УДК 347.83:34:002.1
DOI https://doi.org/10.32849/2663-5313/2019.9.17

Ольга Бакалінська,
докт. юрид. наук,
провідний науковий співробітник
відділу правового забезпечення ринкової економіки
Науково-дослідного інституту приватного права і підприємництва
імені академіка Ф.Г. Бурчака Національної академії правових наук України

Олександр Бакалинський,
заступник директора
Департаменту формування та реалізації державної політики
у сфері кіберзахисту Адміністрації Держспецзв'язку

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

У статті досліджені передумови і особливості формування законодавства України у сфері кібербезпеки, визначені проблеми та перспективи його подальшого розвитку з точки зору оцінки наявних небезпек та загроз. Визначені напрями адаптації чинного законодавства про кібербезпеку до стандартів ЄС у межах реалізації положень Угоди про асоціацію між Україною та ЄС.

Каталізатором змін у сфері кібербезпеки в нашій державі стала гібридна війна, розв'язана РФ із застосуванням як класичної, так і нелетальної зброї, в тому числі в кіберпросторі та через кіберпростір. Виклики та загрози національній безпеці України в кіберпросторі призвели до створення Стратегії кібербезпеки України, що була впроваджена указом Президента України від 15 березня 2016 року, а реалізація її положень призвела до прийняття Закону України «Про основні засади забезпечення кібербезпеки України».

Сьогодні законодавче регулювання кіберзахисту в Україні знаходиться на початку свого формування, проте найскладніший етап – визначення стратегії, меж та напрямів державної політики забезпечення кіберзахисту пройдено. Безумовно, на цьому шляху ще багато проблем, але є і досягнення. Невирішеними є питання державно-приватної взаємодії, ще не сформовані переліки об'єктів критичної інфраструктури, триває розроблення підходів до кібероборони, попереду ще великий пласт проблем та обсяг роботи, спрямованої на нормативно-правове врегулювання у сфері кібербезпеки.

Найбільш перспективними напрямами розвитку національної системи кіберзахисту, на нашу думку, є: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни) громадян та культури безпекового поводження в кіберпросторі, впровадження систем інформаційного комплаєнсу.

Ключові слова: безпека інформації, інформаційна безпека, кіберпростір, кібербезпека.

Постановка проблеми. Кіберпростір – це новий канал для створення і поширення різноманітної інформації, він став новим двигуном зростання економіки, новою платформою соціального управління, новим способом міжнародного співробітництва, до того ж і зовсім новою сферою державного суверенітету. Однак кіберпростір не тільки надає нам ресурси, можливості, але і містить загрози. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом більш вразливим до кіберзагроз, посилюючи небезпеку, з якою стикаються люди, включаючи вразливих осіб, таких як діти. Для зменшення цих ризиків необхідно вжити всіх необхідних заходів для поліпшення кібербезпеки у світі, щоб мережеві та інформаційні системи, комунікаційні мережі, цифрові продукти, послуги та пристрої, якими користуються громадяни, організації та підприємства – починаючи від малих та середніх до значних, що визначені в Рекомендації Комісії 2003/361/ЄС [1], для операторів критичної інфраструктури – краще захищені від кіберзагроз.

Кібербезпека сучасної держави має прямий вплив на всі складові частини її політики. Голова КНР Сі Цзіньпін зазначив, що в наші дні національна безпека неможлива без її кібербезпеки, а модернізація країни неможлива без її інформатизації [2, с. 172].

Мета – дослідити передумови і особливості формування законодавства України у сфері кібербезпеки, визначити проблеми та перспективи його подальшого розвитку з точки зору оцінки наявних небезпек та загроз.

Виклад основного матеріалу. Кібернапади – це найбільші ризики, з якими може стикнутися будь-яка організація. За даними глобального огляду, проведеного об'єднанням ISACA, тільки 38% респондентів вважають, що вони підготовлені до кібернападів, решта, 83%, відносять кібернапади до однієї з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки [3].

