МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ
№ 4(47), 2016
ВИДАЄТЬСЯ ЩОКВАРТАЛЬНО

ЗАСНОВНИК

Державний науково-дослідний інститут МВС України; Національний авіаційний університет; Національна академія внутрішніх справ

НАКАЗОМ

МОН України від 16.05.2016 № 515 науково-практичний журнал "Сучасна спеціальна техніка" включено до переліку наукових фахових видань України з технічних наук

ЗАРЕЄСТРОВАНО

Міністерством юстиції України 13 лютого 2015 року
Свідоцтво – серія КВ № 21221-11021Р

НАУКОВА РАДА

д.т.н. Богданов О.М., д.т.н. Додонов О.Г., д.т.н. Дудикевич В.Б.,
д.т.н. Задирака В.К., д.ю.н. Проценко Т.О.

РЕДАКЦІЙНА КОЛЕГІЯ:

Головний редактор
доктор технічних наук Рибальський О.В.

Заступник головного редактора
доктор технічних наук Хорошко В.О.

Відповідальний секретар
кандидат технічних наук Марченко О.С.

д.т.н. Єрохін В.Ф.
д.т.н. Железняк В.К.
д.т.н. Карпінський М.П.
д.ю.н. Криволапчук В.О.
д.т.н. Кобозева А.А.
д.т.н. Конахович Г.Ф.
д.т.н. Корченко О.Г.
д.т.н. Ленков С.В.
д.т.н. Максимович В.М.
д.в.н. Мосов С.П.
д.т.н. Мохор В.В.
д.ю.н. Орлов Ю.Ю.
д.т.н. Юдін О.К.
к.ю.н. Артеменко П.П.
к.ю.н. Лопатін С.І.
к.т.н. Писаренко В.Г.
к.ю.н. Садченко О.О.
к.ю.н. Смерницький Д.В.
к.т.н. Циганов О.Г.

Рекомендовано до друку рішенням Вченої ради ДНДІ МВС України
(протокол № 6 від 07.12.2016 р.)

За точність викладеного матеріалу відповідальність несуть автори статей та їх рецензенти.

При передруку матеріалів посилання на науково-практичний журнал "Сучасна спеціальна техніка" є обов'язковим

© Державний науково-дослідний інститут МВС України, 2016

СИСТЕМИ ТА МЕТОДИ ОБРОБКИ ІНФОРМАЦІЇ

Лєнков С.В., Лєнков Є.С. Формалізована методика оптимізації параметрів стратегії технічного обслуговування за ресурсом складних виробів тривалої експлуатації 3

Лопатін С.І., Буран В.В. Перспективні напрями розвитку систем відеоаналітики 9

Мовчан М.А., Осьмак С.Г. Експериментальні методи визначення ефективності захисних матеріалів під час впливу засобів ураження 15

Самчишин О.В., Орищук І.О. Методика складання рейтингу електронних засобів масової комунікації при організації процесу їх контент-моніторингу 21

Хорошко В.О., Грищук Р.В. Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї 30

Хорошко В.А., Хохлачева Ю.Е., Моржова Л.И. Выбор элементной базы для беспилотного летательного аппарата 37

Шевченко А.С. Комплексний підхід до побудови системи кібернетичного захисту Збройних Сил України 47

Юрх Н.Г. Оценка эффективности защиты речевой информации 55

ОЗБРОЄННЯ ТА СПЕЦАВТОТРАНСПОРТ

Бакал В.П., Александров М.Є., Дмитрук В.А. Історія розвитку розвантажувальних систем бойового спорядження військовослужбовців у XX ст. 63

Будзинський М.П., Диких О.В., Кисіль М.В., Приходько В.І. Аспекти створення броньованого патрульного катера для спеціальних підрозділів Національної гвардії України 72

Марченко О.С., Вяткіна Л.П. Пересувні блокпости модульної конструкції 81

Толок І.В. Удосконалення процесу технічного обслуговування складних відновлюваних об'єктів авто- та бронетехніки за допомогою імітаційної статистичної моделі 90

СПЕЦІАЛЬНІ РОЗРОБКИ

Білогуров В.А., Заїчко К.В. Огляд систем виявлення та протидії безпілотним повітряним суднам в умовах міської забудови 96

Неня О.В. Сучасні тепловізори для спеціального та повсякденного застосування 108

НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ

Филь Р.С., Филь С.П. Загальні положення про судову експертизу об'єктів права інтелектуальної власності 121

СИСТЕМИ ТА МЕТОДИ ОБРОБКИ ІНФОРМАЦІЇ

УДК 62-7

С.В. Лєнков,
доктор технічних наук, професор,
Є.С. Лєнков,
кандидат технічних наук

ФОРМАЛІЗОВАНА МЕТОДИКА ОПТИМІЗАЦІЇ ПАРАМЕТРІВ СТРАТЕГІЇ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЗА РЕСУРСОМ СКЛАДНИХ ВИРОБІВ ТРИВАЛОЇ ЕКСПЛУАТАЦІЇ

У статті проаналізовані процеси оптимізації параметрів стратегії технічного обслуговування за ресурсом складних виробів тривалої експлуатації. Розроблена формалізована методика на основі алгоритму розв'язання задачі формалізації параметрів технічного обслуговування.

Ключові слова: *технічне обслуговування, надійність, задача оптимізації, ресурс.*

В статье проанализированные процессы оптимизации параметров стратегии технического обслуживания за ресурсом сложных изделий длительной эксплуатации. Разработанная формализированная методика на основе алгоритма решения задачи формализации параметров технического обслуживания.

Ключевые слова: *техническое обслуживание, надежность, задача оптимизации, ресурс.*

In the paper the processes of an optimization of parameters of the strategy of technical service are after the resource of difficult wares of the protracted exploitation are analyzed. Formalized methodology on the basis of algorithm of the decision of the task of formalization of parameters of technical service is worked out.

Keywords: *technical service, reliability, task of optimization, resource.*

Вступ та постановка проблеми

Показники надійності та вартості експлуатації будь-яких складних відновлювальних технічних об'єктів тривалої експлуатації залежать не тільки від конструктивних і технологічних особливостей їх проектування та виробництва, а й від властивостей ремонтопридатності та обслуговуваності, а також від параметрів, закладених у процеси технічного обслуговування (ТО) і ремонту. У цій статті розв'язується задача оптимізації параметрів стратегії ТО за ресурсом.

Виклад основного матеріалу

Задача оптимізації параметрів стратегії ТО за ресурсом представлена такими двома постановками:

за критерієм мінімальної вартості $\min c_э$:

$$T_0(\mathrm{P}^*_{\text{тор с}}) \geq T_0^{\text{тр}};$$

$$c_{\text{э}}(\mathrm{P}^*_{\text{тор с}}) = \min_{\mathrm{P}_{\text{тор}}} c_{\text{э}}(\mathrm{P}_{\text{тор}}), \quad (1)$$

за критерієм максимального коефіцієнта технічного використання $\max K_{\text{ти}}$:

$$T_0(\mathrm{P}^*_{\text{тор к}}) \geq T_0^{\text{тр}};$$

$$K_{\text{ти}}(\mathrm{P}^*_{\text{тор с}}) = \max_{\mathrm{P}_{\text{тор}}} K_{\text{ти}}(\mathrm{P}_{\text{тор}}), \quad (2)$$

де $\mathrm{P}_{\text{тор}}$ – узагальнений параметр, що описує стратегію ТО за ресурсом; $\mathrm{P}^*_{\text{тор с}}$ і $\mathrm{P}^*_{\text{тор к}}$ – оптимальні значення параметра стратегії ТО за ресурсом, що визначаються за критерієм $\min c_{\text{э}}$ і $\max K_{\text{ти}}$ відповідно.

Параметр $\mathrm{P}_{\text{тор}}$ був визначений таким чином [1]:

$$\mathrm{P}_{\text{тор}} = \left\{ \left\langle E_{\text{то}\,j}, T_{\text{то}\,j} \right\rangle; j = \overline{1, N_{\text{то}}} \right\},$$

де $N_{\text{то}}$ – кількість видів ТО; $E_{\text{то}\,j}$ і $T_{\text{то}\,j}$ – відповідно множина обслуговуваних елементів і періодичність ТО j-го виду.

При розробці стратегії ТО за ресурсом, зазвичай, встановлюється постійна періодичність проведення ТО різних видів, “своя” для кожного виду. Принципово важливим є те, що при проведенні ТО за ресурсом обслуговуються (замінюються) всі елементи, включені у відповідні підмножини $E_{\text{то}\,j}$.

Вихідною інформацією для розв’язання таких задач є:

$E_{\text{то}}$ – множина потенційно обслуговуваних елементів даного об’єкта;

$T_0^{\text{тр}}$ – задане необхідне значення середнього наробітку на відмову, яке повинно забезпечуватися при проведенні технічного обслуговування.

Звичайно ж, вихідною інформацією також є вся інформація про об’єкт, яка необхідна для роботи імітаційної статистичної моделі, ця інформація вводиться в базу даних, за допомогою якої отримуються оцінки цільових функцій задач T_0, $c_{\text{э}}$ і $K_{\text{ти}}$ [2].

На рис. 1 представлено алгоритм, який є формальним описом методики розв’язання задачі (1).

Розглянемо коротко роботу алгоритму.

Оператор 1 встановлює початкові значення змінних: i – номер кроку процесу пошуку розв’язання; j – номер виду технічного обслуговування.

Оператор 2 створює допоміжну (спочатку порожню) множину $E^+_{\text{то}\,j}$, в яку в процесі пошуку розв’язання будуть додаватися елементи, що підлягають обслуговуванню при проведенні j-го виду технічного обслуговування. На кожному кроці у множину $E^+_{\text{то}\,j}$ буде додаватися один елемент, узятий із множини $E_{\text{то}}$. Підмножини $E^*_{\text{то}\,j}$ є непересічними (виконуються співвідношення: $\bigcap_j E^*_{\text{то}\,j} = \varnothing$; $\bigcup_j E^*_{\text{то}\,j} \subseteq E_{\text{то}}$).

Оператор 3 вибирає з множини $E_{\text{то}}$ i-й елемент e_i і включає його до множини $E^+_{\text{то}\,j}$. У множині $E_{\text{то}}$ елементи перед цим упорядковуються за зростанням середнього наробітку до відмови. Нумерація елементів, що включаються до множини $E^+_{\text{то}\,j}$, збігається з нумерацією кроків процесу пошуку розв’язання.

Оператор 4 здійснює пошук оптимальної періодичності ТО j-го виду $T^{+}_{\text{то}\,j}$, що задовольняє таку умову:

$$c_{\text{э}}(\langle E^{*}_{\text{то}1}, T^{*}_{\text{то}1}\rangle,...,\langle E^{*}_{\text{то}\,j\text{-}1}, T^{*}_{\text{то}\,j\text{-}1}\rangle,\langle E^{+}_{\text{то}\,j}, T^{+}_{\text{то}\,j}\rangle) \to \min_{T_{\text{то}\,j}}, \quad (3)$$

де $\langle E^{*}_{\text{то}k}, T^{*}_{\text{то}k}\rangle$ – знайдені раніше (у попередніх кроках) оптимальні значення параметрів k-го виду ТО ($k = \overline{1, j-1}$); $\langle E^{+}_{\text{то}\,j}, T^{+}_{\text{то}\,j}\rangle$ – оптимальні значення параметрів ТО j-го виду, знайдені в поточному (i-му) кроці процесу пошуку (оптимальні за умови, що зафіксовані параметри всіх видів ТО з номерами $k = \overline{1, j-1}$).

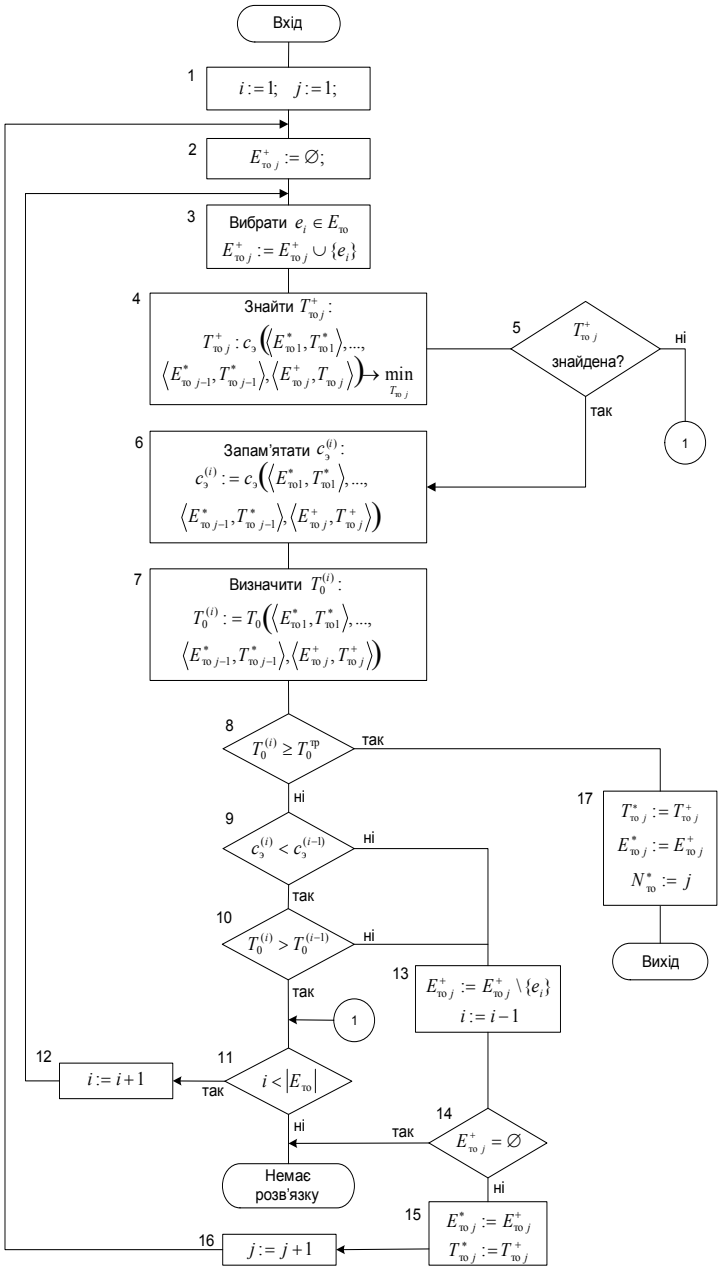


Рис. 1. Алгоритм розв'язання задачі оптимізації параметрів ТО за ресурсом

Якщо величина $T^{+}_{\text{то}\,j}$ не знайдена, це може бути у випадку, якщо функція $c_{\text{э}}(T_{\text{то}\,j})$ не має мінімуму, то оператор 5 передає управління оператору 11 для подальшого включення в множину $E^{+}_{\text{то}\,j}$ наступного елемента з $E_{\text{то}}$ і продовження процесу пошуку.

Умовно оптимальний розв'язок, отриманий після визначення величини $T^{+}_{\text{то}\,j}$ на i-му кроці, будемо позначати

$$\text{Р}^{(i)}_{\text{тор}} = \left\{\left\langle E^{*}_{\text{то}1}, T^{*}_{\text{то}1}\right\rangle, \ldots, \left\langle E^{*}_{\text{то}\,j\text{-}1}, T^{*}_{\text{то}\,j\text{-}1}\right\rangle, \left\langle E^{+}_{\text{то}\,j}, T^{+}_{\text{то}\,j}\right\rangle\right\}. \quad (4)$$

Оператор 6 запам'ятовує в оперативну пам'ять отримане на i-му кроці мінімальне значення питомої вартості експлуатації $c^{(i)}_{\text{э}}$: $c^{(i)}_{\text{э}} = c_{\text{э}}(\text{Р}^{(i)}_{\text{тор}})$.

Оператор 7 визначає величину середнього наробітку на відмову об'єкта $T^{(i)}_{0}$, що одержується при поточних значеннях параметрів ТО $\text{Р}^{(i)}_{\text{тор}}$: $T^{(i)}_{0} = T_0(\text{Р}^{(i)}_{\text{тор}})$.

Оператор 8 перевіряє виконання умови $T^{(i)}_{0} \geq T^{\text{тр}}_{0}$. Якщо ця умова не виконується, то далі виконується оператор 9, який перевіряє умову убування питомої вартості експлуатації $c^{(i)}_{\text{э}}$ шляхом перевірки нерівності

$$c^{(i)}_{\text{э}} < c^{(i-1)}_{\text{э}}. \quad (5)$$

Оператор 10 перевіряє умову зростання рівня безвідмовності об'єкта:

$$T^{(i)}_{0} > T^{(i-1)}_{0}. \quad (6)$$

Параметри $\left\langle E^{+}_{\text{то}\,j}, T^{+}_{\text{то}\,j}\right\rangle$ тут ще підлягають подальшому уточненню.

Унаслідок того, що цільові функції $c_{\text{э}}$ і T_0 отримуються як результат статистичного моделювання, їх значення значною мірою схильні до випадкових флуктуаціям. Це ускладнює формальну перевірку умов (5) і (6). Тому для надійної перевірки цих умов залучається людина-експерт, для якої після завершення кожного кроку розрахунків на екран персонального комп'ютера виводиться необхідна інформація. Аналізуючи цю інформацію, експерт повинен прийняти рішення про те, суттєвими або несуттєвими є отримані прирости показників $c_{\text{э}}$ і T_0.

Якщо експерт вважає, що прирости істотні, то елемент e_i залишається в підмножині $E^{+}_{\text{то}\,j}$, ТО цього елемента є корисним за показниками $c_{\text{э}}$ і (або) T_0. У цьому випадку виконуються оператори 11 і 12, потім робиться спроба включення в $E^{+}_{\text{то}\,j}$ нових елементів з $E_{\text{то}}$.

Оператор 11 перевіряє, чи є невикористані елементи в множині $E_{\text{то},}$ і якщо є, то оператор 12 формує номер наступного елемента, який збігається з номером наступного кроку і передає управління оператору 3 для продовження розрахунків.

Якщо експерт вважатиме отримані прирости несуттєвими, то елемент $e_{\text{і}}$ недоцільно включати до множини $E^{+}_{\text{то}\,j}$ (додавання елемента не привело до істотного поліпшення показників). У цьому випадку елемент $e_{\text{і}}$ виключається з $E^{+}_{\text{то}\,j}$, поточний виконаний крок уважається пробним і його результати скасовуються (оператором 13). Підмножина $E^{+}_{\text{то}\,j}$, що залишилася (якщо вона не порожня), і величина $T^{+}_{\text{то}\,j}$ приймаються як оптимальні параметри ТО j-го виду (оператор 15). Після цього

виконується оператор 16 і далі проводиться спроба ввести ще один вид технічного обслуговування.

Якщо після виключення елемента e_i виявляється, що множина $E^{+}_{\text{то}\,j}$ порожня, то це означає, що введення j-го виду ТО виявилося недоцільним (не привело до поліпшення показників $c_э$ або T_0). Оскільки встановлена вимога $T_0^{\text{тр}}$ не досягнута, задача (1) у цьому випадку не має розв'язку (оператор 14).

Якщо при виконанні оператора 8 виявилося, що отримане в поточному кроці значення $T_0^{(i)}$ задовольняє вимозі $T_0^{(i)} \geq T_0^{\text{тр}}$, то оператор 8 передає управління оператору 17 і на цьому процес пошуку розв'язання завершується. Отримані умовно оптимальні параметри $\left\langle E^{+}_{\text{то}\,j}, T^{+}_{\text{то}\,j} \right\rangle$ приймаються як оптимальні параметри ТО j-го виду: $E^{*}_{\text{то}\,j} := E^{+}_{\text{то}\,j}$; $T^{*}_{\text{то}\,j} := T^{+}_{\text{то}\,j}$.

У результаті виходить остаточний розв'язок задачі:

$$\text{P}^{*}_{\text{тор с}} = \left\{ \left\langle E^{*}_{\text{то1}}, T^{*}_{\text{то1}} \right\rangle, \ldots, \left\langle E^{*}_{\text{то}\,j}, T^{*}_{\text{то}\,j} \right\rangle \right\}.$$

Сформована до цього кроку кількість множин $E^{+}_{\text{то}\,j}$ j приймається як оптимальна кількість видів ТО $N^{*}_{\text{то}}$.

Розглянутий алгоритм є формальним описом запропонованої методики розв'язання задачі (1).

Методика розв'язання задачі (2) аналогічна розглянутій методиці, відмінність полягає тільки в тому, що замість критерію $\min c_э$ використовується критерій $\max K_{\text{ти}}$. Структурна схема алгоритму залишається тією ж, змінюється тільки зміст операторів 4, 6 і 9. У операторі 4 величина $T^{+}_{\text{то}\,j}$ визначається з умови

$$K_{\text{ти}}(\left\langle E^{*}_{\text{то1}}, T^{*}_{\text{то1}} \right\rangle, \ldots, \left\langle E^{*}_{\text{то}\,j\text{-1}}, T^{*}_{\text{то}\,j\text{-1}} \right\rangle, \left\langle E^{+}_{\text{то}\,j}, T^{+}_{\text{то}\,j} \right\rangle) \to \max_{T_{\text{то}\,j}}, \tag{7}$$

в операторі 6 замість питомої вартості експлуатації $c_э^{(i)}$ визначається коефіцієнт технічного використання

$$K^{(i)}_{\text{ти}} := K_{\text{ти}}(\left\langle E^{*}_{\text{то1}}, T^{*}_{\text{то1}} \right\rangle, \ldots, \left\langle E^{*}_{\text{то}\,j\text{-1}}, T^{*}_{\text{то}\,j\text{-1}} \right\rangle, \left\langle E^{+}_{\text{то}\,j}, T^{+}_{\text{то}\,j} \right\rangle), \tag{8}$$

в операторі 9 замість умови (4.23) перевіряється умова

$$K^{(i)}_{\text{ти}} > K^{(i-1)}_{\text{ти}}. \tag{9}$$

Практична реалізація обох методик заснована на застосуванні програми ISMPN.

Висновок

У статті розроблено алгоритм розв'язання задачі оптимізації параметрів стратегії технічного обслуговування за ресурсом складних виробів тривалої експлуатації. Алгоритм є формальним описом запропонованої методики розв'язання задач за критерієм мінімальної вартості та критерієм максимального коефіцієнта технічного використання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Forecasting to reliability complex object radio-electronic technology and optimization parameter their technical usage with use the simulation statistical models: [monography] in English / Sergey Lenkov, Konstantin Borjak, Gennady Banzak, Vadim Braun, etc.; under edition S. V. Lenkov. – Odessa: Publishing house «BMB», 2014. – 252 p.

2. *Ленков С.В.* Моделирование и оптимизация в процессе технического обслуживания по ресурсу сложных технических объектов / С.В. Ленков, В.Н. Цыцарев, Г.В. Банзак // Вісник інженерної академії України. – 2011. – № 3–4. – С. 94–100.

Отримано 04.11.2016
Рецензент Рибальський О.В., д.т.н.

УДК 519.688, 621.377.6

С.І. Лопатін,
кандидат юридичних наук,
старший науковий співробітник,
В.В. Буран,
здобувач ДНДІ МВС України

ПЕРСПЕКТИВНІ НАПРЯМИ РОЗВИТКУ СИСТЕМ ВІДЕОАНАЛІТИКИ

У статті розглянуті перспективні питання розвитку систем відеоаналітики в частині, що стосується ефективності роботи алгоритмів розпізнавання певних подій. Визначені основні принципи предикативної аналітики та відеосемантики.

Ключові слова: *прогностична відеоаналітика, скоринг, розпізнавання, відеосемантика.*

В статье рассмотрены перспективные вопросы развития систем видеоаналитики в части, касающейся эффективности работы алгоритмов распознавания определенных событий. Определены основные принципы предикативной аналитики и видеосемантики.

Ключевые слова: *прогностическая видеоаналитика, скоринг, распознавание, видеосемантика.*

Paper considers perspective development of the systems of videoanalytics in part related to the efficiency of the recognition of the algorithms of a certain event. Basic principles of predicative analysis and videosemantic are defined.

Keywords*: predicative analysts, scoring, recognition, videosemantic.*

Останнім часом системи відеоспостереження стають популярним інструментом, який широко використовується правоохоронними органами в усьому світі. Але відеоматеріалів накопичується дуже багато, дати лад цій інформації складно, а іноді й неможливо. Допомогу в такому випадку може надати аналіз відеоданих. Використовуючи сучасні алгоритми обробки, можна зробити швидкий та ефективний пошук потрібного фрагменту в архівних записах та своєчасне детектування події у відеоряді, що транслюється в реальному часі. Однак існує ще одна проблема – це надлишкова інформація, що є вкрай актуальною для нинішніх систем відеоспостереження, обсяг даних яких значно збільшився. Одним із підходів до її вирішення є автоматична обробка відеоданих або відеоаналіз.

Після вивчення досвіду роботи вітчизняних і зарубіжних компаній, діяльність яких пов'язана з цією проблематикою, слід виділити напрями відеоаналізу, які використовуються у відеоспостереженні для скорочення об'ємів інформації:

- жорстка відеоаналітика;
- гнучка відеоаналітика;
- прогностична відеоаналітика.

Жорстка відеоаналітика заснована на класифікації об'єктів. Основа такої відеоаналітики – детектор об'єктів. Цей алгоритм локалізує в потоці відеокадрів

замкнуті області, які змінюються за певними ознаками. Ці об'єкти намагається аналізувати програма відеоспостереження, щоб обчислити в них корисні цілі: людей, автомобілі тощо. Основна ідея при їх виявленні – це аналіз дій, пересувань і, насамкінець узагальненої картини поведінки, придатної для інтерпретації в соціально-кримінальному сенсі. У жорсткій відеоаналітиці всі моменти визначення класу цілі та її дій вимагають налаштувань, і будь-який збій зони огляду камери (від вітру, вібрації та ін.) або перестановки великих об'єктів на місцевості тягнуть за собою збій у функціонуванні. Незважаючи на це, жорстка аналітика зайняла свою нішу в системах відеоспостереження.

Одним із перспективних напрямів відеоаналітики є так звана гнучка відеоаналітика, чи відеосемантика, яка не має жорстких параметрів і точної формалізації.

Семантика в мовознавстві вивчає сенс одиниць мови, а у відеоаналітиці вивчає сенс одиниць відеоподій. І там і там це – набір знань, об'єднаних між собою певними співвідношеннями. Відеосемантика базується на великому наборі різних типів відеодетекторів, які вивчають властивості об'єкта, його розміри, співвідношення сторін, кольорову гаму, напрямок руху, швидкість, частоту рухів, параметри змін. Усі ці характеристики пов'язані між собою математичними співвідношеннями, які базуються на закономірностях поведінки різних типів об'єктів.

Програма відстежує характерні риси в результаті аналізу статистичних змін, таким чином здійснюється селекція відеоподій за їх семантичними відмінностями. Комп'ютерна програма розкладає відеозапис на смислові одиниці, показуючи ту частину цієї одиниці, яка повністю передає її значення. І замість тривалого відеозапису є одне єдине смислове навантаження, що дає можливість короткого показу скороченого відеосюжета, який повністю передає весь зміст сюжету.

Відеосемантика – короткий логічний виклад відеоінформації шляхом розкладання її на семантичні одиниці (відеосюжети), кожен з яких має свій закінчений зміст, який відрізняється від попереднього і наступного відеосегменту. Відеосемантика відстежує характерні риси відеоконтенту в результаті аналізу статистичних змін, тобто основою є статистика. Відсутність жорстко заданих параметрів і точної формалізації захищає від перешкод, оскільки вони включаються в загальний аналіз і віднімаються самі з себе в результаті різниці статистичних змін [1].

Але людина не завжди може оцінити адекватність поведінки окремих осіб, тому емулюються основні інстинкти людини (реакція на зміну обстановки, на нові звуки, нові образи, нестандартна поведінка та інше) і додається можливість програмного забезпечення аналізувати їх набагато швидше за людину. При цьому використовуються такі переваги комп'ютера над людиною, як невтомність, комп'ютерна логіка та машинний зір.

Сучасні алгоритми обробки відеоряду та потужні комп'ютерні платформи дозволяють обробляти потокове відео без втрат та пропусків інформації. Таким чином, відсікається зайве з відеоконтенту та не витрачається час на пошуки потрібного. У цьому принципова відмінність відеосемантики від класичної відеоаналітики, і досвід показав, що цей підхід реально працює в складних умовах відеоспостереження.

Відеосемантика порівнює не статичні картинки і не пікселі як такі, а зміну характеру активності. Вона працює з динамікою, і знаходить новий рух на тлі інших рухів. Коли об'єкт потрапляє до кадру або починає рухатися, аналізується і запам'ятовується його характер активності, що стає ознакою ідентичності цього об'єкта. Реакція йде на зміну цієї закономірності руху або на появу іншого характеру руху в кадрі, а також їх комбінацій при накладенні.

Для аналізу картини руху використовується безліч видів відеодетекторів. Відеосемантика – надбудова над відеодетекцією, її похідна. І таких похідних у сумі безліч. У відеосемантику входить і похідна від алгоритмів класичної відеоаналітики, але не як самостійні елементи, а лише як імплікатури. Плюсом йде похідна від систем розпізнавання, хоча формально відеосемантика і не розпізнає об'єкти, але вона використовує цей тип детекції для дослідження об'єктів руху. Уся ця математика працює не на ідентифікацію ознак злочину, а лише на пошук відмінностей у статистиці руху. Тобто цілі ставляться не в масштабах штучного інтелекту, а в області простої логіки. Такий підхід дуже практичний і, нехай не замінює людську працю, але значно спрощує її.

Що стосується стійкості для перешкод, то для відеосемантики це поняття відсутнє як клас, тому що будь-яка форма руху – це лише предмет статистичного аналізу, а реакція йде лише на зміну статистики. Картина активності перешкоди входить до минулої статистики, тому при відніманні її з поточної залишається нуль. Це, звичайно, не означає, що відеосемантика не спрацьовує на перешкоди, яким-небудь чином ідентифікуючи їх такими. Але відеосемантика не спрацьовує при кожному погойдуванні гілки, а лише один раз – коли змінилася погода, ставши вітряною. При цьому технологія "коротких даних" скорочує усе, в тому числі і перешкоди. На панелі результатів гілка, що хитається, але тільки один раз за час вітряної погоди (навіть якщо хитання явно не виражене), це в тисячі разів менше кількох годин постійного відеозапису при використанні стандартної відеодетекції.

Але справа не тільки в детекції, функціональність відеосемантики набагато ширша, ніж реакція на корисну мету. Головне завдання відеосемантики – розмежування подій. Саме вона дає можливість скорочувати величезні обсяги інформації, виділяючи корисні дані.

Відеосемантика обчислює однотипні періоди руху і відмежовує один характер поведінки від іншої, утворюючи події. Дана технологія відокремлює лише одне невідоме від іншого невідомого. Події не формалізуються, немає понять типу "бійка", "вбивство", "грабіж", "дія за статтею кримінального кодексу", але є розмежування меж періодів подій. А це означає, що передивитися події можна за секунди, без очікувань їх повного завершення.

Іншим напрямом розвитку відеоаналітики є прогностична відеоаналітика.

Прогностична або предикативна аналітика (Predictive analytics) – це безліч методів статистики, аналізу даних і теорії, які використовуються фахівцями для аналізу поточних та історичних даних чи подій для прогнозу даних та подій у майбутньому [2].

Аналітики вважають, що подальший розвиток світового ринку аналізу піде шляхом активного освоєння "advanced" (просунутої) аналітики, в тому числі предикативного аналізу, побудови симуляторів і варіативних моделей. Аналітика класу "advanced" використовує статистику, описові та предикативні інструменти

"data mining" (розвідки даних), симулятори та оптимізаційні засоби. Кінцева мета застосування всіх цих інструментів – прийняття рішень та ідентифікація можливостей для складання найкращих прогнозів, виявлення процесів, вибірок та інших закономірностей.

За цією інноваційною розробкою стоїть багаторічний досвід групи фізиків-ядерників, які займалися пошуком надслабких сигналів серед великих обсягів даних і розпізнаванням образів заданих сигнатур розпаду частинок серед мільйонів схожих конфігурацій. Завдяки методам, розробленим при вирішенні задач ядерної фізики, а також досвіду колективу у сфері інтелектуального аналізу великих даних (Big Data), технології компанії ефективні в найскладніших умовах.

Щоб предикативний аналіз був успішним, рекомендовано чітко дотримуватися таких стадій: постановка мети, отримання даних із різних джерел, підготовка даних, створення предикативної моделі, оцінка моделі, впровадження моделі, моніторинг ефективності моделі.

Найбільш відомий спосіб використання прогностичної аналітики – це застосування скорингових моделей для оцінювання. Скоринг (score – бал) – це математична модель у вигляді зваженої суми певних характеристик, за допомогою якої на основі минулого досвіду з'ясовується ймовірність події. Суть скорингу полягає в тому, що кожному параметру, що характеризується, надається реальна оцінка в балах. Центральною же сутністю предикативної аналітики є задача визначення предиктора або декількох предикторів (параметрів або сутностей, які впливають на прогнозовані події). Безліч цих предикторів утворює модель предикативної аналітики, яка передбачає певну подію в майбутньому з деяким ступенем ймовірності.

Чим простіше модель (або менша кількість факторів), тим менша ступінь точності моделі. Але завжди будь-яка модель будується на минулій події в минулому і це не означає, що події в майбутньому можуть повторитися при тих самих параметрах внутрішнього середовища. Відповідно, будь-який процес моделювання має імовірнісний характер. Ускладнюючи модель на історичних даних, є ризик її сильно перевчити і, відповідно, вона може перестати бути стійкою в майбутньому.

Основою технології предикативної відеоаналітики є прогнозування розвитку ситуації і відстеження ймовірності виникнення тієї чи іншої події. Це технологія, що дозволяє мінімізувати кількість обчислень при прийнятті рішень про підтвердження або спростування гіпотез, заснованих на оцінці різних обчислюваних характеристик відеоданих. Мінімізація кількості обчислень дає можливість вивільнені обчислювальні ресурси спрямувати на підвищення точності роботи відеоаналітики, що дозволяє значно підвищити ефективність детекторів аналітики в порівнянні з аналогічними рішеннями, створеними за "класичними" технологіями.

Час прийняття рішення розбивається на інтервали спостереження – відрізки часу, через які здійснюється накопичення та обробка інформації. Протягом інтервалу спостереження проводиться одна або кілька оцінок обчислюваних критеріїв і побудова графа, що описує ймовірність розвитку спостережуваної ситуації. Критеріями можуть служити різні статистичні характеристики відеоданих, а також результати глибокого вивчення нейронних мереж. Позитивне прийняття рішення трапляється при проходженні ситуації тільки по певному шляху графа [3].

Предикативна відеоаналітика найбільш затребувана для забезпечення безпеки об'єктів, що характеризуються масовим скупченням людей.

Конкурентною перевагою алгоритму є обробка практично всього динамічного діапазону, що надходить на аналіз зображення і ефективне вилучення корисного сигналу з шуму. Раніше, щоб уникнути помилкових спрацьовувань і знизити навантаження на процесор, розробники, зазвичай, відкидали частину даних, що неминуче призводило до втрати корисної інформації і нездатності працювати в умовах інтенсивних людських скупчень або при низькому освітленні.

Одне з призначень систем штучного інтелекту − попередження про небезпеку для збереження людських життів. Система оцінює психологічний стан осіб: як моменти найбільшої зацікавленості, так і підвищену збудливість та нервозність зловмисника перед вчиненням крадіжки. На основі класифікації активності виробляються рекомендації [4].

Фахівцями спільно з психологами була проведена колосальна робота з визначення статистичних параметрів мікрорухів людей у різних емоційних станах, різного віку, статі, різних темпераментів. Було виявлено 16 ключових статистичних параметрів, завдяки яким поведінковий алгоритм за 30−120 секунд точно визначає емоційний стан особи.

Зараз правоохоронці працюють з подіями, що сталися, рідко − намагаються передбачити дії злочинців, якщо вони вже вчинили ряд злочинів. Але технології дозволять попередити злочин до появи жертв і постраждалих. Ключ до цього − розпізнавання поведінки та емоцій людини.

Засоби предикативної аналітики адресовані фахівцям, тому не застосовуються настільки широко. Експерти вважають, що не варто чекати масових впроваджень в цій області, але тенденції будуть поступово змінюватися. Причина тому − поява феномена великих даних, який підштовхує до пошуку нових засобів обробки інформації.

На думку Еріка Сігеля (Eric Siegel), експерта з предикативного аналізу, викладеного в його однойменній книзі “Predictive Analytics”, сфера застосування предикативного аналізу найбільш поширена у виявленні шахрайських схем та для забезпечення безпеки об’єктів, що характеризуються масовим скупченням людей [5]. Засоби предикативного аналізу дозволяють мінімізувати використання шахраями фальшивих схем тощо.

Програми впровадження систем відеоспостереження здатні поліпшити ставлення громадськості до роботи правоохоронних органів та забезпечити захист поліцейських при виконанні службових обов’язків.

Отже, використання систем відеоспостереження може бути ефективним стримуючим фактором для багатьох незаконних дій. А застосування ефективних алгоритмів відеоаналітики дозволить оперативно приймати рішення залежно від обставин.

Найбільш доцільно використовувати системи відеоаналітики в підрозділах карного розшуку НПУ, превентивної діяльності НПУ, оперативно-технічних заходів НПУ та підрозділів поліції охорони НГУ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Torsten Anstdt, Ivo Keller, Harald Lutz. Практическое руководство по видеоаналитике − Intelligente Videoanalyse: Handbuch Fr Die Praxis.:John Wiley & Sons, 2011. − P. 164.

2. *Торстен Аништедт.* Видеоаналитика: Мифы и реальность / Торстен Аништедт, Иво Келлер, Харальд Лутц // Security Focus, 2012. − 176 с.

3. P. Viola and M.J. Jones. “Rapid Object Detection using a Boosted Cascade of Simple Features”, proceedings IEEE Conf. on Computer Vision and Pattern Recognition (CVPR 2001), 2001.

4. *Эрик Сигель*. Просчитать будущее: Кто кликнет, купит, соврет или умрет / Эрик Сигель // Predictive Analytics. – М. : Альпина Паблишер, 2014. – 374 с. – ISBN 978-5-9614-4541-1.

Отримано 23.11.2016
Рецензент Марченко О.С., к.т.н.

УДК 623.1

М.А. Мовчан,
кандидат юридичних наук,
С.Г. Осьмак

ЕКСПЕРИМЕНТАЛЬНІ МЕТОДИ ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ ЗАХИСНИХ МАТЕРІАЛІВ ПІД ЧАС ВПЛИВУ ЗАСОБІВ УРАЖЕННЯ

У статті висвітлено основні критерії визначення балістичної стійкості засобів бронезахисту. Проаналізовано окремо визначені фактори, що впливають на характеристики стійкості матеріалів до засобів ураження в процесі балістичних випробувань.

Ключові слова: *засоби бронезахисту, засіб ураження, ураження, швидкісний поріг, пробиття, випробування.*

В статье рассмотрены основные критерии определения баллистической стойкости средств бронезащиты. Проанализированы отдельно определенные факторы, влияющие на характеристики устойчивости материалов к средствам поражения в процессе баллистических испытаний.

Ключевые слова: *средства бронезащиты, средство поражения, поражения, скоростной порог, пробитие, испытания.*

In the paper the basic criteria for determining the stability of ballistic body armor means are considered. The factors influencing the stability properties of materials for weapons during ballistic tests are analyzed .

Keywords: *armor, means of destruction, damage, speed limit, penetration, testing.*

Питання визначення якості балістичної стійкості засобів бронезахисту останнім часом досить актуально розглядається як вченими, так і практичними користувачами. Основним критерієм, який так чи інакше розглядається в цьому аспекті, є саме розуміння механізму забезпечення стійкості засобів бронезахисту та визначення основних процесів, що виникають при взаємодії засобів ураження та захисних матеріалів.

Загальне науково-теоретичне підґрунтя дослідження цього питання становлять наукові праці провідних вітчизняних та зарубіжних вчених, таких як Лоторєв В.О., Смерницький Д.В., Бєляков К.І., Марченко О.С., Михальов В.О., Донченко С.О., Чайка І.В., Хоменко В.М., Сільніков М.В., Хімічев В.А., Сальников В.П., Сухорученко В.С., Московченко В.М.

Проте ця проблематика висвітлювалась частково, лише в розрізі самого поняття засобів бронезахисту, їх класифікації. Питання розгляду балістичних матеріалів, а також основних аспектів їх захисних властивостей у системі "засіб ураження – перешкода" практично не досліджувалися.

Практична реалізація розуміння захисних характеристик матеріалів викликана необхідністю розуміння та реалізації найбільш ефективного використання засобів

захисту. До цієї умови належить безпосередньо процес взаємодії засобу ураження із захисним матеріалом та його зміна залежно від умов взаємодії.

Виходячи з наведеного, метою цієї роботи є дослідження методів визначення показників дії окремих засобів ураження на балістичні матеріали, що використовуються при створенні засобів індивідуального бронезахисту та встановлення основних критеріїв оцінки стійкості таких матеріалів.

На цей час основним нормативним документом, що регулює процес створення та виготовлення засобів індивідуального бронезахисту, є ДСТУ В 4103-2002 "Засоби індивідуального захисту. Бронежилети. Загальні технічні умови". Зазначений документ врегульовує порядок виготовлення, поділяє на категорії бронежилети за відповідними класами та окремими видами їх конструктивного виконання [1]. Вимоги ДСТУ В 4104-2002 встановлюють методи визначення відповідності виробів бронезахисту, зокрема бронежилетів, окремим класам захисту [2]. Водночас питання визначення оцінки самих матеріалів на початковому етапі розробки та створення засобів бронезахисту до сфери дії зазначених стандартів не віднесено та не врегульовано загалом.

Реалізація можливості проведення оцінки матеріалів, у першу чергу, дозволить більш якісно визначити характеристики сировини (особливо з появою нових видів матеріалів) та скоротити час розробки захисної структури самого засобу бронезахисту.

Питання визначення характеристик балістичної стійкості матеріалів полягає в дослідженні процесу взаємодії засобів ураження (куля, осколки) з елементами захисту та залежить від впливу численних факторів. Наприклад, умови наближення засобу ураження до захисного елемента характеризуються не тільки швидкістю його поступального руху, що, як правило, становить сотні метрів за секунду, але й характеристиками прецесійно-нутаційного руху кулі, які в початковий момент контакту можуть вважатися випадковими. Саме тому навіть для конкретного процесу взаємодії засобу ураження з перешкодою притаманний випадковий характер, а балістична стійкість захисного елемента в цьому випадку характеризується статистичним розподілом ймовірності непробиття залежно від швидкості вражаючого елемента з урахуванням інших окремих характеристик процесу взаємодії.

