УДК 004.056; 005.8; 519.8 https://doi.org/10.33271/ebdut/87.034

ЗРІЛІСТЬ СИСТЕМИ КІБЕРБЕЗПЕКИ КРАЇНИ В УМОВАХ ВІЙНИ: ТЕНДЕНЦІЇ ОЦІНЮВАННЯ

Т. В. Доценко, доктор філософії, Сумський державний університет,
t.dotscenko@uabs.sumdu.edu.ua, orcid.org/0000-0001-5713-2205,
М. В. Кузьменко, аспірант, Сумський державний університет,
mkuzmenko1984@gmail.com, orcid.org/0009-0008-2049-5190

Методологія дослідження. Під час дослідження використано такі методи, як: індуктивний підхід – при формулюванні сутності поняття зрілості системи кібербезпеки країни у військових умовах; дедуктивним методом виведено поняття оцінювання зрілості системи кібербезпеки країни під час військових дій; шляхом контент-аналізу виділено ключові елементи оцінки зрілості національної системи кібербезпеки в умовах війни; на основі застосування стратегічного аналізу визначено основні вектори оцінювання досліджуваної проблеми, виокремити новітні підходи оцінки національної системи кібербезпеки.

Результати. Визначено останні тенденції оцінювання зрілості системи кібербезпеки країни, враховуючи аспект військових умов: проаналізовано існуючу нормативно-правову законодавчу базу міжнародного та національного рівнів; сформульовано поняття зрілості та оцінювання зрілості системи кібербезпеки країни під час військових дій. У роботі окреслено ключові елементи оцінки зрілості національної системи кібербезпеки в умовах проведення воєнних операцій: адаптивність, суміжність, готовність, партнерство, кіберрезерви, вразливості та загрози, навчання. Визначено основні вектори оцінювання: оцінка кіберзагроз, кібератак, захисту інфраструктури, взаємодії суб'єктів кібербезпеки, рівня підготовки кадрів; виокремлено новітні підходи оцінки системи. Сформовано схему майбутніх ключових викликів, тенденцій, рекомендацій щодо оцінки зрілості національної системи кібербезпеки в умовах війни.

Новизна. Під час дослідження особливостей оцінювання зрілості системи кібербезпеки країни ідентифіковано ключові елементи, вектори, підходи, методики до оцінки системи кіберзахисту. Виявлено слабкі місця та вразливості, визначено наявний прогрес у розвитку кіберзахисту системи, продемонстровано необхідні активності для посилення ефективності національної безпеки в умовах війни.

Практична значущість. Узагальнено досвід попередніх надбань щодо функціонування систем кібербезпеки, виявлено найефективніші практики та методики кіберстійкості, запропоновано рекомендації щодо оцінки зрілості національної системи кібербезпеки в умовах війни, що дозволить оптимізувати наявні та потенційні ресурси, а також допоможе сформувати передумови для подальшої побудови новітньої моделі оцінки кіберзахисту.

Ключові слова: кібербезпека, зрілість системи, методики оцінювання, моделювання кіберзахисту, кіберризики, кібервразливості.

Постановка проблеми. У сучасному світі, де цифрові технології пронизують усі напрямки і сфери життєдіяльності, одним із ключових елементів постає кібербезпека, як складова національної безпеки країни. А зі стрімким розвитком цифрових трансформацій економіки, системи кіберзахисту набувають критичної важливості. Оскільки запровадження новітніх технологій з одного боку дозволяє отримати нові можливості для економічного зростання, інновацій, а з іншого підвищує вразливість до ризику кіберзагроз. Особливо питання кіберзахисту загострюються у державах, що знаходяться

в умовах війни. Наряду з іншими військовими загрозами, кібернапади стають реальними зловмисними діями, що призводить до порушення нормального, безперебійного функціонування інформаційних систем, пошкодження, знищення, викрадення інформації, паралізування комунакаційних систем, зупинки електрозабезпечення, збоїв у фінансових транзакціях, поширення дезінформації населення, що негативно відображається на економіці та безпеці держави. Кібератаки можуть проводитись різними методами, серед яких злам систем безпеки, віруси, фішинг, DDoS-атаки, трояни та інші незаконні операцій [21].

Таким чином, сучасна економіка потребує формування комплексного, системного підходу до кібербезпеки. А в умовах війни, коли до традиційних форм ведення бойових дій додаються кібероперації, відсутність ефективної системи кіберзахисту матиме ще складніші наслідки дестабілізації економіки, підриву довіри до державних інституцій. Все це вимагає від керівництва держави не просто наявності елементарної інфраструктури кіберзахисту, а розвиненої, гнучкої системи оперативного реагуванні на можливі загрози.

В свою чергу якість діючої системи кібербезпеки країни можна забезпечувати через систематичне оцінювання стану такої системи, що передбачає методику щодо вивчення та аналізу її спроможності ідентифікувати, нівелювати та запобігати кіберзагрозам. А зрілість системи кіберзахисту повинна містити технічні, організаційні аспекти, тобто наявність актуальних захисних технологій і технічних засобів, відповідну прозору нормативно-правову основу, високий рівень підготовки і кваліфікації працівників, чіткість кроків реагування на випадки атак, інтеграцію системи кібербезпеки до стратегії національної безпеки держави.

Отже, визначення останніх тенденцій оцінювання зрілості системи кібербезпеки країни в умовах війни є особливо актуальним. Це дозволить узагальнити досвід попередніх надбань, виявити найефективніші практики та методики, оптимізувати ресурси, а також допоможе сформувати передумови для подальшої побудови новітньої моделі оцінки кіберзахисту.

