УДК. 004.056(477)
DOI: 10.31359/2411-5584-2020-40-1-113

Л. Ю. ВЕСЕЛОВА
кандидатка юридичних наук,
доцентка кафедри адміністративної
діяльності поліції Одеського державного
університету внутрішніх справ,
Україна, м. Одеса
e-mail: cvet-Liliya@ukr.net
ORCID 0000-0001-6665-0426

СТАНОВЛЕННЯ ПРАВОВОГО ІНСТИТУТУ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ[1]

Анотація. У статті проведено дослідження становлення правового інституту кібернетичної безпеки. Розглянуто аспекти, які обумовили розвиток інституту кібернетичної безпеки та телекомунікаційних відносин у кібернетичному просторі. Констатовано, що становлення національного правового інституту кібербезпеки напряму пов'язується з розвитком міжнародного права у цій сфері, перш за все європейського, яке слугувало певним стандартом у сфері інформаційної та телекомунікаційної захищеності суспільства.

Ключові слова: кібернетичний простір, гарантування інформаційної безпеки, цифровий світ.

Постановка проблеми. Без сумніву, кібернетична безпека є розвиненим правовим явищем, що має відповідні сформовані нормативно-правові засади. Поряд з цим розвиток кібернетичної безпеки як безпекового явища, а тим більше феномену правових відносин, зокрема, з урахуванням унікальності та особливостей адміністративно-правового регулювання, є історичним процесом, історико-правова характеристика якого зумовлює історичний вираз розвитку цього феномену в правовій системі суспільства.

Дещо спрощено, але за класичним академічним підходом до визначення, під кібернетичною безпекою розуміють певний стан захищеності системи

[1]
Статтю розміщено на сайті збірника: http://econtlaw.nlu.edu.ua.

відносин в інформаційній та телекомунікаційній сферах з використанням комп'ютерної техніки. Перш за все така система відносин формується в специфічному середовищі – кібернетичному просторі. Тобто наявною є ціла мережа інформаційних та телекомунікаційних відносин, з цілою низкою прав та свобод суб'єктів цих відносин. Логічним є також і наслідок – зловживання окремими суб'єктами, порушення визначених прав та свобод людей. У зазначеному контексті кібернетична безпека і є відповідним правовим механізмом щодо охорони прав та свобод суб'єктів інформаційних та телекомунікаційних відносин. У свою чергу, формування зазначеного правового механізму безпосередньо пов'язане з розвитком інформаційного суспільства, телекомунікаційних технологій та наслідками науково-технічного прогресу в цій сфері, що привело до стрімкого зростання інформаційних потоків, колосальних масивів даних, еволюційних змін у системі суспільних відносин – відносин у кібернетичному просторі, які все більше домінують у системі комунікацій на тлі історичного розвитку цивілізації.

Аналіз останніх досліджень і публікацій. Питання щодо становлення правового інституту кібернетичної безпеки розглядалося такими вченими, як І. А. Спасибо (I. A. Spasybo) [1], В. В. Бухарєв (V. V. Bukhariev) [2], С. А. Буяджи (S. A. Buiadzhy) [3] та ін. З урахуванням швидкоплинного розвитку інформаційно-телекомунікаційних технологій правовий інститут кібернетичної безпеки потребує постійного вдосконалення та розвитку, що зумовлює актуальність його подальшого дослідження.

Формулювання цілей. Дослідити та проаналізувати становлення правового інституту кібернетичної безпеки.

Виклад основного матеріалу. У середині XX ст. з'явилися перші електронні обчислювальні машини, що становили більше калькулятори з незначними додатковими функціями. Згодом, із розширенням функціональних можливостей, було розроблено прототипи сучасних комп'ютерів, які сьогодні використовуються в повсякденному житті людей як незамінний атрибут бізнесу, навчання, розваг тощо. Розвиток комп'ютерної техніки супроводжувався розвитком Інтернету – глобальної мережі.