Як правило, балістична стійкість засобів захисту визначається експериментально, тобто безпосередньо в результаті створення взаємодії із засобом ураження.

У результаті наукових та практичних світових досліджень основними характеристиками балістичної стійкості засобів захисту залежно від окремих факторів, що використовуються, є:

– швидкісний поріг кондиційного ураження ($V_{пку}$) – максимальний показник швидкості уражаючого елемента, нижче значення якого досягається (практично 100 %) непробиття засобу захисту. Об'єктивний показник цієї характеристики, як правило, досягається лише в ході контакту засобу ураження (що рухається по нормалі до поверхні елемента захисту) з перешкодою;

– швидкісний поріг наскрізного пробиття ($V_{пнп}$) – мінімальний показник швидкості уражаючого елемента, вище значення якого досягається (практично 100 %) пробиття засобу захисту. Цей показник досягається аналогічно попередньому лише в ході контакту засобу ураження з елементом захисту;

– швидкісний поріг (V_{50}), – показник швидкості уражаючого елемента, при якій ймовірність пробиття, а також непробиття захисного елемента становить

50 %. Ця характеристика досить широко використовується при оцінці якості захисних матеріалів, вхідному контролі бронематеріалів;

– поріг кондиційного ураження відносно кута взаємодії ($\alpha_{пку}$) – значення кута контакту уражаючого елемента із засобом захисту за показниками відхилення траєкторії руху засобу ураження від нормалі до поверхні елемента. Таким чином, при збільшенні значення відхилення траєкторії руху засобу ураження від нормалі в процесі контакту досягається (практично 100 %) непробиття захисного елемента. Існування цієї характеристики пов'язано з тим, що конструктивна зміна кута захисного елемента засобів захисту є одним із способів підвищення його балістичної стійкості [7, с. 6].

Слід зазначити, що згадані характеристики балістичної стійкості засобів захисту припускають ймовірності пробиття захисного елемента залежно від швидкості уражаючого елемента в момент контакту із засобом захисту та кута їх взаємодії. Таким чином, можна свідомо припустити, що чим вище швидкість уражаючого елемента в момент взаємодії із засобом ураження, тим більша ймовірність пробиття захисного елемента і навпаки, але лише при інших рівних умовах. І, відповідно, при максимальному наближенні до 0° кута взаємодії від нормалі до поверхні перешкоди, збільшується ймовірність пробиття захисного елемента [6, с. 86].

На сьогодні, враховуючи вартісно організаційні показники проведення балістичних випробувань, пріоритетним є напрям розробки інформативних методів дослідження балістичних характеристик засобів захисту, практична реалізація яких дозволить визначити оптимальні захисні структури елементів захисту при мінімальних затратах часу і коштів.

Розглянемо більш детально аспекти визначення якісних показників захисних елементів на прикладі визначення значення швидкості кондиційного ураження ($V_{пку}$) при проведенні балістичних випробувань. Безпосередньо при проведенні випробувань проводиться обстріл захисного елемента з варіюванням швидкості вражаючого елемента. Різниця максимальної та мінімальної швидкості при цьому, як правило, має бути не більше 20 м/с. Обов'язковою умовою випробувань є досягнення в діапазоні швидкостей із зазначеною вище різницею результатів як пробиття, так і непробиття захисного елемента.

Варто також зазначити про недоліки такого методу визначення межі значення швидкості кондиційного ураження.

1. Як базова точка визначення $V_{пку}$ використовується випадково отриманий результат – мінімальна швидкість пробиття, ймовірність появи якого близька до нуля.

2. При визначенні використовується не вся інформація, отримана під час проведення випробувань, а тільки результати 5–7 дослідів, тобто менше половини отриманих результатів.

3. Середнє значення результатів випробувань, проведених у зазначеному інтервалі швидкостей [$V_{min\ проб}$ ... ($V_{min\ проб}$ -20 м/с)], може спричинити зміну значення $V_{пку}$ в межах до 20 м/с залежно від конкретно отриманих значень швидкостей у заданому інтервалі.

4. Отримання факту непробиття захисного елемента із залікових влучень не означає 100 % ймовірність непробиття.

5. У цьому процесі не проводиться визначення іншого, не менш важливого значення швидкості межі наскрізного пробиття $V_{пнп}$.

Для визначення значення швидкості межі наскрізного пробиття $V_{пнп}$ слід було б продовжити випробування в діапазоні швидкостей на 20 м/с вище максимальної швидкості непробиття (наприклад, від 540 до 560 м/с), і якщо в цьому діапазоні можливо було б отримати не менше 5–7 результатів пробиття, то їх середнє арифметичне значення є значенням $V_{пнп}$. Якщо ж при швидкості більшій, ніж 560 м/с буде отримано ще непробиття, тоді слід продовжити випробування від цього нового значення максимальної швидкості непробиття за описаною вище методологією.

Аналогічним способом визначається значення межі кондиційного і некондиційного пробиття за кутом. При цьому значення зміни кута повинне бути рівним 2 °, а швидкість при контакті має бути відносно постійною, тобто перебувати в межах ± 10 м/с від заданого значення.

Найбільш вірогідною характеристикою балістичної стійкості засобів захисту, яка визначається за отриманими в балістичних експериментах даними, є швидкісний поріг V_{50}, який досить широко використовується в процесі виробництва засобів захисту як критерій оцінки виготовленої продукції і слугує нормою якості. Зокрема, у військових стандартах США для сталі, що використовується як елемент бронювання засобів захисту, а також для окремих сплавів кольорових металів, зокрема алюмінію марки 5083 і 5456, показник V_{50} є характеристикою оцінки можливості використання цих захисних матеріалів при виробництві бронеавтомобілів [3].

Виходячи з наведеного, значення V_{50} прямо впливає на процес виробництва матеріалів для використання в засобах захисту, а також на ризики виробника і замовника, що зумовлює необхідність удосконалення методик її визначення. Крім того, якість методичного забезпечення, що визначає точність оцінки фактичного рівня захисних характеристик, уносить свій внесок у розвиток і оптимізацію конструктивних параметрів елементів захисту. Підвищення точності і надійності визначення рівня балістичної стійкості засобів захисту дозволяє оптимізувати їх захисну структуру, усунути не обґрунтований запас, мінімізувати масу зразка, що насамкінець визначає технічну досконалість засобу захисту в цілому.

На цей час до захисних структур з мінімально допустимою масою досить часто висувається вимога забезпечення 100 %-го непробиття при впливі певного засобу ураження. При оцінці якості конкретної захисної структури, наприклад під час приймання продукції у виробництві, призначеної для забезпечення балістичного захисту, проводяться випробування на підтвердження заданих вимог. З позицій теорії ймовірності та математичної статистики, надійність захисної структури матеріалу можна оцінити шляхом визначення значення позитивної ймовірності і, залежно від кількості випробувань та отриманих фактів пробиття, встановити нижню межу можливості забезпечення балістичної стійкості захисного елемента, яка і характеризує його надійність [4, с. 63].

Значення $V_{50,}$ зокрема, є статистичним. Для його визначення необхідно провести досить велику кількість випробувань. Важливим аспектом є визначення умов, що забезпечують зменшення обсягу випробувань без зниження об'єктивності одержаного результату.

Як склалося практично, методика експериментального визначення V_{50} полягає в проведенні певної кількості балістичних випробувань (не менше 20 дослідів) із

прямопропорційною змінною швидкістю ураження, тобто зменшення швидкості уражаючого елемента при наступному пострілі після отримання пробиття випробовуваного елемента або збільшення швидкості уражаючого елемента після його непробиття. Випробування проводяться, починаючи із заданої в технічних вимогах швидкості, з поступовою зміною швидкості уражаючого елемента як у бік зростання, так і її зниження, при цьому в процесі випробувань визначаються:

– $V_{max\ непр}$ – показник максимальної швидкості непробиття зразка, тобто це швидкість, при якій відсутній пробій, однак при збільшенні цього показника швидкості результатом випробувань є лише пробиття зразка;

– $V_{min\ проб}$ – показник мінімальної швидкості пробиття випробовуваного зразка, тобто швидкість, нижче якої не спостерігаються випадки його пробиття [5, с. 172].

З огляду на викладене допустимі 2 варіанти.

1) $V_{min\ проб} < V_{max\ непр}$, тобто є зона змішаних результатів – діапазон швидкостей, у якому спостерігається як пробиття, так і непробиття. Цей випадок характерний для більшості захисних матеріалів на основі спеціальних тканин та металу, при цьому показник зазначеної швидкісної зони досягає значень десятків метрів на секунду.

2) $V_{min\ проб} > V_{max\ непр}$, тобто зона змішаних результатів відсутня, таким чином межа між граничними межами пробиття і непробиття випробовуваного зразка досить різка. На практиці такий випадок зустрічається відносно рідко.

Безпосередньо в процесі проведення випробувань швидкість може варіюватися у великих межах, тому, перш за все, є важливим аспектом визначення залікового діапазону швидкостей, оскільки непробиття випробовуваного зразка при відносно низькій швидкості, а також його пробиття при високій швидкості очевидні і не несуть значимої інформативності. Найбільш інформативними є результати, отримані в діапазоні швидкостей, наближених до значень зони змішаних результатів. При цьому показники межі цієї зони мають істотне значення і повинні бути підтвердженими.

З огляду на викладене та підсумовуючи наведене, варто зазначити, що на цей час питання практичного вирішення реалізації можливості проведення оцінки матеріалів балістичного захисту досить вузько реалізовано. Безумовно, саме практична реалізація визначених методів дозволить більш якісно досліджувати захисні структури та матеріали, що використовуються для створення засобів індивідуального бронезахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Засоби індивідуального захисту. Бронежилети. Загальні технічні умови : ДСТУ В 4103-2002. – Введ. в дію 12.06.2002. – К. : Держстандарт України, 2002. – 15 с.

2. Засоби індивідуального захисту. Вироби бронезахисту. Методи контролю балістичної стійкості бронежилетів : ДСТУ В 4104-2002. – Введ. в дію 12.06.2002. – К. : Держстандарт України, 2002. – 19 с.

3. MIL-STD-662F, MILITARY STANDARD: V50 BALLISTIC TEST FOR ARMOR (18 DEC 1997) [Електронний ресурс]. – Режим доступу : URL : http://everyspec.com/MIL-STD/MIL-STD-0500-0699/MIL-STD-662F_6718.

4. Сильников М. В., Химичев В. А. Средства индивидуальной бронезащиты. Учебное пособие / Под общей редакцией В. П. Сальникова. Санкт-Петербургский университет МВД России; Академия права, экономики и безопасности жизнедеятельности. – СПб.: Фонд "Университет", 2000. – 480 с. (Серия: "Спецтехника органов внутренних дел").

5. Легкие баллистические материалы / Под ред. А. Бхатнагара. – М.: Техносфера, 2011. – 392 с.

6. Материалы и защитные структуры для локального и индивидуального бронирования / В.А. Григорян, И.Ф. Кобылкин, В.М. Маринин, Е.Н. Чистяков. Под ред. В.А. Григоряна. – М.: Изд. РадиоСофт, 2008. – 406 с.

7. Средства индивидуальной бронезащиты (Руководство службы). – М.: Братишка, 2004. – 80 с.

Отримано 04.11.2016
Рецензент Марченко О.С., к.т.н.

УДК 004.738.5

О.В. Самчишин,
кандидат технічних наук
І.О. Орищук

МЕТОДИКА СКЛАДАННЯ РЕЙТИНГУ ЕЛЕКТРОННИХ ЗАСОБІВ МАСОВОЇ КОМУНІКАЦІЇ ПРИ ОРГАНІЗАЦІЇ ПРОЦЕСУ ЇХ КОНТЕНТ-МОНІТОРИНГУ

У статті розглянуто проблематику ранжування електронних засобів масової комунікації – джерел інформаційних повідомлень з метою оптимізації їх вибору для вирішення завдань моніторингу інформаційного простору. Запропоновано методику складання рейтингу електронних засобів масової комунікації, в основу якої покладено метод парних порівнянь та метод експертних оцінок. Такий підхід, на відміну від відомих, забезпечує урахування важливості обраних критеріїв моніторингу залежно від поставлених завдань.

Ключові слова: *електронні засоби масової комунікації, метод парних порівнянь, метод експертних оцінок, ранжування джерел інформаційних повідомлень.*

В статье рассмотрено проблематику ранжирования электронных средств массовой коммуникации – источников информационных сообщений с целью оптимизации их выбора для решения мониторинга информационного пространства. Предложена методика составления рейтинга электронных средств массовой коммуникации, в основу которой положено метод парных сравнений и метод экспертных оценок. Такой подход, в отличие от известных, обеспечивает учет важности выбранных критериев мониторинга в зависимости от поставленных задач.

Ключевые слова: *электронные средства массовой коммуникации, метод парных сравнений, метод экспертных оценок, ранжирование источников информационных сообщений.*

The paper deals with the issues of ranging the electronic means of mass communication as the sources of data messages in order to optimize their choice for solving of monitoring problems in the information space. It is suggested the rating method of electronic means of mass communication based on the paired comparison method and expert assessments. This approach, unlike the known ones, ensures the importance of selected monitoring criteria in the terms of assigned tasks.

Key words: *electronic means of mass communication, paired comparison method, expert assessment, ranging of information message sources.*

Постановка проблеми

Сучасна епоха інформатизації усіх сфер діяльності суспільства характеризує електронні засоби масової комунікації (е-ЗМК) як основне джерело розповсюдження новинної, оглядової та іншої інформації. Регулярний моніторинг таких матеріалів державними та приватними аналітичними структурами дозволяє не тільки аналізувати стан справ у будь-якій сфері інтересу, а й відкриває можливості прогнозування розвитку ситуації.

Моніторинг інформаційних повідомлень (далі – ІП) в е-ЗМК силовими структурами будь якої розвиненої держави спрямований, як правило, на своєчасне виявлення загроз в інформаційній сфері. При цьому основними завданнями моніторингу е-ЗМК є виявлення повідомлень заданого змісту в засобах масової інформації, блогосфері і соціальних мережах та їх джерел, аналіз тенденцій розвитку породжуваних негативними повідомленнями ситуацій за актуальними тематиками, як основи для побудови логічних послідовностей щодо виявлення можливих інформаційних компаній протиборчої сторони.

У процесі організації моніторингу е-ЗМК важлива роль відводиться функції каталогізації інформаційних повідомлень з подальшим їх накопиченням в спеціалізованій базі даних за визначеними тематиками, що становлять інтерес [1]. Однак ключову роль у процесі організації моніторингу е-ЗМК відіграє процедура оптимального вибору джерел ІП. Ця процедура є складноформалізованою, оскільки на вибір джерел ІП впливає достатньо велика кількість факторів, а тому потребує подальшого уточнення та доопрацювання

Аналіз останніх досліджень і публікацій

Аналіз найбільш відомих вітчизняних та іноземних інформаційно-аналітичних систем InfoStream, Медіалогія, Silobreaker тощо та рейтингів джерел ІП, які вони формують, показав, що перелік показників, на основі яких складаються рейтинги, дуже широкий [3–5]. Так рейтинг джерел ІП може складатися за регіональним, тематичним, мовним показником, за значимістю або впливовістю для тієї або іншої цільової аудиторії, обсягом цитування, об'єму реалізованої реклами тощо [1].

У зв'язку зі значною кількістю е-ЗМК, можливостей мережі Інтернет з динамічного розповсюдження ІП та обмеженість технічних ресурсів інформаційних систем щодо їх аналізу встановлено, що сьогодні виникає потреба оптимізації складу і кількості джерел за умови одночасного забезпечення відповідної якості вирішення завдань моніторингу. При цьому оптимізація складу і кількості джерел може досягатися за рахунок оптимального ранжування джерел ІП – складання відповідного рейтингу.

Метою статті є підвищення ефективності організації процесу моніторингу е-ЗМК за рахунок удосконалення методики складання їх рейтингу.

Викладення основного матеріалу дослідження

Відомо, що перелік показників, за якими можливо здійснити ранжування джерел ІП, може бути достатньо різноманітним [2]. Однак їх повне врахування недоцільне і обмежується завданнями, для яких складається рейтинг джерел ІП. Тому для вирішення задачі моніторингу е-ЗМК з метою виявлення і оцінювання, наприклад, рівня негативного інформаційно-психологічного впливу на цільову аудиторію доцільно обирати тільки ті джерела, які відповідають умовам регіональності, а тематика їх публікацій – відповідно завданням моніторингу. Крім того, варто обмежитись такими показниками, як: оригінальність, продуктивність, стабільність та індекс цитування джерела [1].

Основним та таким, що визначає зміст процедури вибору джерел ІП є завдання та мета моніторингу. Тому під час вибору джерел ІП обов'язковим є визначення *ступеня відповідності джерела заданій тематиці* (K_m), яка, у свою чергу, прямо залежить від завдань моніторингу. Ступінь відповідності джерела тематиці, завданням та меті моніторингу K_m пропонується визначати методом експертних оцінок у двійковій формі, тобто:

$$K_m = \begin{cases} 1 & \text{відповідає} \\ 0 & \text{не відповідає} \end{cases}. \quad (1)$$

Так, вибір для моніторингу найбільш оригінальних джерел ІП за виразом (1) дозволяє зменшити не тільки формальне але й змістовне дублювання інформації. Наприклад, для вирішення цієї проблеми необхідно уникати вибору до списку джерел моніторингу новинних інтеграторів.

Критерій оригінальності джерела ІП (K_{opd}) пропонується визначати як співвідношення кількості повідомлень, що самостійно формуються та публікуються джерелом до загальної кількості публікацій цього джерела за одиницю часу, тобто

$$K_{opd} = \frac{n_{opd}}{N_d} \quad (2)$$

де n_{opd} – кількість оригінальних (ексклюзивних) ІП d-го джерела; $N_{d\_}$ загальна кількість ІП d-го джерела.

Одним з критеріїв відбору джерела є відбір за кількістю публікацій, який використовується для максимального охоплення переліку ІП. Проведені інформаційним центром "Елвісті" дослідження показують що приблизно 20 % найбільш продуктивних джерел публікують 80 % документів [6]. Але виникає протиріччя – чим більш продуктивне джерело, тим більше воно містить запозичених з інших джерел повідомлень. Це знов породжує проблему дублювання ІП та ускладнює процес їх статистичної і аналітичної обробки. Тому пропонується відбір джерел за кількістю публікацій проводити з оригінальних, а їх кількість обмежувати шляхом ранжування за кількістю публікацій та відбору з них найбільш продуктивних.

Обчислення *показника продуктивності* d-го джерела серед обраних пропонується здійснювати за формулою:

$$K_{npd} = \frac{N_d}{\sum_{d=1}^{D} N_d}, \quad (3)$$

де D – загальна кількість обраних для ранжування джерел.

З практики [2] відомо, що при організації моніторингу є-ЗМК серед множини проблем підбору і аналізу джерел ІП суттєве значення має врахування показника стабільності джерела, тому т*ематична стабільність* джерела може бути визначена як кореляція наборів тематичних рубрик, яким відповідають ІП з цього джерела в різні періоди часу [7]. Для обчислення рівня відхилення (нестабільності) K_{cm} джерела ІП пропонується скористатися критерієм, що заснований на лінійній метриці, а саме

$$K_{cm} = \frac{1}{Q}\sum_{i=1}^{Q}\frac{S_i}{R_i}, \quad (4)$$

де Q – кількість рубрик джерела; S_i – середньоквадратичне відхилення за i-ю рубрикою за визначений період часу; R_i – діапазон значень ІП за і-ю рубрикою.

З виразу (4) видно, що значення K_{cm} враховує не тільки кількість тематичних відхилень, але й відхилення за кількістю попадань у рубрики, а саме фактичну кількість ІП від джерел, що належать до цієї рубрики. У [7] показано, що виключну стабільність мають, як правило, джерела, що містять не більше 6 рубрик.

Прикладом стабільних джерел є великі інформаційні агенції, що регулярно поставляють користувачам приблизно однакові об'єми інформації протягом тривалого часу.

Прикладом нестабільних джерел можуть служити джерела, що активно діють протягом декількох діб, а потім припиняють свою роботу, публікують інформацію хаотично в часі як за кількістю, так й об'ємом повідомлень.

Нестабільні джерела також можуть представляти інтерес під час виконання специфічних задач моніторингу, але вони не формують основні тенденції в інформаційному просторі. Їх доцільно використовувати при несистематичному аналізі інформаційного простору.

На сьогодні найбільш розповсюдженим критерієм ранжування як окремих документів, так і окремих веб-сайтів є кількість посилань на них інших джерел – індекс цитування.

Індекс цитування є-ЗМК – це доля посилань на матеріали цього джерела в загальній кількості посилань на ресурси визначеного переліку джерел.

Для оцінки рівня цитування окремих документів і веб-ресурсів у мережевих пошукових системах використовують відому модель А. Бредера, критерій PageRank, SALSA, h-індекс та інші [8]. Однак при оцінювання рівня цитування новинних веб-ресурсів як джерел ІП необхідно враховувати ряд умов, які передбачають некоректним використання зазначених вище моделей. Зокрема через підвищену динаміку новинних потоків, відсутність прямих гіперпосилань на деякі Web-ресурси, необхідність врахування у новинних потоках не тільки гіперпосилання, а й контекстних посилань на об'єкти відкритої і закритої частини Web-простору, відсутність врахування дублювання інформації.

При досліджені цитування документів джерела ІП іншими веб-ресурсами, проведеного інформаційним центром "Елвісті" [6] було вперше запропоновано підхід, у якому для кожного ІП, яке належить до визначеного джерела – веб-сайту, виявляються вихідні посилання на інші джерела та отримується розподілення новинних джерел за кількістю веб-сайтів, що мають на них посилання.

Приклад ранжування списку новинних джерел подано в таблиці 1.

Таблиця 1

Список новинних джерел

Web-сайт	Кількість web-сайтів, що посилаються	Ранг джерела
ІА "Інтерфакс"	1051	1
"РосБізнесКонсалтинг"	983	2
"Reuters"	882	3
ІТАР-ТАСС	787	4
РІА "Новости"	773	5
УНІАН	675	6
Радіо "Свобода"	662	7
НТВ	631	8
"Коммерсант"	623	9
ВВС	598	10

Обчислення значення показника цитування *d*-го джерела пропонується здійснювати як відношення кількості посилань на інформаційні повідомлення цього джерела до загальній кількості посилань на ресурси визначеного переліку джерел згідно з критерієм

$$K_{цd} = \frac{L_d}{\sum_{d=1}^{D} L_d}, \qquad (5)$$

де L_d – кількість посилань на повідомлення *d*-го джерела.

З аналізу найбільш популярних новинних е-ЗМК (див. табл. 1) встановлено, що числове значення запропонованих показників залежно від джерела може змінюватись у досить великому діапазоні. Діапазон залежить від кількості ІП на даному сайті та періоду визначеному для моніторингу (від декількох ІП до десятків тисяч). Тому в процесі організації моніторингу е-ЗМК необхідно вводити інтервальну шкалу (табл. 2) нормованих коефіцієнтів однакових показників різних джерел з метою додержання метричності.

Таблиця 2

Інтервальна шкала нормованих коефіцієнтів для побудови рейтингу е-ЗМК

Назва показника	Визначення коефіцієнта	Інтервал зміни значень показника за K_i критерієм ранжування	Ранг показника
Відповідність джерела тематиці	$K_m = \begin{cases} 1 & \text{відповідає} \\ 0 & \text{не відповідає} \end{cases}$		
Показник оригінальності джерела	$K_{opd} = \frac{n_{opd}}{N_d}$	0-0,01 0,01-0,1 0,1-0,2 0,2-0,3 0,3-0,4 0,5-0,6 0,6-0,7 0,7-0,8 0,8-0,9 0,9-1	1 2 3 4 5 6 7 8 9 10
Показник продуктивності джерела	$K_{npd} = \frac{N_d}{\sum_{d=1}^{D} N_d}$	0-0,01 0,01-0,1 0,1-0,2 0,2-0,3 0,3-0,4 0,5-0,6 0,6-0,7 0,7-0,8 0,8-0,9 0,9-1	1 2 3 4 5 6 7 8 9 10

Назва показника	Визначення коефіцієнта	Інтервал зміни значень показника за K_i критерієм ранжування	Ранг показника
Показник стабільності джерела	$K_{ст} = \frac{1}{Q}\sum_{i=1}^{Q}\frac{S_i}{R_i}$	0-0,01 0,01-0,1 0,1-0,2 0,2-0,3 0,3-0,4 0,5-0,6 0,6-0,7 0,7-0,8 0,8-0,9 0,9-1	1 2 3 4 5 6 7 8 9 10
Індекс цитування джерела	$K_{цd} = \frac{L_d}{\sum_{d=1}^{D} L_d}$	0-0,01 0,01-0,1 0,1-0,2 0,2-0,3 0,3-0,4 0,5-0,6 0,6-0,7 0,7-0,8 0,8-0,9 0,9-1	1 2 3 4 5 6 7 8 9 10

Залежно від завдань моніторингу завжди вважається за необхідне визначати і враховувати важливість коефіцієнтів однакових показників різних е-ЗМК. При цьому важливість кожного коефіцієнта буде також різною. Так як оцінювання показників за обраним критерієм проводиться для достатньо великої кількості джерел (обмежених тільки технічними ресурсами посту моніторингу), то для досягнення заданої точності оцінювання пропонується скористатися методом парних порівнянь [9].

Вектор важливості визначених критеріїв $\alpha = (\alpha_1, \alpha_2, ..., \alpha_K)$ характеризується важливістю відповідного коефіцієнта. Тобто $\alpha_i \geq \alpha_j$, якщо критерій f_i має перевагу над критерієм f_j. При цьому

$$\sum_{k=1}^{K} \alpha_k = 1, \quad \alpha_k \geq 0. \tag{6}$$

Складання матриці парних порівнянь проводиться за умови, що всі діагональні елементи дорівнюють одиниці, а значення решти елементів $K = \left[K_{ij} \right]$ групою експертів визначається за таких умов:

2 – якщо критерій *i* важливіший ніж критерій *j;*

1 – якщо критерій *i* і *j* мають однакову важливість;

0 – якщо критерій *i* менш важливіший ніж критерій *j.*

Підраховується рівень важливості кожного коефіцієнта K_i як

$$K_i = \sum_{j=1}^{n} K_{ij}. \tag{7}$$

Визначається загальний рівень важливості коефіцієнтів усіх критеріїв Kc, тобто

$$Kc = \sum_{i=1}^{n} K_i . \tag{8}$$

Розраховується важливість визначених коефіцієнтів згідно з виразом

$$\alpha_i = \frac{K_i}{Kc} \cdot \tag{9}$$

Таким чином, визначивши кількісні значення нормованих коефіцієнтів обраних показників та розрахувавши їх важливість, можна провести оптимальне ранжування джерел ІП (скласти рейтинг е-ЗМК) відповідно до поставлених завдань, використавши при цьому метод вагових коефіцієнтів за допомогою адитивної згортки.

У цьому випадку будується цільова функція вигляду

$$f\left(X\right) = K_m \sum_{i=2}^{5} \alpha_k K_i \left(X\right). \tag{10}$$

й вирішується завдання побудови рейтингу е-ЗМК за оптимізацією скалярного критерію, тобто

$$z = f\left(X\right) \to \max, \text{ за умови } X \in D , \tag{11}$$

де D – кількість обраних для ранжування джерел, X – кількість е-ЗМК вибраних для вирішення конкретної задачі моніторингу.

Наведемо практичний приклад застосування запропонованої методики (1) – (11) складання рейтингу е-ЗМК при організації моніторингу.

Вхідні дані. При постановці завдання на моніторинг визначено деяку тематику, що становить інтерес. Кількість джерел, за якими можна проводити моніторинг, дорівнює 40 новинним сайтам. Після розрахунку відповідності джерел тематиці поставленого завдання K_m, отримано 5 е-ЗМК, які необхідно розташувати за рейтингом відповідно до завдань моніторингу. За виразами (2) – (5) для кожного джерела розраховано визначені коефіцієнти та значення показників K_i, тобто

1-джерело – $K_{орф}$ =2, $K_{прф}$ =3, $K_{ст}$ =6, $K_{цф}$ =4,

2-джерело – $K_{орф}$ =7, $K_{прф}$ =5, $K_{ст}$ =2, $K_{цф}$ =4,

3-джерело – $K_{орф}$ =3, $K_{прф}$ =8, $K_{ст}$ =4, $K_{цф}$ =6,

4-джерело – $K_{орф}$ =9, $K_{прф}$ =1, $K_{ст}$ =6, $K_{цф}$ =3,

5-джерело – $K_{орф}$ =4, $K_{прф}$ =3, $K_{ст}$ =5, $K_{цф}$ =1.

За допомогою групи з 5-ти експертів розраховано важливості визначених критеріїв методом парних порівнянь. Дані наведено в табл. 3.

Таблиця 3

Рівень важливості коефіцієнтів K_i для першого е-ЗМК

	K_{opd}	K_{npd}	$K_{ст}$	$K_{цd}$	K_i
K_{opd}	1	0	2	2	5
K_{npd}	2	1	2	2	7
$K_{ст}$	0	0	1	0	1
$K_{цd}$	0	0	2	1	3

Тоді значення важливості розглянутих коефіцієнтів за формулою (9) дорівнює:

$$\alpha_{K_{opd}} = \frac{5}{16} = 0{,}3125;\ \alpha_{K_{npd}} = \frac{7}{16} = 0{,}4375;\ \alpha_{K_{ст}} = \frac{1}{16} = 0{,}0625;\ \alpha_{K_{цd}} = \frac{3}{16} = 0{,}1875.$$

Далі обчислено адитивну згортку на основі методу вагових коефіцієнтів для кожного джерела за формулою (10):

$$f(1) = 1\times(0{,}3125\times 2 + 0{,}4375\times 3 + 0{,}0625\times 6 + 0{,}1875\times 4) = 3{,}06;$$
$$f(2) = 1\times(0{,}3125\times 7 + 0{,}4375\times 5 + 0{,}0625\times 2 + 0{,}1875\times 4) = 5{,}25$$
$$f(3) = 1\times(0{,}3125\times 3 + 0{,}4375\times 8 + 0{,}0625\times 4 + 0{,}1875\times 6) = 5{,}81$$
$$f(4) = 1\times(0{,}3125\times 9 + 0{,}4375\times 1 + 0{,}0625\times 6 + 0{,}1875\times 3) = 4{,}19$$
$$f(5) = 1\times(0{,}3125\times 4 + 0{,}4375\times 3 + 0{,}0625\times 5 + 0{,}1875\times 1) = 3{,}13$$

З приведених даних випливає те, що для визначеного завдання на моніторинг джерела ІП розподілені за таким рейтингом (табл. 4).

Таблиця 4

Рейтинг електронних засобів масової комунікації при організації контент-моніторингу

Позиція в рейтингу	Номер е-ЗМК	Значення цільової функції
1	3-джерело	5,81
2	2-джерело	5,25
3	4-джерело	4,19
4	5-джерело	3,12
5	1-джерело	3,06

Отже, запропонована методика складання рейтингу електронних засобів масової комунікації забезпечує оптимізацію складу і кількості джерел шляхом

складання рейтингу за найбільш впливовими показниками відповідно до цілей і задач моніторингу, що забезпечує підвищення ефективності процесу організації моніторингу е-ЗМК, зменшення залучених людських та технічних ресурсів для вирішення поставлених завдань.

Висновки та перспективи подальших досліджень

Таким чином, в статті показано, що з метою визначення пріоритетності вибору джерел для організації їх моніторингу необхідно здійснювати їх ранжування. Доведено, що для побудови їх рейтингів доцільно скористатися рядом критеріїв, що розраховують відповідні показники залежно від задач моніторингу та характеристик джерел інформаційних повідомлень. Це дозволяє оптимізувати вибір джерел відповідно до задач моніторингу, виявляти першоджерела інформаційних повідомлень, значно скоротити витрати часу і засобів шляхом ігнорування або виключення з аналізу найменш інформативних джерел.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 634 с.

2. Грищук Р. В. Особливості організації та ведення моніторингу електронних засобів масової комунікації / Р. В. Грищук, О. В. Манько, І. О. Орищук // Інформаційна Безпека. Східноукраїнський національний університет ім. Володимира Даля. – 2014. – № 3–4 (15–16). – С. 10–14.

3. InfoStream. Мониторинг новостей из Интернет: технология, система, сервис: научно-методическое пособие / А.Н. Григорьев, Д.В. Ландэ, С.А. Бороденков та ін. – К., ООО "Старт-98", 2007. – 40 с. [Електронний ресурс]. – Режим доступу : http://infostream.ua/news36/.

4. Информационно-аналитическая система Медиология [Електронний ресурс]. – Режим доступу : http://www.mlg.ru/company/technologies/.

5. Silobreaker [Електронний ресурс]. – Режим доступу : http://www.silobreaker.com/.

6. Ранжирование источников информации в системе мониторинга новостей InfoStream / Д.В. Ландэ, С.М. Брайчевский, А.Т. Дармохвал, А.Ю.Морозов // Труды 10-ой Всероссийской научной конференции "Электронные библиотеки: перспективные методы и технологии, электронные коллекции"- RCDL'2008, Дубна, Россия, 2008. – С. 213–219.

7. Ландэ Д.В. Стабильность источников как один из параметров информационных потоков / Д.В. Ландэ, А.Н. Григорьев, С.М. Брайчевский // Компьютерная лингвистика и интеллектуальные технологии: По материалам ежегодной Международной конференции "Диалог". Вып.7 (14). – М. : РГГУ, 2008. – 649 с.

8. Основы моделирования и оценки электронных информационных потоков: монография / Д.В. Ландэ, В.Н. Фурашев, С.М. Брайчевский, А.Н. Григорьев. – К. : Инжиниринг, 2006. – 176 с.

9. Коломоец Ф.Г. Основы системного анализа и теории принятия решений: пособие для исследователей, управленцев и студентов вузов / Ф.Г. Коломоец. – Мн. : Тесей, 2006. – 300 с.

Отримано 27.10.2016

Рецензент Рибальський О.В., д.т.н.

УДК 007.51:004.491

В.О. Хорошко,
доктор технічних наук, професор,
Р.В. Грищук,
доктор технічних наук, старший науковий співробітник

КІБЕРНЕТИЧНА ЗБРОЯ: КЛАСИФІКАЦІЯ, БАЗОВІ ПРИНЦИПИ ПОБУДОВИ, МЕТОДИ ТА ЗАСОБИ ЗАСТОСУВАННЯ Й ЗАХИСТУ ВІД НЕЇ

У статті запропоновано нову класифікацію кібернетичної зброї, яка позбавлена від більшості недоліків відомих класифікацій. Розкрито характерні ознаки, властиві кібернетичній зброї, та визначено основні завдання, що покладаються на неї її розпорядниками.

Ключові слова: *кібернетична зброя, класифікація, кібервійна, кібербезпека, кібервплив, кіберрозвідка, кіберзахист.*

В статье представлено новую классификацию кибернетического оружия в которой отсутствуют недостатки известных классификаций. Раскрыты характерные признаки, свойственные кибернетическому оружию, и определены основные задания, возложенные на него его распорядителями.

Ключевые слова: *кибернетическое оружие, классификация, кибервойна, кибербезопасность, кибервоздействие, киберразведка, киберзащита.*

In the paper it is suggested a new classification of cyber weapon without drawbacks of previous classifications. Main characteristics relevant to cyber weapon are revealed and the main tasks designated to it by the owners are defined.

Keywords*: cyber weapon, classification, cyber war, cyber security, cyberattack, cyber intelligence, cyber protection.*

Постановка проблеми в загальному вигляді та її зв'язок з важливими практичними завданнями. У статті аргументовано доведено та показано те, що кібернетична зброя (далі – КЗб) на сьогодні є одним з найновіших й найдієвіших зразків сучасної зброї [1]. Крім того, в попередніх дослідженнях розкрито етимологію поняття зброя та показано сучасні підходи до її трансформації в кібернетичну. Тому, незважаючи на те, що на сьогодні вже встановлено сутність та зміст КЗб, невирішеною остаточно залишається проблема формалізації простору ознак, належність від яких дозволятиме здійснювати класифікацію кібернетичної зброї.

Аналіз останніх досліджень і публікацій показав, що на сьогодні відомо три основні класифікації КЗб: американська, яка розроблена в 2011 році в Пентагоні та є загальноприйнятою в США для всіх силових структур, та дві класифікації, розроблені незалежно одна від одної експертами П. Пассері та П. Паганіні. Є й інші підходи до класифікації, зокрема В. Каберника [1; 2; 3; 4].

Так, відомості щодо класифікації КЗб в США мають гриф обмеження доступу. Друга класифікація наведена у квітні 2012 року в статті *"What is a Cyber Weapon?"* П. Пассері. Класифікація П. Пассері показує, що КЗб класифікується за чотирма параметрами: точність (націлювання на досягнення конкретної мети та зменшення при цьому побічних збитків); рівень проникнення; скритність; ресурсоємність. Як видно з приведеної класифікації, автор для спрощення її сприйняття застосував метод аналогій. Така класифікація очевидно є неповною.

Альтернативний варіант класифікації КЗб запропоновано П. Паганіні у квітні 2012 року в статті *"Cyber Weapons"*. В основу класифікації покладено спектр її дії. Так, за спектром дії КЗб буває низького, середнього та високого потенціалу. До КЗб низького потенціалу належить зброя, яка є шкідливою, але такою, що не спроможна проникати до конкретної цілі та завдавати їй прямої шкоди. До КЗб середнього потенціалу належить зброя, що може проникати на об'єкт кібернетичного впливу, але не спроможна досягати конкретної мети. При цьому вона за будь-яких умов завдає збитків інфраструктурі та противнику. Кібернетична зброя високого потенціалу здатна до проникнення на об'єкт, долаючи систему захисту, та водночас спроможна завдати катастрофічних збитків. Приведена класифікація також є досить умовною як і попередня, що значно обмежує її застосування на практиці.

У статті В. Каберника теж запропоновано класифікацію КЗб, яка, на нашу думку, є найбільш повною, але відсутність у її описі ознак комплексності суттєво звужує всебічний опис характеристик такої зброї [4; 1].

Метою статті є розроблення принципово нової класифікації кібернетичної зброї, яка позбавлена від недоліків відомих класифікацій та, на відміну від них, спроможна описувати характеристики будь-якого зразка кібернетичної зброї незалежно від його спектра дії.

Викладення основного матеріалу дослідження. Для досягнення поставленої в статті мети було розглянуто та досліджено базові підходи до побудови класифікацій, які ґрунтовно розкрито в [1]. Об'єм статті не дозволяє більш ґрунтовно розглянути зазначене вище питання, а тому далі пропонуємо зупинитися суто на предметі цього дослідження.

Під класифікацією КБз будемо розуміти розподілення усіх можливих її видів на взаємопов'язані класи, визначені на підставі найбільш суттєвих та важливих у практичному відношенні ознак [1].

Зважаючи на прийняте визначення, класифікація видів КЗб за умови вибору правильних суттєвих ознаках класифікації має забезпечити вирішення таких основних завдань: розкрити основні зв'язки між видами КЗб; допомогти практикам орієнтуватися в найскладніших ситуаціях, правильно класифікувати нові зразки, типи і види КЗб, що будуть виникати в майбутньому; стати основою для формування правильних узагальнюючих висновків та прогнозів як виникнення і розвитку нових видів КЗб, так і відповідних способів ведення збройної боротьби; стати основою для обґрунтування нової та вдосконалення існуючих технологій у галузі нових видів зброї; забезпечити швидкий пошук інформації про види КЗб в сучасних інформаційно-пошукових системах. Крім того, класифікація видів КЗб має забезпечувати ефективну цілеспрямовану роботу з подальшого дослідження впливу вражаючих факторів того чи іншого виду зброї на об'єкти ураження, оскільки більшість наявної в доступній літературі інформації щодо впливу новітніх видів

зброї на ті чи інші об'єкти має уривчастий і, як правило, лише описовий характер. Використання такої інформації є неефективним. На підтвердження цьому можна привести такі аргументи.

По-перше, уражаючі фактори зброї не завжди чітко визначені і класифіковані за ефективністю впливу на об'єкти. По-друге, не зазначаються умови проведення й основні обмеження при проведенні досліджень щодо впливу вражаючих факторів новітніх видів зброї на ті чи інші об'єкти, а якщо і наводяться, то вони, як правило, різні. Різняться також методології і критерії обґрунтування мінімально ефективних рівнів їх впливу. Унаслідок цього вже одержані окремі практичні результати впливу новітніх видів зброї на ті чи інші об'єкти, але їх неможливо звести до однотипних умов та обмежень, а тому і неможливо провести їх порівняльний аналіз і зробити правильні наукові й практичні висновки та прогнози. По-третє, не вирішено остаточно питання оцінювання значимості тих чи інших уражаючих факторів при їхньому впливі на організм людини, військову техніку, навколишнє середовище. Отже, наявність приведених вище аргументів суттєво стримує роботу дослідників, а одержувані окремі висновки і прогнози не завжди адекватно відображають справжній стан справ. Саме тому ще й досі не створено узагальненої, універсальної класифікації КЗб. Розглянемо хоча б загалом, якою повинна бути така класифікація на сучасному рівні розвитку наукових знань.

На основі проведеного аналізу відомих класифікацій пропонується узагальнена класифікація, яка може бути використана для опису широкого спектру зразків КБз. З урахуванням того, що КБз досить різноманітна, то основним принципом, який можна покласти в основу класифікації є ознаковий. Вперше такий підхід було реалізовано для класифікації кібератак у [5].

Пропонується класифікувати КБз за такими базовими ознаками: призначення, масштабність застосування; характер вражаючої дії; спосіб доставки; керованість; деструктивний вплив; оперативність; місце базування; рівень маскування; спосіб виготовлення; спектр дії; об'єкти ураження; рівень впливу на об'єкти ураження; прицільні властивості; інтегральний ефект; тип зв'язків та рівень взаємодії; наслідки; принцип генерування; самоорганізація; тривалість ефекту; латентність. Класифікаційний граф КБз наведено у вигляді рисунку в [1].