З огляду на вищенаведений вислів варто визначитися з термінами. До сьогодні в публікаціях можна зустріти різні поняття, що використовуються як синоніми, зокрема: «безпека інформації», «інформаційна безпека» та «кібербезпека». Автори, підміняючи між собою ці поняття, вводять суспільство в оману.

Поняття «безпека інформації» визначено у ISO/IEC 27000 п. 3.28 (information security). «Безпека інформації» – збереження конфіденційності (3.10), цілісності (3.36) та доступності (3.7) інформації. Відповідно до Примітки 1 для кваліфікації безпеки у сфері інформації мають ураховуватися і інші властивості, такі як справжність (3.6), звітність, неприйняття (3.48) та надійність (3.55) [4]. У національному вимірі поняття безпеки інформації передбачає захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи знищенням даних [5].

Уперше поняття «інформаційної безпеки» в Україні було визначено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537-V [6], в якому інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Згідно із Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» вирішення проблеми інформаційної безпеки має здійснюватися шляхом: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва із цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [6]. Як бачимо, поняття «інформаційна безпека» набагато ширше, ніж поняття безпеки інформації, і зовсім не зводиться до неї.

Стандарт ICO/IEC 27032 надає визначення «кібербезпеки» через категорію безпеки кіберпростору – збереження конфіденційності, цілісності та доступності інформації в кіберпросторі. При цьому кіберпростором є середовище, що виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [7]. Відповідно до ДСТ України ISO/IEC 27032:2016 п. 4.21 кіберпростір – це складне середовище, що виникає в процесі взаємодії людей, програмного забезпечення і послуг Інтернет-послуг Інтернету, за допомогою технологічних пристроїв або об'єднаних мереж, яка не існує в будь-якій фізичній формі [8].

Аналіз останніх досліджень і публікацій. Дослідження цієї проблеми можна розпочати з термінології, яку було визначено в міжнародному стандарті ISO/IEC 27032:2012. Серед науковців варто виділити праці: Алпеєва А., Архіпова О., Чепуренко Я., Мохора В., Богданова О., Грибуніна В., Горбатько О. Напрями розвитку кібербезпеки було описано Лєбєдєвим В., Огородніковим Д., Олейніком М., Прозоровим Д., Свищевим А., Брежнєвим Є., Коваленком А., Ілляшенком О. Аналізу оцінки ризиків кібербезпеки в банківській сфері присвячено роботу Євсеєва С. та інших. Наразі тема щодо безпеки в кіберпросторі є найпоширенішою і найбільш затребуваною суспільством, оскільки це стосується кожного, хто стикається зі світом інформаційних технологій.

За наявності подібних ризиків формування власного підходу до забезпечення кібербезпеки сьогодні представляється необхідним для будь-якої держави. Таким чином, розвиток такого нового типу протистояння, як інформаційна боротьба, перехід гонки технічних озброєнь у кіберпростір також зумовлюють актуальність дослідження відносин держав у сфері кібербезпеки. На думку фахівців збройних сил США в області кібербезпеки, станом на 2008 рік у технічному плані повна адекватна система кіберзахисту передбачала побудову та використання таких основних підсистем: підсистеми захисту (Protection Capabilities), що забезпечує скритність випромінювань радіоелектронних засобів, систем і засобів зв'язку, комп'ютерну безпеку (Computer Security) і інформаційну безпеку (InfoSec); підсистеми виявлення (Detection Capabilities), що забезпечує розпізнавання аномалій у мережі за рахунок застосування систем їх виявлення; підсистеми реагування на зміни технічних параметрів і обстановки (Reaction Capabilities), що забезпечує відновлення (в тому числі реконфігурацію) і виконання інших процесів інформаційних операцій [9].

