DOI: 10.58254/viti.3.2023.10.81

УДК 355. 424

Радченко М. М. ORCID: 0000-0002-8272-0727 (ВІТІ ім. Героїв Крут)
Шаповал В. М. ORCID: 0000-0003-4637-9362 (ВІТІ ім. Героїв Крут)
Терещенко Т. П. ORCID: 0000-0002-9659-7897 (ВІТІ ім. Героїв Крут)
Дикий О. В ORCID: 0000-0001-7327-8589 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ РОЗРАХУНКУ КІЛЬКІСНИХ ПОКАЗНИКІВ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАХИСТУ КРИТИЧНОГО ОБ'ЄКТА ІНФРАСТРУКТУРИ ВІД УДАРІВ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

Зростання потенційних можливостей застосування безпілотних комплексів, які призначені виконувати бойові завдання в повітрі, на землі, на/під водою, ніж будь-коли раніше веде до збільшення загроз для оборонного ландшафту учасників сил оборони. Це стає причиною зростання швидкими темпами інтересу до технологій, які знешкоджують загрози подібного типу. Для сторони, яка захищає критичний об'єкт від повітряного нападу з боку безпілотного авіаційного комплексу (або групи) завжди актуальне питання гарантованої ефективності або економічної співмірності способів захисту від низько-вартісних атак, які можуть здійснюватися такими комплексами.

Процес функціонування критичного об'єкта інфраструктури, який містить у своєму складі розгорнуту систему захисту, пункт керування та підсистеми з критичним обладнанням, через які здійснюється загальне цільове призначення цього об'єкта, пропонується описувати за аналогією з моделлю процесу функціонування відновлюваної системи з обмеженою надійністю елементів. Для кількісної оцінки пропонується взяти комплексний показник надійності функціонування відновлюваної системи.

Отримані показники для кількісної оцінки ефективності захищеності критичного об'єкта інфраструктури від повітряних атак в подальшому будуть конвертуватися в конкретні пропозиції для осіб, які приймають рішення щодо підбору засобів необхідних видів протидії безпілотним авіаційним комплексам для нарощування системи захисту, і які вимагаються для обґрунтування фінансово-економічних затрат при здоланні такого типу загроз.

Напрямками подальших досліджень з метою забезпечення заданих показників захисту критичного об'єкта інфраструктури стане методика розрахунку резервування засобів захисту.

Ключові слова: *інтенсивність атак, кількісні показники ефективності, час відновлення, час нормального функціонування, критичний об'єкт інфраструктури, система захисту від БпАК.*

M. Radchenko, V. Shapoval, T. Tereshchenko, O. Dykyi Model for calculating quantitative indicators for assessing the efficiency of protecting a critical infrastructure object from impacts of unmanned aviation complexes.

The growing potential for the use of unmanned systems, which are designed to perform combat missions in the air, on the ground, on/under water than ever before, leads to an increase in threats to the defense landscape of defense forces. This is the reason for the rapid growth of interest in technologies that neutralize threats of this type. For the party that protects a critical object from an air attack by an unmanned aircraft complex (or group), the issue of guaranteed effectiveness or economic proportionality of methods of protection against low-cost attacks that can be carried out by such complexes is always relevant. The answer to this question begins with the availability of a device for calculating quantitative indicators for evaluating the effectiveness of protecting a critical infrastructure object from an air attack.

The process of functioning of a critical infrastructure object, which includes a deployed protection system, a control point and subsystems with critical equipment, through which the general purpose of this object is carried out, is proposed to be described by analogy with the model of the process of functioning of a renewable system with limited element reliability. In order to quantitatively assess the effectiveness of the protection of a critical infrastructure object from air attacks by unmanned aerial systems, it is proposed to take a comprehensive indicator of the reliability of the functioning of the renewable system, which consists of the following components: the readiness factor, the vulnerability factor and the protection from air attacks. Expressions of calculation formulas are given in accordance with the proposed process description model.

The obtained indicators for the quantitative assessment of the effectiveness of the protection of a critical infrastructure object from air attacks will be converted into specific proposals for persons who make decisions on the selection of the necessary types of countermeasures against unmanned aircraft systems for the expansion of the defense system, and which are required for the justification of financial and economic costs when overcoming this type of threat.