За призначенням КБз поділяється на: розвідувальну; захисну; зброю кібернетичного впливу. Розвідувальна зброя призначена для добування інформації з кіберпростору або в кіберпросторі шляхом моніторингу кібернетичних систем та процесів, які в них протікають під час функціонування. Кібернетична зброя захисту призначена для забезпечення та підтримання заданого рівня кібербезпеки. Зброя, що призначена для здійснення кібернетичного впливу на елементи кіберпростору противника з метою порушення процесів управління в кібернетичних системах, називаються зброєю кібернетичного впливу.

За масштабами застосування КБз може бути: глобальна, стратегічна, тактична. Застосування КБз несе глобальний характер, коли масштаб від її застосування потенційно може поширюватися на всі держави, в яких функціонують об'єкти з критичною кібернетичною інфраструктурою. Стратегічний масштаб застосування КБз поширюється на міждержавний (регіональний) рівень. Тактична КБз за масштабом застосування орієнтована переважно на застосування на національному рівні.

За характером уражаючої дії КБз поділяється на: зброю масового ураження, зброю функціонального ураження, функціонального придушення, функціонального

виведення з ладу. Кібернетична зброя масового ураження має такий характер вражаючої дії, який співвимірний з наслідками, що виникають унаслідок застосування зброї масового ураження (ядерної, хімічно, біологічної). Застосування КБз функціонального ураження призводить до ураження окремих функцій, що виконуються об'єктом, внаслідок чого він втрачає здатність до виконання цільової задачі. Кібернетична зброя функціонального придушення передбачає функціональне придушення, що призводить до комплексної дії на об'єкт з критичною кібернетичною інфраструктурою внаслідок чого він втрачає здатність до виконання цільової задачі протягом заданого інтервалу часу. Результатом функціонального виведення з ладу є генерація необоротних процесів, що призводять до виведення з ладу об'єктів впливу.

За способом доставки КБз поділяється на таку, що може доставлятися: природними носіями або штучними носіями. Природним носієм доставки КБз є людина. Наприклад, інсайдер. Штучними носіями є всі інші засоби, що не є об'єктами біологічного походження.

За керованістю КБз поділяється на: керовану і некеровану. Керована КБз передбачає постійне або періодичне управління процесом її бойового застосування. Некерована КБз – це зброя яка не потребує зовнішнього втручання в процесі її цільового застосування.

За деструктивним впливом КБз може бути: безпечна, небезпечна. Ця класифікаційна ознака є специфічною. Вона властива тільки КБз, оскільки "зброя" в принципі не буває "безпечною" або "небезпечною". До безпечної, з точки зору руйнівних властивостей, можна віднести зброю, яка не призводить до фізичних руйнувань інфраструктури об'єкта, а порушує властивості безпеки інформації на ньому. Наприклад, розвідувальна КБз призводить до порушення конфіденційності інформації на об'єкті, що розвідується, але жодним чином не руйнує його інфраструктуру. Небезпечна – зброя, деструктивний вплив від якої має прояви як для інфраструктури об'єкта, так і для безпеки інформації, яка на ньому циркулює.

За оперативністю КБз може бути: миттєвої дії; повільної дії з накопиченням; тимчасової дії; довгострокової дії. Миттєва дія КБз співвимірна з масштабом часу, протягом якого вона проявляє деструктивний вплив на об'єкт або суб'єкт впливу. Кібернетична зброя повільної дії з накопиченням – це зразок зброї, корисний ефект від застосування якої поступово накопичується і при досягненні заданого рівня насичення проявляє свої деструктивні властивості. За оперативністю КБз тимчасової дії орієнтована на виконання своїх деструктивних функцій протягом деякого відносно нетривалого інтервалу часу. Довгострокова дія КБз характеризується відносно тривалим інтервалом часу, протягом якого вона використовується за призначенням.

За місцем базування КБз буває: космічного базування, повітряного базування, наземного базування, морського базування, підземного базування, змішаного базування. Місце базування КБз визначається, виходячи, в першу чергу, із того кола задач, які на неї покладаються. Переважно КБз має змішане базування.

За рівнем маскування КБз може бути: замаскованою; незамаскованою. Замаскована КБз передбачає застосування елементів маскування. Незамаскована – навпаки, такі елементи не використовує.

За способом виготовлення КБз поділяється на: кустарну, промислову, змішану. Кустарне виробництво передбачає виготовлення зразка несерійного характеру, як

правило, особою або групою осіб та не передбачає залучення державного фінансування. Кібернетична зброя промислового виготовлення – це зброя, яка виготовляється, зазвичай, на замовлення держави або групи держав із залученням її промислових потужностей. Кібернетична зброя за змішаним способом виготовлення поєднує в собі елементи кустарного та промислового виробництва. *За спектром дії* КБз можна поділяти на зброю: низького потенціалу; середнього потенціалу; високого потенціалу. Кібернетична зброя низького потенціалу призводить до деструктивного впливу, що не чинить об'єкту впливу безпосередньої шкоди. Прикладом такої зброї є спеціалізоване програмне забезпечення для генерації потужного потоку трафіку з метою тимчасового перевантаження ресурсів системи, що призводить до заподіяння тимчасової шкоди об'єкту впливу без нанесення йому будь-яких фізичних пошкоджень. Кібернетична зброя середнього потенціалу – це зброя, застосування якої призводить до функціонального ураження або придушення, але не до функціонального виведення з ладу об'єкта впливу. Кібернетична зброя високого потенціалу – це зброя, що здатна досягати об'єкта впливу шляхом обходу його систем захисту й здатна до його функціонального виведення з ладу.

Цілями ураження КБз можуть бути: об'єкти з критичною кібернетичною інфраструктурою; суб'єкти управління. Об'єкти з критичною кібернетичною інфраструктурою – це матеріальні чи віртуальні об'єкти й системи, порушення або припинення функціонування яких призводить до втрати управління, руйнування інфраструктури, незворотних негативних змін або руйнувань економіки країни, суб'єкта або адміністративно-територіальної одиниці, або до впливу на безпеку населення, яке мешкає на цих територіях. Суб'єкт управління як ціль ураження – це особа, група людей або організація, що приймає управлінські рішення та керує об'єктами з критичною кібернетичною інфраструктурою шляхом впливу на них.

За рівнем впливу на об'єкти ураження: об'єкти, що підлягають відновленню; об'єкти, що не підлягають відновленню. Вплив КБз на об'єкти ураження може мати дуальний характер: об'єкти можуть підлягати відновленню за деякий часовий термін або ж такому відновленню не підлягають.

За рівнем впливу на суб'єкти ураження КБз може бути: смертельної дії; несмертельної дії; настроювальної дії. Кібернетична зброя смертельної дії передбачає завдання смертельних збитків протиборчій стороні в живій силі. Кібернетична зброя несмертельної дії не призводить до загибелі живої сили протиборчої сторони. Кібернетична зброя з настроювальною дією – це зброя, властивості якої щодо впливу на живу силу протиборчої сторони налаштовуються у процесі її застосування шляхом виставлення порогу кібернетичного впливу.

За прицільними властивостями КБз буває двох видів: високоточною та неприцільною. Високоточна КБз призначена для нанесення високоточних ударів по визначеним цілям кібернетичного впливу. Неприцільна – це зброя, яка не володіє прицільними властивостями щодо конкретних цілей.

За типом зв'язків та рівнем взаємодії: поодинока; групова. Кібернетична зброя, що належить до класу поодинокої, передбачає застосування її без залучення додаткових допоміжних модулів. До групової відносять КБз, яка для досягнення своєї мети використовує додаткові модулі, що у своїй сукупності дозволяють досягнути поставленої перед нею цілі.

Кібернетична зброя *за наслідками* поділяється на: глобальну, регіональну, локальну. Застосування КБз несе глобальний характер, коли масштаб від її застосування потенційно може призвести до загибелі людської цивілізації. Стратегічний масштаб застосування кібернетичної зброї означає її здатність до зміни ролі й призначення кібернетичних систем на міждержавному (регіональному) рівні. Тактична КБз за масштабом застосування призначена для вирішення задач тактичного рівня у визначеному регіоні.

За генеруванням КБз може бути: самогенеруюча; з часовим механізмом; за настанням визначеної події. Самогенеруюча КБз – це зброя, яка не потребує зовнішнього втручання для приведення її в готовність до виконання задач. Генерування за часовим механізмом передбачає приведення в готовність зброї у визначений момент часу. Настання визначеної події інколи також виступає підставою для виконання КБз своїх функцій.

За рівнем інтегрального ефекту КБз поділяється на: зброю часткового ефекту, зброю з повним ефектом. Інтегральний ефект від застосування КБз має дві форми прояву: часткову, коли ефект має лише локальні частинні наслідки, та повну форму прояву, коли ефект носить глобальний характер.

За самоорганізацією КБз буває: самоорганізованою; за окремою командою. Самоорганізованість КБз – це процес упорядкування елементів одного рівня в системі за рахунок внутрішніх закладених функцій, без зовнішнього специфічного впливу. Самоорганізація КБз за окремою командою передбачає реалізацію визначеного вище процесу при надходженні відповідного зовнішнього специфічного впливу – команди.

За часом тривалості ефекту КБз буває: миттєвого ефекту, відкладеного ефекту. Миттєвий ефект від застосування КБз проявляється в масштабі часу, співвимірному з часом її цільового застосування. Якщо ефект від застосування КБз проявляється дещо пізніше від моменту початку її застосування за цільовим призначенням, то така зброя є зброєю з відкладеним ефектом.

За латентністю КБз буває: негайного прояву, відкладеного прояву. Кібернетична зброя, яка проявляє себе належним чином у процесі застосування, є зброєю негайного прояву. У протилежному випадку, коли латентний період є досить тривалим, – КБз може бути кібернетичною зброю з відкладеним проявом.

Перевагою запропонованої класифікації, порівняно з відомими є те, що КБз, яка класифікується за ознаковим принципом, може в кожному конкретному випадку при визначенні загального класу містити не тільки одну, але й більше компонент будь-якої з ознак. Крім того, покладений в основу класифікації ознаковий принцип забезпечує розширення множини ознак, за якими можна здійснювати класифікацію.

Покажемо приклад застосування розробленої класифікації на практиці. Такий зразок КБз, як *Stuxnet* може бути класифікований таким чином. *Stuxnet* – це КБз, яка призначена для здійснення керованого небезпечного кібервпливу стратегічного характеру, спрямованого на функціональне виведення з ладу об'єктів з критичною кібернетичною інфраструктурою. Зразок має довгострокову дію. Характеризується наземним базуванням та доставляється природним носієм. Рівень маскування характеризує його як невидимий зразок промислового походження, спрямований для нанесення кібервпливу з метою невідновлення об'єктів впливу. *Stuxnet* є високоточним зразком з повним рівнем інтегрального ефекту групового

характеру, що має глобальні наслідки й самогенерується. Зброя є самоорганізованою з відкладеним часом тривалості ефекту й відкладеним проявом.

Висновки. Запропонована класифікація на відміну від відомих забезпечує формалізацію вимог до новостворюваних зразків КБз. Вона не претендує на закінченість, не є остаточною, а тому буде доповнюватися, уточнюватися і розвиватися в майбутньому з вдосконаленням цієї зброї і способів її застосування. Водночас така класифікація дає можливість більш чітко уявити особливості механізму дії КБз на всі можливі об'єкти ураження, спрогнозувати тенденції її розвитку, а також передбачити заходи щодо захисту від факторів її ураження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Г*рищук Р.В.* Основи кібернетичної безпеки : монографія / Р.В. Грищук, Ю.Г. Даник ; за заг. ред. проф. Ю.Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

2. *Passeri P.* What is a Cyber Weapon? / P. Passeri. [Electronic resource]. - Access mode : http://www.hackmageddon.com/2012/04/22/what-is-a-cyber-weapon/#comments.

3. *Paganini P.* Cyber Weapons. / *P. Paganini*. [Electronic resource]. - Access mode : http:// securityaffairs.co/wordpress/3896/intelligence/cyber-weapons.html.

4. *Каберник В.В.* Проблемы классификации кибероружия / В.В. Каберник // Вестн. МГИМО. – 2013. – № 2 (29) – С. 72–73.

5. *Корченко О.Г.* Ознаковий принцип формування класифікацій кібератак / О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк та ін. // Вісник Східноукраїнського національного університету імені Володимира Даля – № 4 (146) – Ч. 1, 2010. – С. 184–193.

Отримано 01.11.2016
Рецензент Рибальський О.В., д.т.н

УДК 681.3.06

В.А. Хорошко,
доктор технических наук, профессор,
Ю.Е. Хохлачева,
кандидат технических наук, доцент,
Л.И. Моржова

ВЫБОР ЭЛЕМЕНТНОЙ БАЗЫ ДЛЯ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

В работе рассматривается методика выбора элементной базы для бортового вычислителя беспилотного летательного аппарата и его проектирование.
Ключевые слова: *элементная база, микропроцессорные наборы, бортовой вычислитель, беспилотный летательный аппарат.*

В роботі розглядається методика вибору елементної бази для бортового обчислювача безпілотного літального апарату і його проектування.
Ключові слова: *елементна база, мікропроцесорні набори, бортовий обчислювач, безпілотний літальний апарат.*

In this paper the method of choice for the elemental base for board calculator of unmanned aerial vehicle and its design is considered.
Keywords: *electronic components, chipset, onboard computer, unmanned aerial vehicle.*

Введение

Выбор элементной базы и проектирования бортового вычислителя (далее – БВ) для беспилотного летательного аппарата (далее – БПЛА) весьма сложная и ответственная задача, при решении которой необходимо учитывать различные факторы.

Большой выбор микропроцессорных наборов (далее – МПН) и однокристальных микро-ЭВМ (далее – ОМЭВМ) требует системного подхода к выбору аппаратного обеспечения БВ.

Так как в настоящее время БПЛА являются основными элементами информационно-разведывательными средствами обеспечения информацией, поэтому резко возросли требования к их бортовой аппаратуре.

Важнейшими аспектами эффективности применения БПЛА является:

1) развитие и усовершенствование систем видеонаблюдения обстановки;

2) разработка БВ;

3) предоставление информационного обеспечения, достаточного для принятия решений;

4) увеличение разведзащищенности каналов связи и управления БПЛА;

5) увеличение скорости передачи данных в каналах связи;

6) разработка и внедрение новых концепций, реализация которых является принятой по критерию “эффективность-стоимость-время” [1].

Как видно из выше сказанного все пункты завязаны на пункте “2”. Кроме того, цифровое оборудование БПЛА все больше приближается по своим характеристикам к интеллектуальным микропроцессорным системам, что позволяет создавать очень гибкую политику проведения разведки, приближающуюся по

своим функциям и механизмам перестраиваемых вычислительных структур. Именно поэтому современные БВ можно называть составной частью интеллектуальной разведывательной системы (далее – ИРС), реализованной на базе МПН и ОМЭВМ [2].

Потребность в решении сложных задач обработки информации в реальном масштабе времени с высокой точностью определяет актуальность проблемы выбора элементной базы для БВ. При этом сложная задача представляется в виде совокупности взаимосвязанных подзадач, которые решаются последовательно-параллельно.

Анализ публикации

В настоящее время используются несколько методов выбора МПН и ОМЭВМ. Один из методов использует бенчмарковские программы, ускоряет процесс разработки за счет того, что длина бенчмарка ограничена и содержит 100-200 команд, анализируемых МПН и ОМЭВМ, однако при их применении при составлении программы требует изучения и учета систем команд всех МПН и ОМЭВМ, что достаточно сложно и трудоемко [3; 4].

Другой подход к выбору заключается в следующем. Разработчику необходимо составить таблицу основных характеристик всех существующих МПН и ОМЭВМ, ограничиваясь выбором из нескольких характеристик одинаковой значимости (не более 12) [4; 5]. Эталонным считается гипотетический микропроцессор (а для ОМЭВМ однокристальная ЭВМ), с лучшими показателями. Далее они сравниваются по всем показателям с базовыми. Микропроцессор или микро ЭВМ, характеристики которого наиболее близки к эталонным, считается лучшим. Оценки, полученные при использовании данной методики, не отражают многих особенностей и специфики их применения на объекте, поэтому являются приближенными и пригодны только для предварительной ориентации. Таким образом, сведения различные по своей природе показателей в единую целевую функцию с параметрами, определяемыми с помощью экспертных оценок, трудоемко из-за большого объема вычислений. Кроме того, данная методика не ориентирована на проектирование и разработку БВ и не учитывает структуру алгоритма, для которого разрабатывается БВ.

Наиболее перспективным методом, который используют при разработке БВ, являются кросс-моделирующие средства [6]. Однако в этом случае разработчику необходимо обращаться к банку данных кросс-моделирующих программ, ориентированных на построение и отладку программ для всех микропроцессоров и ОМ ЭВМ на языке высокого уровня, что не везде приемлемо.

Цель работы

В статье предлагается автоматизированная процедура выбора компонентов для проектируемых БВ по критерию быстродействие – аппаратные затраты.

Основная часть

Алгоритм процедуры выбора элементной базы для БВ приведен на рис.1. Суть метода заключается в следующем. Разработке по заданному алгоритму, который должен быть реализован в БВ, составляет программу на языке высокого уровня, которая реализуется на ЭВМ. В процессе ее выполнения составляется таблица, где дается информация о количестве содержащихся в объектном модуле коротких машинных операций типа: сложения, вычитания, пересылки и сдвига. По завершении выполнения исходной программы анализирующая программа обращается по второй таблице, в которой приведены времена выполнения коротких операций различными МПН и ОМЭВМ. Перемножив соответствующие графы двух таблиц, а затем просуммировав результаты, рассчитывают предварительную оценку времени выполнения заданного алгоритма на всех МПН или ОМЭВМ.

Даже из множества всех МПН или ОМЭВМ с помощью оценок выбираются такие, которые удовлетворяют по быстродействию техническое задание (далее –

ТЗ). В полученном подмножестве находим элемент, требующий минимальных затрат по основным критериям, заданным в ТЗ, к которым относятся: объем памяти запоминающего устройства L; разрядность чисел $n_ч$, команд $n_к$, запоминающего арифметического устройства $n_{зу}$; скорость ввода $V_{вв}$ и вывода $V_{выв}$ информации. Затем разрабатывается программа в системе команд выбранного микропроцессора или ОМЭВМ и рассчитываются точные характеристики по критериям быстродействие – аппаратурные затраты (т.е. быстродействие V). Большое внимание в БВ уделяется требованиям надежности, безотказной работе P(T) и готовности вычислителя $K_г(t)$ к работе. Так же, к основным характеристикам БВ относят: потребляемую мощность, габариты, массу и требования эксплуатации (допустимые значения постоянных перегрузок, амплитуды и частоты вибрации, давления и температуры окружающей среды и т.п.). Кроме того, обязательно указывается режим работы БВ по времени.

Быстродействие БВ определяется при помощи следующего выражения:

$$V = \frac{1}{\sum_{i=1}^{n} f_i T_i}, \quad (1)$$

где f_i – частота выполнения операции i-го типа,

T_i – время на выполнение этой операции.

Разрядность чисел для БВ с плавающим запятой в двоичных разрядах.

$$n_2 = n_{Зп} + n_п + n_{Зм} + n_{м,} \quad (2)$$

где, $n_{Зп}$ – разрядность знака порядка;

$n_п$ – разрядность порядка;

$n_{Зм,}$ $n_м$ – разрядность соответственно знака мантиссы и самой мантиссы.

Разрядность чисел для БВ с фиксированной запятой двоичных разрядах

$$n_г' = n_{Зп} + n_м. \quad (3)$$

Разрядность запоминающего устройства определяется длинной слова, которое может быть записано в ячейку памяти (т.е. максимальная длина слова (числа), которое может перерабатываться).

Объем памяти запоминающего устройства

$$L = \mu + n_1, \quad (4)$$

где μ – количество ячеек запоминающего устройства;

n – разрядность одной ячейки.

Скорость работы БВ на ввод и на вывод описывается следующим образом:

$$\begin{cases} V_{вв} = \dfrac{1}{\tau_{вв}} \\ V_{выв} = \dfrac{1}{\tau_{выв}} \end{cases}, \quad (5)$$

где $\tau_{вв}$ и $\tau_{выв}$ – время, приходящееся соответственно на ввод и вывод одного n-разрядного числа.

Для оценки надежности БВ выбираем характеристику W, определяющую вероятность правильности вычислений:

$$W = k_г(t)P(T). \quad (6)$$

где T – время выполнения задачи;
$k_г$ – коэффициент готовности БВ [6].

Коэффициент готовности определяется по времени наработки на отказ $T_{но}$ и среднему времени для устранения неисправности $T_{сун}$ с помощью следующей зависимости:

$$k_г(t) = \frac{T_{но}}{T_{но} \cdot T_{сун}} \quad (7)$$

Вероятность безотказной работы БВ

$$P(t) = [1 - P_{сб}(T)]\,[1 - P_{отк}(T)]. \quad (8)$$

Подставив выражение (7) и (8) в (6), получаем

$$W = \frac{[1 - P_{сб}(T)][1 - P_{отк}(T)]T_{но}}{T_{но} + T_{сун}} \quad (9)$$

Обобщающей характеристикой БВ является производительность E (или критерий эффективности применения вычислителя), под которой будем понимать количество решаемых задач от момента ввода программы и до выдачи команды управления в единицу времени.

В соответствии с методикой [8] для оценки эффективности определим время решения тестовой (эталонной) задачи:

$$T_э = T_{вв}(1-\varepsilon_1) + T_с + T_г + T_к + T_р + T_{выв}(1-\varepsilon_2), \quad (10)$$

где $T_{вв}$ – время ввода программы;
$T_с$ – время работы БВ при управлении;
$T_г$ – время, расходуемое на обмен информации между запоминающими устройствами;
$T_{выв}$ – время выдачи команд управления;
$T_к$ – время контроля функционирования БВ (в процессе решения задачи);
ε_1 и ε_2 – коэффициенты совмещения ввода и вывода информации с процессом решения;
$T_р$ – время профилактического осмотра и ремонта.

Если предположить, что $T_р = \beta T_э$, то критерий можно записать как

$$E_р = \frac{1-\beta}{T_{вв}(1-\varepsilon_1) + T_с + T_г + T_к + T_{выв}(1-\varepsilon_2)}. \quad (11)$$

Зная количество исходных чисел N_1, чисел в программе $N_{пр}$, чисел в выходной информации N_2, а так же V, $V_{вв}$ и $V_{выв}$, найдем следующие временные параметры:

$$\left.\begin{aligned} T_{вв} &= \frac{N_1 + N_{пр}}{V_{вв}}; \\ T_c &= \frac{N_c}{V}; \\ T_{выв} &= \frac{N_2}{V_{выв}}; \end{aligned}\right\}, \qquad (12)$$

где N_c – количество операций, выполняемых БВ в тестовой программе.

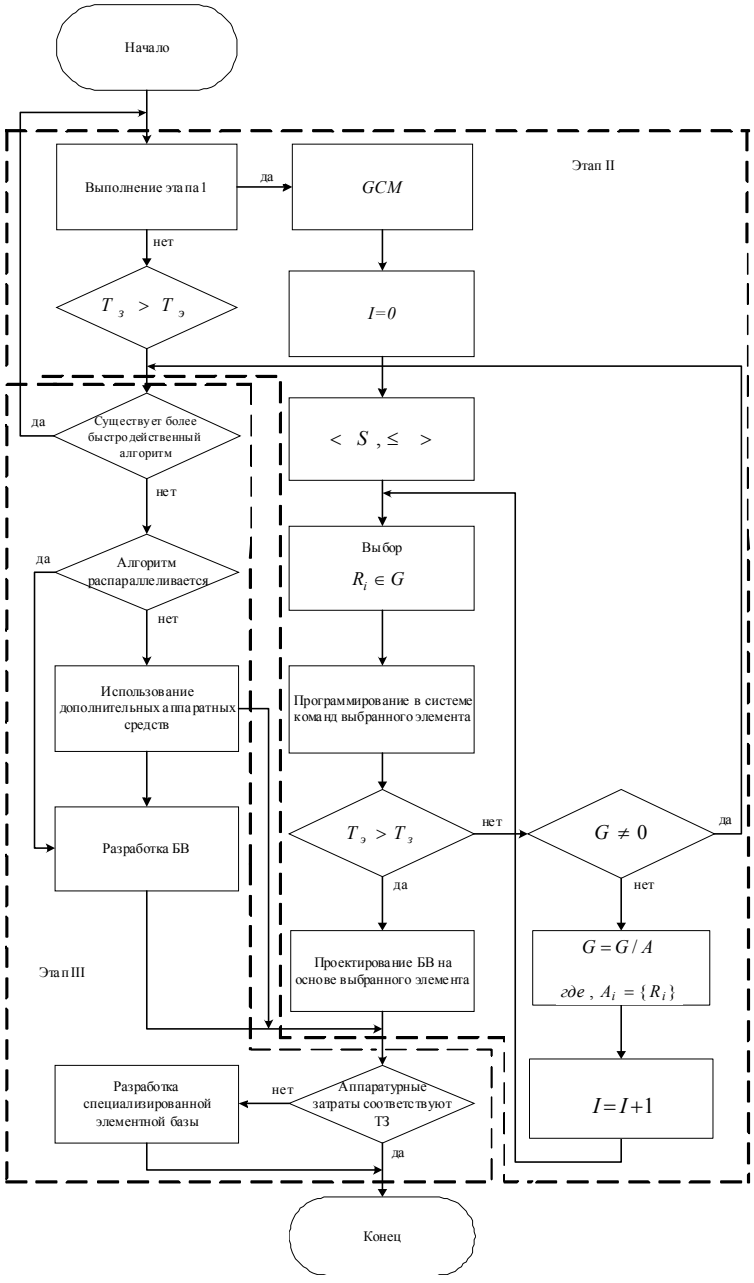


Рис.1. Алгоритм процедуры выбора элементной базы для БВ

Следовательно, время обмена информации можно записать в виде:

$$T_{г} = \sum_{(v)} [(Z_{1v} + Z_{2v})\tau_v + (S_v + S_v^*)\frac{\tau_{ov}}{2}]\frac{1}{D_v}, \qquad (13)$$

где Z_{1v} – количество чисел и команд, пересылаемых в оперативное запоминающее устройство (ЗУ) из v-го постоянного ЗУ;

Z_{2v} – количество чисел и команд, пересылаемых из ОЗУ в v-е ПЗУ;

S_v, S_v^* – соответственно номера обращения к v-м ПЗУ для считывания или записи информации в ОЗУ;

τ_v, τ_{ov} – время (чисел) работы соответственно ОЗУ и ПЗУ;

D_v – коэффициент выигрыша времени при совмещении передачи информации из ОЗУ в ПЗУ и наоборот.

Подставив в выражение (11) формулы (12) и (13), определим

$$E = \frac{1-\beta}{\frac{N_1 + N_{пр}}{V_{вв}(1-\varepsilon_1)} + \frac{N_c}{V} + \sum_{(v)} [(Z_{1v} + Z_{2v})\tau_v + (S_v + S_v^*)\frac{\tau_{ov}}{2}]\frac{1}{D_v} + T_к + \frac{N_2}{V_{выв}}(1-\varepsilon_2)}. \qquad (14)$$

Необходимо отметить, что критерий эффективности использования БВ определяется для нескольких режимов управления полетом.

Теперь переходим к выбору элементной базы для БВ. Предложенную методику выбора и проектирования БВ условно можно разбить на три этапа.

Этап I – предварительная обработка выбранного алгоритма на ЭВМ и получение оценочных временных характеристик выполнения программы на соответствующей элементной базе и ее оценки по выражениям (1):(14).

Этап II – выбор элементной базы для БВ, удовлетворяющей требованиям ТЗ. По предварительным оценкам (этап I) выбирает элементную базу с минимальными аппаратными затратами и уточняют время реализации алгоритма на выбранной элементной базе.

Этап III – проектирование БВ. Анализируется возможность использования более быстродействующих алгоритмов. Если такой существует, переходим к этапу I, иначе исходя из ТЗ и выбранного алгоритма, предлагается либо проектировать БВ, либо заказывать специализированную элементную базу, или за счет введения дополнительного оборудования часть функций алгоритма выполняемых программно, реализовывать аппаратно.

Рассмотрим более подробно каждый из этапов.

Этап I состоит из семи блоков, выполняемых последовательно (рис. 2).

После написания исходной программы на языке высокого уровня нумеруются операторы исходного модуля и в него включается отлаживающая программа “Шлях”, которая в процессе выполнения выдает на печать последовательность меток, имеющихся в анализируемой программе.

Поэтому предварительно нумеруются все операторы исходного модуля.

Анализируемая программа транслируется в объектный модуль и реализуется на ЭВМ. По завершении выполнения программы полученная информации отражает число обращений к тому или иному оператору исходного модуля.

Затем анализируется объектный модуль, т.е. определяется соответствие оператора исходного модуля, написанного на языке высокого уровня, оператору

или ряду операторов объектного модуля, реализованным на языке АССЕМБЛЕР. Так как частота обращений к соответствующим операторам исходного модуля в процессе его выполнения известна из программы “Шлях”, то легко рассчитать число соответствующих коротких операций, имеющихся в программе

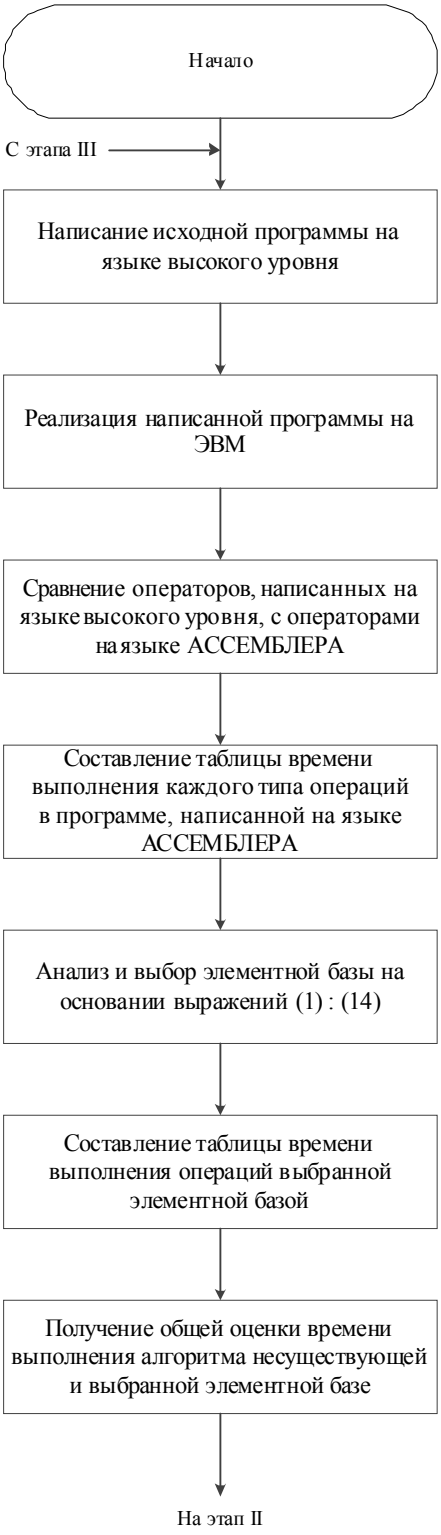


Рис. 2. Алгоритм процедуры выполнения этапа I

Все операторы АССЕМБЛЕРА объединены по типу операций в девять групп и представлены в виде таблицы. Аналогично составляется таблица, содержащая времена выполнения каждого типа операций на различных типах элементной базы, которая выбрана и проанализирована на основании выражений (1):(14). Перемножив соответствующие графы таблицы, а затем просуммировав результаты по каждому набору элементов базы, получим общую оценку времени выполнения алгоритма на существующей элементной базе.

Таким образом, на этапе I методики получены статистические данные о времени выполнения алгоритма при различных исходных данных и найдена максимальная оценка времени, исходя из быстродействия и реализуемого алгоритма.

Временные оценки, полученные на этапе I, не совсем точны, поскольку исходные программы пишутся не в системе команд, используемой элементной базы, а на языке высокого уровня, и объектный код, который анализируется на данном этапе, получен через транслятор, вносящий основную погрешность и избыточность. Поэтому для различных алгоритмов оценки, рассчитанные на этапе I, носят сравнительный характер и бывают в два ряда больше или меньше истинных, рассчитанных при программировании в системе команд элементной базы.

Для определения точных оценок по временным и аппаратным затратам переходим к этапу II, который реализуется следующим образом:

1. По рассчитанным на этапе I оценкам и показателям из всего множества элементной базы M составляется подмножества $G \in M$, удовлетворяющее по быстродействию требования ТЗ T_3.

2. Подмножества G частично упорядывается по критерию минимальных аппаратурных затрат $<G,\leq>$ [9] и из него выбирается первый элемент $R_i \in G$.

3. Для найденной элементной базы в системе его команд разработчик составляет программу и оценивает ее по быстродействию. Если полученная оценка удовлетворяет требованиям ТЗ, то переходим к проектированию БВ, реализованного на основе выбранной элементной базе, и к уточненной проверке аппаратных затрат (этап III, п. 2), иначе из подмножества G удаляется элемент

$$G \frac{\infty}{1} / Ri .$$

4. Если $G \neq \varnothing$, из него выбирается следующий элемент R_{i+1} и процедура повторяется, начиная с п. 3, иначе осуществляется переход к этапу III.

Этап III методики практически мало отличается от известных методик [3; 4; 5; 6; 9]. Он выполняется с самого начала лишь в том случае, если ни один из

предложенных наборов элементной базы не удовлетворяет по быстродействию ТЗ. Следовательно, необходимо проверить и проанализировать возможность использования других более быстродействующих алгоритмов. Если такие алгоритмы существуют, необходимо повторить все расчеты сначала, т.е. перейти к этапу I, иначе либо разрабатывается БВ при возможности распараллеливания алгоритма, либо используются дополнительные аппаратные затраты, позволяющие некоторые функции, выполняемые программно, реализовать аппаратно.

Затем сравнивают аппаратные затраты, полученные при проектировании с указанными в ТЗ. Если аппаратурные затраты не удовлетворяют ТЗ, то рекомендуется разрабывать заказную специализированную элементную базу, обеспечивающую заданное быстродействие и аппаратурные затраты. Если аппаратурные затраты не превышают объема и весо-габаритных характеристик аппаратуры, заданных в ТЗ на БВ, процесс выбора элементной базы и проектирования БВ заканчивается.

Выводы

Предположенная методика выбора элементной базы для БВ беспилотного летательного аппарата и проектирование его позволяет анализировать программу на языке высокого уровня и носит универсальный характер, что упрощает процедуру выбора элементной базы, так как нет необходимости учитывать системы команд всех наборов элементов базы, и как в следствие уменьшается время проектирования БВ. Методика предусматривает возможность анализа всего алгоритма, а не выбранной его части, как в методе банчмарковских программ, обеспечивает высокую достоверность полученных результатов. В процессе работы и отладки алгоритма на ЭВМ параллельно с получением искомых оценок проверяется работоспособность предположенных алгоритмов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Алєксєєв С.В.* Безпілотні літальні засоби: історія та перспективи розвитку / С.В. Алєксєєв // Сучасна спеціальна техніка. – № 3 (38). – 2014. – С. 89–98.

2. *Хорошко В.А.* Система обработки видеоинформации поступающей с беспилотников / В.А. Хорошко, Ю.Е. Хохлачева // Сб. науч. трудов НАУ "Защита информации". – Вып. 22. – 2015. – С. 60–74.

3. *Кофоррон Дж.* Технические средства микропроцессорных систем. Практический курс / Дж. Кофоррон. – М. : Мир, 1983. – 190 с.

4. *Трояновский В.М.* Применение микропроцессоров и микроЭВМ / В.М. Трояновский. – М. : Высшая школа, Микропроцессоры. – Вып. 5. – 1998. – 160 с.

5. *Соботка З.* Микропроцессорные системы. Изд. 2-е / З. Соботка, Я. Стары. – М. : Энерноиздат, 1992. – 496 с.

6. Специализированные ЦВМ: Учебник для вузов / В.Б. Смолов, В.В. Барященков, В.Д. Байков и др. Под ред. В.Б. Смолова Изд. 3-е. – М. : Высшая школа, 2001. – 309 с.

7. *Креденцер Б.П.* Техническое обслуживание и надежность систем с временным резервированием / Б.П. Креденцер. – К. : Феникс, 2016. – 384 с.

8. Основи надійності інформаційних систем / С.М. Головань, О.В. Корнейко, О.С. Петров та ін. – Луганськ : Вид-во "Ноулідж", 2012. – 335 с.

9. МикроЭВМ / Пер. с англ. Под ред. А. Дирксона. Изд. 2-е. – М. : Энергоиздат, 2001. – 328 с.

Отримано 02.12.2016
Рецензент Рибальський О.В., д.т.н

УДК 004.056.5

А.С. Шевченко,
кандидат технічних наук

КОМПЛЕКСНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМИ КІБЕРНЕТИЧНОГО ЗАХИСТУ ЗБРОЙНИХ СИЛ УКРАЇНИ

У статті розглядаються питання аналізу побудови та захисту кіберпростору Збройних Сил України на основі комплексного застосування наявних систем захисту інформації та кібернетичної безпеки.

Ключові слова: *кіберпростір, рівні кіберпростору, кібернетичний захист, системи захисту інформації, міжмережні екрани, системи виявлення та запобігання вторгненням, DLP, SIEM, VPN, антивірусний захист, розмежування доступу, системи аналізу захищеності.*

В статье рассматриваются вопросы анализа построения и защиты киберпространства Вооруженных Сил Украины на основе комплексного применения существующих систем защиты информации и кибернетической безопасности.

Ключевые слова: *киберпространство, уровни киберпространства, кибернетическая защита, системы защиты информации, межсетевые экраны, системы обнаружения и предотвращения вторжений, DLP, SIEM, VPN, антивирусная защита, разграничение доступа, системы анализа защищенности.*

Paper deals with the analysis of the construction and protection of cyberspace of the Armed Forces of Ukraine on the basis of an integrated application of existing systems of information protection and cybersecurity are considered.

Keywords: *cyberspace, levels of cyberspace, cyberprotection, systems of information protection, firewalls, systems of dection and prevention of attacks, DLP, SIEM, antivirus protection, access isolation, systems of an analysis of protection.*

Вступ

Кібербезпека – найбільш актуальний напрям захисту інформації на фоні глобальної інформатизації сучасного суспільства, включаючи і збройні сили держави. На сьогодні розвиток інформаційних технологій значно розширив можливості військового управління та збільшив можливості противника в реалізації атак на критичні елементи інформаційної інфраструктури.

У період із 2014 та до нині, під час анексії Автономної республіки Крим та в ході бойових дій на Сході України з боку Російської Федерації здійснюються масовані кібернетичні атаки на елементи критичної інформаційної інфраструктури як держави, так і Збройних Сил України.

Під час бойових дій реалізуються концепції інформаційних та кібернетичних операцій, які направленні на особовий склад та систему управління ЗС України. Система управління ЗС спирається на інформаційно-телекомунікаційні системи (далі – ІТС) при передачі команд бойового управління та здійснення повсякденної життєдіяльності.

Реалізація атак у кібернетичному просторі ЗС України призводить до витоку інформації, несанкціонованого доступу та порушення керованості елементами ІТС, відмови в доступі до ресурсів та систем, дезінформації особового складу ЗС. Наявність вразливостей ІТС, систем захисту інформації та низька підготовленість особового складу ЗС призводить до суттєвих ризиків інформаційної безпеки, а успішна реалізація кібернетичних атак – до значних збитків. З огляду на це, актуальним та невідкладним є захист кіберпростору ЗС України.

Аналіз останніх досліджень та публікацій показав, що на сьогодні значно актуалізувались питання забезпечення захисту інформації та кібербезпеки. Основні напрями наукових досліджень направлені на розвиток методологічної бази, формування концептуальних підходів, правових засад та термінології в галузі кібернетичної безпеки [1–5].

Мета

Стан інформаційної та кібернетичної безпеки у ЗС України вимагає негайного впровадження систем захисту інформації та кібернетичної безпеки. На сьогодні відсутні системи, які б дозволяли забезпечити захист інформації та кібернетичну безпеку ЗС в цілому. Тому для побудови системи кібернетичного захисту пропонується використання комплексного підходу, який дозволить поєднати існуючі системи та механізми захисту інформації для більш ефективного захисту кіберпростору ЗС України.

Метою роботи є підвищення безпеки кіберпростору ЗС України за рахунок комплексного використання наявних систем захисту інформації та кібернетичної безпеки.

Постановка завдання

Завданням дослідження є аналіз структури стану безпеки кіберпростору ЗС України та розробка рекомендацій щодо комплексного застосування систем захисту інформації та кібернетичної безпеки для його захисту.

Обмеження. В роботі розглядаються питання реалізації захисту кібернетичного простору технічними засобами.

Викладення основного матеріалу дослідження

Кібернетичний простір – це електронне інформаційне середовище, утворене організованою сукупністю взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [6].

Захист кіберпростору повинен здійснюватися безперервно на землі, в повітрі, морі та космосі [7; 8]. Реалізація захисту має враховувати середовища розповсюдження інформаційних потоків, включаючи і електромагнітний спектр (ЕМС).

Заходи захисту кіберпростору ЗС України повинні реалізовуватись на організаційному, технічному та правовому рівнях.

Організаційні заходи захисту кіберпростору у ЗС передбачають розробку правил доступу та роботи особового складу в ІТС, порядку обробки інформації та навчання основам інформаційної та кібернетичної безпеки. Крім того, особовий склад ЗС повинен бути навчений основам протистояння розвідці противника в інформаційному просторі – соціальній інженерії.

Більш детально розглянемо питання захисту кіберпростору ЗС України технічними засобами (програмними, апаратно-програмними).

Технічні заходи захисту кіберпростору передбачають захист електронного середовища ІТС Збройних Сил України.

Ураховуючи особливості побудови ІТС та сучасних систем захисту інформації, можна виділити такі функціональні рівні кіберпростору (рис. 1):

рівень інформаційних систем (програмного забезпечення);

рівень кінцевого телекомунікаційного обладнання;

рівень мережного телекомунікаційного обладнання;

рівень транспортної телекомунікаційної мережі [8].

Під час управління військами зазначені функціональні рівні кіберпростору взаємодіють з рівнями, які об'єднують особовий склад та фізичне середовище (стаціонарні та польові об'єкти). Впровадження захисту кіберпростору не повинно обмежуватись стаціонарною компонентою. Реалізація захисту польових елементів зумовлюється їх критичністю внаслідок функціонування за межами контрольованої зони впритул до засобів технічної розвідки противника, розвідки ліній зв'язку.

