DOI:**10.33099/2311-7249/2023-48-3-147-156**

УДК: 004.02+004.49+004.075

Машталір Вадим Віталійович *(доктор історичних наук, професор)*
Гук Олександр Миколайович *(доктор філософії)*
Толмачов Ігор В'ячеславович
Фараон Сергій Іванович *(доктор філософії)*

Національний університет оборони України, Київ, Україна

ПРОГНОЗУВАННЯ СТУПЕНЮ КІБЕРВПЛИВУ НА ГЕТЕРОГЕННІ ІНФОРМАЦІЙНІ СИСТЕМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ З УРАХУВАННЯМ ЙОГО ЕВОЛЮЦІЇ

З розвитком новітніх інформаційних технологій кіберпростір стає середовищем, у якому відбувається протиборство між суб'єктами міжнародних відносин у вигляді ведення кібервійн, а також інформаційних, мережецентричних, асиметричних, гібридних війн. З'являється тенденція використання стратегій асиметричних непрямих дій, заснованих на комбінації військових зусиль з політичними, економічними та інформаційно-психологічними методами впливу на супротивника для вирішення завдань, які раніше вирішувалися лише з використанням військової сили. В умовах цілеспрямованих інформаційно-технічних впливів і відсутності належних фахових знань про кіберпростір, розуміння цілей та характеру дій у ньому, а також динаміки змін означеного, виникла потреба розроблення методу прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення. Основне завдання методу полягає у забезпеченні кібербезпеки держави за активного протистояння у кіберпросторі. Цей метод враховує сукупність факторів (загроз), що раніше не мали місця, а також еволюцію кібервпливів. Гетерогенні інформаційні системи є складними технічними системами та мають притаманні їм властивості, тому доцільно для їх опису застосовувати декомпозицію на окремі інформаційні системи. Метою статті є розроблення методу прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення для забезпечення їх сталого функціонування в умовах кібервпливу. У статті застосовано аналітичний метод для розгляду останніх досліджень, публікацій та наукових джерел стосовно функціонування гетерогенних інформаційних систем військового призначення, цілочисельного програмування, максимального елементу та теорії оптимального розподілу ресурсів для прогнозування ступеню кібервпливу. Зазначений методологічний підхід дав змогу визначити набір засобів парирування зовнішніх впливів для кожного елементу гетерогенних інформаційних систем. Подано узагальнену структуру гетерогенних інформаційних систем, яка дозволяє формалізувати процес прогнозування ступеню кібервпливу. Розроблено метод прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення та подано його формалізований математичний опис. Елементом наукової новизни є те що запропонований підхід базується на оптимальному розподілі засобів парирування зовнішніх впливів, які в свою чергу поділяються на види, за взаємопов'язаними елементами гетерогенних інформаційних систем. Сутність запропонованого підходу полягає у виборі для кожного з елементів системи та відповідного набору джерел кібервпливу, що діє на них з метою порушення сталого функціонування, оптимального розподілу типів засобів парирування зовнішніх впливів. Теоретична значущість дослідження полягає у тому, що на основі відомих математичних методів оптимального розподілу ресурсів під час синтезу складних систем, отримано новий підхід, що враховує еволюцію кібервпливів на гетерогенні інформаційні системи військового призначення. Практична цінність полягає у тому, що застосування зазначеного методу, є необхідним кроком для визначення придатності гетерогенних інформаційних систем військового призначення до виконання цільової функції, та дозволить на етапі створення гетерогенних інформаційних систем військового призначення визначити можливі уразливості.

Ключові слова: *прогнозування, ступінь кібервпливу, гетерогенні інформаційні системи військового призначення, метод максимального елементу, кіберзагрози, кібербезпека, кіберпростір, кібератаки, кібервплив.*

Вступ

Постановка проблеми. Сфера застосування інформаційних технологій об'єднує всіх користувачів інформаційної інфраструктури, що використовують її послуги для задоволення власних потреб. Дуже важливо підтримувати

цілісність мереж і стежити за їх безпекою. З'явились принципово нові технології збору, зберігання і обробки інформації на базі архітектур клієнт-сервер. Зокрема, створюються розподілені корпоративні мережі, розподілені інформаційні системи, що використовують в якості транспортного середовища Internet; ускладнюються структури запитів користувачів з одночасним підвищенням ціни, якості та часу їх обробки; поширюються спектри загроз кібербезпеці і ускладнення сценаріїв їх реалізації. Всі ці зміни передбачають створення принципово нових механізмів забезпечення цілеспрямованого функціонування сучасних інформаційних систем.

Комплексний підхід до забезпечення сталого функціонування сучасних інформаційних систем на цей час застосовується не повною мірою. Вказана обставина є причиною виникнення суперечності між прагненням забезпечити стійке функціонування інформаційних систем в умовах деструктивних впливів і відсутністю теоретичних, методичних та організаційно-технічних основ його забезпечення. Тому суть проблеми полягає в необхідності створення теоретико-методологічних засад забезпечення стійкого функціонування інформаційних систем в умовах деструктивних впливів і науковому обґрунтуванні принципів побудови та функціонування системи забезпечення цілеспрямованого функціонування сучасних інформаційних систем в цих умовах.

Таким чином, з метою забезпечення сталого функціонування гетерогенних інформаційних систем військового призначення (далі – ГтІС ВП) в умовах кібервпливу, необхідно вірно спрогнозувати ступінь кібервпливу на них.

Аналіз останніх досліджень і публікацій. Питання стійкості систем стосовно зовнішніх інформаційних впливів досліджувалось І. Ю. Субачем, В. Л. Бурячком, С. В. Толюпою [2; 3]. Питання створення інтелектуальних інформаційних систем та спеціалізованого програмного забезпечення для автоматизованих систем управління досліджувались у роботах А. І. Сбітнєва, О. Ю. Пермякова, В. Б. Толубка [3; 4; 5; 18]. Роботи І. Ю. Субача, В. Л. Бурячка, С. П. Євсеєва, В. М. Чернеги [2; 3; 6; 7; 10] присвячені питанням кібербезпеки, здебільшого акцентують увагу на методах виявлення та розпізнавання кібервпливів. Водночас процеси функціонування автоматизованих систем управління та розподілених ГтІС ВП у таких умовах детально не розглядаються.

В існуючих роботах не достатньо повно розглянуто підхід до реалізації засобів протидії зовнішньому дестабілізуючому кібервпливу противника з метою забезпечення сталого функціонування інформаційних систем військового призначення.

Також, не повною мірою розглянуто питання розроблення конкретних дієвих алгоритмів і методик стосовно оцінювання або прогнозування стійкості ГтІС ВП в умовах кібервпливу. Крім того, сьогодні актуальною проблемою є розроблення комплексу аналітичних моделей і методів оцінювання процесу функціонування ГтІС ВП в умовах кібервпливу та прогнозування його наслідків.

