної космічної програми України в частині, що стосується створення та використання космічної техніки військового та подвійного призначення;

формування та організація виконання замовлень на роботи, пов'язані зі створенням і використанням космічної техніки військового, а також разом із центральним органом виконавчої влади, що реалізує державну політику у сфері космічної діяльності – космічної техніки подвійного призначення на основі Загальнодержавної цільової науково-технічної космічної програми України;

регламентування використання космічної техніки у сфері оборони України;

забезпечення разом із центральним органом виконавчої влади, що реалізує державну політику у сфері космічної діяльності, функціонування і розвиток об'єктів наземної та космічної інфраструктури;

участь у здійсненні сертифікації космічної техніки військового призначення;

провадження відповідно до законодавства України космічної діяльності у сфері оборони та національної безпеки України;

формування військово-технічної політики з питань, віднесених до компетенції відділу;

організацію виконання Конституції і законів України, актів Президента України, Верховної Ради України, Кабінету Міністрів України, наказів МО України, інших центральних органів виконавчої влади в межах компетенції відділу, здійснення контролю за їх реалізацією;

здійснення підготовки інформаційно-аналітичних матеріалів для інформування Президента України, Верховної Ради України, Кабінету Міністрів України та Ради національної безпеки і оборони України щодо космічної підтримки МО України та ЗС України;

подання пропозицій до державних цільових програм та участь у їх погодженні, підготовці до затвердження та моніторингу їх виконання;

підготовку та подання пропозицій щодо уточнення переліку завдань і заходів: загальнодержавної цільової науково-технічної космічної програми; державної програми розвитку ЗС України; державної програми розвитку озброєння та військової техніки;

участь у проведенні оборонного огляду в МО України та ЗС України;

координування діяльності структурних підрозділів, підпорядкованих МО України та ГШ ЗС України, органів військового управління, установ та організацій МО України та ЗС України з питань космічної підтримки у сфері безпеки і оборони;

визначення напрямків здійснення наукової та науково-технічної діяльності, проведення фундаментальних і пошукових досліджень з питань космічної діяльності;

участь у розробленні та визначенні порядку застосування стандартів для задоволення потреб оборони України за напрямом космічної діяльності;

підготовка пропозицій до бюджетного запиту на виконання заходів з питань космічної діяльності;

організація розроблення та подання в установленому порядку на затвердження проєктів рішень на відкриття (закриття), технічних вимог, технічних завдань на виконання науково-дослідних та дослідно-конструкторських робіт, здійснення контролю за їх виконанням (безпосередньо та через військові представництва МО України) з питань космічної діяльності;

подання пропозицій до плану міжнародного співробітництва МО України та участь в організації міжнародного оборонного співробітництва, підготовці заходів міжнародного оборонного співробітництва з питань космічної діяльності у сфері безпеки і оборони за участю МО України та його заступників;

організація розроблення та впровадження космічних технологій у воєнній сфері, сфері оборони і військового будівництва.

На перших етапах зазначеному відділу необхідно врегулювати нормативно-правову базу держави, що формує єдину нормативну базу космічної діяльності у сфері оборони України, та організувати розроблення нормативно-правової бази з космічної підтримки стратегічного та оперативного рівнів.

Пропозиції щодо першочергових нормативно-правових актів з організації космічної діяльності в сфері безпеки і оборони та космічної підтримки стратегічного та оперативного рівнів зазначені у таблиці 1.

Таблиця 1

Пропозиції щодо першочергових нормативно-правових актів

№ з/п	Назва нормативно-правового акту	Заходи
1	Указ Президента України «Про державну космічну політику України»	Ініціювати розроблення зазначеного Указу та участь на рівні співвиконавця та погрожуючого центрального органу виконавчої влади. В положеннях Указу чітко визначити цілі та заходи розвитку космічної підтримки сектору безпеки та оборони
2	Указ Президента України «Про стратегію національної безпеки України»	Внесення змін щодо визначення ролі та місця космічної діяльності України в системі безпеки і оборони держави
3	Указ Президента України «Про Стратегічний оборонний бюлетень»	Внесення змін щодо розвитку та впровадження космічної діяльності України в системі безпеки і оборони та космічної безпеки держави
4	Указ Президента України «Про затвердження Положення про взаємодію МО України та ДКА України при здійсненні космічної діяльності»	Враховуючи те, що розробник ДКАУ протягом 20 років зміг затвердити тільки зміни у діюче тимчасове положення, пропонується ініціювати перед Кабінетом Міністрів України передачу розробки та затвердження зазначеного указу МОУ
5	Закон України «Про космічну діяльність»	Внести зміни щодо питань космічної діяльності в сфері безпеки і оборони відповідно до вимог сьогодення, особливо з гармонізації розподілу повноважень та сфер відповідальності в сфері космічної діяльності сектору безпеки і оборони
6	Наказ МО України «Про космічну політику МО України та ЗС України»	Розробити проєкт документа з урахуванням вже затверджених законодавчих та нормативних актів із впровадження та реалізації космічної політики та стратегії України в секторі безпеки і оборони. Визначити напрямки та порядок впровадження космічної підтримки в МО України та ЗС України
7	Наказ МО України «Космічні операції»	Розробити проєкт документа з врахуванням стандартів НАТО та вимоги до перспективної створюваної системи космічної підтримки ЗС України
8	Міжвідомчі накази щодо організації, координації та обміну космічними продуктами та послугами	Розробити проєкти документів з врахуванням досвіду, стандартів НАТО та вимоги до перспективної створюваної системи космічної підтримки ЗС України
9	Інструкції та порядки з забезпечення космічної підтримки оперативно-тактичного рівня	Розробити проєкти документів з врахуванням досвіду, стандартів НАТО та вимоги до перспективної створюваної системи космічної підтримки ЗС України

Формування та розвиток системи космічної підтримки оперативно-тактичного рівня операцій (бойових дій) ЗС України може полягати у:

створенні посади офіцера з космічної підтримки оперативно-тактичного рівня для організації забезпечення космічними послугами та продуктами з функцією збору, аналізу та обробки потреби (запитів) у космічних послугах структурних підрозділів ЗС України та здійснення заходів щодо їх надання за видами космічного забезпечення;

впровадженні в діяльність органів військового управління, військових командувань та видів ЗС України офіцера з космічної підтримки під час планування та проведення операцій (бойових дій) відповідно до стандартів НАТО;

використанні програмно-технічних комплексів із забезпечення даними від об’єктів космічної діяльності під час планування та проведення операцій (бойових дій) ЗС України;

використанні інструкцій та протоколів з космічної підтримки під час планування та проведення операцій (бойових дій) ЗС України.

Відповідно, до основних функцій офіцера з космічної підтримки доцільно віднести:

організацію та розвиток оперативності системи космічної підтримки операцій ЗС України;

організацію отримання споживачами (J2, J3, J5, J6 та ін.) космічних продуктів та послуг від видів космічного забезпечення пріоритетом, який визначив командувач;

знання інструкцій, порядків та методик з організації інформаційної взаємодії між споживачами та об'єктами космічної діяльності;

проведення моніторингу щодо стану використання споживачами космічних продуктів та послуг при плануванні та проведенні операцій (бойових дій) ЗС України;

оцінку космічної обстановки;

підготовку пропозицій щодо залучення космічних послуг та продуктів для планування та проведення операцій (бойових дій) ЗС України;

організацію надання космічної інформації та послуг командирам різних ланок управління з рекомендаціями стосовно їх використання;

надання консультаційної допомоги споживачам у використанні космічних послуг та продуктів;

здійснення координації з групами з планування застосування засобів РЕБ з метою запобігання перешкоджанню мирному використанню космосу;

вивчення впливу електромагнітних перешкод на отримання космічної продукції та послуг;

координацію з J3 і J6;

організацію надання відповідним споживачам інформації про заплановані та незаплановані збої в роботі об'єктів космічної діяльності та їхній можливий вплив на планування та проведення операції ЗС України;

організацію заходів щодо відновлення персоналу з космічного забезпечення;

розробку пропозицій до замислу, рішення та плану командувача з відповідними показниками ефективності використання космічних продуктів та послуг під час проведення операції;

знання стану використання противником об'єктів космічної діяльності, його можливий вплив на отримання даних від видів космічного забезпечення та розробка пропозицій щодо протидії;

визначення критично важливих для виконання операцій (бойових дій) ЗС України космічних послуг і продуктів та планування заходів щодо їхньої стійкості та живучості;

налагодження та підтримка взаємодії зі споживачами та постійна координація їх щодо спроможності видів космічного забезпечення;

постійний моніторинг метеорологічних даних щодо впливу космічної/земної погоди на забезпечення даними від об'єктів космічної діяльності;

взаємодію з J6 щодо питань супутникового зв'язку;

організацію технічного обслуговування засобів та систем космічної підтримки операцій (бойових дій) ЗС України;

розвиток/вдосконалення фахових навичок з питань космічної підтримки та видів космічного забезпечення;

формування доповіді щодо ефективності космічної підтримки та роботи видів космічного забезпечення, а також щодо інших проблем, що виникли під час проведення операції (бойових дій) ЗС України. Такі матеріали можуть бути використані під час аналізу та підбиття підсумків проведення операції;

знання завдання на проведення операції (бойових дій) ЗС України з метою визначення впливу космічних продуктів та послуг на успішне виконання завдання та звернення уваги на впливи, які можуть сприяти появі відповідних ризиків;

участь у розробці планів;

здійснення моніторингу поточних операцій (бойових) дій ЗС України;

кваліфіковане використання космічних систем та засобів у рамках військових угрупувань різних видів та родів військ.

Відповідно, офіцер космічної підтримки бере участь у плануванні операції та вносить пропозиції командувачу до Плану операції.

Отже, космічна підтримка є частиною стратегічної та оперативної оцінки ситуації та здійснює свій внесок у всебічну підготовку операційного середовища.

Потенційно стратегічна перевага ЗС України багато в чому залежіть від спроможностей та вразливостей космічної підтримки та космічного забезпечення, відповідно, вони повинні враховуватись під час повсякденної діяльності та плануванні операцій (бойових дій).

Спроможності системи космічної підтримки та космічного забезпечення повинні використовуватись під час аналізу центрів тяжіння, на всіх етапах планування та розробки варіантів проведення операцій.

Висновки з даного дослідження та перспективи подальших досліджень у даному напрямку

Запропоновані пропозиції нададуть змогу:

забезпечити формування системи управління космічною діяльністю та космічною підтримкою стратегічного та оперативного рівня у МО України та ЗС України, організацію та розвиток взаємодії і міжвідомчої координації при вирішенні завдань (виконанні заходів), підвищення відповідальності та ефективності застосування (використання) космічної техніки, використання космічного простору для забезпечення виконання завдань МО України та ЗС України, формування і провадження заходів космічної діяльності;

забезпечити фахове та ефективне застосування (використання) сучасної космічної техніки, використання спеціальної космічної інформації (космічних продуктів) і космічних послуг відповідно до вимог МО України та ЗС України;

забезпечити формування єдиної воєнно-космічної науково-педагогічної школи, підготовку фахівців за визначеними спеціальностями та спеціалізаціями відповідно до вимог МО України та ЗС України;

забезпечити автоматизоване отримання космічних продуктів та послуг визначеної точності, достовірності та оперативності, достатніх для прийняття своєчасних і обґрунтованих рішень, ефективного управління військами (силами) та застосування зброї органами військового управління та військового командування, угрупуваннями військ (сил) ЗС України.

Впровадження пропозицій надасть змогу побудувати єдину адаптовану систему використання спроможностей космосу у сфері безпеки і оборони України, що збільшить область використання продуктів та послуг космічної діяльності у повсякденній діяльності та під час планування операцій (бойових) дій.

Подібні системи космічної підтримки створені та діють у НАТО та її країнах-членах. На сьогодні зазначені країни створюють системи, які забезпечують підтримку та реалізацію космічних операцій або проведення операцій у космосі, але це є наступний етап розвитку космічної діяльності та космічної підтримки у сфері безпеки та оборони [7–9], який нашій державі не досягти без створення основи для застосування своїх космічних спроможностей і інтеграції з космічними спроможностями НАТО та інших союзницьких сил за єдиними принципами та стандартами.

ЛІТЕРАТУРА

1. Анисенко О. В. Розвиток космічної галузі в Україні / О. В. Анисенко, Д. О. Бабіна // Агросвіт. 2018. № 11. С. 55–59.

2. JAPCC Filling the Vacuum – A Framework for a NATO Space Policy 2012 // NATO. URL: https://fas.org.

3. Міністри оборони НАТО схвалили нову космічну політику, 14.10.2011 р. (NATO Defence Ministers approve new space policy, discuss readiness and mission in Afghanistan, 27 Jun. 2019) // NATO – News. URL: https://www.nato.int.

4. Космос: найостанніший кордон НАТО, 18 березня 2020 р. // NATO. URL: https://www.nato.int/docu/review/uk/articles/2020/03/18/kosmos-najostannshij-kordon-nato/ index.html.

5. Угода НАТО із стандартизації AJP-3.3 «AlliedJointPublication-3.3 (AJP-3.3)», dated April 2016 // URL: https://www.japcc.org.

6. Статут СВ США FM 3-14 «Космічна підтримка операцій Сухопутних військ», 18.05.2005 (Field Manual 3-14 (FM 3-14): Space Support to Army Operations, 18 May 2005) // URL: https://fas.org.

7. Статут КНШ ЗС США JP 3-14 «Космічні операції», 29.05.2013 (Joint Publication 3-14 (JP 3-14): Space Operations, 29 May 2013) // URL: https://www.japcc.org.

8. Статут ВПС США AFDD 3-14 «Космічні операції», 19.06.2012 (Air Force Doctrine Document 3-14 (AFDD 3-14): Space Operations, 19 June 2012) // URL: https://www.e-publishing.af.mil.

9. Статут ВПС США AFDD 3-14.1 «Протикосмічні операції», 02.08.2004, зі змінами 28.07.2011 (Air Force Doctrine Document 3-14.1 (AFDD 3-14.1): Counter space Operations, 2 August 2004. Incorporating Change 1, 28 July 2011) // URL: https://www.e-publishing.af.mil.

УДК 004.75

Радченко М. М. (ВІТІ ім. Героїв Крут)
Драглюк О. В. (ВІТІ ім. Героїв Крут)
Дикий О. В. (ВІТІ ім. Героїв Крут)
Коротков М. М. (ВІТІ ім. Героїв Крут)
Павлюк Д. О. (ВІТІ ім. Героїв Крут)

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ VIRTUAL DESKTOP INFRASTRUCTURE В ІНФОРМАЦІЙНИХ ІНФРАСТРУКТУРАХ УЧАСНИКІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ

З метою виконання завдань Стратегій національної та воєнної безпеки України щодо забезпечення упровадження сучасних інформаційних технологій, автоматизації управлінських процесів і цифровізації діяльності в силах оборони України з відповідним рівнем захищеності інформації, що обробляється, проводяться заходи щодо приведення існуючої інформаційної інфраструктури до сучасних вимог.

Технічна компонента інформаційної інфраструктури органів управління учасників сектору безпеки та оборони зазвичай складається з наборів інформаційних та інформаційно-аналітичних систем, які різні за призначенням, але однакові за практичною реалізацією в технологіях «товстого» та «тонкого» клієнтів (термінального сервера) клієнт-серверних архітектур розгортання обчислювальних мереж. У статті коротко наведені їхні переваги та недоліки.

З огляду на те, що роль інформаційних технологій в системах управління полягає у забезпеченні досягнення показників достатньої якості управлінських рішень службовими особами органів управління, а точніше: в розв'язанні протиріччя між зростаючими складністю, розмірністю, динамічністю задач управління – з одного боку, і зростаючими вимогами до оперативності, раціональності, обґрунтованості, результативності цих рішень – з іншого боку, то перебудова інформаційної інфраструктури повинна ґрунтуватися на завідомо доказаних світовою практикою у своїй ефективності технологіях.

Логічним продовженням розвитку технології термінального сервера є віртуалізація робочих столів (Virtual Desktop Infrastructure – VDI). На думку авторів статті, створення віртуальних робочих станцій за робочими місцями службових осіб органів управління учасників сектору безпеки та оборони – це один зі шляхів забезпечення якісного виконання завдань службовими особами в інфраструктурі єдиного інформаційного середовища.

У статті наданий короткий огляд продуктів вендорів, які є світовими лідерами у наданні послуг з віртуалізації, функціонально-технічних можливостей VDI, обґрунтування та шляхи впровадження наведеної технології в діючу інформаційну інфраструктуру органів управління учасників сектору безпеки та оборони.

Застосування наведеної технології дозволить існуючій архітектурі набути низки переваг за наступними напрямами: підвищення ефективності централізованого управління та надання сервісів; підвищення безпеки інформації; гнучкість в роботі та реалізація масштабування; ефективне використання фінансів на підтримку і розвиток інформаційної інфраструктури; створення умов до переходу на хмарні технології.

Ключові слова: *інформаційна інфраструктура, віртуалізація робочих столів, інформаційна технологія.*

M. Radchenko, O. Draglyuk, O. Dykyi, M. Korotkov, D. Pavlyuk ***Application of Virtual Desktop Infrastructure technologies in information infrastructures of participants in the security and defense sector.***

In order to fulfill the tasks of the Strategies of National and Military Security of Ukraine to ensure the introduction of modern information technologies, automation of management processes and digitalization of activities in the defense forces of Ukraine with an appropriate level of information security, which is processed, measures are being taken to bring the existing information infrastructure to modern requirements.

The technical component of the information infrastructure of the security and defense sector actors usually consists of sets of information and information-analytical systems, which are different in purpose, but the same in practice in the technology of «thick» and «thin» clients (terminal server) client-server architectures deployment of computer networks. The article briefly lists their advantages and disadvantages.

Considering that the role of information technologies in management systems is to ensure the achievement of indicators of sufficient quality of management decisions by officials of management bodies, or rather: in solving the contradiction between the growing complexity, dimension, dynamism of management tasks - on the one hand, and growing requirements for efficiency, rationality, validity, effectiveness of their decisions, on the other hand, the restructuring of the information infrastructure should be based on the technology that has been obviously proven by world practice in its effectiveness.

A logical continuation of the development of terminal server technology is desktop virtualization (Virtual Desktop Infrastructure – VDI). According to the authors of the article, the creation of virtual workstations for the jobs

of officials of the governing bodies of the security and defense sector is one of the ways to ensure quality performance of tasks by officials in the infrastructure of a single information environment.

