УДК 342.951

АЛЕКСЕЄВА О.А., заступник начальника підрозділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6629-3606.

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ВПРОВАДЖЕННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ СТАНДАРТІВ З УРАХУВАННЯМ МІЖНАРОДНИХ СТАНДАРТІВ З ПИТАНЬ КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ

Анотація. *У статті висвітлено питання правового забезпечення впровадження сучасних інформаційних стандартів з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту. Міститься аналіз міжнародних стандартів з питань кібербезпеки та кіберзахисту. Розглядаються шляхи вироблення і адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами ЄС та НАТО. Висвітлено встановлені чинним законодавством вимоги щодо віднесення об'єктів до об'єктів критичної інфраструктури з урахуванням міжнародних стандартів у цій сфері. Визначено брак підзаконних нормативних актів, спрямованих на забезпечення сумісності інформаційних стандартів зі стандартами НАТО та ЄС. Внесені пропозиції щодо удосконалення правової регламентації впровадження сучасних інформаційних стандартів з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту.*

Ключові слова: *правове забезпечення, кібербезпека, інформаційні стандарти, міжнародні стандарти з питань кібербезпеки, об'єкти критичної інформаційної інфраструктури.*

Summary. *The article highlights the issue of legal support for the implementation of modern information standards, taking into account international standards on cyber security and cyber protection. It contains an analysis of international standards on cyber security and cyber protection. Ways of developing and operational adaptation of state policy in the field of cyber security aimed at the development of cyberspace, achieving compatibility with relevant EU and NATO standards are being considered. The requirements established by the current legislation regarding the classification of objects as critical infrastructure, taking into account international standards in this area, are highlighted. A lack of bylaws aimed at ensuring the compatibility of information standards with NATO and EU standards was identified. Proposals have been made to improve the legal regulation of the implementation of modern information standards, taking into account international standards on cyber security and cyber protection.*

Keywords: *legal support, information standards, cyber security, international standards, objects of critical information infrastructure.*

Постановка проблеми. Сьогодні інформація є важливим ресурсом, охорона якого має суттєве значення. За наявності великого обсягу конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки [1, с. 80-81]. Одним із дієвих способів охорони такої інформації є управління інформаційною безпекою на основі відповідних стандартів інформаційної безпеки [2].

У питаннях розроблення стандартів у сферах нових технологій (зокрема щодо штучного інтелекту, хмарних технологій, квантових обчислень та квантових комунікацій) Україна виходить з того, що Інтернет має залишатися глобальним та відкритим,

технології повинні орієнтуватися на людину, її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження повинні здійснюватися лише відповідно до закону [3].

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" функціонування національної системи кібербезпеки забезпечується шляхом вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО, а також з урахуванням "кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту" [4]. Водночас, проблемою залишається забезпечення такої сумісності, впровадження сучасних інформаційних стандартів в умовах воєнного стану. Одна з причин такого стану справ полягає у недостатній регламентації приписів цього Закону на рівні підзаконних нормативно-правових актів.

Результати аналізу наукових публікацій. Міжнародні стандарти інформаційної безпеки досліджувалися такими вітчизняними і зарубіжними науковцями, як О.В. Дикий, М.О. Флюнт [1], В.М. Брижко, В.Г. Пилипчук [5] Д.С. Бірюков [6], С.Л. Гнатюк [7], А.М. Гуз [18], В.Л. Бурячко, К.І. Бєляков, В.М. Бутузов, В.Д. Гавловський, М.В. Гуцалюк, Д.В. Дубов, В.В. Петров, О.В. Орлов, О.Д. Довгань, В.П. Шеломенцев, та інші. Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України досліджені у відділі інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень [7]. Водночас, євроатлантичні прагнення України однозначно передбачають подальшу гармонізацію законодавства України з правом ЄС, а також забезпечення сумісності державної політики у сфері кібербезпеки з відповідними стандартами Європейського Союзу та НАТО. Під цим кутом зору залишаються недостатньо дослідженими окремі аспекти приведення національних інформаційних стандартів у відповідність до міжнародних стандартів в інформаційній сфері. Проблематика впровадження інформаційних стандартів загострюється в умовах воєнного стану, що зумовлює актуальність цієї статті.

Метою статті є удосконалення правової регламентації впровадження сучасних інформаційних стандартів з урахуванням міжнародних стандартів з питань кібербезпеки й кіберзахисту та кращих світових практик у цій сфері.

