УДК 323:351

КОНЦЕПТУАЛЬНІ ЗАСАДИ ОГЛЯДУ СТАНУ КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Семенченко Андрій Іванович,
доктор наук з державного управління, професор

Мялковський Данило Владиславович

Станіславський Тарас Володимирович

У статті розглянуто концептуальні засади організації та проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Актуальність цього дослідження зумовлена як вимогами чинного законодавства, так і тенденціями розвитку сфери національної безпеки та оборони, невідповідністю державної політики та державного управління вимогам надійного та оперативного реагування на кіберзагрози, розривом та неузгодженістю між сукупністю концептуальних документів і їх реальною імплементацією, відсутністю ефективної координації та взаємодії складових національної системи кібербезпеки щодо кіберзахисту критичної інформаційної інфраструктури. У статті обґрунтовано й запропоновано концептуальні засади комплексного механізму державного управління оглядом стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, з урахуванням міжнародного досвіду в цій сфері, насамперед країн НАТО та Європейського Союзу.

Огляд стану кіберзахисту є однією із складових частин Комплексного огляду сектору безпеки та оборони. Він, серед інших видів огляду, вперше визначений в Законі України «Про національну безпеку України».

Зважаючи на міжнародний досвід та застосовуючи запроваджений у Законі уніфікований підхід, основну мету огляду стану кіберзахисту запропоновано сформулювати як «визначення реального стану захищеності й готовності об'єктів огляду до запобігання кіберінцидентам, оперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак, ліквідації їхніх наслідків, відновлення функціонування цих об'єктів і систем». Також у статті запропоновано систему принципів проведення огляду стану кіберзахисту, завдання, які повинні бути вирішені під час його проведення, механізми їх вирішення та представлення результатів.

Ключові слова: кібербезпека, кіберзахист, критична інформаційна інфраструктура, огляд, спостереження, вимірювання, аналіз, оцінювання.

Semenchenko Andrii, Mialkovskyi Danylo, Stanislavskyi Taras

CONCEPTUAL PRINCIPLES OF REVIEW OF CYBERNETIC DEFENCE OF STATE INFORMATIVE RESOURCES AND CRITICAL INFORMATIVE INFRASTRUCTURE

Conceptual principles of organization and realization of Inspection of the condition of cyberprotection of critical informative infrastructure, state informative resources and information

are considered in the article, a requirement in relation to defense of that is set by a law. Actuality of research of that is conditioned by both the requirements of current legislation and progress of sphere of national safety and defensive trends, by disparity of public administration and state policy to the requirements of the reliable and operative reacting on cyber threats, by a break and inconsistency between totality of conceptual documents and them real implementation, by absence of effective co-ordination and co-operation of constituents of the National cybersecurity system for real ensuring cyberprotection of critical informative infrastructure.

The article substantiates and proposes the conceptual foundations of an integrated mechanism of state governance of Inspection of the state of cyber defense of critical information infrastructure, state information resources and information, the requirement for protection of which is established by law, taking into account international experience in this field, especially NATO countries and the EU.

An Inspection of the condition of cyber protection is a component of a Comprehensive inspection of the security and defense sector. Among other types of inspection, he was defined in the Law of Ukraine "On National Security of Ukraine".

Taking into account international experience and applying the unified approach introduced by the Law, the main objective of the Inspection of the condition of cyber defense is proposed as "to determine the real condition of the security and readiness of the objects to prevent cyber incidents, to respond promptly to cyber threats, to prevent, detect and protect against cyberattacks, to eliminate them, repair of functioning of these objects and systems". Also, the article proposes a system of principles for realization this Inspection, the tasks to be solved during its conduct, the mechanisms for their realization and presentation of its results.

Keywords: cybersecurity, cyber protection, critical informative infrastructure, strategic management, Inspection, measuring, analysis, evaluation.

Постановка проблеми. Динамічний розвиток інформаційно-комунікативних технологій (ІКТ), їх проникнення в усі сфери життєдіяльності особи, суспільства та держави є основою таких світових тенденцій як глобалізація, цифрова трансформація світового суспільства та економіки, сталого розвитку, забезпечення конкурентоспроможності тощо. Однак ІКТ одночасно актуалізують проблеми інформаційної безпеки, кібербезпеки та кіберзахисту, особливо для об'єктів критичної інформаційної інфраструктури (ОКІІ), зумовлені як збільшенням кількості та підвищенням складності кіберзагроз, кіберінцидентів, кібератак, насамперед з боку Російської Федерації [1], так і недостатньою готовністю (відповідністю сучасним вимогам) національної системи кібербезпеки до ефективної їх нейтралізації та протидії цим кіберзагрозам.

