Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України

Legal Support of Cybersecurity of Critical Information Infrastructure of Ukraine

Мирослав Ковалів [1], **Руслан Скриньковський** [2], **Юрій Назар** [1], **Сергій Єсімов** [1], **Іван Красницький** [1], **Христина Кайдрович** [2], **Святослав Князь** [3], **Юлія Кемська** [3]

Myroslav Kovaliv, Ruslan Skrynkovskyy, Yurii Nazar, Serhii Yesimov, Ivan Krasnytskyi, Khrystyna Kaydrovych, Sviatoslav Kniaz, Yuliia Kemska

[1] *Lviv State University of Internal Affairs*
26 Horodotska Street, Lviv, 79007, Ukraine

[2] *Lviv University of Business and Law*
99 Kulparkivska Street, Lviv, 79021, Ukraine

[3] *Lviv Polytechnic National University*
12 Stepana Bandery Street, Lviv, 79013, Ukraine

DOI: 10.22178/pos.69-12

JEL Classification: H56, K39

Received 29.03.2021
Accepted 26.04.2021
Published online 30.04.2021

Corresponding Author:
Myroslav Kovaliv
mkovaliv1@ukr.net

Анотація. У статті на основі методології системного підходу представлено дослідження теоретико-правових засад правового забезпечення кібербезпеки критичної інформаційної інфраструктури України. Розглянуто чинне законодавство та проаналізовано підзаконні нормативно-правові акти України у галузі кібербезпеки критичної інформаційної інфраструктури. Зазначено, що сьогодні в Україні важливо забезпечити ефективне управління регіональними системами захисту інформації, а також безперебійне і ефективне функціонування об'єктів інформаційної інфраструктури, особливо – критичної інфраструктури. Для того, щоб домогтися цих результатів на практиці, необхідно на перший план поставити реалізацію таких основних завдань, як розвиток кадрового потенціалу в галузі забезпечення кібербезпеки і розвиток національної галузі інформаційних технологій. Обґрунтовано, що проблема забезпечення кібербезпеки вимагає вдосконалення правових, організаційних і технічних механізмів регулювання суспільних відносин, що виникають в інформаційній сфері. Зроблено висновок про те, що забезпечення кібербезпеки критичної інформаційної інфраструктури України можливе шляхом: визначення об'єктів даної структури, вирішення проблем кібербезпеки об'єктів з дуже довгим життєвим циклом, розробки методики модернізації критичної інформаційної інфраструктури для кожної організації, технології та інформаційної структури, які є об'єктами критичної інформаційної інфраструктури.

Ключові слова: кібербезпека; критична інфраструктура; інформаційна інфраструктура; правове регулювання; комп'ютерні інциденти.

Abstract. The article presents a study of the theoretical and legal foundations of the legal support of cybersecurity of the critical information infrastructure of Ukraine based on the system approach methodology. The current legislation is considered, and the bylaws of Ukraine in the field of cybersecurity of critical information infrastructure are analyzed. It is noted that today in Ukraine, it is important to ensure effective management of regional information security systems and the smooth and efficient operation of information infrastructure, especially critical infrastructure. To achieve these results in practice, it is necessary to prioritize implementing such critical tasks as the development of human resources in cybersecurity and the development of the national field of information technology. It is substantiated that cybersecurity is required to improve legal, organizational, and technical mechanisms

for regulating public relations that arise in the information sphere. It is concluded that cybersecurity of critical information infrastructure of Ukraine is possible by identifying objects of this structure, solving problems of cybersecurity of objects with a very long life cycle, developing methods of modernization of critical information infrastructure for each organization, technology and information structure, which are the objects of critical information infrastructure.

Keywords: cybersecurity; critical infrastructure; information infrastructure; legal regulation; computer incidents.

