УДК 342.951

МАНУІЛОВ Я.С., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-8149-2745.

ПИТАННЯ РОЗРОБКИ ІНДИКАТОРІВ ОЦІНКИ СТАНУ КІБЕРБЕЗПЕКИ

Анотація. *Визначено поняття та особливості проведення оцінки стану кібербезпеки. Розглянуто сучасні інструменти, мету та завдання проведення аналізу ризиків кібербезпеки. Деталізовано зміст та значення ключових показників ефективності у сфері кібербезпеки. Висвітлено сучасні методики та моделі проведення оцінки стану кібербезпеки з використанням показників та метрик. Узагальнено зарубіжний досвід у сфері використання показників кібербезпеки з метою проведення оцінки її ефективності. Окреслено подальші шляхи удосконалення проведення оцінки стану кібербезпеки та актуалізовано необхідність розробки та запровадження базових індикаторів стану кібербезпеки, індикаторів розвитку національної системи кібербезпеки та індикаторів стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів, а також інформації, вимога щодо захисту якої встановлена законом.*

Ключові слова: *кібербезпека, кіберзахист, оцінка, ландшафт кіберзагроз, ризики, критична інформаційна інфраструктура, індикатори, програмне забезпечення, правовий режим воєнного стану.*

Summary*. The concept and features of conducting an assessment of the state of cyber security are defined. Modern tools, purpose and tasks of cyber security risk analysis are considered. The content and significance of key performance indicators in the field of cyber security are detailed. Modern methods and models for assessing the state of cyber security using indicators and metrics are highlighted. The foreign experience in the field of using cyber security indicators for the purpose of assessing its effectiveness is summarized. Further ways of improving the assessment of the state of cyber security are outlined and the need to develop and introduce basic indicators of the state of cyber security, indicators of the development of the national cyber security system and indicators of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law, is actualized.*

Keywords: *cyber security, cyber defense, assessment, cyber threat landscape, risks, critical information infrastructure, indicators, software, martial law, vulnerability management.*

Постановка проблеми. Поширення ландшафту загроз та ускладнення інструментарію їх реалізації спонукає уряди провідних країн удосконалювати архітектуру національних систем кібезбезпеки, змінювати стратегію і тактику протидії кіберзагрозам. На перманентній основі вносяться зміни до існуючих моделей протидії кіберзагрозам, які пов'язані із розумінням недостатньої можливості побудувати абсолютно невразливі та удосконалені системи кіберзахисту. Як переконливо демонструє світова практика, будь-які інформаційно-комунікаційні системи можуть бути уражені внаслідок кібератаки незалежно від рівня їх захисту. Тому набуває великого значення розробка сучасних механізмів максимально швидкого виявлення вразливостей і кібератак, швидкого реагування та поширення інформації про них для мінімізації негативних наслідків та запобігання збиткам. За таких умов швидкозмінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка

зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи безпечне функціонування національного сегмента кіберпростору, передбачати нові можливості для цифровізації всіх сфер суспільного життя. Кібервійна повністю змінила підходи бізнесу та держави до питань кібербезпеки. У той же час інформаційні системи стають дедалі складнішими, нові архітектури та методи побудови на тлі зростаючих ризиків зумовлюють потреби у подальшому розвитку нових сучасних рішень та появі принципово нових підходів до захисту інформаційно-комунікаційних систем та мереж держави та приватного сектору.

На жаль, все ще не були розроблені критерії оцінки стану кібербезпеки – індикатори виконання Стратегії кібербезпеки України, що значно ускладнювало процес моніторингу її результативності [1, с. 101]. Такий стан справ переконливо засвідчує, що в Україні не розроблені показники-індикатори оцінку стану кібербезпеки, що значно ускладнює формування єдиного методологічного підходу до процесів оцінки її результативності, особливо в умовах правового режиму воєнного стану, масштабних хакерських атак та посягань на об'єкти критичної інфраструктури. Адже поточна ситуація вимагає прискіпливої уваги до питань визначення та впровадження загальноприйнятих критеріїв, метриків та показників, на підставі яких здійснюється оцінка ризиків та загроз для кібербезпеки. Результати проведеного аналізу мають дозволити визначити пропозиції щодо розробки індикаторів стану кібербезпеки в Україні.