Важливий крок в історії створення Інтернету було здійснено в 1965 р. американськими вченими Т. Меррилл (T. Merrill) та Л. Дж. Робертс (L. J. Roberts). Вони вперше здійснили підключення віддалених на значну відстань один від одного комп'ютерів, коли одна машина знаходилася у штаті Массачусетс, а інша – в Каліфорнії. Експеримент було проведено з використанням низькошвидкісної телефонної лінії. У результаті було створено першу, хоча й невелику, широкомасштабну комп'ютерну мережу. Проведений експеримент приніс розуміння того, що загальні комп'ютери можуть працювати разом,

виконувати програми і за необхідності вилучати дані на видаленому комп'ютері, проте система комутованих телефонних ліній для цього абсолютно не підходила [1].

На початку 90-х рр. було створено спеціальне програмне забезпечення на підключення декількох комп'ютерів до глобальної мережі – «WorldWideWeb» («WWW»). У квітні 1993 р. було здійснено випуск вихідного коду WorldWideWeb у суспільне надбання, що означало, що кожен може його використовувати і створювати на його основі програмне забезпечення без ліцензійних відрахувань. У цьому ж році Національний центр прикладних систем для суперкомп'ютерів (National Center for Supercomputing Applications) випустив програму Mosaic, яка стала одним із перших браузерів. Спочатку вона була доступна тільки для машин під управлінням операційної системи Unix і у формі вихідного коду, але вже в грудні 1993 р. Mosaic поставлявся з установниками (інсталяторами) для операційних систем Apple Macintosh і Microsoft Windows. Mosaic дуже швидко ставав популярним, а разом з ним і всесвітня мережа [2, с. 39].

Науково-технічний прогрес у сфері кібернетики, інформації та телекомунікацій сформував поряд із важливими факторами цивілізаційного розвитку людства передумови поширення негативних явищ, процесів з порушеннями низки основоположних прав і свобод громадян – кібернетичні правопорушення. Саме поширення загроз у кібернетичному просторі зумовило формування безпекознавчого напряму – кібербезпеки та розвиток відповідного правового інституту як механізму охорони прав суб'єктів у кіберпросторі [4]. Розвиток зазначеного правового інституту має свої певні історичні межі з врахуванням технологічного розвитку та впровадження норм міжнародного права.

Першим, у глобальному контексті, законодавчим актом, що врегульовував забезпечення кібербезпеки, був «Закон про боротьбу з комп'ютерними шахрайством та комп'ютерними зловживанням» (The Computer Fraud and Abuse Act), прийнятий у США в 1986 р. [3, с. 146]. Важливим надбанням цього закону було визнання проблеми щодо можливості вчинення неправомірних дій в інформаційній сфері, що дало поштовх до розвитку інституту кібербезпеки. Закон закріпив відповідальність за несанкціоноване втручання в роботу комп'ютерних систем чи викрадення інформації з них. Крім того, актом передбачено санкції до осіб, які вчиняють дії подібного характеру [2, с. 40].

У розвиток правового забезпечення кібербезпеки було прийнято у 1989 р. Рекомендації R(89)9 Радою Європи, якою було закріплено:

по-перше, чіткий перелік дій, які набувають ознак кіберправопорушень;

по-друге, головні аспекти розробки та побудови єдиної стратегії протидії негативним діям у кіберпросторі [5].

Подальший еволюційний розвиток інституту кібернетичної безпеки супроводжувався одночасним впровадженням відповідних правових норм як у міжнародному праві, так і в національних законодавствах, на основі імплементації міжнародно-правових норм.

У 2000 р. Організацією Об'єднаних Націй було прийнято Віденську декларацію про злочинність та правосуддя: відповіді на виклики XXI ст. Зазначений правовий акт ще не визначав у сучасному контексті проблеми кібернетичної безпеки та відповідно не закріплював правові запобіжники нормами права у цій сфері. Поряд з тим було зорієнтовано на розроблення завдань, рекомендацій та програми дій, спрямованих на запобігання правопорушенням, що пов'язані з використанням комп'ютерної техніки.