ВСТУП

Правове регулювання створення і використання інформаційної інфраструктури в Україні безпосередньо пов'язане з правовим забезпеченням безпеки усіх учасників цього процесу (інформаційних відносин). Організація нових форм взаємодії державних органів влади з фізичними і юридичними особами повинна здійснюватися за певними стандартами електронних форм взаємодії. Використання інформаційної інфраструктури створює суспільні відносини, регулювання яких має здійснюватися за допомогою правових норм, а розробка, прийняття, застосування і виконання обов'язкових вимог до інформаційних технологій має здійснюватися на основі норм технічного регулювання. Інформаційні відносини, які виникають при використанні цифрових технологій, вимагають: визначення державного підходу до правового регулювання поданих відносин; розробки методології забезпечення інформаційної безпеки інформаційної інфраструктури та її користувачів. У цьому випадку формування національного законодавства в галузі створення і використання інформаційної інфраструктури є невідкладним завданням будь-якої держави, включаючи Україну.

Проблеми правового забезпечення кібербезпеки критичної інформаційної інфраструктури України неодноразово знаходили відображення у працях О. Баранова, П. Гарасима, К. Бєлякова, С. Божок, І. Діордіци, В. Ліпкана, Н. Коваленка, Б. Кормича, І. Кушнір, О. Малашка, Ю. Максименка, М. Микитюка, Л. Сопільника, М. Стрельбіцького, О. Тихомиров, О. Юдіна та ін. Визнаючи теоретичну і практичну цінність окремих досліджень за проблемою, доцільно відмітити, що у наукових і навчально-методичних працях вищезгаданих та інших українських вчених-юристів існує цілий ряд дискусійних питань і розбіжностей у поглядах щодо вирішення наукових і практичних проблем у сфері правового забезпечення кібербезпеки критичної інформаційної інфраструктури України.

Метою статті є дослідження правового забезпечення кібербезпеки критичної інформаційної інфраструктури України.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У 2017 р. в Україні прийнято Закон "Про основні засади кібербезпеки України" [1], в якому визначено критично важливі об'єкти інфраструктури – "… підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей" [1].

Критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури [1]: сукупність інформаційних систем, інформаційно-телекомунікаційних мереж, автоматизованих систем управління суб'єктів критичної інформаційної інфраструктури, у тому числі мережі електрозв'язку, що використовуються для організації взаємодії таких об'єктів [2, 3, 4].

У Стратегії розвитку інформаційного суспільства в Україні [5], зазначено, що "інформаційна інфраструктура – сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних

структур, механізмів, що забезпечують їх функціонування".

З огляду на вищевказані дефініції можна стверджувати, що подані поняття є подібними, але різняться між собою. Так, критична інформаційна інфраструктура відрізняється від інформаційної інфраструктури включенням автоматизованої системи управління суб'єктів критичної інформаційної інфраструктури та систем електрозв'язку в якості об'єктів критичної інформаційної інфраструктури.

Відповідно до чинного Закону України "Про Національну програму інформатизації" [6] під об'єктом інформатизації доцільно розуміти сукупність інформаційних ресурсів, засобів і систем обробки інформації (відомостей та/або даних [7]), які використовуються відповідно до заданої інформаційної технології, засобів забезпечення, приміщень або об'єктів (будівель, споруд, технічних засобів), в яких ці засоби і системи встановлені, або приміщень і об'єктів, призначених для ведення конфіденційних переговорів [6]. До об'єктів критичної інформаційної інфраструктури доцільно віднести автоматизовані системи управління, що належать державним установам і органам влади, юридичним і фізичним особам-підприємцям, які забезпечують взаємодію зазначених систем або мереж, що функціонують у сфері охорони здоров'я, освіти і науки, транспорту, зв'язку, енергетики, банківській сфері та інших сферах фінансового ринку, паливно-енергетичного комплексу, у галузі атомної енергії, оборонної, ракетно-космічної, гірничодобувної, металургійної, хімічної промисловості і т. д.