Тому, актуальним завданням є розроблення методу, за допомогою якого, буде можливим спрогнозувати ступінь кібервпливу, що забезпечить своєчасне виявлення, а також його нейтралізацію та створить передумови стійкого функціонування ГтІС ВП.

Метою статті є розроблення методу прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення для забезпечення їх сталого функціонування в умовах кібервпливу.

Виклад основного матеріалу дослідження

Механізми забезпечення стійкого функціонування ГтІС ВП являють собою структуровану, відповідно до заданої множини ресурсів інформаційних мереж та рівнів їх деталізації, сукупність програмно-технічних засобів, організаційних заходів і методичних положень, спрямованих на активну чи пасивну протидію кібервпливу в інформаційній системі в цілому або в окремих її елементах.

У [1] надані такі визначення:

електронна комунікаційна мережа – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг;

електронна комунікація (телекомунікація, електрозв'язок) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій.

Проте відсутні дефініції стосовно інформаційних систем. Відповідно до керівних документів, що діють у Збройних Силах України [8; 11], інформаційна система – це сукупність обладнання, методів та процедур, і, в разі необхідності, персоналу, організованого для виконання функцій обробки інформації.

У військовій справі основною функцією інформаційних систем є автоматизація процесів управління військами і зброєю, під якою розуміється процес створення і втілення в роботу органів управління систем і засобів автоматизації з потрібним математичним, програмним, інформаційним і лінгвістичним забезпеченням. Теоретичною основою автоматизації управління військами є теорія управління військами, теоретичні основи військової кібернетики та інформатики [5].

ГтІС ВП, зокрема, системи передачі даних, створюються на основі принципів побудови розподілених обчислювальних мереж, в яких на окремих об'єктах розгорнуті локальні обчислювальні мережі, що об'єднують автоматизовані робочі місця для виконання

завдань збору, обробки, зберігання та відображення інформації.

Гетерогенна розподілена обчислювальна система являє собою множину обчислювальних вузлів різної апаратної архітектури і різної обчислювальної потужності, об'єднаних лініями зв'язку [9]. Гетерогенні інформаційні системи містять технічні засоби обробки даних, програмне забезпечення і відповідний персонал. Чотири складові частини утворюють внутрішню інформаційну основу:

засоби фіксації та збору інформації;

засоби збереження інформації;

засоби аналізу, обробки і представлення інформації;

засоби передачі відповідних даних та повідомлень.

Тому, *гетерогенною інформаційною системою* слід вважати складну організаційно-технічну структуру, що є засобом збору, збереження, аналізу і передачі інформації для прийняття обґрунтованих рішень у процесі планування операцій та управління військами під час ведення бойових дій.

Більшість інформаційних систем є гетерогенними та складаються з різноманітних програмно-апаратних засобів під управлінням різних операційних систем, що є суттєвою перепоною для досягнення необхідної якості обслуговування, стійкості для багатьох інформаційних систем військового призначення. Інтеграція різнотипних інформаційних систем сектору безпеки і оборони України, у тому числі й автоматизованих систем військового призначення, призвела до вразливості таких систем і дій зловмисників через кіберпростір. Функціювання гетерогенних інформаційних систем в умовах цілеспрямованих інформаційно-технічних впливів, зокрема кібервпливу противника, а також невизначеність знань про кіберпростір та діючі фактори, цілі та динаміки їх змін, призвели до потреби створення методології та технологій забезпечення сталого функціонування ГтІС ВП в умовах кібервпливу [9].

У [10] надано таке визначення *кібервпливу* – це цілеспрямований процес застосування усього наявного комплексу засобів і заходів впливу на визначені елементи кіберпростору з метою порушення процесів управління в кібернетичних системах протиборчої сторони шляхом зміни нормальних режимів їх функціонування з подальшим, або співвимірним у часі впливом, взяттям їх під власне управління та контроль.

Безумовно, що кібервпливи є успішними лише за виконання низки умов. Однією з основних умов є умова існування в сторони, що планує здійснити кібервплив повної інформаційної бази даних про об'єкти впливу за всіма сферами життєдіяльності (суспільно-політичне становище, паролі доступу до інформаційно-комунікаційних систем та мережевого обладнання, систем управління зброєю, систем управління об'єктами атомної енергетики, транспорту, банківської системи, державних органів управління тощо).

Сучасні інформаційні технології дають змогу проникати не лише у відкриті системи, а також у локальні закриті системи, що не мають виходу до загальних мереж. Для цього використовуються будь-які можливості доступу до них, в тому числі безпровідні засоби прийому-передачі інформації. Проникнення у локальні мережі використовується не лише для контролю за потоками інформації та її збору, а також з метою порушення нормального їх функціонування, за допомогою заздалегідь вмонтованих програмних та апаратних закладок. *Об'єктами кібервпливу* можуть виступати системи управління, кібернетичні системи живої та неживої природи, а саме: технічні системи різного призначення; соціум; соціотехнічні системи.

Наприкінці 2022 року, компанія з кібербезпеки Mandiant проаналізувала кіберфізичну атаку за участю угруповання хакерів Sandworm (укр. – пісочний хробак), націлену на об'єкт української критичної інфраструктури. В атаці використовувалася нова техніка, що впливала на промислові системи управління (далі – АСУ ТП) та операційні технології (далі – ОТ), що призвело до незапланованого відключення електроенергії під час ракетних ударів по Україні. Sandworm розгорнула новий варіант шкідливого програмного забезпечення CADDYWIPER в IT-середовищі жертви, демонструючи можливості кіберфізичних атак, що розвиваються, після вторгнення в Україну. Незважаючи на видалення артефактів, це не вплинуло на гіпервізор чи віртуальну машину SCADA, що вказує на потенційну відсутність координації між зловмисниками. Дана атака підкреслила інвестиції росії в атакуючі кіберможливості на ОТ-системи. Перехід Sandworm до обтічних, легких методів «Living off the Land» (укр. – життя на землі) передбачає збільшення швидкості та масштабу, що ускладнює виявлення.

Час атаки збігся з активними бойовими діями росії, що свідчить про стратегічне розгортання та гібридну війну. Еволюція тактики Sandworm наголошує на пріоритетах росії в ОТ-атаках, відображаючи перехід від відключень електроенергії в Україні в 2015–2016 роках до більш цілеспрямованих та раціональних підходів. Також простежується зв'язок між атакою Sandworm у червні 2022 року та атакою Volt Typhoon (укр. – Тайфун Вольт), спрямованою на критичну інфраструктуру США. Для досягнення своєї мети Volt Typhoon також надає велику увагу скритності, покладаючись майже виключно метод «Living off the Land» [12].