The article provides a brief overview of the products of vendors who are world leaders in providing virtualization services, VDI functionality and capabilities, rationale and ways to implement this technology in the existing information infrastructure of the security and defense sector.

The application of this technology will allow the existing architecture to gain a number of advantages in the following areas: improving the efficiency of centralized management and service delivery; improving information security; flexibility in work and implementation of scaling; effective use of finances to support and develop information infrastructure; creating conditions for the transition to cloud technologies.

Keywords: *information infrastructure, desktop virtualization, information technology.*

Постановка завдання у загальному вигляді

Реформування сфери безпеки і оборони за стандартами НАТО належить до найважливіших пріоритетів як зовнішньої, так і внутрішньої політики України. На ряду із іншими важливими заходами щодо вдосконалення систем управління, формування оборонних ресурсів і прийняття на озброєння нових зразків озброєння та військової техніки є створення сучасної інформаційної інфраструктури спеціального призначення. На законодавчому рівні підтримка цих процесів здійснюється низкою відповідних актів, в яких загострюється увага на завданнях відповідного характеру.

Для прикладу, відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» [1] (далі – Стратегія), одним із основних напрямків зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки є здійснення цифрової трансформації, забезпечення надання адміністративних послуг через безпечне «єдине вікно» з використанням сучасних інформаційних технологій, поширення цифрової грамотності, а також визначено основним завданням системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури в умовах цифрової трансформації.

В Стратегії наведені напрями та завдання реформування і розвитку сектору безпеки й оборони. У зв'язку з цим зазначено, що зміцнення бойового потенціалу ЗС України, інших складових сил оборони можливо здійснити такими сприятливими для розвитку інформаційно-телекомунікаційних технологій (далі – ІТ-технологій) шляхами, як:

удосконалення та розвиток на основі сучасних технологій систем управління, телекомунікацій, розвідки, логістики;

посилення взаємодії органів сектору безпеки і оборони у виконанні спільних завдань;

створення системи ефективного управління та координації діяльності органів сектору безпеки і оборони, удосконалення її архітектури;

завершення створення та формування сучасних спроможностей національної системи кібербезпеки, зміцнення системи суб'єктів забезпечення кібербезпеки і координації кібероборони.

В Стратегії воєнної безпеки України [2] – наступному документі розвитку воєнної складової безпеки країни – визначена мета забезпечення реалізації державної політики у сфері оборони та пріоритетні шляхи її реалізації у сфері оборони та військового будівництва. Досягнення цілей реалізації державної політики у воєнній сфері передбачається здійснити шляхом виконання завдань за пріоритетом – запровадження об'єднаного керівництва з підготовки та ведення всеохоплюючої оборони України, зокрема:

упровадження сучасних інформаційних та космічних технологій, автоматизація управлінських процесів і цифровізація діяльності в силах оборони України з відповідним рівнем захищеності інформації, що обробляється.

Вирішення наведених завдань потребує здійснення цілеспрямованих, скоординованих за термінами, обсягами ресурсного забезпечення заходів щодо приведення існуючої інформаційної інфраструктури до сучасних потреб.

Аналіз останніх досліджень і публікацій

Публікацій на тему перебудови інформаційної інфраструктури складових сил оборони з огляду на важливість питання існує достатня кількість. Нижче наведемо деякі з них.

Згідно з [3] реакція органів управління оборонного відомства України на зростаючі вимоги щодо оперативності надання інформації для прогнозування розвитку ситуацій і забезпечення оперативного управління характеризується інтенсивним впровадженням та використанням електронних систем, баз даних, реєстрів, архівів, аналітичних систем, систем моніторингу. У цьому процесі враховуються тенденції розвитку та використання інформаційних технологій в державному секторі. Автори [3], виходячи із фінансової доцільності та технологічної можливості, зазначають необхідність створення єдиної захищеної ІТ-структури оборонного відомства, яка забезпечить централізацію всіх існуючих в МО України та ЗС України інформаційних та інформаційно-аналітичних систем, програмних комплексів та баз даних на базі єдиної захищеної та катастрофостійкої технологічної платформи, основним елементом (ядром) в якій пропонується використання центру обробки даних (далі – ЦОД), що забезпечуватиме роботу єдиної масштабованої, високонадійної автоматизованої відомчої системи (рис. 1).

Автори [3] відмічають, що наявність такої платформи значно полегшить створення будь-яких проєктів у сфері інформатизації та оптимізує витрати на комплексну систему захисту інформації (далі – КСЗІ).

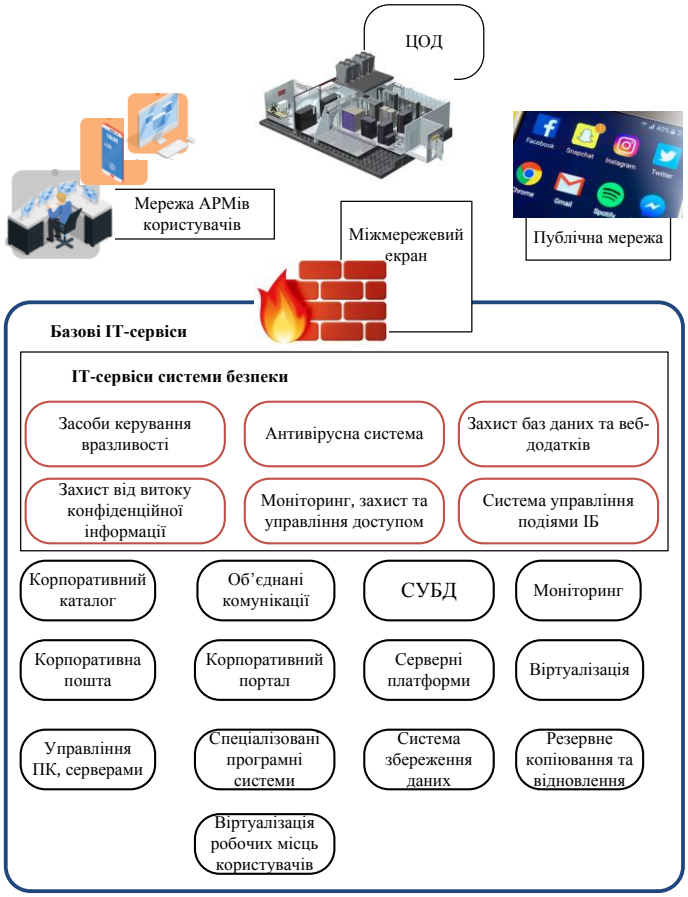


Рис. 1. Компоненти єдиної захищеної відомчої ІТ-структури

У статті [4] на прикладі оборонного відомства показано, що протягом тривалого часу в інформаційних інфраструктурах спеціального призначення створювались та розвивались окремі автоматизовані, інформаційні, інформаційно-аналітичні та інші програмні системи, які забезпечували інформаційну підтримку лише окремих функціональних процесів управління, що сформувало такі характеристики територіально розподіленої інформаційної інфраструктури оборонного відомства країни, як відокремленість та ізольованість її складових. Тому побудова інформаційної системи, яка функціонує у вигляді єдиної платформи та забезпечує прозоре управління функціональними процесами, гнучко адаптується під будь-які зміни, – є одним із пріоритетних завдань вдосконалення інформаційної інфраструктури не тільки ЗС України, але й складових сил оборони у цілому.

Оскільки роль інформаційних технологій в системах управління полягає у забезпеченні досягнення показників достатньої якості управлінських рішень службовими особами органів управління, а точніше: в розв'язанні протиріччя між зростаючими складністю, розмірністю, динамічністю задач управління – з одного боку, і зростаючими вимогами до оперативності, раціональності, обґрунтованості, результативності їхніх рішень – з іншого, то цілісна інформаційна інфраструктура має будуватися на досвіді впровадження передових інформаційних технологій, які показали свою ефективність.

Сфера застосування ІТ повинна охоплювати практично всі етапи і складові управлінської діяльності на макрорівні корпоративно-центричної моделі управління складових сил оборони, і на мікрорівні – застосування зброї чи засобів ураження і є системоутворюючим фактором сучасних процесів прийняття рішення, що дозволить досягнути якісно нового етапу розвитку воєнного мистецтва – переходу від управління військами в ході конфлікту до управління конфліктом у цілому [5].

Отже, робота щодо пошуку ефективних шляхів впровадження нових інформаційних технологій, які практикуються світовими ІТ-спільнотами, триває, тому автори цієї статті вважають актуальним дослідження прикладних застосувань технологій Virtual Desktop Infrastructure (далі – VDI) в інформаційних інфраструктурах складових сектору безпеки і оборони.

Метою роботи є аналіз функціонально-технологічних можливостей технології VDI та обґрунтування пропозицій щодо її застосування в інформаційних інфраструктурах складових сектору безпеки і оборони.

Виклад основного матеріалу

Виконання завдань, які забезпечуються локальними обчислювальними мережами органів управління (далі – ОУ) учасників сектору безпеки і оборони визначаються функціональними повноваженнями службових осіб, які, як наведено в [5] на прикладі оборонного відомства, виражаються у здійсненні:

процесів оперативного планування на етапі підготовки операцій (бойових дій) щодо розподілу особового складу органу військового управління по пунктах управління та розмежування доступу службових осіб до даних, які використовуються;

формування деталізованого переліку заходів (завдань), що виконуються службовими особами структурних підрозділів штабу на етапі підготовки операцій (бойових дій);

доведення запланованих завдань до службових осіб штабу та контроль їх виконання;

формування проєктів електронних документів щодо організації роботи штабу при плануванні операцій (бойових дій);

ведення спеціалізованого військового діловодства в ОУ – автоматизована розробка, пошук і відпрацювання бойових (оперативних) документів за напрямами всебічного забезпечення і логістики;

проведення оперативно-тактичних розрахунків та інформаційно-аналітичної підтримки прийняття рішень, де передують оцінки фізико-географічних умов регіону проведення

операцій (бойових дій), противника, розрахунки переміщення сил та засобів, визначення маршрутів прольоту армійської авіації тощо;

інформаційного обміну між користувачами та постачальниками інформації як в середині ОУ, так і ззовні (відповідно до категорій терміновості та прав доступу до них службових осіб, автоматизоване ведення адресних книг, журналів і формування звітної документації), реалізації вимог керівних документів щодо організації обміну інформацією;

геоінформаційного забезпечення службових осіб шляхом надійного доступу до просторових даних із поданням їх в наочній формі (електронна картографічна інформація про місцевість, автоматизація процесів створення, оновлення та підготовки до друку топографічних карт усього масштабного ряду, формування електронних карт різних масштабів, доведення до ОУ та військ (сил) електронної картографічної інформації про місцевість, об'єкти на ній, цифрових даних обстановки) та ін.

Очевидно, що робота службових осіб (далі – користувачів) в ОУ відбувається в умовах високої багатоаспектності та складності задач управління. Тому критично важливим стає забезпечення розроблення, впровадження та використання сучасних ІТ, починаючи з постановки завдань, визначення джерел отримання інформації, застосування математичних засобів інформаційно-аналітичної підтримки – до створення цілісної інформаційної інфраструктури складових сектору безпеки й оборони.

Відповідно, під кожен напрям діяльності створювались свої підсистеми автоматизованого управління, основою яких є клієнт-серверна архітектура розгортання. Як наведено в [3; 5], технічна компонента інформаційної інфраструктури ОУ може складатися із таких наборів інформаційних та інформаційно-аналітичних систем, які різні за призначенням, але однакові за принципами побудови технологічних платформ, як: підсистема організації роботи штабу, підсистема електронного документообігу, інформаційно-довідкова підсистема, інформаційно-розрахункова підсистема, підсистема інформаційного обміну, геоінформаційні системи, інформаційно-аналітична система автоматизованого обліку особового складу, інформаційно-аналітична система обліку майна (житла) та ін.

Коротко кажучи, традиційні клієнт-серверні архітектури розгортання обчислювальних мереж, в яких є сервери – вузли-постачальники деяких специфічних функцій (сервісів) і клієнти – споживачі цих функцій, у практичній реалізації набуті технологіями «товстого» та «тонкого» клієнтів. Кожна з них визначає власні або використовує наявні правила взаємодії між клієнтом і сервером (протоколами взаємодії). Переваги і недоліки наведених технологій розглянемо нижче.

1. Архітектура розгортання «товстий клієнт» (рис. 2).

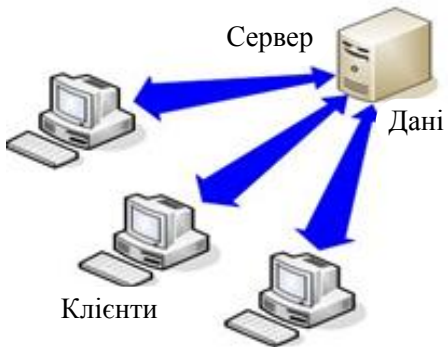


Рис. 2. «Товстий клієнт» – робоча станція або ПК, що працює під управлінням власної дискової ОС і має необхідний набір ПЗ

«Товстий клієнт» в архітектурі «клієнт – сервер» являє собою клієнтський мережевий додаток, запущений під керуванням локальної (дискової) операційної системи (далі – ОС), що забезпечує (на противагу «тонкому клієнтові») повну функціональність і незалежність від центрального сервера. При цьому можливе забезпечення роботи багатьом користувачам навіть при обривах зв'язку із сервером. Такий додаток поєднує компонент подання даних (графічний користувальницький інтерфейс ОС) і прикладний компонент (обчислювальні потужності комп'ютера клієнта). Часто сервер у цьому випадку є лише сховищем даних, а вся робота з обробки та подання даних переноситься на

персональний комп'ютер (далі – ПК) користувача. До мережевих серверів «товсті клієнти» звертаються в основному за додатковими послугами (наприклад, доступ до WEB-сервера чи до відомчої бази даних).

Переваги:

наділений широкою функціональністю на відміну від «тонкого клієнта»;

можливість автономної роботи навіть при обривах зв'язку із сервером;

висока швидкодія (залежить від технічних характеристик робочої станції користувача).

Недоліки:

ускладнене адміністрування прикладних функцій через відсутність централізації;

великий розмір дистрибутива;

проблеми з віддаленим доступом до даних, що виражаються у складності відновлення даних, узгодження їх з іншими клієнтами і пов'язаної з цим неактуальністю даних;

ресурсозатратне обслуговування робочих місць (установка, налаштування і супроводження життєвого циклу, необхідність оновлення ліцензійного програмного забезпечення (далі – ПЗ) та відповідного апаратного забезпечення, кібернетичного захисту на кожному робочому місці);

ускладнений і ресурсозатратний контроль виконання політики безпеки або збільшення її вартості при територіальному розосередженні підрозділів;

висока вартість виконання вимог КСЗІ при мобільному виконанні робочого місця чи здійсненні масштабування.

2. Архітектура термінальний сервер («тонкий клієнт») (рис. 3)**.**

Суть полягає в розміщенні додатків на одному сервері відразу для двох і більшої кількості користувачів. Користувачі отримують «хмарний» доступ до певних додатків і спеціалізованих програм. Клієнт лише виводить віддалений користувацький інтерфейс, що фізично розміщений на сервері.

У термінальному доступі всі співробітники отримують доступ до однієї ОС і одному набору додатків на всіх через відомчу мережу або Інтернет. (Наприклад, так працюють з програмою 1С-Підприємство).

Серверні обчислення із «тонким клієнтом» (SBC) або служба віддаленого робочого столу (RDS) дозволяють користувачу віддалено підключатися до програми, яка працює на серверній інфраструктурі, що розміщена у ЦОД. Далі доставка додатків здійснюється шляхом їх встановлення і запуску на самому сервері. В цьому випадку використовують багатокористувацьку версію програми, яка затребувана для створення окремих сеансів роботи користувачів. Кожен користувач підключається до власного окремого та захищеного сеансу цієї програми через свій термінал.

При термінальному доступі створюються окремі облікові записи всіх користувачів, які надають доступ до одночасної роботи в єдиній ОС так, щоб користувачі не створювали завад один одному. На клієнтські комп'ютери встановлюються спеціальні додатки, які дають користувачам можливість працювати з окремими сесіями на термінальному сервері. При цьому слід пам'ятати, що не всі виробники випускають програмні продукти, які здатні працювати в термінальному режимі, – у такому випадку немає можливості запускати будь-який додаток.

Основна функціональна можливість, яку надає термінальний сервер, – це віддалений доступ до додатків ОС, які встановлені на сервері. У користувача на пристрої повинна бути встановлена програма-клієнт, яка здійснює підключення терміналу до термінального сервера. Найпростіший приклад, програма «Підключення до віддаленого робочого столу», яка вбудована в будь-яку ОС Windows. Доступ може бути надано або до всього робочого столу, або до певного додатку, який відкривається у так званому безшовному вікні. У першому випадку на екрані користувача запуститься термінальна сесія, яка і «закриє» собою

поточний робочий стіл. У другому випадку для користувача не буде навіть помітно, що програма, яка запущена в окремому вікні, не з його ПК, а на сервері.

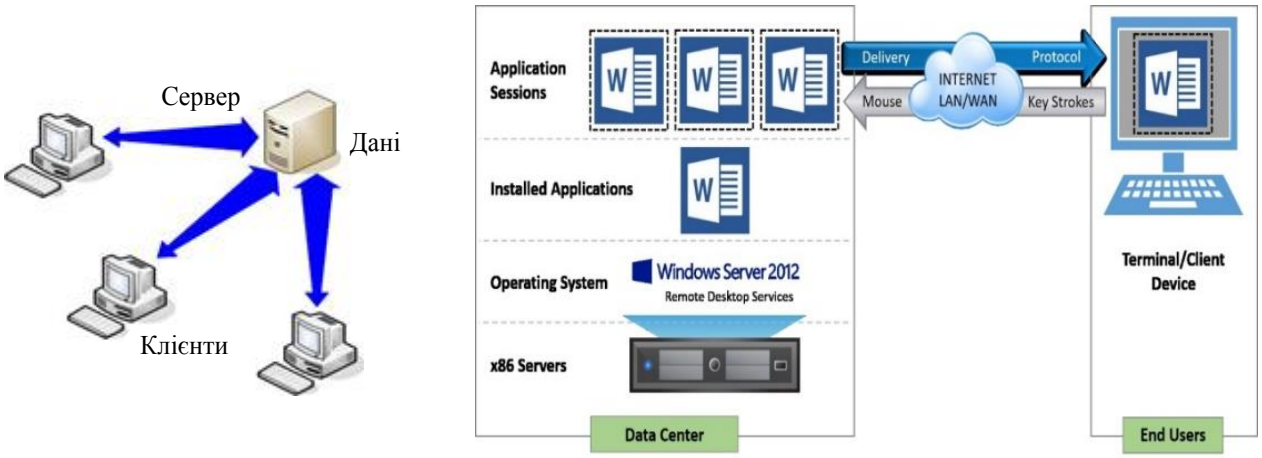


Рис. 3. Робота «тонкого клієнта» в сесії застосунку Word ОС Windows

Переваги:

централізоване управління;

просте адміністрування, дешевше розгортання;

масштабованість;

безпека, захищеність файлів (дані зберігаються на сервері);

зменшення витрат на модернізацію обладнання (клієнтські термінали потребують менших витрат на утримання за рахунок збільшеного терміну роботи);

економія трафіку у WAN-мережах, і як наслідок, зменшення затребуваної пропускної спроможності і вартості трафіку, що орендується. У випадку з термінальним доступом трафік, який раніше проходив між клієнтськими станціями і серверами, замінюється на трафік передачі зображення на віддалений екран користувача.

