ISSN 0136-8168. Вісник Львівського університету. Серія юридична. 2018. Випуск 67. С. 170–179
Visnyk of the Lviv University. Series Law. 2018. Issue 67. P. 170–179

КОНСТИТУЦІЙНЕ ПРАВО

УДК 342.

КІБЕРНЕТИЧНА БЕЗПЕКА ЯК НОВІТНІЙ НАПРЯМ ІНФОРМАЦІЙНОЇ СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: КОНСТИТУЦІЙНО-ПРАВОВИЙ АСПЕКТ

П. Демченко

Інститут держави і права ім. В. М. Корецького НАН України
Вул. Трьохсвятительська 4, Київ, Україна, 01001,
E-mail: phildem18011993@gmail.com

Розглянуто проблематику щодо визначення місця кібернетичної безпеки в якості новітнього напряму інформаційної складової в системі національної безпеки України. Обґрунтовано наявність викликів та загроз у сфері використання кібернетичного простору, які можуть становити загрозу інтересам України. Розглянуто поняття та сутність кібернетичної безпеки з погляду правової науки, визначено проблематику забезпечення інформаційного суверенітету України на сьогодні та вказано на важливість положень норм Конституції України щодо реалізації концепції кібернетичної безпеки України в межах сучасної системи національної безпеки України. Проаналізовано основні положення нормативно-правових актів у сфері забезпечення кібернетичної безпеки в Україні. Підсумовано, що будучи новітнім напрямом національної безпеки України, в основу реалізації концепції кібернетичної безпеки України покладено саме норми Основного Закону – Конституції України, що обумовлюється проголошенням захисту незалежності та суверенітету України, прав і свобод людини та громадянина, інтересів суспільства та держави загалом, як основоположного завдання держави та обов'язку всього народу України.

Ключові слова: безпекова політика, кіберпростір, критична інфраструктура, суверенітет, виклики та загрози.

DOI: http://dx.doi.org/10.30970/vla.2018.67.170

Актуальність необхідності забезпечення кібернетичної безпеки України та утворення чіткого правового механізму її реалізації обумовлене наявними досягненнями науково-технічного прогресу людства за останні 50–70 років, впровадженням комп'ютерної техніки й електронних програм у повсякденну діяльність людини та використання на рівні органів державної влади забезпечує спрощення при вирішенні багатьох завдань. Водночас, наявні в світі приклади використання зазначених високотехнологічних виробів з метою вчинення неправомірних діянь та використання останніх у якості високоточної новітньої зброї, втручання у діяльність електронних систем державного значення та незаконне заволодіння інформацією є підставою для необхідності вироблення гнучкої безпекової політики щодо забезпечення гарантій захисту кібернетичного простору та інформаційного суверенітету України.

Відповідну проблематику розглянуто у наукових працях В. Антонова, О. Баранова, В. Бутузова, І. Діордіци, М. Дмитренка, Б. Кормича, В. Фурашева та інших. Але кібернетична безпека як певне новітнє явище для системи національної безпеки України потребує детального підходу дослідження з погляду положень

Конституції України, а також характеристики основних законодавчих положень у цій сфері.

У такому випадку основна мета дослідження полягає у визначенні поняття та сутності кібернетичної безпеки України, окресленні конституційних та нормативно-правових положень щодо її реалізації в межах забезпечення інформаційного суверенітету та національної безпеки на сучасному етапі розвитку Української держави, описі основних функцій та завдань національної системи кібернетичної безпеки України.

Але перш ніж визначити сутність кібернетичної безпеки України як одного з напрямів забезпечення та реалізації інформаційної складової національної безпеки України необхідно окреслити причини, які об'єктивно обумовлюють її необхідність обґрунтування з погляду положень Основного Закону – Конституції України та існуючих законодавчих актів, які регулюють правові відносини в сфері національної безпеки України на цей момент.

