Кухарська Наталія Павлівна, кандидат фізико-математичних наук, доцент, доцент кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності, Львів, Україна.
ORCID: 0000-0002-0896-8361.
E-mail: kukharska.n@gmail.com.
Полотай Орест Іванович, кандидат технічних наук, доцент кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності, Львів, Україна.
ORCID: 0000-0003-4593-8601.
E-mail: orest.polotaj@gmail.com.

Kukharska Nataliia, candidate of physical and mathematical sciences, associate professor, associate professor of information security academic department, Lviv state university of life safety, Lviv, Ukraine.
Polotai Orest, candidate of technical sciences, associate professor of information security academic department, Lviv state university of life safety, Lviv, Ukraine.

DOI: 10.20535/2411-1031.2019.7.2.190559
УДК 004.056.53

ВІКТОР ГОРЛИНСЬКИЙ,
БОРИС ГОРЛИНСЬКИЙ

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Показано, що глобалізаційний вплив на кіберпростір, що проявляється у розповсюдженні кіберзлочинності, кібертероризму та інформаційній експансії, потребує його надійного захисту, а забезпечення кібербезпеки України в умовах проведення Операції об'єднаних сил, постає невід'ємною складовою і чинником забезпечення національної безпеки. Доведено, що побудова усталеної системи інформаційної безпеки держави в умовах глобалізації та розвитку інформаційних технологій і телекомунікаційних систем потребує з'ясування системоутворювальних основ і базових принципів системи забезпечення кібербезпеки як найважливішої складової інформаційної безпеки України. На підставі аналізу наукових публікацій стверджується, що дослідження проблеми забезпечення інформаційної безпеки відбувається, як правило, за двома основними напрямами – інформаційно-психологічному, спрямованому на захист свідомості від негативного інформаційного впливу та інформаційно-технічному, в якому основним об'єктом захисту є інформаційні ресурси в інформаційно-телекомунікаційних системах. Обґрунтовано, що методологічною основою розв'язання цього питання є системний підхід, який дозволяє враховувати у розумінні інформаційної безпеки як системного явища, не тільки певні види інформаційних загроз, але і багатофункціональність і багатовимірність предметного поля інформаційної безпеки. Доведено, що на підставі визначення об'єктів, що потребують захисту, розгалуження функцій і секторів відповідальності державних і приватних структур, доцільно розрізняти предметні області інформаційної та кібербезпеки. Сформульовано визначення інформаційної безпеки в широкому сенсі поняття, як сфери національної безпеки, що характеризується всебічною (правовою, економічною, техніко-технологічною і організаційною) захищеністю усталеного функціонування інформаційного простору, захищеністю інформаційних, інформаційно-технологічних і безпекових інтересів держави і

суспільства, інформаційних і прав, і свобод людини. Запропоновано підхід, згідно з яким, важливо, по-перше, відокремлювати змістовну сторону понять інформаційної та кібербезпеки як у широкому, так і вузькому сенсі слова, по-друге, згідно із сферою охоплення інформаційного і кіберпросторів, розрізняти їх функціональний зміст у державному, національному і глобальному вимірах. Зроблено висновок, що подальше розроблення науково-теоретичних, правових, організаційних засад забезпечення кібербезпеки, є одним з найважливіших завдань української науки, особливо в умовах на шляху до євроатлантичної інтеграції України.

Ключові слова: інформатизація; інформаційні загрози; інформаційна безпека; кібербезпека; інформаційний простір; кіберпростір; кіберзагрози.

Постановка проблеми. Однією з важливіших умов побудови в Україні суспільства сталого розвитку, згідно з вимогами ЮНЕСКО, є створення відкритого інформаційного суспільства. Але реалізація ідей інформаційного суспільства як наслідку цифрової революції, на шляху до євроатлантичної інтеграції України, можлива лише за умов забезпечення сталої системи забезпечення інформаційної безпеки.