Результати аналізу наукових публікацій. Загальні та спеціальні методи оцінки стану кібербезпеки досліджували у своїх працях: В. Мохор, С. Гончар, О. Дибач [2], Н. Барченко, В. Любчак та Т. Лаврик [3], А. Єріна, І. Гончар та С. Заєць [4]. Міжнародні стандарти кіберстійкості та методологія оцінювання ризиків кіберзагроз в зарубіжних країнах були предметом уваги: О. Федієнка [5] та О. Панченко [6]. Оцінку стану кібербезпеки критичної інформаційної інфраструктури ретельно вивчали: І. Ткаченко, В. Козачок, С. Гахов та В. Дмітрієв [7], А. Положенцев та В. Сидоренко [8]. Проте жоден із вказаних фахівців та експертів предметно не здійснював розгляд актуальних питань оцінки ризиків кібербезпеки.

Метою статті є узагальнення кращих практик та сучасної методології оцінки кіберризиків та визначення подальших шляхів удосконалення національної системи кібербезпеки через призму розробки та впровадження індикаторів оцінки стану кібербезпеки в умовах правового режиму воєнного стану.

Виклад основного матеріалу. За підсумками 2023 року світова індустрія кібербезпеки, виходячи із сучасних викликів та загроз, наблизилася до необхідності переосмислення принципів та алгоритмів побудови надійного кіберзахисту, оперативного реагування на масштабні кіберризики в умовах суттєвого розширення ландшафту кіберзагроз, пов`язаних із застосуванням технологій штучного інтелекту (від крадіжок даних до експлуатаційних вразливостей інфраструктури тощо). У 2024 році світову кібербезпеку очікував період активної фази необхідності практичного впровадження та посилення кіберзахисту інформаційно-комунікаційних і комп'ютерних систем, критичної інформаційної інфраструктури з огляду на постійне удосконалення злочинних та хакерських посягань у цьому сегменті.

За таких умов важливою складовою забезпечення кібербезпеки є її оцінка. Оцінювання стану кібербезпеки – процес вивчення результатів застосування заходів з кіберзахисту систем, об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що експлуатуються на об'єктах критичної інфраструктури для визначення стану захищеності таких об'єктів та проведення огляду та ефективності вжитих у цій площині

заходів. Оцінка ризиків кібербезпеки – це процес виявлення, кількісної оцінки та управління ризиками для систем та даних інформаційно-комунікаційних технологій.

Інструменти аналізу ризиків кібербезпеки покликані допомогти реально оцінити її поточний стан, виявити вразливості, які можуть використовувати хакери або інші кіберзлочинці. Ці інструменти використовують різні методи та методології для виявлення потенційних ризиків, включаючи сканування вразливостей, тестування на проникнення та аналіз кіберзагроз. Використання цих інструментів може значно покращити розуміння ризиків кібербезпеки, розробити планові стратегії їхньої мінімізації. Цілком логічно, що оцінка ризиків спрямована на виявлення потенційних загроз та вразливостей, перспективну розробку плану щодо зниження загрози цих ризиків та їхніх негативних наслідків. Однією з ключових переваг використання інструментів аналізу ризиків кібербезпеки є те, що вони можуть допомогти організаціям, державним та приватним структурам розставити пріоритети у своїх інвестиціях в кібербезпеку, визначити слабкі місця та вразливості. Виявляючи найбільш критичні вразливості та ризики, можливим є ефективний розподіл ресурсів та визначення успішного алгоритму ліквідації кіберзагроз.