Стрімкий розвиток технологій за останні 40 років надав людству можливість залучати комп'ютерні технології те електронно-автоматизовані системи у найрізноманітніші аспекти життя. У сфері державного будівництва, електронну техніку вже давно використовують у межах координації між органами державної влади, надання послуг населенню, слугує основою для реалізації новітніх підходів функціонування механізму державної влади, серед котрих можна навести концепцію функціонування електронного уряду та проведення електронних виборів.

У той же момент, досягнення науково-технічного прогресу у вигляді сучасних інформаційних технологій створює умови використання останніх з метою скоєння правопорушень, націлених проти прав і свобод людини та громадянина, державного суверенітету України, зриву планування та виконання стратегічних завдань і розвитку держави загалом. Особливо важливо враховувати факт, що скоєння відповідних дій, спрямованих на досягнення конкретної мети з використанням комп'ютерної техніки, електронних програм та систем на сьогодні стало не тільки справою одної особи чи певної групи осіб, які володіють відповідними матеріальними засобами та навичками. Останнім часом поширюється питання використання комп'ютерних технології військовими, розвідувальними та контррозвідувальними, правоохоронними підрозділами певних держав світу з метою підриву основ національної безпеки іншої держави, що має слабкорозвинутий захист критичної інфраструктури у кібернетичному просторі.

З цього приводу доцільно відзначити думку М. Дмитренка, відповідно до якої впровадження високих наукомісних технологій, нанотехнологій у всі сфери суспільного життя, де провідна роль належить мікроелектроніці, оптоелектроніці, інформаційним технологіям, новим технологіям виробництва високоякісних матеріалів, які активно використовують для розроблення нових зразків високоточної та «високоінтелектуальної» зброї [6, с. 4]. Відповідний підхід до характеристики використання сучасних інформаційних технологій також розглядали на 27-му Саміті держав-членів НАТО у Варшаві 8–9 липня 2016 р., у процесі котрого було визнано кібернетичний простір «п'ятим полем бою» сучасної війни та прийнято рішення на розроблення стратегії відповідно до викликів та загроз у кібернетичній сфері, вплив на котру найчастіше відчувається зі Сходу [18].

Визначення східного вектора загроз кібернетичній безпеці держав Північноатлантичного альянсу є цілком обумовленим лише вже на основі оцінки можливостей, утворених у 2016 р. Військ інформаційних операцій Збройних Сил Російської Федерації, які визнані одними з 5-ти найпотужніших кібернетичних

військ у світі та поступаються лише аналогічним підрозділам армій Сполучених Штатів Америки, Китайської Народної Республіки, Великої Британії та Південної Кореї [17].

Окрім того, приклад втручання Росії у критичну кібернетичну інфраструктуру виборчого процесу під час президентських виборів у США в 2016 р. та у Франції в 2017 р. вказує, наскільки далеко може зайти російське керівництво в підриві основ демократії у розвинутих державах світу. Відповідні події мають бути враховані в Україні при розробленні та реформуванні законодавства у сфері реалізації кібернетичної безпеки та при забезпечені безпеки критичної інфраструктури виборчого процесу напередодні президентських та парламентських виборів у 2019 р.

У чому ж полягає сутність поняття «кібернетична безпека» та яке його місце у якості відповідного напряму інформаційної складової системи національної безпеки України на сьогодні?

Потрібно зазначити, що введення термінів «кібернетична безпека» та «кібербезпека» як юридичної категорії у якості конкретного предмета правового регулювання викликало свого часу багато запитань з погляду теорії та практики. Уперше термін «кібернетичний» використав американський письменник Ульям Гібсон у романі «Нейромант» у 1984 р. та став основою для розвитку нового літературного жанру – кіберпанку та закріплення відповідних термінів за новітніми досягненнями у сфері високих технологій у 80-х роках XX ст. [20]. В якості юридичного терміна, поняття «кібернетична безпека» вперше з'явилось у середині 1990-х років в актах уряду США, щодо проголошення початку широкомасштабного дослідження забезпечення кібернетичної безпеки в цій державі [2].