Для забезпечення безпеки кіберпростору ЗС України необхідне впровадження комплексу систем та механізмів захисту ІТС на різних функціональних рівнях кіберпростору. До таких систем та механізмів належать:

системи розмежування доступу користувачі до елементів ІТС;
системи міжмережного екранування на основі фаерволів (*Firewall*);
системи та механізми криптографічного захисту інформації;
віртуальні приватні мережі *VPN*;
системи антивірусного захисту елементів ІТС;
системи виявлення та запобігання вторгненням (*IDS/IPS*);
механізми автентифікації, авторизації та аудиту (*AAA*);
системи попередження втрати даних (*DLP – data loss prevention*);
системи управління інформаційною безпекою та подіями (*SIEM*);
системи аналізу захищеності (САЗ) [9–11].

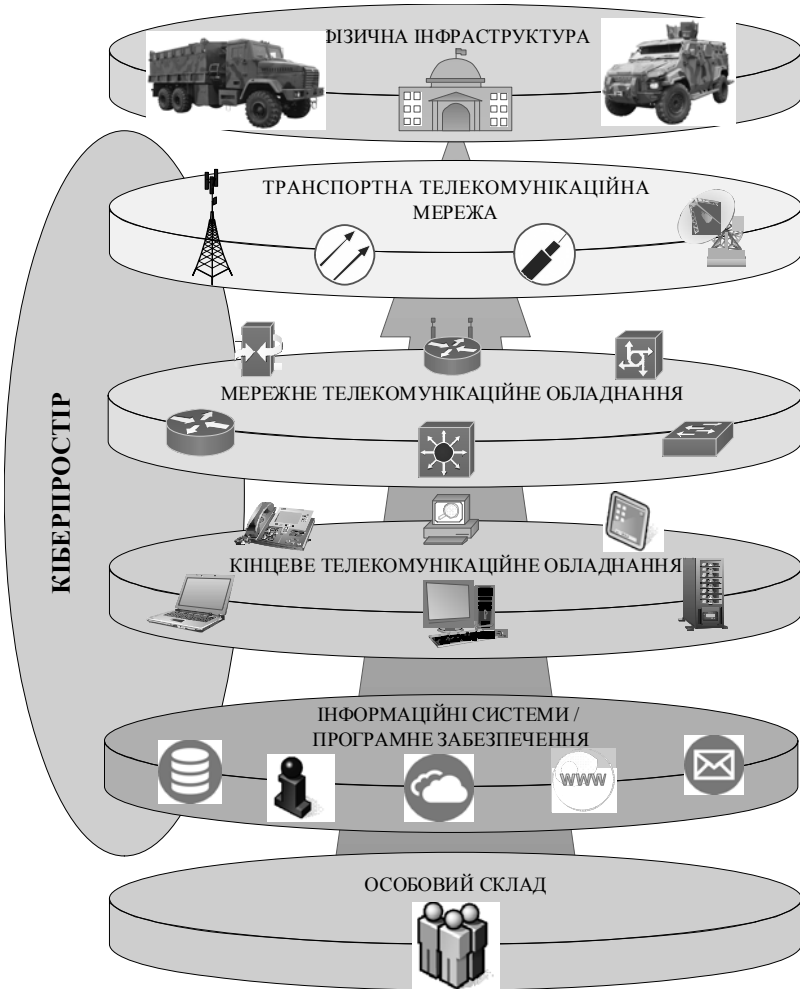


Рис. 1. Функціональні рівні кіберпростору Збройних Сил України

Представимо основні місця розташування програмних та апаратно-програмних засобів захисту інформації та кібернетичної безпеки відповідно до функціональних рівнів кіберпростору (рис. 1).

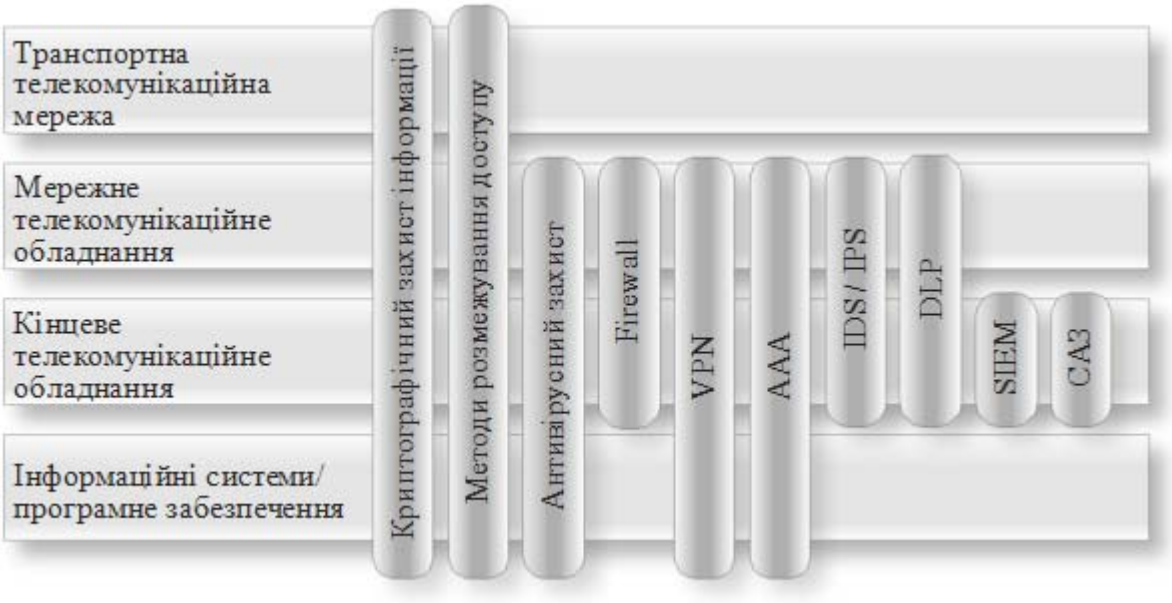


Рис. 2. Системи і механізми захисту інформації інформаційно-телекомунікаційних систем спеціального призначення

Розглянемо більш детально функціонування деяких систем та механізмів захисту інформації при захисті кібернетичного простору ЗС України.

Криптографічний захист інформації один з основних інструментів, що реалізує функції на кожному з функціональних рівнів кіберпростору, включаючи і реалізацію криптографічних функцій в інших системах захисту інформації: *VPN*, міжмережних екранах (механізм *deep packet inspection*), автентифікації тощо. Криптографічний захист інформації забезпечує конфіденційність та цілісність інформації.

Методи розмежування доступу використовуються для забезпечення розділення доступу суб'єктів чи груп суб'єктів до множини об'єктів ІТС. Як правило, розмежування доступу ґрунтується на впровадженні матриці доступу відповідно до існуючої політики безпеки. Розмежування доступу реалізується шляхом упровадження облікових записів користувачів різних рівнів згідно з повноваженнями та застосування політик безпеки (групових, локальних). Останні реалізуються, як правило, в операційних системах.

Методи розмежування доступу напряму не належать до механізмів захисту інформації, але значною мірою дозволяють забезпечити виконання політик безпеки інформації.

Розмежування доступу реалізовується на всіх функціональних рівнях кіберпростору.

Міжмережне екранування здійснюється за допомогою фаерволів (міжмережних екранів, анг. *Firewall*, нім. *Brandmauer*). Міжмережні екрани (МЕ) − комплекс апаратно-програмних чи програмних засобів, що здійснює контроль та фільтрацію інформаційних потоків відповідно до заданих правил політики безпеки.

На сьогодні міжмережні екрани реалізуються в таких виконаннях.

1. *Апаратно-програмні МЕ* реалізуються як окремі мережні пристрої. На цей час упроваджена концепція *Next Generation Firewall* (*NGFW*) − сучасні міжмережні екрани, крім функцій фільтрації трафіку, здійснюють антивірусний захист, створення каналів *VPN*, виявлення та захист від вторгнень та інші.

2. *Програмні МЕ* реалізуються у вигляді інтегрованого програмного забезпечення операційних систем, фаерволів, антивірусного програмного забезпечення, окремого спеціалізованого програмного забезпечення.

Сучасні міжмережні екрани (*NGFW*) дозволяються реалізувати фільтрацію трафіку за IP-адресами, портами відправника та отримувача, протоколами, здійснювати перевірку трафіку за вмістом (*App Control, Web Control, Email proxy*), блокування підозрілого трафіку (*Spam Blocker*, *APT Blocker*) та інші функції.

Для ефективного захисту інформації в ІТС Збройних Сил України доцільно використовувати МЕ для захисту мереж (критичних сегментів мережі − *DMZ*), критичних елементів ІТС та автоматизованих робочих місць. У першому та другому випадках використовуються апаратно-програмні МЕ, у третьому − програмні МЕ.

Віртуальні приватні мережі VPN використовуються для забезпечення захищеного обміну інформацією між мережами (*site-to-site*) та захищеного доступу віддалених користувачів. Суть *VPN* полягає в створенні криптографічно захищеного віртуального тунелю, що забезпечує конфіденційність та цілісність при обміні інформацією.

Як правило, використовуються схеми організації каналів *VPN*: мережа-мережа, клієнт-сервер. До основних протоколів віртуальних приватних мереж належать протоколи *IPsec, L2TP, PPTP, TLS* (*SSL*).

Серверні програмні модулі протоколів *VPN* реалізуються в серверних операційних системах, маршрутизаторах, *NGFW* та інших засобах.

Функції *VPN* інтегровані майже в усі сучасні маршрутизатори, що знижує затрати на організацію захищених каналів зв'язку.

Системи антивірусного захисту є невід'ємною складовою будь-якого елементу ІТС. Антивірусне програмне забезпечення, разом з існуючими методами (сигнатурним, евристичним, виявлення аномалій), впроваджує нові технології та механізми захисту − "пісочниця", емуляція, реалізація декількох антивірусних модулів тощо.

На сьогодні реалізовані основні підходи щодо антивірусного захисту: системи антивірусного захист шлюзів (*gateway antivirus*) та захист кінцевих точок (*end point security*). Для ефективного антивірусного захисту доцільне провадження обох підходів.

Аналогічно до інших програмних засобів існують як комерційні, так і умовно безкоштовні антивірусні засоби: ці засоби мають обмежені функціональні можливості.

Системи виявлення та запобігання вторгненням (*IDS/IPS*) − це програмно-апаратні чи програмні засоби, які призначені для виявлення фактів несанкціонованого доступу (НСД) до ІТС чи підозрілої активності. Системи виявлення вторгнення *IDS* дозволяють виявляти кібернетичні атаки, системи запобігання вторгненнями *IPS* реалізують функції захисту, що дозволяють блокувати НСД чи несанкціоновані дії.

Здебільшого виділяють три основні класи *IDS*: мережні (*Network-based IDS, NIDS*), вузлові (*Host-based IDS, HIDS*) та гібридні.

Архітектура *IDS/IPS* ґрунтується на використанні консольних та сенсорних систем. У системі кібернетичного захисту сенсори збирають інформацію про небезпечну активність та надсилають до консолей, які систематизують, журналюють та здійснюють управління.

На сьогодні існує ряд реалізацій *IDS/IPS* передовими розробниками засобів захисту інформації та програмних засобів з відкритим кодом: *Snot, OSSEC, Prelude, Bro* та інші.

Разом із ефективністю виявлення кібернетичних атак та своєчасної їх нейтралізації досить важливими є реалізація систематизації несанкціонованих дій та їх візуалізація, що дозволяє адекватно оцінювати стан кібернетичної безпеки.

Механізми автентифікації, авторизації та аудиту (*AAA – authentication, authorization, accounting*) – невід'ємні механізми захисту програмного забезпечення (*web*, баз даних тощо), операційних систем, інформаційних систем, систем захисту тощо.

Механізми автентифікації та авторизації забезпечують санкціонований доступ користувачів до систем (засобів) та надання повноважень відповідно до політики безпеки.

Механізми аудиту дозволяють на основі журналів (логів) здійснювати запис подій та інцидентів порушення інформаційної безпеки. Аудит дозволяє проводити розслідування інцидентів та виявлення порушників, які діють усупереч політиці інформаційної безпеки.

Механізми AAA тією чи іншою мірою реалізуються на усіх функціональних рівнях кіберпростору.

Системи попередження втрати даних (*DLP – Data Loss Prevention*) – системи, які досить інтенсивно розвиваються останнім часом. В ІТС Збройних Сил України існує велика кількість інформації, яка не належить до інформації з обмеженим доступом, але в сукупності розкриває певні відомості. Це – поштові адреси, телефонні номери, особисті ідентифікаційні номери, банківські реквізити установ, технологічна інформація тощо. Окремі з цих відомостей не становлять відносної цінності але в сукупності втрата зазначених масивів інформації є суттєвим ризиком інформаційної безпеки ЗС України.

Системи *DLP* на основі застосування криптографічних методів захисту, розмежування доступу дозволяють забезпечити збереження даних користувачів та організацій, блокувати доступ до несанкціонованих каналів. Деякі модулі *DLP* на *NGFW* забезпечують перевірку вмісту трафіку на наявність конфіденційних даних.

Сукупність розрізнених систем та механізмів захисту, незважаючи на свою функціональність, не відображає цілісної картини стану інформаційної безпеки організації.

Системи SIEM. Для реалізації моніторингу і аудиту подій інформаційної безпеки мережі в цілому використовуються системи *SIEM* (*Security Information and Event Management*). Ці системи включають у себе засоби автоматизованого збору подій, їх формалізації та узагальнення, відображення у зручному для аналізу вигляді. *SIEM* дозволяють проводити моніторинг та аудит стану інформаційної безпеки одночасно від багатьох робочих станцій, мережних пристроїв з різними платформами.

Системи аналізу захищеності (сканери безпеки) призначені для проведення аналізу та дослідження власних систем на наявність вразливостей. САЗ забезпечують аудит інформаційної безпеки мереж, операційних систем, систем управління базами даних та іншого спеціалізованого програмного забезпечення. Використання САЗ дозволяє вчасно виявляти вразливості ІТС, елементів ІТС та систем захисту інформації на основі пасивного або активного сканування. На сьогодні САЗ здебільшого інтегруються з SIEM. У комплексі ці системи дозволяють більш ефективно проводити аудит стану інформаційної безпеки та вчасно перекривати вразливості систем.

Впровадження наведених систем та механізмів захисту інформації дозволить забезпечити безпеку кіберпростору ЗС України. Системи захисту реалізують свої основні функції на рівні програмного забезпечення та мережного обладнання. Впровадження складних технологічних систем захисту інформації на кінцеві пристрої – здебільшого автоматизовані робочі місця, спричинить значні труднощі, що викличе необхідність у висококваліфікованих кадрах з кіберзахисту. У зв'язку з цим, основний напрям забезпечення безпеки кіберпростору ЗС України повинен бути направлений на впровадження мережних засобів захисту – шлюзів безпеки (*security gateway*). На сьогодні шлюзи безпеки становлять такі засоби захисту, як *NGFW*, *UTM* (*Unified Threat Management*) та *NFIPS* (*Next-Generation Intrusion Prevention System*). Кожен із цих засобів захисту включає тією чи іншою мірою набір систем, які розглядались у статті. Відповідно до досліджень NSS labs до основних лідерів у галузі кібернетичної безпеки належать: *Cisco, WatchGuard, Check Point, Dell SonicWall, Fortinet, McAfee* та інші [12].

Вибір засобів захисту для потреб ЗС України питання досить складне. Окрім впровадження функцій захисту, слід враховувати можливість централізованого моніторингу стану інформаційної безпеки та кібернетичних атак, так як, наприклад, реалізують засоби *WatchGuard Dimension* [13] або *Cisco FirePower* [14].

Забезпечення кібербезпеки Збройних Сил України – завдання яке потребує значних фінансових затрат, тому до його вирішення потрібно підійти комплексно, враховуючи досвід країн НАТО та США. Впровадження систем та механізмів захисту інформації дозволять забезпечити комплексний захист кіберпростору ЗС України з урахуванням стаціонарної та польової компоненти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Шаховал О.А.* Рекомендації щодо розробки стратегії забезпечення кібербезпеки України / О.А. Шаховал, І.Л. Лозова, С.О. Гнатюк // Захист інформації, – 2016. – Т. 18, № 1. – С. 57–65.

2. *Головка А.А.* Захист кіберпростору як складова інформаційної безпеки України в умовах гібридної війни / А.А. Головка // Young Scientist. – 2016. – № 4 (31). – С. 333–336.

3. *Титаренко О.М.* Стратегія захисту національного кіберпростору: досвід Франції / О.М. Титаренко // Новітні інформаційно-комунікаційні технології (30 березня – 30 квітня 2015 р.) : ІІІ наук.-практ. семінар : тези доп. – Дніпропетровськ : ДРІДУ НАДУ, 2015 [Електронний ресурс]. – Режим доступу: http://www.dridu.dp.ua/ konf/konf_dridu/itis%20seminar %202015/s1.html#sec3.

4. Развитие киберпространства и информационная безопасность / В.И. Хаханов, С.В. Чумаченко, Е.И. Литвинова, А.С. Мищенко // Радіоелектроніка, інформатика, управління. – 2013. – № 1. – С. 151–157.

5. *Шеломенцев В.П.* Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 2 (28). – С. 299–309.

6. Військовий стандарт 01.004.004. (Видання 1). Воєнна політика, безпека та стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення. – К. : Міністерство оборони України, 2014 р. – 22 с.

7. Стратегія кібербезпеки України [Електроний ресурс]. – Режим доступу : http:// zakon5.rada.gov.ua/laws/show/96/2016.

8. Cyberspace operations : Air Force Doctrine Document 3-12. – DOD US. – Government Printing Office, 2010. – 60 p.

9. *Шевченко А.С.* Забезпечення захисту кіберпростору ЗСУ / А.С. Шевченко // Телеком. Телекоммуникации и сети. Военная связь. Технологии, решения, проекты. – 2016. – Специальный выпуск. – С. 68–71.

10. *Поповский В.В.* Защита информации в телекоммуникационных системах : учебник : в 2-х т. / В.В. Поповский, А.В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 1. – 238 с.

11. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М. : ДМК Пресс, 2012. – 592 с.

12. NSS Labs Announces 2016 NGFW Group Test Results [Електроний ресурс]. – Режим доступу : https://www.nsslabs.com/company/news/press-releases/nss-labs-announces-2016-ngfw-group-test-results/.

13. WatchGuard Dimension. Oceans of data instantly become security intelligence [Електроний ресурс]. – Режим доступу : http://www.watchguard.com/wgrd-products/dimension.

14. *Лукацкий А.* Контроль и мониторинг периметра сети / А. Лукацкий [Електроний ресурс]. – Режим доступу : https:// www.cisco.com/ c/dam/ m/ru _ru/ events/ 2016/ cisco-security-roadshow/ pdf/ 4_ Firepower. pdf.

Отримано 28.11.2016
Рецензент Рибальський О.В., д.т.н

УДК 681.391

Н.Г. Юрх

ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

В статье рассматривается оценка защищенности речевой информации путем анализа эффективности зашумления речевого сигнала различными видами помех.

Ключевые слова: *разборчивость речи, речевой сигнал, акустический шум.*

У статті розглядається оцінка захищеності мовленнєвої інформації шляхом аналізу ефективності зашумлення мовного сигналу різними видами перешкод.

Ключові слова: *розбірливість мови, мовленнєвий сигнал, акустичний шум.*

In this paper the estimation of the security of speech information is examined by the analysis of efficiency of noise of speech signal by the different types of hindrances.

Key words: *legibility of speech, speech signal, acoustic noise.*

Защита речевой информации является одной из главных задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта информационной деятельности. Для перехвата информации злоумышленник может использовать все многообразие портативных средств акустической разведки.

В зависимости от важности речевой информации и поставленной задачи защиты предлагаются два критерия:

– в принятом (перехваченном) сообщении невозможно определить содержание информации и предмет повествования;

– в принятом сообщении невозможно определить присутствие информационных речевых сигналов.

Данные критерии предлагается ввести в связи с тем, что невозможно полностью исключить утечку информации. В любом случае вероятность утечки информации будет больше нуля, поэтому нужно определить допустимые границы.

Информативность речи характеризуется ее разборчивостью, под которой понимают относительное или процентное количество правильно принятых специально тренированными слушателями элементов речи из общего количества переданных по тракту. Соотношения между понятностью речи и соответствующими ей значениями разборчивости приведены в таблице 1.

Таблица 1

Разборчивость речи для разных градаций понятности передачи

Понятность	Разборчивость, %	
	слоговая, S	словесная, W
предельно допустимая	25–40	75–87
удовлетворительная	40–56	87–93
хорошая	56–80	93–98
отличная	80 и выше	98 и выше

Понятность речи была определена для обычных абонентов в процессе ведения телефонных переговоров. При этом понятность считалась отличной, если переговоры велись без переспросов; хорошей, если были отдельные переспросы редко встречающихся слов или неизвестных фамилий, названий и т.д., о которых нельзя догадаться по смыслу; удовлетворительной, если требовались частые неоднократные переспросы одного и того же материала в передаче отдельных слов по буквам и с полным напряжением слуха. В этой связи в [1] предложено в качестве предельных значений разборчивости слогов и слов принять соответственно S = 25 % и W = 75 %. Но там же [1] рассматривается количественная оценка достоверности сообщений по схеме Кента, в соответствии с которой диапазон возможных изменений достоверности разбивается на 7 интервалов и достоверность конкретной информации оценивается в шансах:

– достоверная информация (вероятность отсутствия ложной информации близка к 1);

– почти определенно, что информация достоверна (9 шансов против одного);

– имеется много шансов, что информация достоверна (3 шанса против одного);

– шансы примерно равны (1 за, 1 против);

– имеется много шансов что информация недостоверна (3 шанса против одного);

– почти определенно, что информация недостоверна (9 шансов против одного);

– недостоверная информация (вероятность ложной информации близка к 1).

Видимо, при оценке защищенности речевой информации следует ориентироваться на 3 последних шанса. Но если в качестве допустимой нормы принять разборчивость слов W = 75 %, то в соответствии с приведенной на рис. 1 зависимостью фразой разборчивости от разборчивости слов получим разборчивость фраз I = 93 %, т.е. отдадим противнику практически достоверную информацию (9 шансов против одного).

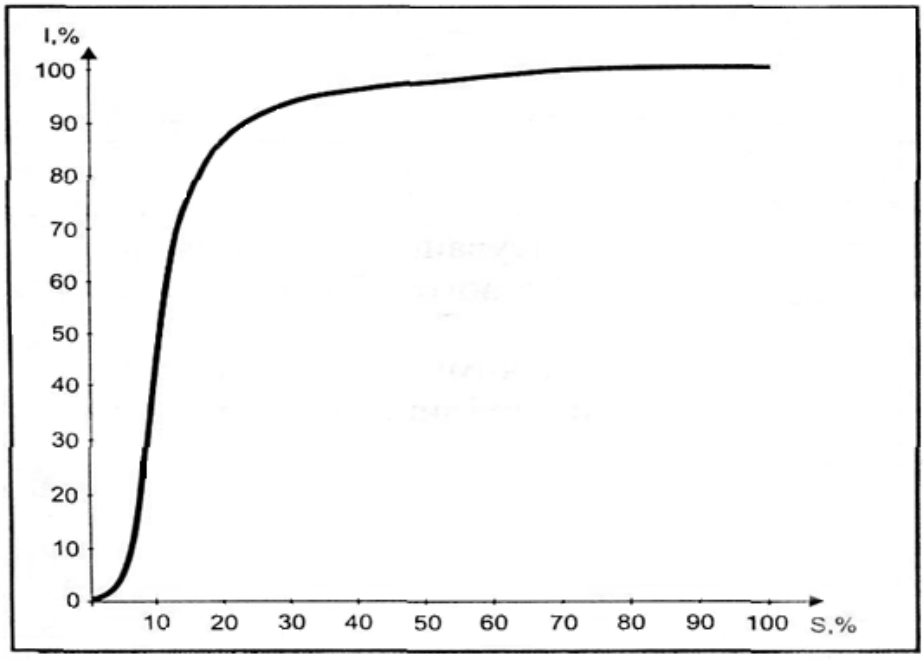


Рис. 1. Зависимость фразовой разборчивости от разборчивости слов

С учетом сказанного предлагается в качестве допустимой нормы для первого критерия (невозможно определить содержание информации и предмет повествования) принять разборчивость слов W = 30–40 %, что будет соответствовать разборчивости фраз I = 18–33 % и шестому интервалу схемы Кента (3 шанса против одного), а для второго критерия (отсутствие признаков речи) W = 15–20 %, что будет соответствовать седьмому интервалу схемы Кента (9 шансов против одного, что информация недостоверна).

В то же время известно, что если записанную речевую информацию с низкой разборчивостью представить тренированной бригаде артикулянтов, то после трехкратного прослушивания текстов и обмена мнениями после каждого прослушивания разборчивость повышается примерно вдвое. Поэтому можно принять в качестве нормируемых значений разборчивости слов W = 18 % для первого критерия и W = 8 % для второго критерия. В том случае, если нет возможности записать информацию в целях ее последующего прослушивания, то можно ориентироваться на приведенные ранее значения W = 30–40 % и I = 18–33%, выбрав для однозначности W = 36 %. На практике во многих случаях удобнее оперировать не разборчивостью речевой информации, а отношением напряжений сигнала к помехе (шуму). Воспользуемся зависимостью словесной разборчивости речи *W*.

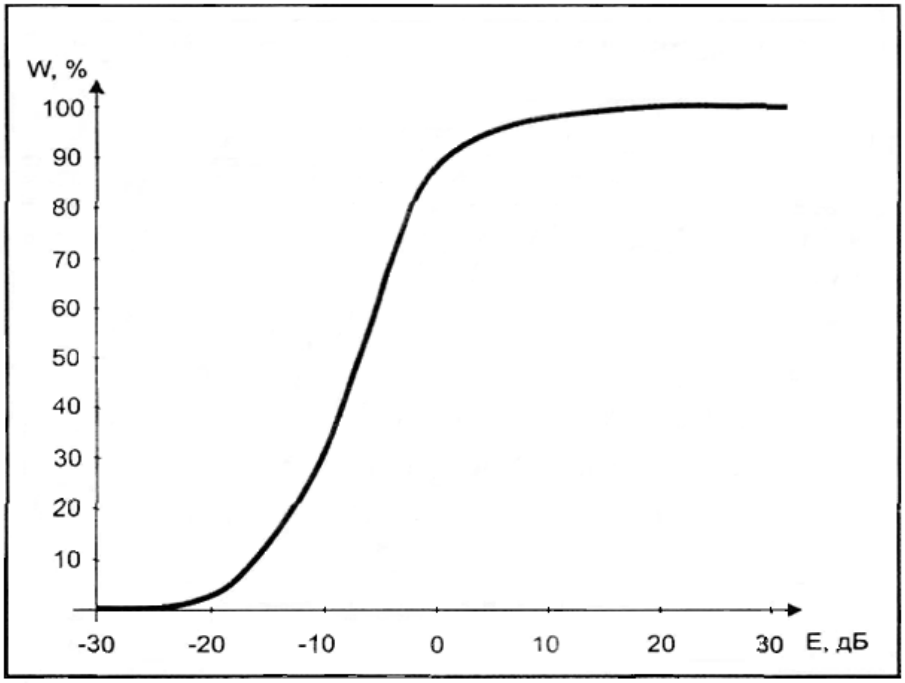


Рис. 2. Зависимость словесной разборчивости речи W от интегрального отношения сигнал/ ”белый” шум в полосе частот 175-5600 Гц от интегрального отношения сигнал/ шум E в полосе частот 175-5600 Гц

Из рис. 2 находим, что значению W = 18 % соответствует E = -11 дБ, значению W = 8 % соответствует E = -14 дБ. Результаты приведены в таблице 2.

Таблица 2

Параметры защищенности речевой информации

Критерий	Разборчивость слов, W%	Отношение речевой сигнал/“белый” шум, E, дб
Отсутствие смысловой информации (предмета повествования)	18	-11
Отсутствие признаков речи	8	-14

Графиками зависимости разборчивости речи от отношения сигнал/шум можно пользоваться только для случая неискаженной речи. Если ограничивать полосу частот или пропускать речевой сигнал через тракт с неравномерной амплитудно-частотной характеристикой, то зависимостью $W = f(E)$ пользоваться нельзя.

Оценку акустической и вибрационной защищенности речевой информации предлагается производить в пяти октавных полосах со среднегеометрическими частотами 250 Гц, 500 Гц, 1000 Гц, 2000 Гц, 4000 Гц, что вполне допустимо, поскольку спектр акустических помех в помещениях и на улице не имеет резких выбросов и равномерно спадает с ростом частоты. Звукоизоляция ограждающих конструкций помещений и зданий (двери, окна, стены, межэтажные перекрытия) обычно монотонно растет с увеличением частоты или остается практически неизменной в диапазоне речевых частот в отличие от неравномерных электроакустических характеристик вспомогательных технических средств и систем, эксплуатируемых в защищаемых помещениях, для которых оценку защищенности в пяти октавных полосах вряд ли можно использовать.

Измерение и последующий расчет акустической защищенности проводят в следующей последовательности.

1. Выставляют требуемый уровень акустического сигнала L_{si} перед ограждающей конструкцией для каждой i-й октавной полосы.

2. Измеряют уровни акустических сигналов L_{ci} и акустических помех $L_{ші}$, в месте возможного размещения аппаратуры речевой разведки (в точке контроля).

3. Рассчитывают отношения, “уровень речевого сигнала/уровень шума” $E_i = L_{ci} - L_{ші}$, дБ.

4. По полученным значениям E_i находят разборчивость слов W, которую сравнивают с допустимой, на основании чего делают вывод о защищенности информации по данному каналу.

Такой же алгоритм предлагается для оценки вибрационной защищенности речевой информации. Однако в [2] предлагается уровень скрываемого сигнала L_{ci} определить по формуле

$$L_{ci} = L_{si} - Q_i + M_{ap} + G_i.$$

где L_{si} – средний спектральный уровень речевого сигнала в месте установки источника тестовых акустических сигналов в i-й октавной полосе, дБ; Q_i – коэффициент ослабления уровня речевого сигнала в i-й октавной полосе при его распространении в тракте “источник речи – приемник аппаратуры речевой разведки”, дБ:

$$Q_i = L_{si} - L_{ci}$$

правда, вводить без необходимости излишнее значение Q_i не имеет смысла;

$$M_{ap}=10lg(N_p/N_k),$$

где N_p – чувствительность микрофона аппаратуры акустической разведки, мВ/Па;

N_k – чувствительность микрофона аппаратуры контроля, мВ/Па.

Введение в форму коэффициента M_{ap} ошибочно, поскольку уровень скрываемого речевого сигнала L_{ci} на входе аппаратуры разведки в точке возможного ее размещения не зависит от чувствительности микрофона, а определяется только уровнем исходного сигнала и его затуханием при распространении до места установки микрофона. Имело смысл учитывать собственные шумы аппаратуры разведки и контроля, если бы они превышали или хотя бы были соизмеримы с акустическими шумами, но акустические шумы в помещениях и, тем более, уличные шумы существенно превышают шумы аппаратуры контроля.

G_i – коэффициент пространственной селекции микрофона аппаратуры акустической разведки в i-й октавной полосе, дБ. Введение данного коэффициента в формулу также ошибочно, поскольку величина сигнала в месте размещения аппаратуры разведки не зависит ни от чувствительности, ни от селективности микрофона. Если и учитывать коэффициент пространственной селекции, то только при оценке акустических помех, т.е. не увеличивать уровень сигнала, а уменьшить уровень помех, что физически объяснимо. При этом следует учитывать, что если сигнал и помеха воздействуют на микрофон с одного направления, то применение направленных микрофонов не дает выигрыша в соотношении сигнал/помеха.

Поэтому в общем случае следует определить отношение речевой сигнал/шум E_i, в контрольной точке при заданном значении исходного речевого сигнала и по полученному отношению определить разборчивость слов W.

При проектировании и реконструкции объектов в качестве нормы требуется задавать для проектировщиков звукоизоляцию ограждающих конструкций, определяемую как $Q_i = L_{si} - L_{ci}$.

Для речи со средним уровнем громкости на расстоянии 1 м от источника можно принять интегральный уровень L_s = 70 дБ, а для очень громкой речи, усиленной техническими устройствами, L_s = 84 дБ [2].

Соответствующие этим уровням значения речи в октавных полосах приведены в таблице 3. Допустимый уровень акустического речевого сигнала в месте возможного размещения аппаратуры противника определяется по формуле

$$L_{ci} = L_{ши} + E_i.$$

Таблица 3

Уровни речевого сигнала в октавных полосах

Номер полосы речевого сигнала	Средняя частота октавной полосы, Гц	Уровни речи в октавных полосах L_s, дБ	
		L_s=70 дБ	L_s=84 дБ
1.	250	66	80
2.	500	66	80
3.	1000	61	75
4.	2000	56	70
5.	3000	53	67

Чтобы получить значения E_i для W = 18 %, W = 36 % и не проводить сложных расчетов, воспользуемся значениями E_i, для ближайших значений W = 20 % и W = 40 %, для розового шума. Спектр реальных акустических помех равномерно уменьшается с ростом частоты по закону, близкому для розового шума (таблица 4). При выборе уровней акустических шумов для нормирования внутри зданий проанализированы результаты около сотни измерений и выбраны уровни шума, вероятность появления ниже которых не превышает 0,3.

Статистика по измерению шумов на улице существенно уступает количеству измерений внутри зданий (были проведены около 30 измерений).

Таблица 4

Значения сигнала/розовый шум

Словесная разборчивость, W, %	Отношение с/ш E_i в октавных полосах					Отношение с/ш в полосе частот 180–5600 Гц
	250	500	1000	2000	4000	
20	-5,9	-5,9	-11,4	-15,9	-19,4	-8,8
40	-1,9	-1,9	-7,4	-11,9	-15,4	-4,9

Значения звукоизоляции, определяемые из выражения

$Q_i = L_{si} - L_{ci} = L_{si} - L_{ши} - E_i$ и округленные до целого числа, приведены в таблице 5.

Примерно похожие требования по звукоизоляции приведены в материалах по защите конфиденциальной информации, правда, в них приводятся нормированные значения коэффициентов звукоизоляции, независимы от частоты, в то время, как видно из таблицы 5, требования к звукоизоляции внутренних конструкций на частоте 4000 Гц по отношению к частоте 250 Гц выше более чем на 20 дБ.

Кроме того, обеспечивать неоправданно высокую звукоизоляцию на низких частотах довольно сложно, а заниженные значения звукоизоляции на высоких частотах могут привести к утечке информации. После возведения объекта и пуска его в эксплуатацию необходимо провести контрольные исследования акустической защищенности выделенных помещений объекта.

Таблица 5

Рекомендуемые значения звукоизоляции ограждающих конструкций

Конструкция	Звукоизоляция конструкций, Q_i, дБ				
	250	500	1000	2000	4000
Окна, наружные стены, выходящие на: тихую улицу;	28	32	39	44	49
шумную улицу.	16	20	27	32	37
Внутренние конструкции	33	36	43	48	53

В материалах по конфиденциальной информации вибрационную защищенность предлагается оценивать с помощью коэффициента виброизоляции, понимая под ним отношение вибросигнала на озвучиваемой конструкции к вибрационному сигналу на границе контролируемой зоны.

Реально вибрационный сигнал V_{c2} на границе контролируемой зоны определяется по формуле

$$V_{c2} = PxK_1/K_2,$$

где P – акустическое давление на конструкцию;
$K_1 = V_{c1}/P$ – коэффициент преобразования акустического давления P в вибрационный сигнал V_{c1};
$K_2=V_{c1}/V_{c2}$ – коэффициент виброизоляции конструкции в относительных единицах (дБ)

$$V_{c2} = P + K_1 - K_2.$$

Таким образом, значение V_{c2} при нормированном давлении P зависит от двух коэффициентов и поэтому ориентироваться только на один из коэффициентов нельзя, тем более численно приравнивать K_2 к коэффициенту звукоизоляции.

В качестве примера к сказанному рассмотрим экспериментальные результаты измерения вибрации на наружной стене здания, при которых акустическое воздействие осуществлялось на эту стену в кабинете на 3 этаже, измерение вибрации V_1 производилось на стене в этом же помещении, а затем на внутренней стороне стены на 2 этаже измерялась вибрация V_2.

Измерения проводились точным импульсным шумомером RFT 00017 с вибродатчиком КД 35. Акустическое воздействие осуществлялось шумовым сигналом в октавных полосах.

Результаты измерения вибрации приведены в таблице 6, а результаты расчетов в таблице 7.

Таблица 6

Результаты измерения вибрации на стене

Номер октавной полосы	L_T, дБ	ΔL, дБ	$V_{ш1}$, дБ	$V_{ш2}$, дБ	$V_{(с+ш)1}$, дБ	$V_{(с+ш)2}$, дБ
1.	83	17	14	15	14	15
2.	86	20	10	14	14	16
3.	92	31	5	9	26	25
4.	86	30	3	4	24	13
5.	88	35	2	2	32	14

Таблица 7

Результаты расчета показателей защищенности

Номер октавной полосы	V_{c1},дБ	V_{c2}, дБ	E_1, дБ	E_2, дБ	E_H, дБ	K_1, дБ	K_2, дБ
1.	-	-	-	-	-5,9	-	-
2.	12	12	-18	-22	-5,9	-74	0
3.	26	25	-10	-15	-11,4	-66	1
4.	24	12	-9	-22	-15,9	-62	12
5.	32	14	-5	-23	-19,4	-56	18

В таблицах введены обозначения:

L_T – уровень тестового акустического сигнала;

ΔL – превышение уровня тестового сигнала над нормированным для суммарного давления 70 дБ;

$V_{ш1}$, $V_{ш2}$ – уровни вибрационных шумов соответственно на стене в помещении и этажом ниже; $V_{(с+ш)1}$ $V_{(с+ш)2}$ – суммарные уровни сигнала и шума в измеряемых точках;

$V_{с1}$,$V_{с2}$ – уровни вибрации сигналов в измеряемых точках;

E_1, E_2 – отношение сигнал/шум в контрольных точках;

$E_н$ – нормированные отношения сигнал/шум для розового шума и разборчивости слов W = 0,2 (таблица 7).

Как видно из таблицы 7, коэффициент виброизоляции стены K_2 не превышает 20 дБ, а на частоте 500 Гц $К_2 = 0$, но за счет низкого преобразования K_1 акустического давления в вибрационный сигнал соотношение сигнал/шум в контрольной точке 2 на всех частотах меньше нормированного $E_н$.

Выводы

Защита речевой информации достигается совокупностью инженерных решений, проведением организационных и технических мероприятий.

В зависимости от характеристики объекта и предъявляемых требований к эффективности защиты речевой информации используют те или иные методы и средства, где в качестве показателя оценки используют словесную разборчивость речи W.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Покровский Н.Б.* Расчет и измерение разборчивости речи / Н.Б. Покровский. – М. : Связьиздат, 1962. – 390 с.

2. *Железняк В.К.* Некоторые методические подходы к оценке эффективности защиты речевой информации / В.К. Железняк, Ю.К. Макаров, А.А. Хореев // Специальная техника. – 2000. – № 4. – С. 12–16.

Отримано 27.10.2016

Рецензент Рибальський О.В., д.т.н

ОЗБРОЄННЯ ТА СПЕЦАВТОТРАНСПОРТ

УДК 687.157

В.П. Бакал,
кандидат юридичних наук,
М.Є. Александров,
здобувач ДНДІ МВС України,
В.А. Дмитрук,
здобувач ДНДІ МВС України

ІСТОРІЯ РОЗВИТКУ РОЗВАНТАЖУВАЛЬНИХ СИСТЕМ БОЙОВОГО СПОРЯДЖЕННЯ ВІЙСЬКОВОСЛУЖБОВЦІВ У XX ст.

У статті проаналізовано історію розвитку розвантажувальних систем бойового спорядження військовослужбовців у XX столітті. Вивчені їх типи, конструкція, особливості створення та основні напрями вдосконалення.

Ключові слова: *розвантажувальні системи, ремінно-плечові системи, розвантажувальні жилети, спорядження.*

В статье проанализирована история развития разгрузочных систем боевого снаряжения военнослужащих в XX веке. Изучены их типы, конструкция, особенности создания и основные пути усовершенствования.

Ключевые слова: *разгрузочные системы, ременно-плечевые системы, разгрузочные жилеты, снаряжение.*

Paper analyzes the history of the development of military load-carried equipment systems in the twentieth century. We study their types, design, features of the creation and the main ways of their improvement.

Keywords: *load-carried systems, load bearing equipment, load bearing vests, equipment.*

Для успішного виконання поставлених завдань під час бойових операцій бійцю будь-якої військової спеціальності необхідно нести на собі повний бойовий комплект та інші види екіпірування. Для раціонального розміщення предметів бойового екіпірування на тілі військовослужбовця застосовують розвантажувальні системи – вироби швейної або шкіряно-галантарейної промисловості, які дозволяють розміщувати спорядження на різних ділянках тіла та забезпечують зручність використання екіпірування в бою. Питання розробки та вдосконалення розвантажувальних систем є актуальним в умовах політичної нестабільності у світі та військових конфліктів, які на сьогодні ведуться в багатьох "гарячих точках" планети. З метою проектування нових типів розвантажувальних систем доцільно розглянути історію їх виникнення та вдосконалення, а також основні сучасні концепції розвитку.

Метою статті є розгляд розвитку конструкцій розвантажувальних систем бойового спорядження військовослужбовців у XX столітті.

До середини XX століття в більшості армій світу для перенесення боєзапасу до особистої зброї, шанцевого інструменту, індивідуального запасу питної води та продовольчих пайків використовувалися ремінно-плечові системи (РПС), що складалися з поясного ременя та плечових ременів-лямок з можливістю регулювання. Подібні системи активно використовувалися із середини XIX ст. та були актуальними напередодні Другої світової війни. Наприклад, у Робітничо-селянській червоній армії (РСЧА) у 1941 році для носіння спорядження бійців різних спеціальностей використовувалася система із поясного ременя та плечових лямок [1]. Подібні ж системи використовувалися в інших країнах під час Другої світової війни. Однак такі системи мали суттєвий недолік: більшість елементів спорядження розміщувалася на поясі, що створювало навантаження на поперек та обмежувало рухомість. Плечові лямки, завдяки невеликий ширині, тиснули на плечі, що спричиняло швидку втомлюваність бійців та натирання. Деякі елементи спорядження, наприклад, мала піхотна лопата, фляга, гранатна сумка та сумка для сухарів у стрільців РСЧА розміщувалась позаду (рис. 1), що створювало незручність при носінні та використанні цих елементів. До того ж інші елементи спорядження (наприклад, протигазна сумка або сержантський планшет) використовувалися окремо від системи, носилися через плече та в бойових умовах носилися під РПС. Разом із перекинутими через плече шинеллю та плащ-наметом у скатці, це створювало додаткові незручності при користуванні РПС.