Ефективність, сталість і захищеність державного інформаційного простору є важливим чинником надійного забезпечення національної безпеки, передумовою переходу українського суспільства на більш високу ступінь сталого розвитку. Інформаційно-телекомунікаційна складова стає одним із найважливіших елементів інформаційної безпеки суспільства і держави. Телекомунікаційні технологій підвищують ефективність управління силами оборони, бойові можливості техніки і озброєння. Але, поряд з якісними позитивними зрушеннями, розвиток цифрового світу зумовив виникнення нових небезпек, поширення випадків незаконного збирання, зберігання, використання, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність набула транснаціонального характеру та здатності завдати значної шкоди інтересам особи, суспільства і держави [1]. На погляд дослідників і експертів, кіберпростір залишається критично слабкою складовою національної безпеки та зберігає певний ступінь уразливості до кіберзагроз. Об’єктами кібератак і кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій [2]. Джерелом таких загроз стають іноземні спеціальні структури, організовані злочинні хакерські групи, терористичні та екстремістські організації [3]. В умовах проведення операції об’єднаних сил, розв’язання проблеми вдосконалення національної системи кібербезпеки, надійного захисту національного кіберпростору, постає найактуальнішим завданням теорії і практики державотворення.

Отже, необхідність побудови сталої та надійної системи забезпечення кібербезпеки України в умовах інтернаціоналізації кіберзлочинності, розповсюдження кібертероризму та інформаційної експансії в кіберпросторі, в першу чергу, потребує з’ясування теоретичних засад її відокремлення від системи інформаційної безпеки України як підсистемного утворення.

Аналіз останніх досліджень і публікацій. Питання, що пов’язані з утвердженням принципів інформаційного суспільства та їхнього неоднозначного впливу на людину і суспільство, теоретично були поставлені в працях Д. Белла, З. Бжезинского, Ж. Бодрийяра, Ю. Габермаса, У. Дайзарда, П. Дракера, М. Кастельса, Н. Луманна, М. Маклюэна, Й. Масуды, Дж. Мартина, А. Некласи, М. Постера, Т. Стоуньера, Е. Тоффлера, А. Турена та інших представників філософії постмодерну. Але, найбільш системне відображення, проблема формування системи захисту та інформаційного простору в умовах глобалізації та вільного обігу інформації, знайшла в роботах О. Баранова, М. Гуцалюка, Р. Калюжного, Б. Кормича, А. Кузьменка, О. Литвиненка, М. Мазура, В. Остроухова, Г. Почепцова, О. Сосніна, А. Старіша, В. Толубки, М. Швеця.

Безпосередньо, поняття, складові системи забезпечення кібербезпеки, її функції та завдання розглядаються у наукових працях вітчизняних дослідників, а саме: Є. Бабича, О. Баранова, В. Богуша, В. Бурячка, Д. Дубова, С. Морозюк, І. Діордіци, О. Климчука, О. Корнейки, С. Мельника, В. Кащука, А. Марущака, М. Ожевана, С. Толюпи, В. Фурашева, В. Хорошка, В. Шеломенцева. Поряд з суттєвими і плідними результатами наукових досліджень у сфері кібербезпеки, залишається низка теоретичних питань, що потребують поглиблення, з'ясування і конкретизації, розкриття яких, дозволить якісно підвищити рівень захисту національного кіберпростору. Одним з таких актуальних питань, постає розроблення і обґрунтування принципів і теоретичних положень побудови теоретичної моделі системи кібербезпеки. Але вирішення цієї проблеми, в першу чергу, потребує з'ясування теоретичних засад її відокремлення як складової системи інформаційної безпеки.

Метою статті є визначення і обґрунтування теоретичних засад відокремлення кібербезпеки як підсистемного утворення інформаційної безпеки України.

