DOI: https://doi.org/10.26565/1992-2337-2022-1-04

УДК 004.01

Євген Олександрович Живило
кандидат наук з державного управління,
начальник кафедри зв'язку та автоматизованих систем управління
Інституту забезпечення військ (сил) та інформаційних технологій
Національного університету оборони України імені Івана Черняховського, м. Київ, Україна
https://orcid.org/0000-0003-4077-7853

ДИФІНІЦІЙНІ ПРОБЛЕМАТИКИ СФЕР КРИПТОГРАФІЧНОГО ТА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, КІБЕРЗАХИСТУ І ПРОТИДІЇ ТЕХНІЧНИМ РОЗВІДКАМ

Анотація. Сьогодні виконання заходів кіберзахисту інформаційно-комунікаційних систем і об'єктів критичної інфраструктури держави, протидія та реагування на комп'ютерні інциденти та кібервпливи – залишається одним з серйозних завдань у сфері інформаційної безпеки та кібербезпеки держави.

Визначаючи напрями зовнішньополітичної діяльності України у галузі кібербезпеки, Стратегією встановлено, що Україна активізує свою участь і партнерство в міжнародних процесах стандартизації та сертифікації у сфері кібербезпеки, збільшить свою "присутність" в міжнародних, регіональних та інших органах та інститутах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією цієї сфери в геополітичному сенсі.

Виходячи з необхідності наукового обґрунтування інституційних засад розвитку системи кібербезпеки, на особливу увагу заслуговують питання розроблення стандартів у сферах нових IT-технологій (зокрема щодо штучного інтелекту, хмарних баз даних, квантових обчислень і комунікацій) та базової архітектури Інтернету.

Здійснений огляд проблемного поля дослідження свідчить про те, що в цілому мережа Інтернет повинна бути всеосяжною та відкритою, технології які в ній підтримуються та застосовуються повинні орієнтуватися на людину, її базові свободи, гарантувати відповідний нейтралітет до її приватного життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження повинні здійснюватися лише відповідно до законів та нормативів (стандартів). Позиція України полягає в тому, що користування тими, чи іншими технологічними процесами мають бути законними та безпечним, відповідно до існуючих етичних норм.

Чинні законодавчі та підзаконні акти держави, чинні національні стандарти, в тому числі і ті, що розроблювались та впроваджувались були сформульовані з врахуванням перспективних напрямів розвитку механізмів інституціонального забезпечення системи кібернетичної безпеки та ґрунтувались на євроатлантичному досвіді. Це дозволило доволі ефективно імплементувати їх до нормативно-правової бази України.

Як цитувати: Живило Є. О. Дифініційні проблематики сфер криптографічного та технічного захисту інформації, кіберзахисту і протидії технічним розвідкам. *Державне будівництво*. 2022. № 1(31). С. 46–58. DOI: https://doi.org/10.26565/1992-2337-2022-1-04

In cites: Zhyvylo, Ye.O. (2022). Defining issues of cryptographic and technical information security, cybersecurity and countering technical intelligence. *State Formation, 1(31), 46–58*. DOI: https://doi.org/10.26565/1992-2337-2022-1-04 [in Ukrainian]

Попри це, під час аналізу й узагальнення теоретичних підходів до сутності та змісту деяких визначень експерти дійшли до відповідної нормативно-правової колізії, а саме, що національні стандарти містять вимоги у частково аналогічних сферах життєдіяльності українського суспільства, тільки з іншими назвами, наприклад: "інформаційна безпека", "безпека інформаційних технологій", а також "кібербезпека".

Отже, автором детально розглянуто теоретичну та практичну значущість означеного проєкту Закону України "Про внесення змін до деяких законів України щодо стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам" за ініціативою народних депутатів України Федієнко О. П., Клочко А. А. та інших, реєстраційний № 6568 від 28 січня 2022 р. (перше читання).