Також варто зауважити, що тодішні ремінно-плечові системи передбачали наявність певних конструктивних елементів для використання елементів спорядження разом із цією системою. Наприклад, парні підсумки для гвинтівки в Червоній армії та потрійні підсумки для карабінів у Вермахті мали на зворотному боці кільця, до яких за допомогою металевих гачків кріпилися плечові лямки РПС.

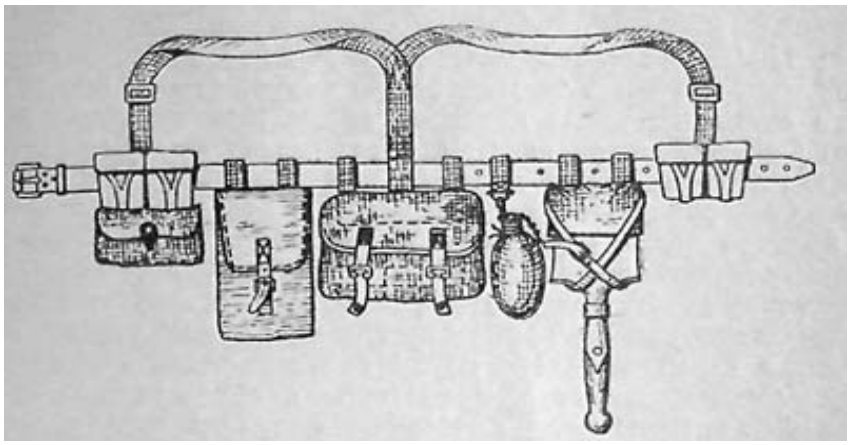


Рис. 1. Спорядження стрільця РСЧА, 1941 рік

Водночас у різних країнах почалися пошуки альтернативи ремінно-поясним системам. У 1942 році в парашутних частинах Італійської армії з'явилися жилети, на нагрудній та наспинній частині яких були розміщені кишені для магазинів під пістолет-кулемет BERETTA M1938A (рис. 2) [2]. Такий жилет мав ряд переваг

над ремінно-поясними системами. По-перше, навантаження рівномірно розподілялося по грудях та спині. По-друге, магазини пістолета-кулемета прикривали від куль життєво-важливі ділянки тіла (серце, грудну клітину, легені), що сприяло захисту військовослужбовця від поранень. По-третє, жилет можна було швидко перегорнути таким чином, щоб наспинні кишені опинилися на рівні грудей, тобто забезпечувався швидкий доступ до боєприпасів.

Рис 2. Італійський парашутист із жилетом з кишенями-підсумками для пістолета-кулемета BERETTA M1938A

У тому ж 1942 році розвантажувальна система, подібна до жилету, з'явилася у Великобританії. Полковник Ріверс-Макверсон на основі традиційного англійського шкіряного безрукавного жилета Jerkin створив розвантажувальний жилет Battle Jerkin [3]. Він виготовлявся з брезенту та мав великі нагрудні, бічні та задні накладні кишені (рис. 3). Перевагою цього жилета була велика ємність кишень, що дозволяла розміщувати боєприпаси до будь якого типу зброї, а також інше спеціальне спорядження. Наприклад, у нагрудних кишенях могли розміщуватися із однаковою зручністю магазини до пістолета-кулемета STEN або до кулемета BREN, тож Battle Jerkin міг вільно використовуватися як автоматником, так і кулеметником.

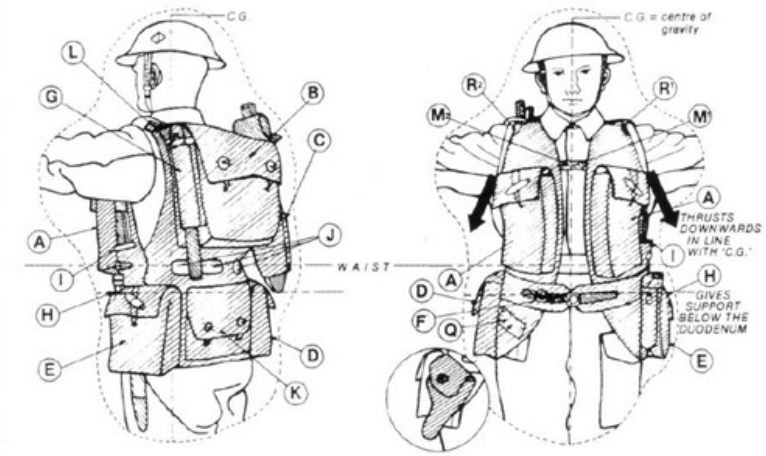
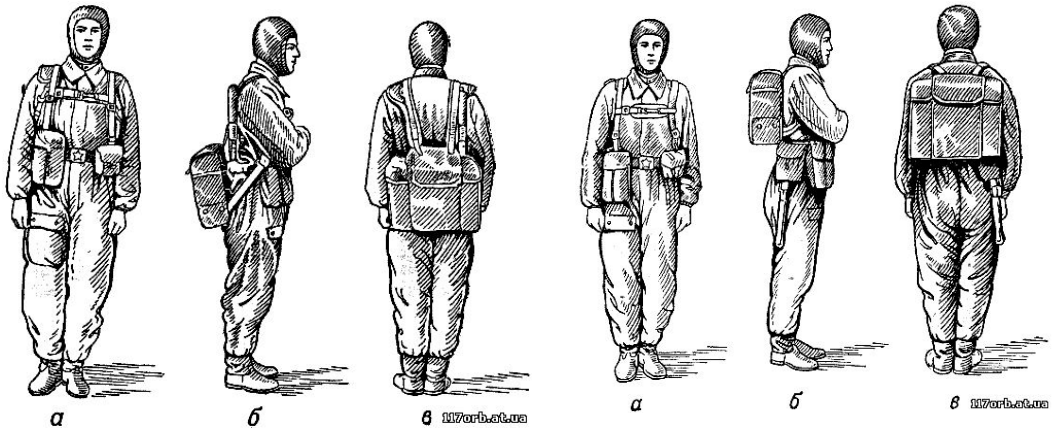


Рис. 3. Розвантажувальний жилет Battle Jerkin, 1942 рік

Після завершення Другої світової війни розробники розвантажувальних систем зосередили свою увагу на пристосуванні спорядження військовослужбовця під нові зразки стрілецької зброї. Варто зазначити, що в більшості армій усе ж залишалися ремінно-плечові системи старої конструкції, натомість нові, прогресивні розвантажувальні системи розроблялися переважно для сил спеціальних операцій. Як приклад, можна навести рюкзак десантника РД-54, створений у СРСР для повітряно-десантних військ. Це була розвантажувальна система, що складалася з ранця з великим переднім відділенням та двома об'ємними бічними кишенями, а також плечових ременів, до яких кріпилися підсумки для магазинів автомата АК-47, гранатна сумка та чохол для лопати. Плечові ремені разом із підсумками комбінувалися із поясним ременем [4]. Рюкзак створювався спеціально для парашутистів, тому система плечових ременів РД-54 дозволяла регулювати його положення на тілі військовослужбовця: під час стрибка з парашутом рюкзак на спині переміщувався на лінію стегон, а в бойовому положенні підіймався на спину (рис. 4).



а б

Рис. 4. Рюкзак РД-54: а) – в положенні для стрибка; б) – в бойовому положенні

Поява на озброєнні автоматів (штурмових гвинтівок) у другій половині 50-х років XX ст. змусила шукати оптимальне місце для розташування магазинів для цього типу зброї на спорядженні, адже довгий магазин (як правило, ємність магазинів – 20–30 патронів) на поясі знижував рухомість військовослужбовця та створював незручності при пересуванні повзком.

У кінці 50-х років у Китайській Народній Республиці, де на той час було налагоджено випуск автоматів "Тип-56" та самозарядних карабінів "Тип-56" – копій радянських АК-47 та СКС відповідно, були створені розвантажувальні системи "Тип-56" та "Тип-63" [5]. Вони складалися з плечових та бічних ременів та нагрудної деталі, до якої нашивалися кишені-підсумки для магазинів автомата або карабіну. "Тип 63" також містив по дві кишені для гранат. Магазини розміщувалися на рівні грудей та не ускладнювали рухів. Ці розвантажувальні системи стали широко відомими під час війни у Вьєтнамі 1965 – 1973 рр., коли "Тип-56" та "Тип-63" разом із автоматами широко поставлялися Китаєм армії Північного В'єтнаму та Національного фронту визволення Південного В'єтнаму (рис. 5).

Рис. 5. Бійці Національного фронту визволення Південного В'єтнаму із розвантажувальними системами "Тип-56" (по центру) та "Тип-63" (справа)

На відміну від своїх супротивників, армія США продовжувала використовувати як спорядження ремінно-плечові системи. Під час війни у В'єтнамі американцями широко застосовувалася система MLCE (Modernized Load-Carrying Equipment). У цій системі широко використовувалися синтетичні матеріали замість брезенту, плечові ремені були розширені для зменшення тиску на плечі під вагою спорядження, рюкзак зміщено до попереку для створення оптимального балансу системи. Система MLCE також використовувалась в армії Ізраїля (Цахал), бійці якої використовували елементи цієї РПС для створення жилетів. Підсумки нашивалися на бронежилети М1952 та М-69, утворюючи таким чином системи індивідуального бронезахисту з елементами розміщення спорядження (рис. 6). Створення подібних систем в ізраїльській армії було також результатом зміни характеру бойових дій: від ведення повномасштабних бойових дій Шестиденної війни у 70-х роках Цахал перейшов до контрпартизанських акцій та боїв у місті. Бойова обстановка в цих умовах диктувала необхідність у більш зручному, ніж РПС розвантажувальному жилеті [6].

Рис. 6. Бійці ізраїльської армії у бронежилетах з елементами спорядження розвантажувальних систем

У Радянському союзі при польовій формі одягу тривалий час використовувалася ремінно-плечова система зі стандартним набором підсумків, фляги та малої піхотної лопати. Непрактичність цієї системи була виявлена в ході бойових дій в Афганістані (1979–1989). У перший же рік перебування Обмеженого контингенту виявилося, що для бойових дій у гірській місцевості в умовах антипартизанської боротьби необхідні більш зручні системи спорядження. Афганські моджахеди мали на оснащені китайські розвантажувальні жилети "Тип-56" та ремінно-плечові системи парних підсумків. Відповідно, трофеями користувалися й радянські військовослужбовці. Промисловість СРСР не налагоджувала виробництво вітчизняних розвантажувальних систем аж до 1987 року, тож бійці в Афганістані виготовляли розвантажувальні жилети та системи в речових ремонтних майстернях частин (рис. 7). Наприклад, на жилет, пошитий із плащ-наметів, нашивалися штатні підсумки або кишені від рюкзака РД-54 [7]. Перевагою створення саморобних жилетів була можливість виготовити комплект під конкретну військову спеціальність (кулеметник, снайпер тощо), тоді як трофейні китайські розвантажувальні системи вміщали тільки магазини для автоматів Калашнікова різних модифікацій.

а б

Рис. 7. Саморобні розвантажувальні системи часів війни в Афганістані 1979–1989 рр.: а) з підсумків рюкзака РД-54; б) зі штатних підсумків автоматів АК/АКМ

У 1987 році радянська промисловість налагодила випуск вітчизняних розвантажувальних систем. Першим був "Пояс-А", котрий, як і його китайських аналог, містив три кишені для магазинів АК та чотири сумки для гранат. "Пояс-А" створювався з урахуванням побажань та бойового досвіду радянських бійців. Так, між кишенями для магазинів нашивалися еластичні тасьми для розміщення між ними реактивних освітлювальних патронів та інших пристроїв. Кишені для гранат розмістили одна над одною, що полегшувало доступ до них. У зв'язку із появою підствольних гранатометів до "Поясу-А" було виготовлено доповнення "Пояс-Б", який містив 10 пострілів ВОГ-25 та кріпився до "Поясу-А" за допомогою лямок. У 1988 році на оснащення повітряно-десантних військ стала надходити "бойова викладка десантника" (БВД), це був жилет з кишенями для магазинів

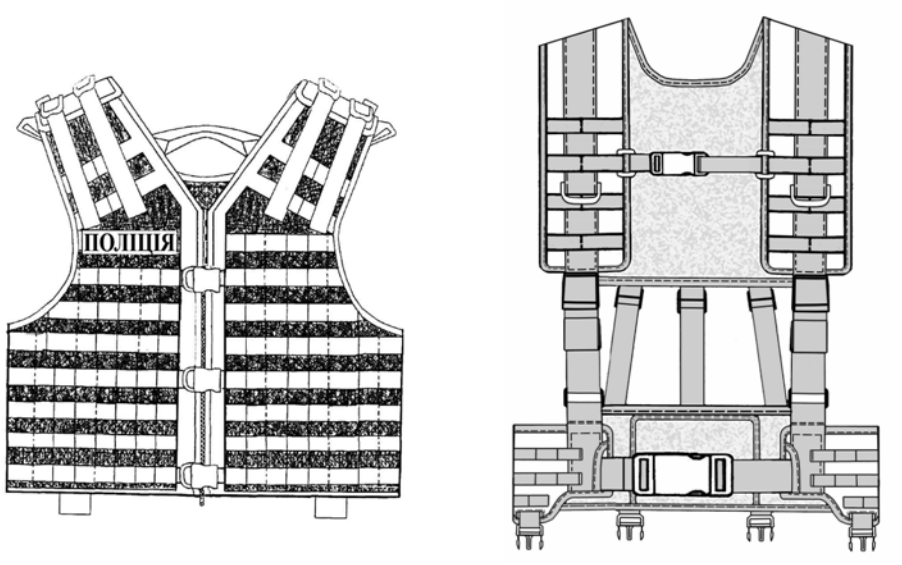
АК, гранат та іншого спорядження на нагрудній та наспинній частинах (рис. 8). Обидві системи широко використовувались на заключному етапі війни в Афганістані (1988–89 рр.), під чса бойових дій у "гарячих точках" СРСР та війни в Чеченській Республиці (1994–1996) [8].

а б

Рис. 8 Радянські розвантажувальні системи: а) "Пояс А" та "Пояс Б"; б) бойова викладка десантника (БВД)

Майже для всіх розвантажувальних систем характерним недоліком було використання підсумків під конкретний тип стрілецької зброї, що робило незручним використання таких систем різними спеціальностями військовослужбовців. Створення ж розвантажувальних систем під окремі види зброї було б трудомістким та недоцільним. Саме тому на початку 90-х років у США була створена система Pouch Attachment Ladder System(PALS) – модульна система кріплення спорядження, яка дозволяла кріпити різне спорядження відповідно до спеціальності військовослужбовця. Для використання разом з PALS був прийнятий на озброєння США та країн НАТО комплект MOLLE (Modular Lightweight Load-carrying equipment) – комплект спорядження, що оздоблений системою PALS. Для кріплення елементів MOLLE використовуються спеціальні застібки-кліпси, що дозволяють регулювати висоту розміщення та ступінь вільності спорядження на PALS [9]. Елементи системи MOLLE можуть застосовуватися як у розвантажувальних жилетах, так і в ремінно-плечових системах.

Система MOLLE визначила концепцію розроблення розвантажувальних систем по всьому світу. Відповідно до цієї концепції здійснюється розробка розвантажувальних систем і в Україні. Постановою Кабінету Міністрів України від 30 вересня 2015 року № 823 "Про обмеження поліцейських" затверджені описи та зразки розвантажувального жилета та розвантажувальної поясної системи з підсумками, що за конструкцією є ремінно-плечовою системою [10]. І жилет, і розвантажувальна поясна система мають платформи системи MOLLE для кріплення підсумків та іншого спорядження (рис. 9).



а б

Рис. 9 Розвантажувальні системи Національної поліції України:
а) розвантажувальний жилет; б) розвантажувальна поясна система

Іншою складовою вдосконалення розвантажувальних систем на сучасному етапі є використання їх у комбінації із системами індивідуального бронезахисту. Наприклад, розвантажувальний жилет для аеромобільних військ Великобританії AERO Assault Plate Carrier, конструктивною особливістю якого є можливість застосування підсумків типу "Кенгуру", в яких можна розміщувати магазини для різних видів стрілецького озброєння, а також засоби зв'язку (рис. 10). AERO Assault Plate Carrier дає змогу застосовувати всі види бронеплит, які широко використовуються в країнах НАТО. Крім того, жилет обладнаний системою швидкого скидання [11].

Рис. 10. Розвантажувальний жилет AERO Assault Plate Carrier із можливістю застосування елементів бронезахисту

Отже, розглянувши історію розвитку розвантажувальних систем, можна зробити такі висновки:

– основними видами розвантажувальних систем є ремінно-плечові системи та розвантажувальні жилети;

– розвиток розвантажувальних систем невід'ємно пов'язаний із удосконаленням стрілецької зброї, а також із характером бойових дій;

– на сучасному етапі розширюється асортимент розвантажувальних систем та спорядження до них за рахунок використання універсальних систем кріплення;

– для підвищення захисту військовослужбовців відбувається комбінація різних типів розвантажувальних систем із засобами індивідуального бронезахисту.

Вивчення історії та концепцій розвитку розвантажувальних систем сьогодні дозволяють розробити нові сучасні системи для структурних підрозділів Національної поліції України та Національної гвардії України, які виконують спеціальні завдання, у тому числі в умовах війни. Використання розвантажувальних жилетів та ремінно-плечових систем із універсальними системами кріплення розширює тактичні можливості окремого бійця та підрозділу в цілому, дозволяє розміщувати на розвантажувальних системах елементи спорядження до найсучаснішої вітчизняної та іноземної стрілецької зброї. В умовах Антитерористичної операції на Сході України під час бойових дій розвантажувальні системи, розроблені із урахуванням світового досвіду, дозволяють правильно розподіляти навантаження елементів спорядження на тіло військовослужбовця, підвищуючи боєздатність бійців. Використання сучасних розвантажувальних жилетів із можливістю розміщення елементів індивідуального бронезахисту підвищує захищеність бійців, що дозволяє у критичній ситуації врятувати їх життя та здоров'я.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Инструкция по укладке, пригонке, сборке и надеванию походного снаряжения бойца пехоты Красной Армии Главное Интендантское Управление РККА Воениздат НКО СССР 1941г. – 45 с.

2. *Jowett P.* The Italian Army 1940-45 (3). Italy 1943-45. / P. Jowett. – Oxford: Osprey Publishing, 2001 – 48 p.

3. История снаряжения, Battle jerkin, Великобритания [Електронний ресурс]. – Режим доступу : http://sputnik-gear.livejournal.com/2586.html

4. РД-54. Рюкзак десантника [Електронний ресурс]. – Режим доступу : http://www.russianarms.ru/forum/index.php?topic=7481.0

5. Разгрузочные системы [Електронний ресурс]. – Режим доступу : http://russianguns.ru/forum/index.php?topic=168.0

6. Тактические разгрузочные системы армии Израиля [Електронний ресурс]. – Режим доступу : http://army-news.ru/2014/08/takticheskie-razgruzochnye-sistemy-armii-izrailya/

7. *Сухолесский А.В.* Спецназ ГРУ в Афганистане 1979 – 1989 / А.В. Сухолесский – Королев : – Издательство "Арктика 4Д", 2005 – 124 с.

8. Армейский "лифчик" – история советской разгрузки [Електронний ресурс]. – Режим доступу : http://www.gunscity.ru/323-armejjskijj-lifchik-istorija-sovetskojj-razgruzki.html

9. Несущая платформа MOLLE (PALS) и её варианты [Електронний ресурс]. – Режим доступу : http://rus.1gb.ru/note/abmolle.htm

10. Про одностріл поліцейських : Постанова Кабінету Міністрів України від 30 вересня 2015 року № 823 [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/823-2015-%D0%BF

11. Aero Assault Basic Armor Carrier [Електронний ресурс]. – Режим доступу : http://www.eagleindustries.com/products/detail.aspx?id=3087

Отримано 22.11.2016

Рецензент Марченко О.С., к.т.н.

УДК 629.3.01

М.П. Будзинський,
здобувач ДНДІ МВС України,
О.В. Диких,
М.В.Кисіль,
В.І. Приходько

АСПЕКТИ СТВОРЕННЯ БРОНЬОВАНОГО ПАТРУЛЬНОГО КАТЕРА ДЛЯ СПЕЦІАЛЬНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

У статті розглянуто історію розвитку патрульних катерів, основні світові виробники сучасних броньованих патрульних катерів, можливість виготовлення броньованого патрульного катера на підприємствах України для потреб сил спеціального призначення Національної гвардії України, військово-морських сил, прикордонних підрозділів, сил реагування на надзвичайні ситуації.

Ідеться про технічні характеристики основних діючих патрульних катерів армій різних країн та налагодження виробництва цього виду продукції на підприємствах України.

Ключові слова: *патрульний катер, тактико-технічні характеристики, озброєння, протикульний бронезахист.*

В статье рассмотрена история развития патрульных катеров, основные мировые производители патрульных катеров, возможность изготовления бронированного патрульного катера на предприятиях Украины для нужд сил спецопераций Национальной гвардии Украины, военно-морских сил, пограничных подразделений, сил реагирования на чрезвычайные ситуации.

Речь идет о технических характеристиках основных действующих патрульных катеров армий разных стран и организацию производства данного вида продукции на предприятиях Украины.

Ключевые слова: *патрульный катер, тактико-технические характеристики, вооружение, противопульная бронезащита.*

Paper considers the history of the development of patrol boats, the world's main manufacturers of patrol boats, the possibility of manufacturing of armored patrol boat at the enterprises of Ukraine for the needs of special operations forces of the Ukrainian National Guard, Navy, border units, forces of the reaction of emergency.

Technical characteristics of the main existing patrol boats of the armies of different countries and the organization of production of this type of production on the enterprises of Ukraine are coinsidered.

Keywords: *patrol boat, performance characteristics, weapons, armor antibullet protection .*

Відновлена в березні 2014 року, Національна гвардія України стала високомобільним військовим формуванням, яке забезпечене сучасним озброєнням та висококваліфікованими кадрами. Гвардійці виконують бойові задачі в зоні проведення

антитерористичної операції, стоять на захисті життя, прав, свобод і законних інтересів громадян України, забезпечують державну безпеку і захист державного кордону, припиняють терористичну діяльність.

Бойові задачі, які спрямовані на захист конституційного ладу в Україні та збереження цілісності її території, вживання заходів щодо припинення діяльності незаконних воєнізованих або збройних формувань, терористичних організацій, організованих груп і злочинних організацій Національна гвардія зможе виконати тільки маючи на озброєнні новітню техніку та обладнання.

Для оснащення підрозділів Національної гвардії України новою сучасною технікою підприємства України освоюють випуск продукції військового призначення із застосуванням нових технічних розробок, матеріалів та технологій.

У статті наведений матеріал про виготовлення на підприємствах України броньованих патрульних катерів, які на сьогодні необхідні спеціальним підрозділам Національної гвардії, Прикордонної служби, Державної служби з надзвичайних ситуацій та Збройним Силам України, адже до недавнього часу у Військово-морських силах клас патрульних катерів був узагалі відсутній.

До класу патрульних катерів належать швидкохідні високоманеврові катери тоннажем 10–500 тонн, як правило, з динамічним принципом підтримки, що дозволяє розвинути швидкість 30–50 вузлів (1 міжнародний вузол = 1 морська миля/година = 1,852 км/год.) та які мають легке артилерійське або кулеметне озброєння та броньований захист [8].

За тоннажем катери розділяються на великі і малі, межею між якими є водотоннажність приблизно у 100 тонн. В окремий підклас малих патрульних катерів виділяються жорстконадувні гумові катери типу RIB (від англ. *Rigged Inflatable Boats*), легкі патрульні катери типу Mk5 “Пегас” і SOC-R (англ. *Special Operations Craft-Riverine*) та їх аналоги.

Ці катери призначені для роботи в прибережній зоні морів (до 20 миль), річках, при максимальному віддаленні від місця дислокації до 100 миль. Використовуються для патрулювання акваторій, оборони стратегічних об’єктів, забезпечення безпеки суден на незахищених рейдах, виявлення, перехоплення і затримання малих цілей, забезпечення дій підрозділів спеціального призначення зі швидкої доставки груп до 18 осіб зі зброєю, спорядженням та обладнанням, а також для проведення пошуково-рятувальних робіт.

Збройні конфлікти, як правило, стимулювали розвиток військової техніки. Тому і виробництво патрульних катерів розпочалося в період Першої світової війни. У Англії з 1915 року будували патрульні кораблі типу “P” тоннажем близько 600 тонн і швидкістю ходу 23 вузли. На озброєнні вони мали 102-мм і 40-мм гармати, глибинні бомби і торпедні апарати. У США в 1918 році було закладено серію патрульних катерів типу “Ігл” водотоннажністю 500 тонн і швидкістю ходу 18 вузлів. Вони мали на озброєнні 102-мм і 76-мм гармати та бомбомет. У російському флоті в 1917 році було закладено серію посильних суден чотирьох різних типів – “Кобчик”, “Голуб”, “Бекас” і “Філін” водотоннажністю від 350 до 530 тонн і швидкістю до 15 вузлів. Кораблі озброювалися гарматами калібром 75 або 102 мм, на деяких з них додатково встановлювали малокаліберні зенітні гармати. У жовтні 1917 року їх класифікували як новий клас – сторожові судна. Вони призначалися для охорони з’єднань кораблів і конвоїв від атак підводних човнів, торпедних катерів і несення дозорної служби.

Подальший розвиток патрульні катери отримали під час Другої світової війни – вони були наймасовішим типом суден, які випускалися в цей період. Частина американських патрульних катерів була передана СРСР за програмою ленд-лізу: усього було отримано 76 катерів типу SC-110 (за радянською класифікацією – великі мисливці типу БО-1 і БО-2) і 60 одиниць малих мисливців типу МО-1. Побудовані фірмою "Елко", патрульні катери типу SC-110 мали водотоннажність 126 тонн, 40-мм гармату "Бофорс", два 20-мм автомати "Ерлікон", два реактивні бомбомети "Хеджехонг" і два штокових бомбомети. При такому озброєнні корабель міг пройти 1800 миль на швидкості 20 вузлів.

Третім етапом розвитку патрульних катерів спочатку в ВМС США, а слід за ним і у флотах інших держав став період локальних конфліктів 1950-х-1960-х років. Ознакою цього етапу стало зменшення тоннажу і озброєння катерів та збільшення швидкохідності руху і маневреності [1].

На верфі United States Marine Inc будувалися катери спеціальних операцій Крафт – Riverine, призначені для бойових завдань малої дальності на річках і морському побережжі. Ці судна використовувалися в основному для проведення таємних бойових завдань, часто працюючи в нічний час, практично без підтримки з повітря. Катер SOC-R комплектувався чотирма членами екіпажу та міг перевозити ще вісім спецназівців ВМС США і 370 кілограмів вантажу. Має довжину 10 метрів, загальну масу 9400 кг, два двигуни по 440 к.с. забезпечували швидкість до 40 вузлів, запасу пального вистачало на 230 км. Озброєння залежно від комплектації складалось із двох кулеметів M240B калібру 7,62 мм., кулемету M2HB калібру 12,7 мм., при необхідності встановлювалися 2 гранатомети Mk 19 або ж 2 кулемети GAU-17 miniguns калібру 7,62 мм. Використовуються для несення дозорної (патрульної) служби в прибережній зоні, боротьби з торпедними, сторожовими і артилерійськими катерами противника, охорони територіальних вод, проведення поліцейських, митних, рибоохоронних та спеціальних операцій. Стоять на озброєнні військово-морських сил і берегової охорони багатьох країн [2].

Рис. 1. Катер SOC-R

У 1991 році на озброєння Швецького Королівського Десантного Корпусу прийнятий катер Combat Boat 90 (CB90). Це швидкохідний військовий катер, розроблений компанією Dockstavarvet. Може використовуватися як швидкохідний засіб нападу та берегового захисту, патрульний катер чи спеціальний плавзасіб вогневої підтримки; може також використовуватися для розвідки, огляду та операцій зі збору розвідувальної інформації.

На сьогодні ці катери використовують військово-морські сили низки країн, у тому числі Норвегії (S90N), Греції та Мексики (CB90 HMN), Малайзії і Бразилії. Американська компанія SAFE Boats зі штату Вашингтон викупила у шведській верфі Dockstavarvet ліцензію на побудову цих катерів. Конструкція катера забезпечує йому пристойну морехідність, високу швидкість, ефективність та безпеку в різноманітних ситуаціях. Корпус катера виготовлений із алюмінію, довжиною 14,9 м, шириною 3,8 м при цьому має водозаміщення 18 т та класичну конфігурацію корпусу з оберненою сідловатістю палуби, вузьку рампу на носі, через яку одночасно проходить одна особа по ширині.

Катер вміщує 21-го повністю озброєного спецназівця і 4,5 тонни вантажу. Рульова рубка захищена від куль та уламків, у ній розташовано два робочих місця для екіпажу та одне додаткове з відкидним поворотним кріслом. Під кабіною знаходиться перебірка, що має прохід на посадкову носову рампу, яка забезпечує швидке десантування чи евакуацію поранених на берег, навіть не підготовлений для цього.

Відсік для десанту та їх вантажу розташований у середній частині катера, четверту частину корми займає відкрита палуба і може використовуватися як плавучий командний пункт із додатковим обладнанням зв'язку, або ж як артилерійський катер з можливістю установки гармат.

Стандартне озброєння складається з трьох кулеметів Браунінг M2HB, 12.7-мм кулемета (чи 40-мм гранатомета) закріпленого на турелі в кормовій частині рубки, при необхідності він замінюється на дистанційно керовану стабілізовану кулеметну турель. Спарений 12.7-мм кулемет встановлений перед місцем для рульового. Крім того, катер обладнаний одним гранатометом Mk 19 і модифікованою системою Hellfire RBS 17 SSM. Додатково він може переносити 2.8 тонн морських мін або ж шість глибинних бомб.

Як силова установка використовується два дизельних двигуни потужністю по 600 кВт, які дозволяють розвивати швидкість 45 вузлів, при цьому забезпечуючи високу маневреність на мілководді у прибережних зонах. На катерах, які використовуються в цивільному секторі, встановлюються двигуни потужністю по 550 кВт, які забезпечують швидкість до 45 вузлів. Як рушій використовуються водомети Kamewa FF, які частково заглиблені в направляючій насадці. Це дозволяє катеру додатково, паралельно із підводними засобами управління виконувати вкрай різкі маневри, у тому числі і на високих швидкостях. Максимальний запас ходу складає 440 кілометрів при швидкості 20 вузлів (37 км/год).

На сьогодні загалом випущено більше 220 катерів CB90 різних модифікацій, у тому числі ряд варіантів були побудовані за спеціальними вимогами. Катер CB90HI – це експортний варіант Strb HS 90, де літера S означає "Skyddad" (швецькою "захищений"), рівень його захисту відповідає рівню 4 STANAG НАТО. При цьому вага катера збільшилась на 3,8 тонни, тому на ньому встановлені більш потужні двигуни. А ще ця модель має захист від зброї масового враження,

що реалізовується шляхом підтримання підвищеного тиску у відсіках, кондиціонер та систему охолодження палива для перебування у тропічних умовах, генератор на 220 вольт.

Ще одна модель CB90 HEX – це гібрид між CB90H та CB90N і у норвежському флоті називається Stridsbet 90N (SB90N). Модель CB90 HEX була оптимізована для Королівських ВМС Малайзії, ВМФ Мексики, Швецького Королівського Десантного Корпусу та Грецької берегової охорони.

Модель CB90 NL ("Ledning" – командування, керівництво "швед.") оснащена системою управління батальйонного рівня, компьютерним і комунікаційним обладнанням, резервним генератором для забезпечення електроживлення при непрацюючих двигунах [3].

Рис. 2. Катер CB90 ВМС США

В основі російського найшвидкіснішого патрульного катера проекту 03160 "Раптор", який є на озброєнні ВМФ, – швидкісні катери CB90. Проект розроблений у КБ ВАТ "Ленінградський суднобудівний завод "Пелла", де на верфі в місті Відрадне Ленінградської області було збудовано кілька одиниць.

Рубка катера з двома робочими місцями екіпажу та органами управління зміщена до носової частини катера, вона має броньовий захист класу 5 та 5а, ілюмінатори виконані з кулестійкого скла товщиною 39 мм. Десантне відділення розташоване за рубкою. Для висадки та посадки десанту використовуються верхні та задні люки десантного відсіку або прохід від носової апарелі через рубку.

До складу екіпажу входить дві особи та 20 десантників. Машинне відділення розміщено в кормовій частині судна, згідно з інформацією виробника, воно укомплектоване двома американськими турбодизелями CATERPILLAR C18 ACERT E-rating (1150 к.с. при 2300 об/хв, робочим об'ємом 18,1 літрів, конфігурація блоку циліндрів – L6), та водометними рушіями англійського виробництва Rolls-Royce Kamewa 36A3 HS.

Озброєння складається з бойового модуля “Управа-Корд”: кулемет “КПВТ” калібру 14,5-мм, гіростабілізованого оптико-електронного модуля (ГОЕМ) і системи управління вогнем; БДМ та два кулемети “Печеніг” калібру 7,62-мм на вертлюжних установках побортно [4].

Рис. 3. Катер “Раптор”

“Гюрза” – клас річкових броньованих катерів спроектований “Дослідно-проектним центром кораблебудування” (Україна, Миколаїв). Будівництво катерів проводиться ПАТ “Завод “Ленінська кузня”. Два кораблі класу “Гюрза” були поставлені прикордонним військам Узбекистану в рамках програми експортного контролю та відповідних аспектів безпеки (EXBS), фінансованою Держдепом США. Корабель планувалось використовувати на кордоні з Афганістаном на річці Амудар’я для боротьби з контрабандою зброї та наркотиків. На основі проекту 58150 був розроблений проект 58155 (“Гюрза-М”) – бронекатери дещо більшого розміру з потужнішим та сучаснішим озброєнням.

Бронекатери призначені для несення бойової вахти в прибережній морській смузі. До переліку завдань входять: патрулювання, охорона водних рубежів, боротьба з малорозмірними судами супротивника, захист берегових стаціонарних і плавучих гідротехнічних об’єктів та споруд, сприяння десантним і прикордонним групам, забезпечення безпеки мореплавання, а також сприяння в питаннях розвідки, доставки, постачання [5].

Озброєння катера складають два дистанційно керовані морські бойові модулі БМ-5М.01 “Катран-М” виробництва ДП “Миколаївський ремонтно-механічний завод”, які є варіантом бойового модуля БМ-3 “Штурм” для бронетехніки. Кожен модуль “Катран-М” має 30-мм автоматичну гармату ЗТМ-1, 30-мм автоматичний гранатомет КБА-117 та 7,62-мм кулемет КТ, а також дві ПТРК “Бар’єр” з лазерною системою наведення. Катер оснащений оптико-електронною системою керування вогнем а також має комплект переносного ЗРК.

Крім того, катер обладнаний РЛС “Дельта-М”, оптико-електронною системою управління вогнем артилерії малого і середнього калібру ОЕлС “Sarmat”, датчиками виявлення лазерного випромінювання.

11 листопада 2015 року в Києві відбувся урочистий спуск на воду першого катера “Гюрза-М”, побудованого для ВМС України. Судно назвали “Білгород-Дністровський”.

7 квітня 2016 року відбулась урочиста закладка наступних чотирьох малих броньованих артилерійських катерів проекту 58155 на замовлення Міністерства оборони України.

Повна водотоннажність катера 54 т, довжина 23,0 м, ширина: 4,8 м. два двигуни: ГЕУ 2 забезпечують швидкість 25 вузлів при дальності плавання 900 миль. Екіпаж судна – 5 осіб. Ходова рубка та два відсіки моторний і зброї – броньовані.

Рис. 4. Катер проекту “Гюрза”

Катер UMS-PATROL-1000, розроблений компанією ТОВ “УМС-БОТ” (Україна, Київ) для несення патрульної служби та інших аналогічних функцій, призначений для перевезення людей і малогабаритних вантажів на річках, водосховищах і в прибережній зоні морів.

Конструкція катера становить надміцний зварений корпус з алюмінієво-магнієвого сплаву марки 5083 довжиною 11,4 м, шириною 3,42 м, катер вміщує до 15 осіб. Непотоплюваність корпусу забезпечується заповненням міжкорпусного і трюмного простору спеціальною морською двокомпонентною пінополіуретановою піною. У катері передбачена простора ходова рубка, носова каюта, камбуз, гальюн. Проходи по палубі вздовж правого і лівого борту судна забезпечують безпечне переміщення екіпажу по всій довжині судна. У базовій комплектації катера передбачені системи автономного опалення, система водопостачання, фекальна система, радіонавігаційне устаткування, системи активної і пасивної непотоплюваності. У кормовій частині розташований моторний відсік. Встановлені двигуни VOLVO PENTA D6-330, загальною потужністю 660 к.с. з системою електронного рульового управління забезпечують максимальну швидкість 40 вузлів, на економічному ході у 32 вузли дальність плавання до 1000 км.

Рис. 5. Катер UMS-PATROL-1000

Збудовано кілька патрульних катерів для потреб Прикордонної служби України та пожежно-рятувальний катер для Державної служби з надзвичайних ситуацій України.

Пожежно-рятувальний катер UMS 1000 водотонажністю 7 т, оснащений двома дизельними двигунами, потужністю 306 к.с. На ньому встановлена насосна станція Darley PSM 1500 з подачею води 100 літрів за секунду, два стаціонарних лафетних ствола, при цьому забезпечується робота ще шести ручних пожежних стволів, пінобак на 200 л піноутворювача [6].

Катер UMS 1000 обладнаний трьома комплектами обладнання для порятунку на воді. У його складі – рятувальні круги, рятувальні жилети, надувний човен з мотором. Катер оснащений медичним обладнанням і засобами зв'язку.

Катер може гасити пожежі на водних об'єктах та будинках, розташованих поруч з водою, на відстані до 100 метрів. Але найголовніша перевага катера в тому, що на воді він може підійти до будь-якого місця, де виникла пожежа на березі, куди по суші через будівлі чи через бездоріжжя складно, а іноді і взагалі неможливо під'їхати пожежними автомобілями.

Рис. 6. Пожежно-рятувальний катер UMS 1000

Загалом Україна має величезну наукову та технічну базу для побудови суден різних типів, у тому числі і патрульних катерів. Ще цілий ряд вітчизняних підприємств, не згаданих у тексті раніше, мають великий досвід у проектуванні та виготовленні суден різного призначення та водозаміщення, від невеликих буксирів до океанських лайнерів, від риболовецьких сейнерів до військових авіаносних крейсерів. Серед них всесвітньо відомий суднобудівний завод "Океан", ПАТ "Чорноморський суднобудівельний завод", Державне підприємство "Суднобудівний завод ім. 61 Комунара", суднобудівно-судноремонтний завод "Нібулон", які розміщені в місті Миколаєві. Також у інших припортових містах України сконцентровані наукові центри та виробничі потужності з випуску продукції мореплавства: Маріуполі (Азовський судноремонтний завод та завод "АЗОВ ВЕРФ"), Запоріжжі (ВАТ "Запорізький суднобудівний-судноремонтний завод" та суднобудівна компанія "SIATA"), Херсоні (ВАТ "Херсонський суднобудівний завод"), Одесі (відокремлений самостійний підрозділ "Судноверф Україна", Одеський Національний Морський університет) [7].

Отже, потенційні можливості українського суднобудування дозволяють задовольнити потреби Збройних Сил, Національної гвардії України у плавзасобах різного призначення, в тому числі і у патрульних катерах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Патрульний катер [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/ Патрульний_катер

2. Special Operations Craft-Riverine (SOC-R) [Електронний ресурс]. – Режим доступу : / https://en.wikipedia.org/wiki/ Special_Operations_ Craft_ Riverine_(SOC-R)

3. Патрульные катера проекта 03160 [Електронний ресурс]. – Режим доступу : https://ru.wikipedia.org/wiki/Патрульные_катера_проекта_03160

4. Річкові броньовані катери проекту 58150 [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/Річкові_броньовані_катери_проекту_58150

5. Малі броньовані артилерійські катери проекту 58155 [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/Малі_броньовані_артилерійські_катери_проекту_58155

6. Катер-UMS-1000 [Електронний ресурс]. – Режим доступу : http://www.milnavigator.com/uk/ kater-ums-1000/

7. Суднобудівна промисловість України [Електронний ресурс]. – Режим доступу :https://uk.wikipedia.org/wiki/ Суднобудівна_промисловість_України

8. Вузол (одиниця швидкості) [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/ Вузол_(одиниця_швидкості)

Отримано 07.11.2016
Рецензент Марченко О.С., к.т.н.

УДК 623.1

О.С. Марченко,
кандидат технічних наук,
Л.П. Вяткіна

ПЕРЕСУВНІ БЛОКПОСТИ МОДУЛЬНОЇ КОНСТРУКЦІЇ

У статті наведені результати дослідження можливості розробки та виготовлення на підприємствах України пересувних кулезахисних пристроїв модульної конструкції для потреб підрозділів Національної поліції та Національної гвардії України. Визначено основні тактико-технічні та економічні характеристики захисних пристроїв.

***Ключові слова**: бронеелемент, захисний матеріал, уражаючий елемент, балістична стійкість, модульна конструкція.*

В статье приведены результаты исследования возможности разработки и изготовления на предприятиях Украины передвижных пулезащитные устройств модульной конструкции для нужд подразделений Национальной полиции и Национальной гвардии Украины. Определены основные тактико-технические и экономические характеристики защитных устройств.

***Ключевые слова:** бронеелемент, защитный материал, поражающий элемент, баллистическая стойкость, модульная конструкция.*

Paper presents the results of a study of the ability of the development and production at the enterprises of Ukraine of bulletproof mobile devices of modular design for the needs of the units of the National Police and the National Guard of Ukraine. The main tactical and technical and economic characteristics of the protective devices are identified.