Виклад основного матеріалу. Перша спроба сертифікації з інформаційної безпеки відбулася в Стенфордському консорціумі ще в 1990-х роках, коли значна частина завдань, які виконувалися вручну, перейшла на комп'ютер та отримала автоматизацію [7]. Це зумовило потребу створення системи стандартів інформаційної безпеки, яка б гарантувала її ефективність та універсальність [8].

У загальному розумінні стандарти інформаційної безпеки – це стандарти забезпечення захисту, призначені для взаємодії між виробниками, споживачами і експертами з кваліфікації продуктів інформаційних технологій у процесі створення та експлуатації захищених систем оброблення інформації. Загальні (рамкові) стандарти можуть доповнюватись галузевими стандартами (спеціальні вимоги у медичній, авіакосмічній, автомобільній, фінансовій галузях) та стандартами щодо безпечного використання певних технологій (наприклад хмарних обчислень) [9].

Особливим різновидом інформаційних стандартів є міжнародні стандарти кібербезпеки – опубліковані методи, основною метою яких є зниження ризиків, включаючи запобігання або пом'якшення наслідків кібератак [9]. За допомогою цих методів фахівці з кібербезпеки намагаються захистити кібернетичне середовище, яке

охоплює користувачів, мережі, пристрої, інше програмне забезпечення, інформацію, служби та системи, які можуть бути підключені (безпосередньо або опосередковано) до інформаційних мереж. Розроблені та опубліковані стандарти є керівними положеннями під час забезпечення захисту інформації в кіберпросторі [1, с. 81].

Сучасні міжнародні стандарти класифіковано за функціональним призначенням на чотири групи: 1) стандарти для огляду і введення в термінологію; 2) стандарти, які визначають обов'язкові вимоги до системи управління інформаційною безпекою; 3) стандарти, що визначають вимоги і рекомендації для аудиту системи управління інформаційною безпекою; 4) стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення системи управління інформаційною безпекою (далі – СУІБ) [1, с. 81]. Остання є частиною загальної системи управління, яка ґрунтується на підході, котрий враховує бізнес-ризики і призначений для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки (далі – ІБ) [10]. СУІБ охоплює три основні компоненти: конфіденційність, можливість застосування й цілісність. Ці стандарти дозволяють керувати конфіденційністю, захищати систему від несанкціонованого доступу, а також додатково орієнтовані на роботу з персональними даними та криптографічною інформацією з урахуванням підвищеного рівня кібербезпеки [8].

На сучасному етапі розробкою міжнародних стандартів займаються утворена ще в 1947 році Міжнародна організація з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). В сфері інформаційних технологій, ISO та IEC організований спільний технічний комітет (ISO/IEC JTC1), основним завданням якого є підготовка Міжнародних стандартів інформаційної безпеки.

Найбільш поширеним є всесвітньо визнаний стандарт 27001 "Інформаційні технології – Методи і засоби забезпечення безпеки – Система менеджменту інформаційної безпеки – Загальні відомості та словник", який фокусується на системах управління інформаційною безпекою (ISMS). Цей стандарт встановлює набір заходів та процедур для захисту конфіденційності, цілісності та доступності інформації, управління ризиками в контексті клієнтських даних, а також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації [11].

Найбільш значною за обсягом є група стандартів ISO/IEC 27002 (ISO/IEC 17799: 2005) "Інформаційні технології – Технології безпеки – Практичні правила управління інформаційної безпеки". Стандарт надає кращі практичні поради з менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки [8]. Інформаційна безпека визначається цим стандартом як "збереження конфіденційності (впевненості в тому, що інформація доступна тільки тим, хто уповноважений мати такий доступ), цілісності (гарантії точності і повноти інформації, а також методів її обробки) і доступності (гарантії того, що уповноважені користувачі мають доступ до інформації та пов'язаних з нею ресурсів)" [12]. Цей стандарт також призначено для використання в розробленні установчих документів з управління інформаційною безпекою з урахуванням специфічних ризиків інформаційної безпеки [1, с. 83].

Стандарт ISO/IEC 27003 "Інформаційні технології – Технології безпеки – Системи управління інформаційною безпекою. Керівництво" містить керівні вказівки щодо вимог до системи управління інформаційною безпекою (СУІБ) і надає рекомендації, можливості та дозволи щодо них. Метою зазначеного стандарту є надання допомоги під час реалізації СУІБ у межах організації відповідно до ISO/IEC 27001 [13].

