УДК 351.86

А. І. Семенченко,
д. н. держ. упр., професор, Національна академія державного управління при Президентові України
Д. В. Мялковський,
аспірант, Інститут підготовки кадрів державної служби зайнятості України
Т. В. Станіславський,
аспірант, Інститут підготовки кадрів державної служби зайнятості України

НАУКОВО-МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ПРОВЕДЕННЯ ОГЛЯДУ КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

A. Semenchenko,
Doctor of Science in Public Administration, Professor, National Academy of Public Administration under the President of Ukraine
D. Mialkovskyi,
Student of PhDdegreeprograms Institute of Personnel Training of the State Employment Service of Ukraine
T. Stanislavskyi,
Student of PhD degree programs Institute of Personnel Training of the State Employment Service of Ukraine

SCIENTIFIC AND METHODOLOGICAL APPROACHES TO A REVIEW OF CYBERPROTECTION OF PUBLIC INFORMATION RESOURCES AND CRITICAL INFORMATION INFRASTRUCTURE

У статті розглянуто науково-методологічні підходи до організації та проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, актуальність дослідження яких обумовлена 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 та кіберінценденти. У статті визначається мета проведення огляду, для досягнення якої запроваджується система принципів, заходів і суб'єктів їх реалізації, об'єднаних єдиним задумом. Це дозволяє перманентно оцінювати стан захищеності державних інформаційних ресурсів та критичної інформаційної інфраструктури, оцінюючи його не тільки з точки зору запобігання кіберінцидентам та кібератакам, а й готовності та спроможності відповідних суб'єктів дооперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак, а такождо відновляння роботи систем, які можуть постраждати в наслідок вдалих атак. Запропонований у статті спосіб проведення огляду системно його ув'язує з інформаційно-аналітичним забезпеченням Стратегії кібербез-

пеки України, планами заходів з її реалізації, періодичним проведенням огляду національної системи кібербезпеки тощо, чітко визначає її місто в цих процесах.

The article deals with the scientific and methodological approaches to the organization and implementation of the review of the state of cyber protection of critical information infrastructure, public information resources and information, the demand for protection of which is established by law, the urgency of which study is due both to the requirements of the current legislation and to the development trends of the national security and defense, inconsistency of state policy and public administration with the requirements of reliable and prompt response to cyber-threats and cyber-incidents. The article defines the purpose of conducting the survey, for achieving which a system of principles, measures and subjects of their implementation is implemented, united by a single plan. It allows to permanently assess the condition of the protection of state information resources and critical information infrastructure, assessing it not only from the point of view of preventing cyber incidents and cyberattacks, but also the readiness and ability of the relevant actors to respond promptly to cyber threats, prevention, detection and protection against cyberattacks, and as well as the restoration of systems that could suffer as a result of successful attacks. The method of the review proposed in the article systematically links it with the information-analytical support of the Strategy of Ukraine's cybersecurity, plans for its implementation, periodic review of the national cybersecurity system, etc., clearly defines its city in these processes.

Ключові слова: кібербезпека, кіберзахист, критична інформаційна інфратруктура, огляд стану кіберзахисту, науково-методологічні підходи.

Key words: cybersecurity, cyberprotection, purpose of conducting the survey,assess the condition of the protection critical informationinfrastructure.

ПОСТАНОВКА ПРОБЛЕМИ

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

Успішне розв'язання цієї проблеми передбачає розробку окремої публічної політики та здійснення публічного адміністрування у сфері кібербезпеки та кіберзахисту на основі якісної та оперативної вхідної інформації — основи прийняття управлінських рішень на всіх рівнях, у тому числі на стратегічному рівні.

При цьому існують два принципово різні підходи до організації та проведення огляду стану кіберзахисту. Згідно з першим підходом передбачається розробка окремого комплексупроцедур спостереження, вимірювання, аналізу та оцінювання, орієнтованих на формування та виконання загальнодержавних концептуальних, програмних та планових документів. Другий підхід орієнтовано на ефективне використання вже існуючих в 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 його розробку та впровадження, але саме він потенційно в найбільший ступені відповідає потребам інформаційно-аналітичного забезпечення процесам формування та реалізації публічної політики та адміністрування в цій сфері. Головною перевагою другого підходу є суттєве зменшення витрат на проведення огляду, у тому числі, часових витрат та на підготовку суб'єктів та об'єктів кіберзахисту до проведення вищевказаних процедур. Другий підхід можна також розглядати як підготовчий (попередній) етап до переходу до першого підходу. Враховуючи особливості сучасного розвитку України, про які йшла мова вище, насамперед щодо необхідності якомога швидшого прийняття рішень з розв'язання проблем у сфері кібербезпеки та кіберзахисту з мінімально можливими при цьому ресурсними витратами, розглянемо більш детально другій підхід до організації та проведення огляду.