Аналіз останніх досліджень і публікацій. Зазначимо, що кожна галузь має свої особливості забезпечення кіберзахисту, що підтверджують трактати сучасних науковців: у сфері охорони здоров'я – Хамід К. та ін. [9], Рокко Б. та ін. [19], Васильєва Т. та ін. [24]; у фінансовій сфері – Сігетова К. та ін. [21], Лєонов С. та ін. [16], Доценко Т. та ін. [7]; у сфері комп'ютерних наук – Дженкінс Дж. та ін. [13]; та ін.

Особливої уваги заслуговують роботи вчених щодо різних підходів до оцінювання та побудови моделей систем кібербезпеки: Алгулієв Р. та ін. [18] пропонують підхід до оцінки критичності функціональних вразливостей компонентів кіберфізичної системи. Моделюванню процесів кібербезпеки присвячені праці таких фахівців галузі, як: Фоліно, Ф. та ін. [8] щодо застосування моделі розподіленої класифікації шкідливого програмного забезпечення; Анджелеллі М. та ін. [17], Кротті Дж. та ін.[4] представляють моделі оцінювання і прогнозування кіберризиків; Се Джей [25] пропонує модель оцінки поінформованості сприйняття та запобігання ризикам у сфері кібербезпеки; та ін.

У статті Хаускен К. [14] досліджуються операції, методології, стратегії в оборонній літературі; Карло А. та ін. [2] аналізують особливості кібератак на критичну інфраструктуру та супутниковий зв'язок; Альджохані Т. та ін. [1] розкривають прогалини, стандартизацію та пом'якшення кібератак на енергетичні інфраструктури як сучасної зброї війни. Також сучасні науковці, такі як: Кравчук Д. та ін. [15] аналізують соціальні аспекти інформаційної безпеки в умовах гібридної війни в Україні; Кремер Ф. та ін. [3] пропонують можливі рішення для страхування ризиків кібервійни; Шарма М. [20] описує роль експертних систем на основі штучного інтелекту в кіберзахисті при збройних конфліктах; Шмюзер Й. та ін. [22] висвітлюють сильні сторони та недоліки порад щодо безпеки та конфіденційності під час російського вторгнення в Україну у Twitter; Хансен Ф. [10] обговорює специфіку російської миротворчої військової діяльності в Україні; та ін.

Отже, досліджуване питання визначення останніх тенденцій оцінювання зрілості системи кібербезпеки країни в умовах

війни є переважно новим, а з огляду на сучасні військові умови, є мало вивченим і потребує поглибленого розгляду.

Формулювання мети статті. Метою статті є визначення останніх тенденцій оцінювання зрілості системи кібербезпеки країни в умовах війни.

Виклад основного матеріалу дослідження. Для дослідження зрілості системи кібербезпеки необхідно наголосити на існуючій нормативно-правовій базі, законах, постановах та міжнародних документах, що регулюють та координують напрям кіберзахисту на міжнародному та національному рівнях. Міжнародна діяльність вектору дослідження базуються на таких стандартах та угодах: Конвенція Ради Європи про кіберзлочинність – Будапештська конвенція [26], Нормативні документи ООН щодо кібербезпеки – Резолюції Генеральної Асамблеї ООН «Міжнародне співробітництво в кіберпросторі», міжнародні стандарти управління інформаційною безпекою та управління ризиками ISO/IEC 27001 [11], ISO/IEC 27002 [12], та ін. Також Європейське законодавство регулюється Європейською кіберстратегією [23], Директивою ЄС NIS 2 [5], Директивою про кібербезпеку критичних суб'єктів [6], та ін.

В Україні діє Закон України «Про основні засади забезпечення кібербезпеки України» [30], Стратегія кібербезпеки України [31], Постанови Кабінету Міністрів України: «Про затвердження Положення про Державну службу спеціального зв'язку та захисту інформації України» [27], «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури України» [28], Постанова НБУ «Про затвердження Положення про організацію кіберзахисту в банківській системі України» № 178 [29] тощо.

На основі індуктивного підходу сформульовано поняття зрілості системи кібербезпеки країни в умовах війни як здатності держави ефективно координувати та нівелювати загрози у кіберпросторі, спроможність національної кіберінфраструктури протистояти кібератакам, захищатися від кіберзагроз, ідентифікувати кіберризики, оперативно адаптуватися до нових небезпек, своєчасно коригувати зміни у системі кіберзахисту, що виникають у відповідь на тиск і напади ворога, інтегруючи відповідні рекомендації до стратегії національної безпеки. Дедуктивним методом виведено поняття оцінювання зрілості системи кібербезпеки країни в умовах війни як процесу вимірювання рівня спроможності національної кіберсистеми протистояти кіберзлочинам, включаючи аналіз поточного стану захищеності, ідентифікацію вразливостей, оцінку готовності реагувати на атаки, виділення векторів подальшого вдосконалення.

Для реалізації оцінювання зрілості системи кібербезпеки виділено головні складові її оцінки шляхом контент-аналізу. Так, ключові елементи оцінки зрілості національної системи кібербезпеки у військових умовах включають ряд аспектів, представлених на рисунку 1.