The directions of further research in order to ensure the specified indicators of the protection of a critical infrastructure object will be the method of calculating the reservation of protection means.

Keywords: *intensity of attacks, quantitative indicators of effectiveness, recovery time, time of normal operation, critical infrastructure object, anti-UAC protection system.*

Постановка завдання у загальному вигляді. Сучасна військово-політична обстановка у світі свідчить про виникнення нових загроз, пов'язаних із удосконаленням технологічної складової протиборчих сторін. Найбільш економічно розвинені держави активно розробляють та приймають на озброєння комплекси із безпілотними апаратами різного призначення разом із засобами протидії їм. Тому створення вітчизняних сучасних систем протидії загрозам, що виникають від застосування безпілотних комплексів, є актуальним завданням. Огляд загальних трендів розвитку перспективних видів озброєння [1] у збройних силах різних країн для розвідки та моніторингу, ретрансляції радіосигналів, цілевказівки та нанесення вогневого ураження ворожому учаснику воєнного конфлікту показує активне застосування технологій створення безпілотних роботизованих комплексів, які діють на землі, в повітрі на воді чи під водою.

У Стратегії національної безпеки України, затвердженій Указом Президента України від 14 вересня 2020 р. № 392 [2], зазначається, що використання робототехніки та автономних безпілотних апаратів є одним із сучасних напрямів розроблення систем озброєнь. Розробка, виробництво безпілотних роботизованих систем, а також комплексів боротьби з ними, переживають бурхливе зростання в усьому світі. На ринок цього сегмента новітньої техніки виходять країни, які раніше не здійснювали наукових розробок і виробництва безпілотних літальних апаратів чи безпілотних наземних апаратів, а безперечними ж лідерами в цій галузі залишаються США, Ізраїль, Німеччина та Туреччина, що відображається у пріоритетах за обсягами фінансування їхніх програм зі створення та модернізації подібних систем. Експерти безпілотної техніки, для прикладу, прогнозують, що провідні країни світу матимуть до 2025 р. у складі бойової авіації до 80% безпілотної складової [3].

На сьогодні підрозділи сектору безпеки та оборони знаходяться під постійним впливом різноманітної номенклатури безпілотних авіаційних комплексів (далі – БпАК). Комплекси БпАК впливають на бойові порядки підрозділів, критичні об'єкти інфраструктури логістичного забезпечення та пунктів управління учасників сил оборони розвідкою і вогневим ураженням боєприпасами (в тому числі що баражують безпілотними літальними апаратами – камікадзе), як протягом підготовки, так і при веденні бойових дій. Не на останньому місці застосування противником засобів протидії безпілотним засобам наших підрозділів. З метою захисту військ та об'єктів інфраструктур учасників сил безпеки та оборони від подібного впливу виникає необхідність розробки систем, що забезпечать протидію БпАК.

Таким чином, робота щодо пошуку шляхів впровадження сучасних технологій захисту від БпАК, які практикуються світовими військово-промисловими групами, триває, тому дослідження підходів розрахунку кількісних показників оцінки ефективності захисту (коефіцієнти готовності, вразливості та захищеності) критичних об'єктів інфраструктури складових сектору безпеки та оборони автори цієї статті вважають актуальним.

Аналіз останніх досліджень і публікацій. Публікацій на тему розробки формалізованих моделей щодо повітряного захисту критичних об'єктів складових сил оборони і країни у цілому з огляду на важливість питання існує достатня кількість. Нижче наведемо деякі з них.