На думку окремих авторів, система кіберзахисту, створена відповідно до вищезазначених вимог, не забезпечує повною мірою кібербезпеки об'єкта інформатизації і, в першу чергу, органів державної влади та оборони. Забезпечення кібербезпеки цих органів має здійснюватися єдиною інтелектуальною системою кібербезпеки, що є частиною системи інформаційної безпеки. При цьому в основу побудови перспективної системи кібербезпеки має бути покладено поняття еволюції системи, тобто здатність її адаптації через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак) і технологій, що застосовуються для протидії їм протягом свого життєвого циклу [10, с. 5]. Безумовно, створення такої системи можливо лише шляхом поєднання всього спектру заходів державного регулювання від законодавчого регулювання до ефективного та відповідального правозастосування, в основі яких буде лежати ризик-менеджмент.

У сучасних умовах структура кіберкомандування США охоплює понад 50 тис. осіб і представляє собою складну багаторівневу структуру, що об'єднує зусилля Міністерства оборони США, АНБ та Кіберкомандування США і нараховує 133 бойові команди чисельністю понад 6,2 тис. осіб.

Каталізатором законодавчих змін у сфері кібербезпеки в нашій державі стала гібридна війна, розв'язана РФ із застосуванням як класичної, так і нелетальної зброї, в тому числі в кіберпросторі та через кіберпростір. Завдяки методам інформаційної війни Україна за лічені дні тільки в Криму втратила 27 000 км^2, частину населення понад 2,5 млн. осіб [11], 21–25 травня 2014 року відбулися DDoS-атаки і злом сайту ЦВК під час президентських виборів, внаслідок яких на сайті з'явилися помилкові результати. Незважаючи на повідомлення про злом, саме ці дані були озвучені в новинах на російському Першому каналі як реальні результати виборів в Україні, 23 грудня 2015 року за допомогою троянської програми BlackEnergy3, у використанні якої були раніше помічені російські хакери, було відключено близько 30 підстанцій Прикарпаттяобленерго, у зв'язку із чим більш 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго. Ці та багато інших, але не так широко відомих кібератак змусили не тільки серйозно задуматися і переглянути підходи до кібербезпеки лідируючі технологічні компанії, але і в цілому винести це питання на державний рівень. Виклики та загрози національній безпеці України в кіберпросторі призвели до створення Стратегії кібербезпеки України, що була впроваджена указом Президента України від 15 березня 2016 року [12], а реалізація її положень призвела до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [13].

Метою статті є аналіз законодавства України у сфері кібербезпеки, а також визначення проблем, пріоритетів та напрямів розвитку нормативно-правового регулювання у сфері кібербезпеки.

До прийняття Закону України «Про основні засади забезпечення кібербезпеки України» правову основу кібербезпеки України становили Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та інші закони, Конвенція Ради Європи про кіберзлочинність [14], інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також інші нормативно-правові акти.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повнова-

ження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

При цьому ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» визначає, що кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

Необхідно зауважити на те, що дія Закону України «Про основні засади здійснення кібербезпеки України» не поширюється на відносини та послуги, пов'язані зі змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах у мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), а також не стосується інформаційно-телекомунікаційних систем, у яких циркулює інформація, яка складає державну таємницю. Проте запровадження положень Закону у цій сфері може розглядатися як істотне порушення прав людини відповідно до положень Європейської конвенції про захист прав людини і основних свобод, зокрема ст. 10 Конвенції [15].

Забезпечення кібербезпеки в Україні ґрунтується на принципах: верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом; забезпечення національних інтересів України; відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі; державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері; пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права в разі вчинення агресивних дій у кіберпросторі; пріоритетності запобіжних заходів; невідворотності покарання за вчинення кіберзлочинів; пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки та ін.

Національна система кібербезпеки представляє собою комплексну систему взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією України, Службою безпеки України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами, Національним банком України, діяльність яких спрямована на забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Провідним суб'єктом національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України [16], на яку припадає близько 80% навантаження та яка забезпечує формування та реалізацію державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту.