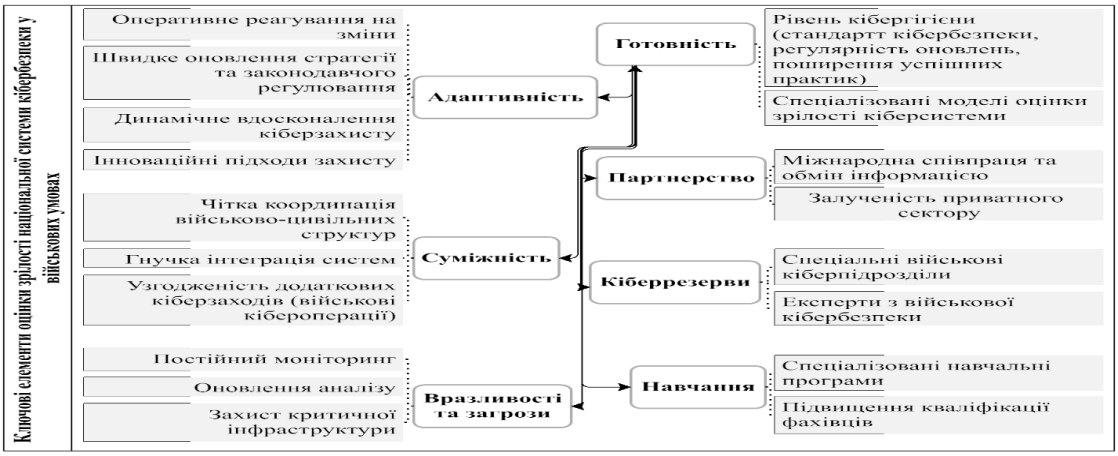

Рис.1. Схема ключових елементів оцінки зрілості національної системи кібербезпеки у військових умовах*

**Побудовано авторами за допомогою Bizagi Modeler*

Також, для комплексного оцінювання системи кіберзахисту, шляхом стратегічного аналізу, сформульовано не тільки її певні складові, а й визначено основні вектори, за якими рекомендовано оцінювати зрілость системи кібербезпеки, що представлено в таблиці. 1.

Таблиця 1

Основні вектори оцінювання зрілості системи кібербезпеки в умовах війни*

Назва	Опис
Оцінка кіберзагроз	оцінка типів загроз та оцінка рівнів загроз, що виникають у країні під час військових умов, оцінка здатності вчасного виявлення та нівелювання кіберзагроз
Оцінка кібератак	оцінка інцедентів у військовий час, оцінка швидкості реакції на атаки, оцінка ефективрсті заходів протидії атакам, оцінка оперативності відновлення працездатності системи після нападів
Оцінка захисту інфраструктури	оцінка ступеня захищеності фундаментальних секторів, а саме: енергетичної, комунікаційної, транспортної, фінансової систем
Оцінка взаємодії суб'єктів кібербезпеки	оцінка рівня координації та інтеграції між державними структурами, приватним сектором, міжнародними організаціями
Оцінка рівня підготовки кадрів	оцінка рівня компетентності спеціалістів, оцінка частоти та систематичності, безперервності професійного розвитку, оцінка якості проведення навчань і тренінгів, оцінка якості та доступності навчальних інструментів, оцінка рівня готовності персоналу, оцінка відповідності кадрів стандартам безпеки за військових умов

**Сформовано авторами*

Серед новітніх підходів оцінки національної системи кібербезпеки відмічено оцінку та прогнозування кіберризиків (щодо зростання спрямованих кібератак з боку ворога, порушення роботи критичних систем, фінансових інститутів і промислових мереж, інформаційних атак), оцінку вразливостей (щодо технічних вразливостей базової інфраструктури, невідповідних умов мережевої системи, організаційних вразливостей, людської недбалості чи некомпетентності), оцінку шкідливого програмного забезпечення (щодо програм, призначених для цілеспрямованих масштабних атак на урядові системи, фінансові заклади, організації охорони здоров'я, системи керування важливими промисловими процесами), оцінку обізнаності про кіберзагрози у військових умовах (щодо обізнаності військових, населення, цивільних кадрів про військові кіберзагрози), а саме:

1. Методика оцінки критичності вразливостей компонентів кіберфізичної системи – комплексний кількісний метод, що включає застосування загальної системи оцінки вразливостей для кількісного аналізу вразливостей, генерування баєсівського графа атак на основі структури кіберфізичної системи з урахуванням відомих вразливостей, ранжування та визначення найвразливіших компонентів системи на основі використання методу багатокритеріального аналізу та прийняття рішень PROMETHEE II (формула 1) [18]. Передбачає оцінювання на основі моделі загроз і трьох сценаріїв кібератак на кіберфізичну систему.

$$\theta(\alpha) = \theta^{+}(\alpha) - \theta^{-}(\alpha) \qquad (1)$$
$$\theta^{+}(\alpha) = \frac{\sum_{o \in G} \pi(\alpha, o)}{m-1}$$
$$\theta^{-}(\alpha) = \frac{\sum_{o \in G} \pi(o, \alpha)}{m-1}$$

де θ – чистий переважаючий потік, θ^{+}, θ^{-} – відповідно позитивний і негативний переважаючий потік, α – альтернатива, G – набір доступних альтернатив, о - вузол.

Для оцінки використовуються компоненти щодо транспортування природного газу по трубопроводу, та наступні показники-критерії: базова оцінка, оцінка впливу, підпоказник придатності до експлуатації, вектор атаки, взаємодія користувача, необхідні привілеї, складність використання.