Варто зазначити, що в зарубіжних державах (передусім в англомовних країнах) існує проблематика розуміння термінів «кібернетична безпека» і «кібербезпека» та, як наслідок, доцільність використання цих термінів у площині юридичних відносин. На думку Дж. Франсело, активне використання вищезазначених термінів (англ. «cybersecurity» та «cybersecurity») призводить до виникнення протиріч при здійсненні повноважень керівниками структурних підрозділів служб безпеки різних держав світу та при здійсненні правового аналізу експертами з питань національної та інформаційної безпеки щодо питання сутності юридичного вираження та особливостей порядку застосування зазначених термінів [21].

Щодо вітчизняної термінології, то відповідно до Великого тлумачного словника сучасної української мови складне поняття «кібернетична безпека» означає: «кібернетичний – той, що стосується кібернетики; який створено, працює на основі принципів, методів кібернетики», а своєю чергою «безпека – стан, коли кому-, чому-небудь ніщо не загрожує» [4, с. 106, с. 108].

В аспекті вітчизняної юридичної науки на сьогодні також існує декілька підходів до визначення кібернетичної безпеки з урахуванням існуючого стану правовідносин у сфері забезпечення кібернетичної безпеки в Україні. На думку В. Фурашева, кібернетична безпека є таким станом здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, передусім – несвідомого, негативного впливу (управління) інформації [19, с. 166]. О. Баранов запропонував визначати кібернетичну безпеку як певний стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [2]. В. Бутузов запропонував розуміти кібернетичну безпеку як стан захищеності життєво важливих прав і свобод людини, суспільства та держави у кібернетичному просторі від внутрішніх та зовнішніх протиправних посягань та загроз таких посягань [3, с. 176]. Власний підхід до розуміння

кібернетичної безпеки подав І. Діордіца, під яким поняття кібернетична безпека необхідно розуміти як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі, в якому можливе безперешкодне створення, зібрання, одержання, зберігання, використання, поширення, охорони, захисту інформації, а у вузькому розумінні – стан індивіда, суспільства та держави, де відсутня будь-яка небезпека [5].

Як ми бачимо, при формулюванні поняття «кібернетична безпека» досить поширеним є використання правових категорії, пов'язаних із власне інформаційною безпекою. Особливість такого підходу до закріплення кібернетичної безпеки як інформаційної складової національної безпеки України визначається загальною характеристикою усієї системи національної безпеки України. Потрібно зазначити, що відповідно до ст. 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Зазначене конституційне положення хоча не повною мірою визначає складові системи національної безпеки України, але водночас має важливі аспекти, в одному з котрих саме захист існування Української держави є справою всього її народу, а в іншому – визначається на конституційному рівні забезпечення інформаційної складової національної безпеки України як основоположної в межах останньої [7].

Окрім того, доцільно наголосити на тому, що система національної безпеки України є складним та багатогранним явищем, що охоплює напрями безпеки існування та розвитку Української держави і суспільства на сучасному етапі їх розвитку, а також гарантування захисту прав і свобод людини та громадянина в Україні, захистом інтересів суспільства та держави. З приладу визначення конституційно-правової характеристики системи національної безпеки, у розумінні котрого визначаються основні структурні елементи цієї системи, В. Антонов запропонував розуміти систему національної безпеки України як сукупність окремих, відносно самостійних і необхідно взаємопов'язаних та відокремлених елементів, що утворюють певну цілісність, яка забезпечує розвиток та захищеність життєво важливих інтересів людини і громадянина, суспільства та держави від внутрішніх і зовнішніх загроз. У такому випадку найважливішими структурними елементами національної безпеки України на цьому етапі розвитку необхідно вважати її економічну, політичну, інформаційну, військову, соціальну, культурну складові відповідної системи [1, с. 104–105].