Стандарт ISO/IEC 27004 "Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимірювання" є керівництвом для вибору, проектування, управління і поліпшення засобів і методів вимірювання ефективності та результативності системи [14]. Цей стандарт включає політику управління ризиками інформаційної безпеки, цілі контролю, процеси та процедури, підтримку процесу її перегляду, допомогу у визначенні того, чи потрібно змінювати або вдосконалювати будь-який із процесів чи контроль СУІБ. За цим стандартом СУІБ має додаткові ключові компоненти, такі як: 1) оцінка ризику інформаційної безпеки; 2) обробка ризиків інформаційної безпеки, включаючи детермінацію та здійснення контролю. Зрозуміло, що жодне вимірювання контролю не може гарантувати повну інформаційну безпеку [1, с. 83-84].

Група стандартів ISO/IEC 27005 (BS 7799-3: 2006) "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки" (ISO/IEC 27005:2011, IDT) забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації. Зміст цих стандартів допомагає: встановити контекст управління ризиками (наприклад, обсяг, зобов'язання щодо дотримання, підходи/методи, що підлягають використанню, а також відповідні політики та критерії, такі як толерантність або апетит до ризику організації); високоякісно або якісно оцінити (тобто ідентифікувати, аналізувати та оцінювати) відповідні інформаційні ризики, беручи до уваги інформаційні активи, загрози, існуючі контролі та вразливі місця, щоб визначити імовірність сценаріїв інцидентів або інцидентів, а також очікувані комерційні наслідки, якщо вони мали місце, визначити "рівень ризику"; використовувати (наприклад, змінювати елементи інформаційної безпеки), зберігати (приймати), уникати та/або поділяти (з третіми сторонами) ризики відповідно, використовуючи ці "рівні ризику" для визначення їх пріоритету [15].

Незважаючи на те, що це тільки рекомендаційний, а не обов'язковий стандарт, його призначення полягає в тому, що управління ризиками – один з найважливіших процесів для інформаційної безпеки [1, с. 84]. Організація повинна визначити свій підхід до управління ризиками, залежно, наприклад, від сфери застосування СУІБ, контексту управління ризиками чи галузевого сектору [16].

З практичної точки зору вельми важливим є стандарт ISO/IEC 27033, котрий включає в себе декілька частин, з яких найбільш вагомими є ISO/IEC 27033-1 "Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Основні концепції управління мережевою безпекою" та ISO/IEC 27033-3 "Інформаційні технології – Методи забезпечення безпеки – Мережева безпека – Базові мережеві сценарії – загрози, методи проектування та механізми контролю", що має практичне значення [17].

Стандарт ISO/IEC 27035 "Інформаційні технології – Методи забезпечення безпеки – Управління інцидентами безпеки" є одним з цінних стандартів в групі з практичною вартістю в галузі управління інцидентами з інформаційної безпеки, адже стандарт є рекомендацією щодо виявлення, реєстрації та оцінки інформації, випадків порушення безпеки і уразливості [1, с. 85]. Цей стандарт складається з п'яти етапів: планування та підготовка, виявлення та звітування, оцінка та прийняття рішень, реагування, а також навчання та постійне вдосконалення.

Серед стандартів, що визначають вимоги і рекомендації для аудиту СУІБ, виділяються: ISO/IEC 27006 "Інформаційні технології – Методи забезпечення безпеки – Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою", що розширює вимоги стандарту ISO 17021 спеціально для органів, які проводять аудит і

сертифікацію СУІБ; ISO/IEC 27007 “Інформаційні технології – Методи забезпечення безпеки – Керівництво по аудиту – Систем менеджменту інформаційної безпеки”, що пропонує рекомендації з проведення аудитів СУІБ з боку сертифікаційних організацій. Він корисний для аудиторів цих організацій; ISO/IEC TR 27008 “Інформаційні технології – Методи забезпечення безпеки – Керівництво для аудиторів щодо механізмів контролю СУІБ”, що є додатковим стандартом до ISO 19011 спеціально для СУІБ. Він спеціалізований для аудиту коштів управління інформаційною безпекою в організації [7].

На думку фахівців, перевагами застосування Міжнародних стандартів ISO 27000-х є: забезпечення безперервності, мінімізація ризиків, забезпечення комплексного та централізованого контролю рівня захисту інформації, забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів інформаційно-комунікаційних систем та мереж, зниження витрат на інформаційну безпеку [1, с. 84].

