МОДЕЛІ ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ГАРАНТУВАННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

МАЄТНИЙ Михайло Ігорович - науковий співробітник, Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

https://orcid.org/0000-0001-9123-0706

УДК 351.862:340.13
DOI 10.32782/EP.2021.2.13

Стаття присвячена дослідженню проблематики формування та реалізації моделей правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури. Метою статті є дослідження особливостей моделей правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури. Визначено, що зміни, які сформували у суспільстві інформаційно-комунікативні технології, привели до трансформації підходів щодо реалізації функцій безпеки державою. Особливо важливим стали питання пошуку моделей правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури. Виходячи з необхідності удосконалення правового регулювання сфери гарантування кібербезпеки, проаналізовано сучасний стан нормативно-правових актів у сфері гарантування безпеки критичної інформаційної інфраструктури в Україні. З'ясовано, що відповідно до Національного індексу кібербезпеки, який у т. ч. аналізує стан чинного законодавства, значного прогресу у рейтингу Національного індексу кібербезпеки за 2019-2021 рр. Україна не досягла. Визначено гарантування показників кібербезпеки Україною та можливості для подальшого розвитку. Обґрунтовано актуальні напрями формування правового гарантування сфери гарантування безпеки критичної інформаційної інфраструктури: прийняття Стратегії кібербезпеки України; прийняття законодавчих актів, що регулюватимуть функціонування безпечного кіберсередовища та інформаційної інфраструктури; прийняття законодавчих актів щодо боротьби з кіберзлочинністю, розширення міжнародного співробітництва у сфері боротьби з кіберзлочинами, стимулювання нарощення фахового потенціалу у сфері захисту критичної інформаційної інфраструктури.

Ключові слова: правове регулювання, інформаційна інфраструктура, державна політика, критична інфраструктура, кібербезпека.

Постановка проблеми

У сучасному світі одним з ключових драйверів розвитку стали інформаційно-комунікативні технології, які формують нові параметри технологічних, виробничих та суспільних відносин. Значний вплив цифрових технологій на людську діяльність створює додаткові можливості в розвитку держави, економічної та соціальної систем, перетвореннях процесів управління та реалізації безпеки. У міру посилення проникнення цифрових технологій у процеси реалізації основних економічних процесів, виникають нові ризики, що несуть у собі як локальну, так і глобальну небезпеку. Усе більшої важливості набувають питання, пов'язані із захистом критичної інформаційної інфраструктури.

Розповсюдженість інформаційно-комунікативних технологій породжує суттєву залежність держави, підприємств, інфраструктурних об'єктів від зовнішніх несанкціонованих втручань з метою вчинення злочинів,

атак, шахрайств та терористичних актів. Сьогоднішні масштаби негативного впливу на системи забезпечення безпеки вийшли на міжнародний рівень, коли за допомогою втручань в інформаційну інфраструктуру проводиться гібридна інформаційна війна.

Посилення, кількість, а також масштабність зазначених загроз прискорило впровадження правових механізмів, які регулюють інформаційну безпеку як складову частину у системі національної безпеки держави. Значної актуальності набувають питання реалізації інформаційної безпеки об'єктів критичної інфраструктури – національної, регіональних і галузевих інформаційних систем, що інтегровані у важливі об'єкти економічної сфери та напрямів, пов'язаних із забезпеченням безпеки держави.

Аналіз останніх досліджень і публікацій

Низку питань, пов'язаних з моделями правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури розглядали у своїх працях вітчизняні та зарубіжні дослідники, а саме: О. Бакалінська, О. Бакалинський, А. Карцхія, П. Кірануді, К. Крістінсен, М. Латинін, Г. Макаренко, К. Петерсен, А. Петров,- А. Саррі, М. Сергін та ін. Враховуючи особливу важливість для функціонування держави, суспільства, систем підтримання життєдіяльності, безпечного господарювання важливим є дослідження особливостей формування та реалізації моделей правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури. Зазначене передбачає потребу аналізу правових аспектів та регулювання, що виникають у процесі реалізації функцій безпеки критичної інформаційної інфраструктури.