Сутність самої інформаційної безпеки, що своєю чергою основою для визначення місця кібернетичного напряму системи національної безпеки України, полягає у її нормативно-правовому закріпленні як стану захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації (п. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.» 537-V від 09.01.2007 р.) [15].

Але необхідно зазначити, що в Україні були спроби значно ширше закріпити на правовому рівні основи інформаційної безпеки шляхом визначення окремої правової категорії – інформаційного суверенітету України. У цьому випадку потрібно зазначити факт, відповідно до котрого декілька разів до Верховної Ради України вносили законопроекти щодо інформаційного суверенітету та інфор-

маційної безпеки України. Відповідно до ст. 2 законопроекту «Про інформаційний суверенітет та інформаційну безпеку України», який вніс В. Шевченко на розгляд до Верховної Ради України, інформаційний суверенітет – «це право держави на формування і здійснення національної інформаційної політики відповідно до Конституції та законодавства України, міжнародного права в національному інформаційному просторі України» [11]. В аналогічному законопроекті, який вніс Л. Лук'яненко, поняття інформаційного суверенітету визначено «як право держави на формування і здійснення національної інформаційної політики відповідно до Конституції України і законодавства України, міжнародного права в національному інформаційному просторі України» [10]. Окремої уваги заслуговує формулювання поняття інформаційного суверенітету в ст. 2 законопроекту авторства І. Чижа, відповідно до котрого «інформаційний суверенітет України – це невід'ємне право людини, суспільства, держави на самовизначення та участь у формуванні, розвитку і здійсненні національної інформаційної політики відповідно до Конституції та чинного законодавства України, міжнародного права в національному інформаційному просторі України» [12].

Втім, жодний зі зазначених проектів законодавчих актів щодо забезпечення інформаційного суверенітету та інформаційної безпеки України не був прийнятий Верховною Радою України, що необхідно вважати негативним поступом законодавчої гілки влади в розробленні загальної державної концепції щодо забезпечення інформаційної складової національної безпеки України на межі XX–XXI ст. та стало однією з умов прояву наслідків у наш час.

Відповідно до аналізу зазначених вище положень законопроектів, можна зробити висновок, що основою забезпечення інформаційного суверенітету слугують положення ст. 1; ч. 1 ст. 2; ч. 1 ст. 9; та ч. 1 ст. 17 Конституції України, зміст яких вказує на обов'язковість необхідності забезпечення безпекової політики в межах забезпечення інформаційного суверенітету та є правовим підґрунтям для забезпечення, розвитку і реалізації кібернетичної безпеки України у сучасному інформаційному просторі з урахуванням загроз та викликів сьогодення критичної інфраструктури. Водночас необхідно вказати, що зазначені норми Основного Закону України не є єдиними конституційно-правовими приписами у сфері забезпечення кібернетичної безпеки України. Суттєву роль у реалізації кібернетичної безпеки України в межах інформаційної складової системи національної безпеки України також відіграватимуть конституційні положення щодо затвердження унітарного державного устрою, цілісності та недоторканості державної території (ст. 2 Конституції України) визнання людини, її життя і здоров'я, честі та гідності, недоторканості і безпеки як найвищої соціальної цінностів Україні (ч. 1 ст. 3 Конституції України), визнання єдиним носієм суверенітету та носієм влади в Україні її народу (ч. 2 ст. 5 Конституції України), закріплення принципу розподілу влади (ч. 1 ст. 6 Конституції України), визнання та додержання принципу верховенства права в Україні (ч. 1 ст. 8 Конституції України) [7].

На підставі поданих положень, варто вказати на думку Б. Кормича, що саме норми Конституції України являтимуть собою головну роль у розвитку та забезпеченні системи національної безпеки України, що веде до їх провідної ролі у разі розроблення, реформування та реалізації будь-якої правової концепції кібернетичної безпеки в межах інформаційного суверенітету України [8, с. 39].

