Соціально-правові студії. 2020. Випуск 3 (9). С. 18-25
Social & Legal Studios. 2020. Issue 3 (9). P. 18-25

UDC (УДК) 004.056.53:351.746.2
JEL Classification: K 30

Живко Зінаїда Богданівна,
доктор економічних наук, професор,
професор кафедри менеджменту
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: professor2007@ukr.net
ORCID ID: 0000-0002-4045-669X

Рудий Тарас Володимирович,
кандидат технічних наук, доцент,
доцент кафедри інформаційного та аналітичного забезпечення
діяльності правоохоронних органів
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: tarasrudyy@gmail.com
ORCID ID: 0000-0002-4106-4313

Сеник Володимир Васильович,
кандидат технічних наук, доцент,
завідувач кафедри інформаційного та аналітичного забезпечення
діяльності правоохоронних органів
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: v.v.senyk@gmail.com
ORCID ID: 0000-0002-0428-6443

Родченко Світлана Сергіївна,
кандидат економічних наук,
старший викладач кафедри
фінансово-економічної безпеки, обліку і аудиту
Харківського національного університету міського господарства
імені О. М. Бекетова
(Харків, Україна)
e-mail: svrodchenko@gmail.com
ORCID ID: 0000-0002-8611-2796

ПРОБЛЕМИ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ: СТАН І ПЕРСПЕКТИВИ

Анотація. Проаналізовано сучасний стан забезпечення кібербезпеки в Україні, акцентовано на основних аспектах нормативно-правового забезпечення інформаційної безпеки держави. Встановлено основні задекларовані заходи протидії загрозам інформаційній безпеці держави загалом та за окремими її видами. Зазначено про відсутність практичного виконання цих заходів.

Визначено основні проблеми у забезпеченні кібербезпеки: неефективність нормативно-правової бази та системи управління; відсутність єдиної стратегії кіберзахисту; незадовільний рівень державного управління у сфері кіберзахисту; відсутність трансформаційного підходу до управління національною кібербезпекою з боку держави; розмитість вимог до систем захисту інформації; використання застарілих стандартів.

Ключові поняття: кібербезпека, інформаційна безпека держави, нормативно-правове забезпечення, кіберзахист.

Zhyvko Zinaida,
Doctor of Economic, Professor,
Professor of the Department of Management,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: professor2007@ukr.net
ORCID ID: 0000-0002-4045-669X

Rudyi Taras,
PhD (Technical), Associate Professor,
Associate Professor of the Department of
Information and Analytical Support of Law Enforcement Agencies activity,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: tarasrudyy@gmail.com
ORCID ID: 0000-0002-4106-4313

Senyk Volodymyr,
PhD (Technical), Associate Professor,
Head of the Department of
Information and Analytical Support of Law Enforcement Agencies activity,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: v.v.senyk@gmail.com
ORCID ID: 0000-0002-0428-6443
(Lviv, Ukraine)

Rodchenko Svitlana,
PhD (Economics), Senior Lecturer of the Department of
Financial and Economic Security, Accounting and Audit,
O. M. Beketov National University of Urban Economy
(Kharkiv, Ukraine)
e-mail: svrodchenko@gmail.com
ORCID ID: 0000-0002-8611-2796

PROBLEMS OF THE LEGAL FRAMEWORK FOR PROVIDING CYBER SECURITY IN UKRAINE: CURRENT SITUATION AND PROSPECTS

Abstract. The lack of comprehensible legal and regulatory instruments ensuring cyber security of Ukraine and protecting the information space of the State, systematic, effective and efficient responses to cyber threats require further research on the subject.

The mentioned problems cannot be solved without the introduction of modern laws, regulations and new State policy in the sphere of digital security.

The aim of the study, on the basis of the mentioned problems, is to analyze the reasons for the inadequate providing of cyber security of the State in general and the problems of the inefficiency of the regulatory framework in particular.

The authors' idea of strengthening the response to cybercrime, including its organized forms, updates the processing and public discussion of amendments and additions to existing legislation, in particular the expansion of chapter XVI of the Criminal Code of Ukraine "Crimes in the sphere of electronic computers (computers), systems and computer networks".