Законодавством [1—5], що стосуються національної безпеки, зокрема сфери кібербезпеки та кіберзахисту, визначено низку неугоджених між собою та нерозкритих 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 кіберзахисту. До цих

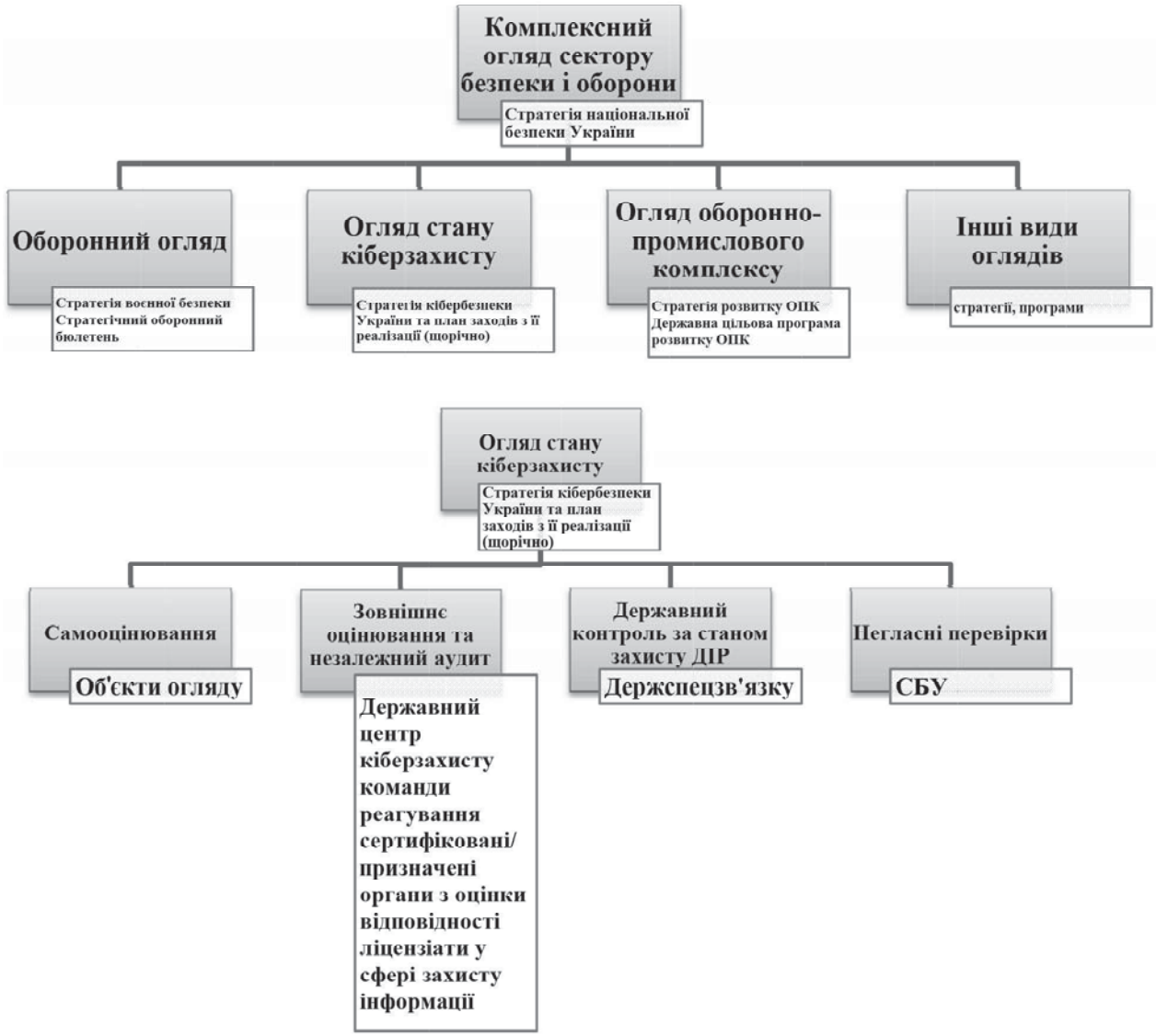

Рис. 1. Огляд стану кіберзахисту в організаційно-правовому механізмі комплексного огляду сектору безпеки і оборони