2. Модель розподіленої класифікації здовмисного програмного забезпечення (VFL_MoE) – підхід комплексного виявлення зловмисного ПЗ, що грунтується на архітектурі нечисельної групи експертів подібної до «Mixture of Experts (MoE)» для федералізованого, децентралізованого навчання, а також застосування вертикального інтегрованого навчання за допомогою поєднання методів зменшення даних і умовних обчислень, з розподіленим алгоритмом для навчання моделі (формула 2) [8]. Точність моделі забезпечується компромісом між продуктивністю, конфіденційністю та енергозбереженням.

$$\begin{gathered} OM = \left[OM_g\ OE_i\right]^t \\ f(a) = \tilde{g}(a_0)^t[f_i(a_i)]^t, \\ A = A_0 * A_1 * A_m, A \to [0,1], \\ a = [a_0, \dots, a_m]^t \in A_i, \tilde{g}(a_0) \\ = Softmax\ (Top(g(a_0), l) \end{gathered} \quad (2)$$

де OM – оптимізована модель VFL_MoE; M_g та E_i – відповідно оптимізовані параметри розріджених воріт та експертних класифікаторів; $f(a)$ – функція класифікацій, a – вхідні маркери, $g(a_0)$ – механізм воріт, що втілює принцип умовних обчислень, $Softmax$ – функція забезпечення імовірнісної інтерпретації оцінок, Top – функція повернення вектора.

Для розрахунків використовується набор даних KronoDroid як еталон у сфері кібербезпеки, щодо доброякісних і безпечних, а також шкідливих зразків програмного забезпечення Android, з їх динамічними та статичними ознаками. Ключові показники оцінки моделі: показник точності, площа під робочими характеристиками приймача, оцінка F1, рівень хибнопозитивних результатів.

3. Модель оцінки кіберризиків – підхід для визначення пріоритетів кібервразливості, врегулювання невизначеності кіберризику [17]. Передбачає застосування середньоквантільної регресії для прогнозування впливу кібервразливостей (формула 3), введення індексу точності для врахування невідомих вразливостей і прогнозування рангу, на освнові якісних і кількісних оцінок ризиків.

$$F_{A|B}(A \le a|b) = \frac{P(A \le a \wedge B = b)}{P(B = b)}, \quad (3)$$

де $F_{A|B}$ – кількість, що описується функцією середнього кумулятивного розподілу, якої стосується умовний розподіл, ймовірність рівнів пріоритету; A оцінок серйозності та тяжкості вразливостей, база даних Computer Security Incident Response Team щодо оновлень вразливостей, Exploit Database та Vul Database – регресори з ненульовою масою ймовірності; $P(A \le a \wedge B = b)$ – ймовірність впливу з характеристиками кібервразливості; $P(B = b)$ – ймовірність ознак.

Для оцінки кібербезпеки цифрової системи використано бази даних: Shodan Internet Exposure Daschboard щодо відкриттх хостів або IP-адрес з відомими вразливими місцями, National Vulnerability Database щодо експлойтів, які використовують вразливості, та їх цін, Tenable оцінка щодо рейтингу пріоритету вразливостей.

Модель сприйняття та запобігання ризикам мережевої обізнаності (the Deep Reinforcement Learning-assisted Network Awareness Risk Perception and Prevention Model (DRL-NARPP)) – підхід для виявлення шкідливих дій у сфері кібербезпеки на основі концепції обізнаності про мережу та її стан [25]. Передбачає застосування моделі дослідження ризиків на основі алгоритму глибокого підкріплювального навчання Q-Learning з використанням мережевої обізнаності для виявлення зловмисної активності у сфері кіберзахисту. Такий алгоритм включає постійні монітоинг і оцінку стану мережі IoT з огляду факторів конфігурації активів, шаблонів трафіку, вразливостей, а також забезпечує автономне навчання та адаптацію до змін мережевих налаштувань, виявляючи ризики в реальному часі. Ефективність моделі перевіряється коефіцієнтом виявлення аномалій, коефіцієнтом точності прогнозування атак, коефіцієнтом оцінки ризику мережі та рівнем хибних результатів.

При цьому динаміка кіберстану характеризується формулою 4:

$$y(t) = f\big(t, y, e, d;\ \theta(t, a, p)\big); y(t_0) \quad (4)$$

де y, e, d – це відповідно фізичні стани, контрольний вхід і збурення; $\theta(t, a, p)$ – кібер-

стани в часі (t) відповідно з кібератакою (a) та захистом (p).

Для оцінки моделі використано набор даних Kaggle Edge-IIoTset Cyber Security Dataset щодо кібербезпеки стосовно звичайної мережевої активності та зловмисних атак.

В свою чергу, для забезпечення адекватної стійкості системи кіберзахисту, її готовності до нових загроз, потрібно оцінювати та прогнозувати майбутні ключові виклики та тенденції, та рекомендації до них, що у найближчі року можуть формувати область кіберконфліктів для держав з активними військовими діями (рисунок 2).