У Державному центрі кіберзахисту та протидії кіберзагрозам Держспецзв'язку є структурований підрозділ Computer response team

of Ukraine (далі – CERT-UA) – команда реагування на комп'ютерні надзвичайні події України, основною метою якого є забезпечення захисту інформаційних ресурсів та інформаційних та телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. CERT-UA періодично публікує рекомендації, які стосуються безпеки поштового сервісу, із протидії загрозі інсайдера, усунення вразливостей, пов'язаних із некоректним налаштуванням DNS-серверів, із самостійного пошуку та ліквідації веб-шеллів тощо.

Закон України «Про основні засади забезпечення кібербезпеки України» заклав загальну архітектуру національної системи кібербезпеки та розподіляє завдання та повноваження між основними суб'єктами забезпечення кібербезпеки (Національним координаційним центром кібербезпеки, Міністерством оборони, Генеральним штабом Збройних Сил, Державною службою спеціального зв'язку та захисту інформації, Службою безпеки, Національною поліцією, Національним банком, розвідувальними органами України), передбачає створення умов для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації, та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян.

Реалізація положень Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки України» передбачає розроблення та застосування якісно нового законодавства у сфері кібербезпеки, що засноване на напрацьованому за п'ять років гібридної війни досвіді, усвідомленні та імплементації досвіду та нормативних документів ЄС та НАТО. Зокрема, підлягають розробленню такі нормативно-правові акти: Закон України «Про критичну інфраструктуру та її захист», постанови Кабінету Міністрів України, зокрема: «Порядок формування переліку об'єктів критичної інформаційної інфраструктури», «Порядок формування переліку об'єктів критичної інформаційної інфраструктури», «Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури» (прийняті 19 червня 2019 р. № 518), «Про затвердження Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також під час усунення їхніх наслідків», «Вимоги щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та Порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури». Мають бути створені: реєстр об'єктів критичної інформаційної інфраструктури, перелік об'єктів критичної інфраструктури, реєстр аудиторів інформаційної безпеки. Результатом впровадження зазначених нормативних актів має стати Комплексний огляд сектору безпеки і оборони, частиною якого має стати огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Важливим кроком на шляху створення сучасної системи кіберзахисту України стало прийняття Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [17], яким встановлено: визначення загальних вимог із кіберзахисту об'єктів критичної інфраструктури; встановлення обов'язкових заходів забезпечення захисту від кібератак; запобігання порушенню конфіденційності; цілісності та доступності інформаційних ресурсів; сталого функціонування.

Варто відзначити, що розвиток законодавства у сфері кібербезпеки в Україні безпосередньо пов'язаний з євроінтеграційними прагненнями України та розвитком правового регулювання електронної комерції в межах СОТ.

27 червня 2014 року України уклала Угоду про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [18]. У ст. 3 Додатку XVII (Нормативно-правове наближення до набуття повного режиму внутрішнього ринку в конкретному секторі) зазначено: «1. Згідно зі статтями 114, 124, 133 та 139 Глави 6 «Заснування підприємницької діяльності, торгівля послугами та електронна торгівля» та Глави 7 «Поточні платежі і рух капіталу» Розділу IV цієї Угоди та статті 2(1) цього Додатка Україна імплементує і на постійній основі впроваджує чинне законодавство ЄС, зазначене в Доповненнях, у свою національну правову систему відповідно до статті 2(2) цього Додатка» [19].

У січні 2012 року в ЄС було ініційовано реформування законодавства Європейського Союзу у сфері захисту персональних даних із метою приведення його у відповідність

до вимог «цифрової епохи» та виконання Стратегії Єдиного Цифрового Ринку Європи (Digital Single Market Strategy). У зв'язку із цим були підготовлені два документи: Директива 2016/680 Європейського Парламенту та Ради ЄС від 27 квітня 2016 р. про захист фізичних осіб стосовно обробки персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань та про вільне переміщення таких даних, а також про скасування Рамкового Рішення Ради 2008/977 та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних (GDPR) [20].