інструментів, насамперед відносяться: самооцінка об'єктів критичної інфраструктури (ОКІ) стану кіберзахисту їх об'єктів критичної інформаційної інфраструктури (ОКІІ), що базуються, у тому числі, на застосуванні механізмів державно-приватного партнерства [6]; зовнішні оцінки за результатами проведення державного контролю, незалежного аудиту, негласних перевірок готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів та інші. Проблема полягає як у відсутності або неповної формалізації кожного з вищевказаних інструментів, більшість з яких знаходяться поки що тільки в стадії своєї розробки та становлення, так і в їх комплексному застосуванню з урахуванням переваг та вад кожного з них.

Саме таким комплексним об'єднуючим механізмом оцінюваннястану кіберзахисту відповідно до другого підходу, на думку авторів, повинен бути механізм державного управління "оглядом стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом", якій сформульовано в статтях 22 та 27 Закону України "Про національну безпеку України"[3] без розкриття його сутності та змісту, що актуалізує тему дослідження.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Нормативно-правові аспекти системи кібербезпеки розглядалися у працях К. Александера (Alexander K.), Дж. Ліпмана (Liepman, J), В. Мазурова, Р. Олдрича (Aldrich R.), Є. Старостиної, М. Шмітта (Schmitt M.), А. Щетилова. Серед вітчизняних науковців необхідно відмітити праці В. Бурячка, Р. Грищука, Ю. Даника, О. Довганя, Д. Дубова, В. Петрова, Т. Тропініної та ін.

Але в Україні досліджень з питань огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, недостатньо.

ВИОКРЕМЛЕННЯ НЕ ВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

У загальній проблемі забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури та дер-

жавних інформаційних ресурсів особливо актуальною є проблема розробки та впровадження науково-методологічних підходів до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури з урахуванням міжнародного досвіду в цій сфері.

МЕТА СТАТТІ

Метою статті є обгрунтування та розробка науково- методологічних підходів до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури з урахуванням міжнародного досвіду в цій сфері.

ОСНОВНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, вперше як одна з складовихКомплексного огляду сектору безпеки і оборони зазначена в Законі України "Про національну безпеку України" [3], якій також включає оборонний огляд, огляд громадської безпеки та цивільного захисту, огляд оборонно-промислового комплексу, огляд розвідувальних органів України та огляд загальнодержавної системи боротьби з тероризмом. Але на відміну від деяких інших складових Комплексного огляду сектору безпеки і оборони в національному та міжнародному законодавстві та наукових працях на сьогодні відсутнє чітке визначення терміну, сутності та змісту огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Так, законом [3] визначені:

комплексний огляд сектору безпеки і оборони- процедура оцінювання стану і готовності складових сектору безпеки і оборони до виконання завдань за призначенням, за результатами якої розробляються та уточняються 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 і 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 і готовності оборонно-промислового комплексу стосовно задоволення потреби сектору безпеки і оборони в озброєнні, військовій та спеціальній техніці.

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

Окрім того, п.4.4 Стратегії кібербезпеки України [4] та п. 3 статті 8 Закону України "Про основні засади захисту кібербезпеки України [2] передбачена процедура "періодичного проведення огляду національної системи кібербезпеки та розроблення індикаторів стану кібербезпеки" як одного з пріоритетних напрямів діяльності національної системи кібербезпеки, але без чіткого її визначення, взаємозв'язку з іншими оглядами сектору безпеки та оборони, насамперед оглядом стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, а також з комплексним оглядом сектора безпеки та оборони, що є колізією вищевказаних законодавчих актів з Законом України "Про національну безпеку України" (рис. 1).