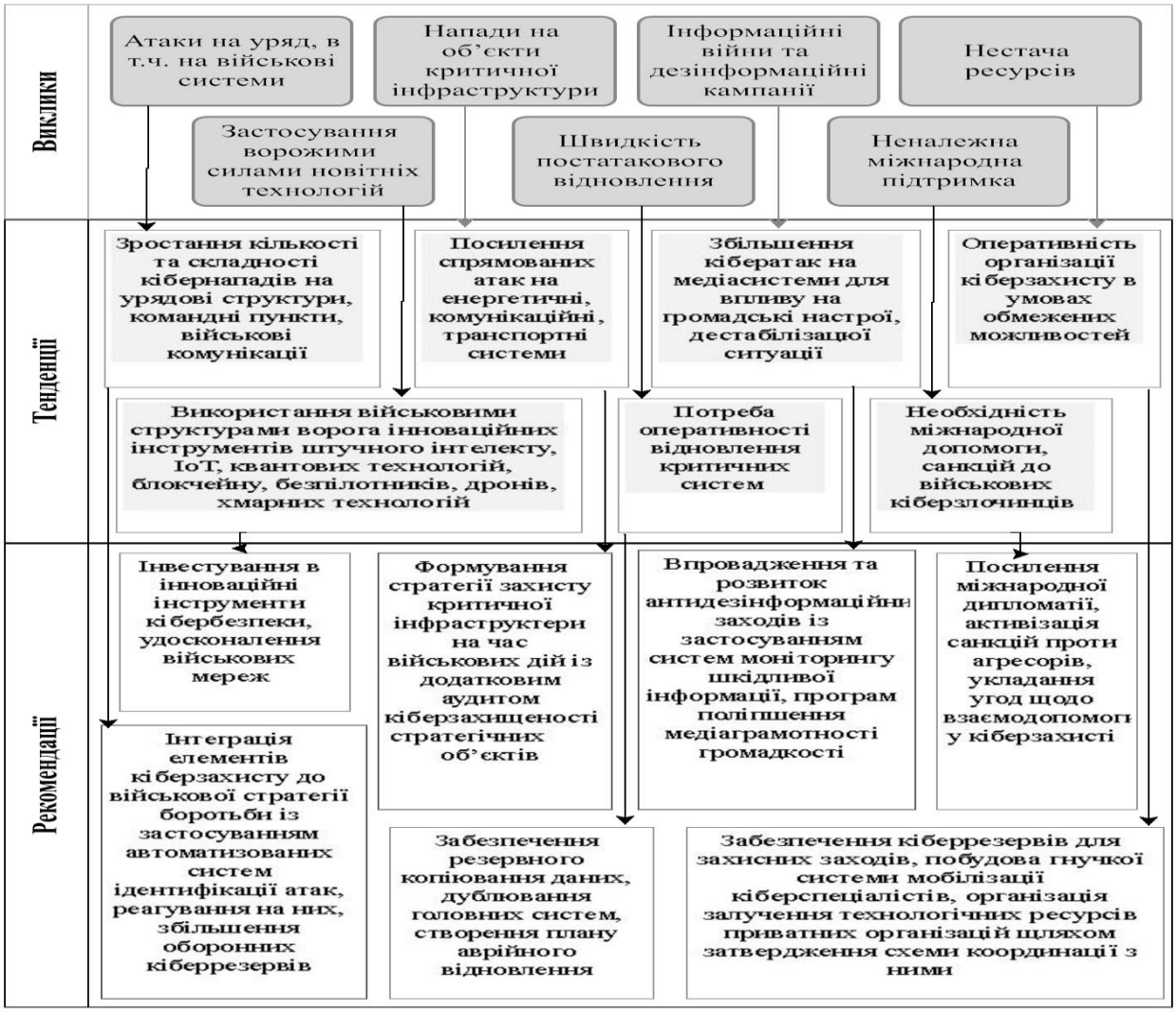

Рис.2. Схема майбутніх ключових викликів, тенденцій, рекомендацій щодо оцінки зрілості національної системи кібербезпеки в умовах війни*

**Побудовано авторами за допомогою Bizagi Modeler*

Зазначена схема описує унікальність і інтенсивність військових кіберзагроз, створюючи нові виклики для держав, що опиняються у військових умовах.

Висновки. Оскільки кібератаки у сучасному економічному світі стають все більш поширеними, рекомендується, щоб кожна країна на глобальному та локальному рівнях мала системи оцінки кіберзахисту для виявлення загроз та вразливих місць, з якими вони стикаються, визначення ймовірного впливу у разі виникнення цих загроз. При чому військові умови вимагають значного прискорення розвитку та оцінки зрілості кібербезпеки держави, оскільки кіберзахист стає критично важливим для забезпечення національної безпеки і стійкості країни.

Отже, у дослідженні було визначено останні тенденції оцінювання зрілості сис-

теми кібербезпеки країни, в тому числі враховуючи аспект військових умов:зазначено існуючу нормативно-правову законодавчу базу міжнародного та національного рівнів; застосовуючи індуктивний підхід, сформульовано поняття зрілості системи кібербезпеки країни у військових умовах; дедуктивним методом виведено поняття оцінювання зрілості системи кібербезпеки країни під час військових дій. У роботі на основі контент-аналізу окреслено ключові елементи оцінки зрілості національної системи кібербезпеки за воєнних операцій: адаптивність, суміжність, готовність, партнерство, кіберрезерви, вразливості і загрози, навчання. Далі, із застосуванням стратегічного аналізу, визначено основні вектори оцінювання досліджуваної проблеми: оцінка кіберзагроз, оцінка кібератак, оцінка захисту інфраструктури, оцінка взаємодії суб'єктів кібербезпеки, оцінка рівня підготовки кадрів. Після чого відмічено новітні підходи оцінки національної системи кібербезпеки: методика оцінки критичності вразливостей компонентів кіберфізичної системи; модель розподіленої класифікації здовмисного програмного забезпечення; модель оцінки кіберризиків; модель сприйняття та запобігання ризикам мережевої обізнаності. В результаті сформовано схему майбутніх ключових викликів, тенденцій, рекомендацій щодо оцінки зрілості національної системи кібербезпеки в умовах війни.

Оцінювання зрілості системи кібербезпеки країни головним чином дозволяє виявити слабкі місця та вразливості, оцінити наявний прогрес у розвитку кіберзахисту системи, визначити необхідні активності для посилення ефективності національної безпеки в умовах війни.