Отже, можна визнати, що кібернетична безпека є особливим новітнім напрямом інформаційної складової системи національної безпеки України, в основу котрої покладено положення норм Конституції України. Реалізація

зазначених конституційних приписів у сфері кібернетичної безпеки України відіграє суттєву роль для загального забезпечення реалізації безпекової політики в усіх визначених законодавством сферах щодо безпекової політики.

Будучи новітнім напрямом інформаційної складової системи національної безпеки України, основні засади реалізації кібернетичної безпеки в Україні можна простежити у відповідних, відносно нещодавно прийнятих нормативно-правових актах: Указ Президента України «Про рішення Ради національної безпеки та оборони України від 27.01.2016 р. № 96/2016 «Про Стратегію кібернетичної безпеки України» від 15.03.2016 р.; Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. та новий Закон України «Про національну безпеку України» №2469-VIII від 21.06.2018 р.

Потрібно зазначити, що саме Стратегія кібернетичної безпеки України стала основою для вироблення концепції з реалізації кібернетичної безпеки в Україні на основі визначення об'єктивних викликів та загроз, передусім пов'язаних зі збройною агресією Росії проти України. Відповідний нормативно-правовий акт є довгостроковим, який націлений на забезпечення гнучкої відповіді на наявні виклики та загрози кібернетичному простору України та вказує на завдання відповідних органів державної влади в Україні щодо її реалізації. Окремою рисою Стратегії кібернетичної безпеки України варто також визначити закріплення в п. 4 «Пріоритети та напрямки забезпечення кібернетичної безпеки України» необхідності розроблення та вдосконалення існуючої електронної інфраструктури в Україні, забезпечення підготовки кадрів та міжнародного співробітництва у сфері забезпечення кібернетичної безпеки України (передусім з відповідними структурами ЄС та НАТО) [16]. Загалом, саме Стратегія стала, окреслюючи коло завдань, що стоять перед Українською державою в сфері забезпечення безпеки в кібернетичному просторі, підґрунтям для подальшої розробки законодавства в сфері кібернетичної безпеки України.

Іншим нормативно-правовим актом, який регулює питання забезпечення кібернетичної безпеки в Україні є Закон України «Про основи кібернетичної безпеки України» № 2163-VIII від 05.10.2017 р. Особливість цього Закону полягає у наявності в ст. 1 чіткого категоріального апарату в сфері забезпечення кібернетичної безпеки в Україні, а відповідно до п. 5 ч. 1 ст. 1 кібербезпека закріплюється як захищеність життєво важливих інтересів людини та громадянина, суспільства і 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. Також необхідно наголосити на тому, що концепція забезпечення кібернетичної безпеки України в зазначеному Законі полягає у її забезпеченні побудови національної системи кібернетичної безпеки, в основу котрої покладені реалізація управлінських та технологічних підходів щодо її забезпечення державою та її народом в інформаційному, економічному, політичному, військових напрямах. Важливою рисою Закону України «Про основні засади забезпечення кібернетичної безпеки України» № 2163-VIII від 05.10.2017 р. є визначення основних засад забезпечення інтересів людини та громадянина, суспільства та держави, закріплення повноважень органів державної влади, підприємств, установ та організацій у сфері забезпечення кібернетичного простору України (ст. 5); принципів забезпечення кібернетичної безпеки України (ст. 7); основних об'єктів, які становлять критичну інфраструктуру України (ст. 6); закріпляє положення щодо національної системи кібернетичної безпеки України (ст. 8) [14].