Сьогодні в Україні тривають процеси гармонізації та введення в дію сучасних міжнародних стандартів інформаційної безпеки, насамперед – серії міжнародних стандартів ISO/IEC 27000, яка постійно доповнюється новими документами. Впровадження СУІБ відповідно до ISO/IEC 27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів [7].

Крім зазначених стандартів, важливими для кібербезпеки є стандарти захисту від несанкціонованого доступу, серед яких виділяються: ISO/IEC 15408 – міжнародний стандарт, що визначає вимоги до реалізації послуг безпеки та забезпечення гарантій оцінки; FIPS 140 – набір стандартів, який визначає вимоги до криптографічних модулів; CWA 14167 – набір стандартів, який визначає вимоги до криптографічного модуля для послуг генерування ключів провайдером послуг сертифікації; CWA 14170, CWA 14171, CWA 14172 – набір стандартів, який визначає вимоги щодо створення, виготовлення та оцінки відповідності продуктів, систем і застосувань електронного підпису [8].

З наведеного аналізу видно, що стандарти забезпечення інформаційної безпеки на будь-якому об’єкті критичної інфраструктури передбачають: визначення цілей забезпечення інформаційної безпеки комп'ютерних систем; створення ефективної системи управління інформаційною безпекою; розрахунок сукупності деталізованих якісних і кількісних показників для оцінки відповідності інформаційної безпеки поставленим цілям; застосування інструментарію забезпечення інформаційної безпеки і оцінки її поточного стану; використання методик управління безпекою, які дозволяють об'єктивно оцінити захищеність інформаційних активів і управляти інформаційною безпекою компанії [9].

Застосування цих стандартів є обов’язковим для: всіх суб’єктів господарювання, якщо це передбачено в технічних регламентах чи інших нормативно-правових актах; учасників угоди (контракту) щодо розроблення, виготовлення чи постачання продукції, якщо в ній (ньому) є посилання на певні стандарти; виробника чи постачальника продукції, якщо він склав декларацію про відповідність продукції певним стандартам чи застосував позначення цих стандартів у її маркуванні; виробника чи постачальника, якщо його продукція сертифікована щодо дотримання вимог стандартів [18, с. 155].

Стандарти з інформаційної безпеки містять рекомендації з управління інформаційною безпекою, призначені для співробітників, відповідальних за створення, впровадження й підтримку заходів, які забезпечують безпеку державному підприємству або недержавній організації [18, с. 158].

Викладені міжнародні стандарти використовуються з урахуванням норм чинного законодавства. Вони є певним орієнтиром для розроблення та прийняття вітчизняних стандартів, внутрішньодержавних правил та інструкцій.

Національним органом стандартизації є державне підприємство "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" (ДП УкрНДНЦ), яким протягом 2015 – 2018 рр: підготовлено і затверджено у якості національних стандартів України чотири випуски цієї серії (ДСТУ ISO/IEC 27000:2015 "Огляд і словник", 27001:2015 "Вимоги", 27002:2015 "Звід практик щодо заходів інформаційної безпеки", 27005:2015 "Управління ризиками інформаційної безпеки"); оновлено серію національних стандартів ДСТУ ISO/IEC 270XX:2017 щодо методів захисту в системах менеджменту інформаційної безпеки (2017 р.); введено в дію стандарти цієї ж серії "Настанови щодо аудиту систем керування інформаційною безпекою", "Керування інцидентами інформаційної безпеки" і "Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій" (2018 р.) [19].

Також в Україні акредитовано та впроваджено два галузеві міжнародні стандарти: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги" (ISO/IEC 27001:2005, MOD) та ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 "Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою" (ISO/IEC 27002:2005, MOD) [1, с. 85-86].

Таким чином, в Україні база для стандартизації інформаційної безпеки постійно оновлюється і стає дедалі сучаснішою та диверсифікованою, за рахунок чого ситуація в цій галузі загалом розвивається в оптимальному напрямку для стандартизації вимог до об'єктів кіберзахисту [7].

Вимога щодо стандартизації інформаційної та кібернетичної безпеки міститься безпосередньо в нормах чинного законодавства України.

