ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКИ УКРАЇНИ

Сергій ЛУКАШЕВИЧ,

канд. юрид. наук, доцент,
доцент кафедри права гуманітарно-правового факультету Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна
https://orcid.org/0000-0001-8386-6237
s.lukashevych@khai.edu

Розглянуто теоретичні підвалини та практичні сенси в царині правового забезпечення захисту інформації та кібербезпеки України. Наголошено, що важливу роль відіграють в цьому процесі міжнародно-правові акти, ратифіковані Україною. відокремлено процеси та явища суспільного буття що визначають забезпечення захисту інформації та кібербезпеки як одне із першочергових завдань, що стоїть перед державою, та передбачає насамперед побудову власної законодавчої системи в царині захисту інформації, кібербезпеки, кіберзахитсту та забезпечення функціонування об'єктів критичної інфраструктури. Визнано, що необхідною складовою захисту інформації та кібербезпеки є додержання національної Стратегії з кібербезпеки, постійне доповнення її відповідними заходами. Запропоновано запровадити заходи систематичного широкомасштабного інформування населення про загрози, що можуть мати місце при використанні мережевих, хмарних та інших інтернет-ресурсів.

Ключові слова: *захист інформації, кібербезпека, кіберзахист.*

The theoretical foundations and practical meanings of rule-making in the field of information protection and cyber security of Ukraine are considered. It was emphasized that international legal acts ratified by Ukraine play an important role in this process. the processes and phenomena of social life are separated, which determine the provision of information protection and cyber security as one of the primary tasks facing the state, and first of all provides for the construction of its own legislative system in the field of information protection, cyber security, cyber defense and ensuring the functioning of critical infrastructure facilities. It is recognized that a necessary component of information protection and cyber security is compliance with the National Cyber Security Strategy, its constant addition with appropriate measures. It is proposed to implement measures of systematic large-scale informing of the population about the threats that may occur when using network, cloud and other Internet resources.

Keywords: *information protection, cyber security, cyber protection.*

Розвиток інформаційного суспільства та супутні йому зміни наукового світогляду призвели до перегляду багатьох уявлень про суспільство та майже усі явища і процеси, що в ньому відбуваються. Нагальною проблемою людства стає боротьба за ресурси, які людина на побутовому рівні сторіччями вважала майже невичерпними – чисте повітря, питна вода, родючі землі тощо. Можна припустити, що в майбутньому боротьба за них набуватиме дедалі більш жорстких та витончених форм, з використанням потужного потенціалу цифрових та кібер можливостей [1, Лукашевич/ Lukashevych, 2020], які уже використовуються як «звичайними» злочинцями, так і транснаціональними злочинними корпораціями з разгалудженою структурою та значними ресурсами [2, Гудмен/ Goodman, 2019].

Правове забезпечення в царині захисту інформації та кібербезпеки реалізується на двох взаємопов'язаних рівнях – на рівні міжнародно-правових актів, підписаних та ратифікованих Україною та на рівні національного законодавства України.

На міжнародному рівні визначальним актом в сфері правового забезпечення захисту інформації та кібербезпеки є Конвенція про кіберзлочинність прийнята Радою Європи у 2001 році (ратифікована Україною 07.09.2005 р.). Конвенція про кіберзлочинність передбачає здійснення певних рекомендованих дій на рівні держав-учасників і на міжнародному рівні, основними з яких є: розробка в національних кримінальних кодексах положень про злочини проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж та інформації, про злочини, пов'язані з використанням комп'ютерних засобів, з вмістом даних, з порушенням авторського права і суміжних прав; визначення додаткових видів відповідальності і санкцій (включення до складу злочинів таких видів, як замах на вчинення злочину, співучасть у ньому або підбурювання до його здійснення в розглядуваній сфері); встановлення кримінальної відповідальності юридичних осіб тощо. Спільними принципами міжнародного співробітництва в сфері кібербезпеки, кіберзахисту та захисту інформації названі: загальні принципи взаємної допомоги; можливість транскордонного доступу до збережених комп'ютерних даних з відповідної згоди або до загальнодоступних даних, взаємної допомоги у зв'язку з оцінкою збережених електронних даних, взаємна правова допомога зі збору даних про рух інформації у реальному часі; створення мережі 24/7 [3].