Мета статті

Метою статті є дослідження особливостей моделей правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури.

Виклад основного матеріалу

Сучасна діяльність держави, суб'єктів господарювання, громадян, різноманітних об'єднань, інфраструктурних об'єктів поступово втрачає повноцінне існування без взаємодії зі сферою інформаційно-комунікативних технологій (ІКТ). Подальший розвиток промислової революції, в основі якої знаходиться інтенсивне використання інформаційно-комунікаційних зв'язків, віддалених з'єднань, засобів обробки та зберігання інформації, потребує забезпечення державою чіткого бачення загроз та скоординованих дій щодо реалізації функцій безпеки [1]. Виходячи з викладеного, реалізація складних завдань у сфері гарантування безпеки інформаційної інфраструктури знаходиться як у технічній так і в правовій площині. В умовах «цифрової революції» сфера права змінюється та розширюється під впливом можливостей сучасних цифрових технологій, що знаходить відображення в безлічі нових правових явищ, пов'язаних з появою нових суб'єктів і об'єктів правового регулювання, специфікою правовідносин у цифровій реальності, осмислення поняття та змісту цифрових прав [2]. Правові заходи відіграють ключову роль у запобіганні кіберзлочинності та боротьби з нею, включаючи кримінальну відповідальність, процесуальні повноваження, визначені моделі міжнародного співробітництва, відповідальність приватних операторів інтернет-мережі.

Питання проблематики кібербезпеки постало як ніколи актуально, особливо у контексті об'єднання зусиль виробників і користувачів інформації різних форм власності. К. Шваб наголосив на необхідності спільними зусиллями держави, бізнесу та громадянського суспільства підтримувати безпеку та надійність державних функцій, комунікацій та особистої інформації, що знаходиться та переміщується на цифрових платформах [3].

Дані, які свідчать про вплив сторонніх осіб на інформацію, з кожним днем кількісно зростають. Лише в першій половині 2018 р. було порушено більш ніж 4,5 млрд записів [4]. Кожну секунду створюються чотири нові шкідливі програми. У доповіді Центру стратегічних та міжнародних досліджень (CSIS) та McAfee зазначається, що в 2017 р. кіберзлочинність вартувала світові майже 600 млрд дол витрат, або 0,8 % світового ВВП, у той час як у 2014 р. глобальні збитки ста-

новили близько 500 млрд дол, або 0,7% світового ВВП [5]. За інформацією Світового економічного форуму, проблеми у гарантування кібербезпеки залишається ключовим у сприйнятті глобальних ризиків. Враховуючи наслідки COVID-19, прискорення четвертої промислової революції, розширилася цифровізація людської взаємодії, електронна комерція, онлайн-освіта та віддалена робота. Швидке прискорення автоматизації, маніпулювання інформацією, прогалини в технологічному регулюванні та прогалини в технологічних навичках та можливостях посилить проблематику реалізації кібербезпеки. Очікується, що держави та недержавні суб'єкти у майбутньому братимуть участь у все більш небезпечних кібератаках [6].

Застаріла цифрова інфраструктура, відсутність сучасних технологічних рішень та програмних засобів захисту дозволяє стороннім суб'єктам вчиняти доступ до державної інформації з обмеженим доступом, контролювати роботу критично важливих мереж та фінансових рахунків. Наприклад, використання кіберзлочинцями Штучного Інтелекту (Artificial Intelligence) може створити ризики, які полягають у наступних ключових проблемах кібербезпеки: збільшення складності кібератак; асиметрія дій – кібератаки/захист; збільшення поверхні атаки/операції оцифрування; балансування ризиків та експлуатаційних можливостей [7].

Вітчизняний досвід визначення поняття критичної інфраструктури спирається на низку як прийнятих законодавчих актів, так і розроблених законопроєктів. Так, у проєкті Закону України «Про критичну інфраструктуру та її захист» під критичною інфраструктурою передбачалося визначити стратегічно важливу для економіки та національної безпеки сукупність об'єктів, порушення діяльності яких може зашкодити ключовим національним інтересам [8].