За своєю географією найбільше атак відбувається з території росії, але також можуть використовуватись майданчики союзних нам країн для проведення кібератак, що ускладнює остаточну ідентифікацію. Від початку війни тренд на зростання кількості кібератак зберігається.

Зокрема, у [13] висвітлено, що у ІІІ кварталі 2022 року за допомогою засобів системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд. подій. Кількість зареєстрованих та опрацьованих кіберінцидентів зросла – від 64 до 115. У ІІІ кварталі 2022 року фіксується істотне зростання активності хакерських груп стосовно поширення шкідливого програмного забезпечення, серед якого є як програми, що викрадають дані, так і ті, що спрямовані на знищення даних. Порівняно зі статистичними даними за ІІ квартал 2022 року, кількість кіберінцидентів з високим рівнем критичності зросла на 128%. Порівняно з І та ІІ кварталами, у ІІІ кварталі 2022 року кількість критичних подій кіберінцидентів, джерелом яких є IP-адреси росії, зросла у 35 разів. Також, порівняно з ІІ кварталом 2022 року, майже вдвічі зросла кількість детектованих подій інформаційної безпеки, пов'язаних із активним скануванням, джерелом яких є IP-адреси росії.

Проаналізувавши дії росії в кіберпросторі, можна виділити ряд принципових особливостей їх організації і проведення [13]:

вплив на критичну інформаційну інфраструктуру здебільшого має перманентний характер;

кіберпростір використовується росією як для проведення кібератак на Україну так і для проведення інформаційних операцій;

завжди спостерігається активізація дій росії в кіберпросторі в період важливих подій, політичних чи економічних змін у країні. Крім того відбуваються збільшення кіберінцидентів перед початком бойових дій. Тож можна вважати, що кібератаки тісно пов'язані з проведенням військових, інформаційних операцій чи політичних кроків. Так, наприклад, більше ніж за місяць до повномасштабного вторгнення на територію України, в середині січня, росія провела масштабну кібератаку проти понад 20 українських урядових установ, намагаючись знизити здатність країни протистояти майбутньому військовому нападу;

головні цілі росії у кіберпросторі: шпіонаж (отримання розвідданих щодо логістики, озброєння, планів та операцій Сил безпеки та оборони); спроби виведення з ладу об'єктів критичної інформаційної інфраструктури; позбавлення доступу громадян до державних послуг та сервісів, банківського обслуговування. На рисунку 1 авторами наведені випадки збігу кінетичних дій з кібератаками.

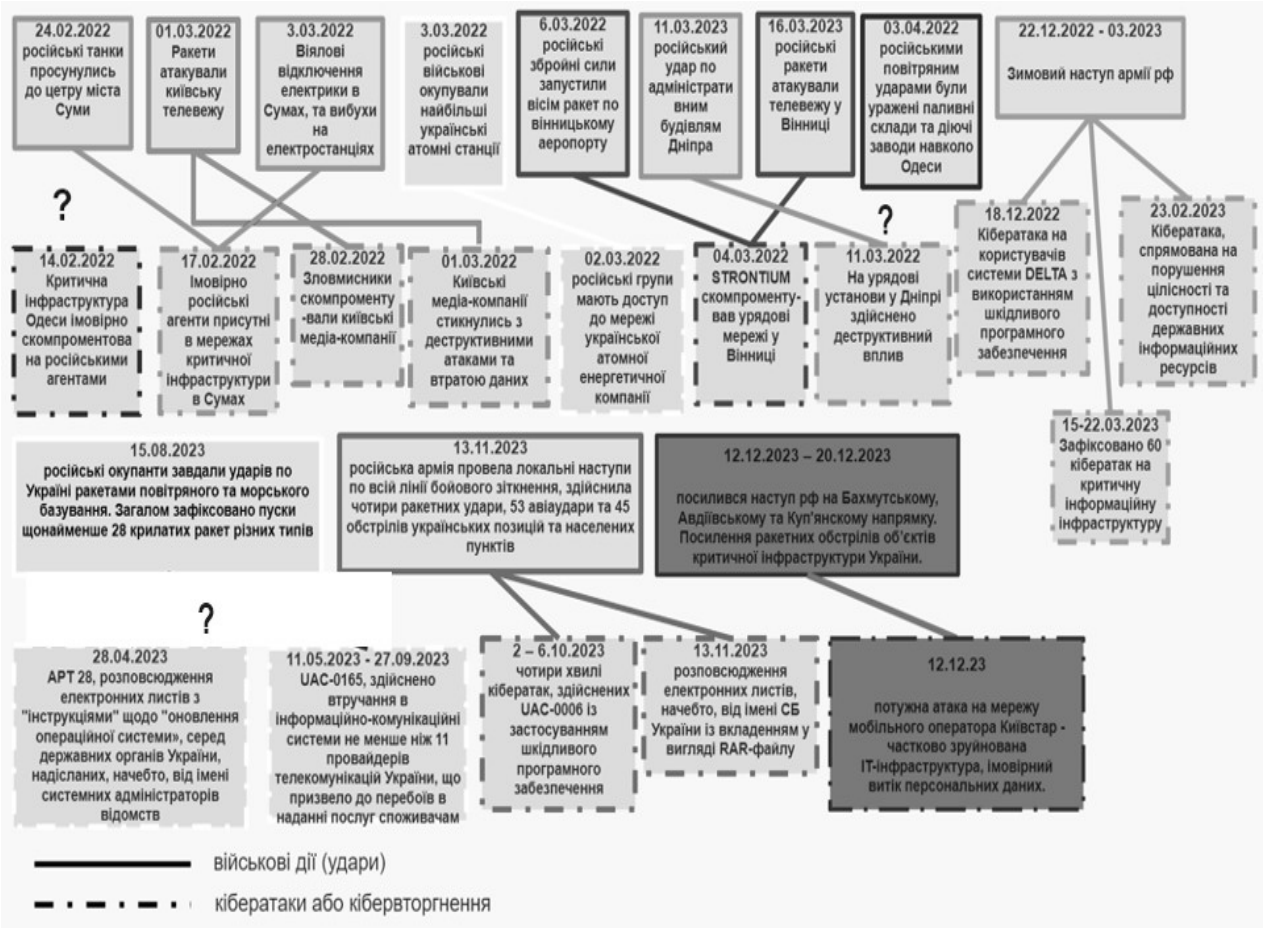

Рисунок 1 – Хронологія збігу кінетичних дій військових формувань рф з кібератаками

З початку вторгнення росії в Україну, за спостереженнями компанії Microsoft, російські групи кіберзагроз виконують дії на підтримку стратегічних і тактичних цілей своїх військових формувань. Хронологія військових ударів і кібервторгнень свідчить про кілька прикладів кібероперацій і військових операцій, що схоже, працюють у тандемі з метою спільного досягнення цілі, хоча неясно, чи існує координація, централізоване виконання завдань або просто загальний набір зрозумілих пріоритетів, що визначають кореляцію. Іноді кібератаки безпосередньо передували військовій атаці, водночас ці випадки були рідкісними. Для того, щоб зробити висновок стосовно наявності або спростування такого збігу, необхідний значно більший обсяг статистичних даних.