Першим та важливим кроком в оцінці ризиків кібербезпеки є визначення систем та даних, які потребують захисту. У зв'язку з цим необхідно визначити загрози, які потенційно можуть завдати шкоди цим системам та даним. Загрози можуть включати все: від хакерів і шкідливих програм до стихійних лих і людської помилки. Після того, як визначено загрози, необхідно кількісно оцінити їхню потенційну дію. Це включає оцінку ймовірності виникнення кожної загрози і шкоди, яка може бути заподіяна. Останнім кроком є розробка плану зниження цих ризиків. Це може включати впровадження таких заходів безпеки як: брандмауери, антивірусне програмне забезпечення або резервне копіювання. Цей план може також передбачати навчання співробітників захисту від онлайн-загроз або розробку політик для боротьби з несанкціонованими витоками даних. Оцінка ризиків кібербезпеки допомагає краще розуміти вразливість систем до кібератак, а також розставити пріоритети у витратах на забезпечення безпеки. Виявляючи конкретні загрози та роблячи кроки щодо їх усунення, проведення оцінки сприяє зниженню загального рівня ризику та надає змогу налагодити захист від будь-яких витоків даних.

Також оцінка ризиків спрямована на виявлення вразливостей та розробку рекомендаційних рішень для зниження або усунення ризиків. Фактори, що враховуються при оцінці кіберризиків: характер та масштаби комп'ютерних систем та даних організації; загрози, створювані системи як внутрішніми, і зовнішніми джерелами; вразливість системи до кібератак; аналіз та узагальнення за наслідками успішної атаки на систему. Важливим в контексті здійснення оцінки ризиків кібербезпеки є проведення рейтингу ризиків, що надає можливість оцінити та кількісно визначати той чи інший ризик. Оцінка ризиків спрямована на надання пріоритетного списку ризиків у порядку ранжиру, що дає змогу розподілити ресурси таким чином, щоб якнайкраще організувати захист найважливіших систем. Існує безліч різних методів розрахунку ризику, але всі вони, як правило, ґрунтуються на таких факторах, як: виявлення та оцінка загроз; оцінка вразливості; оцінка кожної загрози-вразливості.

Загрози можуть виходити із внутрішніх або зовнішніх джерел і бути навмисними (наприклад, кібератаки) або випадковими. Оптимальним методом оцінки загроз є метод експертних оцінок, у якому експертам пропонується оцінити можливість реалізації певного переліку загроз. У якості критеріїв оцінки небезпеки конкретної загрози доцільно вибрати можливість виникнення джерела загрози, ступінь його готовності

здійснити атаку, а також визначити фатальність для систем від реалізації тієї чи іншої загрози. Коефіцієнт небезпеки загрози обчислюється на підставі балів (дискретно від 1 до 10), виставлених експертом за трьома вказаними критеріями. Після виявлення загроз їх необхідно оцінити, щоб визначити їхню потенційну дію та ймовірні масштаби. Це включає оцінку як самої загрози (наприклад, скільки людей може постраждати в результаті витоку даних), так і ймовірності того, що це відбудеться (наприклад, наскільки ймовірно, що кібератака буде успішною). Після оцінки загроз необхідно оцінити вразливості – це слабкі місця в системі безпеки, якими можуть скористатися зловмисники або хакери. Вразливість системи – це причини та передумови, які зумовлюють порушення безпеки системи чи безпеки інформації, яка у ній обробляється. У якості критеріїв оцінки небезпеки вразливості можна визначити: фатальність наявності в системі вразливості, доступність вразливості для джерел загроз, а також кількість вразливостей певного типу для системи або частота їх появи. Виявлення та усунення вразливостей важливі для зниження ризику. Нарешті, як тільки вся відповідна інформація зібрана, її необхідно узагальнити в кількісну оцінку кожної пари "загроза-вразливість". У подальшому ця оцінка може бути використана для визначення пріоритетності ризиків та загроз.