Законом України «Про основні засади забезпечення кібербезпеки України» сформульовано визначення критичної інформаційної інфраструктури як сукупності об'єктів критичної інформаційної інфраструктури. Крім того, об'єктами критичної інфраструктури є підприємства, організації та установи різних форм власності, які здійснюють безпосередньо технологічні процеси, надають послуги, важливі для економічної та промислової сфери, життєдіяльності суспільства та безпеки населення, припинення або порушення роботи яких може погіршити стан національної безпеки й оборони України, екологічні показники, заподіяти майнову шкоду, загрожувати людському життю та здоров'ю [9].

У Стратегії розвитку інформаційного суспільства в Україні інформаційну інфраструктуру запропоновано розглядати як поєднані різноманітні інформаційні (автоматизовані) системи, інформаційні ресурси, телекомунікаційні мережі та канали передавання даних, комунікаційних засобів і управління потоками інформації, а також організаційно-технічні структури та механізми забезпечення їх функціонування [10].

Посилила правове регулювання сфери гарантування безпеки критичної інформаційної інфраструктури України прийнята Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [11], що визначила загальні вимоги до системи кіберзахисту об'єктів критичної інфраструктури; встановила обов'язкові заходи забезпечення захисту від кібератак; окреслила дії по запобіганню порушення конфіденційності, цілісності та доступності інформаційних ресурсів та ін. У проєкті Закону України «Про національну безпеку України» передбачалося, що комплексний огляд сектору безпеки й оборони повинен включати, крім іншого, проведення огляду стану кіберзахисту інформаційних ресурсів держави та критичної інформаційної інфраструктури [12].

Закон України «Про основні засади забезпечення кібербезпеки України» [9] та Стратегія кібербезпеки України [13] сформували основи моделі взаємодії суб'єктів гарантування кібербезпеки та розподіл завдань та повноважень, що реалізують Національний координаційний центр кібербезпеки, Державна служба спеціального зв'язку та захисту інформації, Міністерство оборони, Генеральний штабом Збройних Сил, Служба безпеки, Національна поліція, Національний банк, розвідувальні органи України, діяльність яких має гарантувати кібербезпеку та

взаємопов'язані політичні, науково-технічні, інформаційні, освітні, організаційні, правові, оперативно-розшукові, розвідувальні, контррозвідувальні, оборонні, інженерно-технічні заходи, та криптографічний та технічний захист національних інформаційних ресурсів, кіберзахист об'єктів критичної інформаційної інфраструктури [14].

Багато країн світу адаптували чинне законодавство, запровадивши положення, які розширюють чинні закони, включаючи злочинну діяльність, що здійснюється в Інтернеті або сприяє використанню ІКТ. Незважаючи на широкий спектр зусиль, спрямованих на створення сприятливого правового середовища для боротьби з кіберзлочинністю, залишаються труднощі щодо забезпечення належних правових рамок. Ці проблеми включають, серед іншого, потреби: розробки сучасного та чіткого законодавства про кіберзлочинність після визнання зловживання новою технологією та виявлення прогалин у кримінальному законодавстві; розробки процедур електронних доказів; забезпечення криміналізації нових видів злочинів в Інтернеті; впровадження нових інструментів розслідування у відповідь на збільшення використання правопорушниками ІКТ для підготовки та виконання своїх правопорушень; баланс безпеки та прав [15].

Питання обліку об'єктів критичної інформаційної інфраструктури було унормовано постановою Кабінету Міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» [16], яка визначила механізми формування національного та секторальних переліків об'єктів критичної інформаційної інфраструктури та особливості внесення у державний реєстр об'єктів критичної інформаційної інфраструктури.