Тому, спираючись на введену в дію Стратегію кібербезпеки, яка набрала чинності 28.08.2021 р. і очевидно що у процесі досягнення визначених нею цілей потрібен системний підхід, питання законодавчого регулювання та стандартизації у сфері кіберзахисту і визначення конкретного суб'єкта стандартизації за даним напрямком діяльності є вкрай важливими.

Ключові слова: кіберзагрози, національна система кібербезпеки, стандартизація, спроможності національної системи кібербезпеки, нормативно-правовий акт, нормативний документ.

Постановка проблеми. Розвиток механізмів інституціонального забезпечення функціонування організаційних структур, підготовка та ведення активних дій в кібернетичному просторі, а також відповідних питань організації діяльності органів військового управління всіх рівнів, їх взаємодія та забезпечення здійснюється відповідно до Стратегії кібербезпеки і є одним із пріоритетів у системі національної безпеки України. Визначено, що реалізація пріоритету із забезпечення кібербезпеки буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Розбудова національної системи кібербезпеки здійснюється відповідно до визначених управлінських функцій основних суб'єктів на засадах стримування та кіберстійкості, при цьому питання взаємодії між суб'єктами сектору безпеки і оборони держави здійснюються шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.

Для досягнення визначених Стратегією кібербезпеки стратегічних цілей Україна, зокрема, повинен забезпечуватись:

– постійний перегляд та оновлення вимог щодо кіберзахисту об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури з урахуванням сучасних міжнародних стандартів з питань кібербезпеки;

– розроблення національних стандартів у сфері кібербезпеки, організаційних та технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів;

– залучення на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення проектів нормативно-правових актів, нормативних документів та стандартів у цій сфері;

– поглиблення співпраці з Міжнародним союзом електрозв'язку у сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації за цими складовими (у рамках міжнародного співробітництва у сфері кібербезпеки, спрямованого, передусім, на забезпечення незалежності і державного суверенітету, відновлення територіальної цілісності України) [1].

Тому теоретичні підходи до визначення сутності та змісту положень та їх змістовного навантаження, забезпечення правових рамок для функціонування системи кібербезпеки, усвідомлення необхідності щодо питань розроблення стандартів у сфері інформаційно-комунікаційних систем та технологій є вкрай об'єктивною проблематикою.

Аналіз останніх досліджень і публікацій. Водночас, стандартизація у сферах кіберзахисту, криптографічного та технічного захисту інформації, протидії технічним розвідкам є дуже специфічною, передбачає визначення спеціальної термінології, вимог до систем документації, процесів та процедур управління, дії, взаємодії суб'єктів забезпечення кібербезпеки між собою та з іншими суб'єктами як державної, так і приватної форми власності. Об'єкти стандартизації кіберзахисту, криптографічного та технічного захисту інформації, протидії технічним розвідкам є значно ширшими ніж об'єкти стандартизації, на які розповсюджується дія Закону України "Про стандартизацію".

Забезпечення кіберзахисту критичної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, реалізується в переважній більшості шляхом побудови комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і напряму пов'язаним із криптографічним та технічним захистом інформації в цих системах [1].

Стандартизація і нормативне регулювання у сферах технічного та криптографічного захисту інформації є невід'ємним практичним елементом кіберзахисту і їх необхідно розглядати в одній площині регулювання та застосування. Однак, використання загальних правил Закону України "Про стандартизацію" щодо унормування та сталого визначення у сферах кіберзахисту, криптографічного та технічного захисту інформації, протидії

технічним розвідкам не дає можливості повною мірою створити правові основи для подолання викликів та загроз для національної безпеки і оборони держави в умовах стрімкого розвитку новітніх чи нешаблонних технологій для протидії перевазі супротивника у військовій силі.

Адже проблеми дослідження сталого функціонування об'єктів критичної інфраструктури держави, порядку запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем можна вирішити й вирішувати надалі тільки за умов тісної взаємодії всіх зацікавлених представників держави і суспільства.