Стратегія та Порядок денний були оприлюднені навесні 2015 року, в липні 2016 року Європейська Комісія презентувала «Додаткові заходи зі сприяння розвитку індустрії кіберзахисту», а 06.07.2016 була ухвалена Директива ЄС щодо заходів із забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (DIRECTIVE (EU) 2016/1148 – NIS Directive). Ця Директива закладає єдині правила та вимоги у сфері кібербезпеки для всіх країн ЄС, але залишає за кожною країною-членом право вжити власних заходів щодо імплементації норм цієї Директиви в національне законодавство (це мало б бути зроблено у країнах ЄС до 9 травня 2018 року) [21].

Для досягнення мети Директиви (забезпечення більш високого рівня мережевої та інформаційної безпеки в межах Європейського Союзу) необхідно вжити заходів у трьох основних напрямках:

– підвищити спроможність системи кібербезпеки на національному рівні;

– підвищити рівень пан-європейського співробітництва;

– запровадити управління ризиками та зобов'язати сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових послуг.

Важливе значення для подальшого розвитку законодавчого регулювання у сфері кібербезпеки має також Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. Вважаємо за необхідне врахувати положення цього документу під час розроблення як національного нормативного акта, так і локальних актів суб'єктів господарювання.

Особливої уваги заслуговують визначені Директивою 2008/114/ЄС Наскрізні критерії оцінки ЄКІ, зазначені в параграфі 1, що включають:

1) критерій нещасних випадків (оцінюється потенційна кількість смертельних випадків або отриманих травм);

2) критерій економічних результатів (оцінюється значущість економічних втрат та/або погіршення продуктів чи послуг, у тому числі потенційні екологічні наслідки);

3) критерій суспільних наслідків (оцінюється вплив на суспільну довіру, фізичні страждання, порушення повсякденного життя, в тому числі ненадання основних послуг).

Граничні значення наскрізних критеріїв повинні встановлюватися з урахуванням серйозності наслідків, спричинених пошкодженням або знищенням конкретної інфраструктури. Точні граничні значення наскрізних критеріїв у кожному конкретному випадку визначають відповідні держави-члени для певної критичної інфраструктурі. Кожна держава-член повинна щорічно інформувати Комісію про кількість інфраструктур у кожному секторі, щодо яких проводилися обговорення про граничні значення наскрізних критеріїв. Секторальні критерії повинні враховувати особливості окремих секторів ЄКІ. При цьому кожна держава-член повинна перевірити наявність безпекового плану оператора (БПО) або аналогічних інструментів, спрямованих на вирішення питань у кожній визначеній ЄКІ, що розташовується на її території. Якщо держава-член встановила, що БПО або аналогічні інструменти існують і регулярно оновлюються, необхідність здійснення подальших імплементаційних дій відсутня [21].

Зазначені положення знайшли своє відображення в Проекті Закону України «Про критичну інфраструктуру та її захист», що наразі знаходиться на розгляді профільного комітету Верховної Ради України, а також проектах Постанов Уряду: «Порядку та критеріїв віднесення об'єктів до об'єктів критичної інфраструктури», а також «Порядку формування переліку об'єктів критичної інформаційної інфраструктури».

Необхідно звернути увагу на нормативно-правове регулювання кібербезпеки в банківському секторі України. Стрімкий розвиток нормативно-правового забезпечення у сфері кібербезпеки банківського сектору є можливим завдяки незалежному становищу Національного банку, яке визначається Законом України «Про Національний банк» [22].

Забезпечення безпеки в кіберпросторі не вичерпується заходами державного регулювання і контролю, а в багатьох випадках залежить від свідомої і відповідальної поведінки учасників правовідносин, зокрема суб'єктів господарювання. Підвищений інтерес у кібер-

злочинців викликає ринок криптовалют та електронної комерції. За допомогою різних способів здійснення атак хакери здійснюють крадіжки електронних грошей безпосередньо у їхніх власників, або ж використовують для цього підручні ресурси – гаманці, біржі та інше. Кібератаки на суб'єктів господарювання та їх діяльність можуть набувати абсолютно різних форм. Це може бути фішинг, який здійснюється, наприклад, за допомогою розсилки електронних повідомлень співробітникам або використання шкідливого програмного забезпечення.