Недоліки:

непрацездатність сервера може зробити непрацездатною всю обчислювальну мережу;

не можна створити повністю ізольоване середовище з окремим набором прав і програм.

Ізоляція відбувається на рівні сесії, і якщо додаток одного з користувачів викликає збій на рівні ОС, то разом із винуватцем, який викликав збій, будуть змушені перезавантажувати свої додатки й інші користувачі, які працюють на цьому ж сервері.

Деякі виробники не підтримують програмні продукти в термінальному середовищі, наприклад, Autodesk AutoCAD, а для деякого ПЗ необхідні права адміністратора.

Разом з тим загальносвітові тенденції розвитку IT-технологій [6] дають змогу констатувати факт еволюції статичних комп'ютерних систем до віртуальних за рівнями, які наведені на рисунку 4.

Говорячи про технології віртуалізації, які стали невід'ємною частиною сучасних IT-інфраструктур державних секторів, необхідно зазначити, що на перше місце виходять питання побудови високопродуктивної, масштабованої, ефективно керованої та безпечної інфраструктури.

У різних країнах із різною швидкістю відбувалося впровадження нових систем, а також оптимізація витрат на підтримку існуючих. Україна не є виключенням і фактично нині триває перший етап практичного застосування засобів віртуалізації, який можна охарактеризувати як «застосування віртуалізації в умовах існуючої IT-інфраструктури». Наступним етапом буде зміна компонентів самої інфраструктури з урахуванням можливостей віртуалізації, як нинішніх, так і перспективних.

Логічним продовженням розвитку технології термінального сервера стала віртуалізація робочих столів (VDI) – створення віртуальних робочих станцій за робочими місцями користувачів, що і пропонується авторами дійсної статті як один зі шляхів забезпечення якісного виконання завдань службовими особами ОУ.

Рис. 4. Еволюція системного підходу побудови IT-інфраструктури

Розглянемо детальніше особливості VDI.

3. «Тонкий клієнт» в технології VDI.

VDI – це концепція, в якій дані з ПК користувача зберігаються централізовано на сервері в ЦОД, а у кожного користувача ПК – віртуальний. Розгортається особлива інфраструктура для віддаленої роботи, при якій на основі одного фізичного сервера створюється кілька віртуальних, що дозволяє запускати дві і більше ОС у віддаленому режимі. З архітектурної точки зору адміністратор сервера для паралельної роботи кожного користувача створює віртуальний повноцінний робочий стіл з окремим набором додатків, програм, документів і доступів. Операційна система, профіль користувача, політики настільних ПК та програми обробляються як окремі компоненти, які абстрагуються від базової машини, а потім передаються разом з метою створення робочих столів користувачам. Підключення і вся робота користувачів йде через «прошарок» – «тонкий клієнт» (рис. 5).

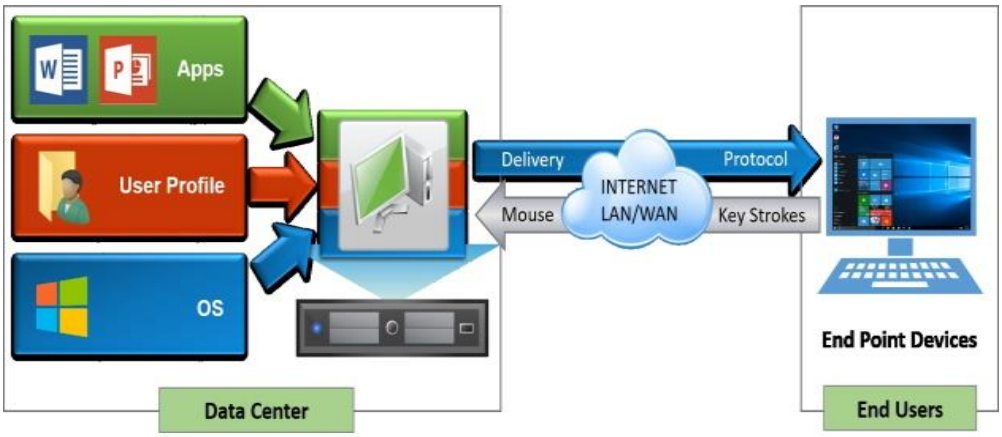


Рис. 5. Набір компонентів віртуального робочого столу для «тонкого клієнта»

Замість того, щоб підключатися до відокремленого, захищеного індивідуального сеансу програми, користувач тепер підключається до відокремленого, захищеного індивідуального примірника ОС сервера, в якому містяться затребувані застосунки.

Існує два типи інфраструктури VDI: зі збереженням стану і без збереження стану. У випадку зі збереженням стану користувачеві надається певний віртуальний робочий стіл, до якого він може постійно підключатися і котрий він може налаштувати відповідно до своїх потреб, оскільки зміни зберігаються після скидання підключення. Іншими словами, віртуальний робочий стіл у VDI зі збереженням стану працює аналогічно фізичному комп'ютеру.

Інфраструктура VDI без збереження стану, в якій користувачам надаються стандартні віртуальні робочі столи і зміни не зберігаються, є більш простим і дешевшим варіантом, оскільки немає необхідності зберігати налаштування віртуальних робочих столів після завершення сеансу. Цей спосіб VDI часто використовується в організаціях із великою кількістю співробітників, що виконують стандартні завдання, або при вирішенні обмеженої кількості завдань, що повторюються, для яких не потрібно налаштовувати віртуальні робочі місця.

Відповідно до [7] 80 % світових організацій вже включили технологію VDI у стратегії розвитку ІТ-інфраструктур і очікують прогнозоване зменшення адміністративних витрат на 70 %, на електроенергію – 97 %, а дозвіл працювати своїм 70 % співробітникам з мобільних пристроїв з будь-якого місця і в будь-який час дасть на 98 % збільшення продуктивності їхньої роботи.

Впровадження VDI в роботу службових осіб в ОУ учасників сектору безпеки і оборони із врахуванням обмежень державного регулятора із захисту інформації теж може бути доцільним і обґрунтованим за нижче наведеними напрямками.

Централізація ІТ-сервісів. Перехід до «хмарної» моделі обслуговування. Оскільки зростання пропускної здатності каналів передачі даних і якості сервісів дозволяє уникнути необхідності їхнього розміщення в безпосередній близькості від користувачів, створюється можливість здійснення централізації ІТ-сервісів в одному чи декількох ЦОД або створення умов переходу до «хмарної» моделі обслуговування. Перехід до такої моделі можливий, оскільки обмін великого об'єму частини трафіку між користувацькими додатками здійснюється в середині серверів ЦОД, а на робоче місце користувача передаються лише дані, що змінилися.

Централізоване управління. Спрощення підтримки та оновлення робочих місць. Централізовані робочі столи на рівні із централізованим управлінням для 1-2 адміністраторів (незалежно від їх територіального розміщення у мережі) дають можливість для кожного робочого столу виконувати набагато простіше такі завдання, як: резервне копіювання,

оновлення ПЗ та налаштування ОС, чи встановлення нових програм. Контроль за діями користувачів, керування різнорідним парком апаратного забезпечення відбувається з однієї точки мережі.

Технологія VDI дозволяє створювати віртуальні робочі столи з єдиного образу, що підтримується та оновлюється централізовано, а також надає гнучкості при переході на нові версії ОС, оскільки не вимагає негайної відмови від існуючої ОС або заміни клієнтського пристрою.

Організація віддаленої роботи. Гнучкість в роботі та масштабованість. За допомогою VDI можливе забезпечення доступу до будь-якої програми, навіть якщо користувачі знаходяться за межами контрольованої зони відомчої мережі та не мають доступу до своїх робочих місць. На відміну від термінального доступу VDI дозволяє запустити більш широкий спектр додатків завдяки використанню клієнтських версій ОС. За рахунок ізоляції робочих середовищ користувачів на рівні віртуальних машин (далі – ВМ) для кожної ОС і користувача можуть бути виконані індивідуальні налаштування, що не перемежовуються з іншими користувачами, наприклад, деяким з них можуть надаватися права локальних адміністраторів. Технологія VDI дозволяє гнучко змінювати апаратну конфігурацію ВМ, швидко створювати або повторно розгортати віртуальні робочі столи, що доречно у разі територіально-розподіленої роботи окремих підрозділів, наприклад, у випадку коли немає можливості оперативно доставити користувачу нову робочу станцію або при відсутності у філіальному підрозділі підмінного фонду комп'ютерів і комплектуючих.

Заощадження операційних витрат. Впровадження середовища віртуального робочого столу разом із найкращими практиками щодо управління зображеннями, виправленнями та профілями за допомогою централізованого розгортання додатків призведе до економії операційних витрат порівняно з традиційним управлінням робочих столів. Капітальні витрати на початку проєкту VDI будуть вищими з розгортанням інфраструктури, проте зниження операційних витрат будуть пов'язані із: закупівлею ліцензій на ПЗ (завдяки встановленню набору користувацьких додатків не на кожен ПК, а на один сервер); зменшеними затратами на електроенергію (завдяки зниженню електроспоживання клієнтських пристроїв до рівня 7–15 Вт); модернізацією парку обчислювальної техніки (завдяки витратам тільки на серверну частину, більш тривалого терміну експлуатації «тонких» або «нульових» клієнтів); зменшенням штату технічної підтримки; обслуговуванням і ремонтом системи у цілому.

Підвищення безпеки інформації. Технологія VDI задовольняє потреби, які висуває діяльність користувачів без компрометації безпеки, контролю, керованості та здійснює відповідність вимогам щодо нормативних обмежень державного регулятора по захисту інформації.

При кожному підключенні користувача до свого віртуального робочого столу завжди створюється нова ВМ з налаштуваннями особистого оточення. У разі зараження шкідливим ПЗ досить просто перепідключитися до свого віртуального робочого столу, внаслідок чого під користувача буде автоматично створена нова ВМ з особистими налаштуваннями оточення, груповими політиками й особистими файлами.

Завдяки централізованому зберіганню призначених для користувачів даних VDI дозволяє спростити механізми резервування й аварійного відновлення робочих столів. Технологія дозволяє реалізувати різні сценарії катастрофостійкості, наприклад, із використанням територіально-розподілених кластерів, автоматичного перемикання на резервний ЦОД або виділення користувачам двох віртуальних робочих столів у різних ЦОД.

Очевидно, що виконання вимог щодо захисту інформації повинно здійснюватися в рамках впровадження хмарних обчислень в державні інформаційні інфраструктури учасників сектору безпеки і оборони, як наведено в [8; 9].

Недоліки VDI. Основним недоліком, що перешкоджає широкому поширенню VDI, залишається висока вартість впровадження порівняно з фізичними робочими станціями або термінальним доступом [10]. Чималу частку у вартості відіграють ліцензії на ПЗ віртуалізації, ОС Windows і брокери VDI. Наприклад, на сьогодні для легального використання клієнтських ОС Windows потрібно або мати ліцензію Windows з чинним Software Assurance на кожен пристрій, з якого здійснюється підключення до віртуальних робочих столів, або щорічну передплатну підписку Windows VDA. До цього додаються витрати на серверні ОС Microsoft Windows і в ряді випадків Microsoft SQL Server, що потрібно для функціонування більшості VDI-рішень, а також вимоги щодо ліцензування брокерів VDI (як правило, за кількістю користувачів або активних підключень).

Витрати на апаратне забезпечення. При реалізації у відомстві сценарію інсталяції наведеної технології не з нуля (при збільшенні кількості робочих місць, при масовій модернізації) у випадку, коли вже є в наявності достатня кількість функціонуючих ПК, то їх можна використати як «тонкі клієнти» після здійснення відповідних доналаштувань. Водночас, для запуску великої кількості віртуальних робочих столів (їх зберігання) потрібне здійснення достатньо затратного апаратного забезпечення, такого як: високопродуктивних серверів із багатоядерними процесорами та великим об'ємом оперативної пам'яті; виділені системи зберігання даних, які здатні надавати необхідні обсяги дискового простору і з високими характеристиками IOPS (кількість операцій введення/виводу в секунду), щоб забезпечити як типові навантаження, так і періодичні пікові; клієнтських терміналів, які необхідні для розгортання VDI.

Клієнтські пристрої («тонкі клієнти») залишаються вельми недешевим задоволенням. За ціну брендового кінцевого пристрою «тонкого клієнта» можна придбати ПК початкового рівня, достатнього для вирішення типових офісних завдань. Крім того, для роботи деяких функцій VDI (підключення сканерів, інтеграція з VOIP-клієнтами та ін.) може знадобитися придбання клієнтського пристрою з ОС Windows Embedded/IOT, що відрізняється більш високою вартістю.

Вимога доступу до мережі. VDI, як і переважна більшість сучасних IT-сервісів, вимагає наявності надійного високошвидкісного мережевого доступу до ЦОД. Незважаючи на розвиток бездротового і мобільного Інтернету далеко не завжди швидкість і стабільність підключення задовольняють комфортну роботу.

Рівень підготовки кваліфікованих спеціалістів ІТ. Якщо для управління фізичними робочими станціями досить фахівця початкового рівня, то для організації VDI потрібно спеціально підготовлений співробітник або група, які б розбиралися у платформах віртуалізації.

Огляд компаній-вендорів, які надають послуги VDI, що наведений у звіті компанії IDC Market Scape щодо проведених досліджень ринку надання послуг VDI за 2019–2020 роки [11], свідчить, що лідерами ринку є: Citrix і VMware. Решта – це учасники другого ешелону: Microsoft, Amazon, Parallels, CloudJumper, Huawei та ін.

Доцільно коротко зупинитись на продуктах Citrix і VMware. У мережі Інтернет достатньо порівнянь як відносно незалежних, так і ангажованих за одну чи за іншу сторону [12–14]. Якщо говорити про кожного лідера окремо, то VMware може бути цікавим завдяки широкому набору власних продуктів і рішень, які йдуть у складі бандла Horizon або інтегруються з ним. VMware надає найбільш повний і функціональний набір продуктів, на якому можливо побудувати закінчену VDI-інфраструктуру з нуля. VMware виходить вперед завдяки реалізації в Horizon таких можливостей, які раніше були сильними сторонами Citrix – доставка додатків з термінальних серверів, а також протокол Blast, який оптимізований для роботи через повільні, ненадійні канали.

З іншого боку, компанія Citrix зайняла частину ринку завдяки поширеності рішень з організації термінального доступу – XenApp, а також пропозицій широких можливостей

щодо інтеграції з різними платформами віртуалізації (власний гіпервізор Citrix XenServer, Microsoft Hyper-V, Nutanix AHV і VMware vSphere) чи зі хмарними сервісами інших вендорів – Microsoft Azure і Amazon AWS. Забезпечення крос-платформеності і партнерство з іншими виробниками систем віртуалізації є сильними сторонами Citrix.

Висновки

Отже, наведені функціонально-технологічні можливості VDI – створення віртуальних робочих столів за робочими місцями службових осіб органів управління – учасників сектору безпеки і оборони, – дозволить набути переваг існуючим інформаційним інфраструктурам за наступними напрямами: централізоване управління та надання сервісів; безпека інформації; гнучкість в роботі та реалізація масштабування; ефективне використання фінансів на підтримку і розвиток інформаційної інфраструктури; створення умов до переходу на хмарні технології.

В реаліях сьогодення впровадження засобів віртуалізації проводитиметься в умовах діючої ІТ-інфраструктури. Найдоцільнішим варіантом забезпечення міграції буде здійснення переналаштування визначеного парку ПК в «тонкі клієнти», резервування серверів в ЦОД, оплати ліцензій ПЗ обраного вендора, налаштування високошвидкісних каналів передачі даних, задання відповідного алгоритму переходу на VDI водночас із паралельним процесом закінчення життєвих циклів існуючих ІТС.

Переваги технології VDI, які наведені в статті, – очевидні, проте постає питання правильної оптимальної конфігурації для різних пунктів управління, переліку функціональних сервісів, які надаватимуться відповідним службовим особам, що і буде напрямом подальших досліджень.

ЛІТЕРАТУРА

1. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020 // URL: https://www.president.gov.ua/news/volodimir-zelenskij-zatverdiv-strategiyu-nacionalnoyi-bezpek-63577 (дата звернення: 15.01.2022).

2. Про рішення Ради національної безпеки і оборони України «Про Стратегію воєнної безпеки України»^ Указ Президента України від 25.03.2021 № 121/2021 // URL: https://www.president.gov.ua/documents/1212021-37661 (дата звернення: 15.01.2022).

3. Гудима О. П., Шиятий О. Б. ІТ-структура армії // Оборонний вісник. Київ. 2016. № 8/2016. С. 4–7. URL: https://issuu.com/defensebulletin/docs/ov_08_2016_ukr (дата звернення: 15.01.2022).

4. Кірпічніков Ю. А., Андрощук О. В., Головченко О. В., Петрушен М. В. Визначення технологічних рішень щодо створення Єдиної інформаційної системи управління оборонними ресурсами // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ. 2019. № 1(65). С. 86–91.

5. Пермяков О. Ю. Організація інформаційних систем Збройних Сил України: навч. посіб. / О. Ю. Пермяков, Н. О. Королюк, С. І. Фараон. К.: Національний університет оборони України імені Івана Черняховського, 2019. 134 с.

6. Колесов А. Виртуализация инфраструктуры – ключевое направление в ИТ // Портал «itWeek». 31.05.2011. URL: https://www.itweek.ru/infrastructure/article/ detail.php?ID=131652 (дата звернення: 15.01.2022).