Успішне розв'язання окреслених проблем передбачає розробку окремої публічної політики та здійснення публічного адміністрування у сфері кібербезпеки й кіберзахисту на основі якісної оперативної вхідної інформації – основи прийняття управлінських рішень на всіх рівнях, у т. ч. й на стратегічному.

Законами України «Про основні засади забезпечення кібербезпеки України» [2] та «Про національну безпеку України» [3], законодавчими актами [1; 4; 5], що стосуються національної безпеки, зокрема сфери кібербезпеки та кіберзахисту, визначено низку неузгоджених між собою та не розкритих за своїм змістом, об'єктами, суб'єктами (їх чітких функцій та завдань, взаємодії між собою) тощо інструментів отримання достовірної, точної, повної, своєчасної інформації про стан кіберзахищеності. До цих інструментів належать: самооцінка об'єктів критичної інфраструктури (ОКІ) щодо стану кіберзахисту об'єктів критичної інформаційної інфраструктури, що базуються на застосуванні механізмів державно-приватного партнерства [6]; зовнішні оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та державний контроль, незалежний аудит, негласні перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів та ін. Проблема полягає як у відсутності або неповній формалізації кожного з вищевказаних інструментів, більшість із яких поки що перебувають у стадії

розробки та становлення, так і в їх комплексному застосуванні з урахуванням переваг та вад кожного з них.

Саме таким комплексним об'єднуючим механізмом оцінювання стану кіберзахисту, на думку авторів, повинен бути механізм державного управління – «огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом», який сформульовано в статтях 22 та 27 Закону України «Про національну безпеку України» [3] без розкриття сутності та змісту цього механізму, що актуалізує тему дослідження.

Аналіз останніх наукових досліджень і публікацій. Нормативно-правові аспекти системи кібербезпеки розглядались у працях К. Александера (*K. Alexander*), Дж. Ліпмана (*J. Liepman*), В. Мазурова, Р. Олдрича (*R. Aldrich*), Є. Старостиної, М. Шмітта (*M. Schmitt*), А. Щетилова. На теренах вітчизняної науки необхідно зазначити праці В. Бурячка, Р. Грищука, Ю. Даника, О. Довганя, Д. Дубова, В. Петрова, Т. Тропіної та інших учених.

Але в Україні обмаль досліджень, які стосуються огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Виділення не вирішених раніше частин загальної проблеми. У загальній проблемі забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури та державних інформаційних ресурсів особливо актуальною є проблема розробки й упровадження концептуальних засад механізму державного управління здійснення огляду з метою отримання актуальної інформації про реальний стан кіберзахисту цих об'єктів з урахуванням міжнародного досвіду в цій сфері, насамперед країн НАТО та ЄС.

Метою статті є обґрунтування й розробка концептуальних засад комплексного механізму державного управління оглядом стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, з урахуванням міжнародного досвіду в цій сфері, насамперед країн НАТО та ЄС.

Основні результати дослідження. Огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, як одна із складових частин Комплексного огляду сектору безпеки і оборони вперше визначена в Законі України «Про національну безпеку України» [3]. Цей Закон також включає оборонний огляд, огляд громадської безпеки та цивільного захисту, огляд оборонно-промислового комплексу (ОПК), огляд розвідувальних органів України та огляд загальнодержавної системи боротьби з тероризмом (*рис. 1*).

Але, на відміну від деяких інших складових Комплексного огляду сектору безпеки і оборони, в національному й міжнародному законодавстві та наукових працях на сьогодні відсутнє чітке визначення терміну, сутності та змісту огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Рис. 1. **Огляд стану кіберзахисту в організаційно-правовому механізмі комплексного огляду сектору безпеки та оборони**

Джерело: складено авторами.