Авторами з урахуванням міжнародного досвіду, зокрема [7] та шляхом застосування запровадженого в законі уніфікованого підходу до визначення вищенаведених оглядів у сфері національної безпеки України, пропонується таке визначення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, а саме це — процедура періодичного спостереження, вимірювання, аналізу та оцінювання стану і готовності кіберзахисту об'єктів критичної інформаційної інфраструктури, інформаційно-телекомунікаційних систем (ІТС), в яких обробляються та зберігаються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом;спостереження стану кіберзахисту-активне, систематичне, цілеспрямоване, планомірне і вивчення реального стану кіберзахисту, спрямованих на запобігання кіберінцидентам, виявлення, попередження та припинення кібератак, ліквідацію їх наслідків, здатності об'єктів критичної інформаційної інфраструктури до відновлення роботи після кібератак та кіберінцидентів.

Виходячи з законодавства, головну мету огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури (далі — огляд) пропонується сформулювати як: визначення стану захищеності і готовності державних інформаційних ресурсів та критичної інформаційної інфраструктури до запобігання кіберінцидентам, оперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак, ліквідації їх наслідків, відновлення функціонування цих об'єктів і систем.

Система принципів проведення огляду повинна базуватись на загальних принципах кібербезпеки, визначених в статті 7 закону [2], які з урахуванням його особливостей доцільно трансформувати в такі:

системного та комплексного застосування інструментів огляду з урахуванням їх специфіки, утому числі, переваг, вад, обмежень на використання, тощо кожного з них;

координованості та забезпечення балансу між окремими видами оглядів в 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;

Рис. 2. Складові комплексного огляду сектору безпеки та оборони

об'єктивності, який полягає в тому, що огляд проводиться на основі вихідних даних власників (розпорядників, операторів) об'єктів огляду, що відображають реальний стан кіберзахисту;

результативності, який грунтується 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 отриманні при виконанні 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 їх галузевої та об'єктової специфіки;

— оцінювання затверджених власниками (розпорядниками) об'єктів огляду ризиків та відповідних ним політик інформаційної безпеки;

— наявність на об'єктах огляду систем інформаційної безпеки, відповідність їх створення, уведення в експлуатацію, експлуатації та модернізації вимогам міжнародних та 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 та, 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 та планових документів у сфері кібербезпеки та кіберзахисту, насамперед Стратегії кібербезпеки України та плану заходів з її реалізації;

— впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

— впровадження стратегічного планування та програмно-цільового забезпечення у сфері розвитку кіберзахисту, у тому числі, формування завдань та проектів до Національної програми інформатизації;

— оцінка ефективності протоколів взаємодії об'єктів огляду, команд реагування на комп'ютерні надзвичайні події (команд реагування) при кібератаках та кіберінцідентах, інших суб'єктів забезпечення кібербезпеки та кіберзахисту;

— оцінка достатності та ефективності 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.

— оцінка 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 та 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 бути підгрунтям для формування державної політики у сфері кібербезпеки та кіберзахисту, зокрема розробки (корегування) Стратегії кібербезпеки та планів з її реалізації, а його відкрита частина повинна оприлюднюватись.

При цьому законодавством чітко не визначено місце і роль такого важливого огляду як "періодичне проведення огляду національної системи кібербезпеки" в комплексному огляді сектору безпеки і оборони, формуванні та реалізації Стратегії національної безпеки України, Стратегії кібербезпеки України та інших документів, а також його взаємодія з оглядом стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Водночас механізм виконання Стратегії кібербезпеки України, що передбачає щороку розробляти і затверджувати плани заходів з її реалізації та щопівроку інформувати про стан їх виконання, є декларативним, ресурсна непідтриманим, вкрай інерційним. Так, наприклад, плани заходів з реалізації Стратегії кібербезпеки України у 2017 та 2018 роках приймались з запізненням відповідно на 3 та 7 місяців, а систему індикаторів стану кібербезпеки, яка має включати в себе підсистему індикаторів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, й досі нерозроблено.

Тому, на думку авторів, крім вищевказаних варіантів застосування огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури (автономного та у складі комплексного огляду сектору безпеки та оборони) необхідно також передбачити його застосування у складі процедури періодичного проведення огляду національної системи кібербезпеки, якій може також здійснюватися або автономно або у складі комплексного огляду сектору безпеки та оборони.