Для оцінки ризиків та загроз кібербезпеки інформаційно-комунікаційних систем необхідно насамперед виділяти її активи. Сукупність активів системи – усі засоби та технічні рішення, які необхідні для її штатного функціонування і знаходяться в її розпорядженні (апаратні засоби, програмне забезпечення, службова інформація, що зберігається тощо). Процес оцінки ризиків для кожного з активів повинен враховувати вартість самого активу та характеристику можливостей порушення його штатного функціонування. При цьому важливо враховувати, як всю сукупність загроз, так і всю сукупність уразливостей, які є взаємопов`язаними для здійснення оцінки ризиків кібербезпеки. В реальних умовах одна і та ж загроза кібербезпеці для інформаційно-комунікаційних систем може реалізуватися через декілька вразливостей. Саме виявлення вразливостей в технічних та організаційних контролях є важливим та актуальним завданням, що, у свою чергу, впливають на конфіденційність, цілісність та доступність продуктів інформаційних технологій (наприклад, систем, обладнання, програмного забезпечення та послуг).

Існуючі методи ранжування загроз та вразливостей формують їхню оцінку незалежно один від одного. Однак загрози не становлять небезпеки для об'єкта без наявності вразливостей, що їм відповідають. Також вразливості не знижують рівень кібербезпеки інфокомунікаційної системи, якщо немає загроз, які можуть виникнути. Отже, оцінку загроз та вразливостей слід проводити комплексно з використанням, як правило, таких критеріїв:

– критерій 1 – можливість виникнення джерела загрози у достатньому оточенні від системи для реалізації загрози;

– критерій 2 – ступінь готовності джерела загрози її реалізувати;

– критерій 3 – поширеність в системі вразливостей з урахуванням їх сукупності, через які може реалізуватися загроза;

– критерій 4 – доступність для реалізації загрози вразливостей із сукупності вразливостей, через які може реалізуватися ця загроза;

– критерій 5 – фатальність для системи за наслідками реалізації загрози.

На підставі вказаних критеріїв оцінка ризиків кібербезпеки проводиться за таким алгоритмом: 1) визначається перелік активів системи; 2) визначається сукупність загроз для кібербезпеки; 3) для кожної із загроз визначається сукупність уразливостей, через

які вона може реалізуватися; 4) групою експертів проводиться оцінка коефіцієнта небезпеки по кожній із загроз; 5) здійснюється ранжування загроз щодо зменшення коефіцієнта їх небезпеки. Таким чином, для кожного активу формується індивідуальний ранжований за ступенем небезпеки перелік загроз, а для кожного з активів визначаються ризики кібербезпеки за його вартістю та максимальним значенням коефіцієнта небезпеки загрози для такого активу.

Оцінка ризиків кібербезпеки проводиться поетапно (етапи полягають у ідентифікації загроз, уразливостей та активів) різними методами управління, з метою якісного чи кількісного аналізу загроз, визначення факторів ризику системи, пошуку оптимального рішення шляхом кластеризації. Варто зазначити, що чіткої методики розрахунку величин ризиків немає, тому згідно із кращими практиками зарубіжного досвіду, організації повинні вживати всіх можливих дій, а саме: дотримання усіма співробітниками організації засад кібергігієни та внутрішніх положень безпеки, використання сучасних засобів захисту від новітніх атак та загроз, а також сучасних систем управління ризиками кібербезпеки.

Загалом в сучасних умовах таке поняття, як "ризик кібербезпеки" безпосередньо пов'язаний з автоматизацією робочого процесу, тому управління цими ризиками також має бути автоматизовано за допомогою ПЗ для цих цілей (аналіз вразливості, захист інформації, інше). Процес впровадження ПЗ дозволяє організувати такі важливі аспекти, як: ідентифікацію ризику, оцінку його прояву та наслідки, побудова послідовності дій, залучення необхідних сил та засобів, проведення моніторингу, відстеження важливих моментів, виявлення потрібної інформації, навчання працівників необхідним діям для зниження вразливостей та деградації систем.