Автори методики [4] розрахунку ефективності прикриття дій наземних сил підрозділами протиповітряної оборони (далі – ППО), яка дає можливість оцінити ефективність ведення бойових дій зенітно-ракетних комплексів (далі – ЗРК) або зенітно-артилерійських комплексів (далі – ЗАК) при відбитті нападу з повітря, пропонували використовувати теорію ймовірностей для вибору параметрів елементів і структури підрозділів ППО. На підставі моделі марківських процесів розроблена модель оцінювання ефективності ППО з урахуванням інформаційних зв'язків між ЗРК (ЗАК), що забезпечує прогнозування ефективності стрільби вогневих засобів ППО у різних умовах очікуваних і поточних бойових дій. Таким чином, враховуються кількість засобів радіолокаційної інформації та структура інформаційних зв'язків між батареями ЗРК. Це впливає на середнє значення вірогідності виявлення повітряної цілі під час протиповітряного бою з урахуванням знищення командних пунктів наземних сил, що очікувано допоможе військовому командирові підрозділів ППО різного рівня ієрархії оцінювати варіанти структури своїх підрозділів ППО, вибирати раціональні інформаційні

зв'язки з кращою ефективністю прикриття та допоможе прийняти правильне рішення на відбиття ударів з повітря.

У наступному джерелі [5] здійснена оцінка ефективності бою (дій) підрозділів ППО в оборонному бою, яка враховує вибір показників ефективності бою (дій) та надає можливість створювати моделі оцінки бою (дій) для підрозділів ППО за допомогою математичного апарату, використовуючи теорію марківських процесів з безперервним часом і дискретними станами, тобто виникає можливість застосування методу аналітико-стохастичного моделювання. Наведений підхід дозволяє розраховувати ефективність бою (дій) підрозділів ППО по прикриттю загальновійськових підрозділів в оборонному бою. Методику можна адаптувати для розрахунку ефективності бою (дій) підрозділів ППО, які мають батареї зі змішаним складом зенітних засобів, що буде основою успішного виконання поставлених бойових завдань.

В [6] запропонована методика визначення достатнього рівня ефективності застосування підрозділу ППО Сухопутних військ (далі – СВ) при захисті загальновійськових підрозділів від ударів повітряного противника дає можливість визначити показники та критерії для оцінювання ефективності бойових дій підрозділів ППО СВ залежно від прогнозованого ступеня боєздатності загальновійськового підрозділу в ході загальновійськового бою (наскільки визначений склад сил та засобів ППО дозволяє зберегти визначену боєздатність загальновійськових підрозділів, що прикриваються від ударів з повітря).

Таким чином, для здійснення ефективного захисту критичного об'єкта інфраструктури (далі – КОІ) від впливу повітряних атак БпАК, необхідно визначити правила розподілу повітряних атак, націлених на КОІ, вибрати аналітичну модель оцінки його захищеності в умовах впливу такого типу атак для розрахунку коефіцієнтів готовності, вразливості та захищеності.

Мета статті: розробка моделі розрахунку кількісних показників оцінки ефективності захисту КОІ з системою захисту від БпАК в умовах впливу на нього потоку повітряних атак.

Виклад основного матеріалу. Розглянемо процес функціонування КОІ, який містить у своєму складі розгорнуту систему захисту (далі – СЗ), пункт керування (далі – ПК) та різні за функціональним призначенням підсистеми з критичним обладнанням (далі – ПКО) цього ж об'єкта (наприклад, у випадку гідроелектростанції це – гідросилове обладнання, водопідпірні та водоскидні споруди, енергетичні споруди, судноплавні й лісосплавні споруди тощо) s, де $s = 1, 2, \ldots, S$, і S це – загальна кількість підсистем з критичним обладнанням об'єкта, що захищається (рис. 1). Кожна ПКО виконує свій функціонал, який направлений на загальне цільове призначення об'єкта та складається з деякої споруди, технічних засобів, які розміщені в ній, і особового складу, який забезпечує його роботу. Прогнозується, що по КОІ наноситься повітряний удар БпАК, а саме на систему захисту поступає потік БпАК, які атакують.

Введемо обмеження для запропонованої моделі функціонування КОІ в умовах повітряних атак:

на вхід КОІ надходить сумарний потік випадкових потоків повітряних атак, який в сумі наближається до простішого [7];

після СЗ виходить простий потік, який наближається до простішого;

під час повітряних атак інтервали функціонування КОІ розподілені за експоненціальним законом [8] (рис. 2, 3);

повітряні загрози, які надходять в потоці атак, співпадають з вразливостями КОІ з інтервалами часу, розподіленими за експоненціальним законом.