Виклад основного матеріалу дослідження. Глобалізація є однією з головних тенденцій у розвитку сучасного цифрового світу, що істотно впливає на Україну. Глобалізаційний вплив на кіберпростір, що проявляється у інтернаціоналізації кіберзлочинності, кібертероризму, інформаційній експансії у кіберпросторі, потребує його надійного захисту, а забезпечення кібербезпеки, особливо в умовах проведення операції об'єднаних сил, постає невід'ємною складовою сучасних світових процесів. Збиток, який завдає кіберзлочинність, завдяки використанню найновіших інформаційно-комунікаційних технологій, на переконання експертів, значно зростає у всьому світі [4].

Отже, у контексті сучасного геополітичного стану, в якому опинилася Україна, проблема надійного захисту національного кіберпростору і протидія загрозам національній безпеці, що виникають у кіберпросторі, набула важливого науково-теоретичного і практичного значення. Але дана проблема є похідною від багатьох питань, що стоять перед утвердженням принципів інформаційного суспільства та забезпечення інформаційної безпеки в Україні. Саме у такому контексті – у зв'язку з питанням побудови інформаційного суспільства в Україні, наведено визначення поняття "інформаційна безпека" у Законі України "Про основні заходи розвитку інформаційного суспільства в Україні на 2007-2015 роки". В цьому Законі інформаційна безпека визначається як "стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації" [5]. Але у наведеному визначенні вже можна побачити певне протиріччя, або методологічну неузгодженість між змістом понять, що визначають об'єкти інформаційної безпеки.

Теоретичне вирішення проблеми забезпечення інформаційної безпеки в Україні, здійснюється, переважно, за двома основними напрямами. В дослідженнях за першим напрямом акцентується увага на технологічній, правовій і організаційній захищеності телекомунікаційних систем та інформаційних ресурсів держави як основного об'єкту забезпечення інформаційної безпеки, а поняття інформаційної безпеки пов'язується, переважно, зі захистом даних. У дослідженнях за другим напрямом, спираючись на гуманітарні аспекти негативних наслідків впливу інформації та інформаційних технологій на суспільство, колективну та індивідуальну свідомість, автори роблять наголос на необхідності протидії інформаційним загрозам, у контексті їх негативного впливу на свідомість, пропонуючи розв'язання проблеми захисту інформаційного простору в ідеологічному, психологічному і правовому ключі. У межах другого напряму відокремлюють, як об'єкт захисту, національну свідомість та життєвоважливі інформаційні інтереси людини і суспільства, що захищаються також нормами національного права. *Тобто, у межах загального об'єкту забезпечення інформаційної безпеки – інтересів людини, суспільства і*

держави, в одному випадку, пропонується розглядати інформаційні ресурси і телекомунікаційні системи держави, в іншому, – індивідуальну, суспільну, національну свідомість та інтереси громадян [6]. Теоретичне розв'язання означеного протиріччя між інформаційно-психологічним та інформаційно-технічним аспектами інформаційної та кібербезпеки має важливу теоретичну і практичну значущість для сталого функціонування національної безпеки як цілісної і надійної системи і стає можливим за умов застосування системного підходу до забезпечення інформаційної безпеки України [7], [8].

Тотальна залежність життєстійкості суспільства і держави від сталості функціонування і захищеності інформації в телекомунікаційних системах, зумовлює необхідність розв'язання поставленої теоретичної проблеми на підставі науково обґрунтованого розмежування сфер охоплення, завдань, аспектів захисту, що вирішуються в полі відповідальності державних і приватних структур забезпечення інформаційної безпеки в її широкому розумінні. У свою чергу, це потребує розмежування сфер діяльності і завдань, що вирішуються згідно зі сферами охоплення предметного поля інформаційної безпеки, яке має багатовимірний характер та відокремлення кібернетичного простору. У даному контексті можна цілком погодитись з твердженням про те, що поняття "кібербезпека" та "інформаційна безпека" є спорідненими, проте не тотожними. Предметна сфера інформаційної безпеки містить більш широкий спектр питань, зокрема, щодо забезпечення позитивного іміджу держави на міжнародному рівні, інформаційних прав і свобод її громадян, інформаційного суверенітету, інформаційно-психологічного протиборства, здійснення правоохоронної та контррозвідувальної діяльності з цих питань тощо [9]. З погляду на проблему через призму системного підходу, це є вимогою врахування впливу на систему забезпечення кібербезпеки не тільки внутрісистемних, але і ззовні системних зв'язків, що функціонально поєднують систему забезпечення кібербезпеки з системами інформаційної і національної безпеки.