Окремо варто відзначити новоприйнятий Закон України «Про національну безпеку України» № 2469-VIII від 21.06.2018 р., у якому відповідно до положення ч. 1 ст. 31 визначено основоположну роль Стратегії кібернетичної безпеки, як довгострокового документа планування з визначенням національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектора безпеки й оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів [13]. Закріплення Стратегії кібернетичної безпеки України в Законі України «Про національну безпеку України» №2469-VIII від 21.06.2018 р. по суті є визнанням законодавцем кібернетичної безпеки як новітнього напряму забезпечення всієї системи національної безпеки України.

Варто наголосити, що забезпечення національної системи кібернетичної безпеки України покладається на основних суб'єктів: Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний Штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до положень Конституції і законів України виконують в установленому порядку покладені на них компетенції у сфері забезпечення кібернетичної безпеки України (ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібернетичної безпеки України» № 2163-VIII від 05.10.2017 р.) [14].

Окрім того, доцільно відзначити, що до системи органів щодо забезпечення кібернетичної безпеки в Україні потрібно віднести утворений у межах робочого органу Ради національної безпеки та оборони Національний координаційний центр кібернетичної безпеки. Його діяльність регулює Положення «Про Національний координаційний центр кібербезпеки» затвердженим Указом Президента України від 7 червня 2016 р. № 242/2016, а також у рядову команду реагування на комп'ютерні надзвичайні події України CERN-UA, основні завдання котрої закріплені в ст. 9 Закону України «Про основні засади забезпечення кібернетичної безпеки України» № 2163-VIII від 05.10.2017 р. [9/14]. Утворення відповідних суб'єктів забезпечення кібернетичної безпеки України полягає у випадках необхідності оперативного усунення загроз критичній інфраструктурі та кібернетичному простору України за неможливості детального розгляду ситуації та розроблення плану дії основними суб'єктами національної системи кібернетичної безпеки України.

Отже, можемо зробити висновок, що кібернетична безпека України є врегульованим Конституцією та законами України напрямом інформаційної складової загальної системи національної безпеки України, завдання котрого полягає у забезпеченні безпеки прав і свобод людини та громадянина, інтересів суспільства та держави, охорони критичної інфраструктури України та доступу до інформаційних даних, підтримання загальної обороноздатності України та можливості вчасного планування відповіді викликам та загрозам, що становлять небезпеку існування Української держави.

Список використаних джерел

1. *Антонов В. О.* Конституційно-правові засади національної безпеки України: монографія. Київ: Талком, 2017. 576 с.
2. *Баранов О. А.* Про тлумачення та визначення поняття «кібербезпека». URL: http://ippi.org.ua/baranov-oa-pro-tlumachennya-ta-viznachennya-ponyattya -»kiberbezpeka»
3. *Бутузов В. М.* Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КИТ., 2010. 408 с.
4. Великий тлумачний словник сучасної української мови / уклад. О. О. Єрошенко. Донецьк: ТОВ «Глорія Трейд», 2012. 864 с.
5. *Діордіца І. В.* Поняття та зміст національної системи кібербезпеки. URL: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki
6. *Дмитренко М. А.* Політична система України: розвиток в умовах глобалізації та інформаційної революції. Київ: Знання України,2008. 544 с.
7. Конституція України: Закон України від 28.06.1996 р.№294к/ВР-96 // Відомості Верховної ради України від 23.07.1996 р. №30 Ст. 141.
8. *Кормич Б. А.* Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ: Кондор, 2004. 384 с.
9. Про затвердження Положення «Про Національний координаційний центр кібербезпеки»: Указ Президента України від 7 червня 2016 року № 242/2016 URL: https://-www.president.gov.ua/documents/962016-19836
10. Про інформаційний суверенітет та інформаційну безпеку України: Проект Закону України №1207- від 04.02.1998 р. URL: w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=-&pf3511=20812&pf35401
11. Про інформаційний суверенітет та інформаційну безпеку України: Проект Закону України №1207-д від 7 липня 1998 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_-1?pf3511=4192
12. Про інформаційний суверенітет та інформаційну безпеку України: Проект Закону України №1207-дп від 12 серпня 1999 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/-webproc4_1?pf3511=5871
13. Про національну безпеку України: Закон України №2469-VIII від 21.06.2018 р. URL: http://zakon.rada.gov.ua/laws/show/2469-19
14. Про основні засади забезпечення кібернетичної безпеки України: Закон України № 2163-VIII від 05.10.2017 р. URL: http://zakon.rada.gov.ua/laws/show/2163-19
15. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України 537-V від 09.01.2007 р. URL: http://zakon.rada.gov.ua/laws/show/537-16
16. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року №96/2016 URL: https://www.president.gov.ua/documents/962016-19836
17. Россия – в топ-5 мировых кибермармий. URL: https: jam-news.net/?p=11304&lang=ru.
18. Саміт НАТО у Варшаві: стримування Росії з простягнутою до неї рукою. URL: https://www.dw.com/uk/саміт-нато-у-варшаві-стримування-росії-з-простягнутою-до-неї-рукою/a-19389540.
19. *Фурашев В. Н.* Кібернетичний та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. Київ. 2012. № 2. С. 162–169.
20. *Gibson W.* Neoromancer. 1984. URL: http://readli.net/neyromant-sbornik
21. *Franscella J.* Cybersecurityvs Cyber Security : When, Why and How to Use the Term. URL: http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html