Результати дослідження можуть допомогти фахівцям сфери кіберзахисту приймати більш обґрунтовані рішення при виявленні вразливостей і ризиків системи кібербезпеки для забезпечення заходів безпеки та запобігання кібератакам. Це дозволить узагальнити наявний досвід кібербезпеки, виявити найефективніші практики та методики кіберзахисту, направити ресурси на найефективніші заходи кіберстійкості, допоможе сформувати передумови для розробки новітньої адаптивної моделі оцінки системи кіберзахисту.

Робота виконана в рамках теми дослідження «Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором», номер державної реєстрації: № 0124U000544.

Література

1. Aljohani T.M. Cyberattacks on Energy Infrastructures as Modern War Weapons-Part II: Gaps, Standardization, and Mitigation. *IEEE Technology and Society Magazine*. 2024. 43(2). 70-77. https://doi.org/10.1109/MTS.2024.3395697

2. Carlo A., & Obergfaell K. Cyber attacks on critical infrastructures and satellite communications. *International Journal of Critical Infrastructure Protection*, 2024. 46. 100701. https://doi.org/10.1016/j.ijcip.2024.100701

3. Cremer F., Sheehan B., Mullins M., Fortmann M., Ryan B.J., & Materne S. On the insurability of cyber warfare: An investigation into the German cyber insurance market. *Computers & Security*. 2024. 142. 103886. https://doi.org/10.1016/j.cose.2024.103886

4. Crotty J., & Daniel E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*. 2022. (ahead-of-print). https://doi.org/10.1108/ACI-07-2022-0178.

5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. (2022). European Union. http://data.europa.eu/eli/dir/2022/2555/2022-12-27

6. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. (2022). European Union. http://data.europa.eu/eli/dir/2022/2557/oj

7. Dotsenko T., Dvořák M., Lyeonov S., & Kovács A. Socially relevant factors of organizational mortality of enterprises: context of corporate sustainability in European countries. *Economics and Sociology*. 2023. 16(1). 284-299. DOI: 10.14254/2071-789X.2023/16-1/18.

8. Folino F., Folino G., Pisani F.S., Pontieri L., & Sabatino P. Efficiently approaching vertical federated learning by combining data reduction and conditional computation techniques. *Journal of Big Data*. 2024. 11(1). 77. https://doi.org/10.1186/s40537-024-00933-6

9. Hameed K., Naha R., & Hameed F. Digital transformation for sustainable health and well-being: a review and future research directions. *Discover Sustainability*. 2024. 5(1). 104. https://doi.org/10.1007/s43621-024-00273-8

10. Hansen F.S. The Russian approach to peacekeeping. *International Affairs*. 2024. 100(3), 1023-1042. https://doi.org/10.1093/ia/iiae072

11. INFORMATION SECURITY CONTROLS. (2022). In *ISO/IEC 27001:2022* (S. 28-36). IT Governance Publishing. https://doi.org/10.2307/j.ctv30qq13d.8

12. ISO 27002. (2023). In *ISO 27001/ISO 27002* (S. 71-76). IT Governance Publishing. https://doi.org/10.2307/jj.9039966.9

13. Jenkins J., & Roy K. Exploring deep convolutional generative adversarial networks (DCGAN) in biometric systems: a survey study. *Discov Artif Intell.* 2024. **4**, 42 https://doi.org/10.1007/s44163-024-00138-z.

14. Kjell Hausken Fifty Years of Operations Research in Defense. *European Journal of Operational Research.* 2024. 318. Issue 2. 355-368, https://doi.org/10.1016/j.ejor.2023.12.023.

15. Krawczyk D., Babenko V., Yemchuk L., Lienkov S., Dzhulii V., Dzhulii L., & Muliar I. Analysis of Information Security Under the Conditions of Hybrid War in Ukraine: Social Aspects. *Management Systems in Production Engineering.* 2024. 32(2). 235-243. https://doi.org/10.2478/mspe-2024-0023

16. Lyeonov S., Kuzmenko O., Yarovenko H. & Dotsenko T. The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. *Marketing and Management of Innovations.* 2019. 3. 308-326. http://doi.org/10.21272/mmi.2019.3-24.

17. Mario Angelelli, Serena Arima, Christian Catalano, & Enrico Ciavolino. A robust statistical framework for cyber-vulnerability prioritisation under partial information in threat intelligence. *Expert Systems with Applications.* 2024. 255 B. https://doi.org/10.1016/j.eswa.2024.124572.

18. Rasim Alguliyev, Ramiz Aliguliyev, Lyudmila Sukhostat An approach for assessing the functional vulnerabilities criticality of CPS components. *Cyber Security and Applications.* 2024. Volume 3. https://doi.org/10.1016/j.csa.2024.100058.

19. Rocco B., Moschovas M.C., Saikali S. *et al.* Insights from telesurgery expert conference on recent clinical experience and current status of remote surgery. *J Robotic Surg.* 2024. 18. 240. https://doi.org/10.1007/s11701-024-01984-w.

20. Sharma M. The World War III and the emerging role of AI based expert systems in cyber defense. In *The Emerging Role of AI-Based Expert Systems in Cyber Defense and Security*. 2024.

21. Sigetová K., Užíková L., Dotsenko T., & Boyko A. Recent trends in the financial crime of the world. Financial and Credit Activity Problems of Theory and Practice. 2022. 5(46). 258-270. https://doi.org/10.55643/fcaptp.5.46.2022.3897.