При цьому ієрархічну модель взаємодії вищевказаних оглядів, як складових комплексного огляду, можна представити схематично (рис. 2).

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 тому числі у відповідних завданнях Національної програми інформатизації, при створенні та забезпеченні функціонування Національної телекомунікаційної мережі, тощо.

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 в 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 вже здійснюється або передбачається оброблення державних інформаційних ресурсів, та ОКІІ, які згідно із законодавством визначаються Урядом за пропозиціями відповідних державних органів. Якщо на сьогодні законодавством передбачено систему критеріїв визначення ОКІ і, відповідно, є підходи до формування переліку ОКІІ та їх внесення до Державного реєстру ОКІІ, то стосовно формування переліку державних електронних інформаційних ресурсів, які повинні бути захищені, вони просто відсутні. Система державних інформаційних ресурсів вкрай неоднорідна, складна, включає різні по важливості та значущості ресурси, які потребують різних підходів до їх кіберзахисту. Цеобумовлює необхідність їх диференціації (категоризації) з поділом як мінімум на такі, що потребують обов'язкового кіберзахисту з включенням їх до переліку ОКІІ та внесення до Державного реєстру ОКІІ. Наприклад, такі загальнодержавні електронні інформаційні ресурси: Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Державний реєстр фізичних осіб-платників податків, тощо і такі, що не потребують спеціальних заходів для їх кіберзахисту. Такій підхід дозволить спростити, розвантажити та здешевити систему кіберзахисту державних інформаційних ресурсів.

Центральним органом виконавчої влади, які й повинен безпосередньо здійснювати державне управління (регулювання) проведенням огляду, законодавством визначено Держспецзв'язку, але без конкретизації та деталізації його завдань та функцій з цієї проблеми, насамперед щодо організації, координації, контролю, тощо процедур спостереження, вимірювання, аналізу та оцінювання стану і готовності кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, а також його повноважень щодо отримання самооцінок ОКІ та зовнішніх оцінок огляду (за результатами проведення незалежного аудиту, оцінювання стану захищеності, державного контролю за станом захисту інформації, 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 надаватидо Кабінету Міністрів України, якій його погоджує у встановленому порядку подає длярозгляду і затвердження Радою національної безпеки і оборони України.

Оцінювання ефективності заходів з кіберзахисту може здійснюватись підрозділами захисту інформації / інформаційної безпеки власників (розпорядників) ОКІ-(самооцінювання) або, на договірних засадах, Державним центром кіберзахисту, командами реагування на надзвичайні комп'ютерні події, які відповідають встановленим для них вимогам, а також підприємствами, установами і організаціями, які мають відповідну компетенцію (ліцензію) на право провадження господарської діяльності у сфері захисту інформації, або здійснюють аудит інформаційної безпеки.

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

— об'єктів спостереження та вимірювання, включаючи процеси інформаційної безпеки та заходи безпеки;

— методики спостереження, вимірювання, аналізу та оцінювання, які можуть бути застосовані для гарантування достовірності та обгрунтованості їх результатів;

— причин, підстав та суб'єктів проведення спостереження, вимірювання, аналізу та оцінювання.

При проведенні 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 єобгрунтований вибір системи показників вимірювання стану кіберзахисту об'єктів огляду, яка обумовлена 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 вектору 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;

— розробки загального вектору вимірювання (оцінювання) стану кіберзахисту об'єктів огляду з подальшим його раціональним розподілом серед часткових підсистем показників (індикаторів) кожної складової огляду;

— розробки єдиного для всіх складових огляду "уніфікованого" вектору вимірювання (оцінювання) стану кіберзахисту об'єктів огляду;

— вибір 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 з вищевказаних підходів має свої переваги та вади. Так найменш витратним є перший підхід, реалізація якого окрім того потребує й найменших зусиль. Але просте об'єднання існуючих підсистем вимірювання (оцінювання) стану кіберзахисту об'єктів огляду може не в повній мірі 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, даний підхід не враховує міжнародний досвід розроблення та застосування аналогічних процедур.