В контексті цього з'ясовано, що тут відмінності виявляються в семантичному характері застосовуваних термінів. У Порядку формування переліку об'єктів критичної інформаційної інфраструктури, затвердженого постановою Кабінету Міністрів України від 09.10.2020 р. № 943, з метою визначення сукупності інформаційних об'єктів і ресурсів, систем і засобів обробки інформації зазначено, що "… всі об'єкти інформаційної інфраструктури (автоматизовані, інформаційні, телекомунікаційні, інформаційно-телекомунікаційні системи, автоматизовані системи управління технологічними процесами), що експлуатуються на об'єкті критичної інфраструктури", а також представлено загальні засади взаємозв'язку Національної програми інформатизації та системи планування економічного і соціального розвитку України [8]. В контексті цього доцільно також відмітити, що у Законі України "Про основні засади кібербезпеки України" [1] для визначення тих же відносин застосовується поняття "об'єкт критичної інформаційної інфраструктури". Загальне розуміння поданих відносин у вищевказаних нормативно-правових актах тотожне.

За результатами дослідження встановлено, що у Законі України "Про основні засади кібербезпеки України" [1] є певні недоліки. Зокрема, поданий Закон України [1] не визначає підстави віднесення організацій (незалежно від форми власності) до суб'єктів критичної інформаційної інфраструктури і, як наслідок, інформаційні системи, інформаційно-телекомунікаційні мережі та автоматизовані системи управління, які належать цим організаціям, виходячи із Порядку формування переліку об'єктів критичної інформаційної інфраструктури [8], також не зазначені. Така невизначеність уповільнює ідентифікацію критичних інформаційних систем і знижує рівень ефективності забезпечення безпеки.

Поряд з тим також з'ясовано, що у чинному законодавстві України існує певна неузгодженість і недоопрацювання. Так, розділ XVI "Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" Кримінального кодексу України (далі – ККУ) [9] не визначає відповідальність за заподіяння шкоди критичній інформаційній інфраструктурі України. Пов'язано це з тим, що ст. 363 "Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється" ККУ повинна охоплювати поняття заподіяння шкоди у контексті ст.ст. 113 та 114 Кримінального кодексу України [9]. Не визначення юридичної відповідальності за заподіяння шкоди критичній інформаційній інфраструктурі України у Кримінальному кодексі України є недоробкою законодавця.

Аналіз нормативно-правових документів в галузі забезпечення безпеки критичної інформаційної інфраструктури, передачі та обміну

інформації (відомостей та/або даних) у даній системі дозволяє розглянути наступну структуру органів виконавчої влади України.

Так, відповідно до ч. 1 ст. 5 Закону України "Про основні засади кібербезпеки України" [1] Президент України здійснює координацію діяльності у сфері кібербезпеки, включаючи забезпечення безпеки критичної інформаційної інфраструктури, як складової національної безпеки України (через очолювану ним Раду національної безпеки і оборони України).

Указом Президента України від 07.06.2016 р. № 242/2016 утворено Національний координаційний центр кібербезпеки та призначено керівником Центру секретаря Ради національної безпеки і оборони України [10].

Кабінет Міністрів України здійснює державний контроль у сфері безпеки критичної інформаційної інфраструктури, визначає порядок підготовки і використання ресурсів єдиної мережі електрозв'язку для забезпечення функціонування значущих об'єктів критичної інформаційної інфраструктури та механізм визначення категорій даних об'єктів.

Постановою Кабінету Міністрів України від 19.06.2019 р. № 518 визначено Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [11].

Відповідно до чинного Закону України "Про Службу безпеки України" [12], на Службу безпеки України покладено функції органу виконавчої влади, уповноваженого в галузі реагування на комп'ютерні надзвичайні події, що здійснює підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління Служби безпеки України (Ситуаційний центр забезпечення кібербезпеки Служби безпеки України).

Державна служба спеціального зв'язку та захисту інформації України забезпечує функціонування інформаційних систем, інформаційно-телекомунікаційних мереж і автоматизованих систем управління, що знаходяться на території України, в дипломатичних представництвах і консульських установах України. Державна служба спеціального зв'язку та захисту інформації України уповноважена [13]: оцінювати безпеку критичної інформаційної інфраструктури; координувати дії суб'єктів критичної інформаційної інфраструктури у сфері обміну і надання інформації про комп'ютерні інциденти, використання засобів, призначених для попередження, виявлення та ліквідації наслідків комп'ютерних атак і реагування на комп'ютерні інциденти; здійснювати правове регулювання діяльності Національного координаційного центру реагування на комп'ютерні інциденти; вносити пропозиції (рекомендації) для вдосконалення нормативно-правового регулювання.