7. Бараш Л. Инфраструктура виртуального десктопа. Почему технология VDI становится популярнее в отечественном корпсекторе? 25 июня 2019 г. // «Компьютерное Обозрение». URL: https://ko.com.ua/infrastruktura_virtualnogo_desktopa_pochemu_tehnologiya_vdi_stanovitsya_populyarnee_v_otechestvennom_korpsektore (дата звернення: 15.01.2022).

8. Нерознак Є. І., Остапчук В. М., Драглюк О. В., Радченко М. М., Коротков М. М. Аналіз можливостей хмарних технологій при застосуванні в інформаційній інфраструктурі складових сил оборони // Вісник ВІТІ. Київ. 2021. № 1. С. 53–68.

9. Аксенов В. Архитектура G-Cloud в облаках // Ассоциация «BISA». 21 октября 2016 г. URL: https://bis-expert.ru/articles/54528 (дата звернення: 15.01.2022).

10. Коновалов А. Немного о дизайне VDI // Блог, посвященный технологиям виртуализации и смежным с ними областям. 04.09.2017. URL: http://blog.vmpress.org/2017/09/vdi-1.html (дата звернення: 15.01.2022).

11. Звіт IDC MarketScape: Worldwide Virtual Client Computing 2019–2020 Prondor Assessment (Doc # US45752419, січень 2020) // URL: https://www.idc.com/getdoc.jsp?containerId=US45752419 (дата звернення: 15.01.2022).

12. Порівняйте віртуальні програми та настільні комп'ютери Citrix та VMware Horizon View // IT-Central Station. URL: https://www.itcentralstation.com/products/comparisons/vmware-horizon-view_vs_xendesktop (дата звернення: 15.01.2022).

13. Citrix: вебсайт. URL: https://www.citrix.ru/products/xenapp-xendesktop/compare.html (дата звернення: 15.01.2022).

14. VMware: вебсайт. URL: https://www.vmware.com/company/why-choose-vmware/workspace-transformation.html (дата звернення: 15.01.2022).

УДК 654.1-192
Сінько В. В. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ФАКТОРІВ, ЯКІ ВПЛИВАЮТЬ НА НАДІЙНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ МЕРЕЖІ ВІЙСЬКОВОГО ЗВ'ЯЗКУ

Телекомунікаційне обладнання (ТКО) знаходить все більш широке застосування, причому витрати на складання програмних комплексів для ТКО ростуть швидше, ніж вартість відповідного апаратного устаткування. Тому, природно, основні зусилля повинні бути спрямовані на розробку надійних програм для ТКО.

ТКО мережі військового зв'язку (МВЗ) використовується для вирішення завдань державного управління, управління військами і зброєю, екологічно небезпечними та економічно важливими виробництвами тощо. Це обладнання функціонує в умовах деструктивних впливів, метою якого є руйнування інформаційних ресурсів, порушення штатних режимів функціонування і, як наслідок, зрив виконання покладених на таке обладнання функцій. Порушення, припинення або невірне його функціонування може призвести до серйозних наслідків, усунення яких потребує витрачання значних часових, людських і матеріальних ресурсів. Це визначає необхідність організації захисту ТКО МВЗ від таких впливів.

У статті проаналізовано фактори, що впливають на надійність програмного забезпечення ТКО, а також фактори, що дестабілізують програмний продукт та визначають його низьку якість.

Також проведено повну класифікацію внутрішніх та зовнішніх факторів, що дає можливість побачити повну проблематику даної теми в загальному вигляді та зробити висновок щодо покращення надійності програмного забезпечення ТКО.

Ключові слова: *програмне забезпечення, помилки, надійність програмного забезпечення.*

V. Sinko ***Analysis of factors that affect the reliability of telecommunications equipment of the military communications network.***

Telecommunication equipment is increasingly used, and the cost of assembling software for telecommunication equipment is growing faster than the cost of the corresponding hardware. Therefore, naturally, the main efforts should be aimed at developing reliable programs for solid waste.

Telecommunication equipment of the military communication network is used to solve problems of public administration, management of troops and weapons, environmentally hazardous and economically important industries, etc. This equipment operates in conditions of destructive influences, the purpose of which is the destruction of information resources, violation of regular operating modes and, as a consequence, disruption of the functions assigned to such equipment. Violation, cessation or malfunction can lead to serious consequences, the elimination of which requires the expenditure of significant time, human and material resources. This determines the need to organize the protection of solid waste of the military communications network from such influences.

The article analyzes the factors that affect the reliability of telecommunications equipment software, as well as factors that destabilize the software product and determine its low quality.

A full classification of internal and external factors was also carried out, which gives an opportunity to see the full issues of this topic in general and to draw a conclusion on improving the reliability of telecommunications equipment software.

Keywords: *software, bugs, software reliability.*

Постановка завдання у загальному вигляді

Результати експлуатації сучасного ТКО МВЗ показали, що реальні значення показників надійності відрізняються від заявлених виробником. Одна з причин цього є широке використання у складі ТКО обчислювальних елементів та застосування спеціалізованого (прикладного) програмного забезпечення (ПЗ), що, у свою чергу, призводить до виникнення нових джерел відмов – збоїв у роботі ПЗ обладнання, які суттєво впливають на показники надійності системи в цілому. Порушення штатних режимів функціонування ТКО і, як наслідок, зрив виконання покладених на нього функцій може призвести до серйозних наслідків, усунення яких потребує витрачання значних часових, людських і матеріальних ресурсів.

Досвід проведення Операції об'єднаних сил показав, що при екстрених ситуаціях військовослужбовці, дякуючи своєму досвіду, можуть провести ремонт ТКО, але швидко замінити чи провести аналіз помилок ПЗ майже неможливо.

Також варто зазначити, що теорія надійності ПЗ ще не розроблена на такому рівні, як теорія надійності апаратного устаткування. Це пов'язано з особливостями та відмінностями ПЗ від традиційних технічних систем, для яких спочатку розроблялася теорія надійності.

Тому необхідно провести аналіз факторів, що суттєво впливають на надійність ПЗ ТКО МВЗ, та в подальшому знайти або покращити існуючий метод зменшення помилок та підвищення якості ПЗ. Такий аналіз допоможе уникнути тієї кількості помилок в ПЗ, що є сьогодні.

Аналіз останніх публікацій

На сьогодні виконано ряд наукових робіт, присвячених теоретичним дослідженням надійності телекомунікаційних систем та мереж. У [1−8] основна увага приділяється основам теорії надійності: поняттям, визначенням і постулатам, докладній класифікації відмов, характеристикам надійності при раптових і поступових відмовах. У зазначених джерелах виявлено базові характеристики надійності як показники безвідмовності, ремонтопридатності, довговічності, зберігання. Розглянуто загальні методи розрахунку надійності технічних систем різного призначення як нерезервованих, так і резервованих. У публікації [9] проведено оцінку надійності обладнання мережі спеціального призначення з урахуванням збоїв. Запропонована аналітична модель надійності ТКО мереж зв'язку спеціального призначення, при повній та обмеженій інформації з урахуванням збоїв та стійких відмов. Стаття Білла Грема, Пола Н. Леру, Тодда Лендрі [10] присвячена статичному і динамічному аналізу програмного коду на наявність різноманітних дефектів і слабких місць. В літературі [11−17] представлені різні моделі надійності ПЗ, їхня класифікація, наведені приклади з використанням цих моделей.

Отже, методологія, яка представлена у виділених інформаційних джерелах, не враховує особливості застосування ТКО та не дозволяє застосувати її в повному обсязі при оцінці надійності ПЗ. Це зумовлює більш глибоко розглянути дану тему та проаналізувати фактори, що впливають на надійність ПЗ ТКО МВЗ.

Тому, **метою статті** є аналіз факторів, що впливають на надійність ПЗ ТКО МВЗ.

Виклад основного матеріалу дослідження

Проведений аналіз наукової літератури дозволив визначити фактори, що впливають на надійність функціонування ПЗ ТКО та поділити їх на внутрішні і зовнішні. До внутрішніх факторів, які впливають на надійності функціонування ПЗ ТКО, можна віднести:

1. Системні помилки проєктування при встановленні цілей і завдань створення ПЗ, при формулюванні вимог до функцій і характеристик ПЗ. Системні помилки і недоліки визначення вимог до ПЗ характеризуються, перш за все, неповною інформацією про реальні процеси функціонування ТКО. Крім того, ці процеси часто залежать від самих алгоритмів і тому не можуть бути досить визначені й описані заздалегідь без дослідження функціонування ПЗ у взаємодії із зовнішнім середовищем. На початкових етапах розробки не завжди вдається точно і повно сформулювати цільове завдання всієї системи, а також цільові завдання основних функціональних груп програм, і ці завдання уточнюються в процесі проєктування. Відповідно до цього уточнюються і конкретизуються специфікації на функціональні компоненти і виявляються відхилення від уточненого завдання вимог, які можуть кваліфікуватися як системні помилки. У багатьох випадках відсутня повна адекватність умов отримання передбачуваних і реальних характеристик зовнішнього середовища, що може бути причиною складних і важко виявлених помилок. Це посилюється тим, що часто неможливо заздалегідь передбачити все розмаїття можливих зовнішніх умов і реальних варіантів сценаріїв функціонування і застосування версій програмних продуктів.

У процесі супроводу системні помилки зазвичай є переважаючими (близько 60–80 % від усіх помилок) [18].

2. Помилки визначення характеристик системи та умов і параметрів зовнішньої середовища, прийнятих в процесі розробки ПЗ за вихідні, можуть бути результатом

аналітичних розрахунків, моделювання або дослідження аналогічних систем. У ряді випадків може бути відсутня повна адекватність передбачуваних і реальних характеристик, що є причиною складних системних помилок, які важко виявити. Ситуація з такими помилками додатково ускладнюється тим, що експерименти з перевірки взаємодії ПЗ з реальною зовнішнім середовищем у всій області зміни характеристик часто є складними і коштовними, а в окремих випадках, при створенні небезпечних ситуацій, – неприпустимими. У цих випадках доводиться використовувати моделювання й імітацію зовнішнього середовища з явним спрощенням її окремих елементів і характеристик, хоча ступінь спрощення не завжди можна оцінити з необхідною точністю. Однак, повної адекватності моделей зовнішнього середовища і реальної системи домогтися важко, а в багатьох випадках і неможливо, що може бути причиною значного числа дефектів [19].

3. Алгоритмічні помилки розробки при безпосередній специфікації функцій ПЗ, при визначенні структури і взаємодії компонентів ПЗ, а також при використанні інформації з баз даних. До цих помилок можна віднести, перш за все, помилки, обумовлені некоректною постановкою функціональних завдань, коли в специфікаціях не в повному обсязі обумовлені всі умови, необхідні для отримання правильного результату. Помилки даного типу, обумовлені неповним урахуванням всіх умов вирішення завдань, є найбільш частими в цій групі і складають до 70 % всіх алгоритмічних помилок або близько 30 % загальної кількості помилок на початкових етапах проєктування. Проведений аналіз показав [20], що до алгоритмічних помилок також слід віднести помилки зв’язків модулів і функціональних груп ПЗ. Цей вид помилок становить 6–8 % від загальної кількості. Алгоритмічні помилки виявляються в неповному обліку діапазонів зміни змінних, в неправильній оцінці точності використовуваних і одержуваних величин, в неправильному обліку зв’язків між різними змінними, в неадекватному поданні формалізованих умов рішення задачі в специфікаціях або схемах, які підлягають програмуванню.

4. Помилки програмування в текстах програм і описах даних, а також у вихідній і результуючій документації на компоненти і ПЗ в цілому. У процесі налаштування основна частина помилок в програмах виявляється і усувається, проте завжди є ризик пропуску декількох помилок. Будь-яке налаштування ПЗ може показати наявність помилок, але не може довести їхню відсутність. У процесі тестування і налаштування ПЗ практично неможливе виконання абсолютно повних перевірок, що гарантують відсутність неперевірених компонентів програми і повне виявлення всіх можливих помилок. В результаті в ПЗ завжди існує певна кількість невиявлених помилок.

5. Недостатню ефективність використовуваних методів і засобів оперативного захисту програм й даних від збоїв і відмов, та забезпечення надійності функціонування ПЗ в умовах випадкових негативних впливів.

Зовнішніми факторами, які впливають на надійності функціонування ПЗ ТКО, є:

1. Кваліфікація оперативного та обслуговуючого персоналу, що визначає їх дії в процесі експлуатації та проведення технічного обслуговування ТКО.

2. Спотворення вихідної інформації, що поступає від користувачів. У підготовці та введенні вихідних даних у ВС бере участь людина. Це призводить до того, що відповідна частина даних характеризується невисокою достовірністю з ймовірністю помилки близько 10^{-3} на 1 байт. В автоматичних пристроях підготовки та передачі інформації ймовірність помилки може бути значно нижче і досягати значення 10^{-6}–10^{-7}. Але і при такій достовірності дані не завжди придатні для обробки без проведення контролю і попередньої селекції та можуть залишатися істотною причиною відмов або збоїв при їх обробці. Підвищення достовірності вихідної інформації може проводитись з використанням надмірності, при підготовці первинних даних і при введенні їх в ТКО. Ця надмірність використовується для виявлення спотворень і виключення помилкових даних, а в окремих випадках і для виправлення помилок.

3. Спотворення в каналах передачі інформації мереж зв'язку, що надходить від зовнішніх джерел, а також неприпустимі для конкретного ТКО характеристики потоків трафіку.

4. Збої і відмови у ТКО. Відмови і збої в ТКО є фактором, що істотно впливають на надійність функціонування ПЗ. За останні роки досягнуто значних успіхів у підвищенні надійності ТКО. Особливо, що стосується зниження ймовірності повної відмови ТКО. Існують системи, які характеризуються середнім часом напрацювання на відмову, що обчислюються десятками тисяч годин, однак при використанні в ТКО однопроцесорних систем середній час напрацювання на відмову, як правило, вимірюється сотнями годин. Значно частіше відбуваються збої. Більшість з них виявляється і усувається засобами апаратурного контролю і не впливає на виконання програм. Однак деяка частина збоїв ТКО може призвести до спотворень виконання програм або до спотворення змінних. Причинами таких збоїв є переважно зовнішні впливи на ТКО. Ще частіше відбуваються збої, які не вдається виявити і зафіксувати при функціонуванні ПЗ у процесі нормальної обробки інформації та управління. Такі збої проявляються в випадкові моменти часу, і практично неможливо добитися їх повторюваності. Труднощі їх реєстрації і вивчення, а також незацікавленість фірм, які виробляють ТКО, у виявленні характеристик збоїв призводять до того, що достовірні дані про них практично відсутні. Проте спотворення змінних і процесу виконання ПЗ через збої ТКО іноді призводять до зациклення, зупинки або спотворення масивів даних.

5. Зміни складу і конфігурації ТКО за межі, які перевірені при випробуваннях або сертифікації і відображені в експлуатаційній документації.

Висновки

Отже, проведений аналіз дозволив провести класифікацію факторів, що впливають на надійність ПЗ ТКО МВЗ. Повністю виключити всі ці фактори неможливо. Тому необхідно розробляти засоби і методи зменшення їхнього впливу на надійність ПЗ. Ймовірно, найкращим способом одержати надійне ПЗ є зведення до мінімуму кількості помилок і їхніх наслідків в ході розробки комплексу програм. Однак не існує перевіреного способу створення надійного ПЗ. Відсутня поки і теоретична основа методики розробки безпомилкових програм. Тому в подальшому слід проаналізувати вже існуючі методи покращення якості ПЗ та запропонувати новий метод, що покращить показники якості ПЗ ТКО МВЗ.

ЛІТЕРАТУРА:

1. Василевський О. М., Поджаренко В. О. Нормування показників надійності технічних засобів: навч. посіб. Вінниця: ВНТУ, 2010. 129 с.

2. Павлюк О. М., Медиковський М. О. та ін. Основи теорії надійності технічних систем: навч. посіб. Львів: Львівська політехніка, 2021. 208 с.

3. Нечипоренко О. М. Основи надійності літальних апаратів: навч. посіб. К.: НТУУ «КПІ», 2010. 240 с.

4. Парасюк В. І. Основи надійності технічних систем: навч. посіб. до лаб. практикуму / В. І. Парасюк, А. В. Кондратьєв. Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2010. 72 с.

5. Яковина В. С., Сенів М. М. Основи теорії надійності програмних систем: навч. посіб. Львів: Видавництво Львівської політехніки, 2020. 248 с.

6. A.Petrov, V. Khoroshko, L. Scherbak, M. Aleksander. Reliability Basics of Information Systems / Published by AGH University of Science and Technology Press. Krakow, 2016. P. 247.

7. Mark L. Ayers. Telecommunications System Reliability Engineering, Theory, and Practice (IEEE Press Series on Networks and Service Management Book 21) 1st Edition, Kindle Edition / Published by J. Wiley, Inc. // New Jersey, 2012. P. 371.

8. P. Stavroulakis. Reliability, Survivability and Quality of Large Scale Telecommunication Systems: Case Study: Olympic Games 1st Edition / Published by Wiley // Technical University of Crete. Greece, 2003. P. 370.

9. Mogylevych, D. I., Kononova, I. V., Kredentser, B. P. and Karadschow I. Comprehensive Reliability Assessment Technique of Telecommunication Networks Equipment with Reducible Structure // Visnyk NTUU KPI. Seriia: Radiotekhnika Radioaparatobuduvannia. 2020. № 80. P. 39–47. DOI: 10.20535/RADAP.2020.80.39-47.

10. Тодд Лендри, Пол Н. Леру, Грэм Б. Использование статического и динамического анализа для повышения качества продукции и эффективности разработки // Операционная система реального времени QNX. URL: http://www.swd.ru/ index.php3/pid=828.

11. Y. Kim, K. Song, H. Pham, I. Chang. A Software Reliability Model with Dependent Failure and Optimal Release Time // Symmetry. 2022. Vol. 14, P. 343. DOI: 10.3390/sym14020343.

12. Olli Salmela. Reliability Assessment of Telecommunications Equipment. Department of Electrical and Communications Engineering, Helsinki University of Technology, 2015 March.

13. Keiller, Peter A. and Miller, Douglas R. On the Use and the Performance of Software Reliability Growth Models // Software Reliability and Safety, Elsvier. 1991. P. 95–117. [ANSI91] ANSI/IEEE, «Standard Glossary of Software Engineering Terminology», STD-729-1991, ANSI/IEEE, 1991.

14. Peng Cao, Ziqiang Luo, Software Reliability Qualitative Evaluation Based on Modified Delphi Hierarchy Process. Proceedings of the 3rd International Conference on Mechatronics, Robotics and Automation. Published by Atlantis Press. 2015. Vol. 15. P. 1392–1396.