Для проведення повноформатної оцінки використовуються ключові показники ефективності у сфері кібербезпеки – це не просто числові дані, а кількістно-якісні характеристики, які відображають адаптивність і підготовленість організації в динамічному ландшафті цифрових загроз, підкреслюючи важливість відстеження та постійного вдосконалення стратегій кібербезпеки. Ключові показники ефективності є одночасно інструментами діагностики, які використовуються для проведення оцінки стану кібербезпеки. Ключові показники ефективності (KPI) – це ефективний спосіб виміряти успіх та ефективність будь-якої програми, зокрема кібербезпеку. Без аналізу роботи системи кібербезпеки неможливо оцінити реальний стан безпеки та відповідний рівень захисту. Таким чином, ключові показники ефективності кібербезпеки – це інструменти, які використовуються для оцінки та вимірювання продуктивності та міцності кібербезпеки тієї чи іншої організації. Ці показники можуть надати ключові дані, які допоможуть їм розробити стратегію та визначити пріоритети в тих сферах, де їхні існуючі кіберпроцедури є слабкими, і де вони повинні витрачати більше часу для того, щоб зміцнити свою кіберпозицію. Ключові показники ефективності є вимірюваними метриками, які використовуються для оцінки успіху організації або конкретної діяльності. Вони допомагають оцінити прогрес у досягненні стратегічних цілей та завдань у сфері забезпечення кібербезпеки, надають можливість кількісно оцінити ефективність та відстежувати прогрес з часом, що дозволяє приймати рішення на основі даних і стимулювати постійне вдосконалення.

У 2024 році світова спільнота рекомендувала використовувати сучасні показники кібербезпеки з метою проведення оцінки її ефективності. Ці показники надають розуміння моделей ризиків та загроз, ефективності реагування на інциденти та вразливості систем. В епоху зростаючої довіри до цифрових технологій вони відіграють ключову роль у прийнятті стратегічних та оперативних рішень, підкреслюючи

готовність протистояти ризикам та загрозам, сприяють проведенню порівняльного аналізу кібербезпеки. Ці показники обґрунтовано дозволяють представити чітку картину стану мережевої інфраструктури та обґрунтувати бюджет і ресурси, виділені на ініціативи із забезпечення кібербезпеки. Так до основних показників кібербезпеки, розроблених світовими експертами, відносяться:

• рівень готовності – визначення кількості справних та оновлених пристроїв, сканування вразливостей та керування ними;

• невідомі пристрої у внутрішніх мережах – виявлення мережевих вторгнень (співробітники можуть збільшувати кіберризики та загрожувати безпеці, використовуючи власні пристрої та погано налаштовані пристрої IoT);

• спроба вторгнення – кількість спроб зловмисників отримати несанкціонований доступ;

• інцидент безпеки – кількість зламів інформаційних активів та/або мережі;

• середній час виявлення (MTTD) – час, коли загрози залишаються непоміченими (тобто метрика показує час, необхідний фахівцям для виявлення загроз);

• середній час відновлення (MTTR) – середній час реагування команди фахівців на кібератаку, що визначає якість реалізації плану реагування на інцидент;

• середній час стримування – показує час відгуку компанії та можливості вимірювання її стану кібербезпеки;

• рейтинги безпеки – оцінка ризиків кібербезпеки, визначення показників інформаційної безпеки, які потребують уваги;

• середній рейтинг кібербезпеки третіх осіб;

• показник виправлень – визначення часу на впровадження виправлень безпеки додатків та/або усунення вразливостей із високим ризиком;

• управління доступом – контроль доступу, аналіз доступу (хто з користувачів має права адміністратора);

• показник ризику з боку третіх осіб та потенційних вразливостей;

• середній час реагування третьої особи на інцидент. Інцидент безпеки – це успішна кібератака. Однак метою може бути і певна організація, доступ до якої кіберзлочинці намагаються отримати через третю особу. Чим довше партнер реагує на інцидент, тим більша ймовірність того, що компанія постраждає від витоку даних у майбутньому.