До завдань Національного координаційного центру з комп'ютерних інцидентів віднесені забезпечення координації діяльності суб'єктів критичної інформаційної інфраструктури України з питань виявлення, попередження і ліквідації наслідків комп'ютерних атак і реагування на комп'ютерні інциденти. Передбачено також надання послуг у сфері виявлення, попередження та ліквідації наслідків комп'ютерних атак і реагування на комп'ютерні інциденти для фізичних осіб-підприємців і малого бізнесу, в тому числі для об'єктів, що не відносяться до критичної інформаційної інфраструктури.

Концепція розвитку цифрової економіки та суспільства України на 2018–2020 рр. (у принципі 7 цифровізації "Цифровізація повинна супроводжуватися підвищенням рівня довіри і безпеки") [14] передбачає, що "інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є, зокрема, передумовами одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками". Це аспект знайшов відображення у Плані заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр., а також враховано Кабінетом Міністрів України у 2021 р. в контексті розвитку цифрових інфраструктур, враховуючи розвиток національного сегмента мережі Інтернет.

16.12.2020 р. Кабінет Міністрів України затвердив Порядок функціонування Національної телекомунікаційної мережі та Правила надання послуг, які надаються з використанням Національної телекомунікаційної мережі [15]. У Порядку функціонування Національної телекомунікаційної мережі зазначено, що "… 33. Взаємодія Національної телекомунікаційної мережі з телекомунікаційною мережею

загального користування здійснюється через шлюзи (граничні маршрутизатори), на яких створено комплексну систему захисту інформації відповідно до вимог законодавства у сфері захисту інформації, кіберзахисту та охорони державної таємниці. 34. Взаємодія Національної телекомунікаційної мережі з Інтернетом здійснюється через захищені вузли доступу до Інтернету, на яких створено комплексну систему захисту інформації відповідно до вимог законодавства у сфері захисту інформації, кіберзахисту та охорони державної таємниці" [15].

Відповідно до Закону України "Про основні засади кібербезпеки України" [1] Міністерство цифрової трансформації України за погодженням з Державною службою спеціального зв'язку та захисту інформації України та Службою безпеки України визначає порядок, технічні умови установки і експлуатації засобів, призначених для пошуку ознак комп'ютерних атак в мережах електрозв'язку, які використовуються для організації і захисту взаємодії об'єктів критичної інформаційної інфраструктури. Сюди відноситься інформація: що міститься в реєстрі значущих об'єктів критичної інформаційної інфраструктури України; про відсутність необхідності присвоєння об'єкту критичної інформаційної інфраструктури однієї з категорій критичності; про виключення об'єкта критичної інформаційної інфраструктури з реєстру об'єктів критичної інформаційної інфраструктури, а також про зміну категорії, виходячи із категоризації об'єктів критичної інфраструктури; за підсумками проведення державного контролю у галузі забезпечення безпеки об'єктів критичної інформаційної інфраструктури про порушення вимог щодо забезпечення безпеки об'єктів критичної інформаційної інфраструктури, в результаті якого створюються передумови виникнення комп'ютерних інцидентів; про комп'ютерні інциденти, які пов'язані з функціонуванням об'єктів критичної інформаційної інфраструктури, включаючи дату, час, місце знаходження і/або географічне місце розташування об'єкта критичної інформаційної інфраструктури, на якому стався комп'ютерний інцидент; наявність причинно-наслідкового зв'язку між комп'ютерним інцидентом і комп'ютерною атакою; зв'язок з іншими комп'ютерними інцидентами (при наявності); склад технічних параметрів комп'ютерного інциденту; наслідки комп'ютерного інциденту; у сфері виявлення, попередження та ліквідації наслідків комп'ютерних атак і реагування на комп'ютерні інциденти, що надається суб'єктами критичної інформаційної інфраструктури і іншими суб'єктами, в тому числі іноземними та міжнародними.