У Стратегії кібербезпеки проголошується, що для досягнення цілі кіберзахисту "Безпечні цифрові послуги" Україна спрямує зусилля на забезпечення надійності та безпеки цифрових послуг шляхом розроблення національних стандартів у сфері кібербезпеки, організаційних та технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів. Для досягнення цієї цілі "Україна буде сприяти подальшому дотриманню міжнародного права та стандартів у сфері прав людини, заохочуватиме застосування найкращих практик, а також активізує свої зусилля щодо запобігання зловживанню новими технологіями" [3]. Як релевантну нинішнім європейським стандартам і практикам у сфері кібербезпеки можна розглядати також закладену в Стратегії кібербезпеки ідею активізувати "участь і партнерство України в міжнародних процесах стандартизації та сертифікації у сфері кібербезпеки, розширити представництво в міжнародних, регіональних та інших органах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією у цій сфері" [3].

В Україні підприємства, установи та організації мають право у відповідних сферах діяльності та з урахуванням своїх господарських і професійних потреб організовувати та виконувати роботи із стандартизації, як це передбачено частиною 1 статті 16 Закону України "Про стандартизацію" [21].

Згідно з частиною другою статті 8 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом,

повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством [22].

Законодавством передбачено особливий режим стандартизації, сертифікації, незалежного аудиту та відповідальності за дотримання вимог інформаційної та кібернетичної безпеки для об'єктів, що належать до національної критичної інформаційної інфраструктури.

Аналіз Закону України "Про основні засади забезпечення кібербезпеки України" свідчить, що для всіх об'єктів критичної інфраструктури передбачене: встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури (п. 3 ч. 3 ст. 8 цього Закону); впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту (п. 13 ч. 3 ст. 8 цього Закону); формування Кабінетом Міністрів України вимог та забезпечення функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (ч. 3 ст. 5 цього Закону); відповідальність власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, а також за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки та організацію проведення незалежного аудиту інформаційної безпеки (ч. 4 ст. 6 цього Закону).

Законом "Про основні засади забезпечення кібербезпеки України" передбачено, що функціонування національної системи кібербезпеки забезпечується шляхом створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО (п. 3 ч. 3 ст. 8 цього Закону).

На жаль, процес створення цієї бази з урахуванням міжнародних стандартів у сфері кібербезпеки залишається незавершеним через брак підзаконних актів. Зокрема, викладені вимоги до об'єктів критичної інфраструктури залишаються не достатньо конкретизованими в нормативно-правових актах, а ті, що вже прийняті на виконання цього Закону, не завжди враховують його вимоги у частині "досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО". Найбільш проблемним і водночас актуальним залишається комплекс питань, пов'язаних з формуванням основи національної критичної інфраструктури, включаючи і методи захисту її об'єктів методології та критеріїв формування реєстру (переліку) об'єктів відповідно до міжнародних стандартів з кібербезпеки.

Зокрема, ст. 6 цього Закону передбачено, що критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, затверджуються Кабінетом Міністрів України.

На виконання зазначеного припису Кабінетом Міністрів України прийнято Постанову "Деякі питання об'єктів критичної інформаційної інфраструктури" від 09.10.20 р. № 943, яка визначає алгоритм ідентифікації оператором основних послуг об'єктів критичної інформаційної інфраструктури, що забезпечують функціонування об'єкта критичної інфраструктури та надання ним основних послуг [23].

Згідно з п. 4 Порядку формування переліку об'єктів критичної інформаційної інфраструктури (далі – Порядок) ідентифікація об'єктів критичної інформаційної інфраструктури проводиться у такому порядку: оператор основних послуг визначає всі об'єкти інформаційної інфраструктури (автоматизовані, інформаційні, електронні комунікаційні, інформаційно-комунікаційні системи, автоматизовані системи управління технологічними процесами), що експлуатуються на об'єкті критичної інфраструктури та проводить оцінку їх критичності [23].

Для оцінки критичності об'єкта інформаційної інфраструктури оператор основних послуг використовує такі три критерії: необхідність об'єкта інформаційної інфраструктури як для стійкого та безперервного функціонування об'єкта критичної інфраструктури, так і для надання ним основних послуг; кібератака, кіберінцидент, інцидент з інформаційної безпеки на об'єкті інформаційної інфраструктури істотно впливає на безперервність та стійкість надання об'єктом критичної інфраструктури основних послуг; у разі порушення безперервності та стійкості надання основних послуг об'єктом інформаційної інфраструктури відсутній альтернативний об'єкт (спосіб) для їх надання (п. 5 Порядку) [23]. Об'єкти інформаційної інфраструктури, що відповідають всім трьом критеріям, визначаються оператором основних послуг як об'єкти критичної інформаційної інфраструктури. При цьому категорія критичності об'єкта критичної інформаційної інфраструктури встановлюється за категорією критичності об'єкта критичної інфраструктури.