Кібероперації російської федерації (далі – рф) досі узгоджуються із заходами, спрямованими на деградацію, порушення або дискредитацію українських урядових, військових та економічних функцій, порушення функціонування критично важливої інфраструктури та зменшення доступу української громадськості до інформації [14]. Розглянемо ГтІС ВП, що складається з елементів S (рис. 2), на яку діє набір з М-типів кібервпливу. Елементи ГтІС ВП взаємопов'язані та втрата працездатності одного елемента впливає на працездатність інших елементів ГтІС ВП. Кількість джерел кібервпливу (далі – ДКВ) кожного типу дорівнює N_j, $j=\overline{1, M}$. Під елементами системи слід розуміти робочі станції та сервери досліджуваної ГтІС ВП. Потрібно так згрупувати типи кібервпливу і розподілити їх за елементами ГтІС ВП, щоб функція збитків досягла максимального значення [19].

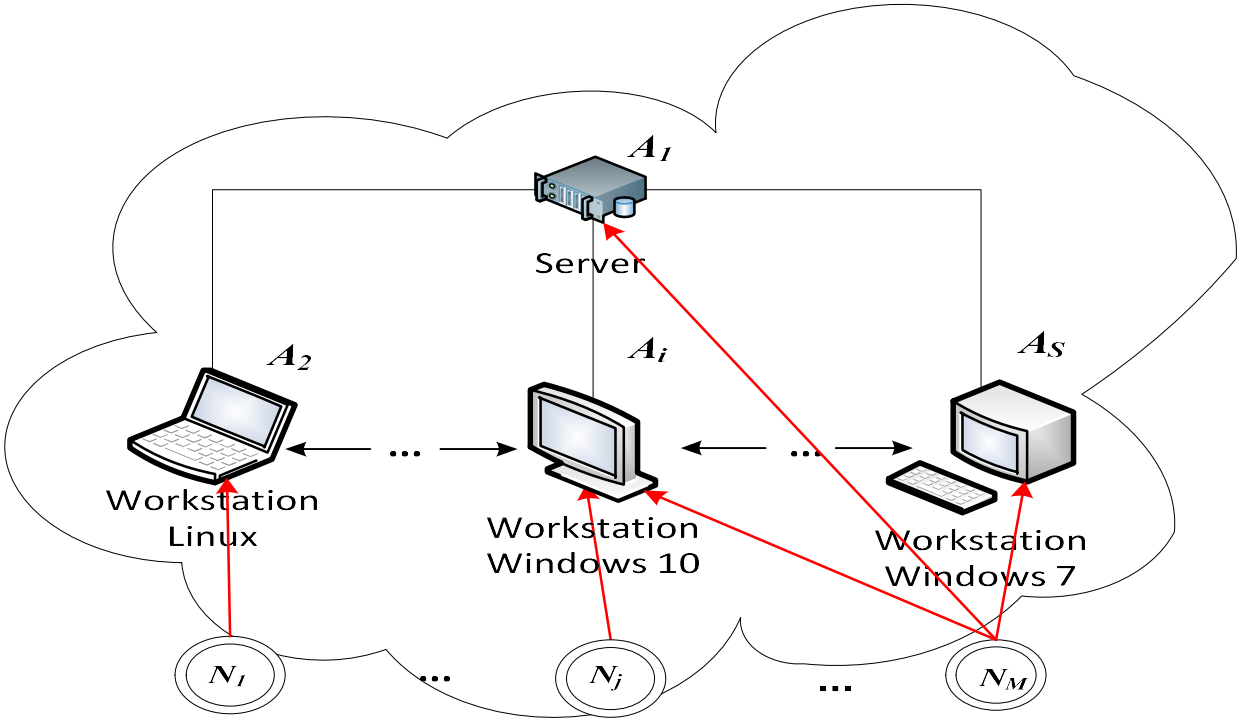

Рисунок 2 – Приклад гетерогенної інформаційної системи та наявних джерел кібервпливу

Отже, потрібно знайти вектор $X=\left\{ x_{ji}, i=\overline{1, S}, j=\overline{1, M} \right\}$ оптимального розподілу ДКВ за взаємопов'язаними елементами ГтІС ВП, щоб функція збитку досягла максимального значення:

$$F(X)=\sum_{i=1}^{S} F_i \cdot \left(1-\prod_{y=1}^{S} \left[1-\alpha_{iy} \left(1-\prod_{j=1}^{M} q_{ji}^{x_{ji}} \right) \right] \right) \to \max_{x_{ji}}, \quad (1)$$

За обмеження його компоненти:

$$\sum_{i=1}^{S} x_{ji} \le N, \ j=\overline{1, M}, \quad (2)$$

і додаткових умовах:

$$x_{ji} \in \{0,1\}, \quad (3)$$

$$\sum_{i=1}^{S}\sum_{j=1}^{M} x_{ji} = N, \quad (4)$$

$$0 \le (p_{ji}=1-q_{ji}) \le 1, \quad (5)$$

$$A_i \ge 0; \ i=\overline{1, S}; j=\overline{1, M}, \quad (6)$$

$$0 \le \alpha_{iy} \le 1; \ i=\overline{1, S}, \quad (7)$$

де A_i – відносна важливість і-го елемента ГтІС;

M – кількість типів кібервпливу;

N – загальна кількість ДКВ, які діють на ГтІС;

S – кількість елементів ГтІС ВП;

p_{ji} – ймовірність того, що ДКВ j-го типу виведе з ладу *i*-й елемент;

q_{ji} – ймовірність того, що ДКВ *j*-го типу не виведе з ладу *i*-й елемент ГтІС ВП;

$q_{ji}^{x_{ji}}$ – ймовірність того, що жодне з x_{ji} ДКВ j-го типу не виведе з ладу *i*-й елемент ГтІС ВП;

$\prod_{j=1}^{M} q_{ji}^{x_{ji}}$ – ймовірність того, що жодне з ДКВ не виведе з ладу і-й елемент ГтІС ВП;

$1-\prod_{j=1}^{M} q_{ji}^{x_j}$ – ймовірність того, що хоча б одне з ДКВ виведе з ладу і-й елемент ГтІС ВП;

$\alpha_{iy}\left(1-\prod_{j=1}^{M} q_{ji}^{x_{ji}}\right)$ – ймовірність того, що ДКВ виведе з ладу *i*-й елемент ГтІС ВП;

$\alpha_{iy}\left(1-\prod_{j=1}^{M} q_{ji}^{x_{ji}}\right)$ – що хоча б одне з ДКВ або зламаний у-ий елемент не виведе з ладу і-й елемент ГтІС ВП.

