

розбудова ефективної системи цивільного захисту є пріоритетом національних інтересів України [5].

Враховуючи вище наведене, доцільно зробити висновок, що екологічна безпека є складовою національної безпеки України, що гарантує відповідно до Конституції України та національного законодавства захист життя, здоров'я громадян, навколишнього природного середовища від реальних та потенційних загроз, що створюють природні чи антропогенні чинники.

ЛІТЕРАТУРА:

1. Абрамов В.І. Глобальна та національна безпека: підручник. Київ : НАДУ. 2016. 784 с.
2. Про охорону навколишнього природного середовища: Закон від 25.06.1991 № 1264-XII. Відомості Верховної Ради України. 1991. №41. Ст. 546.
3. Шульга Є. В. Міжнародно-правова охорона навколишнього середовища від впливу військових конфліктів: проблеми ефективності. Інтернаука. Серія: Юридичні науки. 2017. №1. С.63-69.
4. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради (ВВР). 2018. № 31. ст.241.
5. Стратегії національної безпеки України: Указ Президента України від 14.09.2020. № 392. 2020. Офіційний вісник України від 25.09.2020 р. № 75. стор. 127. стаття 2377. код акта 100870/2020.

Омельченко А. В.,
доктор юридичних наук, професор,
завідувач кафедри цивільного та трудового права
ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»

УДОСКОНАЛЕННЯ ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначаються Законом України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 р. № 2163-VIII [1].

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Закон України «Про основні засади забезпечення кібербезпеки України» та інші закони України, Конвенція про

кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Згідно із ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України» об'єктами кібербезпеки є конституційні права і свободи людини і громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури, а до об'єктів кіберзахисту відносяться комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [1].

Важливим міжнародно-правовим актом у сфері боротьби із кіберзлочинністю є Конвенція про кіберзлочинність від 23 листопада 2001 року, ратифікована Законом України від 07 вересня 2005 р. № 2824-IV [2].

З метою посилення боротьби із кіберзлочинністю та кібератаками вже під час дії правового режиму воєнного стану в Україні були прийняті Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15 березня 2022 р. № 2137-IX [3] та Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 р. № 2149-IX [4].

Зокрема, Законом України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15 березня 2022 р. № 2137-IX визначено, що:

- на вимогу володільця особа, яка здійснює тимчасове вилучення комп'ютерних систем або їх частин, залишає йому копії інформації з таких

комп'ютерних систем або їх частин (за наявності технічної можливості здійснення копіювання) з використанням матеріальних носіїв володільця комп'ютерних систем або їх частин. Копії інформації з комп'ютерних систем або їх частин, які вилучаються, виготовляються з використанням технічних засобів, програмно-технічних засобів, апаратно-програмних комплексів володільця із залученням спеціаліста. Дія цього положення не поширюється на випадки, якщо обіг інформації заборонено законом. Дія цього положення поширюється на інформацію з обмеженим доступом у частині, що не суперечить встановленому законодавством порядку обігу та захисту такої інформації;

- арешт на комп'ютерні системи чи їх частини накладається лише у випадках, якщо вони отримані внаслідок вчинення кримінального правопорушення або є засобом чи знаряддям його вчинення, або зберегли на собі сліди кримінального правопорушення, або у випадках, передбачених п. 2, 3, 4 ч. 2 ст. 170 КПК, або якщо їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, а також якщо доступ до комп'ютерних систем чи їх частин обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту;

- якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку;

- особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчого, прокурора під час здійснення обшуку, відомості про що вносяться до протоколу обшуку;

- визначено порядок зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису [5].

Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 р. № 2149-IX прийнято з метою посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі шляхом оптимізації положень статей 361, 361-1 Кримінального кодексу України. Цим законом внесено зміни до статей 361, 361-1 Кримінального кодексу України з метою приведення термінології у відповідність із Законом України від 16 грудня 2020 року № 1089-IX «Про електронні комунікації» й вимогами іншого законодавства України у сфері кібербезпеки. Також статтю 361 Кримінального кодексу України викладено в новій редакції, якою розмежовується ступінь відповідальності за несанкціоноване втручання в роботу інформаційних

(автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж в залежності від спричинених наслідків, а також посилюються санкції за вчинення відповідного кримінального правопорушення. Водночас вказана стаття передбачає, що втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, не вважається несанкціонованим, якщо таке втручання вчинено відповідно до Порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж. Окрім того, посилено санкції за вчинення кримінального правопорушення, передбаченого статтею 361-1 Кримінального кодексу України [6].

ЛІТЕРАТУРА:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
2. Конвенція про кіберзлочинність від 23 листопада 2001 р. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text
3. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15 березня 2022 р. № 2137-IX. URL : <https://zakon.rada.gov.ua/laws/show/2137-20#Text>
4. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24 березня 2022 р. № 2149-IX. URL : <https://zakon.rada.gov.ua/laws/show/2149-20#Text>
5. Діє Закон щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам. URL : <https://ips.ligazakon.net/document/MN025062?an=2>
6. Проект Закону про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану. URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=7182&skl=10

Аверіна Є. А.,
аспірант кафедри цивільного та трудового права
ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ НОТАРІАЛЬНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