The vulnerability of Ukraine's cyberspace stems from the absence of a single unified cyber security strategy, which requires the transformation of the State governance in the area of cyber security. All these initiatives should form a single programme for transforming cyber security. This approach is based on the development of the legal system for cyber security in Ukraine, which should be implemented in the legal and regulatory framework.

In contrast to ISO / IEC 27000 series, which focuse on information security management, the security criterion of RD TSI 2.5-004-99, which isn't corresponding to current requirements, has accordance with the architecture and parameters of the software and hardware of IS regulation - the integrated comprehensive information security system (CISS).

On distinction to CISS, the organizational and legal structure of IS system should harmonize and implement modern international standards, primarily the ISO/IEC 27000 series of international standards.

A separate problem area is audits of IS systems. In the RD TSI coordinate system, only state-accredited organizations are allowed to conduct audits.

International certificates on information security and IT-audit aren't currently recognized, which negatively affects to the audit quality.

Key concepts: cyber security, State information security, regulation, cyber threats, computer systems, certification, security management, strategy of cyber security, security information system(SIS), information security management system (ISMS).

DOI 10.32518/2617-4162-2020-3-18-25

Вступ

Шлях України у розбудові власної кібербезпеки потребує докорінних і невідкладних змін. Це не лише позиція лідерів вітчизняного кіберзахисту. Необхідність змін підтверджена атаками на об'єкти критичної інфраструктури, багатьма іншими інцидентами, які створили Україні сумнівну репутацію одного з головних кіберполігонів [1].

Законодавча база – важлива складова у забезпеченні інформаційної безпеки (ІБ) та кібербезпеки держави, однак, ураховуючи основні недоліки чинного законодавства у безпековій сфері, його пасивний характер, декларування теоретичних аспектів забезпечення ІБ, безпеки кіберпростору та протидії кіберзлочинності на рівні доктрин, указів, рішень тощо, потрібно розробити механізм практичного впровадження захисту інформації в кіберпросторі. Тобто задається «напрям», якого необхідно дотримуватися за відсутності правового, фінансового та кадрового забезпечення і без жодної відповідальності посадових осіб [2].

Безпека інформаційного і кіберпростору, запровадження диджиталізації процесів управління, гарантування безпеки й сталого функціонування національної критичної інфраструктури, інформаційних систем (ІС) повинні стати не тільки складовими державної політики у сфері розвитку кіберпростору та становлення інформаційного суспільства в Україні, а також включення цих чинників у сферу політичних пріоритетів держави [3].

Вагомий внесок у розв'язання згаданих проблем на теоретичному рівні зробили такі науковці: В. Л. Бурячок, В. О. Хорошко, В. Б. Толубко, А. І. Марущак, М. В. Гуцалюк, К. В. Пестов, В. В. Кравчук. Особливостям організаційно-правового забезпечення протидії кіберзлочинності присвячено праці В. А. Ліпкана, Б. Д. Леонова, В. С. Серьогіна, О. Д. Довганя, Т. Ю. Ткачука, В. С. Демедюка, І. В. Красницького.

З огляду на результати аналізу літературних джерел чітких і зрозумілих нормативно-правових документів та організаційно-правових заходів щодо забезпечення національної системи кібербезпеки, констатуємо, що захист інформаційного простору держави незадовільний. Поділяємо думку д. т. н., проф. Ю. І. Грицюка, що наразі відсутні ефективні та дієві заходи запобігання та протидії кіберзагрозам, а наявні є несистемними, не конкретизованим, відтак – марними. Ці чинники зумовлюють потребу подальших досліджень цієї тематики.

Більшість публікацій стосуються авторського розуміння проблем у системі кібербезпеки, які не можуть бути вирішені без упровадження нових законодавчих, нормативно-правових актів і нової політики держави у сфері безпеки цифрового простору, тобто без розгляду інформаційних відносин із пункту бачення об'єкта правового регулювання [3].

Метою цієї публікації є аналіз причин незадовільного забезпечення інформаційної і кібербезпеки держави взагалі та проблем неефективності нормативно-правової бази зокрема, низки системних проблем у галузі кібербезпеки, ігнорувати які дедалі важче.