Так, Законом [3] визначені:

- *комплексний огляд сектору безпеки і оборони* – процедура оцінювання стану й готовності складових сектору безпеки і оборони до виконання завдань за призначенням, за результатами розробляються й уточнюються концептуальні документи розвитку складових сектору безпеки і оборони та визначаються заходи, спрямовані на досягнення ними необхідних спроможностей до виконання завдань за призначенням у поточних і прогнозованих умовах безпекового середовища;

- *оборонний огляд* – процедура оцінювання стану й готовності сил оборони до виконання завдань з оборони України, стану їх кадрового, фінансового, матеріально-технічного та інших видів забезпечення;

- *огляд оборонно-промислового комплексу України* – процедура оцінювання стану й готовності оборонно-промислового комплексу стосовно задоволення потреби сектору безпеки і оборони в озброєнні, військовій та спеціальній техніці.

Аналіз наведених визначень вказує, по-перше, на застосування уніфікованого підходу до їх формулювань; по-друге, на відсутність формалізованих визначень для інших складових комплексного огляду сектору безпеки і оборони, як-от: огляд громадської безпеки та цивільного захисту, розвідувальних органів України, загальнодержавної системи боротьби з тероризмом.

Авторами з урахуванням міжнародного досвіду, зокрема міжнародного стандарту ISO/IEC 27004:2016 *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation* (Інформаційні технології – Методи захисту – Управління інформаційною безпекою – Моніторинг, вимірювання, аналіз та оцінка) [7] та шляхом застосування запровадженого в Законі уніфікованого підходу до визначення вищенаведених оглядів у сфері національної безпеки України, пропонуються такі визначення:

- *огляд стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури* – це процедура періодичного спостереження, вимірювання, аналізу та оцінювання стану і готовності кіберзахисту об'єктів критичної інформаційної інфраструктури, інформаційно-телекомунікаційних систем, у яких обробляються та зберігаються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом;

- *спостереження стану кіберзахисту* – спостереження стану кіберзахисту критичної інформаційної інфраструктури – активне, систематичне, цілеспрямоване, планомірне вивчення та постійне дослідження об'єктів огляду щодо заходів та засобів із кіберзахисту, котрі вживаються та застосовуються;

- *вимірювання заходів із кіберзахисту* – встановлення ефективності застосованих засобів та вжитих заходів з кіберзахисту для визначення потреби в їх поліпшенні;

- *показник ефективності заходу з* кіберзахисту – показник впливу успішного виконання конкретного заходу з кіберзахисту на спроможність об'єкта огляду запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем;

- *аналіз результатів вимірювання* – діяльність, спрямована на визначення відповідності отриманих результатів вимірювання щодо ефективності заходів із кіберзахисту очікуваним показникам;

- *оцінювання стану* – це процес інтерпретації результатів аналізу вимірювання задля визначення стану захищеності об'єктів огляду та продуктивності вжитих заходів.

Виходячи із законодавства, основну *мету* огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури (далі – *огляд*, *ОСК*) пропонується сформулювати як визначення реального стану захищеності й готовності об'єктів огляду до запобігання кіберінцидентам, оперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак, ліквідації їхніх наслідків, відновлення функціонування цих об'єктів і систем.

Система *принципів* проведення огляду повинна базуватися на загальних принципах кібербезпеки, визначених у статті 7 Закону [2], котрі з урахуванням особливостей ОСК доцільно трансформувати в такі:

- системного та комплексного застосування інструментів огляду з урахуванням їхньої

специфіки, у т. ч. переваг, вад, обмежень на використання тощо кожного з них;

- координованості та забезпечення балансу між окремими видами оглядів у системі оглядів комплексного огляду сектору безпеки і оборони;
- єдності методологічних засад захисту критичної інфраструктури;
- централізації управління процесами огляду;
- застосування програмно-цільового методу планування;
- прозорості використання ресурсів у сфері кіберзахисту;
- системності і паралельності заходів огляду та колегіальності під час прийняття рішень щодо його результатів;
- об'єктивності, який полягає в тому, що огляд проводиться на основі вихідних даних власників (розпорядників, операторів) об'єктів огляду, котрі відображають реальний стан кіберзахисту;
- результативності, який ґрунтується на гарантуванні державою науково-методичного, організаційно-технічного, інформаційного, матеріального та фінансового забезпечення завдань Стратегії кібербезпеки України та з урахуванням фінансово-економічних можливостей держави;
- програмного підходу до планування розвитку заходів і засобів кіберзахисту;
- повноти, який полягає в тому, що процедура ОСК охоплює діяльність усіх суб'єктів огляду;
- забезпечення здійснення демократичного цивільного контролю;
- обмеженої гласності, який полягає в тому, що проведення ОСК є прозорою процедурою, а результати, отримані під час виконання заходів огляду щодо конкретних механізмі кіберзахисту на об'єктах огляду, до певного моменту часу є інформацією з обмеженим доступом.