Поставлене завдання є завданням цілочисельного програмування, оскільки елементи шуканого вектора обмежуються.

Розглянемо вираз (1). Зауважимо, що за умов $x_{ji} \in \{0,1,...,N\}$.усі елементи вектора X нулі, то $F_0 = 0$. Для t-ого етапу припустимо, що буде обраний E_t елемент ГтІС ВП, тоді шукатимемо таке l_0 ДКВ, щоб різниця величин збитку ГтІС ВП на t-ом та (t–1)-ом етапах, визначається за виразом (8):

$$\Delta_{lE}^{+} = F_t^{+} - F_{t-1}^{+} =$$

$$= \sum_{i=1}^{S} A_i \cdot \left(1-\prod_{y=1}^{S}\left[1-\alpha_{iy}\left(1-\prod_{j=1}^{M} q_{ji}^{x_{ji}}\right)\right]\right) - \sum_{i=1}^{S} A_i \cdot \left(1-\prod_{y=1}^{S}\left[1-\alpha_{iy}\left(1-\prod_{j=1}^{M} q_{ji}^{x_{ji}^{t-1}}\right)\right]\right) =$$

$$= \sum_{i=1}^{S} A_l \cdot \left(\prod_{y=1}^{S}\left[1-\alpha_{iy}\left(1-\prod_{j=1}^{M} q_{ji}^{x_{ji}^{t-1}}\right)\right] - \prod_{y=1}^{S}\left[1-\alpha_{iy}\left(1-\prod_{j=1}^{M} q_{ji}^{x_{ji}^{l}}\right)\right]\right) =$$

$$= \sum_{i=1}^{S} A_i \cdot \left(\prod_{u=1}^{S}\left[\alpha_{iy}\prod_{j=1}^{M} q_{ji}^{x_{ji}^{t-1}} - \alpha_{iy} + 1\right] - \prod_{u=1}^{S}\left[\alpha_{iy}\prod_{j=1}^{M} q_{ji}^{x_{ji}^{l}} - \alpha_{iy} + 1\right]\right) = \tag{8}$$

$$= A_{E_t} \cdot \left(\prod_{\substack{u=1 \\ y\neq E_t}}^{S}\left[\alpha_{E_t y}\prod_{j=1}^{M} q_{jE_t}^{x_{jE_t}^{t-1}} - \alpha_{E_t y} + 1\right] - \prod_{\substack{u=1 \\ y\neq E_t}}^{S}\left[\alpha_{E_t y}\prod_{j=1}^{M} q_{jE_t}^{x_{jE_t}^{l}} - \alpha_{E_t y} + 1\right]\right).$$

Позначимо $c_i^t = \prod_{j=1}^{M} q_{ji}^{x_{ji}}$, тоді для розв'язання задачі (1) – (7) потрібно використовувати такий алгоритм:

1. Визначимо початкові змінні:

$$t = l;\ x_i^{(0)} = 1,\ i = \overline{1,S},\ x_{ji}^{(0)} = 0,\ j = \overline{1,M};\ F_0^{+} = 0, \tag{10}$$

2. Обчислимо вектор збільшення величин збитку ГтІС ВП:

$$\Delta_{E_t l_t}^{+} = A_{E_t} \cdot \left(\prod_{\substack{u=1 \\ y\neq E_t}}^{S}\left[\alpha_{E_t y}\, c_{E_t}^{t-1} - \alpha_{E_t y} + 1\right] - \prod_{\substack{u=1 \\ y\neq E_t}}^{S}\left[\alpha_{E_t y}\, c_{E_t}^{t-1}\cdot q_{l_t E_t} - \alpha_{F_t y} + 1\right]\right) \tag{11}$$

3. Виберемо тип засобу, що забезпечує максимальну шкоду на цьому етапі:

$$\Delta_{l_t E_t}^{+} = \max_{\substack{1\le l\le M \\ 1\le E\le S}} \Delta_{lE}^{+} \tag{12}$$

4. Зазначимо вибір у векторі X :

$$x_{ji}^{(t)} = \begin{cases} x_{ji}^{(t-l)}, & j\neq l_t,\ i\neq E_t \\ x_{ji}^{(t-l)}+1, & j=1,\ i=E_t \end{cases} \tag{13}$$

5. Перерахуємо величини c_{E_t} за таким виразом:

$$c_{E_t}^{(t)} = c_{E_t}^{(t-l)} \cdot q_{l_t E_t},\ i = \overline{1,S} \tag{14}$$

6. Отримаємо значення збитків на цьому етапі:

$$F_{t-1}^{+} = F_{t-1}^{+} + \Delta_{l_t E_t}^{+} \tag{15}$$

7. Перейдемо до наступного етапу:

$$t = t+1 \tag{16}$$

8. Якщо $t \le N$, перейдемо до п. 2, інакше до п. 9.

9. Виведемо результат X та максимальну шкоду ГІС ВП F_t^+.

Розглянемо приклад, в якому запропоновано ГтІС ВП (рис. 1), що складається з $S=3$ (2 робочих станцій та серверу) елементів, що володіють відповідно важливістю $A=(10\ 30\ 20)$, причому $\sum_{i=1}^{S} A_i$. Припустимо, що на ГтІС ВП діють $M=4$ видів ДКВ:

шкідливе програмне забезпечення (віруси, хробаки, трояни);

атаки на мережеві протоколи та служби (DDoS-атаки);

експлойти, що використовують уразливості програмного забезпечення;

соціальна інженерія.

Кількість ДКВ кожного типу дорівнює $N_j=2$, припустимо, що на кожен елемент ГтІС ВП ДКВ одного типу може впливати тільки один раз, тобто $x_{ji}\in\{0,1\}$.

Імовірності того, що ДКВ j-го типу не виведе з ладу і-й елемент ГтІС ВП, наведені матрицею:

$$Q=\begin{pmatrix} 0.5 & 0.2 & 0.3 & 0.6 \\ 0.3 & 0.4 & 0.2 & 0.3 \\ 0.5 & 0.2 & 0.3 & 0.4 \end{pmatrix} \quad (17)$$

Коефіцієнт взаємовпливу елементів ГтІС ВП, тобто ймовірності того, що вихід з ладу y-го елементу не спричинить порушення в роботі і -го елементу представлені матрицею α.

$$\alpha=\begin{pmatrix} 0 & 0.9 & 0.2 \\ 0.2 & 0 & 0.2 \\ 0.3 & 0.8 & 0 \end{pmatrix} \quad (18)$$

Потрібно обрати для кожного з $S=3$ такий набір ДКВ $M=4$ типів засобів парирування зовнішніх впливів (далі – ЗПЗВ) так, щоб величина шкоди всій системі за таких впливів була максимальною.