Важливим питанням є оцінка дій держави, спрямована на забезпечення безпеки інформаційної інфраструктури. У якості незалежної міжнародної оцінки можна звернутися до сучасних міжнародних індексів, які характеризують стан реалізації зазначеного питання. Одним із відомих глобальних індексів є Національний індекс кібербезпеки (NCSI), який вимірює готовність країн запобігати кіберзагрозам і управляти кіберінцидентами. NCSI фокусується на вимірних аспектах кібербезпеки, що реалізуються державою: чинне законодавство (правові акти, постанови, накази); адміністративно-суб'єктні структури (сучасні організації, департаменти); формати

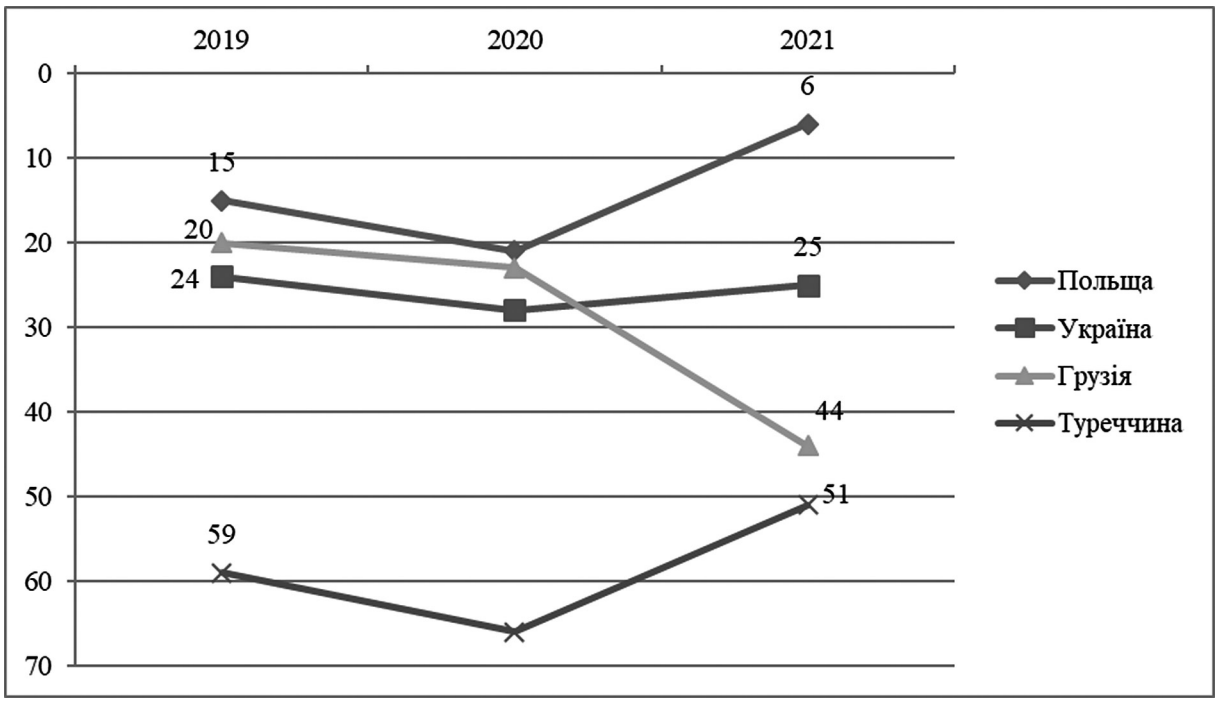

Рис. 1. Динаміка місць у рейтингу окремих країн світу за Національним індексом кібербезпеки, 2019-2021 рр. [18]

співпраці (комітети, робочі групи); результати (політики, технології, програми) [17].

На рис. 1 показана динаміка рейтингу окремих країн світу за Національним індексом кібербезпеки. У 2021 р. Україна отримала 25 місце з індексом 68,83 серед 160 країн у рейтингу Національного індексу кібербезпеки [18]. На жаль, як бачимо з рис. 1, за 2019-2021 рр. значного прогресу у рейтингу Національного індексу кібербезпеки Україна не досягла.