Спрощена структурна схема такого КОІ наведена на рисунку 1, де прийняті наступні позначення:

λ – інтенсивність загального потоку повітряних атак на КОІ, $\lambda = \lambda_З + \lambda_К$;

$\lambda_{КПК}$ – інтенсивність потоку повітряних атак на КОІ, які націлені на його ПК;

$\lambda_{КS}$ – інтенсивність потоку повітряних атак на КОІ, які націлені на деяку ПКО s, де $s = 1, \ldots, S$ після впливу на потік атак СЗ КОІ;

$\lambda_к$ – інтенсивність потоку атак після спрацювання СЗ на відбиття атаки (інтенсивність атак після успішної нейтралізації частини БпАК, що атакують), $\lambda_к = \lambda_{кпк} + \lambda_{кs}$;

$\lambda_з$ – інтенсивність потоку атак, який знешкодила СЗ КОІ;

A_s – деяка ПКО, де $s = 1, \ldots, S$.

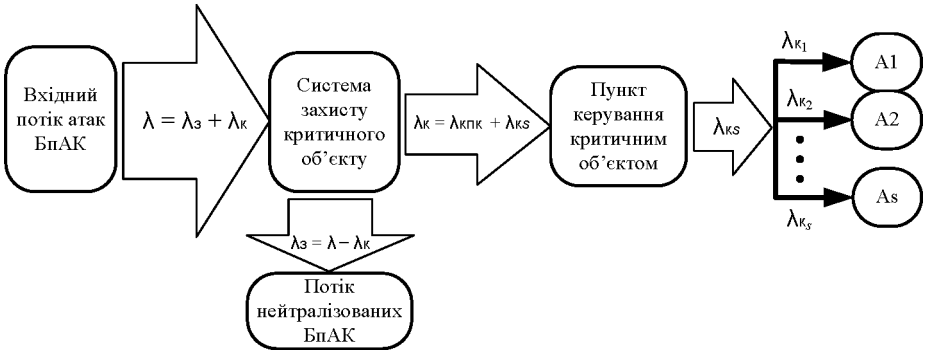

Рис. 1. Спрощена схема розподілу інтенсивностей атак, які впливають на складові КОІ

СЗ критичного об'єкта не є досконалою і тому відбувається тільки розрідження вхідного потоку атак БпАК на КОІ, частина, з яких з інтенсивністю $\lambda_{кпк}$ спрямована на ПК, а частина з інтенсивністю $\lambda_{кs}$ на інші складові КОІ (підсистеми критичного обладнання 1, 2, …, S). Будемо вважати, що вдала повітряна атака на ПК призведе до повного блокування функціонування КОІ у цілому. Вдала атака на обладнання s-ї критичної підсистеми не приведе до повної зупинки КОІ, а лише до втрати здатності виконувати ним свої функції у повному обсязі.

Розглянемо процес функціонування ПК після впливу на нього атаки БпАК. Будемо вважати, що в момент виявлення впливу атаки, а саме після її закінчення, обслуговуючий персонал КОІ одразу приступає до відновлення працездатності обладнання ПК та критичних підсистем s. Тривалість відновлення ПК – випадкова величина $t_{впкi}$, $i = 1, 2, \ldots$, з функцією розподілення $F_{впк}(t) = P\{t_{впк} < t\}$ та кінцевим математичним очікуванням середнього часу відновлення $T_{впк} < \infty$. В момент завершення відновлення ПК, КОІ відновлює нормальне функціонування до моменту впливу наступної повітряної атаки. Тривалість нормального функціонування ПК є випадковою величиною $t_{пкi}$, $i = 1, 2, \ldots$, з функцією розподілення $F_{нфпк}(t) = P\{t_{нфпк} < t\}$, $F_{пк}(t) = P\{t_{пк} < t\}$ та кінцевим математичним очікуванням $T_{нфпк} < \infty$.

Графічне зображення цього процесу зображено на рисунку 2, де прийняті наступні позначення:

t_i – моменти початку впливу повітряних атак на ПК, що не знешкоджені СЗ, де $i = 0, 1, 2, \ldots$;

$t_{впкi}$ – тривалість відновлення ПК після впливу повітряної атаки, де $i = 1, 2, \ldots$;

$t_{пкi}$ – тривалість нормального функціонування ПК, де $i = 1, 2, \ldots$.