Тобто однією з головних проблем залишається неефективна нормативна база та, найголовніше, – відсутнє регламентування системи менеджменту у сфері нормативно-правового забезпечення інформаційних відносин, що повинно забезпечувати динаміку процесів правового забезпечення інформаційної і кібербезпеки в Україні [4].

Таке становище має зумовити глибинні зміни у ставленні нашої держави до безпеки власного інформаційного та кіберпростору, а отже, і до захисту інформації (ЗІ), засобів її оброблення та кіберсередовища, в якому ця інформація циркулює, визначення об'єктів впливу, тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки.

1. Неефективна нормативно-правова база та система управління

На міжнародному і національному рівнях кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед правоохоронними органами усіх держав. Досі не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці [5].

У національній системі права першими та єдиними законодавчими актами у сфері протидії кіберзлочинності, як стратегічної позиції на найвищому політичному рівні, є Закон України «Про основні засади забезпечення кібербезпеки України» та Указ Президента України № 47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Вони законодавчо закріпили кібербезпеку як пріоритет роботи для державних органів і уряду.

Підпунктом 2 пункту 3 статті 8 Закону визначено, що функціонування національної системи кібербезпеки забезпечується шляхом створення нормативно-правової і 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 і НАТО [4].

Неоправданими виявилися очікування, що ці документи стануть основою для розроблення в короткостроковій перспективі ефективної, сучасної нормативно-правової бази, низки інших нормативно-правових актів, які повинні виконувати ключову роль у забезпеченні інформаційної і кібербезпеки в Україні. Проте, зважаючи на продовження агресії РФ, прихід нового уряду, зрушень у сфері забезпечення кібербезпеки, на превеликий жаль, немає.

У чинному законодавстві України ще досі немає наукового обґрунтування концептуальних визначень і формулювань стосовно інформаційних відносин. До тепер немає законодавчого визначення такого базового терміна, як «безпека інформації», хоча таке термінологічне сполучення вживається. Термінологія, що застосовується у сфері інформаційних технологій (ІТ), демонструє брак єдності, неоднозначні тлумачення багатьох понять, зокрема ключових (це стосується і Розділу XVI Кримінального кодексу України, за якими розслідуються кіберзлочини в Україні). Це створює поважні перешкоди як для правотворчої діяльності в інформаційній сфері, так і для правозастосовної, а також зайвий раз засвідчує відсутність системності у розв'язанні вказаних проблем [6].

Законом України «Про основні засади забезпечення кібербезпеки України» визначено термін «кіберзлочин». Цей термін зовсім не узгоджений із Кримінальним кодексом України (ККУ), який містить окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», де використовується термін «комп'ютерний злочин».

Доречно зазначити, що завдяки поширенню так званих «комунікаторів» і «смартфонів», які поєднують властивості мобільних телефонів і комп'ютерів, кіберзлочинність набула значного розвитку, сутність якої охоплює весь спектр суспільно небезпечних діянь у сфері використання ІТ [4]. Закріплені нормативні визначення обчислювальної машини та електронної обчислювальної машини не дозволяють тлумачити сучасні терміни і поняття сфери ІТ, які відповідають їх фізичному змісту, або тлумачити їх надто обмежено.

Поділяємо ідею, викладену в [7], щодо посилення протидії кіберзлочинності, зокрема її організованим формам, яка передбачає: враховуючи тяжкі наслідки, які можуть бути завдані вчиненням кіберзлочинів, ініціювати питання щодо посилення санкцій за вчинення злочинів, передбачених статтями 361, 361-1, 361-2, 362, 363, 363-1 ККУ, доповнивши ці статті відповідними частинами. Це дасть змогу перевести їх у розряд тяжких злочинів, що посилить кримінальну відповідальність за їх учинення, а також розширить перелік негласних слідчих (розшукових) заходів, що можуть бути проведені для їх припинення або документування; посилити державно-приватне партнерство у протидії кіберзлочинності, зокрема у підготовці нормативно-правових документів у цій сфері.

Тобто нині актуальне питання щодо опрацювання та публічного обговорення проблеми внесення змін і доповнень до кримінального і адміністративного законодавства, зокрема розширення Розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» ККУ [6].