Додатковий протокол до Конвенції про кіберзлочинність надає перелік окремих видів злочинів, серед яких: 1) поширення расистських і ксенофобських матеріалів за допомогою комп'ютерних систем (dissemination of racist and xenophobic material through computer systems); 2) мотивована загроза расизму і ксенофобії (racist and xenophobic motivated threat); 3) расистська і ксенофобська мотивована образа (Racist and xenophobic motivated insult); 4) невизнання, надзвичайна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства (denial, gross minimisation, approval or justifii cation of genocide or crimes against humanity) [4].

З метою реалізації положень Конвенції про кіберзлочинність та на виконання приписів Закону України «Про національну безпеку» [5], 27 січня 2016 року Радою національної безпеки та оборони України ухвалено за основу Стратегію кібербезпеки України (уведено в дію Указом Президента від 15 березня 2016 року № 96/2016) з урахуванням викликів, які стоять перед нашою державою: військової агресії російської федерації, посилення тенденцій використання кіберпростору розвідувальними і спеціальними військовими структурами, терористами, криміналітетом [6]. Стратегія передбачає розвиток національної системи забезпечення захисту кіберпростору, своєчасного виявлення та нейтралізації кіберзагроз, а також запобігання їм з урахуванням досвіду та практики країн НАТО і Євросоюзу; визначено також сукупність заходів, пріоритетів та напрямів забезпечення кібербезпеки України, зокрема, створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору і досягнення сумісності з відповідними стандартами ЄС і НАТО, формування конкурентного

середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кібернетичного захисту.

Натепер сформована правова основа у сфері захисту інформації та кібербезпеки України, яка, крім Законів України «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України», «Про інформацію», включає також Доктрину інформаційної безпеки України (введена в дію 25.02.2017 року), Стратегію кібербезпеки України, інші законодавчі та підзаконні нормативно-правові акти. Вивчення цих нормативно-правових актів дає підстави стверджувати, що захист інформації та кібербезпека безпека визначаються як одні з головних пріоритетів у протидії загрозам національній безпеці України.

Отже, правове забезпечення захисту інформації, кібербезпеки та кіберзахисту стає нагальною проблемою як на міжнародному рівні, так і на рівні національних законодавств. Усвідомлення цих загроз також призвело до розробки на законодавчому рівні універсальних понять захисту інформації, кіберзагроз, кібербезпеки, кіберзахисту, захисту об'єктів критичної інфраструктури тощо.

Список використаних джерел:

1. Лукашевич С.Ю. Future crime: криміногенні загрози майбутнього. Забезпечення правопорядку вумовах коронакризи: матеріали панельної дискусії IV Харків. міжнар. юрид. форуму, м. Харків, 23–24ве-рес. 2020 р. / редкол.: В.Я.Тацій, А.П.Гетьман, Ю.Г.Барабаш, Б.М.Головкін. Харків: Право, 2020. 250 с. С. 144-148. URL: http://criminology.nlu.edu.ua/wp-content/uploads/2020/11/4j-forum-2020-zabezpechennya-pravoporyadku-v-umovah-koronakrizi.pdf

2. Гудмен Марк. Злочини майбутнього/ Пер. з англ. І. Мазарчук, Я. Машико. – Харків: Вид-во «Ранок»: Фабула, 2019. – 592 с.

3. Конвенція Ради Європи, «Конвенція про кіберзлочинність». Офіційний вісник України офіційне видання від 10.09.2007. 2007 р., № 65, стор. 107, стаття 2535, код акта 40846/2007. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

4. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text

5. Закон України «Про національну безпеку». Офіційний вісник України офіційне видання від 20.07.2018. 2018 р., № 55, стор. 51, стаття 1903, код акта 90815/2018. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

6. Стратегія кібербезпеки України. Офіційний вісник України офіційне видання від 29.03.2016. 2016 р., № 23, стор. 69, стаття 899, код акта 81164/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text.