Поряд з тим, Кабінет Міністрів України також затвердив Порядок ведення Державного реєстру об'єктів критичної інформаційної інфраструктури України. Цей Реєстр формується і ведеться Державною службою спеціального зв'язку та захисту інформації України з метою обліку, зберігання і надання інформації в електронному та паперовому вигляді про об'єкти критичної інформаційної інфраструктури, що належать на законних підставах суб'єктам критичної інформаційної інфраструктури.

Інформація (відомості та/або дані), яка надається суб'єктами критичної інформаційної інфраструктури, відповідно до Порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування, у Державну службу спеціального зв'язку та захисту інформації України повинна бути актуальною, повною і достовірною.

Тут доцільно також відзначити про активне формування системи правового регулювання використання критичної інформаційної інфраструктури та забезпечення інформаційної безпеки з боку України. Інформаційні війни, які відбуваються сьогодні, включаючи гібридну війну Російської Федерації проти України, передбачають не тільки воєнні дії і/чи інформаційно-психологічні операції, а також проведення кібератак. З огляду на це, формування нормативної основи забезпечення кібербезпеки має бути засноване на чіткій та зрозумілій Стратегії [16, 17, 18, 19, 20]. З'ясовано, що у Стратегії воєнної безпеки України, прийнятої 25.03.2021 р. [21], станом на сьогодні відсутні підходи до забезпечення кібербезпеки як елемента протидії бойового застосування кібератак, і це є проблемою на думку фахівців. Поряд з тим, виходячи з аналізу теорії та практики за проблемою, необхідно також грунтовно доопрацювати положення чинного кримінального законодавства України в частині визначення відповідальності за заподіяння шкоди критичній інформаційній інфраструктурі України.

ВИСНОВКИ

Інформаційна інфраструктура – це частина інформаційної сфери, яка є складно організованою системою, створюваною та функціонуючою на засадах принципів і механізмів міжнародного та національного правового регулювання суспільних відносин.

Проблема забезпечення кібербезпеки вимагає вдосконалення правових, організаційних і технічних механізмів регулювання суспільних відносин, що виникають в інформаційній сфері. Сьогодні в Україні важливо забезпечити ефективне управління регіональними системами захисту інформації, а також безперебійне і ефективне функціонування об'єктів інформаційної інфраструктури, особливо – критичної інфраструктури. Для того, щоб домогтися цих результатів на практиці, необхідно на перший план поставити реалізацію таких основних завдань, як розвиток кадрового потенціалу в галузі забезпечення кібербезпеки і розвиток національної галузі інформаційних технологій. Забезпечення кібербезпеки критичної інформаційної інфраструктури України можливе шляхом: визначення об'єктів даної структури, вирішення проблем кібербезпеки об'єктів з дуже довгим життєвим циклом, розробки методики модернізації критичної інформаційної інфраструктури для кожної організації, технології та інформаційної структури, які є об'єктами критичної інформаційної інфраструктури. Потрібно систематизувати і удосконалити нормативно-правові акти Кабінету Міністрів України та органів виконавчої влади на основі виявлення і виокремлення тих положень, які не відповідають вимогам щодо забезпечення кібербезпеки інформаційних технологій у міжвідомчій взаємодії, виходячи із сучасних реалій сьогодення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