References

1. Antonov, V. O. (2017). *Konstytutsiino-pravovi zasady natsionalno i bezpeky Ukrainy: monohrafiia.* Kyiv: Talkom.
2. Baranov, O. A. *Pro tlumachennia ta vyznachenniaponiattia «ckiberbezpeka»* Retrievered from: http://ippi.org.ua/baranov-oa-pro-tlumachennya-ta-viznachennya-ponyattya -»kiberbezpeka»
3. Butuzov, V. M (2010). *Protydiia kompiuternii zlochynnosti v Ukraini (systemno-strukturnyianaliz): monohrafiia.* Kyiv: KYT.
4. *Velykyi tlumachnyi slovnyk suchasnoi ukrains'koi movy* (2012). O. O. Ieroshenko (Ukl.). Donets'k: «HloriiaTreid» LLC.864.
5. Diorditsa, I. V. *Poniattia ta zmist natsionalnoi systemy kiberbezpeky.* Retrievered from:http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki
6. Dmytrenko, M. A. (2008). *Politychna systema Ukrainy: rozvytok v umovakh hlobalizatsii ta informatsiinoi revoliutsii.* Kyiv: Znannia Ukrainy.
7. Konstytutsiia Ukrainy. (28.06.1996). Zakon. (1996). *Vidomosti Verkhovnoi Rady Ukrainy, 30, Art. 141* (accessed 01.02.2018).
8. Kormych, B. A. (2004). *Informatsiina bezpeka: orhanizatsiino-pravoviosnovy: Navchal»nyj posibnyk.* Kyiv: Kondor.
9. *Pro zatverdzhennia Polozhennia «Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky»* (07.06 2016). Ukaz Prezydenta Ukrainy (2016). Retrievered from: https://www.president.-gov.ua/documents/962016-19836
10. *Pro informatsiinyi suverenitet ta informatsiinu bezpeku Ukrainy* (04.02.1998). Proekt Zakonu (1998). Retrievered from: w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=20812&pf-35401
11. *Pro informatsiinyi suverenitet ta informatsiinu bezpeku Ukrainy* (07.07.1998). Proekt Zakonu (1998). Retrievered from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=4192
12. *Pro informatsiinyi suverenitet ta informatsiinu bezpeku Ukrainy* (12.08. 1999). Proekt Zakonu (1999). Retrievered from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=5871
13. *Pro natsionalnu bezpeku Ukrainy* (21.06.2018). Zakon.(2018). Retrievered from: http://zakon.rada.gov.ua/laws/show/2469-19
14. *Pro osnovni zasady zabezpechennia kibernetychnoi bezpeky Ukrainy* (05.10.2017). Zakon (2017).Retrievered from: http://zakon.rada.gov.ua/laws/show/2163-19
15. *Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 rr.* (09.01.2007). Zakon Ukrainy (2007). Retrievered from: http://zakon.rada.gov.ua/laws/show/537-16
16. *Pro rishennia Radynational»noi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy»* (15.03.2016) Ukaz Prezydenta Ukrainy (2016). Retrievered from: https://www.president.gov.ua/documents/962016-19836
17. *Rossyia – v top-5 myrovyh kyberarmyi.* Retrievered from: https: jam-news.net/?p=11304-&lang=ru.
18. *Samit NATO u Varshavi: strymuvanniaRosii z prostiahnutoiu do neirukoiu.* Retrievered from: http://www.dw.com/uk/samit-nato-u-varshavi-strymuvannia-rosii-z-prostiahnutoiu-do-nei-rukoiu/a-19389540
19. Furashev, V. H. (2012). Kibernetychnyi ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti. *Informatsiia i pravo. 2,* 162–169.
20. Gibson, W. (1984). *Neoromancer.* Retrievered from:: http://readli.net/neyromant-sbornik
21. Franscella, J. *Cybersecurityvs Cyber Security : When, Why and How to Use the Term.* Retrievered from: http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the -Term.html