Огляд передбачає реалізацію таких основних *завдань*:

- визначення галузі (галузей) та об'єктів, щодо яких здійснюватиметься проведення ОСК;
- формування плану заходів з проведення ОСК з урахуванням їхніх галузевої та об'єктової специфіки;
- оцінювання затверджених власниками (розпорядниками) об'єктів огляду ризиків та відповідних політик інформаційної безпеки;
- наявність на об'єктах огляду систем інформаційної безпеки, відповідність їх створення, уведення в експлуатацію, експлуатації та модернізації вимогам міжнародних і галузевих стандартів або наявність комплексних систем захисту інформації з підтвердженою відповідністю, їх періодичні випробування та модернізація;
- визначення на об'єктах огляду підрозділів інформаційної безпеки (захисту інформації) та кіберзахисту, а також їх спроможність виконувати завдання і заходи ОСК, за їх відсутності – залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до проведення огляду, підготовки Звіту про результати його проведення та проектів концептуальних і планових документів у сфері кібербезпеки та кіберзахисту, насамперед Стратегії кібербезпеки України та плану заходів з її реалізації;
- упровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;
- упровадження стратегічного планування та програмно-цільового забезпечення у сфері розвитку кіберзахисту;
- оцінювання ефективності протоколів взаємодії об'єктів огляду, команд реагування на комп'ютерні надзвичайні події при кібератаках та кіберінцидентах, інших суб'єктів забезпечення кібербезпеки та кіберзахисту;
- оцінювання достатності заходів кіберзахисту, заходів з управління ризиками для запобігання та мінімізації впливу кібератак та кіберінцидентів;
- підготовка методичних та навчальних матеріалів для підвищення кваліфікації спеціалістів у сфері кіберзахисту, підготовки кадрів;
- визначення та/або вдосконалення критеріїв ризиків для заходів із здійснення державного контролю у сфері кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури;

- оцінювання стану кадрового, фінансового, матеріально-технічного та інших видів забезпечення, підрозділів, що безпосередньо виконують завдання із кіберзахисту об'єктів огляду.

Відповідно до цих завдань огляд є основним інструментом інформаційно-аналітичного забезпечення формування та виконання Стратегії кібербезпеки України, завдань та проектів до Національної програми інформатизації, інших концептуальних, програмних і планових документів у сфері кібербезпеки та кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

За рішенням Ради національної безпеки і оборони України (РНБОУ), яке вводиться в дію Указом Президента України, огляд може здійснюватися як у складі комплексного огляду сектору безпеки і оборони, так і окремо, але в обох випадках саме на Уряд покладається завдання щодо визначення загального порядку його проведення, насамперед щодо організації, контролю та попереднього схвалювання результатів проведення та надання звіту у встановленому порядку на розгляд і остаточне затвердження РНБОУ. Звіт повинен стати основним інформаційно-аналітичним документом, спрямованим на формування державної політики у сфері кібербезпеки та кіберзахисту, зокрема розробки (корегування) Стратегії кібербезпеки та планів з її реалізації, а його відкрита частина повинна оприлюднюватися.

Результати огляду у складі комплексного огляду сектору безпеки та оборони в агрегованому вигляді повинні застосовуватися при формуванні Стратегії національної безпеки України, після прийняття якої вони в більш конкретизованому та деталізованому вигляді повинні враховуватись та відображатись у Стратегії кібербезпеки України, програмах і планах з її реалізації, інших концептуальних, програмних та планових документах ієрархічної системи нормативно-правових актів у сфері кібербезпеки та кіберзахисту, у т. ч. під час створення та забезпечення функціонування Національної телекомунікаційної мережі, тощо.