У результаті розгляду наведених вище аналітичних моделей, отримаємо матриці наступного виду $X=\{x_j,\ j=\overline{1,M}\}$, $X=\{x_i,\ i=\overline{1,S}\}$, $X=\{x_{ji},\ i=\overline{1,S},\ j=\overline{1,M}\}$,

де M – кількість типів ЗПЗВ;

N – кількість ДКВ, що діють на ГтІС ВП;

S – кількість елементів ГтІС ВП.

Елементи цих матриць відображають, яка кількість засобів певного типу необхідна для того, щоб вивести і-й елемент зі строю. У випадку $X=\{x_i,\ i=\overline{1,S}\}$ використовується один тип ЗПЗВ (M = 1), а при $X=\{x_j,\ j=\overline{1,M}\}$ вся ГтІС ВП розглядається як один елемент (S = 1). Необхідно для кожного елементу обрати ЗПЗВ, щоб нейтралізувати дію зовнішніх впливів та забезпечити стійкість всієї ГтІС ВП.

Розглянемо ГтІС ВП, що складається з S елементів, на і-й елемент ГтІС ВП, діє набір з M типів ДКВ. Набір представлений вектором

$$x_j=\begin{cases}1, \text{якщо } j\text{-е ДКВ діє на елемент}\\ 0, \text{в зворотньому випадку}\end{cases} \quad (19)$$

Необхідно знайти такі ЗПЗВ, щоб максимально забезпечити стійкість елементу ГтІС ВП при впливі такого набору ДКВ.

Для кожного j-го ДКВ була прорахована актуальність, виходячи з неї необхідно здійснити вибір ЗПЗВ, клас яких відповідає рівню актуальності, а саме $K_j=K(\mu_j)$, де K – повний набір ЗПЗВ, μ_j – актуальність НЗВ.

Саме серед цього набору K_j ЗПЗВ, будемо обирати той, використання яких гарантує максимальне значення стійкості *i*-го елементу ГтІС ВП.

Необхідно знайти вектор $Y=\{y_{kj},\ k=\overline{1,K_j},\ j=\overline{1,M}\}$ оптимального розподілу ЗПЗВ по елементам ГтІС ВП, щоб стійкість (12) досягла максимального значення.

$$F(Y)=A\cdot\left(1-\prod_{j=1}^{M}\left[x_j\cdot\prod_{k=1}^{K_j}\varepsilon_{kj}^{y_{kj}}\right]\right)\to\max_{y_{kj}} \quad (20)$$

та додаткових умов

$$\sum_{k=1}^{K_j} y_{kj}=1 \quad (21)$$

$$x_j=\begin{cases}1, \text{якщо } k\text{–е ЗПЗВ використовується проти j–го ДКВ}\\ 0, \text{в зворотньому випадку}\end{cases} \quad (22)$$

$$0\le\varepsilon_{kj}\le 1, \quad (23)$$

$$A\ge 0;\ j=\overline{1,M}, \quad (24)$$

$$\sum_{j=1}^{M} x_j\cdot\prod_{k=1}^{K_j} C_{kj}^{y_{kj}}\le C. \quad (25)$$

де A_i – відносна важливість і-го елемента ГтІС,

M – кількість типів ДКВ,

K_j – кількість ЗПЗВ, які можуть нейтралізувати вплив ДКВ на елемент ГІС,

ε_{kj} – ймовірність, того що k-е ЗПЗВ, не захистить від j - го ДКВ,

C_{kj} – вартість k-е ЗПЗВ,

C – загальна вартість ЗПЗВ,

$\prod_{j=1}^{M}\left[x_j\cdot\prod_{k=1}^{K_j}\varepsilon_{kj}^{y_{kj}}\right]$ – ймовірність того, що жодне з встановлених на елементі ГтІС ВП ЗПЗВ не захистить від ДКВ.

$1-\prod_{j=1}^{M}\left[x_j\cdot\prod_{k=1}^{K_j}\varepsilon_{kj}^{y_{kj}}\right]$ – ймовірність того, що хоча б одне зі встановлених на елементі ГтІС ВП ЗПЗВ захистить від ДКВ.

Використання аналітичної моделі дає змогу спрогнозувати ступінь кібервпливу та визначити набір ЗПЗВ для кожного елементу ГтІС ВП. Для отримання значення показника стійкості всієї ГтІС ВП потрібно визначити суму значень F(Y) по кожному елементу. Так, вирази (1)–(7) формалізують метод прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення та розв'язуються за запропонованим алгоритмом.

Висновки та перспективи подальших досліджень

Забезпечити стале функціонування гетерогенних інформаційних систем військового призначення можливо лише за комплексного вирішення наукових завдань з їх оцінювання під час проєктування, створення та безпосередньо в процесі функціонування, із застосуванням системного підходу. Під час проєктування та створення таких систем, зокрема, необхідно спрогнозувати, які деструктивні впливи будуть діяти на них в процесі функціонування, та здійснити оптимальний розподіл засобів, що будуть їм протидіяти.

Елементом наукової новизни є те що запропонований підхід базується на оптимальному розподілі засобів парирування зовнішніх впливів, які в свою чергу поділяються на види, за взаємопов'язаними елементами гетерогенних інформаційних систем. Сутність запропонованого підходу полягає у виборі для кожного з елементів системи та відповідного набору джерел кібервпливу, що діє на них з метою порушення сталого функціонування, оптимального розподілу типів засобів парирування зовнішніх впливів.

Теоретична значущість дослідження полягає у тому, що на онові відомих математичних методів оптимального розподілу ресурсів при синтезі складних систем, отримано новий підхід, що враховує еволюцію кібервпливів на гетерогенні інформаційні системи військового призначення. Практична цінність полягає у тому що застосування зазначеного методу, є необхідним кроком для визначення придатності гетерогенних інформаційних систем військового призначення до виконання цільової функції, та дозволить на етапі створення гетерогенних інформаційних систем військового призначення визначити можливі уразливості.

Перспективним напрямом подальших досліджень може бути розробка комплексної методики оцінювання або прогнозування ризиків та факторів, що в цілому впливають на гетерогенні інформаційні системи військового призначення, зокрема і з урахуванням кінетичних дій супротивника.