***Keywords:** armoured element, protective material, striking element, ballistic resistance, modular design.*

Забезпечення належного рівня безпеки особового складу підрозділів Національної поліції та Національної гвардії України під час виконання службових обов'язків є одним з актуальних та пріоритетних напрямів. Провідну роль у належному вирішенні цього завдання відіграє науково-технічний процес, зокрема щодо розробки та створення засобів індивідуального та групового бронезахисту залежно від сфери застосування.

Слід зазначити, що на цей час створено велику кількість засобів бронезахисту для різних сфер застосування. Особливо значних успіхів досягнуто в розробленні засобів індивідуального бронезахисту, таких як бронежилети, кулестійкі шоломи та щити. Велика кількість перелічених засобів з різними рівнями захисту, зручних у користуванні та виготовлених за сучасними технологіями дає змогу працівникам правоохоронних органів ефективно вирішувати поставлені завдання із запобігання або припинення правопорушень при одночасному високому рівні безпеки окремого працівника.

Однак з початку проведення в східних областях України антитерористичної операції виникла необхідність тривалого перебування працівників правоохоронних

органів та військовослужбовців в зоні можливого ураження кулями стрілецької зброї або осколками від вибухів артилерійських снарядів і мін. Це зумовило необхідність використання захисних споруд тривалого використання для груп працівників. З цією метою на основних напрямах та магістралях будують стаціонарні залізобетонні блокпости з високим рівнем захисту. Але досить часто виникає потреба взяти під контроль на короткий проміжок часу територію (об'їзну дорогу, другорядну вулицю тощо), яка може потрапити під вплив супротивника. Облаштовувати в таких місцях стаціонарний пост недоцільно через великі обсяги робіт зі спорудження, досить значні витрати коштів та тимчасовий характер захисту.

Тому в таких ситуаціях важливою є можливість забезпечення захисту особового складу за допомогою мобільних засобів – пересувних блокпостів модульної конструкції (далі – ПБМК). У процесі створення таких засобів захисту важливим є створення засобу групового бронезахисту з достатнім рівнем захисних властивостей з одночасним забезпеченням процесу легкого монтажу та демонтажу засобу в потрібному місці. Саме це і зумовлює необхідність проведення дослідження можливості створення пересувних блокпостів модульної конструкції.

У сучасних умовах одним із пріоритетних напрямів діяльності Державного науково-дослідного інституту МВС України є проведення науково-дослідних робіт з питань підвищення захищеності військовослужбовців Національної гвардії та працівників Національної поліції.

Найбільш небезпечними вражаючими факторами для військовослужбовців є кулі, осколки і ударні хвилі від вибуху певних пристроїв та речовин. Зазначені вражаючі фактори також несуть загрозу життю працівникам Національної поліції при проведенні ними спеціальних операцій. Елементи бойової екіпіровки, що забезпечують захист від зазначених уражаючих факторів, і є засобами індивідуального бронезахисту (ЗІБ). До складу ЗІБ входять: бронежилети, кулестійкі шоломи та щити. Однак ЗІБ не забезпечують стовідсоткового рівня захисту, особливо в умовах мінно-артилерійських обстрілів позицій бійців у зоні проведення АТО. Тому для забезпечення належного рівня захисту встановлюються стаціонарні захисні споруди – блокпости – це добре укріплені залізобетонні будови. Також використовують мобільні броньовані пости, схожі на створений підприємством ПрАТ "Практика" (рис. 1).

Рис. 1. Мобільний броньований блокпост

З технічної точки зору, рішення вдале, тим більше, що завдяки мобільності, його можна переносити з місця на місце і встановлювати на найбільш небезпечних ділянках для контролю комунікацій.

Бронестіни і бронескло блокпоста надійно захищають особовий склад від куль та осколків, а турельний кулемет на даху не дасть підійти противнику на відстань пострілу з гранатомета або стрілецької зброї. Бійниці під вікнами і в дверях дозволять персоналу вести прицільний вогонь по нападаючим. І якщо навіть по броньованому модулю буде зроблений постріл з РПГ, гранату має зупинити спеціальна ґратчаста ширма, яка передбачена для дообладнання модуля. Але хоча цей блокпост називається “мобільний”, він обладнаний з розрахунку перебування в ньому персоналу тривалий час. Тому мобільним його можна називати досить умовно, зважаючи на можливість перевстановлення та переміщення лише за допомогою вантажних пристроїв та транспорту.

Водночас необхідність оперативно взяти під контроль ту чи іншу територію або дільницю здійснюється встановленням поста з однієї-двох осіб, захищених лише засобами індивідуального бронезахисту. Тимчасовий характер такого поста робить недоцільним установлення в таких місцях блокпостів тривалого використання.

Забезпечити належний рівень захисту особового складу в таких випадках можливо перш за все шляхом використання пересувних кулестійких щитів, таких як БЗС-75-3 (виробник НВП “Темп-3000”, Україна) або MKST китайського виробництва.

Рис. 2. Пересувний кулестійкий щит БЗС-75-3

Пересувний кулестійкий щит БЗС-75-3 4-го класу захисту (рис. 2) в нижній частині жорстко кріпиться до трикутної рами, на якій розташовано три обгумовані колеса діаметром 100 мм. Два неповоротні колеса укріплені в передній частині рами, а із внутрішньої сторони, по центру рами, розташовано колесо, яке обертається на 360 градусів. У верхній частині щита розташовано віконце з кулестійким склом 4-го класу захисту. Розміри скла – 250 мм × 70 мм, товщина –50 мм.

Розміри щита: висота – 1700 мм, ширина – 500 мм. Вага щита 45 кг.

Пересувний кулестійкий щит MKST (рис. 3) також розміщений на колесах. Його розміри становлять 1000 мм×500 мм, віконця – 200 мм×60 мм. Вага не перевищує 25 кг.

Рис. 3. Пересувний кулестійкий щит MKST

Ці щити призначені для захисту працівників спеціальних підрозділів під час проведення операцій проти озброєних правопорушників на територіях з досить високою якістю покриття дороги або підлогою. З цього випливають основні їх недоліки для використання як захисту для мобільних блокпостів:

– забезпечення захисту лише з фронтальної сторони;
– мала ширина фронтальної пластини;
– ускладнене пересування по ґрунтових поверхнях;
– імовірність проникнення вражаючих елементів в області колісних підставок.

Більш придатним для організації захисту тимчасового блокпоста можна було б вважати щит мобільний на шасі “Бастіон” (рис. 4) виробництва Російської Федерації.

Рис. 4. Щит мобільний “Бастіон”

Щит “Бастіон” обладнаний 3 оглядовими вікнами із склом 5 класу захисту з бійницями і шасі для мобільного пересування.

Розмір центральної секції 1400×625 мм, розмір бічних секцій 312×1400 мм. Вага не більше 150 кг.

Як бачимо з рис. 3, за конструкцією, а також за характеристиками, якби не країна-виробник, щит мобільний на шасі “Бастіон” міг бути більш придатним для вирішення проблеми із захистом особового складу тимчасового блокпоста.

Вивчення світового досвіду з порушеного питання показало, що найбільш ефективним шляхом підвищення рівня захищеності особового складу є створення спеціально спроектованих відносно легких (що можуть монтуватися однією або двома особами) захисних пристроїв модульної конструкції. Прикладом такого пристрою може бути система PROTECTOR виробництва британської компанії Force Development Services (FDS) (рис. 5).

Рис. 5. Контрольно-пропускний пункт облаштований пересувним блокпостом модульної конструкції PROTECTOR виробництва компанії FDS

За конструкцією система PROTECTOR – це набір бронепластин та щита з кулестійкого скла, які з’єднуються за допомогою спеціальних кулестійких елементів.

ПБМК має невелику вагу (230 кг для варіанта зі сталевими бронепластнами та бронесклом, легко завантажується та перевозиться звичайними позашляховиками (типу УАЗ, Hummer тощо), легко збирається та розбирається в місті встановлення силами двох осіб, а також забезпечує захист за 4 класом згідно з ДСТУ В 4103-2002 “Засоби індивідуального захисту. Бронежилети. Загальні технічні умови”.

Також компанією FDS пропонується ПБМК PROTECTOR у полегшеному варіанті виконання вагою 140 кг (бронепластини виготовлені з балістичного пластичного матеріалу) з аналогічним рівнем захисту.

За станом на 28 листопада 2016 року вартість ПБМК PROTECTOR зі сталі становить £6,727.50, а ПБМК PROTECTOR меншої ваги – £11,500, що за курсом

НБУ становить відповідно 214607 грн. та 366850 грн. Термін постачання 12 тижнів з моменту замовлення.

Досить висока ціна одиниці виробу, навіть у варіанті з бронепластнами зі сталі, а також наявність в Україні низки підприємств з виробництва засобів індивідуального бронезахисту та інших броньованих пристроїв спонукала фахівців ДНДІ МВС України на проведення досліджень із можливості налагодження виробництва ПБМК в нашій державі. Для цього були досліджені особливості конструкції системи PROTECTOR та за результатами розроблені вихідні вимоги до ПБМК, які наведені нижче.

ВИХІДНІ ВИМОГИ ДО ПЕРЕСУВНОГО БЛОКПОСТА МОДУЛЬНОЇ КОНСТРУКЦІЇ

1. Пересувний блокпост модульної конструкції для облаштування постів (рис. 6) повинен забезпечувати швидке складання та встановлення захисних укріплень з метою захисту працівників спеціальних підрозділів під час виконання антитерористичних та інших операцій швидкого розгортання.

2. Пересувний блокпост модульної конструкції повинен мати конструкцію, придатну для ручного обслуговування.

3. До складу кулезахисного пристрою мають входити (рис. 7):

1 – фронтальна пластина 1 шт.;

2 – бокові пластини 4 шт.;

3 – захисне кулестійке скло 1 шт.;

4 – з'єднувальні елементи 4 шт.

4. Маса окремого захисного елемента (фронтальної пластини, бокових пластин та кулестійкого скла не повинна перевищувати 20 кг [1].

5. Клас захисту окремих елементів виробу відповідно до ДСТУ 4546:2006 "Захисне скління" та ДСТУ 4547:2006 "Кулетривкість. Вимоги та класифікація" має бути не нижчим ніж:

– фронтальна пластина – ОЗК4;

– бокові пластини – ОЗК4;

– захисне кулестійке скло – СК4;

– з'єднувальні елементи – ОЗК4.

6. Конструкція з'єднувальних елементів повинна забезпечувати:

– надійне з'єднування захисних елементів (захисного кулестійкого скла, фронтальної та бокових пластин) без зниження класу захисту в місцях з'єднання;

– збирання та розбирання кулезахисного пристрою без застосування інструментів за допомогою встановлених на з'єднувальних елементах пристосувань (пружинних або кулачкових затискачів, фіксаторів, фігурних гайок тощо).

[1] Параметр уточняється на етапі розробки.

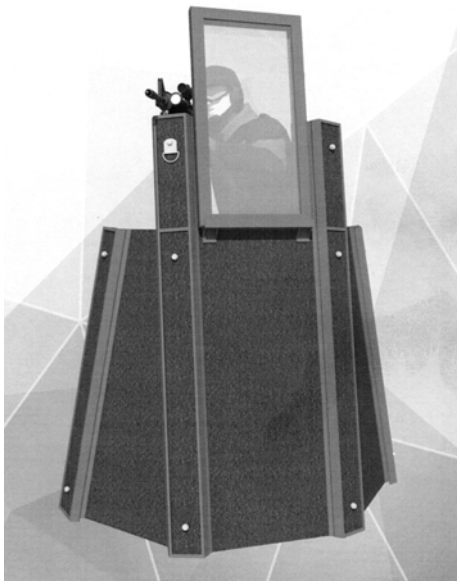


Рис. 6. Загальний вигляд ПБМК

Розміри для довідки.
1 – фронтальна пластина
2 – бокові пластини
3 – захисне кулестійке скло
4 – з'єднувальні елементи

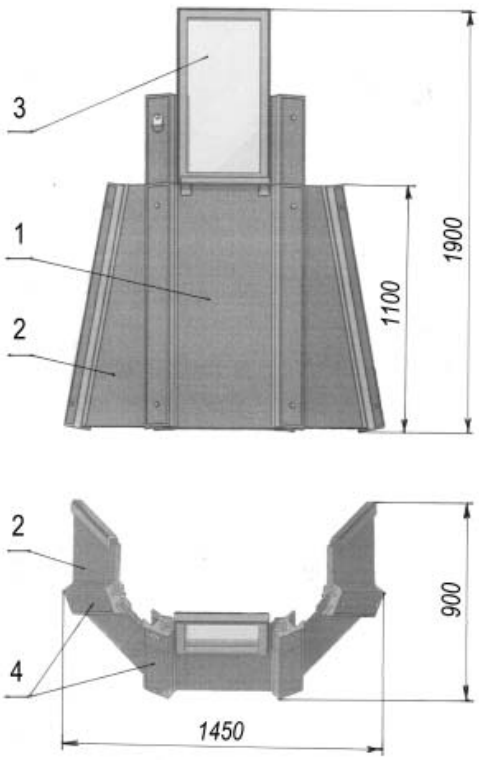


Рис. 7. Основні частини та розміри ПБМК

Потім для опрацювання “Вихідні вимоги до пересувного блокпосту модульної конструкції” були надіслані на підприємства України, що випускають засоби бронезахисту, а саме: ТОВ “Матеріалознавство”, ТОВ “НВП “Темп-3000”, ТОВ “Реформ”, ТОВ “ВЕСТ-ТАНДЕМ” та ПрАТ “Практика”.

Після аналізу та опрацювання вихідних вимог ТОВ “Матеріалознавство” через відсутність необхідної виробничої бази відмовилося брати участь у роботах зі створення ПБМК, ТОВ “НВП “Темп-3000” у разі необхідності зголосилося брати участь у виготовленні окремих елементів конструкції ПБМК. Водночас фахівцями ПрАТ “Практика” проведено аналіз вихідних вимог та з урахуванням виробничих можливостей підприємства за його результатами надано пропозиції щодо конструктивного виконання ПБМК (рис. 8) та надано орієнтовні тактико-технічні характеристики ПБМК (Таблиця 1).

Таблиця 1

Тактико-технічні характеристики ПБМК

№ з/п	Найменування показника	Значення показника	Примітка
1.	Клас балістичного захисту за ДСТУ 3975-2000	ПЗСА-4	
2.	Повна маса виробу, з них: маса броньованих елементів маса бронескла маса з’єднувальних елементів	240 кг 140 кг 55 кг 45 кг	
3.	Габарити виробу	1450 ммх900 ммх 1900 мм	
4.	Час збирання (розбирання) конструкції двома особами	до 15 хв.	

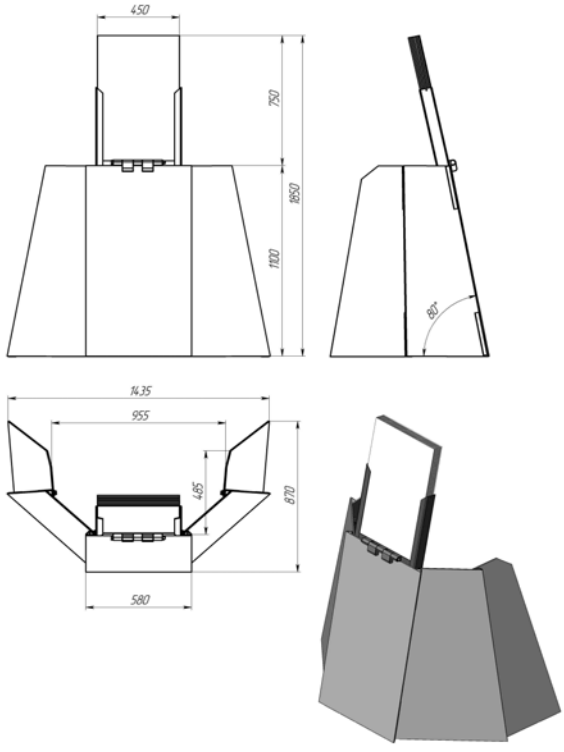


Рис. 8. Проект пересувного блокпоста, запропонований ПрАТ “Практика”

Також було надано результати економічних розрахунків, за якими орієнтовна вартість ПБМК у цінах за станом на листопад 2016 року склала 84 000 грн. Тобто вартість ПБМК PROTECTOR виробництва FDS більше ніж у 2,5 рази вища за вартість ПБМК, запропонованого ПрАТ "Практика", при лише на 10 кг меншій вазі та аналогічних захисних властивостях, що є переконливим аргументом доцільності (у разі зацікавленості підрозділів Національної поліції та Національної гвардії України у оснащенні ПБМК) продовження робіт за участю вітчизняного виробника.

Позитивним також є те, що підприємство може забезпечити як постачання запасних частин так і обслуговування та виконання ремонтних робіт виробу (у разі виникнення такої необхідності). Це важливо, тому що умови експлуатації ПБМК зумовлюють високу вірогідність пошкодження його елементів під час використання в зоні проведення АТО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ ГОСТ 28653:2009 "Зброя стрілецька. Терміни та визначення. – К. : Держспоживстандарт, 2011. – 142 с.

2. ДСТУ В4103-2002. Засоби індивідуального захисту. Загальні технічні умови. – К. : Держспоживстандарт, 2002. – 20 с.

3. ДСТУ В4104-2002. Засоби індивідуального захисту. Вироби броне захисту. Методи контролю балістичної стійкості бронежилетів. – К. : Держспоживстандарт, 2002. – 24 с.

4. ДСТУ 4546;2006. Захисне скління. – К. : Держспоживстандарт, 2006. – 16 с.

5. ДСТУ 4547;2006. Кулетривкість. Вимоги та класифікація. – К. : Держспоживстандарт, 2006. – 12 с.

6. [Електронний ресурс]. – Режим доступу : http://www.forcedevelopment.co.uk.

Отримано 17.11.2016

Рецензент Смерницький Д.В., к.т.н.

УДК 681.3(07)

І.В. Толок,
кандидат педагогічних наук

УДОСКОНАЛЕННЯ ПРОЦЕСУ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ СКЛАДНИХ ВІДНОВЛЮВАНИХ ОБ'ЄКТІВ АВТО- ТА БРОНЕТЕХНІКИ ЗА ДОПОМОГОЮ ІМІТАЦІЙНОЇ СТАТИСТИЧНОЇ МОДЕЛІ

У статті наведені результати вдосконалення процесу технічного обслуговування складного відновлюваного об'єкта авто- та бронетехніки за допомогою імітаційної статистичної моделі. Дослідження проведене на прикладі тестового об'єкта, що має ієрархічну конструктивну структуру. Як результати досліджень отримані залежності для найбільш важливих показників якості процесу технічного обслуговування.

Ключові слова: *технічне обслуговування, авто- та бронетехніка, імітаційна модель, показники якості.*

В статье приведенные результаты усовершенствования процесса технического обслуживания сложного восстанавливаемого объекта авто- и бронетехники с помощью имитационной статистической модели. Исследование приведено на примере тестового объекта, который имеет иерархическую конструктивную структуру. Как результаты исследований получены зависимости для наиболее важных показателей качества процесса технического обслуживания.

Ключевые слова: *техническое обслуживание, авто- и бронетехника, имитационная модель, показатели качества.*

In the papere the results of an improvement of the process of technical maintenance of difficult refurbishable object of auto- and armoured technique by means of simulation statistical model are stated. Research is carried out on the example of test object that has got an hierarchical structural structure. As results of researches several dependences for the most of essential indexes of the quality of process of technical service are got

Keywords*: technical service, auto- and armoured technique, simulation model, indexes of quality.*

Вступ та постановка завдання

Ефективне використання складної військової техніки тривалої експлуатації потребує організації оптимальної системи її технічного обслуговування і ремонту (ТОіР). При цьому виникає протиріччя між обсягом ТОіР та його собівартістю. Для розв'язання цього протиріччя необхідно проводити математичне моделювання процесів ТОіР. Особливо гостро ця проблема стоїть для об'єктів авто- та бронетехніки (далі – об'єктів). Сьогодні експлуатується велика кількість і номенклатура таких об'єктів, більшість з яких виготовлені у 90-ті, 80-ті і навіть 70-ті роки минулого століття. Деякі з них експлуатувались, а значна частка

стояла на збереженні і особливо потребує ретельного обслуговування, ремонту та модернізації. Тобто існує науково-технічна проблема, яку слід терміново розв'язати.

Ця стаття спрямована на розроблення імітаційної статистичної моделі складного відновлюваного об'єкта авто- та бронетехніки, за допомогою якої можна визначати (прогнозувати) показники якості (ПЯ), що характеризують цей процес, при заданих властивостях надійності об'єкта й різних значень параметрів системи технічного обслуговування (СТО).

Визначення основних результатів. У якості ПЯ процесу технічного обслуговування (ТО) будемо використовувати такі показники:

T_0 – середній наробіток на відмову;

$K_{\text{г}}$ – коефіцієнт готовності;

$K_{\text{тв}}$ – коефіцієнт технічного використання;

$c_{\text{уд}}$ – питома вартість експлуатації об'єкта;

$K_{\text{е}}$ – коефіцієнт ефективності ТО [1; 2].

Показники T_0 і $K_{\text{г}}$ є показниками надійності, однак вони містять у собі досить важливу інформацію про якість процесу ТО. Усі зазначені ПЯ оцінюються за допомогою імітаційної статистичної моделі на заданому періоді експлуатації об'єкта $T_{\text{мод}}$. Вочевидь, що значення показників значною мірою залежать від параметрів надійності об'єкта і від параметрів СТО.

Узагальненими параметрами надійності об'єкта є його конструктивна та надійнісна структура та показники надійності складових вузлів і елементів. Конструктивна структура об'єкта задається деревом складеності конструктивних елементів [2]. Дуже наочно це показано на прикладі складних виробів радіоелектронного озброєння, оскільки вони складаються з радіоелементів, електроприладів, гідроприладів тощо, у тому числі, авто- та гусеничної техніки [4]. Коренем дерева є об'єкт у цілому, а вершини дерева – це конструктивні елементи різних рівнів складності. Як ПЯ для кожного конструктивного елемента нижнього рівня задаються: вид закону розподілу наробітку до відмови, середній наробіток до відмови та коефіцієнт варіації. Для всіх інших елементів старших рівнів ПЯ розраховуються програмно з урахуванням надійнісної структури кожного з елементів [3; 4]. Більш детально параметри надійності об'єкта не розглядаються, тому що задача полягає в дослідженні впливу параметрів СТО.

Як параметри СТО приймемо обсяг ТО, що задається множиною елементів $E_{\text{то}}$, що обслуговуються, періодичність проведення ТО $T_{\text{то}}$ та кількість видів ТО $N_{\text{то}}$. Формально СТО будемо представляти такою множиною:

$$CTO = \{E_{\text{то}\,j}, T_{\text{то}\,j}, \tau_{\text{д}\,j}, C_{\text{д}\,j};\ j = \overline{1, N_{\text{то}}}\}, \qquad (1)$$

де $E_{\text{то}\,j}$ – множина елементів об'єкта, які обслуговуються (обновляються) при ТО j-го виду;

$T_{\text{то}\,j}$ – періодичність ТО j-го виду;

$\tau_{\text{д}\,j}$ – витрати часу на діагностування об'єкта при ТО j-го виду;

$C_{\text{д}\,j}$ – вартість діагностування при ТО j-го виду;

$N_{\text{то}}$ – кількість видів ТО.

Кожний із наведених вище ПЯ процесу ТО є функцією від параметрів надійності об'єкта і параметрів СТО. Тому далі визначимо розрахункові співвідношення, які описують ці функції.

Основні розрахункові співвідношення для ПЯ процесу ТО. Середній наробіток на відмову T_0 визначається таким чином:

$$T_0(H_{над}, CTO) = T_{мод} / \bar{n}_{отк}(H_{над}, CTO), \quad (2)$$

де $H_{над}$ – узагальнений параметр, який представляє дані про надійність об'єкта, що закладена в базі даних моделі;

CTO – узагальнений параметр, який визначає параметри СТО (1);

$\bar{n}_{отк}(H_{над}, CTO)$ – середня кількість відмов об'єкта, що виникають на інтервалі експлуатації $T_{мод}$.

Коефіцієнт готовності $K_г$ відповідно до визначення [5] обчислюється за формулою:

$$K_г(H_{над}, CTO) = 1 - \bar{t}_{в\Sigma}(H_{над}, CTO)/(T_{мод} - \bar{t}_{то\Sigma}(CTO)), \quad (3)$$

де $\bar{t}_{в\Sigma}(H_{над}, CTO)$ – середня сумарна тривалість відновлення об'єкта (сумарний час перебування об'єкта в непрацездатному стані) протягом періоду експлуатації $T_{мод}$;

$\bar{t}_{то\Sigma}(CTO)$ – середня сумарна тривалість перебування об'єкта у стані ТО.

Коефіцієнт технічного використання $K_{тв}$ відповідно до визначення у [5] обчислюється за формулою:

$$K_{тв}(H, CTO) = 1 - (\bar{t}_{в\Sigma}(H, CTO) + \bar{t}_{то\Sigma}(CTO))/T_{мод}. \quad (4)$$

Питома вартість експлуатації $c_{уд}$ визначається як сума:

$$c_{уд}(H_{над}, CTO) = c_{уд\,в}(H_{над}, CTO) + c_{уд\,то}(CTO), \quad (5)$$

де $c_{уд\,в}(H_{над}, CTO)$ – питомі витрати вартості на відновлення поточних відмов об'єкта;

$c_{уд\ то}(CTO)$ – питомі витрати вартості на виконання робіт ТО.

Якщо у (5) не визначати накладні витрати, то коефіцієнт ефективності ТО буде мати вираз:

$$K_е(H_{над}, CTO) = (T_0(H_{над}, CTO) - T_0(H_{над}, \varnothing))/(T_0(H_{над}, \varnothing) \cdot c_{уд\,то}(CTO)), \quad (6)$$

де $T_0(H_{над}, \varnothing)$ – середній наробіток на відмову об'єкта у випадку, якщо ТО не проводиться.

Показник $K_е$ має сенс відносного збільшення показника безвідмовності об'єкта (середнього наробітку на відмову T_0), одержуваного за рахунок проведення ТО, що приходиться на одиницю питомої вартості витрат на ТО.

Розглянемо тепер більш детально окремі складові, що входять у вирази (2)–(6).

Величини $\bar{n}_{отк}(H_{над}, CTO)$ і $\bar{t}_{в\Sigma}(H_{над}, CTO)$ утворюються як прямий результат статистичного моделювання й додаткових пояснень не вимагають.

Величина $\bar{t}_{то\Sigma}(CTO)$ обчислюється таким чином:

$$\bar{t}_{то\Sigma}(CTO) \cong T_{мод} \sum_{j=1}^{N_{то}} \frac{\tau_{то\ j}}{T_{то\ j}}, \quad (7)$$

де $\tau_{\text{то } j}$ – тривалість ТО j-го виду.

Величина $\tau_{\text{то } j}$ залежить від обсягу ТО й обчислюється за формулою:

$$\tau_{\text{то } j} = \sum_{i \in I_{\text{то } j}} [\tau_{\text{то } ij}(1 - p_{\text{зам } i}) + \tau_{\text{зам } i} p_{\text{зам } i}] + \tau_{\text{д } j}, \quad (8)$$

де $\tau_{\text{то } ij}$ – тривалість операції по обслуговуванню i-го елемента при ТО j-го виду;
$p_{\text{зам } i}$ – імовірність того, що при ТО буде потрібна заміна i-го елемента;
$\tau_{\text{зам } i}$ – тривалість операції заміни i-го елемента;
$I_{\text{то } j}$ – множина номерів (індексів) елементів, які обслуговуються (обновляються) при ТО j-го виду.

Величина $c_{\text{уд в}}(H_{\text{над}}, CTO)$ – питома вартість витрат на відновлення відмов, визначається за формулою:

$$c_{\text{уд в}}(H_{\text{над}}, CTO) = \sum_{i \in I_E} \overline{\omega}_i(H, CTO) \cdot (C_{0\,i} + C_{\text{зам } i}), \quad (9)$$

де $\overline{\omega}_i(H_{\text{над}}, CTO)$ – середнє значення параметра потоку відмов i-го елемента (отримується в результаті статистичного моделювання);
$C_{0\,i}$ – вартість i-го елемента;
$C_{\text{зам } i}$ – вартість робіт із заміни i-го елемента;
I_E – множина номерів усіх елементів об'єкта РЕТ (елементи, відмови яких моделюються).

Величина $c_{\text{уд то}}(CTO)$ – питома вартість витрат на проведення ТО, визначається таким чином:

$$c_{\text{уд то}}(CTO) = \frac{1}{T_{\text{мод}}} \sum_{j=1}^{N_{\text{то}}} \left[T_{\text{то } j} \sum_{i \in I_{\text{то i}}} [(C_{0\,i} + C_{\text{зам } i}) p_{\text{зам } i} + C_{\text{то } ij}(1 - p_{\text{зам } i})] + C_{\text{д } j} \right], \quad (10)$$

де $I_{\text{то } j}$ – множина номерів елементів, які обслуговуються (обновляються) при ТО j-го виду;
$C_{\text{то } ij}$ – вартість робіт ТО i-го елемента. Інші позначення в (10) були визначені вище.

Результати моделювання. Як тестовий об'єкт для моделювання витрат вибрано автомобіль ГАЗ–66 [6; 7]. Усі вихідні дані, що використовуються в (7) – (10), беруться із БД моделі.

Тимчасові та вартісні показники для всіх елементів умовно задаємо однаковими. У БД моделі введені такі значення показників:

$$\tau_{\text{зам } i} = 1 \text{ год};\ \tau_{\text{то } ij} = 1 \text{ год};\ C_{0\,i} = 10 \text{ у.о.};\ C_{\text{зам } i} = 1 \text{ у.о.};\ C_{\text{то } ij} = 1 \text{ у.о.}$$

Дослідження полягає в багаторазовому моделюванні процесу ТО для вибраного тестового об'єкта з метою одержання значень ПЯ при різних значеннях параметрів СТО.

Моделювання робилося при таких значеннях параметрів моделювання: $T_{\text{мод}} = 20$ років – період експлуатації об'єкта;

$\Delta t = 6$ міс – величина інтервалів часу, в яких робиться нагромадження статистики про відмови;

$N_I = 1000$ – кількість ітерацій моделювання.

Параметри СТО задавалися наступними: $N_{\text{то}} = 1$; $\tau_{\text{д}\,j} = 1$ год; $C_{\text{д}\,j} = 1$ у.о.

Періодичність ТО $T_{\text{то}}$ варіювалася в межах від 1 до 8 міс.

Результати моделювання наведені на рис. 1, 2, 3.

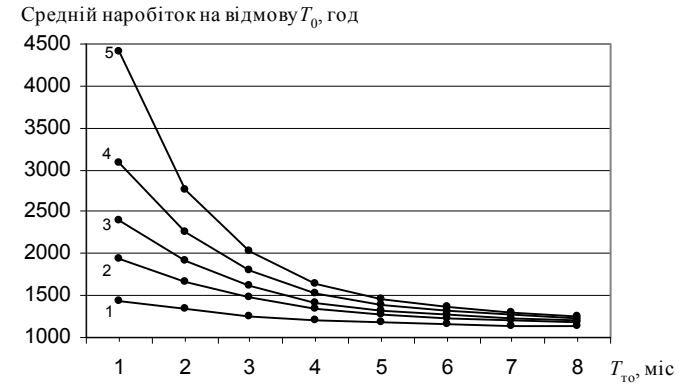


Рис. 1. Розподіл середнього наробітку на відмову $T_{\text{то}}$ год

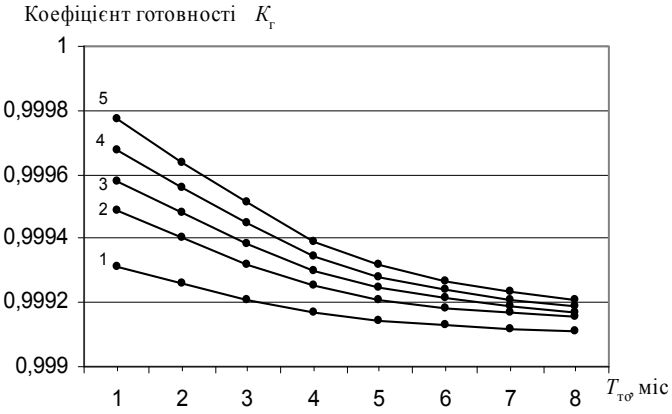


Рис. 2. Розподіл коефіцієнта готовності $K_{\text{г}}$

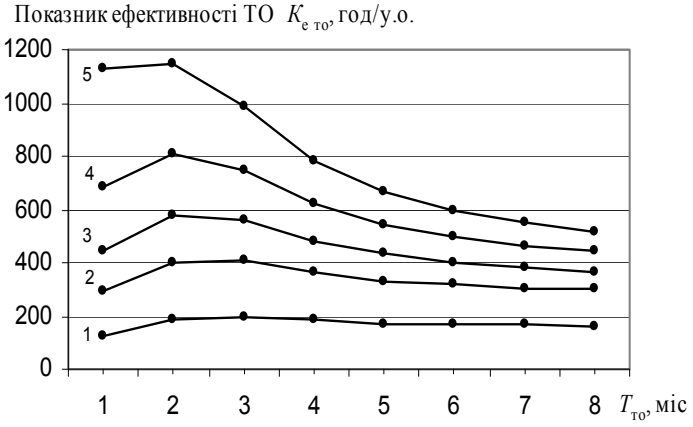


Рис. 3. Розподіл показників ефективності ТО $K_{\text{сто}}$, год/у.о.

Наведені графіки ПЯ дають вичерпну інформацію про властивості досліджуваного процесу ТО та про вплив на процес параметрів СТО. Так, видно, що значення ПЯ T_0 і $K_г$ завжди зменшуються при збільшенні періодичності ТО ($T_{то}$) і при зменшенні обсягу ТО ($E_{то}$). Ця закономірність очевидна з фізичних міркувань і не залежить від почасових і вартісних характеристик елементів об'єкта та параметрів СТО [4].

Величина коефіцієнта технічного використання $K_{тв}$ зростає при збільшенні періодичності $T_{то}$. Це свідчить про те, що сумарний час простою об'єкта в непрацездатному стані зумовлено переважно простоями на ТО – при збільшенні періодичності ТО $T_{то}$ частка часу простою, що припадає на ТО, убуває (за інших рівних умов) і пропорційно цьому зростає величина $K_{тв}$.

Висновок

1. Імітаційна статистична модель процесів ТОіР, що розроблена, досить адекватна реальності й може бути корисним інструментом для аналізу процесів ТО складних відновлюваних об'єктів авато- та бронетехніки.

2. При аналізі процесів ТО складного об'єкта недостатньо обмежуватися деякими окремими "надійнісними" або "вартісними" показниками. Необхідно досліджувати сукупність ПЯ, які спільно характеризують найбільш важливі властивості процесу ТО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Толок И.В.* Определение системы технического обслуживания и ремонта автомобильной техники на предприятиях Министерства обороны Украины и ее критерии эффективности / И.В. Толок // Система управління, навігації та зв'язку. – К. : Центральний науково-дослідний інститут навігації і управління, 2008. – Вип.4(8). – С. 95–97.

2. *Браун В.О.* Моделирование процессов технического обслуживания сложных восстанавливаемых объектов радиоэлектронной техники / В.О. Браун, К.Ф. Боряк, О.Б. Лантвойт, В.Н. Цыцарев // Вісник інженерної академії України. – К., 2008. – № 1. – С.47–52.

3. *Толок И.В.* Построение информационной базы системы технического обслуживания и ремонта автомобильной техники / И.В. Толок // Збірник наукових праць Харківського університету Повітряних Сил ім. І. Кожедуба. – Харків, 2008. – Вип.3(8). – С.146–148.

4. *Боряк К.Ф.* Постановка задачі оптимізації технічного обслуговування складних відновлюваних об'єктів радіоелектронної техніки / К.Ф. Боряк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2008. – № 12. – С. 5–10.

5. ДСТУ 2860-94. Надійність техніки. Терміни та визначення.

6. *Толок И.В.* Анализ диагностирования технического состояния автомобильной техники / И.В. Толок // Журнал Харківського університету Повітряних Сил ім. І. Кожедуба "Системи обробки інформації". – Харків, – 2008. – № 6(73). – С. 124–126.

7. *Зінчик А.Г.* Вибір автомобільних транспортних засобів для комплектування підрозділів Збройних Сил України із використанням математико-статистичних методів експертного оцінювання / А.Г. Зінчик // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2009. – № 20. – С. 45–50.

Отримано 09.11.2016
Рецензент Рибальський О.В., д.т.н.

СПЕЦІАЛЬНІ РОЗРОБКИ

УДК 629.396.969.3

В.А. Білогуров,
К.В. Заїчко

ОГЛЯД СИСТЕМ ВИЯВЛЕННЯ ТА ПРОТИДІЇ БЕЗПІЛОТНИМ ПОВІТРЯНИМ СУДНАМ В УМОВАХ МІСЬКОЇ ЗАБУДОВИ

У статті розглянуто принципи роботи систем та засобів протидії безпілотним повітряним суднам, проведено їхній аналіз, розглянуто вимоги до систем протидії в умовах із щільною міської забудовою, подано основні види загроз.
Ключові слова: *безпілотні повітряні судна, системи та засоби виявлення і протидії БПС, види загроз.*

В статье рассмотрены принципы работы систем и средств противодействия беспилотным воздушным судам, проведен анализ, сформированы требования для работы в условиях городской застройки, представлены основные виды угроз.
Ключевые слова*: беспилотные воздушные судна, системы и средства выявления и противодействия БВС, виды угроз.*

Paper describes the principles of the operation of systems and means of counteraction to the unmanned aircraft, an analysis is carried out, the requirements for working in urban areas are formed, the main types of threats are defined.
Keywords: *unmanned aircraft, systems and tools to identification and counteraction to the unmanned aircraft systems, types of threats.*

Щодня в засобах масової інформації з'являються нові публікації, які стосуються використання і застосування дронів або безпілотних літальних апаратів (БПЛА – unmanned aerial vehicles (UAV)), які зараз у нормативно-правовій спільноті прийнято називати безпілотними авіаційними системами (БАС – Unmanned Aerial Systems (UAS)).

Рис. 1. Доставляння зброї за допомогою БПС

Рис. 2. Доставляння заборонених предметів у місця позбавлення волі

Назва “дрони” або “БПЛА” (UAV) використовуються часто і взаємнозамінно, термін “безпілотні авіаційні системи” стає загальноприйнятим у нормативно-правовій спільноті і в галузі та застосовується для позначення всіх комплексних компонентів повітряних і наземних систем, які містять у собі БПЛА та забезпечують їхню експлуатацію. Однак далі в статті будемо використовувати визначення, які внесені в Повітряний кодекс України, а саме: повітряне судно – апарат, що підтримується в атмосфері в результаті його взаємодії з повітрям, відмінної від взаємодії з повітрям, відбитим від земної поверхні (далі – ПС); безпілотне повітряне судно – повітряне судно, призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза повітряним судном (далі – БПС) [1; 2].

БПС за останні роки стають пристроями, які інтегруються в різні галузі суспільного життя. З однієї сторони, БПС мають позитивний вплив на розвиток різних господарських галузей, як приклад, допомагають обробляти сільськогосподарські угіддя, проводити обстеження складних об’єктів, їх використовують у картографуванні, під час проведення моніторингу лісонасаджень (виявлення незаконної вирубки), при моніторингу корисних копалин тощо. Інша загальновживана назва БПС у засобах масової інформації – дрони, які застосовують як спортивні засоби та розваги. Тенденції розвитку простих та відповідно дешевих моделей БПС свідчать про значне зростання ринку їхнього споживання. Згідно з даними міжнародних аналітичних досліджень станом на 2015 рік валова вартість цієї галузі зросла майже до 1,7 млрд доларів США. Прогнози на майбутні роки свідчать про нарощування темпів зростання зазначеної галузі.

Разом із позитивними тенденціями інтеграції БПС до виробничої, господарської та розважальної діяльності виявлені і негативні наслідки від їхнього протиправного застосування. Дедалі частіше з новин можна отримати інформацію стосовно використання БПС для передачі зброї, (рис. 1) наркотичних засобів та інших заборонених речовин у місця позбавлення волі, (рис. 2) або під час незаконного перетинання кордону. Не менш небезпечним явищем є поява несанкціонованих БПС у зоні злітних смуг аеропортів та під час проведення культурно-масових заходів. Також гостро стоїть проблема щодо використання БПС у таких випадках, як: несанкціоноване зняття інформації, використання

підривних пристроїв, розпилення небезпечних отруйних речовин, постановки радіозавад та порушення функціонування роботи радіочастотних пристроїв (у тому числі Wi-Fi пристроїв). Тож розглянемо основні види небезпек, які можуть виникати при протиправному використанні БПС.

Класифікація видів загроз

За інформацією, отриманою з масових джерел, випадки протиправного застосування БПС можна розділити та відповідно класифікувати за такими напрямами:

– доставляння зброї та вибухових речовин (до місць позбавлення волі або до місць вчинення терористичних заходів);

– розпилення отруйних речовин (та їх наступна активація);

– створення радіозавад;

– зняття інформації (прослуховування та спостереження);

– фото- та відеофіксація інформації (з високою роздільною здатністю);

– контрабанда;

– БПС-камікадзе (одноразове використання з вибухівкою, хімічними або бактеріологічними речовинами);

– БПС з вогнепальною зброєю на борту (для прицільного знищення людей);

– БПС з метою перешкоджання руху повітряних суден (злітно-посадкових загроз) та створення загроз об'єктам з підвищеною небезпекою (атомні станції).

Наглядно класифікація видів загроз схематично представлена на рис. 1.

Рис. 3. Схематичне представлення видів загроз

Отже, з появою нових технологій постійно створюється також можливість для застосування БПС для вчинення протиправних дій у небезпечний для оточуючих спосіб. Тому постає нагальна потреба у знешкодженні БПС, на борту яких можуть бути речовини, що становлять загрозу життю та здоров'ю людей. Особлива увага приділяється протидії БПС в умовах міської забудови, де використання систем та засобів протидії може мати як позитивні, так і негативні наслідки. Вибір технологій та засобів боротьби з БПС є важливим завданням у діяльності правоохоронних органів.