Загальна схема проведення огляду стану готовності кіберзахисту об'єктів огляду та підготовки за його результатами звіту представлена на *рис. 2.*

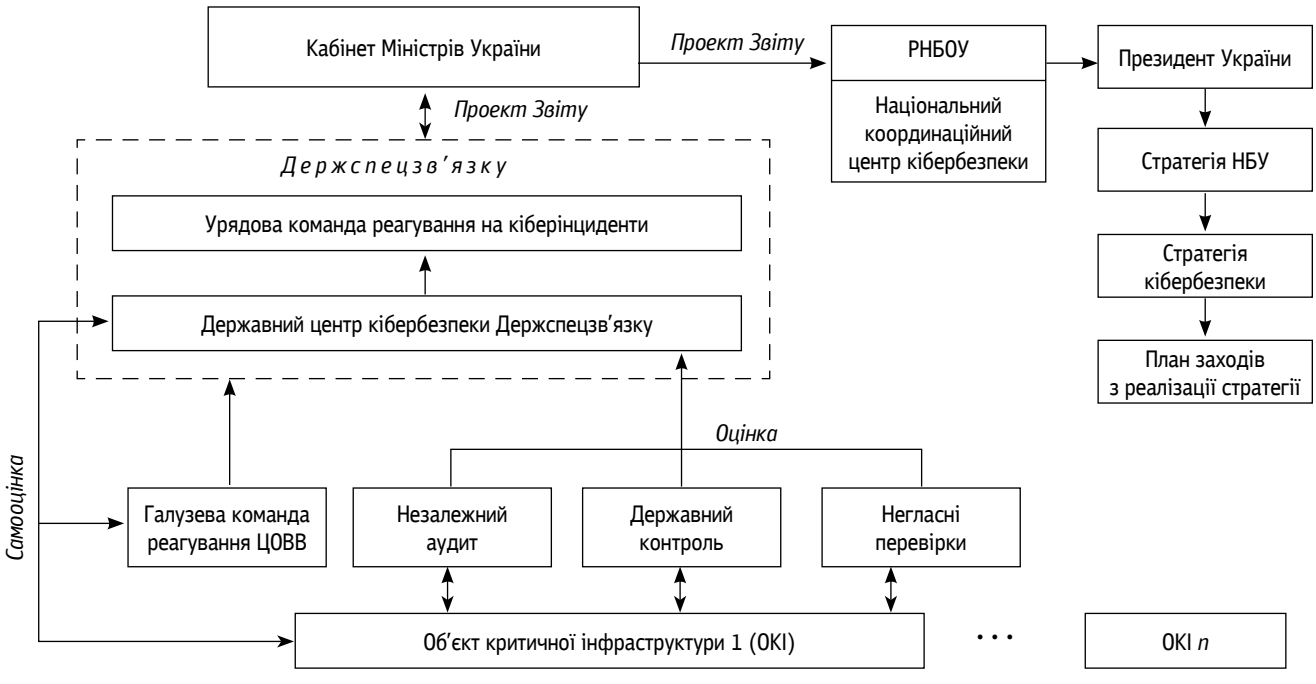

Рис. 2. **Загальна схема проведення огляду стану готовності кіберзахисту об'єктів огляду та підготовки звіту**

Джерело: складено авторами.

Суб'єктами проведення огляду є: державні органи, відповідальні за формування переліку об'єктів критичної інформаційної інфраструктури та їх внесення до Державного реєстру об'єктів критичної інформаційної інфраструктури, проведення незалежного аудиту, державного контролю та негласних перевірок у цій сфері; Національний координаційний центр кібербезпеки; Державний центр кіберзахисту; команди реагування на комп'ютерні надзвичайні події; володільці (розпорядники) об'єктів критичної інфраструктури.

Об'єктами проведення огляду є: інформаційно-телекомунікаційні системи, в яких обробляються/зберігаються державні інформаційні ресурси; ОКІІ, які згідно із законодавством визначаються Урядом за пропозиціями відповідних державних органів. Якщо на сьогодні законодавством передбачено систему критеріїв визначення ОКІ і, відповідно, існують підходи щодо формування переліку ОКІІ та їх внесення до Державного реєстру ОКІІ, то стосовно переліку державних електронних інформаційних ресурсів, які повинні бути захищені, вони просто відсутні.