Декларація також поклала обов'язок на всі держави – члени Організації Об'єднаних Націй працювати в напрямі зміцнення їх можливостей щодо попередження, розслідування і переслідування злочинів, пов'язаних з використанням високих технологій і комп'ютерів [6]. У тому ж році Європейським Союзом було прийнято Конвенцію про взаємодопомогу в кримінальних справах між членами ЄС, у рамках якої було закріплено особливості та нові механізми міжнародної взаємодії щодо протидії кіберзлочинам [7].

Таким чином, на рівні міжнародного права було започатковано безпекове сприйняття кібернетичного простору та формування відповідного юридичного інституту, унікального за особливостями та середовищем поширення й, певним чином, самостійної галузі правових відносин. Подальший розвиток кібернетичної безпеки ґрунтувався на сприйнятті окремого правового інституту.

У свою чергу, на необхідності формування глобальної культури кібербезпеки зосереджено основні положення Резолюції Генеральної Асамблеї ООН, прийнятої в 2002 р., окреслено пріоритетні заходи й шляхи створення зазначеної культури в кіберпросторі, та розтлумачено особливі моменти механізму забезпечення цього інституту, зокрема:

необхідність визнання та охорони правового явища кібербезпеки обумовлено стрімким підвищенням кількості залучених до кіберпростору країн;

ефективна кібербезпека досягається не лише прямою діяльністю державних або правоохоронних органів, спрямованої на припинення відповідних протиправних діянь, але й превентивними заходами, крім того, даний процес повинен підтримуватися суспільством;

державні органи повинні: постійно підвищувати рівень безпеки у сфері використання інформаційних технологій та аналізувати фактори, які на нього негативно впливають [8; 9, с. 105].

Резолюцією як правове забезпечення інституту кібербезпеки визначено також ключові вимоги для суб'єктів кібернетичного простору та наголошено на їх неухильному дотриманні, зокрема:

a) обізнаність, тобто суб'єкти повинні бути інформовані про необхідність безпечного функціонування інформаційних систем і мереж, а також про можливості підвищення безпеки;

b) відповідальність за безпеку інформаційних систем та мереж згідно з місцем кожного суб'єкта;

c) реагування, тобто обов'язковість своєчасного застосування заходів щодо запобігання інцидентам, які порушують безпеку, їх виявлення й реагування на них. Суб'єкти повинні обмінюватися в належних випадках інформацією про загрози та фактори уразливості і вводити процедури, що передбачають оперативну й ефективну співпрацю в справі попередження таких інцидентів, тощо;

d) етика, що значить необхідність урахування законних інтересів інших, оскільки інформаційні системи й мережі проникли в усі куточки сучасного суспільства;

e) демократія, яка проявляється в діяльності із забезпечення цінностей, які визнаються демократичним суспільством, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації та комунікації, належний захист інформації особистого характеру, відкритість і гласність;

f) оцінка ризику, яка: дозволяє виявляти загрози та фактори уразливості; має досить широку базу, щоб охопити такі ключові внутрішні та зовнішні аспекти, як технологія, фізичні й людські фактори, застосування методик і послуги третіх осіб, що позначається на безпеці; дає можливість визначити допустимий ступінь ризику; допомагає вибрати належні інструменти контролю, що дозволяють регулювати ризик потенційного збитку інформаційним системам і мережам з урахуванням характеру та значущості інформації, що захищається;

g) проєктування і впровадження засобів забезпечення безпеки;

h) управління забезпеченням безпеки, тобто здійснення комплексного підходу до управління забезпеченням безпеки, спираючись на динамічну оцінку ризику, що охоплює всі рівні діяльності учасників і всі аспекти їх операцій;

i) переоцінка – учасники повинні піддавати питання безпеки інформаційних систем і мереж огляду й повторній оцінці та вносити належні зміни в політику, практику, заходи і процедури забезпечення безпеки, враховуючи при цьому появу нових, зміну колишніх загроз і чинників уразливості [8; 10].