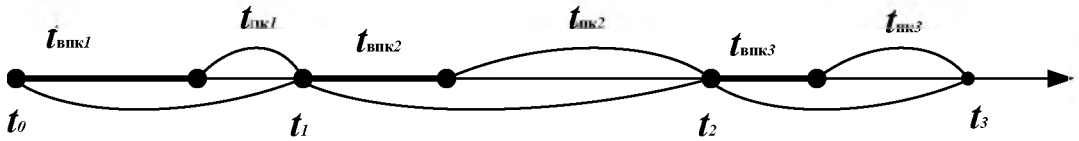

Рис. 2. Графічне зображення процесу функціонування ПК КОІ в умовах впливу повітряних атак з інтенсивністю $\lambda_{кпк}$

Аналогічно функціонує кожна ПКО s при впливі повітряних атак на них з сумарною інтенсивністю $\lambda_{кs}$, що не були нейтралізовані СЗ, де $s = 1, \ldots, S$. Процес функціонування ПКО в умовах впливу повітряних атак відображено на рисунку 3, де прийняті наступні позначення:

$t_{вsi}$ – реалізація випадкових величин часу відновлення працездатності ПКО s після впливу повітряної атаки, де $i = 1, 2, \ldots$;

t_{si} – тривалість нормального функціонування ПКО s після чергового відновлення працездатності КОІ, де $i = 1, 2, 3, \ldots$.

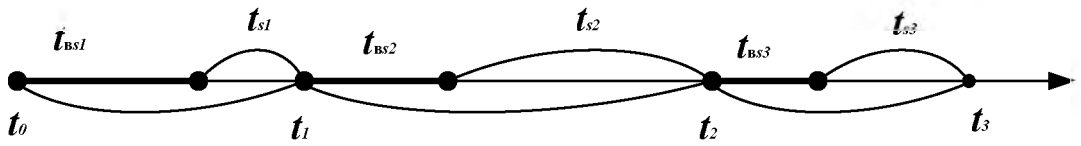

Рис. 3. Графічне зображення процесу функціонування ПКО *s* в умовах впливу повітряних атак з інтенсивністю $\lambda_{кs}$

Отже можна зауважити, що модель процесу функціонування КОІ в умовах впливу потоку повітряних атак перебуває у певній відповідності (аналогічна) до моделі процесу функціонування відновлюваної системи з обмеженою надійністю елементів. Тому для кількісної оцінки ефективності захисту КОІ від повітряних атак БпАК доцільно використати комплексний показник надійності функціонування відновлюваної системи $K_г$ – коефіцієнт готовності [8], коефіцієнти вразливості – $K_{вр}$ та захищеності – $K_з$ від повітряних атак [9].

Під коефіцієнтом готовності КОІ, який функціонує під впливом повітряних атак з інтенсивністю λ, будемо розуміти ймовірність того, що відновлювальний КОІ опиниться працездатним (буде нормально функціонувати) в довільний момент часу.

Визначимо через $p_0(t)$ ймовірність працездатності КОІ в момент часу t, а через $p_1(t)$ ймовірність непрацездатності КОІ в умовах потоку повітряних атак. Тоді зазначимо, що

$$p_0(t) + p_1(t) = 1. \tag{1}$$

Розглянемо формулу для ймовірності $p_0(t)$ під час впливу повітряних атак на КОІ при ураженні ПК, коли випадкові величини $t_{пкi}$ та $t_{впкi}$ (рис. 2) розподілені за експоненціальним законом [9] з параметрами $\lambda_{кпк} = 1/T_{нфпк}$, $\mu_{пк} = 1/T_{впк}$, де $\lambda_{кпк}$ – інтенсивність потоку повітряних атак на ПК; $\mu_{пк}$ – інтенсивність його відновлення; $T_{нфпк}$ – статистична оцінка середнього значення випадкової величини $t_{пкi}$; $T_{впк}$ – статистична оцінка середнього значення випадкової величини $t_{впкi}$.

