УДК 347:004.056.53

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ В УКРАЇНІ

Бакалінська О. О.,
доктор юридичних наук, провідний науковий співробітник відділу правового забезпечення ринкової економіки Науково-дослідного інституту приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України (Київ)

В статті досліджені передумови і особливості формування законодавства України в 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 в межах реалізації положень Угоди про асоціацію між Україною та ЄС.

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

У сучасних умовах роль інформаційного середовища неухильно зростає, а на зміну класичним способам торгівлі і обміну приходить електронна комерція. 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 надає нам не тільки ресурси, можливості, але і містить загрози. Кібербезпека сучасної держави має прямий вплив на всі складові його політики. Голова КНР Сі Цзіньпін зазначив, що в наші дні національна безпека неможлива без її кібербезпеки, а модернізація країни неможлива без її інформатизації[1].

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[2].

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.

---

[1] Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности // Индекс безопасности. 2013. № 1 (104). С. 169—184

[2] Стандарти ISO/IEC захистять від кіберзагроз. URL: http://csm.kiev.ua (дата звернення: 31.08.2016).

Поняття «безпека інформації»[1] визначено в розділі 2 міжнародного стандарта-довідника 27000:2016, в якому визначається, що безпека інформації це збереження конфіденційності (2.12), цілісності (2.40) і можливості застосування (2.9) інформації. Крім того, можуть бути використані інші властивості інформації, такі як справжність (2.8), контрольованість, незаперечність авторства (2.54) і надійність (2.62)[2] .

Вперше поняття інформаційної безпеки було визначено у Законі України від 09.01.2007 р. № 537-V «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»[3], в якому, інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому 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.

Стандарт ICO/IEC 27032 – надає визначення «кібербезпеки» через категорію безпеки кіберпростору – збереження конфіденційності, цілістності та доступності інформації у кіберпросторі. При цьому, кіберпростором є середовище, що виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем[4].

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

При наявності подібних ризиків формування власного підходу до забезпечення кібербезпеки на сьогоднішній день представляється необхідним для будь-якої держави. Таким чином, розвиток такого нового типу протистояння, як інформаційне, перехід гонки озброєнь в гонку технічних озброєнь в кіберпростірі, що також обумовлює актуальність дослідження відносин держав в сфері кібербезпеки. На думку фахівців збройних сил США в області кібербезпеки, в технічному плані повна адекватна система кіберзахисту передбачає 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

---

[1] Архипов А. Приставка кибер-: все ли очевидно // Захист інформації. 2016. № 3. Т. 18. С. 203-209.

[2] Международный ISO/IEC стандарт 27000 Информационные технологии – Методы и средства обеспечения безопасности -Системы менеджмента информационной безопасности – Общие сведения и словарь. ISO/IEC 27000:2016 (E) /А. Горбунов. URL: www.pqm-online.com (дата звернення 01.04.2019).

[3] Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V // Відомості Верховної Ради України. 2007. № 12. ст.102.

[4] ISO/IEC 27032:2012 Information technology -- Security techniques – Guidelines for cybersecurity. URL: www.iso.org/standard/44375.html (дата звернення 01.04.2019)/

забезпечують розпізнавання аномалій в 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[1]. 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[2]. Безумовно, що створення такої системи можливо лише шляхом поєднання всього спектру заходів державного регулювання від законодавчого регулювання до ефективного та відповідального правозастосування.

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

До прийняття Закону України «Про основні засади забезпечення кібербезпеки України»[3], 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[4], 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 у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 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 у кіберпросторі.

---

[1].Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны – реальная угроза национальной безопасности? М.: КРАС АНД, 2011. 96 с.

[2] 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.

[3] Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 // Відомості Верховної Ради. 2017. № 45. ст.403.

[4] Про кіберзлочинність. Конвенція Ради Європи від 21.11.2001 //Офіційний вісник України від 10.09.2007 р., № 65, стор. 107, стаття 2535, код акта 40846/2007.

Нажаль, дія вищевказаного Закону України «Про основні засади забезпечення кібербезпеки України» не поширюється на відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси). 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[1].

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 у 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 низки державних органів, зокрема, 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[2], що забезпечує формування та реалізацію державної політики щодо захисту у 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

[1] Про захист прав людини і основних свобод. Європейська конвенція. від 04.11.1950 // Офіційний вісник України від 16.04.1998. 1998, № 13. № 32 від 23.08.2006. Стор. 270.