Зазначені новели реалізовані також у положеннях Женевської декларації принципів побудови інформаційного суспільства, прийнятої на Всесвітньому саміті з питань інформаційного суспільства у 2003 р. Зокрема, зазначається

необхідність формування, розвитку і впровадження глобальної культури кібернетичної безпеки на основі співпраці, зокрема міжнародної, з усіма зацікавленими сторонами і компетентними міжнародними організаціями. Зорієнтовано на важливості підвищення рівня безпеки й забезпечення захисту даних, на закріпленні принципу недоторканності приватного життя, розширюючи при цьому доступ і масштаб у торговельних операціях. Акцентовано на необхідності звернення уваги на рівень соціально-економічного розвитку кожної країни і врахування пов'язаності з розвитком інформаційного суспільства [11].

Відповідним чином розвивалося законодавство і в Україні. Національний правовий інститут кібернетичної безпеки формувався як невід'ємна складова світової спільноти із врахуванням міжнародного права. Поряд із тим поняття «кібербезпека» не відразу знайшло своє відбиття в національних правових нормах. Початкове формування інституту кібернетичної безпеки здійснювалося опосередковано через суміжні сфери, дотичні до зазначеної проблеми. Початкове запровадження правових норм у контексті забезпечення кібербезпеки в Україні знайшло своє відбиття в законах України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р., «Про Національну програму інформатизації» від 2 жовтня 1992 р., «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р., Про науково-технічну інформацію» від 25 червня 1993 р., «Про охорону прав на топографії інтегральних мікросхем» від 5 листопада 1997 р. тощо.

У розвиток законодавства мали місце ініціативи й інших суб'єктів правового регулювання зазначеної сфери. Упродовж 2000–2001 рр. Президентом України видано укази «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» та «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні». Положення цих актів визначили вектор розвитку діяльності країни у сфері організації інформаційної безпеки, а також на нормативному рівні закріпили особливості використання інноваційної на той час мережі Internet та механізм її державної підтримки, яка мала прояв у [2, с. 44–45]:

створенні в найкоротші строки належних економічних, правових, технічних та інших умов для забезпечення широкого доступу громадян, органів державної влади та органів місцевого самоврядування, суб'єктів підприємницької діяльності до мережі Інтернет;

розвитку та впровадженні сучасних комп'ютерних інформаційних технологій у системі державного управління, фінансовій сфері, підприємницькій діяльності, освіті, наданні медичної та правової допомоги та інших сферах;

вирішенні завдань щодо гарантування інформаційної безпеки держави та недопущенні поширення інформації, розповсюдження якої заборонено відповідно до законодавства тощо [12; 13].

Значним кроком у розвиток національного законодавства, розширення переліку джерел права у сфері забезпечення кібернетичної безпеки є ратифікація Конвенції про кіберзлочинність, прийнятої Радою Європи у 2005 р.

У Преамбулі зазначається, що метою створення документа стала необхідність зупинення дій, спрямованих проти конфіденційності, цілісності й доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їх виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого й надійного міжнародного співробітництва [14].

У Конвенції зроблено спробу щодо класифікації кіберзлочинів, які, на думку міжнародної спільноти, несуть небезпеку щодо обробки та обміну інформацією в комп'ютерних системах, щоправда, як на рівні окремих протиправних діянь, так і на рівні узагальнювальних груп, зокрема:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані, зловживання пристроями);

2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, шахрайство);

3) правопорушення, пов'язані зі змістом (розповсюдження дитячої порнографії);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав [14].