Протягом 30 днів з дати визначення об'єкта критичної інформаційної інфраструктури відомості про об'єкти критичної інформаційної інфраструктури уповноваженому органу (центральний орган виконавчої влади, інший державний орган, який забезпечує формування та/або реалізацію державної політики в одній чи кількох сферах), який на їх основі формує секторальний перелік об'єктів критичної інформаційної інфраструктури, а власник об'єкта критичної інформаційної інфраструктури, що внесений до національного переліку, вживає першочергових заходів із захисту такого об'єкта від кібератак (п. 6, 15 Порядку) [23].

Одним з методологічних недоліків цього Порядку є відсутність будь-якого масштабування "негативного впливу" на інформаційно-телекомунікаційну систему того чи іншого об'єкта (наприклад – тривалість, територіальне охоплення, орієнтовний розмір збитків, ступінь загрози для національної безпеки тощо), а також – відповідно до цього масштабування – шкали її належності/неналежності до критичної інфраструктури [7].

Як вбачається зі змісту п. 8 Порядку, таку оцінку належності/неналежності до критичної інфраструктури дає тільки уповноважений орган, який розглядає надані відомості про об'єкти критичної інформаційної інфраструктури та у разі потреби надає зауваження та рекомендації щодо коректності та/або повноти наданих відомостей.

На думку фахівців, такий процес був би значно продуктивнішим, якби у ньому, поряд з профільними фахівцями, була також передбачена системна участь спеціалістів у сфері національної безпеки, а процедура створення першого національного реєстру об'єктів критичної інфраструктури, мабуть, вимагає більш широких комунікацій та консультацій – у тому числі з приватним сектором [7]. Такий підхід випливає зі змісту

Стратегії кібербезпеки, яка передбачає формування ефективної моделі відносин у сфері кібербезпеки, заснованої на довірі, шляхом залучення на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення проектів нормативно-правових актів, нормативних документів та стандартів у цій сфері [3]. Аналогічний підхід міститься у ч. 3 ст. 6 Закону України "Про основні засади забезпечення кібербезпеки України", відповідно до якої розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій [4].

Слід зауважити, що ідентифікація, категоризація і реєстрація об'єктів критичної інфраструктури є складною проблемою не лише в Україні, але і в інших державах, при чому в різних країнах вирішується вона дуже по-різному.

План заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки, затверджений Розпорядженням Кабінету Міністрів України від 19.12.23 р. № 1163, передбачає:

забезпечення проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав-членів НАТО для досягнення оперативної сумісності (ціль С. 1, пункт 5);

завершення процесів визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, створення та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури, постійний перегляд та оновлення вимог до їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки (ціль К. 1, пункт 45) [24].

У контексті реалізації цих заходів Стратегії кібербезпеки вкрай важливою є:

участь працівників основних суб'єктів національної системи кібербезпеки у спільних тематичних навчаннях з відповідними підрозділами країн-членів НАТО для досягнення оперативної сумісності;

проведення переговорів та консультацій з партнерами з метою підвищення рівня професійної компетентності кіберфахівців основних суб'єктів національної системи кібербезпеки за стандартами освіти НАТО.

Висновки.

Національна система кібербезпеки України нині знаходиться на етапі формування, у тому числі, у частині стандартизації та сертифікації, що зумовлює оновлення її нормативно-правового забезпечення на рівні підзаконних актів з урахуванням сучасних міжнародних стандартів з питань кібербезпеки.

З метою реалізації вимог Закону України "Про основні засади забезпечення кібербезпеки України" потребують оновлення з урахуванням сучасних міжнародних стандартів з питань кібербезпеки:

вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури;

підзаконні нормативно-правові акти з питань захисту об'єктів критичної інфраструктури, зокрема, їх ідентифікації, реєстрації та категоризації.

В аспекті правового захисту об'єктів критичної інфраструктури потребує вивчення міжнародний досвід з питань кібербезпеки, рекомендації, розроблені NIST, Міжнародною організацією зі стандартизації на предмет можливості їх застосування в українських умовах [7].