[2] Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 07.11.2018, № 2155-VIII // Відомості Верховної Ради України. 2006, № 30, ст.258

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.

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.

Реалізація положень Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки України» передбачає розробку та застосування якісно нового законодавства в сфері кібербезпеки і оборони, що засноване на напрацьованому за п'ять років гібридної війни досвіді та імплементації новітніх положень законодавства ЄС та США, зокрема, підлягають розробці наступні нормативні акти: Закон України «Про критичну інфраструктуру та її захист», Порядок віднесення об'єктів критичної інфраструктури, Порядок формування переліку об'єктів критичної інформаційної інфраструктури, Реєстр об'єктів критичної інформаційної інфраструктури, Перелік об'єктів критичної інфраструктури, Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури, Протокол спільних дій як механізм взаємодії суб'єктів кіберзахисту, Положення про аудит інформаційної безпеки об'єктів критичної інфраструктури. Результатом впровадження зазначених нормативних актів має стати Комплексний огляд сектору безпеки і оборони, частиною якого має стати Національний огляд кіберзахисту.

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»[1], якою встановлено: визначення загальних вимог з 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 в 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[2]. В 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 транспонує і на постійній основі впроваджує чинне

[1] 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 р., № 50, стор. 53, стаття 1697, код акта 94896/2019

[2] 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. 2014. № 75, том 1, стор. 83, стаття 2125

законодавство ЄС, зазначене у Доповненнях, у свою національну правову систему відповідно до статті 2(2) цього Додатка[1].

У січні 2012 року в ЄС було ініційовано реформування законодавства Європейського Союзу в сфері захисту персональних даних з метою приведення його у відповідність до вимог "цифрової епохи" та на виконання Стратегії Єдиного Цифрового Ринку Європи (Digital Single Market Strategy). В зв'язку з 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 Регламент (Євросоюз) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних(GDPR)[2].

07.02.2013 р. Європейський Союз ухвалив Стратегію кібербезпеки, метою якої є відкритий, надійний і безпечний кіберпростір. Одразу після оприлюднення Стратегії було розпочато роботу над відповідною директивою. Важливо наголосити, що цей документ розроблявся не окремо від інших напрямків, а в якості частини Стратегії Єдиного Цифрового Ринку (Digital Single Market Strategy), з одного боку, і частини Європейського Порядку Денного з питань безпеки (European Agenda on Security), з іншого.

Стратегія та Порядок денний були оприлюднені навесні 2015 року, в липні 2016 року Європейська Комісія презентувала "Додаткові заходи по сприянню розвитку індустрії кіберзахисту", а 06.07.2016 була ухвалена Директива ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (DIRECTIVE (EU) 2016/1148 – NIS Directive). Ця Директива закладає єдині правила та вимоги в 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 до 9 травня 2018 року)[3].

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

підвищити спроможность 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.

---

[1] Біла книга. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні Матеріал для обговорення (Policy Paper).

[2]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.

[3] 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.

Важливе значення для подальшого розвитку законодавчого регулювання в 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. Відповідно до Директиви встановлюється процедура ідентифікації і визначення європейських критичних інфраструктур («ЄКІ») та сформовані підходи до формування єдиного підходу для оцінювання необхідності покращення охорони та захисту таких інфраструктур з метою сприяння захисту населення. Вважаємо за необхідне врахувати положення цього документу як при розробці національного нормативного акту, 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: (a) критерій нещасних випадків (оцінюється потенційна кількість смертельних випадків або отриманих травм); (b) критерій економічних результатів (оцінюється значущість економічних втрат та/або погіршення продуктів чи послуг, у тому числі потенційні екологічні наслідки); (c) критерій суспільних наслідків (оцінюється вплив на суспільну довіру, фізичні страждання, порушення повсякденного життя, у тому числі ненадання основних послуг).

Граничні значення наскрізних критеріїв повинні встановлюватися з урахуванням серйозності наслідків, спричинених пошкодженням або знищенням конкретної інфраструктури. 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 в 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[1].

На нашу думку, зазначені положення мають бути закріплені в Проекті Закону України «Про критичну інфраструктуру та її захист», а також проектах: Порядку та критеріїв віднесення об'єктів до об'єктів критичної інфраструктури, а також Порядку формування переліку об'єктів критичної інфраструктури та Порядку ведення реєстру об'єктів критичної інфраструктури та інші.