У світовій практиці існує безліч доступних інструментів аналізу ризиків кібербезпеки, але виділяються чотири найбільш популярних:

1. NIST Cybersecurity Framework: NIST Cybersecurity Framework – це структура, що широко використовується для управління та зниження ризиків кібербезпеки. Він містить набір рекомендацій та передових методів для виявлення, оцінки та управління ризиками кібербезпеки.

2. Microsoft Security Risk Detection: Microsoft Security Risk Detection – це хмарний інструмент, який допомагає виявляти вразливість безпеки в програмах до їх розгортання. Він використовує алгоритми машинного навчання для аналізу коду та виявлення потенційних загроз безпеці.

3. QualysGuard: QualysGuard – це хмарний інструмент управління вразливістю, який допомагає організаціям виявляти та усувати вразливості у своїй IT-інфраструктурі. Він забезпечує огляд загроз безпеки в режимі реального часу та допомагає організаціям розставити пріоритети у зусиллях усунення проблем.

4. Rapid7 InsightVM: Rapid7 InsightVM – це інструмент управління вразливістю, який допомагає організаціям виявляти та визначати пріоритети у своєму IT-середовищі.

Він забезпечує видимість ризиків безпеки в режимі реального часу та допомагає організаціям оцінювати ефективність своїх заходів у сфері кібербезпеки.

Ще одна світова методика експрес-оцінки рівня кібербезпеки будь-якої організації передбачає використання 10 груп показників – доменів, які характеризують поточний рівень таких процесів/напрямів кібербезпеки: управління активами; моніторинг подій; керування інцидентами; управління вразливістю; керування доступом; керування конфігураціями; технологічна стійкість; мережева та інфраструктурна безпека; контроль захищеності. Щоб отримати загальну оцінку рівня кібербезпеки організації використовують таку бальну систему: 1 бал – базовий рівень; 2 бали – середній рівень; 3 бали – високий рівень; 4 бали – провідний рівень. Під час проведення оцінки експерти якісним способом аналізують відповідність поточного рівня кожного процесу/напряму кібербезпеки організації запропонованим критеріям. Аналіз повинен виконуватися послідовно від рівня "базовий" до рівня "провідний". Поточний рівень кібербезпеки організації обчислюється за такою формулою: Рівень кібербезпеки = Бали (домен 1) + Бали (домен 2) + … + Бали (домен 10).

Рівень стану кібербезпеки організації визначається за діапазоном значень, до якого потрапляє сума балів за доменом: 1-43 бали – "цифрова гігієна"; 44-66 балів – "класична кібербезпека"; 67-85 балів – "трансформована кібербезпека"; більше 86 балів – "результативна кібербезпека". Оцінка "цифрова гігієна" характеризується відсутністю виділеного структурного підрозділу з кібербезпеки, процеси кібербезпеки перебувають у стадії початкового формування, а безпека забезпечується переважно штатними засобами (ОС, мережевих додатків тощо). "Класична кібербезпека" характеризується: наявністю виділеної функції кібербезпеки; процеси кібербезпеки частково вибудовані; вибір захисних заходів орієнтований переважно на вимоги регуляторів. "Трансформаційна кібербезпека" означає, що: керівництво організації залучене до ключових ініціатив та розуміє необхідність переходу до результативної кібербезпеки; функцію кібербезпеки виділено; фахівці з кібербезпеки регулярно проводять експертизу; процеси кібербезпеки вибудовані та частково автоматизовані. "Результативна кібербезпека" – керівництво бере активну участь в ініціативах з кібербезпеки; сценарії реалізації неприпустимих подій враховані в архітектурі бізнес-систем та кібербезпеки в цілому; експерти з кібербезпеки регулярно підтверджують у практичній площині відсутність можливості реалізації неприпустимих подій/ключових ризиків.