Невирішені частини проблеми. Впевнено можливо стверджувати, що проєктом Закону передбачено внесення змін до Закону України "Про Державну службу спеціального зв'язку та захисту інформації України", якими вводяться терміни "стандартизація криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам", "стандарт криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам" і "орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам". Також передбачено внесення змін до частини другої статті 2 Закону України "Про стандартизацію", відповідно до яких стандартизація у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам не регулюється цим Законом.

Тому, враховуючи запропоновані зміни в існуючу законодавчу нормативно-правову базу та аналізуючи наукові джерела та інші матеріали і прогнози, завдання щодо здійснення стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам буде покладено на Державну службу спеціального зв'язку та захисту інформації України. В цьому ракурсі зазначений суб'єкт наділяється повноваженнями визначати орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам з числа науково-дослідних, науково-виробничих та інших установ і організацій Державної служби спеціального зв'язку та захисту інформації України [1].

За цих умов є вкрай важливо коректно та логічно обґрунтовано виокремити питання стандартизації у сферах кіберзахисту, криптографічного та технічного захисту інформації, протидії технічним розвідкам в окрему сферу регулювання, що забезпечить якісне, деталізоване і всеохоплююче нормативне

регулювання цих сфер з урахуванням сучасних міжнародних стандартів з питань кібербезпеки.

Метою статті є теоретичне узагальнення та надання пропозицій, щодо вирішення наукового завдання, яке полягає в обґрунтуванні оновлення правових засад здійснення кібербезпекової політики, державного регулювання у сфері інформатизації, телекомунікацій та захисту інформації, створення сучасної системи стандартизації норм та правил у системі кібербезпеки України.

Виклад основного матеріалу. Сьогодні Україна проходить тяжкі випробування, на тлі військової окупації Російською Федерацією території України. Ситуація стрімко загострюється, ворог руйнує життєво важливі об'єкти інфраструктури, загрожує життю цивільного населення. Створення правових, економічних та управлінських механізмів реалізації конституційних прав нашого суспільства є одним з головних завдань держави.

Розглядаючи проєкт Закону України реєстраційний № 6568 "Про внесення змін до деяких законів України щодо стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам" слід зауважити, що його автори доволі змістовно та обґрунтовано проаналізували стан і проблеми національного нормативно-правового та організаційного забезпечення у сфері захисту інформації та кібербезпеки.

Регулювання діяльності у зазначеній сфері суспільних відносин здійснюється відповідно до існуючої нормативно-правової бази, а саме:

Закон України "Про Державну службу спеціального зв'язку та захисту інформації України";

Закон України "Про стандартизацію";

Закон України "Про основні засади забезпечення кібербезпеки України";

Закон України "Про захист інформації в інформаційно – телекомунікаційних системах";

Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447.

В цілому сутність проєкту Закону України "Про внесення змін до деяких законів України щодо стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам" зводиться до розгляду питань стандартизації тільки у таких сферах, як "криптографічний та технічний захист інформації, кіберзахист, протидія технічним розвідкам".

При цьому, додаткової уваги з боку наукової спільноти потребує поглиблений аналіз питань щодо змісту і класифікації, за класами та групами і сферою застосування, існуючого нормативно-правового поля за напрямком інформаційної та кібернетичної безпеки, які реалізовані у вимогах Національного класифікатору України "Український класифікатор нормативних документів НК 004:2020" (який є ідентичним щодо International Classification for Standards (ICS), 2015, Seventh edition (Міжнародний класифікатор стандартів, 2015, сьоме видання). Відтак, до його складу включено стандарти і нормативні документи у галузях "криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам" (табл. 1) [5]:

Таблиця 1

Ієрархічний класифікатор

Table 1

Hierarchical classifier

Ієрархічний класифікатор	Сфера застосування
35	ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
35.020	Інформаційні технології (IT) взагалі
	* *Охоплює також загальні аспекти устаткування інформаційних технологій*
35.030	Безпека інформаційних технологій
	* *Охоплює також шифрування*
35.040	Кодування інформації
	* *Охоплює також кодування аудіо-інформації, зображень, мульти-медійної та гіпермедійної інформації, штрихове кодування тощо*
	* *Методи убезпечення в галузі інформаційних технологій, див. 35.030*

Зокрема, в рамках групи "35.030 Безпека інформаційних технологій" в Україні введено велику кількість національних стандартів, які адаптовані до стандартів Європейського Союзу та стосуються як сфер "криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам", так і, наприклад, сфер "інформаційна безпека", "безпека інформаційних технологій" та "кібербезпека". При цьому, в Україні, у сфері стандартизації, не визначено співвідношення термінів "криптографічний захист інформації", "технічний захист інформації", "протидія технічним розвідкам" із термінами міжнародних стандартів, таких як, наприклад, "інформаційна безпека", "безпека

інформаційних технологій" та "кібербезпека". Також, в Україні, у сфері стандартизації, не проведено адаптацію термінів "криптографічний захист інформації", "технічний захист інформації", "протидія технічним розвідкам" до термінологічної бази існуючих міжнародних стандартів, а також не визначене співвідношення між "сферою кіберзахисту" та "сферою кібербезпеки".

У міжнародних стандартах не використовуються безпосередньо терміни "криптографічний захист інформації", "технічний захист інформації", "протидія технічним розвідкам". Відповідно, спершу, ніж вводити зазначену термінологію до Законодавства у сфері стандартизації, спочатку слід гармонізувати терміни "криптографічний захист інформації", "технічний захист інформації", "протидія технічним розвідкам" із вимогами міжнародних стандартів Європейського Союзу у сферах "інформаційна безпека", "безпека інформаційних технологій" та "кібербезпека". Діючі нормативно-правові документи в Україні які адаптовані із стандартами Європейського Союзу ДСТУ (таблиці 2) [5].

Таблиця 2

Вимогами міжнародних стандартів Європейського Союзу у сферах "інформаційна безпека", "безпека інформаційних технологій" та "кібербезпека"

Table 2

The requirements of international standards of the European Union in the fields of "information security", "information technology security" and "cyber security"

№ з/п	Реєстраційний індекс документа	Сфера застосування
1	*ДСТУ ISO/IEC TR 19791:2015*	*Інформаційні технології. Методи захисту. Оцінювання безпеки операційних систем*
2	*ДСТУ ISO/IEC 15946-1:2015*	*Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 1. Загальні положення*
3	*ДСТУ CWA 14167-1:2015*	*Вимоги безпеки до управління сертифікатами електронних підписів. Частина 1. Системні вимоги безпеки*
4	*ДСТУ ISO/IEC 18033-2:2015*	*Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри*
5	*ДСТУ ISO/IEC 27000:2019*	*Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник*
6	*ДСТУ ISO/IEC 27007:2018*	*Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою*
7	*ДСТУ ISO/IEC 18045:2015*	*Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT*

Окреме введення у сферу стандартизації на законодавчому рівні тільки таких сфер, як: “криптографічний захист інформації”, “технічний захист інформації”, “кіберзахист”, “протидія технічним розвідкам”, без розгляду безпосередньо пов’язаних із ними сфер, таких як “електронні комунікації”, “інформаційна безпека” та “кібербезпека”, суперечить, наприклад вимогам частини 3 статті 8 Закону України “Про основні засади забезпечення кібербезпеки України”, де, зокрема зазначено [2]:

“3. Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов’язкових вимог інформаційної безпеки об’єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти критичної інформаційної інфраструктури;

7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту”.

Тому обґрунтовуючи дієвість визначених шляхів функціонування національної системи кібербезпеки та проблеми на напрямку її становлення і розвитку, введення нового терміну “орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам” є передчасним і таким, що не відповідає вимогам єдиного понятійного апарату та чітким критеріям міжнародних стандартів Європейського Союзу.