В Україні, на жаль, немає офіційної державної статистики, яка б об'єктивно відображала відомості про кіберзлочини на основі методів кримінального аналізу (звітність про вчинення кіберзлочинів розпорошена серед різних підрозділів правоохоронних органів). Це негативно впливає на запобіжні заходи, які мають фрагментарний характер, зумовлю-

ючи труднощі у протидії та боротьбі з таким видом суспільно небезпечних діянь [4]. Це безпосередньо зачіпає сферу менеджменту у розробленні і супроводі нормативно-правового забезпечення протидії кіберзлочинності та забезпеченні інформаційної безпеки (ІБ).

Однак, необхідно враховувати, що важливою особливістю функціонування інформаційного простору держави є його висока динамічність і мінливість загроз кібербезпеці. Це обумовлює неможливість створення ефективного організаційно-правового забезпечення у сфері ІБ на період більший, ніж 3–5 років, а реально – до двох років. Тому, щонайменше, щодва роки чинне законодавство у цій сфері потребує корегування відповідно до нових викликів і загроз, а також змін у геополітичному безпековому середовищі, що у нашій державі просто ігнорується.

Отже, однією з головних проблем залишається неефективна нормативно-правова база та, найголовніше, – відсутнє регламентування системи менеджменту у сфері нормативно-правового забезпечення інформаційних відносин, що повинно забезпечувати динаміку процесів правового забезпечення інформаційної і кібербезпеки в Україні.

Необхідно враховувати і те, що розвиток ІТ, систем телекомунікацій відбувається швидше, ніж приймаються нормативно-правові акти, якими вони регулюються.

2. Трансформація державного управління у сфері кібербезпеки

Кіберпростір України є дуже вразливим, бо не існує єдиної об'єднаної стратегії кіберзахисту. Основні завдання в сфері кіберзахисту, які повинні формуватися і реалізовуватися на державному рівні, полягають у такому:

– захисті суверенітету кіберпростору та забезпеченні базової кібербезпеки;

– захисті об'єктів критичної інфраструктури;

– розвитку і запровадженні диджиталізації процесів державного управління та on-line культури;

– протидії кіберзлочинності, шпигунству і тероризму;

– розвитку кіберменеджменту;

– зміцненні міжнародного співробітництва шляхом імплементації у національне законодавство окремих норм нормативно-правових актів, прийнятих в країнах ЄС та НАТО у сфері захисту інформації, які на державному рівні визнаються усіма країнами.

Усі ініціативи з кібербезпеки мають бути сформовані в єдину програму трансформації кібербезпеки. Такий підхід утверджено у розвитку системи права для сфери кібербезпеки в Україні, яка повинна реалізуватися у нормативно-правовому супроводі нинішніх процесів та очікувань.

Щоби система кібербезпеки почала працювати на мінімально необхідному рівні, потрібно внести зміни у чинне законодавство, зокрема закони України «Про захист інформації» та «Про основні засади кібербезпеки».

Регулятори в Україні явно запізнюються з розробленням правової бази для регулювання питань захищеності об'єктів критичної інфраструктури, а також із наповненням змістом і підзаконними актами рамкових законів щодо кіберзахисту та кібербезпеки. На часі розроблення та прийняття низки нормативних документів, зокрема [8]:

– вимог до кіберзахисту об'єктів критичної інфраструктури та оцінка кіберзагроз;

– порядку аудіювання інформаційної безпеки.

Роль держави у розбудові вітчизняної системи кіберзахисту також потребує трансформації. Очевидно, це має бути не функція контролю (як зараз), а більше фасилітації (організація процесу колективного розв'язання проблем) і допомоги у вирішенні проблем кібербезпеки державним і недержавним структурам [8].

Загалом управління кібербезпекою в Україні на державному рівні важко назвати ефективним. Національна система кібербезпеки обмежується переважно участю в ній правоохоронних органів. Приватний бізнес і кіберспільнота до розв'язання важливих питань майже не залучаються.

Як зазначено, немає трансформаційного підходу до управління національною кібербезпекою з боку держави, що передбачає наявність організації, яка візьме на себе функції управління впровадженням програми з кібербезпеки та регулярного контролю за процесом упровадження. Тобто функції регулярного контролю за виконанням програми повинні належати неурядовій структурі, уповноваженій впроваджувати реформи у сфері кібербезпеки.