Система державних інформаційних ресурсів украй неоднорідна, складна, включає різні за важливістю та значущістю ресурси, які потребують різних підходів до їх кіберзахисту. Це зумовлює необхідність їх диференціації (категоризації) з поділом, як мінімум, на такі, що потребують обов'язкового державного регулювання кіберзахисту з включенням їх до переліку ОКІІ та внесенням до Державного реєстру ОКІІ. Наприклад, це такі загальнодержавні електронні інформаційні ресурси, як-от: Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань; Державний реєстр фізичних осіб – платників податків тощо і такі, що не потребують втручання держави щодо визначення спеціальних заходів для їх кіберзахисту. Такий підхід дозволить спростити, розвантажити та здешевити систему кіберзахисту державних інформаційних ресурсів.

При цьому існують два принципово різні підходи щодо організації та проведення огляду стану кіберзахисту. Згідно з першим підходом передбачається розроблення окремого комплексу процедур спостереження, вимірювання, аналізу та оцінювання, орієнтованих на формування й виконання загальнодержавних концептуальних, програмних та планових документів. Другий підхід орієнтовано на ефективне використання вже існуючих у системі кібербезпеки та кіберзахисту процедур, їх уточнення (за необхідності) та раціональне об'єднання в єдину процедуру огляду стану кіберзахисту.

Перший підхід потребує більших зусиль та ресурсів на розробку та впровадження, але саме він потенційно найбільше відповідає потребам інформаційно-аналітичного забезпечення процесам формування й реалізації відповідної публічної політики та адміністрування. Основною перевагою другого підходу є суттєве зменшення ресурсів на проведення огляду, у т. ч. часових витрат і підготовку суб'єктів та об'єктів кіберзахисту. Другий підхід можна також розглядати як підготовчий етап до переходу до першого підходу.

Ураховуючи особливості розвитку України, про які йшлося вище, детально розглянемо другий підхід щодо організації та проведення огляду.

Центральним органом виконавчої влади, який повинен безпосередньо здійснювати державне управління (регулювання) проведенням огляду, законодавством визначено Державну службу спеціального зв'язку та захисту інформації (Держспецзв'язку), але без конкретизації та деталізації завдань та функцій з цієї проблеми, насамперед щодо організації, координації, контролю, процедур спостереження, вимірювання, аналізу та оцінювання стану й готовності кіберзахисту об'єктів критичної інформаційної інфраструктури, інформаційно-телекомунікаційних систем, у яких обробляються/зберігаються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, а також без встановлення повноважень цієї Служби щодо отримування та оброблення результатів самооцінки ОКІ та зовнішніх оцінок (незалежного аудиту, негласних перевірок готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів та інших), формування на їх основі проекту узагальненого звіту про результати огляду.

Проект розробленого звіту Держспецзв'язку має надавати до Кабінету Міністрів України, який його погоджує й у встановленому порядку подає для розгляду і затвердження Радою національної безпеки і оборони України.

Оцінювання ефективності заходів із кіберзахисту може здійснюватися підрозділами захисту інформації/інформаційної безпеки власників (розпорядників) ОКІ (самооцінювання) або на договірних засадах – Державним центром кібер-

захисту, командами реагування на надзвичайні комп'ютерні події, які відповідають встановленим для них вимогам, а також підприємствами, установами та організаціями, які мають ліцензію на право провадження господарської діяльності у сфері захисту інформації або здійснюють аудит інформаційної безпеки.

При цьому самооцінка заходів із кіберзахисту ОКІ є основною процедурою огляду та повинна здійснюватися постійно з урахуванням внутрішнього об'єктового режиму на підставі затверджених власниками (розпорядниками) таких об'єктів ризиків інформаційної безпеки та відповідних запроваджених заходів і процесів безперервності забезпечення кіберзахисту державних інформаційних ресурсів та ОКІ, а також визначених власниками (розпорядниками) ОКІ. Це:

- об'єкти спостереження та вимірювання, включно й процеси та заходи інформаційної безпеки;
- методики спостереження, вимірювання, аналізу та оцінювання, які можуть бути застосовані для гарантування достовірності та обґрунтованості їх результатів;
- суб'єкти та причини й підстави проведення спостереження, вимірювання, аналізу та оцінювання.