Розглянемо найбільш відомі системи та засоби, які виявляють та протидіють несанкціонованому використанню БПС.

Тенденція розвитку систем протидії БПС у країнах Європейської спільноти (далі ЄС) – це, в першу чергу, виявлення об'єкта БПС та наступна локалізація оператора (пульта керування).

Розглянемо системний підхід до вирішення поставлених питань, а саме приклад реалізації технологій Німецької компанії DEDRONE [4].

DEDRONE

Інженери та програмісти цієї компанії для підвищення надійності виявлення БПС, що наближаються до контрольованої території, застосували декілька сенсорів, робота яких ґрунтується на різних фізичних принципах.

Схематично робота датчиків або сенсорів зображена на рис. 4.

Акустичний (аудіо) сенсор. Чутливий направлений мікрофон вловлює коливання повітря звукового діапазону, підсилює електричні сигнали до потрібного для обробки рівня і порівнює їх із даними в пам'яті аналізатора. При тотожності прийнятого сигналу із записаним у пам'яті, сенсор на своєму виході виставляє логічну одиницю.

Ультразвуковий (УЗ) сенсор. Ненаправлений мікрофон вловлює коливання повітря ультразвукового діапазону, підсилює електричні сигнали до потрібного для обробки рівня і порівнює їх з даними в пам'яті аналізатора.

При тотожності прийнятого сигналу із записаним у пам'яті сенсор на своєму виході виставляє логічну одиницю.

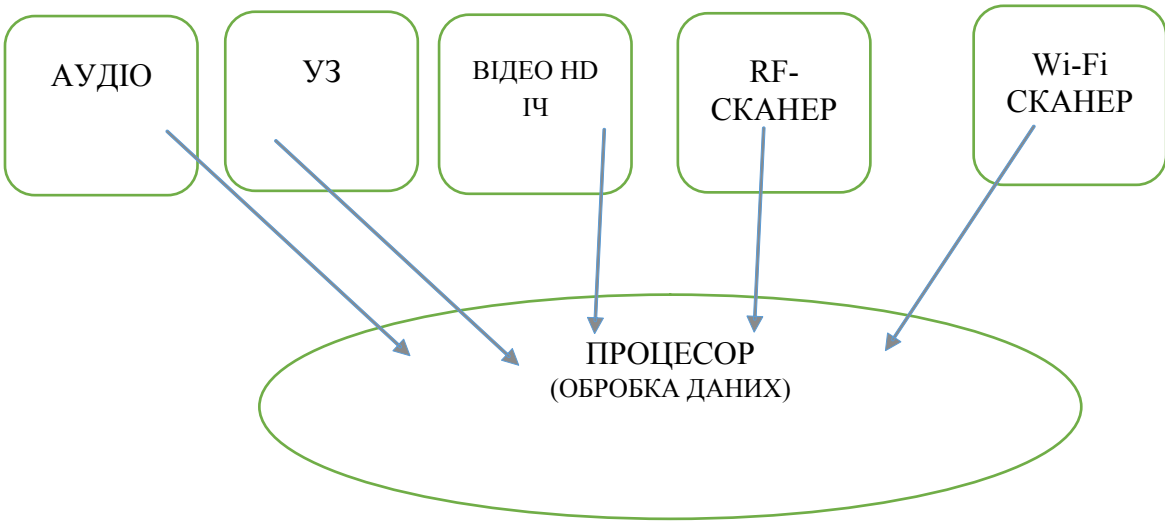


Рис. 4. Структурна схема роботи системи "Dedrone"

Відео (HD) сенсор. Дві відеокамери, одна в оптичному діапазоні, інша в інфрачервоному (ІЧ), контролюють у заданому секторі появу БПС. При тотожності прийнятих зображень із записаними в пам'яті сенсор на своєму виході виставляє логічну одиницю.

Радіочастотний сенсор (RF-сканер). У заданих користувачем частотних діапазонах виявляє наявність характерних для пульту керування БПС радіовипромінювань. При виявленні таких випромінювань у зоні свого контролю на своєму виході виставляє логічну одиницю.

Wi-Fi сканер. Відслідковує у своєму діапазоні рухомі точки доступу. При виявленні рухомих точок доступу сенсор на своєму виході виставляє логічну одиницю.

Процесор – отримує від кожного з сенсорів інформацію, яку порівнює з своєю базою даних і при тотожності більшості з них видає сигнал попередження про появу БПС у просторі, що контролюється.

Зовнішній вигляд конструкції сенсорів (датчиків) зображений на рис. 5. У кожному куту хрестовини розміщені датчики. У центрі – відеосенсор високої роздільної здатності з попередньо визначеною фокусною відстанню. У мобільній версії процесор знаходиться всередині пристрою.

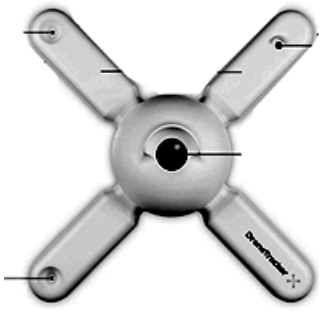


Рис. 5. Зовнішній вигляд системи сенсорів

Розміри, швидкість і різноманітність типів БПС значно ускладнює процес виявлення і відстеження. Система “Dedrone”, аналізуючи шум, розмір, схему руху, частоту, виявляє БПС з певною вірогідністю.

Для забезпечення ідентифікації БПС компанією “Dedrone” отримано домовленість з виробниками БПС щодо можливості досліджень нових моделей і зняття основних характеристик (швидкість руху, телеметрія керування, акустичний малюнок та багато інших), які постійно оновлюються в базі даних системи, яка називається – Дрон-ДНК. Користувачі системи виявлення мають доступ до регулярного оновлення бази даних характеристик БПС.

Сектори (зони параметрів) роботи сенсорів (датчиків), функції яких описано вище, схематично зображено на рис. 6.

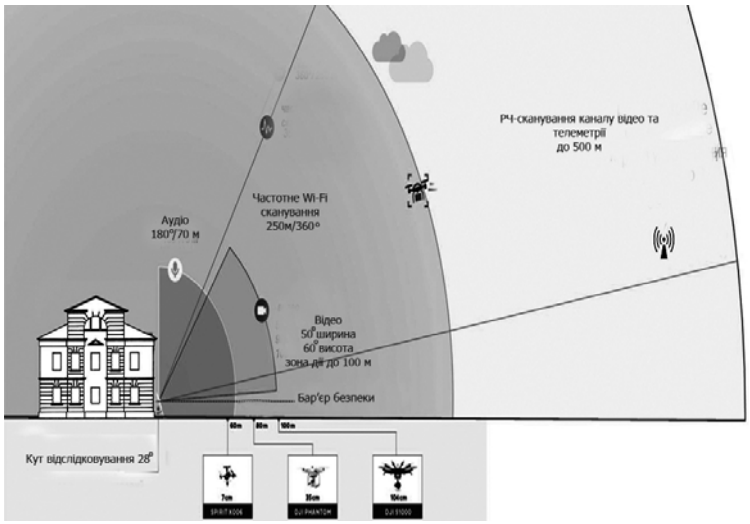


Рис. 6. Сектори роботи сенсорів (датчиків)

Крім місця розміщення об'єкта, значний вплив на систему мають сезонні та погодні коливання, оскільки безпосередньо змінюються фізичні умови роботи сенсорів (датчиків). Відбувається накопичення хибних спрацювань. Крім того, в умовах міста зміна акустичного фону відбувається постійно (шум вулиці, дерев, рух автомобілів (інтенсивність залежно від часу доби), в т.ч. зі спеціальними сигналами тощо. Також існує залежність фізичних параметрів розповсюдження акустичних хвиль від кліматичних умов. На відеосенсори будуть негативно впливати різноманітні джерела освітлення. Представники виробника не дають чітких відповідей щодо можливостей доступу до налаштувань системи або її окремих датчиків (мова йде виключно про зміни порогу чутливості або ступеня довіри).

За інформацією виробників, система проводить документування усіх датчиків, в тому числі проводиться відслідковування руху БПС. У випадку ситуації, яку зображено на рис. 7, відбувається фіксація "атаки" декількох БПС, про що свідчить слід траєкторії польоту. Система передає координати сектору порушення повітряного простору.

Рис. 7. Приклад зображення роботи програмного забезпечення системи Dedrone

За наявності в оснащенні системи не менше 4-х RF-сканерів доступна функція локалізації місця розміщення пульта керування. Система надсилає SMS-повідомлення або в інший спосіб надає координати джерела випромінювання. Для умов міської забудови – це будуть орієнтовні координати (сектор) оскільки відбувається багатократне перевідбиття хвиль від різних об'єктів.

Основні характеристики системи:

– цілодобова робота в автоматичному режимі;

– акустичий та ультразвуковий сенсори виявляють об'єкт на відстані від 50 до 80 м в спектрі від 10 Гц до 96 кГц;

– Wi-Fi сенсор контролює діапазони 2,4 ГГц ISM та 5 ГГц ISM в зоні близької до 360^{R}";

– відеокамера в оптичному діапазоні з роздільною здатністю 1080 пікселів по горизонталі, варіофокальний об'єктив (10 – 90);

– відеокамера в ближньому інфрачервоному (ІЧ) діапазоні з роздільною здатністю 1080 пікселів по горизонталі.

Інший приклад системного підходу до виявлення та протидії БПС – Blighter AUDS (Anti-UAV Defence System) – система, яка розроблена в Великій Британії [5; 6; 9].

Blighter AUDS

Рис. 8. Зовнішній вигляд основних компонентів системи Blighter AUDS

Перший елемент системи – це радар Blighter A400, що працює в сантиметровому діапазоні (Ku band) (на рис. 8 – праворуч). Потужність радара невелика – всього 4 Вт, але цього цілком вистачає, щоб виявляти цілі з ефективною площею відбиття від 0,01 м^2 на відстані від 8 км. Сектор дії радара – 180$^{R"}$.

Завдання радара – виявити БПС, що наближається, якомога раніше. Далі у справу вступає спеціальна довгофокусна відеокамера (дальнього радіуса дії, на рис. 8 – ліворуч).

У системі використовується кольорова камера компанії Chess Synamics з об'єктивом, який здатний 30-кратно змінювати фокусну відстань. Система наведення Gen 3 Cooled. Камера встановлена на спільному електрокерованому підвісі з системою РЕБ компанії Enterprise Control Systems Ltd (три спрямованих антени на рис. 8 – ліворуч).

Отже, сигнал щодо виявлення цілі з радара надходить у систему керування відеокамерами, яка забезпечує "захоплення цілі", її ідентифікацію та прогноз маршруту руху. Якщо БПС продовжує рух у сторону забороненої зони, то після порушення периметра, оператор може дати сигнал на "усунення" вторгнення, для цього вмикається система радіоелектронної боротьби, далі РЕБ, що включає три антени з високим коефіцієнтом підсилення і круговою поляризацією.

Компанія не розкриває параметри системи, але принцип її дії цілком зрозумілий. Система створює локальні перешкоди для БПС на частотах, які використовуються для його зв'язку з пультом дистанційного керування.

Інша система виявлення, розроблена фахівцями відомого світового бренду NEC (Японія), у своєму арсеналі має засоби перехоплення певних видів БПС.

Пропозиції від компанії NEC

Систему, яка запропонувала NEC, можна віднести до систем виявлення без особливих оригінальностей в роботі [8]. Наявний стандартний набір, в основі якого – чутлива оптична камера, яка націлена на певний сектор простору і контролює появу БПС в цьому секторі. Камера може автоматично фокусуватися на БПС навіть у випадку його маневрування. Заявлена дальність виявлення БПС у ясну погоду – 1 км. Крім оптичної, в системі є інфрачервона камера, яка використовується системою в разі настання темноти. Тоді дальність виявлення – 120 м.

До складу комплексу входять також акустичні сенсори, які за допомогою чутливих мікрофонів та підсилювачів здатні виявляти БПС на відстані до сотні метрів.

До складу комплексу входить також детектор випромінювання, який виявляє сигнали обміну БПС з пультом керування оператора (зовнішнього пілота). На основі прийнятої інформації локатор обчислює положення БПС з використанням методу тріангуляції. Чутливість детектора достатня для виявлення сигналів на відстані до 1 км.

Безсумнівна перевага системи – в автоматичному режимі роботи.

Недолік – у відсутності активних режимів блокування польоту БПС у контрольованому просторі.

Мають переваги перед названою інші системи, які активно впливають на БПС при порушенні ним контрольованої території. Це – система AUDS компанії Blighter, яка готова поставити вузьконаправлені перешкоди в зоні дії БПС-порушника. Перешкоди спонукають БПС повернутися в точку запуску або спричинять його відмову. Ще більше можливостей у системи Falcon Schield компанії Selex ES (США) – спеціальне програмне забезпечення та апаратна частина аналізують дані керування БПС – порушником та система намагається перехопити керування, в разі негативного результату генерується радіоперешкода на частоті каналу керування. Приклад результатів роботи системи виявлення наедено на рис. 9.

Рис. 9. Результати виявлення БПС ІЧ-камерою

Personal Drone Detection System

Для боротьби з БПС започатковано проект “Personal Drone Detection System” (США), основна мета якого – виявлення несанкціонованого спостереження за допомогою використання аматорського БПС та його переслідування [8]. Завдяки пристрою під назвою Personal Drone Detection System розробники планують забезпечити захист. Принцип дії системи – локатор виявляє БПС, який наближається до об’єкту в радіусі 15 м з діапазоном робочих частот від 1 МГц до 6,8 ГГц.

За зовнішнім виглядом система нагадує Wi-Fi-роутер (взаємодіють окремі пристрої системи Personal Drone Detection System, які між собою безпосередньо зв’язуються за допомогою технології Wi-Fi), а саме декілька сенсорів, кожен з яких є тим самим датчиком виявлення БПС (рис. 10). БПС виявляються системою як джерела електромагнітного випромінювання, які переміщуються в просторі.

Рис. 10. Зразок реалізації проекту Personal Drone Detection System

Головний модуль управління здатний взаємодіяти з “портативними локаторами” на віддалі до 61 м. Для роботи системи потрібно розмістити по периметру контрольованої зони достатню кількість сенсорів, задіяти командний контролер і синхронізуватися з модулем управління системи. Про наближення БПС сповістить відповідний звуковий сигнал, і буде відправлене повідомлення за допомогою технології GSM. На рис. 11 схематично зображено принцип виявлення БПС, його більш відома назва – принцип тріангуляції, коли за наявністю 3-х азимутів точно визначаються координати джерела випромінювання БПС.

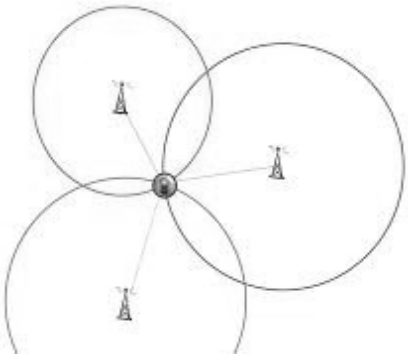


Рис. 11. Принцип виявлення БПС

На рис. 12 показано структурну схему проекту Personal Drone Detection System та взаємозв'язки між її функціональними модулями.

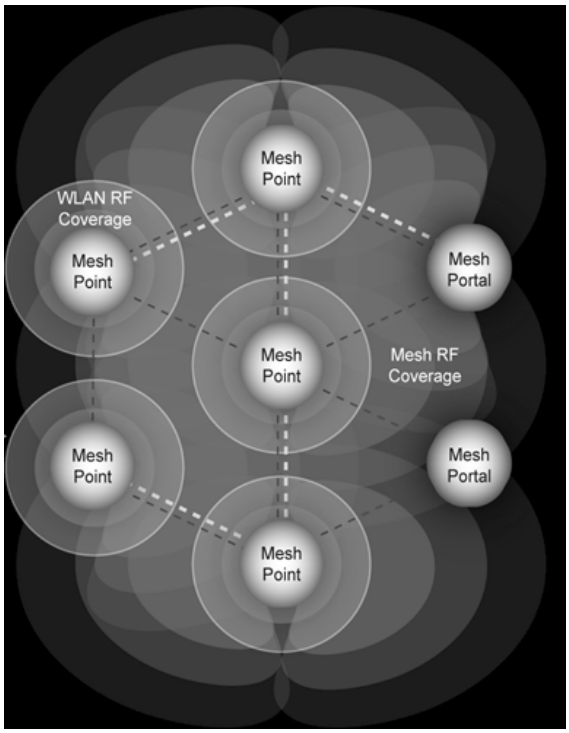


Рис. 12 Структурна схема проекту Personal Drone Detection System

Причиною реалізації цього проекту стала законодавча незахищеність американських громадян, яка виникла внаслідок доступності БПС, що оснащені найбільш сучасними професійними відеокамерами і мають достатньо тривалу автономність польоту. Використання приватних БПС не регулюється Федеральним управлінням цивільної авіації, що веде за собою безвідповідальність і непродуманий вибір маршруту польоту.

Часто траплялося, що БПС ставав причиною інциденту, а саме падіння на чужу приватну власність або винуватцем аварії. Однак знайти власника апарату після його падіння досить часто було не можливо, якщо той не заявив про випадок за власним бажанням. У інших ситуаціях власник БПС легко може залишитися інкогніто.

Альтернативні системи та засоби протидії БПС

Нестандартний спосіб для вирішення поставлених питань можна побачити в рішенні фахівців Південної Кореї, який полягає в тому, що на БПС діють потужними звуковими хвилями. Попередньо в БПС виявили спільну для багатьох із них залежність, яка пов'язана з конструкцією гіроскопа. Останній є практично в кожному БПС, оскільки це основний датчик вимірювання зміни кутів нахилу, зміни курсу тощо. У гіроскопа, як у будь-якої механічної системи, є резонансна частота. Достатньо подіяти на гіроскоп з його резонансною частотою, і він почне видавати параметри, які в результаті призводять до аварії БПС. Це встановив

дослідник Yongdae Kim з південнокорейського інституту KAIST (Korea Advanced Institute of Science and Technology).

Для різних конструкцій гіроскопів резонансні частоти також різні, деякі з них знаходяться у звуковому діапазоні, інші – в ультразвуковому. Дослідники перевірили 15 типів гіроскопів, які застосовуються в популярних БПС. Як правило, це продукти ST Microelectronics і InvenSense. Сім із них були вразливі до акустичної атаки.

У експерименті вчені досліджували вплив звуку на БПС у тестовій камері. За їхніми розрахунками звукова атака потужністю 140 дБ достатня, щоб збивати БПС на відстані 40 метрів.

Гіроскопи відрізняються конструкцією, в деяких з них блокується лише канал орієнтації по горизонталі, цього може бути недостатньо для аварії БПС, тому що в БПС, як правило, є ще магнітометр, який також забезпечує орієнтацію по горизонталі.

Реакції автопілоту БПС у разі втрати каналу керування

Втративши зв'язок з оператором, деякі БПС просто вимушено знижуються вертикально та приземляються на поверхню відносно точки втрати зв'язку з оператором, більш складні моделі можуть повертатися в місце старту в автоматичному режимі. Системи автоматичного повернення в місця старту теж можливо перехопити, створюючи перешкоду на частотах систем супутникової навігації GPS/ГЛОНАСС.

Системи інерційного орієнтування БПС використовуються практично тільки у військових зразках, і можуть бути виведені з ладу внаслідок дії на них потужного спрямованого надвисокочастотного випромінювання.

Сутність інерціальної навігації полягає у визначенні прискорення об'єкта і його кутових швидкостей за допомогою встановлених на об'єкті, що рухається, приладів і пристроїв, а за цими даними – розташування (координат) цього об'єкта, його курсу, швидкості, пройденого шляху та інших. Також визначаються параметри, які необхідні для стабілізації об'єкта і автоматичного управління його рухом.

Висновки

Розглянуті системи та засоби протидії БПС можуть бути рекомендовані для впровадження в діяльність підрозділів поліції (Департамент поліції охорони, підрозділи патрульної поліції Національної поліції України) під час проведення культурно-масових заходів та підрозділів правоохоронних органів Національної гвардії України під час несення служби на важливих державних об'єктах.

Однак слід пам'ятати про переваги та недоліки систем протидії БПС. До основних недоліків слід віднести відсутність гарантованого припинення польоту БПС. Наслідком застосування систем БПС може бути неконтрольоване падіння, в разі чого є висока вірогідність завдання шкоди життю та здоров'ю людей, а також пошкодження майна.

Виникає необхідність у проведенні детальних досліджень систем функціонування керування БПС з метою вдосконалення систем протидії. Комплексний підхід до вдосконалення функціональних модулів систем протидії підвищить позитивний результат їхнього застосування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Повітряний кодекс України : Закон України від 19 травня 2011 р. № 3393-VI [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/ 3393-17.

2. Повітряне право України : навчальний посібник / За заг. ред. д-ра ю.н. В.В. Костицького. – Дрогобич : Коло, 2011. – 552 с.

3. Про радіочастотний ресурс України : Закон України № 1770-III від 01.06.2000 [Електронний ресурс]. – Режим доступу : http://zakon.nau.ua/doc/?code=1770-14.

4. [Електронний ресурс]. – Режим доступу : www.dedrone.com.

5. JDN 2/11 (2011). "Точка зору Великої Британії на безпілотні авіаційні системи" (The UK approach to unmanned aircraft systems). Публікація МО Великої Британії Joint Doctrine Note 2/11, dated 30 March 2011.

6. [Електронний ресурс]. – Режим доступу : http://robotrends.ru/pub/1634/sistema-apollo-shield-obnaruzhit-i-izgonit-_zabludivshiesya_-bla.

7. [Електронний ресурс]. – Режим доступу : http://www.popularmechanics.com/military/weapons/a20914/dod-dhs-buying-drone-jammers/.

8. [Електронний ресурс]. – Режим доступу : http://www.dronedetector.com/.

9. [Електронний ресурс]. – Режим доступу : http://robotrends.ru/pub/1542/bespilotnik-v-polete-ostanovit-blighter-auds.

Отримано 09.11.2016
Рецензент Марченко О.С., к.т.н.

УДК 53.083

О.В. Неня,
кандидат юридичних наук

СУЧАСНІ ТЕПЛОВІЗОРИ ДЛЯ СПЕЦІАЛЬНОГО ТА ПОВСЯКДЕННОГО ЗАСТОСУВАННЯ

Розглянуто принцип роботи тепловізорів, проаналізовано основні технічні параметри, які найбільше впливають як на їх експлуатаційні характеристики, так і на вартість, а також основні переваги і недоліки охолоджуваних і не охолоджуваних тепловізійних систем. Висвітлено сфери та варіанти використання тепловізорів, а також проблемні питання їх застосування підрозділами Збройних сил України, Національної гвардії України та Національної поліції України.

Ключові слова: *тепловізор, ІЧ-випромінювання, температурні характеристики, роздільна здатність, чутливість, відстань виявлення та розпізнавання.*

Рассмотрен принцип работы тепловизоров, проанализировано основные технические параметры, которые наибольшим образом влияют как на их эксплуатационные характеристики, так и на стоимость, а также основные преимущества и недостатки охлаждаемых и неохлаждаемых тепловизионных систем. Освещены сферы и варианты использования тепловизоров, а также проблемные вопросы их применения подразделениями Вооруженных сил Украины, Национальной гвардии Украины и Национальной полиции Украины.

Ключевые слова: *тепловизор, ИК-излучение, температурные характеристики, разрешающая способность, чувствительность, расстояние выявления и распознавания.*

The principle of operation of thermal imagers is considered, an analysis of the main technical parameters, which affect their performance and their cost, as well as the main advantages and disadvantages of cooled and uncooled thermal imaging systems is carried out. The sphere and the use of thermal imagers, as well as problems of their application units of the Armed Forces of Ukraine, National Guard of Ukraine and the National Police of Ukraine are highlighted.

Keywords: *thermal imager, infrared radiation, temperature characteristics, resolution, sensitivity, range of detection and recognition.*

У сучасному світі важко знайти людину, яка ніколи не чула про тепловізори (далі – ТПВ), хоча людей, що хоч раз тримали цей прилад у руках, набереться не так багато. У першу чергу, це пов'язано з тим, що ТПВ поки були і залишаються недешевим "задоволенням".

Застосування ТПВ – це галузь, яка швидко розширюється і має майже необмежений потенціал.

Нині на українському ринку присутня низка виробників і постачальників ТПВ як промислового, так і військового призначення, серед яких: FLIR Systems (США), Fluke Corporation (США), Armasight (США), ATN Corporation (США),

Testo AG (Німеччина), Sofradir (Франція); Pulsar (РФ), Archer (ТОВ "Thermal Vision Technologies" (Україна)) та ін.

Незважаючи на значну кількість пропозицій, висока вартість ТПВ, ціновий сегмент якої починається з кількох десятків тисяч гривень за пристрій з мінімальним набором невисоких технічних характеристик – до мільйонів гривень за ТПВ з високим рівнем якості зображення і хорошим набором додаткових опцій, для багатьох потенційних споживачів так і залишається недосяжною.

Будь-який об'єкт у Всесвіті випромінює енергію, причому велика частина енергії припадає на невидиме людському оку інфрачервоне (далі – ІЧ) випромінювання. Принцип роботи ТПВ заснований саме на цьому явищі: за інтенсивністю ІЧ-випромінювання можна не тільки визначати та ідентифікувати об'єкти різної природи або навіть ділянки однорідної на вигляд поверхні, а й досліджувати багато їх прихованих властивостей.

ТПВ повністю незалежні від зовнішнього освітлення та реєструють тільки ІЧ-випромінювання об'єктів. Як оптичні системи в них використовуються лінзи з германію, оскільки звичайне скло ІЧ-випромінювання не пропускає. З матриці приладу інформація надходить до електронної схеми, де зберігається колірна карта температур (кожній температурі відповідає певний колір і його яскравість), обробляється і виводиться на дисплей в окулярі приладу. У більшості систем реалізовано чорно-біле кодування. Як правило, тепловізійні прилади розділяють на вимірювальні та прилади спостереження. ТПВ для спостереження простіші, а значить і вартість їх нижча. Вони дають змогу бачити ІЧ-промені, трансформуючи їх у видиму для людського ока частину спектра. А ось вимірювальні ТПВ дають змогу ще й отримати повну картину розподілу температур (побудувати теплові карти досліджуваних об'єктів) [1].

Сучасний ТПВ дає змогу обчислювати інтенсивність ІЧ-випромінювання, визначати температурні характеристики, а також з легкістю обчислювати і передавати координати джерела такого випромінювання. При цьому будь-які цифрові показники ТПВ можна переводити в графічне зображення, за яким можна оцінювати різні характеристики об'єкта.

За допомогою ТПВ можна миттєво виміряти температуру десятків тисяч точок будь-якого об'єкта як живої, так і неживої природи, проте холодні об'єкти практично неможливо розрізнити, вони на екрані ТПВ зображуються чорним кольором.

Перші тепловізійні системи були громіздкими, повільними і мали низьку роздільну здатність. Вони будували зображення за допомогою електронно-променевої трубки, а запис зображення можна було здійснювати тільки за допомогою фотографії або магнітної стрічки.

Наприкінці 80-х рр. минулого століття відбулася революція в області технологій виготовлення тепловізійних систем – стали доступними для широкого застосування матричні приймачі випромінювання (матриці в фокальній площині (FPA)), які складаються з масиву ІЧ-приймачів випромінювання, розташованих у фокальній площині об'єктива.

Це був значний прогрес, який привів до підвищення якості зображення і просторової роздільної здатності.

Матричні приймачі випромінювання сучасних ТПВ мають роздільну здатність від 16x16 до 640x480 пікселів і на сьогодні є однією з найдорожчих частин ТПВ,

і значною мірою впливають на його ціну. Є загальне правило – чим вища роздільна здатність детектора, тим дорожче ТПВ і тим кращі його технічні та експлуатаційні характеристики. При цьому, роздільна здатність ТПВ прямо залежить від його типу, – з охолоджуваною або не охолоджуваною матрицею.

Охолодження матриці робить прилад більш точним, але й більш важким і громіздким. Неохолоджувані матриці використовуються в портативних приладах. Такі матриці, як правило, виробляють з аморфного кремнію або оксиду ванадію на різних підкладках, включаючи германій або арсенід галію. Неохолоджувані ТПВ здатні розрізняти різницю температур в 0,1 °С, але мають відносно невелику дальність розпізнавання [2].

Основними перевагами охолоджуваних ТПВ є:

• краща роздільна здатність – вони працюють у більш короткохвильовому діапазоні порівняно з неохолоджуваними ТПВ. З огляду на так званий ефект "вікон" прозорості атмосфери всі ТПВ працюють у двох спектральних діапазонах ІЧ-випромінювання – короткохвильовому (3–5,5 мкм) діапазоні, який більш характерний для охолоджуваних ТПВ (як правило, дальнього радіуса дії), і довгохвильовому (7–14 мкм) – для неохолоджуваних (як правило ближнього радіуса дії).

Цей ефект пов'язаний з молекулярним поглинанням, яке є головною причиною ослаблення випромінювання, причому найбільш сильно випромінювання поглинається парами води, вуглекислим газом і озоном.

Крім того, в розпорядженні розробників тепловізійного обладнання є два типи приймачів (приймаюча матриця), що працюють саме в цих діапазонах довжин хвиль. Також необхідно зазначити, що максимуми щільності випромінювання від об'єктів, що мають температури в інтервалі від 0 до 1000 °С, розташовуються в зазначених хвильових інтервалах. Наприклад, максимальна щільність випромінювання, яка приходить від об'єкта, що має температуру 27 °С, відповідає довжинам хвиль близько 10 мкм. Довгохвильовий діапазон характеризується більш високою температурною роздільною здатністю, що особливо важливо в умовах, коли температура об'єкта обстеження близька до температури навколишнього середовища.

• мають більшу контрастну чутливість – охолоджуваний ТПВ розрізняє перепади в 20 мк при діафрагмі, що дорівнює 5, тоді як неохолоджуваний болометричний – близько 50 мк, при дотриманні умови, що діафрагма дорівнює 1. Це є наслідком різної фізики фотоелектричного і терморезистивного ефектів;

• поєднання перших двох чинників дає третю перевагу – набагато більшу – до 10 км відстань виявлення об'єкту.

Що стосується недоліків охолоджуваних систем, то серед них можна назвати такі:

– висока споживана потужність, викликана роботою пристроїв охолодження;

– тривалий час охолодження – між включенням ТПВ та отриманням зображення може пройти кілька хвилин;

– обмежений термін експлуатації, який прямо залежить від терміну напрацювання на відмову охолоджуючого елемента, – зазвичай це кілька тисяч годин безперервної роботи.

Основними перевагами неохолоджуваних ТПВ є:

– робочий діапазон краще пристосований для спостереження в умовах диму, туману, смогу – в діапазоні 8–14 мікрон ІЧ-випромінювання не поглинається ні парами води, ні вуглекислим газом;

– порівняно (з охолоджуваними ТПВ) невеликий розмір і вага;
– включення і отримання зображення відбувається одночасно;
– значно менша споживана потужність у порівнянні з охолоджуваними ТПВ;
– значний термін напрацювання на відмову.

Ще одним важливим параметром ТПВ є його термочутливість або похибка при вимірюванні температури в двох сусідніх точках. Чим менше показник, тим вища термочутливість, і тим якісніше ІЧ-зображення виводить ТПВ.

ТПВ, що має термочутливість 0,025–0,05 °С, дає змогу розрізняти практично всі предмети, які знаходяться при однаковій температурі.

Ще одним фактором, що істотно впливає на вартість і експлуатаційні характеристики ТПВ, є частота зміни кадрів, яка коливається, як правило, від 9 до 50–60 Гц.

Частота кадрів – це величина, що характеризує швидкість зміни зображення на екрані ТПВ. Низьке значення частоти зміни кадрів ТПВ (9 Гц) свідчить про те, що зміна зображень буде помітна для оператора. Навіть при повільному переміщенні користувача разом з ТПВ цей ефект посилюється. Для тривалої роботи під час руху або зі сценою (картиною), що постійно змінюється перед об'єктивом ТПВ, рекомендуються моделі з частотою кадрів 50/60 Гц [3].

Серед чинників, що також впливають на вартість ТПВ можна назвати наявність вбудованої відеокамери та її роздільну здатність, а також додаткові опції типу "картинка в картинці" – накладення звичайного зображення на ІЧ.

Програмне забезпечення для полегшення аналізу та підготовки звітів мають практично всі сучасні моделі ТПВ [4].

Глибоке освоєння систем теплобачення може відкрити великі можливості, що не використовувалися раніше, як окремою людиною, так і людством у цілому. Починаючи з харчової промисловості та аж до космічних апаратів, тепловізійні можливості стають із кожним днем усе більш необхідними.

Усі сучасні ТПВ є безконтактними вимірювальними приладами. Як уже зазначалося, вони не тільки графічно відображають різниці температур, а й вимірюють і зберігають у пам'яті значення температури в кожній точці зображення об'єкта.

Тепловізійні системи орієнтовані на застосування в різних галузях, мають широкий спектр функціональних можливостей. Так, наприклад, застосування ТПВ зумовлено необхідністю пошуку гарячих (іноді – холодних) місць на температурному полі, наявність яких свідчить про порушення нормального режиму експлуатації об'єкта або обладнання, небезпечних дефектах, втрати або надлишкового використання енергії тощо.

Використовуючи ТПВ, фахівець може виявити найрізноманітніші несправності і миттєво визначити проблемну зону на чіткому і яскравому ІЧ- зображенні. Це можуть бути і трубопроводи, і мікросхеми та резистори, і технологічні резервуари. У ТПВ можна побачити ланцюги, що не працюють, обриви і замикання в нагрівальному елементі. Оскільки практично будь-який несправний вузол або агрегат енергообладнання має теплову аномалію, ТПВ прискорює пошук таких вузлів і ділянок, а також може забезпечити додаткову якісну оцінку зробленому ремонту.

Отже, ТПВ застосовуються для: різноманітних діагностичних досліджень, виявлення дефектів або порушення теплоізоляції й інших тепловтрат на

різноманітних об'єктах, контролю цілісності об'єктів, визначення теплоізоляційних властивостей матеріалів тощо.

Основними сферами застосування ТПВ є [5–7]: будівництво (див. рис. 1); електрообладнання та електронна техніка; паливно-енергетичний комплекс (див. рис. 2); автомобільна, хімічна та авіакосмічна промисловість; металургія (див. рис. 3); машинобудування; суднобудування; медицина тощо [8–10].

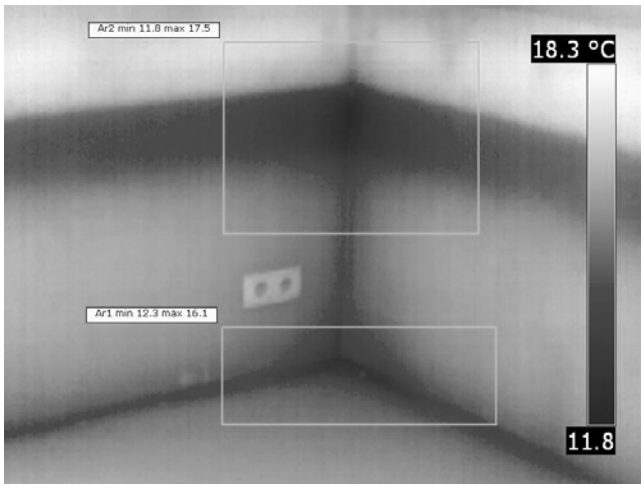


Рис. 1. Зображення на екрані ТПВ області, де не дотримується нормативний рівень теплоізоляції огороджуючих конструкцій під час використання функції "визначення дефекту теплоізоляції"

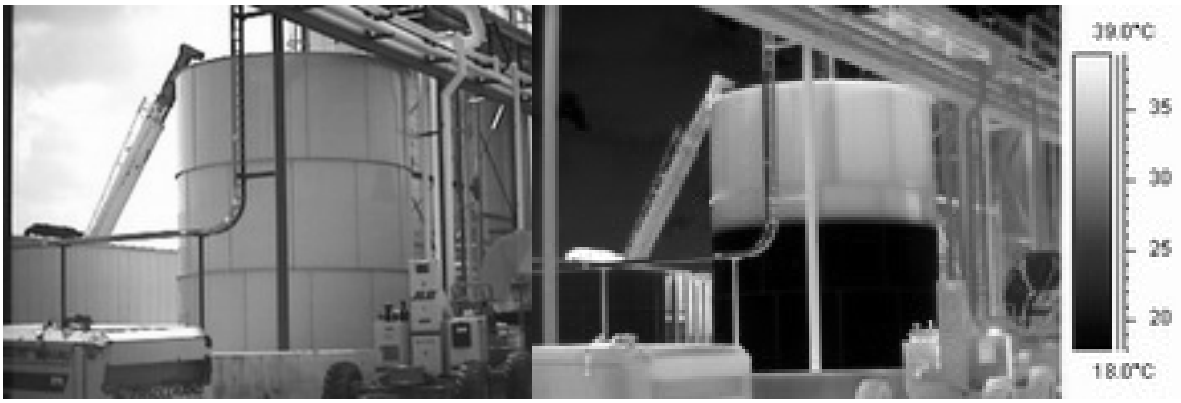


Рис. 2. Перевірка рівня рідини в резервуарах

Теплобачення може мати і такі варіанти використання, як: науково-дослідна діяльність; контроль автоматичних виробничих процесів; тестування компонентів і оболонок; детекція газу; видобуток корисних копалин; перевірка сонячних панелей; ветеринарія; пожежогасіння; пошуково-рятувальні роботи (в тому числі полегшення роботи пожежних рятувальників); астрономія; визначення забруднень; освіта; вимір температурних режимів під час виготовлення паперу, виробництві скла, гуми і пластику, бетонних і залізобетонних виробів; вивчення процесів теплопередачі в моделях, які досліджують в аеродинамічних трубах; дефектоскопія матеріалів та окремих конструкцій під час проведення статичних і динамічних випробувань; персональне використання тощо.

Рис. 3. Контроль температурних режимів доменних печей

Актуальним є використання тепловізійної техніки в мистецтві, зокрема для *спостереження* за станом настінного живопису, картин, кінематографічної продукції, *створення* спеціальних візуальних ефектів, *виявлення* дефектів у структурі фресок, *розкриття* оригіналів, прихованих більш пізніми записами. Так, мистецтвознавці і хранителі музею "Зібрання Філліпса" (Phillips Collection) у Вашингтоні (див. рис. 4), використавши ІЧ-технологію для вивчення шедевра Пабло Пікассо "Блакитна кімната", змогли побачити прихований під мазками фарби портрет людини в жакеті і краватці-метелику [11]. На дивний рельєф мазків звернули увагу фахівці ще в 1954 р., що могло вказувати на наявність прихованого шару. Тільки в 1990-х рр. рентген картини показав нечітке зображення чогось під шаром живопису. У 2008 р. ІЧ-зйомка вперше показала обличчя бородатого чоловіка і руку з трьома кільцями на пальцях [11].

Рис. 4. Використання ІЧ-камери під час роботи мистецтвознавців

Також ефективними ТПВ можуть бути на залізничному транспорті та вокзалах, у метрополітені та в аеропортах. Окрім *спостереження* за буксами, тиристорами, вагонами-холодильниками, енергогосподарством; *виявлення* перегрівів, витоків тепло- і електроенергії, дефектів теплоізоляції в тепловозах і рухомому складі, тепловізійна техніка може бути дуже корисною для контролю пасажиропотоку на наявність осіб з підвищеною температурою тіла. Метою виявлення таких осіб є запобігання поширенню небезпечних захворювань. Використання ТПВ з автокомпенсацією температури дає змогу визначити підвищену температуру тіла людини і, провівши додаткове обстеження (див. рис. 5), запобігти переміщенню через кордон хворих пасажирів, зокрема для виявлення заражених свинячим грипом) [12].

Рис. 5. Виявлення пасажирів з підвищеною температурою

Активно зростає попит на використання ТПВ у сфері охорони і безпеки – для охорони периметра урядових будівель і споруд; *забезпечення безпеки військових об'єктів; прикордонного патрулювання, митного огляду, спостереження* за рухом об'єктів тощо.

Найважливішою сферою, в якій нині застосовуються ТПВ, стала військова справа. Однією зі значних перешкод для військових операцій завжди був нічний час. Також належним чином спостереження неможливе в умовах поганої видимості: в тумані, диму, під час снігопаду та інших подібних явищах. Раніше для виявлення противника в темряві в армії використовували так звані прилади нічного бачення (далі – ПНБ). Проте принцип роботи ТПВ дає йому значні переваги. Справа в тому, що ПНБ вловлює видиме світло і підсилює сигнал і, таким чином, дає змогу бачити за умов поганого освітлення. Використання такого приладу в зазначених вище складних умовах видимості, на відміну від ТПВ, не дає ефекту – він просто зробить туман яскравіше, а в повній темряві, наприклад, в приміщенні, ПНБ не покаже нічого.

ТПВ застосовуються збройними силами як прилади нічного бачення для виявлення теплоконтрастних цілей (живої сили і техніки) в будь-який час доби, незважаючи на використання противником засобів оптичного маскування у видимому діапазоні (наприклад, камуфляж) [13]. Термографічна картина може розповісти операторові ТПВ як про розташування цілі, так і про її розміри, а також інші параметри об'єкта.

Новітні ТПВ дають змогу вести розвідку і визначати цілі на значно більших відстанях в обмежених умовах видимості, а також передавати отримані дані цифровим каналом і продовжувати пошук інших цілей. Більш чітке зображення, що отримується, дає змогу підвищувати ступінь ситуаційної обізнаності, зокрема екіпажам бронетехніки, що дає перевагу під час ведення бою. ТПВ став важливим елементом прицільних комплексів ударної армійської авіації та бронетехніки.

ТПВ на військовому літаку або вертольоті дає змогу вловити в ІЧ-діапазоні хвиль ціль і нанести точковий удар навіть в умовах абсолютної темряви або густого туману.

Застосовуються тепловізійні приціли і для ручної стрілецької зброї, хоча більшою мірою орієнтовані на використання в бойовій техніці. Адже навіть найкомпактніший з приладів цього типу більш громіздкий, ніж обладнання з електронно-оптичним перетворенням зображення 2-го або 3-го покоління, і вимагає більш потужного електроживлення, необхідного для охолодження тепловипромінювача. Крім того, ТПВ, як ми вже зазначали, мають високу вартість: типовий військовий зразок має вартість більше 10 тисяч доларів.