Якщо детально дослідити аспекти показників кібербезпеки України у 2020 р. (рис. 2), то слід зазначити, що реалізацію розробки політики кібербезпеки, захист особистих даних та боротьбу з кіберзлочинністю оцінено у 100%, у той же час, внесок держави у глобальну кібербезпеку отримав 33%, військові кібероперації – 17%, а управління кіберкризою у 0%. Зазначене передбачає потребу в удосконаленні нормативно-правової бази відповідно до питань, які найменш розвинені у сфері забезпечення кібербезпеки.

Дослідження Національних стратегій кіберзахисту (NCSS) та опитування, яке було проведено в 14 державах-членах ЄС, висвітлили стратегічні цілі в галузі кібербезпеки [19]. Визначено, що Національні стратегічні цілі, які передбачають необхідні напрями розвитку кібербезпеки в державах-членах ЄС, найбільш повно реалізують питання, спрямовані на інформування громадян, стимулювання НДДКР та збільшення навчальних та освітніх програм у сферах, пов'язаних із забезпеченням кібербезпеки, що актуально і для України.

Виходячи з викладеного бачення не в повній мірі сформованого нормативно-правового регулювання безпеки критичної інформаційної інфраструктури, дієва модель правового регулювання у сфері гарантування безпеки критичної інформаційної інф-