Сучасний етап формування вітчизняного законодавства є також надзвичайно активним та результативним. Перш за все Указом Президента саме у 2016 р., який введено в дію рішенням Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», вперше було застосовано термін «кібербезпека», ґрунтуючись на сумісних поняттях «кіберпростір, кібератака», зокрема, зазначено, що відкритий та вільний кіберпростір розширює свободу й можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади й активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції. Водночас пере-

ваги сучасного цифрового світу та розвиток інформаційних технологій зумовили виникнення нових загроз національній та міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, умотивованих інтересами окремих держав, груп та осіб [15]. Поряд з цим зазначений нормативний акт непозбавлений суттєвих недоліків, зокрема, хоч і має місце термінологічне використання понять «кіберпростір, кібератака», усе ж сутність цих понять не розкривається і не закріплюється нормативно в понятійному апараті, що звужує подальші перспективи правозастосування.

Стратегією кібербезпеки України визначається наявна проблема порушення прав і свобод громадян України в кіберпросторі, у зв'язку з чим виникає необхідність, по-перше, запровадження належного механізму правового регулювання цієї сфери, а по-друге, забезпечення охорони суспільного інтересу від протиправних посягань всередині неї [2, с. 47].

У Стратегії закріплюються принципи, на яких ґрунтується діяльність щодо досягнення поставленої мети:

верховенство права і повага до прав та свобод людини і громадянина;

забезпечення національних інтересів України;

відкритість, доступність, стабільність та захищеність кіберпростору;

державно-приватне партнерство, широка співпраця з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;

пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикам;

пріоритетність запобіжних заходів;

невідворотність покарання за вчинення кіберзлочинів;

пріоритетність розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

міжнародне співробітництво з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях;

забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки [15].

У розвиток загального процесу правового регулювання у сфері кібернетичної безпеки, певні прогалини Стратегії [15] були вирішені новим Законом України «Про основні засади забезпечення кібербезпеки в Україні», головною метою якого є визначення правових та організаційних засад державної політики, спрямованої на захист життєво важливих інтересів людини і громадя-

нина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України [16]. Слід погодитися з думкою В. В. Бухарєва (V. V. Bukhariev) щодо таких особливостей цього нормативного документа, як:

фактична легалізація законом усіх понять із префіксом «кібер», які до цього часу існували переважно в наукових роботах учених чи положеннях міжнародних нормативно-правових актів;

закріплення на законодавчому рівні принципів, основних напрямів забезпечення та об'єктів кібербезпеки України;

уточнення поняття суб'єктів механізму забезпечення кібербезпеки, а також більш детальне представлення їх повноважень у цій сфері [2, с. 50].

Висновки. Таким чином, дослідивши становлення правового інституту кібернетичної безпеки, констатовано достатньо значний прогрес та сучасний стан правового забезпечення його в Україні. В основі правового забезпечення кібербезпеки вагоме місце посідає обмін інформацією між суб'єктами кібербезпеки. Важливим елементом удосконалення правового забезпечення кібербезпеки, зокрема підвищення рівня обміну даними, є адекватний та паралельний розвиток правового регулювання в межах та на основі прогресу інноваційних інформаційних технологій та Інтернет. Поряд з цим становлення національного правового інституту кібернетичної безпеки напряму пов'язується з розвитком міжнародного права в цій сфері, перш за все європейського, яке слугувало певним стандартом у сфері, інформаційної та телекомунікаційної захищеності суспільства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Спасибо І. А. Щодо історії виникнення глобальної мережі інтернет. *Право та інновації.* 2014. № 3 (7). С. 15–25.
2. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України: дис. … канд. юрид. наук: 12.00.07. Суми. 2018. 221 с.
3. Буяджи С. А. Генезис правового регулювання боротьби з кіберзлочинністю у світі. *Науковий вісник Ужгородського національного університету.* 2014. Вип. 29, ч. 2, т. 4/2. С. 145–149.
4. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / О. Є. Користін, В. М. Бутузов, В. І. Василинчук та ін. Київ: Вид. дім «Скіф», 2012. 728 с.
5. Computer-related crime: recommendation no. R. (89) 9 on computerrelated crime and final report of the European Committee on Crime Problems. Strasbour: Council of Europe, Pub. And Documentation Service; Croton, N. Y.: Manhattan Pub. Co. 1990. 114 p.