Під час самооцінювання або оцінювання ефективності заходів з кіберзахисту об'єкта огляду щонайменше оцінюється виконання загальних вимог забезпечення кіберзахисту, затверджених Урядом, а саме: його власником (розпорядником) або суб'єктом, що здійснює аудит інформаційної безпеки, формуються відомості про запроваджені заходи з кіберзахисту.

При цьому актуальною проблемою є обґрунтований вибір системи показників вимірювання стану кіберзахисту об'єктів огляду, яка зумовлена як різнотипністю цих об'єктів, так і різноманітністю складових огляду, їх цілей, інструментів застосування та підсистем показників і індикаторів, методичних апаратів спостереження, вимірювання, аналізу та оцінювання тощо. Формування загального вектора вимірювання (оцінювання) стану кіберзахисту для таких умов може здійснюватися шляхом:

- об'єднання існуючих підсистем показників (індикаторів) складових огляду в єдину сукупність показників з усуненням дублювання, але без змін існуючих підсистем показників;
- розроблення загального вектора вимірювання (оцінювання) стану кіберзахисту об'єктів огляду з подальшим його раціональним розподілом серед часткових підсистем показників (індикаторів) кожної складової огляду;
- розроблення єдиного для всіх складових огляду «уніфікованого» вектора вимірювання (оцінювання) стану кіберзахисту об'єктів огляду;
- узяття за основу однієї з існуючих міжнародних систем оцінювання стану кіберзахисту з наступною її адаптацією в інтересах супроводження відповідних концептуальних, стратегічних, програмних, планових та прогнозних документів з розподілом показників (індикаторів) між відповідними підсистемами складових огляду.

Кожен із вищевказаних підходів має свої переваги та вади. Так, найменш витратним є перший підхід, реалізація якого потребує ще й найменших зусиль. Але просте об'єднання існуючих підсистем вимірювання (оцінювання) стану кіберзахисту об'єктів огляду може не повною мірою відповідати вимогам ефективного формування та виконання, наприклад, Стратегії кібербезпеки України, оскільки досягнення часткових цілей складових огляду зовсім не означає досягнення його загальної цілі. Крім того, цей підхід не враховує міжнародний досвід розроблення та застосування аналогічних процедур.

Найбільш витратним, на думку авторів, є підхід, що передбачає розроблення «уніфікованого» для всіх складових огляду вектора вимірювання (оцінювання), що фактично означає виключення всіх інших складових огляду, крім однієї. У той же час саме такий підхід дозволяє забезпечити максимальну взаємну узгодженість вихідних даних (результатів оцінювання) складових огляду, спростити процедуру врахування їх результатів при формуванні загальної оцінки стану кіберзахисту за результатами проведення огляду.

Формування системи показників (індикаторів) на основі однієї з міжнародних систем показників (системи показників однієї з провідних країн світу) з адаптацією її до мети та завдань національної політики у сфері кіберзахисту (Стратегії кібербезпеки України), а також розподіл її показників між показниками складових

огляду або без такого розподілу є достатньо раціональним з точки зору розв'язання зазначеної проблеми.

При формуванні системи показників необхідно врахувати той факт, що частина з них має якісний характер, а кількісні показники – різні шкали вимірювань, що суттєво ускладнює процедуру оцінювання.

Тому одним із провідних завдань Держспецзв'язку має бути розроблення типової методики спостереження, вимірювання, аналізу та оцінювання, які можуть бути застосовані для гарантування достовірності та обґрунтованості їх результатів.

ВИСНОВКИ

1. У статті розглянуто концептуальні засади комплексного механізму державного управління оглядом стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, з урахуванням міжнародного досвіду в цій сфері, насамперед країн НАТО та ЄС, а саме: на основі міжнародного досвіду запропоновано терміни «огляд стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури», «спостереження стану кіберзахисту», «вимірювання заходів із кіберзахисту», «показник ефективності заходів із кіберзахисту», «аналіз результатів вимірювання», «оцінювання стану»; визначено мету, об'єкти та суб'єкти, основні завдання, систему принципів огляду кіберзахисту.

2. Уперше запропоновано розглядати механізм державного управління оглядом кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури як раціональне об'єднання механізмів державного контролю, негласних перевірок СБУ щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, державно-приватного партнерства, механізмів самооцінювання та незалежного аудиту.