Список бібліографічних посилань

1. Про електронні комунікації: Закон України від 16.12.2020 №1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 23.09.2023). **2. Субач І. Ю.** Системи виявлення кібернетичних атак: стан справ та перспективи розвитку. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: доповіді та тези доповідей VII наук.-техн. конф, 23–24 жовт. 2014 р. Київ: ВІТІ ДУТ, 2014. С. 60–64. **3. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В.** Інформаційна та кібербезпека: соціотехнічний аспект : підручник за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ. ДУТ, 2015. 288 с. **4. Пермяков О. Ю., Толубко В. Б., Сбітнєв А. І.** Методологічні основи розробки прикладного програмного забезпечення для АСУ військового призначення: монографія. Київ: НАОУ, 2004. 188 с. **5. Пермяков О. Ю., Королюк Н. О., Фараон С. І.** Організація інформаційних систем Збройних Сил України : навчальний посібник. Київ : НУОУ ім. Івана Черняховського, 2019. 143 с. **6. Yevseiev S., Milov O., Opirskyy I., Dunaievska O., Huk O., Pogorelov V., Bondarenko K., Zviertseva N., Melenti Y., Tomashevsky B.** Development of a concept for cybersecurity metrics. *Eastern-European Journal of Enterprise Technjlogies.* 2022. Vol. 4, № 118. P. 6–18. **7. Yevseiev S., Ponomarenko V., Laptiev O., Milov O.** Synergy of building cybersecurity systems : monograph. Kharkiv. PC Technology Center, 2021. 188 p. **8. Військовий стандарт ВСТ 01.112.004 – 2017 (01)**. Військовий зв'язок та інформаційні системи. Словник НАТО з систем зв'язку та інформаційних систем (AAP-31 (Edition 3), IDT). Терміни та визначення. [Чинний від 2017-08-15]. Вид. офіц. Київ : МО України, 2017. 56 с. **9. Гук О. М., Пермяков О. Ю., Нестеров О. М., Уварова Т. В.** Аналіз існуючих підходів щодо оцінювання функціональної стійкості гетерогенних інформаційних систем. *Сучасні інформаційні технології у сфері безпеки і оборони*. 2020. Вип. 3 (39). С. 125–131. **10. Даник Ю. Г., Воробієнко П. П., Чернега В. М.** Основи кібербезпеки та кібероборони: підручник. Одеса : Вид-во ОНАЗ ім. О. С. Попова, 2018. 228 с. **11. Зв'язок та інформаційні системи**. Доктрина. Затв. Головнокомандувачем Збройних Сил України від 02.07.2020 р. №15841/С. **12. Атаки, націлені на критичну інфраструктуру, еволюціонують. 2023.** URL: https://softprom.com/ua/ataki-natsileni-na-kritichnu-infrastrukturu-evolyutsionuyut (дата звернення: 23.09.2023). **13. Левченко О. В., Охрімчук В. В.** Особливості антиукраїнського інформаційного (кібер) впливу на Україну. *Захист інформації*. 2022. Т. 24. № 4. С. 156-163. **14. Microsoft Special Report: Ukraine**. An overview of Russia's cyberattack activity in Ukraine. Digital Security Unit, April 27, 2022. URL: https://www.microsoft.com/en-us/security/business/security-insider/reports/specialreports/special-report-ukraine/ (accessed: 23.09.2023). **15. Барабаш О. В.** Методология построения функционально устойчивых распределенных информационных систем. Київ: НАОУ, 2004. 226 с. **16. Гук О. М., Чередниченко О. Ю.,**

Штонда Р. М., Диба І. О. Дії в кіберпросторі під час підготовки та ведення мережецентричної війни. *Сучасні інформаційні технології у сфері безпеки і оборони.* 2017. Вип. 2(29). С. 107–112. **17. Пеньков В. І., Штонда Р. М., Гук О. М., Мальцева І. Р., Черниш Ю. О.** Методи та засоби протидії шкідливому програмному забезпеченню. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2017. № 2 (29). С. 58-64. **18. Пермяков О. Ю., Сбітнєв А. І.** Інформаційні технології і сучасна збройна боротьба. Луганськ: Знання, 2008. 204 с. **19. Берзин Е. А.** Оптимальное распределение ресурсов и элементы синтеза систем. Под ред. Е. В. Золотова. Москва. Сов. радио, 1974. **20. Основи** моделювання бойових дій військ : підручник / За ред. О. Ю. Пермякова. Київ : НАОУ, 2005.

PROGNOSTICATION THE DEGREE OF CYBER INFLUENCE ON HETEROGENEOUS MILITARY INFORMATION SYSTEMS TAKING INTO ACCOUNT ITS EVOLUTION

Mashtalir Vadym ***(Doctor of Historical Sciences, Professor)***
Huk Oleksandr ***(Philosophy Doctor)***
Tolmachov Igor
Faraon Serhii (Philosophy Doctor)

The National Defence University of Ukraine, Kyiv, Ukraine

Formulation of the problem in general. *With the development of the latest information technologies, cyberspace is becoming an environment in which confrontation between subjects of international relations takes place in the form of cyber warfare, as well as information, network-centric, asymmetric, and hybrid wars. There is a tendency to use strategies of asymmetric indirect actions based on a combination of military efforts with political, economic, information and psychological methods of influencing the enemy to solve problems that were previously solved only by military force. In the context of targeted information and technical influences and the lack of proper professional knowledge of cyberspace, understanding of the goals and nature of actions in it, as well as the dynamics of changes in the above, there is a need to develop a method for predicting the degree of cyber influence on heterogeneous military information systems. The main objective of the method is to ensure the cybersecurity of the State in the context of active confrontation in cyberspace. This method takes into account a set of factors (threats) that have not existed before, as well as the evolution of cyber influences. Heterogeneous information systems are complex technical systems and have inherent properties, so it is advisable to use decomposition into separate information systems to describe them. The aim of the article is to develop a method for predicting the degree of cyber impact on heterogeneous military information systems to ensure their sustainable functioning in the conditions of cyber impact.*

Analysis of recent researches and publications. *In the works of the predecessors, the approach to the implementation of means of countering the external destabilizing cyber influence of the enemy in order to ensure the stable functioning of information systems of military purpose was not sufficiently considered. Also, the issue of developing specific effective algorithms and methods for assessing or predicting the stability of heterogeneous military information systems in conditions of cyber influence has not been fully considered. Today, the development of a set of analytical models and methods for predicting the degree of cyber influence on heterogeneous information systems and its consequences is an urgent problem.*