6. Віденська декларація про злочинність та правосуддя: відповіді на виклики XXI століття: міжнародний документ, декларація від 17 квіт. 2000 р. URL: https://zakon.rada.gov.ua/laws/show/995_443.
7. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу: міжнародний документ, конвенція від 29 травн. 2000 р. URL: https://zakon.rada.gov.ua/laws/show/994_238.
8. Елементи для створення глобальної культури кібербезпеки: резолюція Генеральної Асамблеї ООН від 20 груд. 2002 р. № 57/239. URL: https://zakon.rada.gov.ua/laws/show/995_b42.
9. Волох О. К. Питання кібернетичної безпеки в умовах розбудови інформаційного суспільства. *Юридичний науковий електронний журнал*. 2016. № 4. С. 104–107.
10. Мосьондз С. О. Адміністративно-правова охорона сфери науки в Україні: концептуальне бачення. *Митна справа.* 2012. № 5 (83), ч. 2, кн. 2. С. 102–107.
11. Декларація принципів «Побудова інформаційного суспільства глобальне завдання у новому тисячолітті»: міжнародний документ, декларація від 12 груд. 2003 р. URL: https://zakon.rada.gov.ua/laws/show/995_c57.
12. Про рішення Ради національної безпеки і оборони України від 31 жовт. 2001 р. «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України»: Указ Президента України від 6 груд. 2001 р. № 1193/2001. URL: https://zakon.rada.gov.ua/laws/show/1193/2001.
13. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31 жовт. 2000 р. № 928/2000. URL: https://zakon.rada.gov.ua/laws/show/928/2000.
14. Конвенція про кіберзлочинність: міжнародний документ, конвенція від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575.
15. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 берез. 2016 р. № 96/2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.
16. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19.

REFERENCES

1. Spasybo, I. A. (2014). Shchodo istorii vynyknennia hlobalnoi merezhi internet. [About the history of the emergence of the global Internet]. *Pravo ta innovatsii – Law and Innovation, 3* (7), 15–25 [in Ukrainian].
2. Bukhariev, V. V. (2018). *Administratyvno-pravovi zasady zabezpechennia kiberbezpeky Ukrainy [Administrative and legal framework for ensuring cyber security in Ukraine]*. (PhD thesis). Sumy [in Ukrainian].
3. Buiadzhy, S. A. (2014). Henezys pravovoho rehuliuvannia borotby z kiberzlochynnistiu u sviti [The genesis of the legal regulation of cybercrime in the world]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu – Scientific Bulletin of Uzhgorod National University*, *29* (2), vol. 4/2, 145–149 [in Ukrainian].