Таким чином, кібербезпека та її оцінка будується на трьох ключових аспектах: процеси, технології, експертиза, і саме їхня сукупність відображає реальну оцінку та можливості тієї чи іншої організації подолати наслідки кібератак та впливати на кіберзагрози. Очевидно, що чим вищий рівень кібербезпеки, тим краще побудований кіберзахист. Існує безліч способів її оцінки, які можуть включати різні варіанти перевірок. Найчастіше оцінити поточний стан кібербезпеки необхідно в найкоротші терміни, що може викликати труднощі експертів. Саме для вирішення цього завдання і було розроблено окреслену методику експрес-оцінки стану кібербезпеки. Ключовою особливістю цієї методики є її компактність та можливість отримання швидких високорівневих результатів. Ці результати допоможуть визначити поточний стан кібербезпеки в організації, сфокусувати увагу на пріоритетних сферах та задати вектор подальшого розвитку. За допомогою цієї методики стає можливим: сформувати показники та критерії задля визначення поточного рівня кібербезпеки організації для проведення його оцінки; оцінити поточний рівень стану кібербезпеки тієї чи іншої організації.

Також оцінку стану кібербезпеки, за рекомендаціями світових експертів, проводять на підставі міжнародного зводу рекомендацій CIS (Critical Security Controls) за 18 напрямками [9]: 1) інвентаризація та контроль активів підприємства; 2) інвентаризація та контроль програмних активів; 3) захист даних; 4) безпечна конфігурація корпоративних ресурсів і програмного забезпечення; 5) керування обліковим записом; 6) управління контролем доступу; 7) керування вразливостями; 8) керування журналом аудиту; 9) захист електронної пошти та веб-браузера; 10) захист від шкідливих програм; 11) відновлення даних; 12) управління мережевою інфраструктурою; 13) моніторинг і захист мереж; 14) навчання з питань безпеки; 15) керування у сфері постачання ІТ-послуг; 16) безпека прикладного програмного забезпечення; 17) управління реагуванням на інциденти; 18) тестування.

Очікувано, саме ці інструменти мають допомогти зацікавленим структурам виявляти ризики та загрози кібербезпеки, проводити їхню оцінку з використанням шкали показників, метриків та індикаторів.

В контексті українських реалій основним правовим документом, на підставі якого визначено організаційно-правові, техніко-економічні засади забезпечення кібербезпеки, є Стратегія кібербезпеки України 2021 року [10]. Ефективність її реалізації визначається через постійний моніторинг виконання та спирається на чітку систему індикаторів стану кібербезпеки, які мали ще бути розробленими протягом першого року реалізації Стратегії, тобто ще у 2022 році. Індикатори мають визначати прогрес, якого досягли суб'єкти забезпечення кібербезпеки в реалізації Стратегії з таких питань, як: виконання стратегічних завдань у межах цілей, визначених Стратегією (за кожним завданням); досягнення стратегічних цілей, визначених Стратегією (за кожною ціллю); рівень впливу заходів, що здійснюються в межах Стратегії, на національну систему кібербезпеки та цифрову трансформацію держави. Практичне впровадження індикаторів стану кібербезпеки забезпечить покращення процесу моніторингу виконання Стратегії у реальному часі з використанням сучасних веб-ресурсів (онлайн-платформ), прозорість вжитих заходів для суспільства і держави.