Державні структури, обмежені поточними вимогами законодавства та нормативних документів, не зможуть провести таку трансформацію.

Окрім того, вкрай небажаним і, можливо, буде шкідливим, якщо держава обере шлях, коли для впровадження відповідних вимог щодо кіберзахисту необхідно буде здійснювати затвердження проекту технічних умов у державній інституції. Другим негативним сценарієм у цьому процесі може стати відсилання для сертифікування до процедур безнадійно застарілих комплексних систем захисту інформації (КСЗІ) [8].

3. Проблеми сертифікування систем захисту інформації

Спробуємо пояснити ситуацію. В Україні чинний Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» і розроблено серію нормативних документів системи технічного захисту інформації (ТЗІ), основним із яких є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації комп'ютерних систем від несанкціонованого доступу». Цей документ використовується у проектуванні та створенні КСЗІ державних інформаційних ресурсів, а також спеціалізованих ІС, в яких обробляється інформація з обмеженим доступом, вимога щодо захисту якої визначено законом.

Зараз через брак підзаконних актів вимоги до систем захисту спеціалізованих ІС практично не конкретизовані. Чинною сьогодні є і норма Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (ст. 7), відповідно до положень якого 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.

Тобто під дію цієї норми потрапляють усі системи ЗІ у ІС, їх інформаційна інфраструктура, що вимагає дотримуватись вимог старого стандарту КСЗІ НД ТЗІ 2.5-004-99.

Концепція, внутрішня структура і модель упровадження КСЗІ не відповідають сучасним вимогам до забезпечення ІБ і те, що ця норма досі не вилучена з чинного законодавства, зазнає гострої критики [3]. Це відповідає чинному законодавству, але є дуже суперечливим підходом з урахуванням фундаментальних недоліків і застарілості концептуальної ідеї КСЗІ. Крім того, вони зобов'язують органи державної влади, об'єкти критичної інфраструктури та приватні компанії, які хочуть надавати послуги державним органам (скажімо, інтернет-провайдери), впроваджувати КСЗІ. Вона, окрім того, що морально застаріла, впродовж багатьох років довела свою неефективність [9].

Найнагальнішим кроком є заміна НД ТЗІ більш ефективним і сучасним базовим стандартом і запровадження галузевих стандартів систем ЗІ.

Ця пропозиція не є новою і креативною. Є низка міжнародних стандартів, які зарекомендували себе у розвинених країнах світу та пройшли перевірку часом. Тобто потрібен перехід на міжнародні стандарти безпеки, зокрема галузеві.

Для цього необхідно або адаптувати сучасні міжнародні стандарти систем ЗІ, або розробити та впровадити власні, якісно нові стандарти безпеки для правоохоронних органів, недержавних структур, що є неприйнятним з часових обмежень і матеріальних витрат.

На відміну від найпоширенішої у світі серії стандартів ISO/IEC 27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5-004-99 є відповідність архітектури та параметрів програмно-апаратних засобів ІС регламенту – КСЗІ.

На противагу КСЗІ в організаційно-правову структуру системи ЗІ повинні гармонізуватися та впроваджуватися в дію сучасні міжнародні стандарти, насамперед – серія міжнародних стандартів ISO/IEC 27000.

Необхідно внести зміни до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» і передбачити новий підхід до реалізації способу підтвердження відповідності ІС вимогам із ЗІ шляхом установлення відповідних критеріїв. Мета такого заходу полягає у прийнятті на території України вимог сімейства стандартів систем менеджменту інформаційною безпекою (СМІБ) для окремих категорій інформації, захист якої забезпечується законодавством України.

Сертифікація за стандартами також вимагає проведення регулярних аудиторських перевірок із метою забезпечення відповідності виконання вимог та належного функціонування процесу управління безпекою. Це скорочує розрив, який є зараз між різними нормативними актами та законодавством, допомагає переконати регулюючі органи, що організація постійно дотримується вимог законодавства.

Сертифікацію за стандартом серії ISO/IEC 270XX проводять органи сертифікування, які акредитовані національними організаціями з акредитації. В Україні такою державною організацією є Національне агентство з акредитації України (НААУ).