4. Korystin, O. Ye, Butuzov, V. M., & Vasylynchuk, V. I. (2012). *Protydiia kiberzlochynnosti v Ukraini: pravovi ta orhanizatsiini zasady [Cybercrime in Ukraine: Legal and Organizational Framework]*. Kyiv: Vydavnychyi dim «Skif» [in Ukrainian].
5. Computer-related crime: recommendation no. R. (89) 9 on computerrelated crime and final report of the European Committee on Crime Problems. (1990). Strasbour: Council of Europe, Pub. And Documentation Service; Croton, N. Y.: Manhattan Pub. Co.
6. Videnska deklaratsiia pro zlochynnist ta pravosuddia: vidpovidi na vyklyky XXI stolittia. (2000). [Vienna Declaration on Crime and Justice: Responding to the Challenges of the 21st Century dated April 17, 2000]. Retrieved from https://zakon.rada.gov.ua/laws/show/995_443 [in Ukrainian].
7. Konventsiia pro vzaiemodopomohu v kryminalnykh spravakh mizh derzhavamy-chlenamy Yevropeiskoho Soiuzu. (2002). [Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union dated May 29, 2000]. Retrieved from https://zakon.rada.gov.ua/laws/show/994_238 [in Ukrainian].
8. Elementy dlia stvorennia hlobalnoi kultury kiberbezpeky: rezoliutsiia Heneralnoi Asamblei OON vid 20 hrud. 2002 r. № 57/239. (2002). [Elements for Creating a Global Cybersecurity Culture dated December 20, 2002]. Retrieved from https://zakon.rada.gov.ua/laws/show/995_b42 [in Ukrainian].
9. Volokh, O. K. (2016). Pytannia kibernetychnoi bezpeky v umovakh rozbudovy informatsiinoho suspilstva [Cyber security issues in the conditions of information society development]. *Yurydychnyi naukovyi elektronnyi zhurnal – Legal scientific electronic journal*, *4*, 104–107 [in Ukrainian].
10. Mosondz, S. O. (2012). Administratyvno-pravova okhorona sfery nauky v Ukraini: kontseptualne bachennia [Administrative and Legal Protection of Science in Ukraine: A Conceptual Vision]. *Mytna sprava – Customs business*, *5* (83), part 2, book 2, 102–107 [in Ukrainian].
11. Deklaratsiia pryntsypiv «Pobudova informatsiinoho suspilstva hlobalne zavdannia u novomu tysiacholitti»: mizhnarodnyi dokument, deklaratsiia vid 12 hrud. 2003 r. (2003). [Declaration of Principles «Building an Information Society a Global Challenge in the New Millennium» dated December 12, 2003]. Retrieved from https://zakon.rada.gov.ua/laws/show/995_c57 [in Ukrainian].
12. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 31 zhovt. 2001 r. «Pro zakhody shchodo vdoskonalennia derzhavnoi informatsiinoi polityky ta zabezpechennia informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 06 hrud. 2001 r. № 1193/2001. (2001). [On the decision of the National Security and Defense Council of Ukraine of 31.10. 2001 «On measures to improve the state information policy and ensure information security of Ukraine». Presidential decree dated December 6, 2001]. Retrieved from https://zakon.rada.gov.ua/laws/show/1193/2001 [in Ukrainian].
13. Pro zakhody shchodo rozvytku natsionalnoi skladovoi hlobalnoi informatsiinoi merezhi Internet ta zabezpechennia shyrokoho dostupu do tsiiei merezhi v Ukraini:

Ukaz Prezydenta Ukrainy vid 31 zhovt. 2000 r. №928/2000. (2000). [Measures to develop the national component of the global Internet information network and to ensure wide access to this network in Ukraine. Presidential decree dated October 31, 2000]. Retrieved from https://zakon.rada.gov.ua/laws/show/928/2000 [in Ukrainian].
14. Konventsiia pro kiberzlochynnist: mizhnarodnyi dokument, konventsiia vid 23 lystop. 2001 r. (2001). [Convention on Cybercrime dated November 23, 2001]. Retrieved from https://zakon.rada.gov.ua/laws/show/994_575 [in Ukrainian].
15. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 15 berez. 2016 r. №96/2016. (2016). [On the decision of the National Security and Defense Council of Ukraine «About Ukraine's Cybersecurity Strategy». Presidential decree dated March 15, 2016]. Retrieved from https://zakon5.rada.gov.ua/laws/show/96/2016 [in Ukrainian].
16. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05 zhovt. 2017 r. №2163-VIII. (2017). [On the basic principles of cyber security in Ukraine. Law of Ukraine dated October 05, 2017]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163–19 [in Ukrainian].