На стратегічному рівні задекларовано, що посилення впливу національної системи кібербезпеки на суспільний розвиток має визначатися за такими критеріями: рівень довіри населення до держави щодо безпечності кіберпростору; формування безпечного інформаційного суспільства, в якому до заходів кібербезпеки, крім державних інституцій, залучені приватні суб'єкти та громадяни; рівень захищеності національних інтересів у сфері кібербезпеки. Саме за допомогою розгалуженої системи індикаторів планувалося визначення стану досягнення передумов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Система індикаторів мала включати базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що очікувано мало надати змогу комплексно оцінювати результативність та ефективність реалізації положень Стратегії. Пункт 1 Плану реалізації Стратегії кібербезпеки України, затверджений рішенням РНБО України та введений в дію Указом Президента України від 01.02.22 р. № 37/2022 [11] передбачав, що протягом другого півріччя 2022 року мала бути розроблена система індикаторів стану кібербезпеки, яка включатиме: базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. На жаль, у

зв'язку із російською військовою агресією, яка розпочалася 24 лютого 2022 року, ці заходи залишаються нереалізованими, що засвідчує негативну тенденцію невиконання планових засад реалізації Стратегії кібербезпеки України попри визначені на нормативному рівні терміни.

Висновки.

Узагальнюючи викладене, можна констатувати, що у світі існує безліч методик та методологій проведення оцінювання стану забезпечення кібербезпеки як для державного, так і приватного сектору. Проведене дослідження переконливо засвідчує важливість та актуальність здійснення як поточної так і перспективної оцінки стану кібербезпеки з використанням показників, метриків, критеріїв та індикаторів. На жаль, попри чисельну кількість схвалених останнім часом на державному рівні нормативно-правових актів, присвячених кібербезпековій тематиці, все ще відсутня єдина затверджена методика проведення оцінки стану кібербезпеки з використанням базових індикаторів стану кібербезпеки, індикаторів розвитку національної системи кібербезпеки та індикаторів стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів тощо. За таких умов необхідним є прискорення розробки та затвердження на державному рівні вказаних індикаторів з урахуванням кращих практик зарубіжного та міжнародного досвіду у цій сфері відповідно до планових засад реалізації Стратегії кібербезпеки України.

Використана література

1. Мануілов Я.С. Огляд новел вітчизняного законодавства у сфері забезпечення кібербезпеки (на прикладі Стратегії кібербезпеки на 2021 – 2025 роки). *Інформація і право.* № 4(39)/2021. С. 98-105.

2 Мохор В.В., Гончар С.Ф., Дибач О.М. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. *Ядерна та радіаційна безпека.* 2019. № 2(82). С. 4-8.

3. Барченко Н.Л., Любчак В.О., Лаврик Т.В. Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. *Кібербезпека: освіта, наука, техніка.* 2022. № 2(18). С. 73-85.

4. Єріна, А., Гончар І., Заєць С. Статистичні показники розвитку кібербезпеки в контексті цифрової трансформації економіки та суспільства. *Наука та інновації.* 2021. № 17 (3) С. 3-13.

5. Федієнко О.П. Міжнародні стандарти оцінки кіберстійкості. *Інформація і право.* № 3(50)/2024. С. 124-135.

6. Панченко О.А. Актуальні питання оцінювання ризиків кіберзагроз: аналіз зарубіжного досвіду. *Інформація і право.* № 4(39)/2021. С. 106-112.

7. Ткаченко І.В., Козачок В.А., Гахов С.О., Дмітрієв В.Є. Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідковування кризових індикаторів. *Сучасний захист інформації.* 2020. № 1. С. 54-57.

8. Положенцев А., Сидоренко В. Метод визначення рівня кібербезпеки об'єктів критичної інфраструктури держави: матеріали XVIII міжнар. наук.-практ. конф. молодих учених і студентів *Сучасні проблеми науки*, м. Київ, 4-6 квіт. Київ, 2018 р. С. 102-103.

9. The 18 CIS Critical Security Controls. URL: https://www.cisecurity.org/controls/cis-controls-list

10. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

11. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України": Указ Президента України від 01.02.22 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#n5

* * *