Відповідно до п. 2 ч. 2 ст. 11 Закону України «Про стандартизацію», розпорядження Кабінету Міністрів України від 26.11.2014 № 1163-р «Про визначення державного підприємства, яке виконує функції національного органу стандартизації» та на виконання Програми робіт з національної стандартизації на 2019 рік прийняті національні стандарти, гармонізовані є європейськими та міжнародними стандартами, методом підтвердження з наданням чинності з 01 листопада 2019 року (див. табл.).

Ще один проблемний сегмент – аудит систем ЗІ. У системі координат НД ТЗІ дозвіл на проведення аудиту мають лише акредитовані державою організації. Міжнародні сертифікати

Таблиця

Державні стандарти України для сертифікування систем захисту інформації

1.	ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT)	Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів – на заміну ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
2.	ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) / Поправка N 2:2019 (ISO/IEC 27001:2013/Cor 2:2015, IDT)	Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги
3.	ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT)/ Поправка N 2:2019 ISO/IEC 27002:2013/Cor 2:2015, IDT)	Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки
4.	ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT)	Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки – на заміну ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT)
5.	ДСТУ ISO/IEC 27008:2019 (ISO/IEC TS 27008:2019, IDT)	Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки (Настанова для аудиторів) – на заміну ДСТУ ISO/IEC TR 27008:2018 (ISO/IEC TR 27008:2011, IDT)
6.	ДСТУ ISO/IEC 27011:2018 (ISO/IEC 27011:2016, IDT) / Поправка N 1:2019 (ISO/IEC 27011:2016/Cor 1:2018, IDT)	Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування

* Згруповано авторами.

з ІБ та ІТ-аудиту наразі не визнаються, що негативно впливає на якість аудиту.

Тому для дотримання законодавства України у сфері ІБ доцільним є запровадити і, у подальшому пройшовши попередній аудит третьою стороною, сертифікувати СМІБ відповідно до вимог ISO/IEC 27001. Оскільки власне цей стандарт охоплює найкращі світові практики і методики, використовується і визнається у світі, його впровадження є запорукою системності, підтримання процесів у актуальному ефективному стані.

Висновки

1. Вважаємо, що наявна нормативно-правова база, яка, крім іншого, не охоплює всього спектра сучасних загроз кібернетичній безпеці держави, повинна бути істотно доповненою. На організаційно-правовому рівні необхідно чітко ідентифікувати проблему забезпечення кібербезпеки та своєчасно надавати нові, сучасні правові інструменти для протидії цим загрозам.

2. Пропонуємо внести зміни до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» і передбачити новий підхід до реалізації способу підтвердження відповідності інформаційної системи вимогам із захисту інформації шляхом установлення відповідних критеріїв. Мета такого заходу полягає у законодавчому закріпленні вимог стандартів сімейства систем менеджменту інформаційною безпекою для окремих категорій інформації, захист якої забезпечується законодавством України.

Список використаних джерел

1. Янковський О. Україні потрібна нова кіберстратегія. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/
2. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби з кіберзлочинністю: основні напрями реформування. Аналітична записка. Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/454/
3. Рудий Т. В., Сеник В. В., Рудий А. Т., Сеник С. В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична* / гол. ред. Р. І. Благута. Львів : ЛьвДУВС, 2018. Вип. 1. С. 283–301.
4. Леонов Б. Д., Серьогін В. С. Проблеми правового та експертного забезпечення правоохоронної діяльності у сфері протидії кіберзлочинності. URL: http://academy.ssu.gov.ua/ua/page/page_1581430420.htm

5. Костенко О. В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі. *Інформація і право.* Науково-дослідний інститут інформатики і права Національної академії правових наук України. Київ, 2019. № 3 (30). С. 96–104.
6. Тарасюк А. В. Співвідношення інформаційної та кібернетичної безпеки. *Інформація і право.* 2019. № 4 (31). С. 73–82.
7. Гуцалюк М. В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право.* Науково-дослідний інститут інформатики і права Національної академії правових наук України. Київ, 2019. № 1 (28). С. 118–128.
8. Котляров Ю. Архітектура права сфери кібербезпеки в Україні. URL: https://www.pressreader.com/ukraine/yurydychna-gazeta/20180515/
9. Довгань О. Д., Ткачук Т. Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. Науково-дослідний інститут інформатики і права Національної академії правових наук України. 2019. № 1 (28). С. 86–99.