Стаття надійшла до редакції 10.01.2020 р.
Стаття пройшла рецензування 13.02.2020 р.
Стаття рекомендована до опублікування 21.02.2020 р.

Л. Ю. ВЕСЕЛОВА
кандидат юридических наук, доцент кафедры административной деятельности полиции Одесского государственного университета внутренних дел, Украина, г. Одесса

СТАНОВЛЕНИЕ ПРАВОВОГО ИНСТИТУТА КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ В УКРАИНЕ

Аннотация. В статье проведено исследование становления правового института кибернетической безопасности. Рассмотрены аспекты, которые обусловили развитие института кибернетической безопасности и телекоммуникационных отношений в кибернетическом пространстве. Констатировано, что становление национального правового института кибербезопасности напрямую связывается с развитием международного права в этой сфере, прежде всего европейского, которое служило определенным стандартом в сфере информационной и телекоммуникационной защищенности общества.

Ключевые слова: кибернетическое пространство, гарантирование, информационная безопасность, цифровой мир.

L. Yu. VESELOVA
Candidate of Law, Associate Professor of the Department of Administrative of the Odessa State Police the University of Internal Affairs, Odessa, Ukraine.

ESTABLISHMENT OF THE LEGAL CYBER INSTITUTE IN UKRAINE

Problem setting. No doubt, cyber security is a well-developed legal phenomenon that has relevant regulatory frameworks. At the same time, development of cyber security as security phenomenon, and moreover, the legal relations' phenomenon, in particular, taking into account the uniqueness and peculiarities of administrative and legal regulation, is historical process whose historical and legal characteristic determines historical expression of this phenomenon development in the legal system of society. Taking into account the rapid development of information and telecommunication technologies, the law institute of cyber security requires continuous improvement and development, which makes its further research relevant.

Recent research and publications analysis. The question of becoming a law institute of cyber security was examined by scientists V. V. Bukhariev, S. A. Buiadzhy, I. A. Spasybo, and others.

Paper objective. To examine and analyse the formation of law institute of cyber security.

Paper main body. The stages of becoming of law institute of cyber security are considered in the article. The normative legal acts in the field of cyber security are analyzed. It was determined that the volitional development of cyber security institute was accompanied by simultaneous implementation of relevant legal norms in both international and national law, based on implementation of international legal norms.

Conclusions of the research. Having investigated the establishment of law institute of cyber security, considerable progress has been made and the current state of its legal support in Ukraine has been established. The exchange of information between cyber security entities is important. An important element of improving cyber security law enforcement, in particular improving data sharing, is adequate and parallel development of legal regulation within and on the basis of the advancement of innovative information technologies and the Internet. At the same time, the establishment of a national law institute of cyber security is directly linked to the development of international law in this field and, above all, of European law, which has served as standard in the field of information and telecommunications security of society.

Short Abstract for an article

Abstract. The article researches the formation of a law institute of cyber security. The aspects that led to development of the institute of cyber security and telecommunication relations in cyber space are considered. It is stated that establishment of national law institute of cyber security is directly related to development of international law in this field and,

above all, a European one, which has served as standard in the field of information and telecommunication security of society.

Key words: cyberspace, information security, digital world.

Article details:
Received: 10 January 2020
Revised: 13 Februare 2020
Accepted: 21 February 2020

Рекомендоване цитування: Веселова Л. Ю. Становлення правового інституту кібернетичної безпеки в Україні. *Економічна теорія та право*. 2020. № 1 (40). С. 113–126. DOI: 10.31359/2411-5584-2020-40-1-113.

Suggested Citation: Veselova, L. Yu. (2020). Stanovlennia pravovoho instytutu kibernetychnoi bezpeky v Ukraini [Establishment of the legal cyber institute in Ukraine]. *Ekonomichna teoriia ta pravo – Economic Theory and Law, 1* (40), 113–126. DOI: 10.31359/2411-5584-2020-40-1-113.