3. Визначено й проаналізовано науково-методологічні підходи до формування системи показників вимірювання стану кіберзахисту об'єктів огляду, як-от: об'єднання існуючих підсистем показників (індикаторів) складових огляду в єдину сукупність показників з усуненням дублювання, але без змін існуючих підсистем показників; розроблення загального вектора вимірювання (оцінювання) стану кіберзахисту об'єктів огляду з подальшим його раціональним розподілом серед часткових підсистем показників (індикаторів) кожної складової огляду; розроблення єдиного для всіх складових огляду «уніфікованого» вектора вимірювання (оцінювання) стану кіберзахисту об'єктів огляду; вибір за основу однієї з існуючих міжнародних систем оцінювання стану кіберзахисту з наступною її адаптацією.

4. Визначено місце механізму самооцінки в комплексному механізмі проведення огляду стану кіберзахисту державних інформаційних ресурсів та ОКІІ та його основні завдання.

5. Уточнено й конкретизовано механізм державного управління інформаційно-аналітичним забезпеченням формування та виконання Стратегії кібербезпеки України, інших концептуальних, програмних та планових документів за результатами проведення огляду.

Подальшими перспективами розвитку означеної проблеми передбачається насамперед обґрунтування системи показників у комплексному механізмі проведення огляду стану кіберзахисту державних інформаційних ресурсів та ОКІІ, розвиток механізмів інформаційної взаємодії з питань кібербезпеки та кіберзахисту з міжнародними організаціями, країнами ЄС та НАТО.

Список використаних джерел

1. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1009-2017-р
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 р. № 2163-VIII [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2163-19
3. Закон України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2163-19/print1509543369819103

4. Стратегія кібербезпеки України, схвалена Указом Президента України від 15 березня 2016 р. № 96/2016 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016
5. Стратегія національної безпеки України, схвалена Указом Президента України від 26 травня 2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/287/2015
6. Дубов Д.В. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. – К. : НІСД, 2018. – 84 с.
7. ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation (second edition) [Електронний ресурс]. – Режим доступу : http://www.iso27001security.com/html/27004.html

References

1. Kontseptsiia stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury, skhvalena rozporiadzhenniam Kabinetu Ministriv Ukrainy vid 6 hrudnia 2017 r. № 1009-r [The concept of the creation of a state system for the protection of critical infrastructure, approved by the Cabinet of Ministers of Ukraine Decree of December 6, 2017, No. 1009-r]. (n.d.). *zakon2.rada.gov.ua*. Retrieved from http://zakon2.rada.gov.ua/laws/show/1009-2017-p [in Ukrainian].
2. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» vid 05 zhovtnia 2017 r. № 2163-VIII [Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" dated October 05, 2017, No. 2163-VIII]. (n.d.). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/2163-19 [in Ukrainian].
3. Zakon Ukrainy «Pro natsionalnu bezpeku Ukrainy» vid 21 chervnia 2018 r. № 2469-VIII [Law of Ukraine "On National Security of Ukraine" dated June 21, 2018, No. 2469-VIII]. (n.d.). *zakon2.rada.gov.ua*. Retrieved from http://zakon2.rada.gov.ua/laws/show/2163-19/print1509543369819103 [in Ukrainian].
4. Stratehiia kiberbezpeky Ukrainy, skhvalena Ukazom Prezydenta Ukrainy vid 15 bereznia 2016 r. № 96/2016 [Cybersecurity Strategy of Ukraine, approved by Decree of the President of Ukraine dated March 15, 2016, No. 96/2016]. (n.d.). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/96/2016 [in Ukrainian].
5. Stratehiia natsionalnoi bezpeky Ukrainy, skhvalena Ukazom Prezydenta Ukrainy vid 26 travnia 2015 r. № 287/2015 [The National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated May 26, 2015, No. 287/2015]. (n.d.). *zakon4.rada.gov.ua*. Retrieved from http://zakon4.rada.gov.ua/laws/show/287/2015 [in Ukrainian].
6. Dubov, D.V. (2018). *Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy [Public-private partnership in the field of cybersecurity: international experience and opportunities for Ukraine]*. Kyiv: NISS. (84 p.) [in Ukrainian].
7. ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation (second edition). (n.d.). *www.iso27001security.com*. Retrieved from http://www.iso27001security.com/html/27004.html [in English].