Presenting the main material*. Heterogeneous information systems are complex technical systems and have their inherent properties; therefore it is advisable to apply decomposition into separate information systems for their description. The article applies methods of analysis when considering the latest research, publications and scientific sources regarding the functioning of heterogeneous information systems for military purposes, integer programming, the maximum element and the theory of optimal distribution of resources for prognostication the degree of cyber influence. The specified methodological approach made it possible to determine a set of means of countering external influences for each element of heterogeneous information systems. A generalized structure of heterogeneous information systems is presented, which allows formalizing the process of prognostication the degree of cyber influence. A method of prognostication the degree of cyber influence on heterogeneous military information systems and its formalized mathematical description has been developed.*

An element of scientific novelty *is that the proposed approach is based on the optimal distribution of sources of cyber influence, which in turn are divided into types based on interconnected elements of heterogeneous information systems. The essence of the proposed approach consists in choosing for each of the elements of the system and the corresponding set of sources of cyber influence acting on them with the aim of disrupting the stable functioning, optimal distribution of types of means of countering external influences.*

The theoretical significance *of the research lies in the fact that, based on the update of known mathematical methods of optimal allocation of resources in the synthesis of complex systems, a new approach was obtained that takes into account the evolution of cyber influences on heterogeneous information systems of military purpose.*

The practical value *is that the application of the specified method is a necessary step for determining the suitability of heterogeneous military information systems for the performance of the target function, and will allow identifying possible vulnerabilities at the stage of creating heterogeneous military information systems.*

Conclusion and the perspectives of future researches. *It is possible to ensure sustainable functioning of heterogeneous information systems for military purposes only by comprehensively solving scientific tasks of their evaluation during design, creation and directly in the process of operation, using a systemic approach. During the design and creation of such systems, in particular, it is necessary to predict what destructive influences will act on them during operation, and to carry out the optimal distribution of means that will counteract them. A perspective direction of further research may be the development of a comprehensive methodology for assessing or prognostication risks and factors that generally affect heterogeneous information systems for military purposes, in particular, taking into account the enemy's kinetic actions.*

Keywords: *prognostication, degree of cyber influence, heterogeneous information systems for military purposes, maximum element method, cyber threats, cyber security, cyberspace, cyberattacks, cyber influence.*

References

1. ***About electronic communications*** [online], (2020). Zakon Ukrainy № 1089-IX, 16 December. Available at: https://zakon.rada.gov.ua/laws/show/1089-20#Text [Accessed 23 September 2023]. **2. Subach, I. Yu.,** (2014). Systems for detecting cybernetic attacks: state of affairs and prospects for development. In: *Priorytetni napriamky rozvytku telekomunikatsijnykh system ta merezh spetsial'noho pryznachennia: dopovidi ta tezy dopovidej VII nauk.-tekhn. konf, 23-24 zhovt. 2014 r*. Kyiv: VITI DUT,. 60-64. **3. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V.,** (2015). Information and cyber security: socio-technical aspect : Pidruchnyk za zah. red. d-ra tekhn. nauk, profesora V. B. Tolubka. Kyiv. DUT,. 288. **4. Permiakov, O. Yu., Tolubko, V. B., Sbitniev, A. I.,** (2004). Methodological foundations of development of application software for ACS of military purpose. monohrafiia. Kyiv: NAOU, 188. **5. Permiakov, O. Yu., Koroliuk, N. O., Faraon, S. I.,** (2019). Organization of information systems of the Armed Forces of Ukraine : navchal'nyj posibnyk. Kyiv : NUOU im. Ivana Cherniakhovs'koho, 143. **6. Yevseiev, S., Milov, O., Opirskyy, I., Dunaievska, O., Huk, O., Pogorelov, V., Bondarenko, K., Zviertseva, N., Melenti, Y., Tomashevsky, B.,** (2022). Development of a concept for cybersecurity metrics. *Eastern-European Journal of Enterprise Technjlogies.* 4, 118, 6–18. **7. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O.,** (2021). Synergy of building cybersecurity systems. Monograph. Kharkiv. PC Technology Center. **8. Military standard MST 01.112.004 – 2017 (01),** (2017). *Military communication and information systems. NATO Dictionary of Communication and Information Systems (AAP-31 (Edition 3), IDT). Terms and definitions.* [Chynnyj vid 2017-08-15]. Vyd. ofits. Kyiv : MO Ukrainy, 56. **9. Huk, O. M., Permiakov, O. Yu., Nesterov, O. M., Uvarova, T. V.,** (2020). Analysis of existing approaches to assessing the functional stability of heterogeneous information systems. *Suchasni informatsijni tekhnolohii u sferi bezpeky i oborony.* 3 (39), 125-131. **10. Danyk, Yu. H., Vorobiienko, P. P., Cherneha, V. M.,** (2018). Fundamentals of cyber security and cyber defense : pidruchnyk. Odesa : Vyd-vo ONAZ im. O. S. Popova. **11. Communication and information systems.** Doktryna. Zatv. Holovnokomanduvachem Zbrojnykh Syl Ukrainy vid 02 July 2020 №15841/S. **12. Attacks targeting critical infrastructure are evolving.** [online], (2023). *Softprom*: Available at: https://softprom.com/ua/ataki-natsileni-na-kritichnu-infrastrukturu-evolyutsionuyut [Accessed 23 September 2023]. **13. Levchenko, O. V., Okhrimchuk, V. V.,** (2022). Peculiarities of anti-Ukrainian informational (cyber) influence on Ukraine. *Zakhyst informatsii*.. 24, 4, 156-163. **14. Microsoft Special Report: Ukraine**. An overview of Russia's cyberattack activity in Ukraine. Digital Security Unit, April 27 [online], (2022). Available at: https://www.microsoft.com/en-us/security/business/security-insider/reports/specialreports/special-report-ukraine/ [Accessed 23 September 2023]. **15. Barabash, O. V.,** (2004). Methodology of building functionally stable distributed information systems. Kyiv: NAOU, 226. **16. Huk, O. M., Cherednychenko, O. Yu., Shtonda, R. M., Dyba, I. O.,** (2017). Actions in cyberspace during the preparation and conduct of a network-centric war. *Suchasni informatsijni tekhnolohii u sferi bezpeky i oborony.* 2 (29), 107-112. **17. Pen'kov, V. I., Shtonda, R. M., Huk, O. M., Mal'tseva, I. R., Chernysh, Yu. O.,** (2017). Methods and means of combating malicious software. *Suchasni informatsijni tekhnolohii u sferi bezpeky ta oborony.* 2 (29), 58-64. **18. Permiakov, O. Yu., Sbitniev, A. I.,** (2008). Information technologies and modern armed struggle. Luhans'k: Znannia,. 204. **19. Berzin, E. A.,** (1974). Optimal resource allocation and elements of system synthesis. Pod red. E. V. Zolotova. Moskva. Sov. radio. **20. Basics** of military military action modeling : pidruchnyk / za red. O. Yu. Permiakova. Kyiv. NAOU, 2005.