CYBERSECURITY AS A NEW DIRECTION OF THE INFORMATION COMPONENT OF NATIONAL SECURITY OF UKRAINE: CONSTITUTIONAL LEGAL ASPECT

P. Demchenko

V. M. Koretsky Institute of State and Law
of the National Academy of Sciences of Ukraine,
4, Tryokhsvyatytelska Str., Kyiv, Ukraine, 01001,
e-mail: phildem18011993@gmail.com

The article is devoted to defining the place of cybersecurity of Ukraine, as the latest trend of information component of national security system of Ukraine, which is based on provisions of the Constitution and legislation of Ukraine. The main reasons for the development of the concept of cybernetic security of Ukraine should include the emergence of challenges and threats in information and cyberspace in the context of rapid development of scientific and technological progress of mankind. It is also essential to add that in the conditions of the armed aggression of Russia against Ukraine, the question of protection and its legal reasoning from the point of view of the Constitution of Ukraine with the aim of protecting state sovereignty and independence of the Ukraine is extremely urgent.

In the article the special attention is paid to appearance and development of the term "cybersecurity". The approaches of Ukrainian scholars to determining the cybersecurity from the legal point of view are analysed.

As the basis for the system of national security of Ukraine, the rules of the Constitution of Ukraine define the fundamental focus on the protection of cyberspace and critical infrastructure of Ukraine. It is important to note that the implementation of the cybersecurity of Ukraine is the protection of the rights and freedoms of man and citizen in Ukraine, the interests of society and the state, effective functioning of bodies of state power, of the ability to confront the challenges and threats in the sphere of high technologies.

As well the author considers the problems of determining the informational sovereignty of Ukraine, identifies and consolidates its legal features, including cybersecurity, which is included as part of the overall information security policy in the system of national security of Ukraine.

Special attention is devoted to the recently adopted normative legal acts in the sphere of implementation of cybersecurity in Ukraine, which define the essence and the concept of cybersecurity, the basic principles and tasks for its implementation in Ukraine. The article as well defines the characteristics of the national system of cybersecurity in Ukraine.

The basic principles of activities, tasks, and limits of competence of the relevant entities ensuring the implementation of cybersecurity in Ukraine are analysed.

In conclusion the author singles out the main norms of the Constitution of Ukraine that recognize cybersecurity as a part of the information component of national security of Ukraine.

Keywords: security policy, cyberspace, critical infrastructure, sovereignty, challenges and threats.

Стаття: надійшла до редакції 02.10.2018
прийнята до друку 01.11.2018