1. Pro osnovni zasady kiberbezpeky Ukrainy [On the basic principles of cybersecurity of Ukraine] (Ukraine), 05.10.2017, No 2163-VIII. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian)
   [Про основні засади кібербезпеки України (Україна), 05.10.2017, № 2163-VIII. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text].
2. Hnatiuk, S. O., Riabyi, M. O., & Liadovska, V. M. (2014). Vyznachennia krytychnoi informatsiinoi infrastruktury ta yii zakhystu: analiz pidkhodiv [Critical Information Infrastructure Definition and Protection - Approach Analysis]. *Zv'iazok, 4*, 3–7 (in Ukrainian)
   [Гнатюк, С. О., Рябий, М. О., & Лядовська, В. М. (2014). Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. *Зв'язок, 4*, 3–7].
3. Hnatiuk, S. O., Sydorenko, V. M., & Duksenko, O. P. (2015). Suchasni pidkhody do vyiavlennia ta identyfikatsii naibilsh vazhlyvykh ob'iektiv krytychnoi infrastruktury [Modern approaches to critical infrastructure objects detection and identification]. *Bezpeka informatsii, 21*(3), 269–275. doi: 10.18372/2225-5036.21.9690 (in Ukrainian)
   [Гнатюк, С. О., Сидоренко, В. М., & Дуксенко, О. П. (2015). Сучасні підходи до виявлення та ідентифікації найбільш важливих об'єктів критичної інфраструктури. *Безпека інформації, 21*(3), 269–275. doi: 10.18372/2225-5036.21.9690].
4. Biriukov, D. S., & Kondratov, S. I. (2012). Zakhyst krytychnoi infrastruktury: problemy ta perspektyvy vprovadzhennia v Ukraini [Critical infrastructure protection: problems and prospects of implementation in Ukraine]. Kyiv: NISD (in Ukrainian)
   [Бірюков, Д. С., & Кондратов, С. І. (2012). *Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні*. Київ: НІСД].
5. Stratehiia rozvytku informatsiinoho suspilstva v Ukraini [Information society development strategy in Ukraine] (Ukraine), 15.03.2013, No 386-p. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text (in Ukrainian)
   [Стратегія розвитку інформаційного суспільства в Україні (Україна), 15.03.2013, № 386-р. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text].

6. Pro Natsionalnu prohramu informatyzatsii [About the National Informatization Program] (Ukraine), 04.02.1998, No 74/98-BP. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/74/98-вр#Text (in Ukrainian)
[Про Національну програму інформатизації (Україна), 04.02.1998, № 74/98-ВР. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text].

7. Pro informatsiiu [About information] (Ukraine), 02.10.1992, No 2657- XII. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/2657-12#Text (in Ukrainian)
[Про інформацію (Україна), 02.10.1992, № 2657-XII. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text].

8. Poriadok formuvannia pereliku ob'iektiv krytychnoi informatsiinoi infrastruktury [The order of formation of the list of objects of critical information infrastructure] (Ukraine), 09.10.2020, No 943. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/943-2020-п#Text (in Ukrainian)
[Порядок формування переліку об'єктів критичної інформаційної інфраструктури (Україна), 09.10.2020, № 943. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text].

9. Kryminalnyi kodeks Ukrainy [Criminal codex of Ukraine] (Ukraine), 05.04.2001, No 2341-III. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/2341-14 (in Ukrainian)
[Кримінальний кодекс України (Україна), 05.04.2001, № 2341-III. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/2341-14].

10. Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky [About the National Cyber Security Coordination Center] (Ukraine), 07.06.2016, No 242/2016. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/242/2016#Text (in Ukrainian)
[Про Національний координаційний центр кібербезпеки (Україна), 07.06.2016, № 242/2016. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text].

11. Zahalni vymohy do kiberzakhystu ob'iektiv krytychnoi infrastruktury [General requirements for cyber security of critical infrastructure] (Ukraine), 19.06.2019, No 518. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/518-2019-п#n8 (in Ukrainian)
[Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (Україна), 19.06.2019, № 518. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#n8].

12. Pro Sluzhbu bezpeky Ukrainy [About the Security Service of Ukraine] (Ukraine), 25.03.1992, No 2229-XII. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/2229-12#Text (in Ukrainian)
[Про Службу безпеки України (Україна), 25.03.1992, № 2229-XII. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text].