22. Schmüser J., Sri Ramulu H., Wöhler N., Stransky C., Bensmann F., Dimitrov D., Schellhammer S., Wermke D., Dietze S., Acar Y., & Fahl S. Analyzing Security and Privacy Advice During the 2022 Russian Invasion of Ukraine on Twitter. *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 2024. 1-16. https://doi.org/10.1145/3613904.3642826

23. The EU's Cybersecurity Strategy for the Digital Decade. (2020). European Union. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

24. Vasylieva T., Gavurova B., Dotsenko T., Bilan S., Strzelec M., Khouri S. The Behavioral and Social Dimension of the Public Health System of European Countries: Descriptive, Canonical, and Factor Analysis. Int. J. Environ. *Res. Public Health*. 2023. 20. 4419. https:// doi.org/10.3390/ijerph20054419.

25. Xie J. Application Study on the Reinforcement Learning Strategies in the Network Awareness Risk Perception and Prevention. *Int J Comput Intell Syst 17* . 2024. 112. https://doi.org/10.1007/s44196-024-00492-x.

26. Конвенція про кіберзлочинність, Конвенція Ради Європи (2005). https://zakon.rada.gov.ua/laws/show/994_575#Text

27. Про Державну службу спеціального зв'язку та захисту інформації України, Закон України №. 3475-IV (2024) https://zakon.rada.gov.ua/laws/show/3475-15#Text

28. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України №. 518 (2022) https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

29. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України, Постанова Національного банку України №. 178 (2022) https://zakon.rada.gov.ua/laws/show/v0178500-22#Text

30. Про основні засади забезпечення кібербезпеки України, Закон України №. 2163-VIII (2024) https://zakon.rada.gov.ua/laws/show/2163-19#Text

31. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", Указ Президента України №. 447/2021 (2021) https://zakon.rada.gov.ua/laws/show/447/2021#Text

References

1. Aljohani, T.M. (2024). Cyberattacks on Energy Infrastructures as Modern War Weapons-Part II: Gaps, Standardization, and Mitigation. IEEE Technology and Society Magazine, 43(2), 70-77. https://doi.org/10.1109/MTS.2024.3395697

2. Carlo, A., & Obergfaell, K. (2024). Cyber attacks on critical infrastructures and satellite communications. International Journal of Critical Infrastructure Protection, 46, 100701. https://doi.org/10.1016/j.ijcip.2024.100701

3. Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B.J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. Computers & Security, 142, 103886. https://doi.org/10.1016/j.cose.2024.103886

4. Crotty, J., & Daniel, E. (2022). Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Applied

Computing and Informatics, (ahead-of-print). https://doi.org/10.1108/ACI-07-2022-0178.

5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. (2022). European Union. http://data.europa.eu/eli/dir/2022/2555/2022-12-27

6. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. (2022). European Union. http://data.europa.eu/eli/dir/2022/2557/oj

7. Dotsenko, T., Dvořák, M., Lyeonov, S., & Kovács, A. (2023). Socially relevant factors of organizational mortality of enterprises: context of corporate sustainability in European countries. Economics and Sociology, 16(1), 284-299. DOI: 10.14254/2071- 789X.2023/16-1/18.

8. Folino, F., Folino, G., Pisani, F.S., Pontieri, L., & Sabatino, P. (2024). Efficiently approaching vertical federated learning by combining data reduction and conditional computation techniques. Journal of Big Data, 11(1), 77. https://doi.org/10.1186/s40537-024-00933-6

9. Hameed, K., Naha, R., & Hameed, F. (2024). Digital transformation for sustainable health and well-being: a review and future research directions. Discover Sustainability, 5(1), 104. https://doi.org/10.1007/s43621-024-00273-8

10. Hansen, F.S. (2024). The Russian approach to peacekeeping. International Affairs, 100(3), 1023-1042. https://doi.org/10.1093/ia/iiae072

11. INFORMATION SECURITY CONTROLS. (2022). In ISO/IEC 27001:2022 (S. 28-36). IT Governance Publishing. https://doi.org/10.2307/j.ctv30qq13d.8

12. ISO 27002. (2023). In ISO 27001/ISO 27002 (S. 71-76). IT Governance Publishing. https://doi.org/10.2307/jj.9039966.9

13. Jenkins, J., Roy, K. (2024). Exploring deep convolutional generative adversarial networks (DCGAN) in biometric systems: a survey study. Discov Artif Intell **4**, 42. https://doi.org/10.1007/s44163-024-00138-z.

14. Kjell Hausken. (2024). Fifty Years of Operations Research in Defense. European Journal of Operational Research, 318, Issue 2, 355-368. https://doi.org/10.1016/j.ejor.2023.12.023.

15. Krawczyk, D., Babenko, V., Yemchuk, L., Lienkov, S., Dzhulii, V., Dzhulii, L., & Muliar, I. (2024). Analysis of Information Security Under the Conditions of Hybrid War in Ukraine: Social Aspects. Management Systems in Production Engineering, 32(2), 235-243. https://doi.org/10.2478/mspe-2024-0023

16. Lyeonov, S., Kuzmenko, O., Yarovenko, H., & Dotsenko, T. (2019). The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. Marketing and Management of Innovations, 3, 308-326. http://doi.org/10.21272/mmi.2019.3-24.

17. Mario Angelelli, Serena Arima, Christian Catalano, Enrico Ciavolino. (2024). A robust statistical framework for cyber-vulnerability prioritisation under partial information in threat intelligence. Expert Systems with Applications, 255 B. https://doi.org/10.1016/j.eswa.2024.124572.