Враховуючи наявність такого досвіду і загальну зорієнтованість українського законодавства на міжнародні стандарти у сфері кібербезпеки було б доцільним:

провести в контексті розробки національних індикаторів кібербезпеки процедуру гармонізації або підтвердження відповідних стандартів ДП УкрНДНЦ, офіційно ввести в їх дію з посиланням на норми та спеціальні рекомендації, розроблені NIST, а також Міжнародною організацією зі стандартизації [7];

розширити представництво України в міжнародних, регіональних та інших органах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією у цій сфері, як це передбачено Стратегією кібербезпеки України.

Використана література

1. Дикий О.В., Флюнт М.О. Стандарти інформаційної безпеки: компаративне дослідження. *Право та державне управління*. 2019. № 2 (35). Т. 1. С. 80-87. URL: http://www.pdu-journal.kpu.zp.ua/archive/2_2019/tom_1/16.pdf

2. Стандарти інформаційної безпеки: огляд. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/standarti-informacijnoyi-bezpeki-oglyad

3. Стратегія кібербезпеки безпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради.*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua.laws/show/2163-19#Text

5. Брижко В.М., Пилипчук В.Г. Безпека персональних даних: правові стандарти Європейського Союзу та сучасні прикладні проблеми. *Інформація і право*. № 1(36)/2021. С. 17-28.

6. Бірюков Д.С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. *Науково-інформаційний вісник Академії національної безпеки*. 2015. № 3 – 4. С. 155-170.

7. Гнатюк С.Л. Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України: аналітична записка. – (Відділ інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень). 2018. 18 с. URL: iss.gov.ua/sites/default/files/2018-06/1_cPPP-standarts_27-04_Gn_var_FIN-732b6.pdf

8. Стандарти інформаційної безпеки. URL: https://uk.wikipedia.org/wiki

9. Міжнародні стандарти інформаційної безпеки. URL: https://informationse.curity.palamarchuk.blogspot.com/2021/01/blog-post_13.html

10. Стандарти ISO/IEC захистять від кіберзагроз. URL: http://csm.kiev.ua/index.php?option=com_content& view=article&id=3631%3A-isoiec-&ca tid=122%3A2015-09-15-07-01-23&lang= uk

11. ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. https://www.iso.org/standard/27001.

12. ISO/IEC 27002. URL: https://uk.wikipedia.org/wiki/ISO/IEC_27002

13. ISO/IEC 27003. URL: https://uk.wikipedia.org/wiki/ISO/IEC_27003

14. ISO/IEC 27004:2016. URL: https://www.iso.org/ru/standard/64120.html

15. ISO/IEC 27005. URL: https://uk.wikipedia.org/wiki/ISO/IEC_27005

16. ISO/IEC 27004:2009(E). URL: http:// www.klubok.net/Downloads-index-reqviewdownloaddetails-lid-425.html

17. Вашему бизнесу угрожают хакеры? Стандарт ISO/IEC 27031:2011 предлагает решения. URL: http://www.klubok.net/article3.html

18. Гуз А.М. Становлення та розвиток світових стандартів інформаційної безпеки. *Науковий часопис імені М.П. Драгоманова. Серія "Право"*. 2013. Вип. 21. С. 154-159. URL: https:// enpuir.npu.edu.ua/bitstream/handle/123456789/23381/Guz.pdf?sequence =1&isAllowed=y

19. Про прийняття нормативних документів України, гармонізованих з міжнародними та європейськими нормативними документами, скасування національних стандартів України: наказ ДП УкрНДНЦ від 18.12.15 р. № 193 URL: https://zakon.rada.gov.ua/rada/show/v0193774-15#Text

20. Про прийняття національних нормативних документів, гармонізованих з європейськими нормативними документами, поправки до національного нормативного документа, скасування національних нормативних документів: наказ ДП УкрНДНЦ від 04.08.17 р. № 207. URL: https://zakononline.com.ua/documents/show/82395_82395

21. Про стандартизацію: Закон України від 05.06.14 р. № 1315-VII. URL: https://zakon.rada.gov.ua/laws/show/1315-18#Text

22. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.94 р. № 80. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

23. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.20 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

24. План заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки: Розпорядження Кабінету Міністрів України від 19.12.23 р. № 1163. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text

* * *