Найбільш витратним, на думку авторів, є підхід, що передбачає розробку "уніфікованого" для всіх складових огляду вектору вимірювання (оцінювання), що фактично означає виключення всіх інших складових огляду окрім однієї. Водночас саме такій 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 домети та завданьнаціональної 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 з головних завдань Держспецзв'язку має бути розроблення типової методики спостереження, вимірювання, аналізу та оцінювання, які можуть бути застосовані для гарантування достовірності та обгрунтованості 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"; визначено мету, об'єкти та суб'єкти, основні завдання, систему принципів огляду кіберзахисту.

2. Вперше 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 готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, державно-приватного партнерства, механізмів самооцінювання, незалежного аудиту.

3. Визначено та проаналізовано науково-методологічні підходи до формування системи показників вимірювання стану кіберзахисту об'єктів огляду:

об'єднання існуючих підсистем показників (індикаторів) складових огляду в єдину сукупність показників з усуненням дублювання, але без змін існуючих підсистем показників; розробки загального вектору вимірювання (оцінювання) стану кіберзахисту об'єктів огляду з подальшим його раціональним розподілом серед часткових підсистем показників (індикаторів) кожної складової огляду; розробки єдиного для всіх складових огляду "уніфікованого" вектору 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 основні завдання.

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

6. Запропоновано розширити варіанти застосування огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, а саме не тільки як автономну процедуру та складову комплексного огляду сектору безпеки та оборони, а також передбачити його проведення у складі процедури періодичного проведення огляду національної системи кібербезпеки. Внести відповідні зміни до законів "Про основні засади кібербезпеки України" та "Про національну безпеку України" щодо автономного застосування періодичного проведення огляду національної системи кібербезпеки або у складі комплексного огляду сектору безпеки та оборони.

Подальшими перспективами розвитку даної проблеми передбачається, насамперед обгрунтування системи показників вкомплексному 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, удосконалення категорійно-понятійного апарату, насамперед щодо визначення огляду національної системи кібербезпеки, визначення індикаторів стану кіберзахисту та кібербезпеки, автоматизації процесів проведення огляду стану кіберзахисту державних інформаційних ресурсів та ОКІІ.

Література:

1. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р // Урядовий кур'єр від 10.01.2018-№ 5.

2. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII (Набрання чинності відбудеться 09.05.2018) // Урядовий кур'єр від 15.11.2017- № 215.

3. Закон України "Про національну безпеку України" від 21.06.2018 № 2469-VIII // Урядовий кур'єр від 18.07.2018-№ 132.

4. Указ Президента України від 15.03.2016 № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", Урядовий кур'єр від 18.03.2016-№ 52.

5. Указ Президента України від 26.05.2015 № 287/2015 "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" // Урядовий кур'єр від 29.05.2015-№ 95.

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. Міжнародний стандарт ISO/IEC 27004:2016 Informationtechnology — Securitytechniques — Informationsecuritymanagement — Monitoring, measurement, analysisandevaluation [Електронний ресурс]. — Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:27004:ed-2:v1:en

References:

1. Cabinet of Ministers of Ukraine (2017), "The concept of the creation of a state system for the protection of critical infrastructure", Uriadovyjkur'ier, vol. 5 (2018).

2. Verkhovna Rada of Ukraine (2017), The Law of Ukraine "About the basic principles of providing cyber security of Ukraine", Uriadovyjkur'ier, vol. 215.

3. Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On National Security of Ukraine", Uriadovyjkur'ier, vol. 132.

4. President of Ukraine (2016), Decree "On the decision of the Council of National Security and Defense of Ukraine dated January 27, 2016", Uriadovyjkur'ier, vol. 52.

5. President of Ukraine (2015), Decree "On the decision of the National Security and Defense Council of Ukraine dated May 6, "On the Strategy of National Security of Ukraine", Uriadovyjkur'ier, vol. 95.

6. Dubov, D.V. (2018), Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyj dosvid ta mozhlyvosti dliaUkrainy [Public Private Partnership in Cybersecurity: International Experience and Opportunities for Ukraine: An Analytical Report], the National Institute for Strategic Studies, Kyiv, Ukraine.

7. International Organization for Standardization (2016), "International Standard "ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation", https://www.iso.org/obp/ui/#iso:std:iso-iec:27004:ed-2:v1:en (Accessed 05 Sept 2018).

Стаття надійшла до редакції 07.09.2018 р.