Введення у сферу стандартизації на законодавчому рівні, зокрема, словосполучення “стандартизація у сфері кіберзахисту” без урахування “стандартизації у сфері кібербезпеки”, а також терміну “орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам – науково-дослідна, науково-виробнича чи інша установа

або організація Державної служби спеціального зв'язку та захисту інформації України [6], до функцій якого віднесено розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення, запровадження та застосування стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам", який містить вимогу щодо безпосередньої належності такого органу стандартизації тільки до Державної служби спеціального зв'язку та захисту інформації України, суперечить, наприклад, вимогам Плану реалізації Стратегії кібербезпеки України, що схвалений рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України", яке уведене в дію Указом Президента України від 1 лютого 2022 р. № 37/2022. У розділі "Ціль К.3. Безпечні цифрові послуги", пункт 65 цього Плану має таку редакцію[4]:

"65. Розробити національні стандарти у сфері кібербезпеки, організаційні та технічні вимоги, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів".

При цьому, відповідальними за виконання визначена не тільки Адміністрація Державної служби спеціального зв'язку та захисту інформації України, а ще й Міністерство економіки України та основні суб'єкти національної системи кібербезпеки.

У той же час, до сфери управління Міністерства економіки України належить "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості". А згідно до вимог розпорядження Кабінету Міністрів України від 26 листопада 2014 р. № 1163-р "Про визначення державного підприємства, яке виконує функції національного органу стандартизації", державне підприємство "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" виконує функції національного органу стандартизації (зокрема, наприклад, в рамках групи стандартизації "35.030 Безпека інформаційних технологій"). Також, вважається недоцільним судження, що тільки установа або організація Державної служби спеціального зв'язку та захисту інформації України може виконувати функції органу стандартизації у сферах, що розглядаються в проєкті Закону. За різними, окремими, науковими напрямами, різні науково-дослідні та навчальні центри мають, наприклад, різний рівень акредитації, а також фахівців і науковців різного рівня підготовки.

На підтвердження зазначеного, наприклад, у розділі “Ціль В.2. Формування нової моделі відносин у сфері кібербезпеки” вищевказаного “Плану реалізації Стратегії кібербезпеки України”, пункт 77 має таку редакцію [3]:

“77. Залучати на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення проектів нормативно-правових актів, нормативних документів та стандартів у цій сфері.

Відповідальні за виконання: Кабінет Міністрів України, Національний координаційний центр кібербезпеки, основні суб’єкти національної системи кібербезпеки”.

Також, у розділі “Ціль В.3. Прагматичне міжнародне співробітництво” вищевказаного “Плану реалізації Стратегії кібербезпеки України”, пункт 88 має таку редакцію:

“88. Поглибити співпрацю з Міжнародним союзом електрозв’язку у сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації у цих сферах.

Відповідальні за виконання: Адміністрація Державної служби спеціального зв’язку та захисту інформації України, Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації”.

Отже, підсумовуючи слід погодитись, що деталізоване і всеохоплююче нормативне регулювання у сферах кіберзахисту [1], технічного та криптографічного захисту інформації, протидії технічним розвідкам з урахуванням сучасних міжнародних стандартів з питань кібербезпеки є вкрай важливим.

Тому створення умов для регулювання питань стандартизації у сферах кіберзахисту, криптографічного та технічного захисту інформації, протидії технічним розвідкам актами спеціального законодавства є суттєвим завданням. Розробка та впровадження правових основ для подолання викликів та загроз національній безпеці держави в умовах стрімкого розвитку цифрових технологій та виникнення кіберзагроз забезпечить дієву вертикаль нормативного та стандартизованого регулювання взаємовідносин в цілому.