13. Pro Derzhavnu sluzhbu spetsialnoho zv'iazku ta zakhystu informatsii Ukrainy [About the State Service for Special Communications and Information Protection of Ukraine] (Ukraine), 23.02.2006, No 3475-IV. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/3475-15#Text (in Ukrainian)
[Про Державну службу спеціального зв'язку та захисту інформації України (Україна), 23.02.2006, № 3475-IV. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text].

14. Kontseptsiia rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky [The concept of development of the digital economy and society of Ukraine for 2018-2020] (Ukraine), 17.01.2018, No 67-p. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/67-2018-p#Text (in Ukrainian)
[Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки (Україна), 17.01.2018, № 67-р. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/67-2018-p#Text].

15. Deiaki pytannia funktsionuvannia Natsionalnoi telekomunikatsiinoi merezhi [Some issues of functioning of the National Telecommunication Network] (Ukraine), 16.12.2020, No 1358. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/1358-2020-п#Text (in Ukrainian)
[Деякі питання функціонування Національної телекомунікаційної мережі (Україна), 16.12.2020, № 1358. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/1358-2020-п#Text].

16. Bakalinska, O., & Bakalynskyi, O. (2019). Pravove zabezpechennia kiberbezpeky v Ukraini [Legal support of cybersecurity in Ukraine]. *Pidpryiemnytstvo, hospodarstvo i pravo, 9*, 100–108. doi: 10.32849/2663-5313/2019.9.17 (in Ukrainian)
[Бакалінська, О., & Бакалинський, О. (2019). Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право, 9*, 100–108. doi: 10.32849/2663-5313/2019.9.17].

17. Malashko, O. Ye. (2020). *Administratyvno-pravovi zasady zabezpechennia informatsiinoi bezpeky v Ukraini u konteksti yevropeiskoi intehratsii* [Administrative and legal bases of information security in Ukraine in the context of European integration] (Doctoral thesis); Lvivskyi universytet biznesu ta prava. Lviv (in Ukrainian)
[Малашко, О. Є. (2020). *Адміністративно-правові засади забезпечення інформаційної безпеки в Україні у контексті європейської інтеграції* (Автореферат кандидатської дисертації); Львівський університет бізнесу та права. Львів].

18. Malashko, O. Ye., & Skrynkovskyy, R. M. (2020). Priorytetni napriamy udoskonalennia informatsiinoi bezpeky Ukrainy [Priority areas for improving information security in Ukraine]. *Internauka. Seriia: Yurydychni nauky, 6*(28), 13–19 (in Ukrainian)
[Малашко, О. Є., & Скриньковський, Р. М. (2020). Пріоритетні напрями удосконалення інформаційної безпеки України. *Інтернаука. Серія: Юридичні науки, 6*(28), 13–19].

19. Skrynkovskyy, R. M., & Malashko, O. Ye. (2020). Strukturno-klasyfikatsiina kharakterystyka zabezpechennia informatsiinoi bezpeky [Structural and classification characteristics of information security]. *Internauka. Seriia: Yurydychni nauky, 7*(29), 25–32 (in Ukrainian)
[Скриньковський, Р. М., & Малашко, О. Є. (2020). Структурно-класифікаційна характеристика забезпечення інформаційної безпеки. *Інтернаука. Серія: Юридичні науки, 7*(29), 25–32].

20. Tykhomyrov, O. O. (2014). *Zabezpechennia informatsiinoi bezpeky yak funktsiia suchasnoi derzhavy* [Ensuring information security as a function of the modern state]. Kyiv: Lira (in Ukrainian)
[Тихомиров, О. О. (2014). *Забезпечення інформаційної безпеки як функція сучасної держави*. Київ: Ліра].

21. Stratehiia voiennoi bezpeky Ukrainy “Voienna bezpeka – vseokhopliuiucha oborona” [Military Security Strategy of Ukraine "Military Security - Comprehensive Defense"] (Ukraine), 25.03.2021, No 121/2021. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/121/2021#n2 (in Ukrainian)
[Стратегія воєнної безпеки України «Воєнна безпека – всеохоплююча оборона» (Україна), 25.03.2021, № 121/2021. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n2].