References

1. Yankovskyy, O. (2019). Ukrayini potribna nova kiberstratehiya [Ukraine needs a new Cyber Strategy]. Retrieved from https://www.pravda.com.ua/columns/ 2019/09/14/7226291/ [in Ukr.].
2. Problem chynnoji vittsyznianoji normatyvno-pravovoji bazy u sferi borotby z kiberzlochynnistiu: osnovni napriamy reformuvannia. Analitychna zapyska. Natsionalnyj instytut strahichnyh dislidzhen [Problems of the Current Domestic legal Framework in the fight against Cybercrime: the main Directions of Reform. Analytical note. National Institute for Strategic Studies]. Retrieved from http://www.niss.gov.ua/ articles/454/ [in Ukr.].
3. Rudyy, T. V., Senyk, V. V., Rudyj, A. T., & Senyk, S. V. (2018). Organizatsijno-pravovi, kryminalistychni ta tehnichni aspekty protydiji kiberzlochynnosti v Ukrajini [Organizational, legal, forensic and technical Aspects of Combating Cybercrime in Ukraine]. *Naukovyj visnyk Lvivskoho derzgavnoho universytetu vnutrishnih sprav: Serija jurydychna (Scientific Bulletin of Lviv State University of Internal Affairs. The series is legal),* 1. Lviv: LvDUVS [in Ukr.].
4. Leonov, B. D., & Seriohin, V. S. Problemy pravovoho ta ekspertnoho zabezpechennia pravoohoronnoji dijalnosti u sferi protydiji kiberzlochynnosti [Problems of legal and expert support of law enforcement in the field of combating cybercrime]. Retrieved from http://academy.ssu.gov.ua/ua/page/page_1581430420.htm [in Ukr.].
5. Kostenko, O. V. (2019). Problemy pravovoho rehuliuvannia ta rozvytok kibernetychnoji bezpeky Ukrajiny na suchasnomu etapi [Problems of legal regulation and development of cyber security of Ukraine at the present stage]. *Informatsija i pravo (Information and Law).* Naukovo-doslidnyj instytut informatyky i prava natsionalnoji akademiji pravovyh nauk Ukrajiny. Kyjiv, 3 (30), 96–104 [in Ukr.].
6. Tarasiuk, A. V. (2019). Spivvidnoshennia informatsijnoji ta kibernetychnoji bezpeky [The ratio of information and cyber security]. *Informatsija i pravo (Information and Law).* Naukovo-doslidnyj instytut informatyky i prava natsionalnoji akademiji pravovyh nauk Ukrajiny. Kyjiv, 4 (31), 73–82 [in Ukr.].
7. Hutsaliuk, M. V. (2019). Suchasni tendentsiji organizovanoji kiberzlochynnosti [Current trends in organized cybercrime]. *Informatsija i pravo (Information and Law).* Naukovo-doslidnyj instytut informatyky i prava natsionalnoji akademiji pravovyh nauk Ukrajiny. Kyjiv, 1 (28), 118–128 [in Ukr.].
8. Kotliarov, Yu. Arhitektura prava sfery kiberbezpeky v Ukrajini [Architecture of cybersecurity law in Ukraine]. Retrieved from https://www.pressreader.com/ukraine/yurydychna-gazeta/20180515/ [in Ukr.].
9. Dovhan, O. D., & Tkachuk, T. Y. Kontseptualni zasady zakonodavchoho zabezpechennia informatsijnoji bezpeky Ukrajiny [Conceptual bases of legislative maintenance of information security of Ukraine]. *Informatsija i pravo (Information and Law).* Naukovo-doslidnyj instytut informatyky i prava natsionalnoji akademiji pravovyh nauk Ukrajiny. Kyjiv, 1 (28), 86–99 [in Ukr.].

Стаття: надійшла до редакції 17.07.2020
прийнята до друку 10.09.2020

The article: is received 17.07.2020
is accepted 10.09.2020