Висновки з цього дослідження і перспективи подальших розвідок у цьому напрямі. На підставі цього робиться висновок про те, що уточнення механізмів регулювання питань стандартизації у сферах кіберзахисту, криптографічного та технічного захисту інформації, протидії технічним розвідкам актами спеціального законодавства є вкрай важливим питанням.

При цьому, в розглянутому проєкті Закону існує ряд труднощів у визначенні чіткого змістовного навантаження запропонованого понятійного апарату. Відтак, окреме введення механізмів стандартизації на законодавчому рівні тільки таких сфер, як: “криптографічний захист інформації”, “технічний захист інформації”, “кіберзахист”, “протидія технічним розвідкам”, без розгляду безпосередньо пов’язаних із ними набагато ширшого спектру дій на теоретичному та практичному рівні таких галузей, як “електронні комунікації”, “інформаційна безпека” та “кібербезпека” дозволить уникнути певних труднощів щодо розбіжностей у існуючій та опрацьовуючій єдиній понятійно-категоріальній основі держави.

Наступне, статус, повноваження та призначення “Українського науково-дослідного і навчального центру проблем стандартизації, сертифікації та якості” безпосередньо передбачає виконання функцій національного органу стандартизації у відповідних сферах, що набагато вагоміше, ніж правові основи організації та діяльності Державної служби спеціального зв’язку та захисту інформації України.

Отже, прийняття проєкту Закону України “Про внесення змін до деяких законів України щодо стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам” реєстраційний № 6568 від 28 січня 2022 р. має суттєвий характер щодо створення правових основ для подолання викликів та загроз національній безпеці держави в умовах стрімкого розвитку цифрових технологій та виникнення кіберзагроз за умов його коректного переопрацювання, внесенням відповідних змін у зміст та тлумачення понятійного апарату.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про криптографічний та технічний захист інформації : пояснювальна записка до Проекту Закону України реєстраційний № 6568 від 28.01.2022 р. URL : http://search.ligazakon.ua/l_doc2.nsf/link1/GI06877A.html (дата звернення: 10.04.2022).

2. Про основні засади забезпечення кібербезпеки України : Закон України. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.04.2022).

3. Про Стратегію кібербезпеки України : Указ Президента України "Про рішення Ради національної безпеки і оборони України" від 14 травня 2021 року. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 18.04.2022).

4. Про План реалізації Стратегії кібербезпеки України : Указ Президента України "Про рішення Ради національної безпеки і оборони України" від 30 грудня 2021 р. URL : https://zakon.rada.gov.ua/laws/show/37/2022#Text (дата звернення: 18.04.2022)

5. Про прийняття нормативних документів України, гармонізованих з міжнародними та європейськими нормативними документами, скасування національних стандартів України (із змінами) : Наказ ДП "Український науково-дослідний і навчальний центр проблем

стандартизації, сертифікації та якості" від 18.12.2015 р. № 193. URL : https://docs.dtkt.ua/download/pdf/1041.73996.6 (дата звернення: 15.04.2022).

6. Про внесення змін в деякі закони України відносно стандартизації в сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам : Проект Закону України реєстраційний № 6568 від 28.01.2022 р. URL : http://search.ligazakon.ua/l_doc2.nsf/link1/JI06877A.html (дата звернення: 15.04.2022).

Стаття надійшла до редакції 10.05.2022 р.
Стаття рекомендована до друку 06.06.2022 р.

Zhyvylo Ye. O.
PhD in Public Administration,
Head of the Department of Communications and Automated Control Systems of the Institute of Troops (Forces) and Information Technologies of the Ivan Chernyakhovsky National University of Defense of Ukraine, Kiev, Ukraine
https://orcid.org/0000-0003-4077-7853

DEFINING ISSUES OF CRYPTOGRAPHIC AND TECHNICAL INFORMATION SECURITY, CYBERSECURITY AND COUNTERING TECHNICAL INTELLIGENCE

Abstract. Today, the implementation of measures for cybersecurity of information and communication systems and critical infrastructure of the state, countering and responding to computer incidents and cyber influences - remains one of the major tasks in the field of information security and cybersecurity of the state.