15. Zhu M, Pham H. A two-phase software reliability modeling involving with software fault dependency and imperfect fault removal // Computer Languages, Systems & Structure. 2018. № 53. P. 27–42.

16. Wang H, Fei H, Yu Q, Zhao W, Yan J et al. A motifs-based maximum entropy Markov model for real time reliability prediction in system of systems // Journal of Systems and Software. 2019. № 151. P. 180–193.

17. Organizaci O. ISO-IEC 25010: 2011 Systems and Software Engineering-Systems and Software Quality Requirements and Evaluation (SQuaRE)-System and Software Quality Models. 2011.

18. J. Donovan, K. Prabhu, Building the Network of the Future, Chapman and Hall/CRC. 2017. P. 427.

19. Mark A. Levin, Ted T. Kalal and Jonathan Rodin. Improving Product Reliability and Software Quality. 2nd Edition // Willey Series in Quality and Reliability Engineering. 2019. P. 456.

20. M. Richards, N. Ford. Fundamentals of Software Architecture, O'Reilly Media, Inc. 2020. P. 419.

УДК 621.391:004.89

канд. техн. наук Шаповал В. М. (ВІТІ ім. Героїв Крут)
канд. техн. наук Радзівілов Г. Д. (ВІТІ ім. Героїв Крут)
Османов Р. Н. (ВІТІ ім. Героїв Крут)
Сердюк П. Є. (ВІТІ ім. Героїв Крут)

ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ БРОНЬОВАНОГО АВТОМОБІЛЯ «БАРС-8» ЛОКАЛЬНИМ БРОНЮВАННЯМ

У статті обґрунтовано, що для ефективної боротьби з нерегулярними військовими формуваннями і терористичними угрупуваннями доцільно застосовувати нові зразки бойових машин – броньовані автомобілі. Бронеавтомобіль «Барс-8» успішно пройшов усі етапи: ходові випробування, бездоріжжя, проходження бродів, подолання підйомів і спусків, ведення вогню, випробування підривом, балістичну стійкість та ряд інших важливих тестів. Наведено показники ефективності застосування броньованих автомобілів, викладені погляди на їх використання у складі підрозділів і частин сухопутних військ.

Ключові слова: *сухопутні війська, бойові дії, броньовані автомобілі, військові формування, взвод.*

V. Shapoval, G. Radzivilov, R. Osmanov, P. Serdyuk Improving the level of protection of the armored vehicle «Bars-8» with local reservation.

The article substantiated that in order to effectively combat irregular military formations and terrorist groups, it is advisable to use new samples of combat vehicles – armored vehicles. «Bars-8» has successfully passed all stages – sea trials, off-road, passing of the broads, overcoming the rises and descents, firing, testing of explosion, ballistic stability and a number of other important tests.

Keywords: *ground forces, fighting, armored vehicles, military formations, weapons.*

Бронеавтомобіль «БАРС-8», розроблений українською автобудівною компанією «Богдан Моторс» спільно з НВО «Практика», відповідно до стандартів світових аналогів та з урахуванням вимог Збройних сил України, у лютому 2019 року успішно завершив програму державних випробувань, яка розпочалась на початку 2017 року і тривала понад два роки (рис. 1). Бронемашина успішно пройшла всі етапи: ходові випробування, проходження бродів, подолання бездоріжжя, підйомів і спусків, зручність десантування, ведення вогню, випробування підривом, балістичну стійкість та ряд інших важливих тестів. Він став другою ББМ в Україні після бронеавтомобіля «Козак-2» (НВО «Практика»), яка пройшла державні випробування.

Рис. 1. Бронеавтомобіль, розроблений компанією «Богдан Моторс»

За підсумками випробувань «Богдан Моторс» постачатиме броньовики Збройним силам України і просуватиме бронеавтомобіль на зовнішніх ринках.

Броньовик «БАРС-8» розроблений на базі пікапа американської Ram (підрозділу Fiat Chrysler Automobiles), виконаний на шасі Dodge Ram. Пасажиромісткість базового автомобіля складає до 10 осіб у повному спорядженні. Особливість його конструкції забезпечує комфортну посадку та десантування екіпажу і десанту через широкі бокові й задні двері. Також передбачена можливість евакуації через люк на дах.

«Барс-8» має масу 8 т, шасі підвищеної прохідності з колісною формулою 4×4 з 6,7-літровим турбодизельним двигуном Cummins потужністю 385 к. с., броньований протимінний і балістичний захист за стандартом STANAG 4569 Level 2 та системи забезпечення життєдіяльності екіпажу. Максимальна швидкість обмежена відміткою 110 км/год. Кількість місць – 8 + 2. Машина здатна долати підйоми 60 % і бічні схили 20–40 %. Автомобіль проїжджає броди глибиною до 76 см, завдяки кліренсу в 280 мм може рухатися глибокою колією. На «Барсах» можуть встановлюватися різні бойові модулі, виконані у розвідувальній модифікації з комплексом наземної розвідки «Джеб», комплексом РЕБ «Анклав», варіант санітарно-евакуаційного автомобіля.

Конструкцією бронеавтомобіля передбачено встановлення систем пуску димових гранат, засобів зв’язку і навігації, приладів нічного й денного спостереження, системи регулювання тиску в шинах, системи пожежогасіння моторного відділення, засобів маскування, протиосколкового підбою корпусу, автономної кліматичної системи. Передбачена установка додаткової броні.

Бронеавтомобіль розроблений на Черкаському автозаводі у 2015 році. Він став новою розробкою після створеного у стислі терміни бронеавтомобіля «Барс» для потреб української армії, що відчувала брак техніки у зв’язку з російською агресією (рис. 2). У жовтні 2015 року автомобіль було представлено на виставці «Зброя і безпека» у Києві. Позиціюється як конкурент KrAZ Spartan.

Рис. 2. Бронеавтомобіль «Барс-8» успішно завершив програму державних випробувань

На виставці «Зброя і безпека – 2016» був представлений 120-мм мобільний мінометний комплекс на базі бронеавтомобіля «Барс-8». За інформацією виробника основною сферою використання «БАРС-8» є забезпечення підрозділів Збройних сил України при веденні бойових дій. Машина також може бути задіяною для транспортування особового складу,

перевезення вантажів в умовах бойових дій, виконання тактичних завдань і охорони блокпостів, використання в якості медичного евакуаційного транспорту.

На XV Міжнародній спеціалізованій виставці «Зброя і безпека – 2018» був представлений варіант «Барс-8АР» – машина артилерійської розвідки. Вона обладнана розвідувальним комплексом на базі БпЛА «Лелека» (дальність розвідки до 10 км) і оптичним приладом розвідки ЛПР-1 (модернізований лазерний прилад розвідки з дальністю 7 км). На машині встановлено комплекс виявлення цілей за звуком пострілу.

У січні 2019 року дослідний зразок № 3 машини «Барс-8ММК» разом з мобільною мінометною системою ALAKRAN UKR-MMC, що призначена для встановлення на цей дослідний зразок, була відправлена компанією «Укроборонсервіс» до іспанської компанії Everis Aeroespacial Y Defensa S.L, – партнера у створенні мобільної мінометної системи.

Барс-8ММК (у складі 120-мм автоматизованого мобільного мінометного комплексу UKR-MMC) має боєзапас із 60 споряджених до стрільби мін, підготовка до стрільби з похідного положення – 1 хвилина. Покинути вогневу позицію комплекс здатен за 20 секунд. Обслуга складається з трьох чоловік. Здатен працювати в єдиній системі з машиною артилерійської розвідки. На «Барсах» можуть бути встановлені різні бойові модулі.

Сімейство спеціальних броньованих машин на базі «БАРС-8» передбачає можливість встановлення різних бойових модулів і озброєння.

Мінна стійкість – одна з головних вимог до сучасних бронеавтомобілів. Нині в різних арміях світу використовують широкий спектр броньованої техніки. Її можна розділити на дві основні категорії. Перша, власне, бойові машини – БТР, оснащені штатним озброєнням і призначені для дій безпосередньо на полі бою. Про це повідомляє АрміяInform. Друга – машини логістичних підрозділів, призначені для перевезення особового складу і вантажів у прифронтовій зоні. Як правило, ці машини використовують у складі конвоїв, для патрулювання, як мобільні блокпости або рухомі прикордонні застави. На тлі останніх збройних конфліктів у різних куточках світу попит на цю техніку тільки зростає.

Зі свого боку збройні формування активізували мінну війну: мінують узбіччя, встановлюють радіокеровані СВП (саморобні вибухові пристрої) і фугаси, застосовують начинені вибухівкою транспортні засоби. Тому виробникам бронетехніки доводиться її удосконалювати. Заходи протидії мінній війні ведуться за кількома напрямками. Підвищення захищеності власне транспортний засіб, розробка індукційних систем виявлення вибухових пристроїв і придушення радіосигналів, а також розробка універсальних турелей для установки озброєння для захисту транспортного засобу у разі атаки.

Перші броньовики із захистом днища від підривів на мінах вперше почали створюватися в ПАР (Південно-Африканській Республіці) наприкінці 70-х років минулого століття. Пізніше, на початку XXI століття, армії провідних країн світу перейняли досвід південноафриканських інженерів. Тоді й виникла назва програми – MRAP (Mine Resistant Ambush Protected – «Мінна стійкість і захист від дій із засідок»). Вона передбачала створення сімейства броньованих автомобілів із високим захистом від підриву на мінах, фугасах і підвищені показники балістичного захисту. На різноманітних міжнародних виставках учасники представляли десятки зразків машин, виконаних за технологією MRAP.

На міжнародний ринок озброєнь масово почали надходити машини цього типу, розроблені в США, Великобританії, Україні, Китаї, Польщі, Туреччині, Сербії, Ізраїлі. Спільною рисою бронеавтомобілів є те, що спроєктовані вони так, аби збільшити захищеність екіпажу від уражаючих факторів під час підриву мін і вибухових речовин. Тому головною особливістю корпусу цих машин є клиноподібне днище, посилене додатковими броньованими пластинами. Таке рішення дозволяє зменшити силу вибуху, розсіявши ударну хвилю по обидва боки корпусу.

Днище корпусу таких бронеавтомобілів розташовано високо від землі – сила ударної хвилі знижується пропорційно кубу відстані від місця вибуху до точки її впливу. Звісно, що

після вибухів під машиною не гарантується технічна справність самого бронеавтомобіля, але головне при цьому, що збільшуються шанси виживання екіпажу і десанту.

У Збройних силах України виготовлення бронеавтомобілів із підвищеним протимінним бронезахистом розпочалося фактично з початком війни на Сході України. Перші зразки «Кугуар» і «Спартан» виробництва КрАЗ на шасі Toyota та Ford були прийняті на озброєння ще 2014 року. За роки війни після проведення відповідних випробувань було прийнято на озброєння або допущено до експлуатації декілька видів броньованих автомобілів. Зокрема, це такі бронеавтомобілі, як «Козак-2» і «Козак-2М1» (виробник – ПрАТ «НВО «Практика»); «Барс-8» (виробник – ПрАТ «Богдан Моторс»), а також «Варта» і СБА «Новатор» (виробник – ТОВ «Українська бронетехніка»). За час війни на Донбасі вони врятували життя багатьом захисникам України. Отже, докладніше про них.

Спеціалізований броньований автомобіль «Козак-2» побудовано на рамній основі з додатковим бронюванням. В основі – шасі Iveco Eurocargo 4×4, яке розраховане на 15 т повної маси. Для бронювання використовується 12-мм бронесталь марки «Мінілюкс Протекшн» (Фінляндія), яка відповідає другому рівню STANAG. Також застосовують рознесене бронювання, між бронелистами встановлюють протиосколковий шар із спеціального матеріалу, який також служить як термоізоляція.

Для збільшення живучості під час підриву на машині передбачений цілий комплекс заходів. Сама машина побудована за модульним принципом. V-подібне днище поглинає і розсіює частину енергії вибуху. Воно працює в поєднанні з багатошаровою підлогою, яка також поглинає частину енергії і водночас затримує вторинні осколки. Рівень протимінного захисту автомобіля, що підтверджений реальними підривами, – 6 кг тротилового еквіваленту. І під колесом, і під днищем.

На бронемашині «Козак-2» також встановлені протимінні сидіння, які НВО «Практика» виготовляє самостійно, вивчивши зарубіжний досвід. Сидіння для десанту – підвісні, вони кріпляться до стелі. На бронемашині також встановлено фільтровентиляційну установку. На даху може встановлюватися як дистанційно керований бойовий модуль, так і турель для стрільця. Якщо говорити про турель, то на неї можна встановити різні види озброєння – кулемет або гранатомет. Рівень протимінного захисту спеціалізованого броньованого автомобіля «Козак-2» ПСЗА-5, що підтверджений реальними підривами, – 6 кг тротилового еквіваленту. Прийнятий на озброєння 2017 року.

Бронеавтомобіль «Козак-2М1» відповідає натівському стандарту захисту STANAG 4569 Level2 за захистом від стрілецької зброї та Level3a за протимінним захистом. Тобто, бронемашина здатна витримати обстріл бронебійно-запальними кулями калібру 7,62×39 у будь-якій проєкції та підрив 8 кг міни чи фугасу під колесом. Для підвищення захисту екіпажу та десанту він обладнаний протимінними сидіннями та багатошаровою підлогою. Бронемашина має повністю несучий бронекорпус, що відрізняє її від інших аналогічних бронеавтомобілів, які зазвичай будують на базі позашляховиків чи вантажівок.

«Козак-2М1» із повною вагою 14 т оснащений 280-сильним дизельним двигуном об’ємом 5,9 л та крутним моментом 950 Н*м. Бронеавтомобіль має незалежну підвіску з можливістю блокування всіх коліс, кліренс у 500 мм та вертикальним ходом коліс у 260 мм. Все це забезпечує високу прохідність і мобільність «Козак-2М1», а також його максимальну швидкість у 110 км/год. Загалом під час випробувань машина подолала понад 15 тис. км, зокрема й по місцевості, яка призначена виключно для руху гусеничної техніки. Головним озброєнням «Козак-2М1» є 12,7-мм великокаліберний кулемет НСВ, який встановлений у захищеній турелі. Він забезпечує прицільну стрільбу на відстань до 2 км по наземних цілях. Екіпаж бронемашини становить 8 осіб – 2 члени екіпажу і 6 бійців у десантному відділенні. Прийнята на озброєння у квітні 2020 року.

Спеціалізований бронеавтомобіль «Новатор» із колісною формулою 4×4 виготовлено на базі популярного шасі Ford 550 із значною модернізацією. Завдяки інноваційним

технічним рішенням вдалося врівноважити навантаження на вісі машини рівномірно. Це дозволяє «Новатору», при масі в 9 тонн, розганятися до швидкості в 140 км/год. Крім того, авто має не тільки стандартний бронезахист кабіни від куль калібру 7,62×39, а й бронювання моторного відсіку. При цьому СБА має корисне навантаження не 800 кг (як у звичайних світових аналогів такого класу), а близько 2 тонн.

Спеціалізований бронеавтомобіль «Варта» з колісною формулою 4×4 побудований на шасі вантажівки МАЗ-5434. Виробником заявлена можливість встановлення бойового модуля з кулеметом 7,62 мм, 12,7 мм і башти типу БП-1 – аналогу башти, що встановлюють на

БТР-70/80 і БРДМ-2 з двома кулеметами – 14,5 мм і 7,62 мм. За словами розробника, для бронювання використовують шведську сталь із твердістю 560 компанії ARMOX, на відміну від інших вітчизняних бронеавтомобілів, які використовують сталь із твердістю 500. Це дозволило без зниження бронестійкості зменшити вагу капсули автомобіля на 11 %, як наслідок, збільшилася корисна вантажопідйомність. Водночас броня захищає екіпаж і десант від бронебійного патрона калібру 7,62×39 мм. Завдяки V-подібній формі днища та протимінним сидінням забезпечено захист екіпажу під час підриву міни потужністю 6 кг у тротиловому еквіваленті.

У зв’язку зі збереженням життя військовослужбовців доцільно розглянути питання застосування безекіпажних наземних систем [5].

Напрямок подальшого дослідження полягає у вивченні застосування сучасних роботизованих систем, що є у складі підрозділів і частин сухопутних військ та інших формувань країн НАТО.

Висновки

У статті обґрунтовано, що для ефективної боротьби з військовими формуваннями і терористичними угрупуваннями доцільно застосовувати нові зразки бойових машин – броньовані автомобілі. Бронеавтомобіль «Барс-8» успішно пройшов ходові випробування, бездоріжжя, проходження бродів, ведення вогню, випробування підривом та інші важливі тести. Наведено показники ефективності застосування броньованих автомобілів, викладено погляди на їх використання у складі підрозділів і частин сухопутних військ.

ЛІТЕРАТУРА

1. Шаповал В. В., Радзівілов Г. Д., Османов Р. Н., Сердюк П. Є. Роль і місце сучасних бронеавтомобілів в українських військових формуваннях // Вісник ВІТІ. Комунікаційні та інформаційні системи. 2021. № 2. С. 108–113.

2. Шаповал В. В. Підвищення рівня захищеності пожежних автомобілів локальним бронюванням // Науковий вісник УкрНДІПБ. 2013. № 2 (28). С. 62–64.

3. Астанін В. В., Олефір О. І., Щегель Г. О., Шаповал В. В., Олефір А. О. Композиційні волоконнозміцнені захисні конструкції в умовах ударної взаємодії // Науковий вісник УкрНДІПБ. 2012. № 2 (26). С. 12–20.

4. Астанін В. В., Олефір О. І., Щегель Г. О., Шаповал В. В., Олефір В. С. Полігонні дослідження спричинених пожежею і вибухом ударних пошкоджень // Науковий вісник УкрНДІПБ. 2013. № 2 (28). С. 122–126.

5. Сердюк П. Є., Слюсар В. І. Засоби зв’язку з наземними роботоризованими системами. Сучасний стан і перспективи // Електроніка: наука, технологія, бізнес. 2014. № 7 (139).
С. 66–79.

УДК 621.004.9

канд. техн. наук Штаненко С. С. (ВІТІ ім. Героїв Крут)
Краснобокий А. В. (ВІТІ ім. Героїв Крут)

ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ ШЛЯХОМ ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ КІБЕРБЕЗПЕКИ

У статті розглядається підхід до підвищення кіберстійкості автоматизоаних систем управління технологічними процесами шляхом впровадження інтелектуальних систем кібербезпеки. Передбачається, що в основу побудови запропонованих систем повинно бути покладено поняття «еволюція», тобто здатність адаптації системи через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак). Технічно реалізувати інтелектуальні системи кібербезпеки запропоновано завдяки застосуванню експертної системи і програмованих логічних інтегральних схем, які відносяться до класу катастрофостійких інформаційних систем, характерною особливістю яких, на відміну від відмовостійких систем, є продовження роботи в умовах масових і, можливо, послідовних відмов системи або її підсистем внаслідок проведення кібератак.