Одним із ключових чинників, що сприяє попередженню кібератак, є ефективна система захисту та жорстка система покарань кіберзлочинців, наприклад, така, як існує у США. Україна, на жаль, на даний момент не може похвалитися настільки розвиненим і вдосконаленим законодавством щодо притягнення до відповідальності за незаконні шкідливі дії хакерів [23].

Важливим елементом безпеки господарської діяльності суб'єкта господарювання є політика інформаційної безпеки та заходи корпоративного або інформаційного комплаєнса, що впроваджуються суб'єктом господарювання. Як правило, це певна сукупність правил, вимог, оцінки ризиків та рекомендацій, що визначають порядок інформаційної діяльності суб'єкта господарювання та особливості забезпечення безпеки його діяльності в кіберпросторі. Такі заходи забезпечують належний рівень безпеки інформаційних систем та врахують такі елементи: а) безпеку систем; б) врегулювання інцидентів; в) управління безперервністю бізнесу; г) моніторинг та постійний аудит; ґ) відповідність міжнародним стандартам; д) розслідування інцидентів та притягнення винних до відповідальності.

Окремо необхідно зауважити, що згідно зі статтею 5 Закону (про основні засади) суб'єктами забезпечення кібербезпеки є і окремі громадяни, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. І тому саме від їх відповідальної поведінки в кіберпросторі найчастіше залежить стабільність кіберпростору.

Сьогодні законодавче регулювання кіберзахисту в Україні знаходиться на початку свого формування, проте найскладніший етап – визначення стратегії, меж та напрямів державної політики забезпечення кіберзахисту пройдено. Безумовно, на цьому шляху ще багато проблем, але є і досягнення. Невирішеними є питання державно-приватної взаємодії, ще не сформовані переліки об'єктів критичної інфраструктури, триває розроблення підходів до кібероборони, попереду ще великий пласт проблем та обсяг роботи, спрямованої на нормативно-правове врегулювання у сфері кібербезпеки.

Інформаційна війна, яка відбувається між Росією і Україною, включає не тільки воєнні дії та інформаційно-психологічні операції, а також проведення кібератак. З огляду на це формування нормативної основи забезпечення кібербезпеки має бути засноване на чіткій та зрозумілій Стратегії. Строк дії чинної Стратегії кібербезпеки України завершується наступного року, тому варто розпочинати роботу над новою сучасною Стратегією кібербезпеки України, що має враховувати наявний досвід як професійного середовища, так і іноземних партнерів, саме Стратегія повинна оцінити виклики і визначити перспективи підвищення захищеності в кіберпросторі. Проте це завдання є спільним як для держави, так і для суспільства в цілому, оскільки особливістю кіберпростору є відсутність кордонів і меж, а тому забезпечення безпеки є питанням кожного.

Висновки

Найбільш перспективними напрямами розвитку національної системи кіберзахисту, на нашу думку, є: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни) громадян та культури безпекового поводження в кіберпросторі, впровадження систем інформаційного комплаєнсу та, насамперед, створення довірчих відносин між державою та суспільством, для якого держава повинна грати сервісну роль.

Список використаних джерел:

1. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union.* L 151/15, 7.6.2019

2. Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности. *Индекс безопасности.* 2013. № 1(104). С. 169–184.

3. Стандарти ISO/IEC захистять від кіберзагроз. 31.08.2016. URL: http://csm.kiev.ua. (дата звернення: 02.09.2019).

4. ISO/IEC 27000. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (дата звернення: 02.09.2019).

5. Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи, Постанова Кабінету Міністрів України; Концепція від 20.01.1997 № 40. URL: https://zakon.rada.gov.ua/laws/term/40-97-%D0%BF. (дата звернення: 02.09.2019).