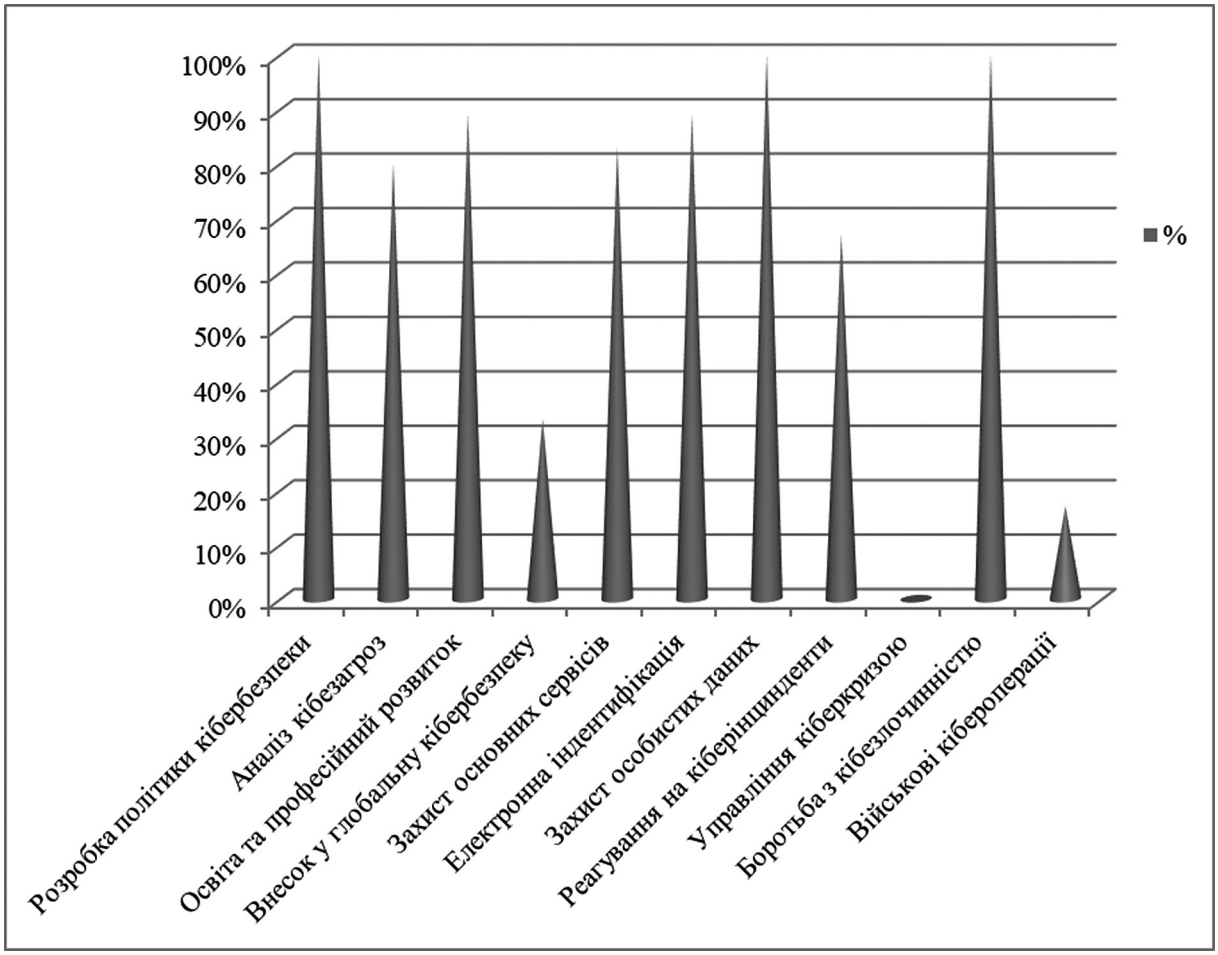

Рис. 2. Відсоток досягнення показників кібербезпеки Україною за даними Національного індексу кібербезпеки, 2020 р. [18]

раструктури має передбачати у своїй основі удосконалення підходів до питань безпеки та заміну існуючої Стратегії кібербезпеки [13] актуальним стратегічним законодавчим актом, що спрямований на формування можливостей для підтримки безпеки у сфері функціонування інформаційно-комунікативних технологій, інформаційної інфраструктури; встановлення актуального суб'єкт-об'єктного складу у системі кібербезпеки; регулювання діяльності суб'єктів забезпечення кібербезпеки та їх обов'язків на основі транспарентності та заходів попереджувального характеру щодо протиправної діяльності в кіберпросторі. Хоча зазначені підходи поступово реалізуються – фахівцями розроблено проєкт Стратегії кібербезпеки України на 2021-2025 рр. [20], яка спирається на засади кіберстійкості, стримування та взаємодії, але на сьогодні вказаний документ не прийнято.

Наступним етапом є питання розроблення нормативно-правової бази, яка регулює засоби захисту органів публічної влади, юридичних та фізичних осіб від кіберзлочинності та формування безпечного кіберсередовища та надійного функціонування інформаційної інфраструктури. Окремим аспектом вбачається розвиток сфери боротьби з кіберзлочинністю на основі внесення змін в чинні законодавчі акти та розроблення нових (кримінальний кодекс, законодавство щодо діяльності інформаційної інфраструктури, банківською діяльністю та ін.). У подальшому необхідним стає приведення законодавства з чинними міжнародними нормами та стандартами, ратифікація міжнародних угод щодо боротьби з кіберзлочинністю та захистом інформаційної інфраструктури.

Моделі правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури передбачає розроблення базових вимог до відповідної інфраструктури та реалізації безпеки; правового визначення системи загальної координації гарантування безпеки; прийняття державної програми щодо підготовки фахівців у сфері захисту критичної інформаційної інфраструктури.

Висновки

Отже, за результатами дослідження визначено, що інформаційно-комунікативні технології формують нові підходи до організації суспільної діяльності. Проникнення цифрових технологій у системи управління, виробництва, забезпечення життєдіяльності, вільного переміщення інформації передбачає підвищену увагу до реалізації державою функцій безпеки. Особливо актуальними є питання правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури.

У дослідженні проаналізований сучасний стан правового регулювання у сфері гарантування безпеки критичної інформаційної інфраструктури в Україні та аспекти показників кібербезпеки України відповідно до рейтингу Національного індексу кібербезпеки, визначено досягнення показників кібербезпеки Україною. Обґрунтовано необхідні напрями забезпечення правового регулювання шляхом прийняття Стратегії кібербезпеки України та інших законодавчих актів, що мають регулювати функціонування безпечного кіберсередовища та інформаційної інфраструктури; удосконалюють сферу боротьби з кіберзлочинністю; розширюють міжнародне співробітництво у сфері боротьби з кіберзлочинами; стимулюють нарощення фахового потенціалу у сфері захисту критичної інформаційної інфраструктури.