Defining the directions of Ukraine's foreign policy in the field of cybersecurity, the Strategy establishes that Ukraine will intensify its participation and partnership in international processes of standardization and certification in the field of cybersecurity, increase its "presence" in international, regional and other standardization bodies and institutes and certification of this area in the geopolitical sense.

Based on the need for scientific substantiation of the institutional framework for the development of cybersecurity, special attention should be paid to the development of standards in the field of new IT technologies (including artificial intelligence, cloud databases, quantum computing and communications) and basic Internet architecture.

The review of the problem field of research shows that in general the Internet should be comprehensive and open, the technologies supported and used in it should be focused on the person, his basic freedoms, guarantee neutrality to his privacy, ensure his privacy in cyberspace, and any restrictions should be carried out only in accordance with laws and regulations (standards). Ukraine's position is that the use of certain technological processes should be legal and safe, in accordance with existing ethical standards.

Current laws and regulations of the state, current national standards, including those developed and implemented, have been formulated taking into account promising areas of development of mechanisms for institutional support of cyber security and based on Euro-Atlantic experience. This allowed them to be implemented quite effectively in the regulatory framework of Ukraine.

Nevertheless, during the analysis and generalization of theoretical approaches to the essence and content of some definitions, experts came to the appropriate legal conflict, namely that national standards contain requirements in partially similar areas of Ukrainian society, only with other names, such as: "information security", "information technology security", and "cybersecurity".

Thus, the author considers in detail the theoretical and practical significance of the draft Law of Ukraine "On Amendments to Some Laws of Ukraine on Standardization in the Areas of

Cryptographic and Technical Protection of Information, Cyber Security, Counteraction to Technical Intelligence" at the initiative of MPs Fedienko O.P., Klochko A. and others, registration number 6568 of "28" January 2022 (first reading).

Therefore, based on the implemented Cyber Security Strategy, which entered into force on 28.08.2021 and it is obvious that in the process of achieving its goals requires a systematic approach, the issue of legislation and standardization in cyber security and defining a specific subject of standardization in this area is extremely important.

Keywords: cyber threats, national cybersecurity system, standardization, capabilities of the national cybersecurity system, normative legal act, normative document.

REFERENCES

1. Pro kryptohrafichnyi ta tekhnichnyi zakhyst informatsii: poiasniuvalna zapyska do Proektu Zakonu Ukrainy reiestratsiinyi № 6568 vid 28.01.2022 r. URL : http://search.ligazakon.ua/l_doc2.nsf/link1/GI06877A.html.

2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

3. Pro Stratehiiu kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text.

4. Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 hrudnia 2021 r. URL : https://zakon.rada.gov.ua/laws/show/37/2022#Text.

5. Pro pryiniattia normatyvnykh dokumentiv Ukrainy, harmonizovanykh z mizhnarodnymy ta yevropeiskymy normatyvnymy dokumentamy, skasuvannia natsionalnykh standartiv Ukrainy (iz zminamy): Nakaz DP «Ukrainskyi naukovo-doslidnyi i navchalnyi tsentr problem standartyzatsii, sertyfikatsii ta yakosti» vid 18.12.2015 r. № 193. URL : https://docs.dtkt.ua/download/pdf/1041.73996.6.

6. Pro vnesennia zmin v deiaki zakony Ukrainy vidnosno standartyzatsii v sferakh kryptohrafichnoho ta tekhnichnoho zakhystu informatsii, kiberzakhystu, protydii tekhnichnym rozvidkam: Proekt Zakonu Ukrainy reiestratsiinyi № 6568 vid 28.01.2022 r. URL : http://search.ligazakon.ua/l_doc2.nsf/link1/JI06877A.html.

The article was received by the editors 10.05.2022.
The article is recommended for printing 06.06.2022.