Тоді для аналізу ймовірності $p_0(t)$ КОІ згідно з [8] можливо долучити наступну формулу (2):

$$p_0(t) = \frac{1}{1+K_в}\left(1 + K_в \cdot e^{-\lambda\left(\frac{1+K_в}{K_в}\right)t}\right), \tag{2}$$

де $K_в = T_{впк}/T_{нфпк}$ – показник норми відновлення КОІ (за рахунок відновлення працездатності ПК).

Використовуючи формулу (2), наведемо формулу (3) для коефіцієнту готовності ПК до початку атаки:

$$\lim p_0(t) = K_{гпк} = 1/(1+K_{впк}) = T_{нфпк}/(T_{нфпк}+T_{впк}). \tag{3}$$

Це означає, що існує стале значення ймовірності $p_0(t)$, яке не залежить від часу [9]. Таким чином ймовірність отримати КОІ працездатним у довільний момент часу в сталому режимі експлуатації, через деякий час після моменту $t = 0$ відповідає постійній величині, яку називають стаціонарним коефіцієнтом готовності. Зазначимо, що формула (3) вірна при довільних функціях розподілення випадкових величин $t_{пкi}$ та $T_{впкi}$. Ця формула найбільш вірогідно відображає фізичну суть коефіцієнта готовності як відносну частину часу, протягом якої КОІ знаходиться у працездатному стані.

Тоді статистична оцінка коефіцієнту готовності ПК (4):

$$K^*_{гпк} = 1/(1+K^*_{впк}) = T^*_{нфпк}/(T^*_{нфпк}+T^*_{впк}), \tag{4}$$

де $T^*_{нфпк}$ – статистична оцінка середнього значення випадкової величини $t_{пкi}$ (рис. 2) в сталому режимі (коли $t \to \infty$) знаходиться за виразом $T^*_{нфпк} = \frac{1}{n}\sum_{j=1}^{n} t_{пкj}$, а $T^*_{впк}$ – статистична оцінка середнього значення випадкової величини $t_{впкi}$ (рис. 2) знаходиться за виразом $T^*_{впк} = \frac{1}{n}\sum_{j=1}^{n} t_{впкj}$.

Розглянемо випадок, коли повітряна атака з інтенсивністю $\lambda_{кs}$ впливає на s-ту ПКО, де $s = 1, \ldots, S$ (рис. 3). Момент впливу повітряної атаки на ПКО s визначає втрату її працездатності та перемикання на режим відновлення. Оскільки всі підсистеми існують незалежно, тоді для s-ї ПКО можливо вивести формули (5), (6) коефіцієнтів готовності $K_{гs}$ та $K^*_{гs}$, де $s = 1, \ldots, S$ аналогічно наведеним вище виразам (3) та (4) для здійснення розрахунків коефіцієнтів для ПК:

$$K_{гs} = 1/(1+K_{вs}) = T_{нфs}/(T_{нфs}+T_{вs}); \quad (5)$$

$$K^*_{гs} = 1/(1+K^*_{вs}) = T^*_{нфs}/(T^*_{нфs}+T^*_{вs}), \quad (6)$$

де $T^*_{нфs} = \frac{1}{n}\sum_{j=1}^{n} t_{sj}$, $T^*_{вs} = \frac{1}{n}\sum_{j=1}^{n} t_{вsj}$.

Для того щоб застати ПКО s в довільний момент часу t в сталому режимі у працездатному стані, необхідно щоб в момент часу t були працездатними всі його підсистеми одночасно. З точки зору надійності таку систему можливо уявити як структурну схему, що складається з S ПКО, і коефіцієнт готовності $K_{гs}$ якої буде розраховуватися за формулою (7):

$$K_{гs} = \prod_{i=1}^{S} K_{гi} = \prod_{i=1}^{S} \frac{T_{нфi}}{(T_{нфi}+T_{вi})}, \quad (7)$$