Література

1. Kruhlov V., Latynin M., Horban A., Petrov A. Public-Private Partnership in Cybersecurity. *CEUR Workshop Proceedings*. 2020. Vol. 2654. P. 619–628.

2. Карцхия А. А., Макаренко Г. И., Сергин М. Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права. *Вопросы кибербезопасности*. 2019. №. 3 (31). С. 18–23.

3. Schwab K. The fourth industrial revolution. New York, Currency Books, 2017. 192 p.

4. 2018: Data Privacy and New Regulations Take Center Stage. Gemalto, 2018. URL: https://www.privacyitalia.eu/wp-content/uploads/2018/10/breach-level-index-report-h1-2018.pdf.

5. Economic Impact of Cybercrime – No Slowing Down. McAfee, 2018. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

6. The Global Risks Report 2021. 16th Edition. WEF: Geneva, 2021. 96 p.

7. AI is the latest weapon cybercriminals are exploiting. WEF. URL: https://www.weforum.org/agenda/2019/09/4-ways-ai-is-changing-cybersecurity-both-in-attack-and-defense/.

8. «Про критичну інфраструктуру та її захист»: проект Закону України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.

9. «Про основні засади забезпечення кібербезпеки України»: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

10. «Про схвалення Стратегії розвитку інформаційного суспільства в Україні»: розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#n8.

11. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»: постанова Кабінету Міністрів України від 19.06.2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

12. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. 2019. № 9. С. 100–107.

13. «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. №96/2016. URL: https://www.president.gov.ua/documents/962016-19836.

14. «Про національну безпеку України»: проєкт Закону України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6353115.

15. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. World Bank and United Nations, 2017. 482 p.

16. «Деякі питання об'єктів критичної інформаційної інфраструктури»: постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text.

17. Methodology. NCSI. URL: https://ncsi.ega.ee/methodology/.

18. National Cyber Security Index. URL: https://ncsi.ega.ee/compare/.

19. Sarri A., Kyranoudi P. Good practices in innovation under NCSS. ENISA, 2019. 44 p.

20. Проєкт Стратегії кібербезпеки України на 2021-2025 рр. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

Maietnyi Mykhailo, *Researcher*
The Ukrainian scientific and research Institute of special equipment and forensic of the Security Service of Ukraine

MODELS OF LEGAL REGULATION IN THE FIELD OF SAFETY OF CRITICAL INFORMATION INFRASTRUCTURE

The article deals with the study of the formation and implementation of models of legal regulation in the field of security of critical information infrastructure. The purpose of the article is to study the features of legal regulation models in the field of security of critical information infrastructure. It is determined that the changes that form information and communication technologies in society have led to the transformation of approaches to the implementation of security functions by the state. The search for legal regulation models in the field of critical information infrastructure security has become of great significance. Based on the need to improve the legal regulation of cybersecurity, the current state of regulations in the field of critical information infrastructure security in Ukraine has been analyzed. It is found out that according to the National Cyber Security Index, which also analyzes the state of current legislation, Ukraine has not made distinguished progress in the ranking of the National Cyber Security Index for 2019-2021.

The provision of cyber security indicators to Ukraine and opportunities for further development have been identified. The current directions of forming legal support in the field of security of critical information infrastructure have been substantiated: adoption of the Cyber Security Strategy of Ukraine; adoption of legislation that will regulate the functioning of a secure cyber environment and information infrastructure; adoption of legislation on combating cybercrime, expanding international cooperation in the fight against cybercrime, stimulating the development of professional capacity in the field of critical information infrastructure protection.

Keywords: *legal regulation, information infrastructure, state policy, critical infrastructure, cybersecurity.*