Ключові слова: *кібербезпека, автоматизована система управління технологічним процесом, програмована логічна інтегральна схема, експертна система.*

S. Shtanenko, A. Krasnobokyi Enhancing the cyber resilience of automated process control system through the implementation of intelligent cybersecurity systems.

The article discusses an approach to increasing the cyber resilience of an automated process control system through the implementation of intelligent cybersecurity systems. It is assumed that the construction of the proposed systems should be based on the concept of "evolution", that is, the ability of the system to adapt due to changes in parameters under the influence of external and internal cyber threats (cyber attacks). Technically, it is proposed to implement intelligent cybersecurity systems through the use of an expert system and programmable logic integrated circuits, which belong to the class of disaster-resistant information systems, a characteristic feature of which, in contrast to fault-tolerant systems, is the continuation of work in conditions of mass and, possibly consecutive failures of the system or its subsystems as a result of cyberattacks.

Keywords: *cybersecurity, automated process control system, programmable logic integrated circuit, expert system.*

Постановка проблеми

Нові цифрові технології і глобальні інформаційні мережі, які вчинили справжню революцію в сфері накопичення, обміну та обробки інформації, поставили нас перед фактом корінної зміни застарілих принципів її захисту в контексті кібербезпеки.

У сучасних умовах питання кібербезпеки переходять із рівня захисту інформації на окремому об’єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації у вузькому сенсі цього слова, а й усього кіберпростору.

На думку фахівців з кібербезпеки, в технічному плані повний адекватний кіберзахист передбачає побудову та використання таких основних підсистем [1]:

підсистема захисту (*Protection Capabilities*) – забезпечує скритність випромінювань радіоелектронних засобів, систем і засобів зв’язку, комп’ютерну безпеку (*Computer Security*) і інформаційну безпеку (*infosec*);

підсистема виявлення (*Detection Capabilities*) – забезпечує розпізнавання аномалій в мережі завдяки застосуванню систем їх виявлення;

підсистема реагування на зміни технічних параметрів і обстановки (*Reaction Capabilities*) – забезпечує відновлення (реконфігурацію) і виконання інших процесів інформаційних операцій.

Однак, розглянута процедура кіберзахисту не в повному обсязі відображає питання пов’язані із кібербезпекою автоматизованих систем управління технологічними процесами (АСУ ТП), які входять до переліку об’єктів критичної інформаційної інфраструктури та

стали невід'ємною частиною управління сучасними складними технічними системами, що на сьогодні є актуальним та своєчасним завданням.

Аналіз останніх досліджень і публікацій

На сьогодні існує багато наукових робіт, присвячених як автоматизації управління АСУ ТП, так і її безпеці. Зокрема, в роботі [2] інтелектуалізацію розглядають як головний напрямок розвитку автоматизації управління, що можливо реалізувати побудовою нечітких лінгвістичних баз даних, підсистем нечіткого виведення. Подальшим розвитком АСУ ТП є інтеграція інтелектуальних систем підтримки прийняття рішень з класичними *SCADA*-системами, використовуючи сенсорні мережі, інтелектуальні середовища.

Одним з перспективних напрямків розвитку АСУ ТП в роботі [3] вважається розробка експертних систем (ЕС), тобто використання можливостей штучного інтелекту для підвищення ефективності автоматизації технологічних процесів.

В роботі [4] пропонується застосовувати систему контролю вразливостей – один з ефективних методів протидії промисловим кіберзагрозам, які являють собою вузькопрофільні програми, розроблені спеціально для промислових систем автоматизації. Вони дозволяють визначити цілісність внутрішнього середовища пристроїв, зафіксувати всі спроби змінити прикладну програму контролера, зміни в конфігурації мережевих пристроїв захисту і управління в енергомережах.

Метою статті є підхід до створення інтелектуальної системи кібербезпеки (ІСКб), яка спроможна забезпечити захист АСУ ПТ від кібератак, при цьому за технічну реалізацію пропонується застосовувати експертні системи та програмовані логічні інтегральні схеми, які відносяться до класу катастрофостійких систем і здатні протидіяти кібервпливам (кібератакам), тим самим підвищуючи кіберстійкість системи.

Викладення основного матеріалу

Сучасні АСУ ТП являють собою комплекс апаратно-програмних засобів, а також персоналу, призначений для управління різними процесами в рамках технологічного процесу, основним завданням яких є підвищення ефективності управління цими процесами, шляхом мінімізації людської участі в цих процесах.

Якщо розглядати сучасні АСУ ТП з точки зору структурної ієрархії, то очевидним стає питання кібербезпеки таких систем. Це пов'язано з тим, що це типові, багаторівневі, розгалужені людино-машинні системи управління, які представлені на трьох рівнях (рис. 1) [5]:

Рис. 1. Структура АСУ ТП

нижній рівень представлений контрольно-вимірювальними приладами, приладами автоматики, виконавчими пристроями управління, пультами сигналізації;

середній рівень реалізується за допомогою застосування програмованих логічних контролерів;

верхній рівень реалізується шляхом застосування системи диспетчерського управління та збору даних у режимі реального часу (*SCADA*-система – *Supervisory Control And Data Acquisition*).

На сьогодні питання, пов'язані з кібербезпекою АСУ ТП при передачі по мережах і каналах зв'язку, вирішуються шляхом застосування засобів криптографічного захисту інформації вітчизняного виробництва. Однак, забезпечення безпеки сучасного телекомунікаційного обладнання та програмного забезпечення від руйнівних впливів (кібератак) є проблемою, тому що відсутня власна інфраструктура (орендовані канали зв'язку) та використовується іноземне програмне забезпечення і телекомунікаційне обладнання.

За результатами проведеного аналізу [6; 7] можемо зробити висновок, що атаки на інформаційні системи великих світових компаній набувають все більш загрозливих масштабів. На боротьбу з наслідками кіберзлочинів у світі витрачаються величезні гроші. Так, наприклад, ліквідація одного хакерського нападу в середньому обходиться в 150 тис. доларів США, а за підрахунками компанії *McAfee* і центру *CSIS* загальна сума фінансових втрат від кіберзлочинності за 2020 рік складає один відсоток світового ВВП, що становить 820 млрд євро. І це лише тільки початок, враховуючи перехід людства на технологію інтернет-речей (*Internet of Things – IoT*).

Аналіз існуючих підходів щодо кіберзахисту сучасних технологічних систем показує, що одним із перспективних напрямків забезпечення безпеки АСУ ПТ є створення ІСКб, які представлятимуть частину загальної системи інформаційної безпеки. При цьому в основу побудови запропонованих систем має бути покладено поняття «еволюція (розвиток)», тобто здатність адаптації системи через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак) шляхом застосовуваних технологій щодо протидії кібератакам протягом всього життєвого циклу [8].

Передбачається, що ІСКб буде функціонувати на верхньому рівні ієрархії побудови АСУ ТП (інтеграція в *SCADA*-систему). Її основними функціями повинні бути виявлення та

аналіз нових кібератак у процесі моніторингу кіберпростору, а також автоматичний вибір параметрів функціонування АСУ ТП в умовах деструктивних впливів без погіршення її основних характеристик [2].

Основою середнього та нижнього рівнів ієрархічної побудови АСУ ТП повинні стати апаратно-програмні засоби, які відносяться до катастрофостійких інформаційних систем (КАІС). Характерною особливістю таких систем, на відміну від відмовостійких, є збереження даних і продовження роботи в умовах масових і, можливо, послідовних відмов системи та пов'язаних між собою підсистем внаслідок проведення кібератак [9; 10].

Для побудови КАІС потрібні відповідні інструментальні засоби – операційна система, що підтримує багатопроцесорну (розпаралелену) роботу та мови програмування, які здатні конструювати віртуальні обчислювальні структури спеціального виду і описувати виконання масово-паралельних, локальних алгоритмів розв'язання трудомістких завдань.

Нині основним способом розпаралелювання завдань є великоблочне розпаралелювання, коли задача розбивається на великі підзадачі і кожен процесор у складі суперкомп'ютера вирішує виділену йому частину задачі. Однак подібний підхід має ряд недоліків.

По-перше, процесори загального призначення менш ефективні, ніж спеціалізовані пристрої.

По-друге, для вирішення певної задачі більша частина процесорної логіки є надмірною, при цьому створення спеціалізованого комп'ютера, який вирішував конкретні задачі, вимагає великих фінансових і часових витрат.

Інший шлях – це використання реконфігурованих логічних пристроїв, коли є можливість змінювати «внутрішню логіку» процесорів, обходячи перераховані вище проблеми [11]. Одним із таких пристроїв цього класу є програмовані логічні інтегральні схеми (ПЛІС), які використовується для створення сучасних цифрових пристроїв з елементами пам'яті. На відміну від звичайних цифрових мікросхем, логіка роботи ПЛІС не визначається при виготовленні, а задається за допомогою програмування (проєктування). Для програмування використовуються програматор і налагоджувальна середа (*Integrated Development Environment – IDE*), які дозволяють задати бажану структуру цифрового пристрою у вигляді принципової електричної схеми або програми на спеціальних мовах опису апаратури: *Verilog, VHDL, AHD*L та ін.

Сучасні ПЛІС являють собою матрицю програмованих логічних елементів з *CPLD* (*Complex Programmable Logic Device*), *FPGA* (*Field-Programmable Gate Array*), *FLEX* (*Flexible Logic Element Matrix*) структурами, на базі яких створюється абсолютно новий напрямок розвитку мікроелектроніки – універсальні мікропроцесорні системи на кристалі (*System-on-Chip – SoC, System-on-a-Programmable-Chip – SoPC, Multiprocessor System-on-Chip – MPSoC*). Такі складні інформаційні системи класу *SoC* складаються з трьох основних цифрових системних блоків: процесор, пам'ять і логіка (рис. 2).

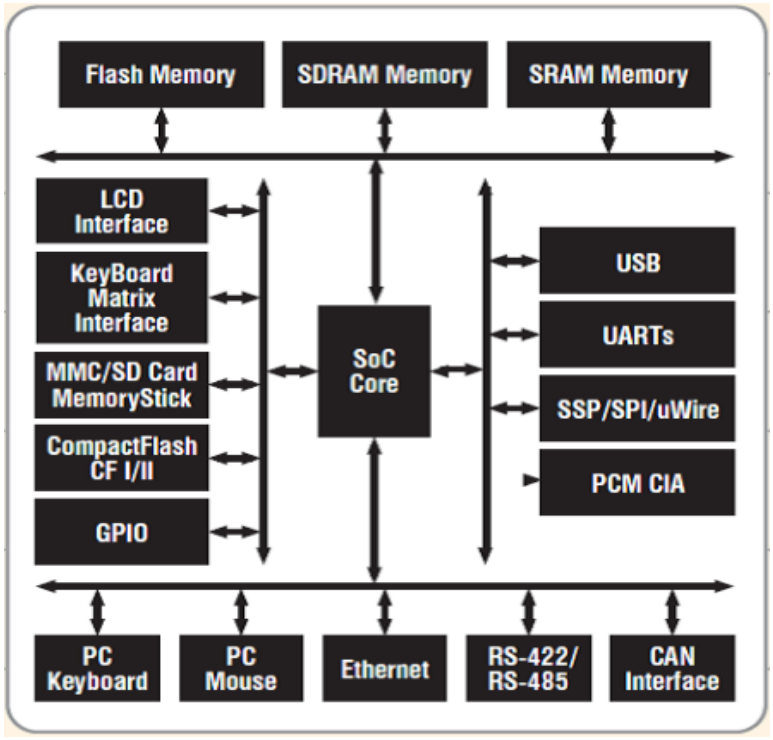


Рис. 2. Структура типової системи на кристалі,
побудованої на основі *ARM*-мікропроцесора

Процесорне ядро реалізує потік управління, коли кожна програма встановлює послідовність виконання операції обробки даних, при цьому дозволяє задавати один з можливих алгоритмів роботи всієї інформаційної системи. Пам'ять використовується за її прямим призначенням – зберігання коду програми процесорного ядра і даних. І нарешті, логіка використовується для реалізації спеціалізованих апаратних пристроїв обробки і проходження даних, склад і призначення яких визначаються кінцевим додатком – потоком даних.

В основі методології проєктування *SoC* лежить принцип повторного використання блоків (*reuse*-блок, *IP*-блок (*Intellectual Property*), складний функціональний блок – СФ-блок), що розробляються в рамках одного проєкту, потім використовуються в інших проєктах.

Фактично весь процес розробки *SoC* ділиться на чотири етапи:

розробка архітектури *SoC* на системному рівні;

вибір *IP*-блоків з бази даних;

проєктування блоків, які залишилися;

інтеграція всіх блоків на кристалі.

Інша принципова особливість *SoC* – це наявність програмованих блоків – процесорів. Виходячи з цього, *SoC* – це не просто інтегральна схема, а комплекс, до складу якого входять як апаратна частина – чип, так і програмна частина – вбудоване програмне забезпечення (*Linux, Windows* тощо) [12; 13].

На сьогодні проєктування *SoC* є розвитком технологій і засобів розробки спеціалізованих інтегральних мікросхем (*Application-Specific Integrated Circuit – ASIC*) і ПЛІС, узагальнена схема традиційного маршруту представлена на рисунку 3.

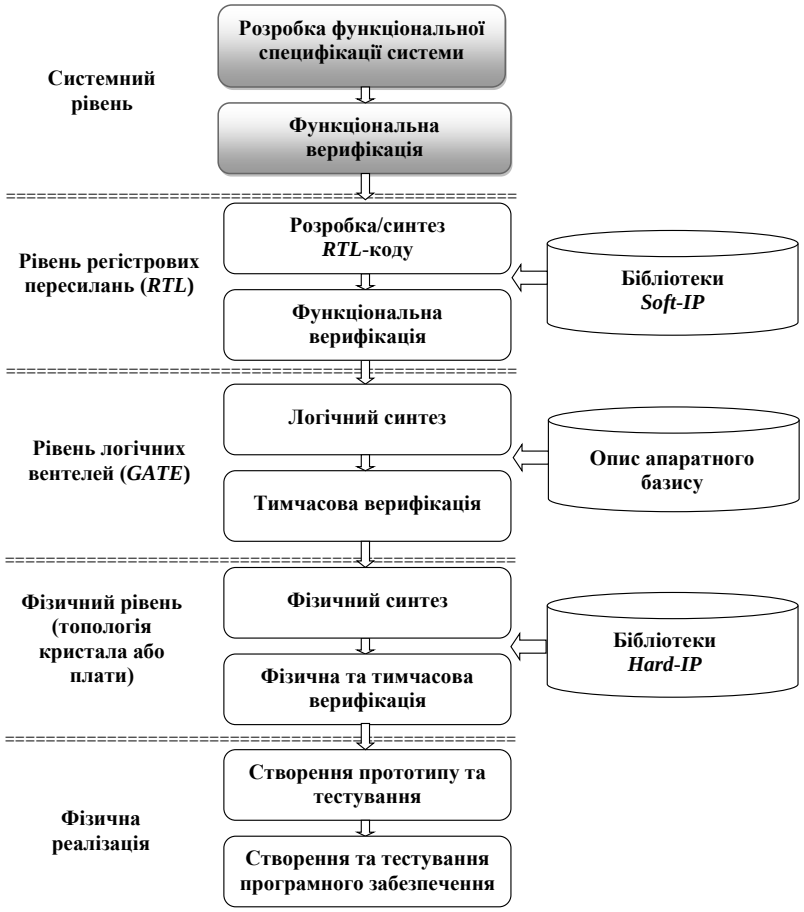


Рис. 3. Узагальнена схема традиційного маршруту

Процес проєктування *SoC* є послідовним, з виділенням технологічних етапів – рівнів, та ітеративним, тобто на кожному етапі можна зробити відкат назад для коригування проєкту. Проєктування програмного забезпечення виконується відокремлено від розробки апаратних засобів, після отримання віртуальних або фізичних прототипів апаратури. На всіх рівнях використовується компонентний підхід. Компоненти – функціональні, схемотехнічні, топологічні і програмні блоки – організовуються в бібліотеки, для повторного використання [14; 15].

Фактично описаний маршрут проєктування не має ніяких принципових відмінностей порівняно з традиційною технологією створення мікропроцесорних систем. При цьому з особливостей слід виділити те, що центральну позицію зайняла програмована апаратура – ПЛІС, з'явилися засоби структурної конфігурації процесорних ядер, САПР ПЛІС, при цьому пакети розробки програмного забезпечення об'єднуються в потужні інструментальні комплекси.

Прикладом такого комплексу може бути САПР фірми *Altera* для проєктування *SoPC* на базі ПЛІС і процесорного ядра *NIOS II*, який містить базові пакети *Quartus II* (ПЛІС), *SoPC Builder* (конфігурується процесорне ядро), *NIOS II IDE* (програмне забезпечення) і багато інших розширень (*DSP Builder, C-to-Hardware Compiler* тощо).

Висновки

Отже, використовуючи реконфігуровані логічні пристрої для створення багатопроцесорних (розпаралелених) структур та експертні системи при побудові інтелектуальної системи кібербезпеки АСУ ТП, ми отримуємо такі переваги, як висока

катастрофостійкість (кіберстійкість), а також продуктивність системи при вирішенні задач, які пов'язані із забезпеченням її кібербезпеки.

При цьому запропоновані катастрофостійкі (кіберстійкі) інформаційні системи мають величезний ресурс резервування і перепрограмування, подальше використання яких пов'язане з оснащенням їх необхідними сенсорами/датчиками в супроводі програм первинної обробки отриманих даних і передачі цих даних на наступні ієрархічні рівні обробки, з метою зберігання та вироблення управлінських рішень.

ЛІТЕРАТУРА

1. Бородакий Ю. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) / Ю. В. Бородакий, А. Ю. Добродеев, И. В. Бутусов // Вопросы кибербезопасности. Москва: НПО «Эшелон», 2014. № 1 (2). С. 5–12.

2. Тарасов В. Б. Интеллектуальные *SCADA*-системы: истоки и перспективы / В. Б. Тарасов, М. Н. Святкина // Машиностроение и компьютерные технологии. 2011. № 13. С. 35.