Цікавим фактом є те, що вже в 1939-1940 рр. у СРСР були дуже серйозні напрацювання щодо ІЧ-приладів. Так, були розроблені та випробувані ІЧ-прилади нічного бачення "Шип" і "Дудка" для нічного водіння танків. Також були створені теплопеленгатори для ВМФ. Однак потім з невідомих причин роботи зі створення ТПВ у СРСР були згорнуті, і лідерство у цій галузі втрачено. У 80-х рр. на основі зарубіжних зразків у СРСР були розроблені і запущені в серійне виробництво ТПВ нульового покоління ("Посібник-1") і першого покоління ("Посібник-2", "Агава-2"). ТПВ "Агава-2" були встановлені на танки Т-90 і деякі модифікації Т-80. Також налагоджено випуск тепловізійних прицілів для стрільби протитанковими керованими реактивними снарядами "ПТКРС".

Наприкінці 90-х рр. минулого століття військові тепловізійні технології в Україні (до речі, як і в Росії) практично не розвивалися, що призвело до значного відставання в цій сфері від країн Заходу [14] .

Нині висока затребуваність у ТПВ українськими військовими у зв'язку з проведенням АТО на Сході України висвітлили певні проблемні питання, зокрема те, що в Україні не налагоджено поряд з іншим військовим знаряддям і повний цикл виробництва ТПВ (зокрема, такого ключового компоненту ТПВ, як мікроболометр). Відсутність такого виробництва, у свою чергу, зумовлює аналогічну проблему з ремонтом закуплених тепловізійних пристроїв іноземного виробництва, а також переданих у рамках допомоги різними країнами.

Разом з цим, окремі складнощі в оснащенні тепловізорами виникають через віднесення цих засобів до товарів подвійного використання [15].

На сьогодні існує проект "Тепловізори для Армії України", автори якого акцентують увагу на таких трьох основних проблемах щодо забезпечення ТПВ Збройних сил України, як: 1) високі ціни; 2) відсутність у постачальників певних "ходових" моделей ТПВ; 3) недостатній асортимент продукції.

З огляду на висвітлені проблеми, основною метою автори проекту вбачають налагодження виробництва всіх ключових компонентів для ТПВ в Україні [16].

Одним зі значних кроків у цьому напрямі стало включення черкаського науково-виробничого комплексу "Фотоприлад" до програми держзамовлення на 2015 рік, у рамках якої підприємство планувало виготовляти ТПВ та прилади нічного бачення [17].

Цікавою також є інформація центру волонтерів "Народний проект" щодо їх замовлення на виготовлення малогабаритних тепловізійних прицілів українського виробництва TUA336T2-8x40-9.

Основні характеристики цього малогабаритного пристрою, які позиціонуються волонтерами, такі [18]:

Роздільна здатність детектора (мікроболометра), пікс.	– 336x256
Цифровий zoom, x	– 2x, 4x
Дистанція виявлення об'єкта, м	– 1500

Дистанція розпізнавання, м – 600
Роздільна здатність дисплея, пікс. – 800x600
Габарити, мм – 70x65x60

Отже, сподівання на розвиток вітчизняного виробництва ТПВ є небезпідставним.

Новітні розробки задля підвищення характеристик, зменшення розмірів і енергоспоживання ТПВ пропонують нові можливості не тільки бойовим підрозділам, а й підрозділам Національної поліції України, зокрема технікокриміналістичного забезпечення, слідчих та патрульних.

Основні напрями застосування тепловізійних приладів у правоохоронній діяльності можна розділити на такі три групи:

– тактичні дії;
– дослідження речових доказів;
– попередження злочинів.

У криміналістичних цілях ТПВ можуть бути застосовані для:

– виявлення невидимих, нестійких термічних слідів;
– дослідження речових доказів і осіб;
– фіксації невидимих термічних слідів і результатів спостереження та дослідження об'єктів і місць кримінального правопорушення тощо.

Під час огляду місць кримінального правопорушення ТПВ можна використовувати для збирання так званих термічних слідів, тобто пошуку, виявлення та фіксації невидимих слідів.

Прикладом таких невидимих термічних слідів можуть бути сліди, що виникли внаслідок:

– сидіння або лежання людини на різних поверхнях (якщо це відбулося недавно);
– дотику людини руками до різних предметів, наприклад, до знарядь злочину (якщо це відбулося недавно);
– дистанційного визначення факту експлуатації транспортного засобу (за теплом, що виділяється двигуном і агрегатами);
– дистанційного визначення місця горіння, яке намагалися приховати, тощо.

Під час обшуку на відкритій місцевості ТПВ можна успішно застосовувати для пошуку таких об'єктів:

– зниклих осіб і тих, що переховуються (див. рис. 6), а також тварин;
– нагрітих предметів (речей) недавно покинутих (наприклад, автомобілів та інших транспортних засобів) або захованих злочинцем (знарядь злочину, трофеїв і т. ін.);
– укриттів, схронів тощо [19].

Особливо ефективним є застосування ТПВ під час пошуку на місцевості людей, що переховуються, оскільки тепло (ІЧ-випромінювання) здатне проникати крізь візуально непрозорі для ока людини перепони, такі як листя дерев, різноманітні матеріали тощо.

Під час проведення слідчих (розшукових) дій у приміщеннях ТПВ дає змогу:

Рис. 6. Підозрюваний ховається за листям дерев

– встановити факт недавнього користування приміщенням;

– визначати кількість осіб, що недавно перебували в цьому приміщенні;

– виявляти предмети, якими недавно користувалася і яким чином (на них сиділи, лежали, тримали в руках тощо).

ТПВ можуть бути успішно застосовані й у багатьох інших сферах діяльності підрозділів Національної поліції України (див. рис. 7), як засіб спостереження вночі та в умовах обмеженої видимості, наприклад крізь дим, туман (див. рис. 8), а також у тих випадках, у яких зараз використовуються звичайні прилади нічного бачення і підсилювачі світла (яскравості) [20–23].

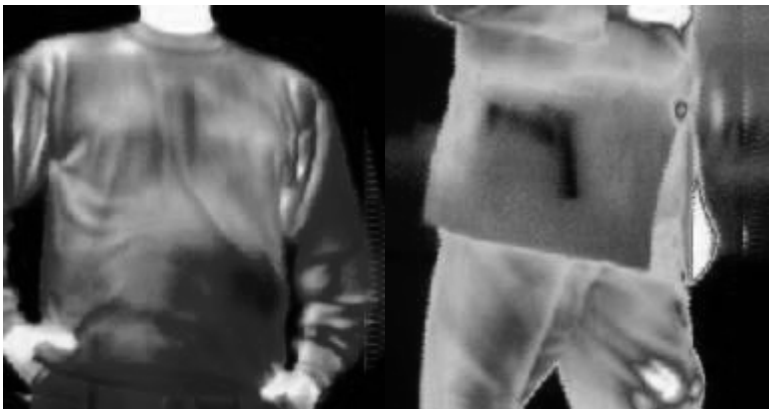


Рис. 7. Пістолет у кишені піджака і за поясом штанів під светром

Рис. 8. За допомогою ТПВ поліцейські бачать у темряві

Отже, широке використання окремими підрозділами Національної поліції України тепловізійних систем є одним із напрямів підвищення ефективності діяльності правоохоронних органів, що дасть змогу оптимізувати їх роботу.

Зокрема, п. 4 розділу ІІ Інструкції про службу прикордонних нарядів Державної прикордонної служби України, яка затверджена наказом МВС України від 19.10.2015 № 1261, регламентовано використання цими підрозділами технічних засобів тепловізійного спостереження, що є позитивним чинником для подальшого їх упровадження в діяльність правоохоронних органів.

Вочевидь, питання впровадження ТПВ у роботу працівників Національної поліції України потребує ретельного вивчення з урахуванням міжнародного досвіду.

Одним із аспектів такого вивчення може стати апробація наявних на ринку тепловізійних пристроїв працівниками відповідних підрозділів Національної поліції України в реальних умовах несення служби із наступним формуванням вимог до технічних характеристик таких пристроїв, а також розроблення нормативно-правової бази їх застосування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тепловизоры [Электронный ресурс]. – Режим доступа : http://cobrashop.com.ua/catalog/archer.

2. *Сычев В.* Американцы создали графеновый неохлаждаемый тепловизор / В. Сычев [Электронный ресурс]. – Режим доступа : https://nplus1.ru/news/2015/11/09/thermo.

3. *Никитин С.* Тепловизоры: все не так просто / С. Никитин // Алгоритм Безопасности, 2011. – № 3 [Электронный ресурс]. – Режим доступа : http://www.algoritm.org/arch/arch.php?id=52&a=1007.

4. Станут ли тепловизоры более доступными? // Электротехнический рынок. – 2011. – № 5(41) [Электронный ресурс]. – Режим доступа : http://www.algoritm.org/arch/arch.php?id=52&a=1007.

5. Области применения тепловизоров [Электронный ресурс]. – Режим доступа : http://www.thermoview.ru/articles/primenenie/;

6. Сферы применения тепловизоров [Электронный ресурс]. – Режим доступа : http://www.ntcexpert.ru/component/content/article/44-k44/523-sfery-primenenija-teplovizorov;

7. Тепловизоры, тепловизионное обследование и диагностика [Электронный ресурс]. – Режим доступа : http://www.infra.su/infrared/inspect.php.

8. Области применения тепловизоров [Электронный ресурс]. – Режим доступа : http://www.thermoview.ru/articles/primenenie/;

9. Тепловизоры в нефтегазовом комплексе [Электронный ресурс]. – Режим доступа : http://www.p640.ru/oilgas.htm.

10. Тепловизоры в металлургии и химической промышленности [Электронный ресурс]. – Режим доступа : http://www.p640.ru/metallurgy.htm.

11. *Лездин Д.* Инфракрасная камера обнаружила скрытую живопись Пикассо / Д. Лездин [Электронный ресурс]. – Режим доступа : http://teplonadzor.ru/pikasso/l.

12. Тепловизоры в пунктах пограничного пропуска помогут выявить больных гриппом [Электронный ресурс]. – Режим доступа : http://www.belta.by/society/view/teplovizory-v-punktah-pogranichnogo-propuska-pomogut-vyjavit-bolnyh-grippom-178057-2016/.

13. МВД приобрело 57 тепловизоров [Электронный ресурс]. – Режим доступа : http://www.unian.net/1001687-x.html.

14. Тепловизоры (инфракрасные ПНВ) [Электронный ресурс]. – Режим доступа : http://www.modernarmy.ru/article/179.

15. Про затвердження Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання : Постанова Кабінету Міністрів України від 28 січня 2004 р. № 86 [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/86-2004-%D0%BF.

16. Тепловизоры для Армии Украины [Электронный ресурс]. – Режим доступа : http://t4a.com.ua/.

17. Черкасский завод получил заказ на производство тепловизоров [Электронный ресурс]. – Режим доступа : http://vestiua.com/ru/news/20141020/58359.html.

18. На линию огня отправили отечественные тепловизоры [Электронный ресурс]. – Режим доступа : http://www.gogetnews.info/news/society/90243-na-liniyu-ognya-otpravili-otechestvennye-teplovizory-video.html.

19. Тепловизор для охраны и безопасности [Электронный ресурс]. – Режим доступа : http://xn––8sbnbifmf0aignkr8d0dza.xn–p1ai/?p=6_2.

20. *Рудаков Б.В.* Основы специальной техники органов внутренних дел (общая часть) :учеб. пос. / Б.В. Рудаков, Д.А. Бражников, А.М. Щукин. – Тюмень : Тюменский институт повышения квалификации сотрудников МВД России, 2013. – 354 с.

21. *Ковалев А.В.* Тепловидение сегодня / А.В. Ковалев, В.Г. Федчишин, М.И. Щербаков // Специальная техника, 1999. – № 3. – С. 13–18.

22. *Гаврилов Л.Н.* Применение техники термовидения / Л. Н. Гаврилов, Н.Л. Гаврилов // Актуальные вопросы применения специальных технических средств в оперативно-розыскной деятельности ОВД : труды X межрегиональной научно-практической конференции. – С.-Пб. – 2004. – С. 183.

23. Тепловизизоры и тепловизионные технологии в криминалистике [Электронный ресурс]. – Режим доступа : http://www.ilt.kharkov.ua/bvi/technology/tk1/kriminalistic_r-1.html.

24. Голландская полиция использует тепловизоры FLIR [Электронный ресурс]. – Режим доступа : http://www.secnews.ru/pr/17187.htm#axzz46uguA3ce.

25. *Алексеев А.* Тепловизоры становятся меньше, а видят всё лучше / А. Алексеев [Электронный ресурс]. – Режим доступа : https://topwar.ru/38270-teplovizory-stanovyatsya-menshe-a-vidyat-vse-luchshe.html.

Отримано 16.11.2016
Рецензент Марченко О.С., к.т.н.

НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ

УДК 347.948:001.89

Р.С. Филь,
здобувач ДНДІ МВС України,
С.П. Филь,
здобувач ДНДІ МВС України

ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО СУДОВУ ЕКСПЕРТИЗУ ОБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

У статті розглянуто загальні положення про судову експертизу об'єктів права інтелектуальної власності. З'ясовано основні вимоги до атестації судових експертів та сучасний стан єдиних методик проведення судових експертиз для різних об'єктів права інтелектуальної власності. Проаналізовано порядок призначення судових експертиз об'єктів права інтелектуальної власності з кримінальних, цивільних та адміністративних справ. Вказано основні проблеми та можливі шляхи їх подолання.

Ключові слова: *права інтелектуальної власності, судова експертиза у сфері інтелектуальної власності, методики проведення судової експертизи.*

В статье рассмотрены общие положения о судебной экспертизе объектов права интеллектуальной собственности. Выяснены основные требования к аттестации судебных экспертов и современное состояние единых методик проведения судебных экспертиз для различных объектов права интеллектуальной собственности. Проанализирован порядок назначения судебных экспертиз объектов права интеллектуальной собственности по уголовным, гражданским и административным делам. Указаны основные проблемы и возможные пути их преодоления.

Ключевые слова: *права интеллектуальной собственности, судебная экспертиза в сфере интеллектуальной собственности, методики проведения судебной экспертизы.*

Paper deals with general provisions of forensic examination of intellectual property rights. Basic requirements for the certification of forensic experts and the current state of uniform methods of forensic examinations for different intellectual property rights are highlighted. The analysis of the procedure of an appointment of judicial examination of intellectual property rights through criminal, civil and administrative cases is carried out. The key problems and possible ways to overcome them are noted.

Keywords: *intellectual property rights, judicial expertise in intellectual property, methods of forensic examination.*

Розвиток інтелектуальної власності створює сприятливе середовище для технологічних інновацій та художньої творчості, що, у свою чергу, заохочує інвестиції, полегшує трансфер технологій, у результаті чого збільшується асортимент товарів і послуг, підвищується їхня якість, з'являються нові можливості для розвитку особистості.

Державна система правової охорони та захисту інтелектуальної власності спрямована на використання продукту інтелектуальної діяльності як стратегічного

ресурсу в системі формування національного багатства та підвищення конкурентоспроможності економіки нашої країни, прискорення інноваційного розвитку та інтеграції України в міжнародний економічний простір.

Особливість інтелектуальної власності полягає в тому, що вона охоплює сукупність галузей економіки і видів суспільної діяльності, які не беруть безпосередньої участі у створенні матеріальних благ. Ці галузі виробляють унікальний продукт – інтелектуальний. Саме такий продукт є одним з основних і необхідних елементів розвитку суспільства і прогресу людства загалом. Об'єкти права інтелектуальної власності (далі – ПІВ) на відміну від об'єктів права власності не завжди мають матеріальну форму. Більше того, їх економічна цінність не залежить від матеріального носія, на якому вони містяться – це лише спосіб передачі авторських думок та ідей іншим особам. У результаті об'єкти ПІВ стають вразливими для недобросовісного використання без згоди їх власника та предметом правопорушень проти ПІВ.

За даними Генеральної Прокуратури України, станом на жовтень 2016 року було відкрито 313 кримінальних справ за фактом скоєння кримінальних правопорушень, пов'язаних з порушенням права інтелектуальної власності: 167 кримінальних справ щодо порушень авторського права і суміжних прав (за ст. 176 Кримінального Кодексу України (далі – КК України)), 14 справ – незаконного використання винаходу, корисних моделей, промислових зразків, топографічних інтегральних мікросхем, сортів рослин, раціоналізаторських пропозицій (ст. 177 КК України) та 132 справ – незаконного використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення погодження товару (ст. 229 КК України) [1; 2, ст. 176, 177 та 229].

Відповідно до статистичного бюлетеню Державної служби статистики України "Адміністративні правопорушення в Україні в 2015 році" протягом звітного року було зафіксовано 187 адміністративних правопорушень, що посягають на об'єкти права інтелектуальної власності, з них тільки по 154 справам прийнято рішення [3]. Також усе частіше органи доходів і зборів України фіксують порушення митних правил при переміщенні товарів через митний кордон України з порушенням прав інтелектуальної власності. Про що свідчать зазначені вище дані Державної служби статистики України, а саме що за 2015 рік було порушено 21 справу про порушення митних правил за фактом ввезення на митну територію України контрафактних товарів. Враховуючи, що дані наведені без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини зони проведення антитерористичної операції, то можна припустити, що реальні показники за цей рік можуть збільшитися.

Будь-яка особа, якій належать майнові та немайнові права на об'єкти ПІВ, має право звернутися до суду за захистом своїх прав на ці об'єкти. На сьогодні захист прав і законних інтересів авторів та правовласників у судовому порядку є найбільш дієвим інструментом у вирішенні спорів. Специфічний характер судових спорів у сфері інтелектуальної власності вимагає залучення фахівців, наділених спеціальними технічними та правовими знаннями, тобто судових експертів.

Серед вагомих наукових досліджень учених щодо питання захисту прав інтелектуальної власності можна виділити Г.О. Андрощука, О.Ф. Дорошенка, М.В. Ковіню, А.Г. Жарінову, О.П. Орлюк, В.І. Нежибореця, Н.М. Мироненка, М.В. Паладія, С.В. Ващенка, Г.В. Корчевного, І.Г. Запорожець, О.М. Головкову,

І.О. Личенка, Ф.О. Кіріленка та ін. Дослідженню питання проведення експертизи у сфері інтелектуальної власності присвячено багато праць, зокрема роботи: А.С. Штефан, О.Ф. Дорошенка, О. Бутнік-Сіверського, Г.К. Дорожко, Н.В. Марченко, І.І. Брус, Ю.Г. Охромєєва, В.М. Шерстюк, Л.Ю. Патроманської, О.О. Разборської, Г.О. Лисенко, Г.В. Прохоров-Лукіна, Н.В. Мещерякової, Т.М. Маслової, Р.Я. Лемик тощо.

Враховуючи фрагментальні наукові дослідження наукових та практичних засад проведення судової експертизи у сфері інтелектуальної власності та актуальність цього питання, воно потребує подальшого наукового аналізу. Саме тому метою статті є аналіз загальних положень про судову експертизу об'єктів права інтелектуальної власності в Україні.

Судово-експертна діяльність здійснюється з метою забезпечення правосуддя України незалежною, кваліфікованою і об'єктивною експертизою, орієнтованою на максимальне використання досягнень науки і техніки. Під поняттям "судова експертиза" розуміють дослідження, які здійснені експертом на основі спеціальних знань матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини справи, що перебуває у провадженні органів досудового розслідування чи суду. Експерти у своїй діяльності керуються Законом України "Про судову експертизу", який визначає основні правові, організаційні та фінансові засади судово-експертної діяльності в Україні [4, ст. 1].

Судовий експерт зобов'язаний: належно проводити повне дослідження і надати обґрунтований та об'єктивний письмовий висновок на вимогу особи або органу, які залучили експерта, судді, суду надати роз'яснення щодо даного ним висновку та заявляти самовідвід за наявності передбачених законодавством підстав, які виключають його участь у справі [4, ст. 12].

Згідно із Законом України "Про судову експертизу" судовим експертам надається право: 1) ознайомлюватися з матеріалами справи, що стосуються предмета судової експертизи, і подавати клопотання про надання додаткових матеріалів; 2) вказувати у висновку експерта на виявлені в ході проведення судової експертизи факти, які мають значення для справи і з приводу яких йому не були поставлені питання; 3) з дозволу особи або органу, які призначили судову експертизу, бути присутнім під час проведення слідчих чи судових дій і заявляти клопотання, що стосуються предмета судової експертизи; 4) подавати скарги на дії особи, у провадженні якої перебуває справа, якщо ці дії порушують права судового експерта; 5) одержувати винагороду за проведення судової експертизи, якщо її виконання не є службовим завданням; 6) проводити на договірних засадах експертні дослідження з питань, що становлять інтерес для юридичних і фізичних осіб, з урахуванням обмежень, передбачених законом [4, ст. 13].

Слід зауважити, що до проведення судових експертиз, крім тих, що проводяться виключно державними спеціалізованими установами, можуть залучатися також судові експерти, які не є працівниками цих установ.

До речі, до державних спеціалізованих установ належать Міністерство юстиції України, Міністерство внутрішніх справ України, Міністерство охорони здоров'я України, Міністерство оборони України, Служба безпеки України та Державна прикордонна служба України.

Згідно з наказом Міністерства внутрішніх справ від 3 листопада 2015 р. № 1343 до експертної служби МВС входять Державний науково-дослідний

експертно-криміналістичний центр МВС України (далі – ДНДЕКЦ) та територіальні підрозділи – науково-дослідні експертно-криміналістичні центри, основними завданнями яких є здійснення судово-експертної діяльності, у межах компетенції проведення експертних досліджень на договірних засадах з питань, що становлять інтерес для юридичних і фізичних осіб, з урахуванням обмежень, передбачених Законом України "Про судову експертизу" тощо [5].

Незалежність судового експерта та правильність його висновку забезпечується ст. 4 Закону України "Про судову експертизу": 1) процесуальним порядком призначення судового експерта; 2) забороною під загрозою передбаченої законом відповідальності втручатися будь-кому в проведення судової експертизи; 3) існуванням установ судових експертиз, незалежних від органів, що здійснюють оперативно-розшукову діяльність, органів досудового розслідування та суду; 4) створенням необхідних умов для діяльності судового експерта, його матеріальним і соціальним забезпеченням; 5) кримінальною відповідальністю судового експерта за дачу свідомо неправдивого висновку та відмову без поважних причин від виконання покладених на нього обов'язків; 6) можливістю призначення повторної судової експертизи; 7) присутністю учасників процесу в передбачених законом випадках під час проведення судової експертизи.

У висновку експерт відображає докладний опис проведених ним досліджень, які ґрунтуються на його наукових, технічних або інших спеціальних знаннях, зроблені в результаті цих досліджень висновки та обґрунтовані відповіді на питання, задані судом.

При оформлені експертного висновку експерту необхідно зазначити: 1) коли, де, ким (ім'я, освіта, спеціальність, свідоцтво про присвоєння кваліфікації судового експерта, стаж експертної роботи, науковий ступінь, вчене звання, посада експерта) та на якій підставі була проведена експертиза; 2) місце і час проведення експертизи; 3) хто був присутній при проведенні експертизи; 4) перелік питань, що були поставлені експертові; 5) опис отриманих експертом матеріалів та які матеріали були використані експертом; 6) докладний опис проведених досліджень, у тому числі методи, застосовані в дослідженні, отримані результати та їх експертна оцінка; 7) обґрунтовані відповіді на кожне поставлене питання [6, ст. 82; 7, ст. 102; 8, ст. 144]. До того ж у висновку експерта повинні відображатися дані про те, що експерта попереджено про кримінальну відповідальність за завідомо неправдивий висновок та за відмову без поважних причин від виконання покладених на нього обов'язків.

Нині судовим експертом може стати будь-яка особа, яка має відповідну вищу освіту, освітньо-кваліфікаційний рівень не нижче спеціаліста. Окрім наявності вищої освіти, майбутньому експерту необхідно пройти процедуру атестації, метою якої є оцінка професійного рівня фахівця, який буде залучатися до проведення судових експертиз або братиме участь у розробках теоретичної та методичної бази судової експертизи.

На жаль, законодавець передбачає підстави, за яких особі, яка має намір отримати (підтвердити) кваліфікацію судового експерта, може бути відмовлено у присвоєнні кваліфікації, а саме: 1) визнання її в установленому законодавством порядку недієздатною; 2) наявності судимості; 3) накладання адміністративного стягнення за вчинення корупційного правопорушення або дисциплінарного стягнення у вигляді позбавлення кваліфікації судового експерта (протягом року

з дня прийняття відповідного рішення); 4) відсутності відповідної вищої освіти; 5) не здача кваліфікаційного іспиту.

Порядок проведення атестації судового експерта здійснюється відповідно до Положення про експертно-кваліфікаційні комісії та атестацію судових експертів [9], а присвоєння чи позбавлення кваліфікаційних класів судового експерта проводиться згідно з Порядком присвоєння кваліфікаційних класів судових експертів працівникам науково-дослідних установ судових експертиз Міністерства юстиції України [10].

Відповідно до Положення працівники науково-дослідних установ судової експертизи та фахівці, які не є працівниками державних спеціалізованих установ, повинні крім того, що мати раніше зазначену відповідну вищу освіту, пройти підготовку або стажування, знати теоретичні, організаційні і процесуальні питання судової експертизи та методичні положення і практику їх застосування за відповідною експертною спеціальністю та скласти кваліфікаційний іспит [9].

Кваліфікація судовому експерту присвоюється згідно зі встановленим переліком видів судових експертиз та експертних спеціальностей у Положенні [9]. Відповідно до цього переліку видів судових експертиз судову експертизу об'єктів ПІВ відносять до V класу експертизи як окремий вид експертизи під назвою "Експертиза у сфері інтелектуальної власності". Такий вид експертизи поділяється на підвиди судових експертиз, які співпадають з назвами об'єктів інтелектуальної власності. Залежно від підвиду експертизи "Експертиза у сфері інтелектуальної власності" розділяються види експертних спеціальностей. До таких видів належать дослідження, пов'язані з літературними, художніми творами, комп'ютерними програмами, компіляціями даних (базами даних), виконаннями, фонограмами, відеограмами, програмами (передачами) організацій мовлення, винаходами, корисними моделями, промисловими зразками, сортами рослин, породами тварин, комерційними (фірмовими) найменуваннями, торговельними марками (знаками для товарів і послуг), географічними зазначеннями, топографіями інтегральних мікросхем, комерційною таємницею (ноу-хау), раціоналізаторськими пропозиціями та економічні дослідження у сфері інтелектуальної власності.

У результаті проведеної атестації експерту видається свідоцтво про присвоєння кваліфікації судового експерта з певного виду експертної спеціальності. Свідоцтво має обмежений термін дії – від 3 до 6 років. По завершенню терміну дії свідоцтва експерт має право його продовжити після того, як підтвердить свою кваліфікацію: для працівників науково-дослідних установ судової експертизи – на п'ять років, для фахівців, які не є працівниками державних спеціалізованих установ – на три роки.

Далі Міністерство юстиції України вносить відомості до державного реєстру атестованих судових експертів щодо видачі свідоцтва експерту. На сьогодні Мін'юст України надає можливість суспільству в електронному вигляді здійснювати запит інформації про атестованих судових експертів у Реєстрі атестованих судових експертів [11]. Отримана інформація запиту може містити такі дані: номер свідоцтва, назву комісії, дату та номер рішення комісії, термін дії свідоцтва, номер та вид експертизи, індекс та вид експертної спеціальності.

Проаналізувавши цей реєстр, можна відмітити, що судові експерти у сфері інтелектуальної власності працюють як у державних спеціалізованих установах Мін'юсту й Міністерства внутрішніх справ України, так і в інших установах або

як самозаймані. Станом на 2015 рік кількість атестованих судових експертів у сфері інтелектуальної власності становила 160, з них 75 експертів працюють у науково-дослідних експертно-криміналістичних установах МВС України, 58 – у науково-дослідних установах Мін'юсту України та 27 – в інших установах і організаціях, не підпорядкованих Мін'юсту України, або як самозайняті особи.

Деякою мірою можна погодитись з думкою С.А. Петренка, який стверджує, що в Україні існує незбалансований розподіл експертів по областях. Він приводить дані, що станом на 2014 рік тільки в МВС було відносно рівномірно розподілено експертів по регіонах України, а в системі експертних установ Мін'юсту здійснилася цілеспрямована концентрація експертів у м. Києві, що, на думку науковця, не є доцільним із позиції розвитку не тільки судової експертизи об'єктів ПІВ, а й цієї сфери взагалі в областях. Також вчений виділяє ще одну негативну тенденції у сфері судової експертизи інтелектуальної власності, яка пов'язана зі зменшенням кількості судових експертів, що не працюють в установах Мін'юсту. У результаті від практичної судово-експертної діяльності за останні роки було відлучено чимало висококваліфікованих професіоналів. Необґрунтовано високі ціни за проходження навчання та стажування при отримані або підтвердженні кваліфікації судового експерта, у порівнянні з безкоштовністю подібної процедури для працівників експертних установ Мін'юсту також негативно впливають на забезпечення експертизи ПІВ [12, с. 81–82].

Для проведення експертизи експерт використовує методики проведення судових експертиз. Ці методики підлягають обов'язковій атестації та державній реєстрації. Процедура їх атестації та реєстрації регламентується постановою Кабінету Міністрів України від 2 липня 2008 р. № 595 [13].

Розробляють такі методики державні спеціалізовані установи міністерств та інших центральних органів виконавчої влади, що здійснюють судово-експертну діяльність. При необхідності до розроблення методик залучаються провідні фахівці з певних галузей знань за їх згодою.

Під поняттям "методика проведення судової експертизи" розуміють результат наукової роботи, що містить систему методів дослідження, які застосовуються в процесі послідовних дій експерта з метою виконання певного експертного завдання [4].

Метою проведення атестації методик є оцінка звіту про наукову роботу, виконану з метою розроблення методик, шляхом проведення його рецензування та апробації методик спеціалізованими установами. Рецензування звіту про наукову роботу проводиться фахівцями з певних галузей знань, які не брали участь у розробленні методики, з метою визначення актуальності та новизни з урахуванням сучасних досягнень науки і техніки, а також можливості використання методик в експертній практиці [13]. Результати атестації методик розглядаються науковими радами спеціалізованих установ, які діють відповідно до Закону України "Про наукову і науково-технічну діяльність" [14].

Після прийняття науковою радою рішення про рекомендацію до впровадження методики в експертну практику її направляють до Мін'юсту на державну реєстрацію. А далі Мін'юст уносить дані про державну реєстрацію методики до Реєстру методик проведення судових експертиз [15]. Нині тільки 7 методик для проведення експертизи у сфері інтелектуальної власності пройшли атестацію, а саме: методика проведення судових експертиз літературних творів, методика проведення судових

експертиз, пов'язаних із кресленнями – об'єктами авторського права, методика проведення досліджень оптичних носіїв, що містять об'єкти авторського права та суміжних прав, методика проведення судової експертизи, пов'язаної з винаходами та корисними моделями, методика проведення судової експертизи, пов'язаної з раціоналізаторськими пропозиціями, методика дослідження ознак контрафактності лазерних компакт-дисків, аудіо- та відеокасет, методика проведення судової експертизи комерційної таємниці та ноу-хау. Розробниками перерахованих методик були установи Мін'юсту України та ДНДЕКЦ МВС України [15].

Ознайомившись із переліком атестованих методик, можна відмітити, що їх кількість не забезпечує здійснення дослідження всього переліку існуючих об'єктів ПІВ. Прогалина виникає з експертизою таких об'єктів, як знаків для товарів і послуг, комерційних (фірмових) найменувань, промислових зразків, топографічних інтегральних мікросхем, сортів рослин та порід тварин, комп'ютерних програм, баз даних, аудіовізуальних творів. На нашу думку, відсутність єдиної методики проведення експертизи, особливо торгових марок, є не припустимою. Адже, виходячи зі статистичних даних про зареєстровані кримінальні правопорушення за ст. 229 КК України, які наведені на початку дослідження, щороку фіксується тенденція кримінальних правопорушень щодо незаконного використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення погодження товару.

У результаті такої ситуації експерту при проведення дослідження об'єктів ПІВ, на які відсутня єдина методика необхідно керуватися власними знаннями в цій галузі для написання обґрунтованого висновку, що може призводити до суттєвих порушень чинного законодавства.

Таку позицію підтримують Г.К. Дорожко та Н.В. Марченко, які стверджують, що відсутність єдиних методик дослідження може стати підґрунтям для проведення повторних експертиз в інших установах, що призводять до затягування судового процесу. Для покращення захисту ПІВ вони підтримують позицію впровадження єдиних методик для всіх можливих об'єктів ПІВ [16, с. 116–120].

Влучно підмітив Ю.Г. Охромєєв, що відсутність методик призводить до виникнення суперечок під час проведення цього виду експертизи, зокрема в методологічних підходах [17].

А.С. Штефан відмічає, що відсутність методик проведення експертиз об'єктів авторського права фактично надає експертові можливість при проведенні дослідження керуватися будь-якими підходами, власними внутрішніми переконаннями та ін. У результаті дослідження, що проводилося за відсутності рекомендацій та визначених законом методик, викладені в судовій експертизі висновки можуть суперечити нормам чинного законодавства та практиці його застосування. Також вона стверджує, що іноді гарантована законодавством у сфері судової експертизи незалежність експерта призводить до обрання ним помилкового шляху дослідження та призводить до необґрунтованих висновків [18, с. 73].

Продовжуючи наше дослідження, ми хотіли звернути увагу на те, що порядок призначення експертизи по кримінальним, адміністративним та цивільним справам має свої особливості. Якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання, то за зверненням сторони кримінального провадження або за дорученням слідчого судді чи суду проводиться експертиза. Крім того, не допускається проведення експертизи для з'ясування юридичних питань [7, ст. 242].

Порядок залучення експерта по кримінальному провадженні встановлює вимоги, за якими можна залучати експерта. До таких вимог належать: 1) сторона обвинувачення залучає експерта за наявності підстав для проведення експертизи, у тому числі за клопотанням сторони захисту чи потерпілого; 2) сторона захисту має право самостійно залучати експертів на договірних умовах для проведення експертизи, у тому числі обов'язкової; 3) експерт може бути залучений слідчим суддею за клопотанням сторони захисту [7, ст. 243].

При розгляді цивільних справ, відповідно, призначення експертизи є обов'язковим у разі заявлення клопотання про призначення експертизи обома сторонами або за клопотанням хоча б однієї зі сторін. Висновок експертизи передбачає встановлення характеру і ступеня ушкодження здоров'я, психічного стану особи та віку особи, якщо про це немає відповідних документів і неможливо їх одержати [8, ст. 145].

В адміністративному судочинстві суд може призначити експертизу для з'ясування обставин, що мають значення для справи і потребують спеціальних знань у галузі науки, мистецтва, техніки, ремесла тощо. До того ж особам, які беруть участь у справі, надається право подати суду питання, на які потрібна відповідь експерта та просити суд призначити експертизу і доручити її проведення відповідній експертній установі або конкретному експерту. Якщо сторони домовилися про залучення експертами певних осіб, суд повинен призначити їх відповідно до цієї домовленості [6, ст. 81].

Якщо проведення експертизи доручено експертній установі, її керівник має право доручити проведення експертизи одному або кільком експертам, якщо судом не визначено конкретних експертів, у разі потреби – замінити виконавців експертизи, заявити клопотання щодо організації проведення досліджень поза межами експертної установи.

Проаналізувавши порядок призначення експертизи по кримінальним, цивільним та адміністративним справам, досить часто виникає ситуація, коли по справі можуть одночасно обидві сторони ухвалювати рішення про призначення експертиз на одні й ті ж самі об'єкти ПІВ. У результатів такої ситуації, як стверджують О.В. Кравчук та Ю.В. Циганюк, виникає питання, як і хто розподілятиме об'єкти дослідження між сторонами та на чиєму боці буде перевага за часом призначення експертизи. Для вирішення такої ситуації вони пропонують врегулювати норми законодавчої бази [19, с. 34–45].

На думку С.А. Петренка, призначення декількох судових експертиз по справі свідчить про складність проведення експертиз у сфері інтелектуальної власності. Адже для встановлення властивостей, ознак та характеристик об'єктів ПІВ, визначення факту їх присутності або використання у матеріальних об'єктах інтелектуальної власності необхідні спеціальні знання, які повинен мати судовий експерт з питань ПІВ [12, с. 80–85].

Отже, підсумовуючи наведене вище, зазначимо, що для ефективного проведення експертизи у сфері інтелектуальної власності потрібно вдосконалити законодавство України в сфері інтелектуальної власності та судової експертизи, в якому чітко визначити єдині методики проведення експертиз усіх об'єктів ПІВ, порядок призначення експертизи по справі на один і той же об'єкт дослідження та оцінку експертного висновку по цьому об'єкту при розгляді справи, рівні критерії для всіх осіб, які планують стати судовими експертами. Оскільки окремий вид експертизи у сфері інтелектуальної власності утворився відносно недавно, у 2002 р., а єдині методики дослідження почали ухвалювати тільки з 2005 р., то, на наш погляд, проблеми, які виникають при проведені експертизи об'єктів ПІВ,

котрі ми розглянули, є типовими, але не вичерпними, тому потребують подальшого наукового обґрунтування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Єдиний звіт про кримінальні правопорушення по державі за січень-жовтень 2016 року / Статистична інформація про зареєстровані кримінальні правопорушення та результати їх досудового розслідування [Електронний ресурс]. – Режим доступу : http://www.gp.gov.ua/ua/stst2011.html?dir_id=112173&libid=100820&c=edit&_c=fo#.

2. Кримінальний кодекс України : Закон України від 5 квітня 2001 року № 2341-III // Відомості Верховної Ради України (ВВР). – 2001. – № 25–26. – Ст. 176, 177, 229.

3. Адміністративні правопорушення в Україні: статистичні бюлетені Державної служби статистики України за 2010–2016 роки.

4. Про судову експертизу : Закон України від 25 лютого 1994 року № 4038-XII // Відомості Верховної Ради України (ВВР). – 1994. – № 28. – Ст. 232.

5. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : Наказ Міністерства внутрішніх справ від 03.11.2015 № 1343 // Офіційний вісник України. – 2015. – № 92. – С. 342. – Ст. 3149.

6. Кодекс адміністративного судочинства України : Закон України від 6 липня 2005 року № 2447-IV // Офіційний вісник України. – 2005. – № 32. – С. 11. – Ст. 1918.

7. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI // Відомості Верховної Ради України (ВВР). – 2013. – № 9–10, № 11–12, № 13. – Ст. 88.

8. Цивільний процесуальний кодекс України : Закон України від 18 березня 2004 року № 1618-IV // Відомості Верховної Ради України (ВВР). – 2004. – № 41–41. – Ст. 492.

9. Про затвердження Положення про експертно-кваліфікаційні комісії та атестацію судових експертів : Наказ Міністерства юстиції України від 3 березня 2015 року № 301/5 // Офіційний вісник України. – 2015. – № 17. – С. 278. – Ст. 468.

10. Про затвердження Порядку присвоєння кваліфікаційних класів судових експертів працівникам науково-дослідних установ судових експертиз Міністерства юстиції України : Наказ Міністерства юстиції України від 30 грудня 2011 року № 3660/5 // Офіційний вісник України. – 2012. – № 3. – С. 151. – Ст. 105.

11. Реєстр атестованих судових експертів [Електронний ресурс]. – Режим доступу : http://rase.minjust.gov.ua.

12. *Петренко С.А.* Місце судової експертизи у справах із захисту прав інтелектуальної власності та удосконалення судово-експертної діяльності / С.А. Петренко // Інтелектуальна власність в Україні: погляд з XXI ст : матеріалами IV Всеукр. наук.-практ. конф. (м. Київ, 25–26 верес. 2014 р.) – Черкаси: Чабаненко Ю.А., 2014. – С. 80–85.

13. Про затвердження Порядку атестації та державної реєстрації методик проведення судових експертиз : Постанова Кабінету Міністрів України від 02 липня 2008 року № 595 // Офіційний вісник України. – 2008. – № 49. – С. 33. – Ст. 1585.

14. Про наукову і науково-технічну діяльність : Закон України від 26 листопада 2015 року № 848-VIII // Відомості Верховної Ради України (ВВР). – 2016. – № 3. – Ст. 25.

15. Реєстр методик проведення судових експертиз [Електронний ресурс]. – Режим доступу: http://rmpse.minjust.gov.ua.

16. *Дорожко Г.К.* Судовий експерт у сфері інтелектуальної власності / Г.К. Дорожко, Н.В. Марченко // Теоретичні і практичні аспекти економіки та інтелектуальної власності. – 2014. – № 1 (10), т. 2. – С. 116–120.

17. *Охромєєв Ю.Г.* Деякі аспекти проведення судової експертизи у сфері інтелектуальної власності / Ю.Г. Охромєєв // Інтелектуальна власність. – 2009. – № 1 (27).

18. *Штефан А.С.* Судова експертиза об'єктів авторського права: проблемні питання незалежності експерта / А.С. Штефан // Теорія і практика інтелектуальної власності. – 2009. – № 3. – С. 72–80.

19. *Кравчук О.В.* Порядок призначення судових експертиз у сфері інтелектуальної власності за новим Кримінальним процесуальним кодексом України / О.В. Кравчук, Ю.В. Циганюк // Криміналістичний вісник. – 2013. – № 2 (20) . – С. 34–45.

Отримано 15.11.2016
Рецензент Марченко О.С., к.т.н.

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА

Modern Special Technics

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

Випусковий редактор
Лелет С.М.
Редакційна група:
Алєксєєва О.В.,
Якубчик Т.В.
Комп'ютерна верстка:
Мухіна Т.М.

Issuing Editor
Lelet S.M.
Editorial Group
Alieksieieva O.V.
(English interpreter)
Yakubchik T.V.
Makeup
Mukhina T.M.

Адреса редакції:
01011, м. Київ, пров. Євгена Гуцала, 4-а
Телефон: (044) 254-95-21
Факс: (044) 280-01-84
E-mail: dndi@mvs.gov.ua
Сайт: http://suchasnaspetstehnika.com/

Підписано до друку 29.12.2016.
Формат 60x80 1/8. Гарнітура Petersburg. Друк офсетний.
Папір офсетний. Ум.-друк. арк. 9,2.
Наклад 100.

Видавець ФОП Озеров Г.В.
м. Харків, вул. Університетська, 3, кв. 9.
Свідоцтво про державну реєстрацію
№ 818604 від 02.03.2000.