Визначимо розрахунок коефіцієнта $K_г$ для КОІ, який функціонує в умовах впливу повітряних атак на ПК з інтенсивністю $\lambda_{кпк}$ та на всі підсистеми s з інтенсивністю $\lambda_{кs}$ (рис. 1). Використовуючи формулу повної ймовірності [10] для сталого режиму функціонування КОІ отримаємо вираз (8):

$$K_г = P_{пк}K_{гпк} + \prod_{i=1}^{S} P_s K_{гi}, \quad (8)$$

де $K_{гпк}$ та $K_{гs}$ розраховуються за формулами (4) та (7) відповідно, а $P_{пк}$ та P_s згідно з [10] виразом (9):

$$P_{пк}=\lambda_{кпк}/(\lambda_{кпк}+\lambda_{кs}),\ P_s=\lambda_{кs}/(\lambda_{кпк}+\lambda_{кs}), \quad (9)$$

де $P_{пк}+P_s = 1$.

Під коефіцієнтом вразливості КОІ – $K_{вр}$ вважатимемо співвідношення інтенсивності потоку атак, які пройшли скрізь захисний вплив СЗ на складові об'єкта – $\lambda_к$ до інтенсивності загального потоку λ атак на КОІ $K_{вр} = \lambda_к/\lambda$, і відповідно, $K_з$ – коефіцієнт захищеності КОІ згідно з [11] знаходимо за виразом $K_з = 1 - K_{вр} = 1 - \lambda_к/\lambda$.

Приклад розрахунку. Розглянемо випадок коли на ПК та ПКО у складі $S = 5$ підсистем впливає не знешкоджена повітряна атака з інтенсивністю відповідно $\lambda_{кпк} = 1/T_{нфпк} = 0{,}1$, $\lambda_{кs} = 1/T_{нфs} = 0{,}1428$, де $s = 1, \ldots, 5$. Приймемо, що середній час нормального функціонування ПК $T_{нфпк} = 10$ годин, а час нормального функціонування s-ї ПКО $T_{нфs} = 7$ годин, де $s = 1, \ldots, 5$. Середній час відновлення працездатності ПК $T_{впк}$ дорівнює 0,5 годин, а час відновлення працездатності кожної s-ї підсистеми $T_{вs} = 1$ година, де $s = 1, \ldots, 5$. Розрахуємо при цих вихідних даних значення стаціонарного коефіцієнта готовності КОІ – $K_г$, коефіцієнта вразливості КОІ – $K_{вр}$ та коефіцієнта захищеності КОІ – $K_з$.

Рішення. Використовуючи формули (3), (5), (7)–(9) проведемо розрахунки:

$$K_{гпк} = T_{нфпк}/(T_{нфпк}+T_{впк}) = 10/(10{,}0+1{,}0) = 0{,}9091;$$

$$K_{гi} = T_{нфi}/(T_{нфi}+T_{вi}) = 7{,}0/(7{,}0+1) = 0{,}875;$$

$$K_{гs} = \Pi_i K_{гi} = 0{,}875^5 = 0{,}5129.$$

Згідно з формулою (9) розраховуємо значення $P_{пк}$ та P_s:

$P_{пк} = \lambda_{кпк}/(\lambda_{кпк}+\lambda_{кs}) = 0{,}1/(0{,}1 + 0{,}1428) = 0{,}4119$, $P_s = 1 - 0{,}4119 = 0{,}8581$.

За допомогою виразу (8) розраховуємо значення коефіцієнта готовності $K_г$ КОІ у цілому:

$$K_г = 0{,}4119 \cdot 0{,}9091 + 0{,}8581 \cdot 0{,}5129 = 0{,}8146.$$

У випадку, коли інтенсивність загального потоку повітряної атаки $\lambda = 30{,}0$, а $\lambda_к = 0{,}2428$ коефіцієнт вразливості КОІ становитиме $K_{вр} = 0{,}2428/30{,}0 = 0{,}0081$, а коефіцієнт захищеності

становитиме $K_з = 1 - K_{вр} = 1 - 0{,}0081 = 0{,}9919$, що дозволить оцінювати захист КОІ та в подальшому приймати рішення, щодо необхідності оптимізації засобів СЗ від БпАК.