3. Самойлова Е. М., Игнатьев А. А. Интеграция искусственного интеллекта в автоматизированные системы управления и проектирования технологических процессов // Вестник Саратовского государственного технического университета. 2010. Вып. 1. С. 127–132.

4. Чертков А. Кибербезопасность промышленной автоматизации // Control engineering. 2017. Vol. 2 (68). P. 22–25.

5. Попова Е. П. Автоматизированные системы управления технологическими процессами. Краснодар: ГБПОУ КК КТК, 2015. 44 с.

6. Гункель Е. Ущерб от хакерских атак превысил в мире триллион долларов // Deutsche Welle. URL: https://www.dw.com/ru/ushherb-ot-hakerskih-atak-v-mire-prevysil-trillion-dollarov/a-55858266.

7. Потери бизнеса от кибератак в рф составили более 10 млн рублей в год // RG.ru. URL: https://rg.ru/2017/04/23/poteri-biznesa-ot-kiberatak-v-rf-sostavili-bolee-10-mln-rublej-v-god.html.

8. Самойлова Е. М. Интеграция искусственного интеллекта в автоматизированные системы управления и проектирования технологических процессов / Е. М. Самойлова, А. А. Игнатьев // Вестник Саратовского государственного технического университета. 2010. № 1. С. 127–132.

9. Елугачев П. А. Проблемы математического моделирования кибер-физических систем на транспорте / П. А. Елугачев, Н. В. Лаходынова, Б. М. Шумилов, Э. А. Эшаров // Информационные системы. автоматизация и системы управления известия. СПБГТИ (ТУ), 2020. № 53 (79). С. 107–115.

10. Павлов А. Н. Структурный анализ катастрофоустойчивой информационной системы / А. Н. Павлов, Б. В. Соколов // Труды СПИИРАН. 2009. № 8. С. 128–151. ISSN 2078-9181.

11. Тарасов И. Е. Проектирование конфигурируемых процессоров на базе ПЛИС // Компоненты и технологии. СПб.: Файнстрит, 2006. № 2. С. 78–83.

12. Тарасов И. Е. ПЛИС Xilinx. Языки описания аппаратуры VHDL и Verilog, САПР, приемы проектирования. Горячая линия, Телеком, 2021. 358 с.

13. Vaibbhav Taraate. PLD Based Designwith VHDL RTL Design, Synthesis and Implementation. Springer Nature Singapore Pte Ltd, 2017. 423 p.

14. Строгонов А. В. , "Реализация Verilog-проектов в базисе академических ПЛИС с применением САПР VTR7.0 // Компоненты и технологии. 2017. Вып. 5. С. 12–17.

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

УДК.621.311.68
Яровий В. С. (ВІТІ ім. Героїв Крут)

ДІАГНОСТУВАННЯ ТА УСУНЕННЯ НЕСПРАВНОСТЕЙ ПЕРЕМИКАННЯ РЕЖИМІВ ЖИВЛЕННЯ ВТОРИННОГО ДЖЕРЕЛА ЕЛЕКТРОЖИВЛЕННЯ

Об'єктом дослідження є блок живлення з комутаційним режимом (SMPS). У статті розглянуто один із варіантів діагностування та усунення несправностей, які можуть виникнути внаслідок експлуатації джерел електроживлення з комутаційним режимом (SMPS). Ремонт даних джерел електроживлення досить складний і залежно від того, які елементи вийшли з ладу, навіть затратний. Тому, як приклад розглянуто найбільш поширені несправності, порядок їх виявлення та один із варіантів усунення виявлених несправностей, який зможе заощадити вартість відновлювальних робіт, що є одним із важливих аспектів в умовах сьогодення.
Ключові слова: *діагностування, несправність, вторинне джерело електроживлення.*

V. Yarovyi Diagnosis and troubleshooting of secondary power switching power switching modes.
The object of research is a switching mode power supply (SMPS). In the article, I will consider one of the options for diagnosing and eliminating malfunctions that may occur as a result of the operation of switched-mode power supplies (SMPS). Repairing these power sources is quite difficult and, depending on which elements have failed, even expensive. Therefore, as an example, the most common malfunctions, the order of their detection, and one of the options for eliminating the detected malfunctions, which can save the cost of restoration work, are considered, which is one of the important aspects in today's conditions.
Keywords: *diagnostics, malfunction, secondary power source.*

Постановка завдання

На сьогодні, в XXI столітті, не можливо уявити собі існування людини, процесів, що відбуваються, без технічних засобів, які працюють за допомогою електроенергії. Для забезпечення тих чи інших засобів, які застосовуються людиною, будь-то в повсякденній життєдіяльності, будь-то при виконанні завдань, які ставляться перед державою, електричною енергією, існує багато видів вторинних джерел електроживлення (ВДЕЖ). Для того, щоб техніка, яка працює від електроживлення, була в працездатному стані, необхідно проводити її технічне діагностування. Як ми знаємо, першочерговий вихід з ладу техніки відбувається з причини невідповідності параметрів електроживлення, яким живиться той чи інший об'єкт. Тому в цій статті буде розглянуто варіант діагностування та відновлення працездатності ВДЕЖ.

Особливу увагу треба приділити технічним об'єктам військового призначення. Тому що від того, як швидко буде визначена, а потім усунута несправність ВДЕЖ, в першу чергу, буде залежати оперативність відновлення працездатності (а це дорогоцінний час) всього зразка озброєння та військової техніки (ОВТ), особливо засобів і систем зв'язку та інформатизації (ЗСЗІ). Бо від наявності, а особливо справності ЗСЗІ, залежить боєготовність і оперативність військових підрозділів, особливо в умовах війни рф проти України.

Мета статті

Розгляд варіанта проведення діагностування та відновлення ВДЕЖ, а саме блока живлення з комутаційним режимом (SMPS).

Виклад основного матеріалу

ВДЕЖ, в даному випадку блоки живлення з комутаційним режимом (SMPS), тепер є стандартними для більшості наших побутових приладів, а також технічних засобів військового призначення. Старомодні лінійні джерела живлення на основі трансформаторів мережевої частоти зникають з обігу, в основному через їхню вартість, великі розміри та вагу. У цій статті пропонується розглянути джерела живлення напруги мережі (120 В або 230 В змінного струму) з потужністю від кількох Вт до кількох сотень Вт.

Блоки живлення, які в собі мають комутаційний режим, є всюди. На рисунку 1 продемонстровано їхні, так би мовити, нутрощі. Великі компоненти високої потужності та невеликі радіатори є типовими для таких ВДЕЖ.

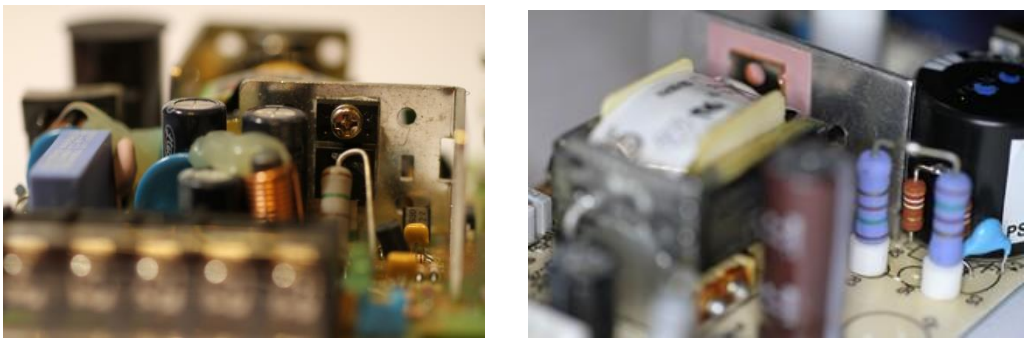


Рис. 1. Приклад внутрішньої частини блоків живлення з комутаційним режимом

Ці пристрої неймовірно надійні, але дуже часто залишаючись без живлення (навіть коли їх навантаження вимкнено), вони все ще залишаються слабкою ланкою. Живлення компонентів здійснюється завдяки високій напрузі, внаслідок чого вони нагріваються, швидко старіють через постійну роботу, а коли виникає стрибок, SMPS є першою складовою частиною техніки, що виходить з ладу. Багато проблем з технікою виникають через несправності джерела електроживлення.

На жаль, ремонт таких ВДЕЖ досить складний. Отже, розглянемо деякі основні ідеї та прийоми, які можливо використовувати як варіант діагностування та відновлення працездатності.

Припустимо, що у нас є ідеально розроблена схема джерела електроживлення, яка раніше працювала ідеально, але вона раптово вийшла з ладу. Спочатку необхідно розглянути загальну блок-схему SMPS, що зображена на рисунку 2.

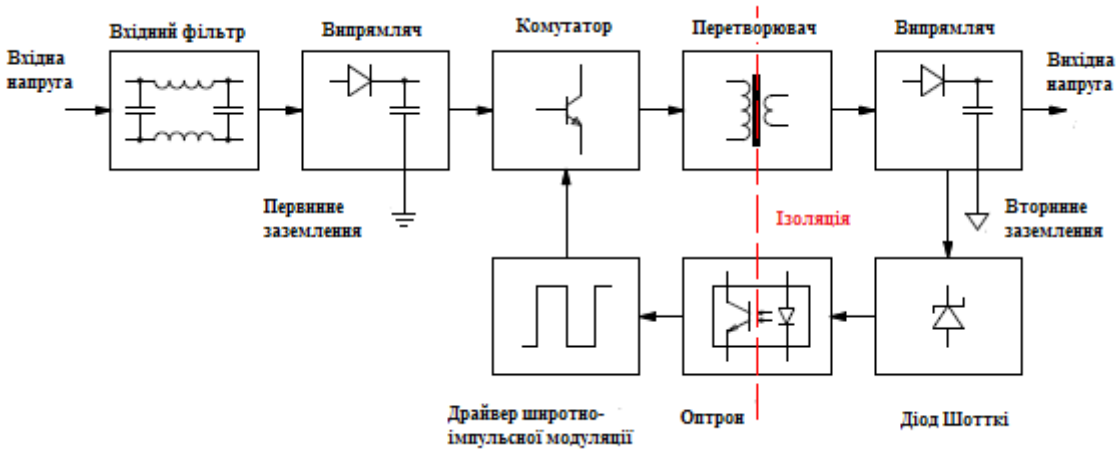


Рис. 2. Структура загальної блок-схеми SMPS

Живлення мережі надходить у ланцюги через мережевий фільтр, воно випрямляється і згладжується для отримання високої напруги постійного струму (кілька сотень вольт). Деякі випрямлячі мають перемикач, який збільшує напругу при роботі з мережею 120 В змінного струму або просто випрямляч при роботі з 230 В. Деякі інші призначені для роботи від 100 В до 240 В змінного струму без перемикачів, а все інше зробить регулятор. Ця висока напруга постійного струму перемикається одним або кількома транзисторами для керування первинною обмоткою феритового трансформатора. На вторинній обмотці напруга випрямляється і фільтрується. Перемикаючі транзистори керуються схемою управління, яка визначає вихідну напругу (і вхідний струм) і відповідно регулює. Ця схема управління дуже часто знаходиться на первинній обмотці і часто живиться від додаткової обмотки трансформатора. Зразок вихідної напруги повертається через оптрон. У деяких випадках

схема керування розташована на вторинній обмотці й керує транзисторами через невеликий додатковий трансформатор. Усі конфігурації мають додаткову схему, яка дозволяє контролеру запускатися при появі живлення.

Завжди існує дуже чітке розділення між сторонами високої та низької напруги (первинною та вторинною обмотками). Це ми можемо побачити на нижній (мідній) стороні друкованої плати як більшого інтервалу у доріжках. Декілька разів у цій зоні видаляється лак для паяльної маски або є отвори та прорізи для збільшення ізоляції. На рисунку 3 цей розподіл позначено пунктирною червоною лінією.

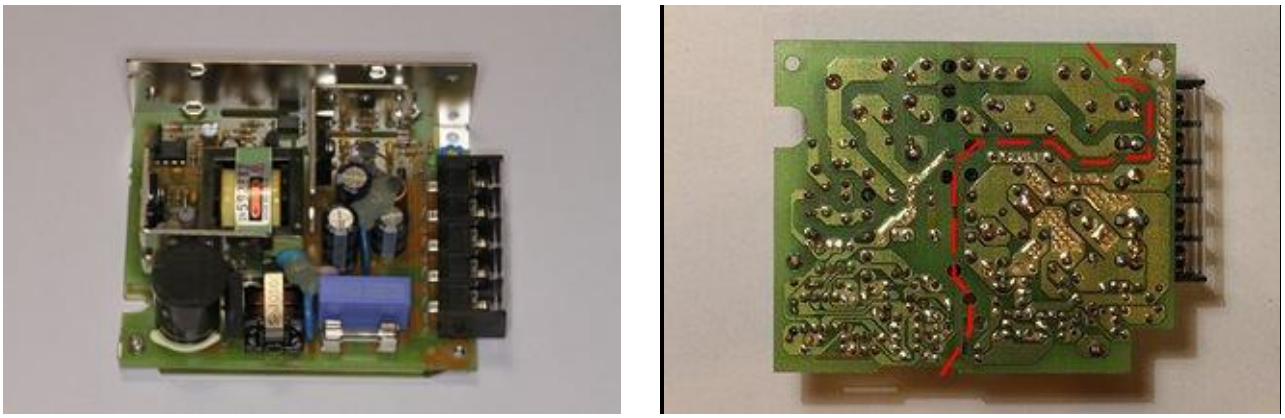


Рис. 3. Варіант розподілу між первинною і вторинною обмотками в класичному стилі

Ця SMPS має розміщення елементів у класичному стилі (наскрізні отвори). Сторона високої напруги знаходиться зліва від пунктирної червоної лінії (рис. 4).

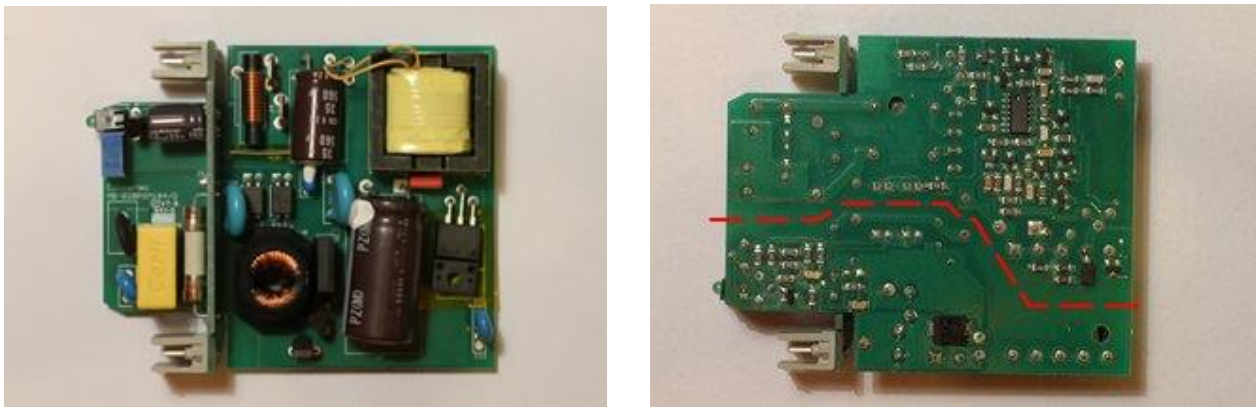


Рис. 4. Варіант розподілу між первинною і вторинною обмотками в сучасному виконанні

Ця SMPS має розміщення сучасних елементів для поверхневого монтажу (SMD). Тут контролер використовує технологію SMD і кріпиться з нижньої сторони. Великий SMD-діод є низьковольтним випрямлячем. Сторона високої напруги знаходиться над пунктирною червоною лінією.

Первинна і вторинна обмотки повністю ізольовані трансформатором постійного струму. Дуже часто, якщо заземлення виходу не підключено до заземлення мережі, невеликий високовольтний конденсатор з'єднує ці дві землі на високій частоті.

Світло-блакитний конденсатор на рисунку 5 є високовольтним конденсатором, який з'єднує низьковольтну землю з заземленням мережі. Звичайно, також є ізоляція постійного струму.

Рис. 5. Зображення високовольтного конденсатора

Перед тим, як проводити діагностування та подальше відновлення несправних елементів, необхідно обов'язково дотримуватися заходів безпеки.

Перед початком робіт необхідно пам'ятати, що SMPS має небезпечні ланцюги: половина елементів схеми безпосередньо підключена до напруги мережі. Великий накопичувальний конденсатор заряджається високою напругою і може бути небезпечним навіть при відключенні електромережі. Не всі SMPS включають проточні резистори (або вони можуть бути несправними), тому конденсатори можуть залишатися зарядженими протягом тривалого часу. Перед початком робіт обов'язково необхідно переконатися, що всі конденсатори повністю розряджені. Щоб розрядити конденсатори, не потрібно замикати їх за допомогою викрутки, замість цього необхідно використовувати відповідний резистор (кілька кОм і кілька Вт), підключений до двох ізольованих щупів, таких, наприклад, як у мультиметра. Після чого необхідно виміряти напругу та переконатися, що вона дорівнює нулю, перш ніж продовжити. Необхідно також мати на увазі, що радіатори дуже часто не заземлені, і вони цілком можуть бути під напругою мережі. Також, використовуючи осцилограф, потрібно бути обережним, бо осцилографи заземлені до джерела живлення, внаслідок чого може статися коротке замикання проводом заземлення (це небезпечно для осцилографа). Тому відновленням справності SMPS повинні проводити досвідчені і кваліфіковані спеціалісти.

Цей SMPS (рис. 6) не має зливного резистора на конденсаторі фільтра високої напруги. Необхідно в даному випадку звернути увагу на резистор 330 кОм, який припаяний на нижній стороні друкованої плати під час ремонтно-відновлювальних робіт, щоб автоматично вчасно розрядити конденсатор і уникнути потенційних ударів електрострумом. На рисунку 6 сторона високої напруги знаходиться праворуч від пунктирної червоної лінії.