18. Rasim Alguliyev, Ramiz Aliguliyev, Lyudmila Sukhostat (2024). An approach for assessing the functional vulnerabilities criticality of CPS components. Cyber Security and Applications, Volume 3. https://doi.org/10.1016/j.csa.2024.100058.

19. Rocco, B., Moschovas, M.C., Saikali, S. *et al.* (2024). Insights from telesurgery expert conference on recent clinical experience and current status of remote surgery. *J Robotic Surg*, 18, 240. https://doi.org/10.1007/s11701-024-01984-w.

20. Sharma, M. (2024). The World War III and the emerging role of AI based expert systems in cyber defense. In The Emerging Role of AI-Based Expert Systems in Cyber Defense and Security.

21. Sigetová, K., Užíková, L., Dotsenko, T., & Boyko, A. (2022). Recent trends in the financial crime of the world. Financial and Credit Activity Problems of Theory and Practice, 5(46), 258-270. https://doi.org/10.55643/fcaptp.5.46.2022.3897.

22. Schmüser, J., Sri Ramulu, H., Wöhler, N., Stransky, C., Bensmann, F., Dimitrov, D., Schellhammer, S., Wermke, D., Dietze, S., Acar, Y., & Fahl, S. (2024). Analyzing Security and Privacy Advice During the 2022 Russian Invasion of Ukraine on Twitter. Proceedings from: *The CHI Conference on Human Factors in Computing Systems*. (pp. 1-16). https://doi.org/10.1145/3613904.3642826

23. The EU's Cybersecurity Strategy for the Digital Decade. (2020). European Union. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

24. Vasylieva, T., Gavurova, B., Dotsenko, T., Bilan, S., Strzelec, M., & Khouri, S. (2023). The Behavioral and Social Dimension of the Public Health System of European Countries: Descriptive, Canonical, and Factor Analysis. Int. J. Environ. Res. Public Health, 20, 4419. https:// doi.org/10.3390/ijerph20054419.

25. Xie, J. (2024). Application Study on the Reinforcement Learning Strategies in the Network Awareness Risk Perception and Prevention. Int J Comput Intell Syst, 17 , 112. https://doi.org/10.1007/s44196-024-00492-x.

26. Konventsiia pro kiberzlochynnist, Konventsiia Rady Yevropy (2005). https://zakon.rada.gov.ua/laws/show/994_575#Text

27. Zakon Ukrainy Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy №. 3475-IV, 2024. https://zakon.rada.gov.ua/laws/show/3475-15#Text

28. Postanova Kabinetu Ministriv Ukrainy Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury №. 518, 2022. https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

29. Postanova Natsionalnoho banku Ukrainy Pro zatverdzhennia Polozhennia pro orhanizatsiiu kiberzakhystu v bankivskii systemi Ukrainy ta vnesennia zmin do Polozhennia pro vyznachennia obiektiv krytychnoi infrastruktury v bankivskii systemi Ukrainy

№. 178, 2022. https://zakon.rada.gov.ua/laws/show/v0178500-22#Text

30. Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy №. 2163-VIII, 2024. https://zakon.rada.gov.ua/laws/show/2163-19#Text

31. Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy» №r. 447/2021 2021. https://zakon.rada.gov.ua/laws/show/447/2021#Text

MATURITY OF THE COUNTRY'S CYBERSECURITY SYSTEM IN THE CONDITIONS OF WAR: ASSESSMENT TRENDS

T. V. Dotsenko, Doctor of Philosophy, Sumy State University,
M. V. Kuzmenko, Post-graduate Student, Sumy State University

Methods. The study used the following methods: an inductive approach to formulating the concept of maturity of the country's cybersecurity system in military conditions; a deductive method to derive the concept of assessing the maturity of the country's cybersecurity system during military operations; content analysis identified the key elements of assessing the maturity of the national cybersecurity system in military operations; strategic analysis identified the main vectors of assessing the problem under study, and the latest approaches to assessing the national cybersecurity system.

Results. The latest trends in assessing the maturity of the country's cybersecurity system, taking into account the aspect of military conditions, are identified: the existing regulatory and legal framework at the international and national levels is indicated; the concept of maturity and assessment of the maturity of the country's cybersecurity system during military operations is formulated. The paper outlines the key elements of assessing the maturity of the national cybersecurity system in military operations: adaptability, interoperability, readiness, partnership, cyber reserves, vulnerabilities and threats, and training. The main vectors of assessment are identified: assessment of cyber threats, cyber attacks, infrastructure protection, interaction of cybersecurity actors, level of personnel training; the latest approaches to system assessment are noted. A scheme of future key challenges, trends, and recommendations for assessing the maturity of the national cybersecurity system in wartime has been formed.

Novelty. The study of the specifics of assessing the maturity of the country's cybersecurity system identifies key elements, vectors, approaches, and methods for assessing the cyber defence system. Weaknesses and vulnerabilities, existing progress in the development of cyber defence of the system are identified, and the necessary activities to enhance the effectiveness of national security in times of war are identified.

Practical value. The experience of previous achievements in the functioning of cybersecurity systems is summarised, the most effective practices and methods of cyber resilience are identified, recommendations for assessing the maturity of the national cybersecurity system in times of war are proposed, which will optimise existing and potential resources, and will help to create the preconditions for further development of the latest model of cyber defence assessment.

Keywords: cybersecurity, system maturity, assessment methods, cyber defence modelling, cyber risks, cyber vulnerabilities.

Надійшла до редакції 29.08.24 р.