Висновки. Таким чином, розглянутий підхід розрахунку кількісних показників оцінки ефективності захисту критичного об'єкта інфраструктури складових сектору безпеки та оборони в умовах повітряних атак БпАК передбачає використання моделі процесу функціонування відновлюваної системи з обмеженою надійністю елементів. Запропонована модель оцінки захисту критичного об'єкта від нападу БпАК дозволяє визначити основні показники ефективності захисту і може використовуватись для розробки оперативних рішень щодо залучення та визначення кількості таких засобів протидії, які б гарантовано забезпечували задані значення відповідних показників захисту.

Предметом подальших досліджень стане методика розрахунку резервування засобів захисту критичного об'єкта інфраструктури для забезпечення заданих показників його захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кваша Т. К. Світові наукові та технологічні тренди у сфері забезпечення національної безпеки / Т. К. Кваша. Київ: УкрІНТЕІ, 2019. 107 с. URL: https://mon.gov.ua/storage/app/media/innovatsii-transfer-tehnologiy/2021/09/30/Svitovi.nauk.tekhn.trend.sfer.zabezp.nats.bezp-2019.30.09.pdf (дата звернення: 27.03.2023).

2. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/news/volodimir-zelenskij-zatverdiv-strategiyu-nacionalnoyi-bezpek-63577 (дата звернення: 27.03.2023).

3. Щодо розвитку виробництва безпілотних роботизованих систем на основі державно-приватного партнерства: аналітична записка // Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/schodo-rozvitku-virobnictva-bezpilotnikh-robotizovanikh-sistem-na (дата звернення: 27.03.2023).

4. Коваленко С. П. Методика розрахунку ефективності прикриття наземних сил підрозділами ППО при веденні локальних конфліктів / С. П. Коваленко, А. Ф. Волков, С. І. Корсунов // Збірник наукових праць Національної академії Національної гвардії України. 2021. Вип. 1. С. 12–23. URL: http://nbuv.gov.ua/UJRN/ znpavs_2021_1_4 (дата звернення: 27.03.2023).

5. Лезік О. В. Розробка рекомендацій командиру підрозділу ППО з підвищення оперативності розрахунку вогневих можливостей підрозділу в умовах оборонного бою / О. В. Лезік, Г. А. Левагін, А. Ф. Волков, М. В. Мужук, В. Ю. Лукашов, М. В. Шевченко // Системи озброєння і військова техніка. 2021. № 3 (67). С. 7–18. URL: https://journal-hnups.com.ua/article/download (звернення: 27.03.2023).

6. Волков А. Ф. Методика визначення достатнього рівня ефективності бойових дій підрозділу протиповітряної оборони сухопутних військ для збереження боєздатності загальновійськових підрозділів, що прикриваються // А. Ф. Волков, О. В. Лезік, М. В. Мужук, І. В. Гуленов, Д. О. Васильченко / Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. № 4 (70). С. 7–14. URL: https://journal-hnups.com.ua/index.php/zhups/article/view/751/649 (дата звернення: 27.03.2023).

7. Давыденко В. П., Доронин Є. М. Основы военной кибернетики. Ленинград: ЛВВИУС, 1980. 314 с.

8. Жердєв М. К., Лєнков С. В., Креденцер Б. П. Фізичні основи теорії надійності: підручник. Київ: Київський національний університет імені Тараса Шевченка, 2008. 215 с.

9. Куцаєв В. В., Радченко М. М., Терещенко Т. П. Модель оцінки готовності інформаційно-телекомунікаційного вузла зв'язку в умовах кібернетичних атак // Збірник наукових праць ВІТІ. Київ, 2019. Вип. 3. С. 43–50 URL: https://www.viti.edu.ua/files/zbk/2019/5_3_2019.pdf (звернення: 27.03. 2023).

10. Вентцель Е. С. Теория вероятностей: учебник для вузов. Москва: Высш. шк., 1999. 576 с.

11. Куцаєв В. В. Радченко М. М. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла // Збірник наукових праць ВІТІ. Київ, 2018. Вип. 2. С. 67–76. URL: https://www.viti.edu.ua/index.php?view=coll_2018_2 (дата звернення: 27.03.2023).