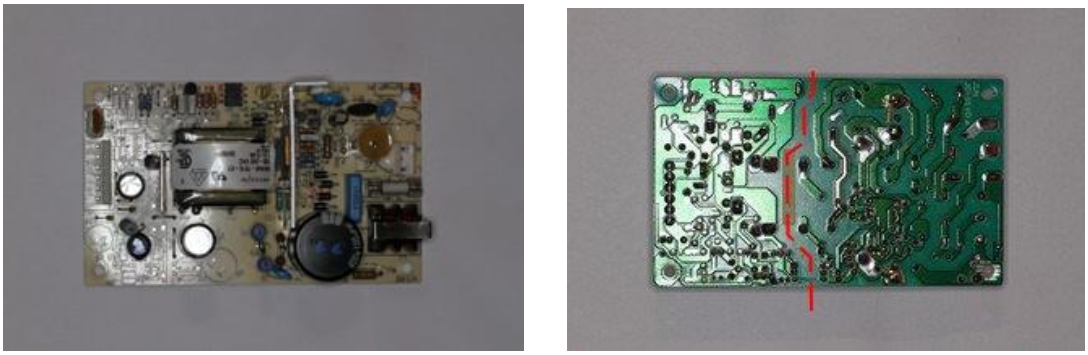


Рис. 6. SMPS без зливного резистора на конденсаторі фільтра високої напруги

Перш ніж приступити до роботи, необхідно провести зовнішній огляд, щоб візуально визначити, якщо це видно, цілісність елементів плати. Зазвичай, спочатку вимикається

живлення SMPS і перевіряється, чи всі конденсатори плати розряджені. Зазвичай несправний електролітичний конденсатор, якщо він не вибухнув, можна легко помітити, оскільки він «роздувається», а його верхня (або нижня) сторона стає куполоподібною. Несправний резистор, який згорів, також можна помітити – він має чорний колір та неприємний запах. Також дуже важливим кроком є огляд феритового трансформатора, якщо він перегорів, то він має відповідний колір та неприємний запах. Зазвичай в ньому закорочуються витки, його відновлення економічно не доцільне, а пошук іншого для заміни є доволі проблематичним. Якщо трансформатор виявився несправним, то доцільніше замінити весь SMPS, що заощадить багато часу. Деякі радіоелементи при роботі нагріваються, і з часом вони приймають світло-коричневий відтінок (те саме стосується частини плати біля них, де вони розміщені): це не завжди є проблемою; світло-коричневий відтінок — це є нормально, чорний, який має неприємний запах – ні.

Перш за все необхідно оглянути мережевий запобіжник SMPS на предмет його цілісності (рис. 7), це дасть нам підказку щодо походження несправності. Перегорілий запобіжник (рис. 8) зазвичай означає багато несправних напівпровідників, цілий, ймовірно, обмежується одним елементом.

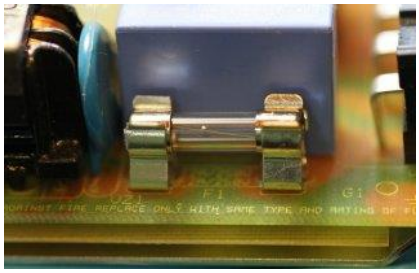


Рис. 7. Справний мережевий запобіжник

Рис. 8. Три запобіжники Ø5 × 20 мм: ліворуч – цілий; посередині – згорів помірним струмом; праворуч – згорів великим струмом

При перевірці запобіжника необхідно звернути увагу на те, який він має вигляд: якщо він лише повільно горів, то несправність не буде катастрофічною, але якщо запобіжник майже «вибухнув», то це свідчить про те, що був великий струм, відповідно коли він вибухнув, слід очікувати багато пошкоджених елементів (особливо напівпровідників). Це не означає, що відновлення не можливе, але слід очікувати, що доведеться провести заміну багатьох елементів. На жаль, деякі запобіжники заповнені піском, і тоді оцінити несправність буде складніше.

Розглянемо декілька варіантів виникнення несправностей.

Відсутність вихідної потужності. SMPS може виходити з ладу різними способами, найпоширенішим є відсутність вихідної потужності. У цьому випадку необхідно почати з перевірки вхідного запобіжника. Якщо запобіжник справний, але на виході немає нічого, ймовірно, всі напівпровідники справні. Зазвичай напівпровідники розриваються закороченими, а резистори (і часто конденсатори) розриваються відкритими.

Одним із варіантів може бути обмежувач пускового струму (NTC). Наступним кроком є перевірка резисторів високої потужності, особливо на первинній обмотці, їхній опір вимірюється по одному в ланцюзі. Якщо значення не відповідає написаному (або кольоровому коду) елементу, необхідно випаяти один елемент і виміряти знову, якщо значення не відповідає заданому, проводиться заміна його на новий.

Перші резистори, які перевіряються, – це резистори, які розміщені послідовно з силовими транзисторами, зазвичай менше ніж один Ом. Іноді регулятор живиться від резистора високої потужності, послідовно зі стабілітроном: якщо резистор справний,

можливо, стабілітрон замикається, тому виникає необхідність перевірити всі діодні переходи за допомогою діодної функції мультиметра. Потім проводиться перевірка конденсаторів.

Відсутність вихідної потужності, перегорів запобіжник. З іншого боку, якщо запобіжник згорів, то в ланцюзі щось пішло не так. Поки що міняти запобіжник не потрібно, бо він просто згорить знову: десь виникло коротке замикання, яке необхідно спочатку усунути. Типовими проблемами є підірвані силові транзистори або випрямні діоди, особливо на первинній обмотці. Необхідно, за допомогою діодної функції мультиметра, перевірити з'єднання, це легко помітити. Багато елементів можуть бути несправними одночасно, і якщо їх усі не замінити, вони можуть знову вибухнути, тому треба бути обережним. Потім необхідно провести перевірку на наявність несправних резисторів, як вказано вище, і несправних конденсаторів.

Якщо силовий транзистор не працює, велика ймовірність того, що багато інших елементів схеми теж не працюють. Часто SMPS включають компоненти захисту, такі як додатковий резистор або стабілітрони, щоб зменшити пошкодження в разі відмови, але не завжди. Перш ніж продовжити заміну, необхідно переконатися, що перевірені всі елементи. Наприклад, перевіряємо, чи все ще працює мікросхема контролера. Доцільно заживити його в автономному режимі за допомогою невеликого зовнішнього джерела живлення постійного струму та перевірити наявність імпульсів на базі транзистора (або затворі). Але деякі мікросхеми не працюватимуть, якщо немає високої напруги для перемикання: спочатку перевіряємо таблицю даних. Якщо занадто багато елементів непрацездатні, ймовірно, доцільніше замінити весь SMPS.

Для того, щоб замінити напівпровідники потрібно спочатку знайти такі самі. Якщо вони недоступні (або занадто дорогі), можна підібрати альтернативні. Звісно, новий напівпровідник повинен мати принаймні такі ж характеристики напруги, струму та потужності або навіть кращі. Для діодів також перевіряється час перемикання: потрібен діод, який принаймні такий же швидкий, як старий, або швидше. Для транзистора перевіряється коефіцієнт посилення та частота зрізу. Для MOSFET перевіряється ємність затвора, яка не повинна перевищувати ємність старого елемента, який замінюється, і порогову напругу затвора, яка має бути подібна до старого елементу.

Після заміни несправних елементів, для першого включення живлення, найпростіший спосіб тестування з використанням лампочки. Цей спосіб обмежить пошкодження, якщо несправність не буде повністю усунуто.

SMPS частково працює. Іноді SMPS може працювати лише частково: він може запускатися на частку секунди, а потім вимикатися, або він може видавати імпульси, намагаючись запуститися кожні кілька секунд і вимикатися через частку секунди, або може видавати неправильну вихідну напругу. В даному випадку, напевно, всі силові напівпровідники справні, тому перше, що потрібно перевірити, це конденсатори.

Крім того, може бути щось не так зі схемою зворотного зв'язку: дієвий метод – подати зовнішню регульовану напругу постійного струму до виходу SMPS (SMPS не підключений до мережі). При поступовому збільшенні напруги постійного струму ми повинні побачити, що ланцюг зворотного зв'язку працює, якщо ми перевищуємо поріг близько номінальної вихідної напруги. Оскільки під час виконання цього тесту немає небезпечних напруг, то для діагностики схеми зворотного зв'язку можна скористатися осцилографом (рис. 9). Можливе також підключення мікросхеми контролера (на первинній обмотці) з тим же джерелом низької напруги, щоб побачити, що відбувається на іншій стороні оптрона.

Рис. 9. Перевірка ланцюга зворотного зв’язку

Перевірка конденсаторів. Електролітичні конденсатори дуже часто стають причиною несправності SMPS. У дешевих конструкціях, де тепловиділення занадто близьке до межі, а вибір компонентів занадто орієнтований на вартість, електролітичні конденсатори є справжніми бомбами уповільненого часу, які в кінцевому підсумку виходять з ладу (іноді буквально вибухаючи). Рідина, електроліт усередині цих елементів має тенденцію випаровуватися та висихати, повністю змінюючи характеристики.

Два синіх електролітичних конденсатора на рисунку 10 є конденсаторами фільтра низької напруги. Ці конденсатори справні.

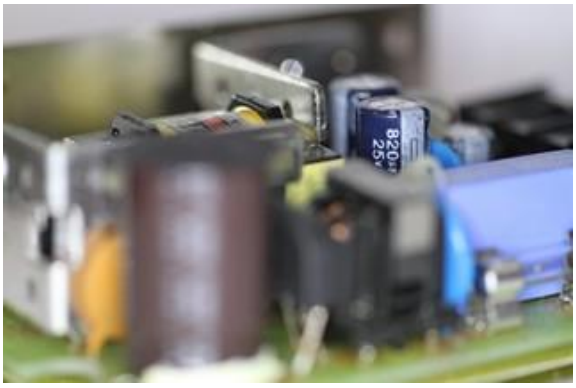


Рис. 10. Вигляд електролітичних конденсаторів

Великий коричневий електролітичний конденсатор на рисунку 11 є високовольтним фільтруючим конденсатором. Цей конденсатор справний.

Рис. 11. Високовольтний фільтруючий конденсатор

Коли електролітичні конденсатори вибухають, вони викидають виступи та мають характерний неприємний запах. Елементи, що розірвалися, легко помітити, але перш ніж йти далі, слід перевірити стан решти ланцюга. Якщо він не може бути очищений або вже занадто покрився корозією, заміна всього SMPS є найкращим і доцільнішим варіантом, оскільки корозійні компоненти або мідні доріжки друкованої плати в підсумку вийдуть з ладу.

На щастя, вибухають не всі електролітичні конденсатори, більшість із них просто безшумно виходять з ладу. Перш за все необхідно візуально оглянути всі конденсатори, їхню форму та сусідство. Якщо їхня форма не циліндрична, або так би мовити «надута» (рис. 12), має куполоподібну верхню або нижню сторону (замість того, щоб бути плоскою) або протікає, то такі конденсатори несправні. Не потрібно витрачати час на вимірювання їхніх параметрів, якщо вони візуально мають не гарний вигляд, вони на 100 % несправні та потребують заміни.

Рис. 12. Загальний вигляд електролітичних конденсаторів:
ліворуч – «надутий» порівняно з новим, що праворуч

Але є такі електролітичні конденсатори, які можуть бути несправними і при цьому на вигляд як нові. Єдиний спосіб знайти несправні – це виміряти їхні параметри. Проведення вимірювання ємності не завжди є достатнім заходом. Набагато краще виміряти еквівалентний послідовний опір (ESR) і порівняти його з завідомо справним конденсатором.

Для заміни несправних необхідно використовувати тільки нові конденсатори.

Діагностування за допомогою лампочки. Після заміни всіх несправних елементів все ще існує ймовірність їх виходу з ладу, особливо якщо спочатку перегорів запобіжник. Отже, при першому тестуванні необхідно замінити запобіжник на лампочку 100 Вт або підключити її послідовно з мережею змінного струму (рис. 13). Приблизно така ж потужність лампочки SMPS. Це обмежує потужність на випадок, якщо коротке замикання ще не усунено, запобігає постійній зміні запобіжників.

Рис. 13. Підключення лампочки послідовно з мережею змінного струму

Коли вмикається живлення (без навантаження), можемо спостерігати, як лампочка блимає на частку секунди, а потім гасне (або злегка світиться). Якщо все ще є коротке замикання, лампочка буде світитися яскраво і стабільно. Тому необхідно швидко вимкнути живлення, розрядити всі конденсатори і знову шукати несправності.

Висновок

У цій статті було розглянуто один із варіантів діагностування та усунення несправностей ВДЕЖ. Цей варіант може зменшити фінансові затрати на відновлення, якщо проводити заміну всього джерела живлення, але може збільшити час на саме діагностування і відновлення, якщо вийшло з ладу багато елементів схеми, внаслідок чого зростуть трудовитрати і, відповідно вартість самої оплати праці фахівця-ремонтника.

Напрямки подальших досліджень. У подальшому необхідно провести дослідження щодо математичного, а також фінансового порівняння витрат на заміну SMPS, діагностування з подальшим відновленням поелементно та витрат часу на виконання вказаних робіт.

ЛІТЕРАТУРА

1. Схемотехніка електронних систем: у 3 кн. Кн. 1. Аналогова схемотехніка та імпульсні пристрої: підручник / В. І. Бойко, А. М. Гуржій, В. Я. Жуйков та ін. 2-ге вид., допов. і перероб. Київ: Вища школа, 2004. 366 с.: іл.

2. Козирський В. В., Волошин С. М. Основи електропостачання: підручник. Київ, 2021. 527 с.

АВТОРИ СТАТЕЙ

1. ***Баканов Валентін Сергійович*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

2. ***Головко Олена Євгеніївна*** – науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

3. ***Дикий Олександр Вікторович*** – начальник науково-дослідної лабораторії науково-дослідного управління (перспектив розвитку телекомунікаційних систем) Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

4. ***Драглюк Олексій Вікторович*** – начальник відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

5. ***Зінченко Михайло Олександрович*** – начальник науково-дослідного управління (перспектив розвитку телекомунікаційних систем) Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

6. ***Карпенко Андрій Олександрович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

7. ***Коротков Михайло Михайлович*** – провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

8. ***Кузавков Василь Вікторович*** – начальник кафедри побудови телекомунікаційних систем факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

9. ***Краснобокий Андрій Васильович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

10. ***Куцаєв Володимир Вікторович*** – науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

11. ***Лазута Роман Григорович*** – старший науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

12. ***Лазута Роман Романович*** – начальник відділу наукового центру Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

13. ***Макарчук Василь Іванович*** – старший науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

14. ***Марчук Олександр Віталійович*** – викладач кафедри кібербезпеки факультету бойового застосування систем управління та зв'язку Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

15. ***Михайлюк Сергій Станіславович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

16. ***Мусієнко Володимир Анатолійович*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

17. ***Османов Руслан Нарімановіч*** – начальник науково-дослідного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна

18. ***Павлюк Дмитро Олександрович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

19. ***Погребняк Сергій Васильович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

20. ***Пономаренко Зоя Миколаївна*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

21. ***Радзівілов Григорій Данилович*** – кандидат технічних наук, доцент, заступник начальника Військового інституту телекомунікацій та інформатизації імені Героїв Крут з наукової роботи, м. Київ, Україна.

22. ***Радченко Микола Миколайович*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

23. ***Руденко Володимир Іванович*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

24. ***Сердюк Павло Євгенійович*** – заступник командира роти Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

25. ***Сінько Вікторія Володимирівна*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

26. ***Хусаінов Павло Валентинович*** – професор кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

27. ***Шаповал Віталій Михайлович*** – начальник науково-дослідного відділу (математичного та програмного забезпечення) Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

28. ***Штаненко Сергій Станіславович*** – докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

29. ***Шугалій Ольга Олександрівна*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

30. ***Шкіцький Дмитро Володимирович*** – головний спеціаліст відділу інформаційних сервісів Управління інформаційних технологій Міністерства оборони України, м. Київ, Україна.

31. ***Яковчук Олександр Вікторович*** – начальник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

32. ***Яровий Віталій Сергійович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

ПАМ'ЯТКА АВТОРУ

Рукопис статті потрібно подавати разом із зазначеними нижче документами українською мовою:

– *актом експертизи* (1 примірник);

– *рецензіями (зовнішньою або внутрішньою)* – за підписом провідного ученого, який працює в даному напрямку досліджень;

– *довідкою про автора (авторів).*

Рукопис, оформлений у текстовому редакторі **Microsoft Word 10** (не нижче), подається у двох видах:

на флеш-пам'яті або CD;

роздрукований на лазерному принтері (1 примірник);

а також може бути надісланий за електронною адресою **naukaviti@gmail.com.**

Формат аркуша – **А4 (210 мм × 297 мм).**

Розмір полів: зліва – **20 мм**, справа – **20 мм**, зверху – **20 мм**, знизу – **20 мм.**

Стиль – **normal** (звичайний); інтервал між рядками – **1,0;** абзацний відступ – **1 см.** Шрифт – **Times New Roman,** розмір шрифту – **12 пт,** із виключенням переносів.

Анотацію друкують курсивом, шрифт **Times New Roman,** розмір шрифту – **10 пт.** Анотацію та ключові слова подають українською та англійською мовами. Обсяг кожної анотації з ключовими словами – не менше ніж **1800 знаків** з пробілами. Анотація повинна бути структурована так: вступ, проблематика, мета, матеріали й методи, результати, висновки. Іншими словами, анотація повинна відображати послідовну логіку опису результатів, описувати основну мету дослідження та підсумовувати найбільш значимі результати. Скорочення слів в анотації не застосовувати.

Після анотації – 3–4 ключові слова українською та англійською мовами.

Література оформляється шрифтом **12 пт.**

Етапи представлення статті для науковців інституту:

1. Стаття подається на розгляд головному редактору та після погодження – відповідальному редактору (науково-організаційний відділ інституту).

2. Після позитивного розгляду редколегією стаття подається коректору (кімната № 5 редакційно-видавничого відділу) для вичитки та корегування.

Виправлення електронного варіанта статті.

Друкування виправленого варіанта статті, отримання розпису коректора про виправлення помилок, що були виявлені, на останньому аркуші статті.

3. Виправлена стаття передається разом із супровідними документами відповідальному редактору для формування комп'ютерного макета збірника.

Не приймаються праці, у яких відсутній повний опис наукових результатів, що засвідчує їх, достовірність, або в яких повторюються результати, опубліковані раніше в інших наукових працях, що входять до списку основних (Постанова ВАК України від 10.02.99 р. № 1 – 02/3).

Статті, які містять загальновідому науково-технічну інформацію, плагіат, не розглядаються й не друкуються.

Редакційна колегія залишає за собою право вносити в рукопис зміни редакційного характеру.

Телефон для довідок: 256-22-37, 256-22-73, внутрішній 442-37, 442-73. Електронна адреса для надання статей: **naukaviti@gmail.com, naukaviti@viti.edu.ua.**