6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V. *Відомості Верховної Ради України* (ВВР). 2007. № 12. Ст. 102

7. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. URL: www.iso.org/standard/44375.html. (дата звернення: 02.09.2019).

8. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. № 448. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128 (дата звернення: 02.09.2019).

9. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны – реальная угроза национальной безопасности? Москва : КРАС АНД, 2011. 96 с.

10. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2). *Вопросы кибербезопасности*. № 1 (2). 2014 . С. 5–12.

11. Бакалинський О.О. «Інформаційний бліцкриг». Правова інформатика. № 2(42)/2014. URL: http://ippi.org.ua/sites/default/files/14booib.pdf. (дата звернення 02.09.2019).

12. Про Стратегію кібербезпеки України : Указ Президента №96/2016 від 15.03.2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 02.09.2019).

13. Про основні засади забезпечення кібербезпеки України : Закон України № № 2163-VIII від 05.10.2017 р. *Відомості Верховної Ради* (ВВР). 2017. № 45. Ст. 403.

14. Про кіберзлочинність. Конвенція Ради Європи від 21.11.2001. *Офіційний вісник України* від 10.09.2007 р. № 65. С. 107. Ст. 2535, код акту 40846/2007.

15. Про захист прав людини і основних свобод. Європейська конвенція. від 04.11.1950. *Офіційний вісник України* від 16.04.1998. № 13 / № 32 від 23.08.2006. С. 270.

16. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 07.11.2018, № 2155-VIII. *Відомості Верховної Ради України* (ВВР). 2006. № 30. Ст. 258.

17. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року. *Офіційний вісник України* від 02.07.2019. 2019. № 50. С. 53. Стаття 1697, код акту 94896/2019.

18. Угода про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014. *Офіційний вісник України* від 26.09.2014. № 75. Том 1. С. 83. Ст. 2125.

19. Біла книга. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Матеріал для обговорення (Policy Paper). URL: parlament.org.ua/2017/12/au_White-book-on-cybersecurity-draft_5 (дата звернення: 02.09.2019).

20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.

21. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30.

22. Про Національний банк України. Закон України від 20.5.1999 № 679-XIV. *Відомості Верховної Ради України* (ВВР). 1999. № 29. Ст. 238.

23. Клименко А. Правовые аспекты кибербезопасности бизнеса. URL: https://cpk.ua/publications/articles/full/pravovyye-aspekty-kiberbezopasnosti-biznesa-2/ (дата звернення: 02.09.2019).

The catalyst for changes in the sphere of cyber-security in our country has been the hybrid war unleashed by the Russian Federation with the use of both classic and non-lethal weapons, through cyberspace and across cyberspace included. Challenges and threats to the national security of Ukraine in the cyberspace led to the creation of the Cyber-security Strategy of Ukraine, which was implemented by the decree of the President of Ukraine of March 15, 2016, and the implementation of its provisions led to the adoption of the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine".

Today, the legislative regulation of cyber defense in Ukraine is at the beginning of its formation, however, the most difficult stage is to define the strategy, boundaries and directions of the state policy of providing cyber defense. It goes without saying that there are still a lot of problems along the way, but there are also some achievements. Issues of public-private cooperation are still unresolved, the lists of critical infrastructure objects and the like have not yet been formed, the development of approaches to cyber defense is still ahead, and there is still a large layer of problems and the amount of work aimed at regulatory policy in the field of cyber security.

In our opinion, the most promising directions of development of the national cyber defense system are: improvement of the legal basis of cyber defense for critical infrastructure facilities; implementation of the system of independent information security audit on critical infrastructure facilities; establishment of sectoral cyber incident response centers; development of international cooperation in the field of cyber security; development of cyber security training system; increase of digital literacy (cyber hygiene rules) of citizens and culture of safe behavior in the cyberspace, introduction of information compliance systems. The most important step is the establishment of trustful relationship between the state and the society, for which the state should play servicing role.

Key words: security of information, informational security, cyberspace, cyber security.