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 кіберзлочинців викликає ринок криптовалют та електронної комерції. За допомогою різних способів здійснення атак, хакери здійснюють крадіжки електронних грошей безпосередньо у їх 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 з 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

[1] 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.*

може похвалитися настільки розвиненим і вдосконаленим законодавством щодо притягнення до відповідальності за незаконні шкідливі дії хакерів[1].

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 у кіберпросторі. Такі заходи забезпечують належний рівень безпеки інформаційних систем, та врахують такі елементи: (a) безпеку систем; (b) врегулювання інцидентів; (c) управління безперервністю бізнесу; (d) моніторинг та постійний аудит; (e) відповідність міжнародним стандартам; (f) розслідування інцидентів та притягнення винних до відповідальності.

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.

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 з огляду на це, варто розпочинати роботу над новою сучасною Стратегією кібербезпеки України, що враховує наявний досвід, оцінює виклики і визначає перспективи підвищення захищеності в кіберпросторі. Проте, це завдання є спільним і для держави і для суспільства в цілому оскільки особливістю кіберпростору є відсутність кордонів і меж, а тому забезпечення безпеки є питанням кожного.

Найбільш перспективними напрямами розвитку національної системи кіберзахисту, на нашу думку, є: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; огляд Національної системи кібербезпеки; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, впровадження систем інформаційного комплаєнсу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности // Индекс безопасности. 2013. № 1 (104). С. 169–184
2. Стандарти ISO/IEC захистять від кіберзагроз. URL: http://csm.kiev.ua (дата звернення: 31.08.2016.)
3. Архипов А. Приставка кибер-: все ли очевидно// Захист інформації. 2016. № 3. Т. 18. С. 203-209.
4. Информационные технологии – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общие сведения и словарь. МЕЖДУНАРОДНЫЙ ISO/IEC СТАНДАРТ 27000/ ISO/IEC 27000:2014 (E). URL: www.pqm-online.com (дата звернення 01.04.2019)/

[1] Клименко А. Правовые аспекты кибербезопасности бизнеса URL: https://cpk.ua/publications/articles/full/pravovyye-aspekty-kiberbezopasnosti-biznesa-2/ (дата звернення 01.04.2019)/

5. 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. 2007, № 12, Ст.102
6. ISO/IEC 27032:2012 Information technology – Security techniques -- Guidelines for cybersecurity. URL: www.iso.org/standard/44375.html (дата звернення 01.04.2019).
7. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны – реальная угроза национальной безопасности? М.: КРАС АНД, 2011. 96 с.
8. 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.
9. Про Стратегію кібербезпеки України: Указ Президента №96/2016 від 15.03.2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016
10. Про основні засади забезпечення кібербезпеки України: Закон України № № 2163-VIII від 05.10.2017 р.// Відомості Верховної Ради (ВВР), 2017, № 45, ст.403
11. Про кіберзлочинність. Конвенція Ради Європи від 21.11.2001. //Офіційний вісник України від 10.09.2007 — 2007 р., № 65, стор. 107, стаття 2535, код акта 40846/2007
12. Про захист прав людини і основних свобод. Європейська конвенція. від 04.11.1950. // Офіційний вісник України від 16.04.1998. 1998 р., № 13. № 32 від 23.08.2006. стор. 270
13. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 07.11.2018, № 2155-VIII // Відомості Верховної Ради України. 2006, № 30, ст.258
14. 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 р., № 50, стор. 53, стаття 1697, код акта 94896/2019
15. 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 — 2014 р., № 75, том 1, стор. 83, стаття 2125
16. Біла книга. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні Матеріал для обговорення (Policy Paper).
17. 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
18. 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
19. Клименко А. Правовые аспекты кибербезопасности бизнеса – URL: https://cpk.ua/publications/articles/full/pravovyye-aspekty-kiberbezopasnosti-biznesa-2/ (дата звернення 01.04.2019).

THE PROBLEMS OF LEGAL PROTECTION OF CYBER SECURITY IN UKRAINE

Bakalinska O. O., Doctor of Legal Sciences, Leading Researcher of the of the department of legal support of a market economy of the Academician F. H. Burchak Scientific Research Institute of Private Law and Entrepreneurship of NALS of Ukraine (Kyiv)

Keywords: information security, cyberspace, cybersecurity.

The article studies the prerequisites and features of the formation of the legislation of Ukraine on cybersecurity, problems and prospects for its further development are identified, taking into account the assessment of existing threats. The authors determined the directions of adaptation of the current legislation on cybersecurity to EU standards in the framework of the implementation of the provisions of the Association Agreement between Ukraine and the EU.