Отже, методологічною основою розв'язання поставленої проблеми, є системний підхід, який має враховувати у розумінні інформаційної безпеки, як системного явища, не тільки класифікацію загроз, але і з'ясування багатофункціональності і багатовимірності предметного поля інформаційної безпеки на підставі розгалуження функцій і класифікації об'єктів, що потребують захисту. Це структурно-функціональний, аналітичний, організаційно-управлінський, інституціональний, фінансово-економічний, соціально-правовий та інші виміри системи забезпечення інформаційної безпеки. Саме такий підхід дозволить не тільки виключити дублювання, скоротити ресурсні витрати та сконцентрувати зусилля на розв'язанні ключової проблеми забезпечення інформаційної безпеки – як проблеми інформаційно-технологічної захищеності життєвоважливих інтересів людини, суспільства і держави, але детально з'ясувати складові системи забезпечення кібербезпеки. В цьому контексті є важливим бачення "контурів майбутньої системи кібербезпеки" як складової концепції розвитку системи спеціального зв'язку та захисту інформації [10].

Згідно з запропонованим підходом і відповідно до об'єкту захисту, пропонується відрізняти такі *проблемні поля інформаційної безпеки:* а) вплив інформаційних загроз на державні інформаційні ресурси, інформаційні системи та інформацію, розглядати в проблемному полі інформаційної безпеки в вузькому сенсі її розуміння – як "інформаційної безпеки держави"; б) вплив інформаційних загроз на державні та приватні інформаційно-технологічні та телекомунікаційні системи, – в проблемному полі кібербезпеки; г) інформаційний вплив на свідомість, культуру і психіку людини передбачається розглядати в теоретичному полі інформаційної безпеки в її широкому сенсі, або в контексті психологічної і духовної безпеки, які в теорії національної безпеки досліджуються в предметному полі гуманітарної безпеки, згідно з об'єктом інформаційного впливу загроз і предметом захисту – свідомості, психіки або культури [6]. Аналогічно припускається розглядати питання негативного інформаційного впливу на політичну, економічну, науково-технологічну, комерційну, демографічну, екологічну сфери діяльності. *Але, в цілому, якщо проблема досліджується переважно в загальному контексті аналізу інформаційних загроз,*

то незалежно від предмету безпосереднього впливу і об'єкту захисту, її правомірно і доцільно вважати аспектом забезпечення інформаційної безпеки в широкому сенсі розуміння цього поняття. Такий підхід передбачає проведення комплексних і системних досліджень інформаційної безпеки, як підсистеми національної безпеки, що пронизує всі рівні суспільного життя та розроблення її концептуальних основ. І лише на даній підставі, стає можливим науково обґрунтоване вироблення загальних основ забезпечення інформаційної безпеки та, зокрема, кібербезпеки, систематизація і в подальшому кодифікація правових актів в цієї сфері як галузі інформаційного права, тобто створення інформаційного кодексу України.

Іншим питанням, що має бути розглянуто в контексті попереднього, – це питання розподілу зон відповідальності в забезпеченні інформаційної безпеки. З врахуванням наукових здобутків у цій сфері, пропонується на підставі розгалуження проблеми регулювання інформаційної безпеки за такими основними напрямами. *По-перше*, це забезпечення інформаційної безпеки держави, захист інформаційних інтересів держави, суспільства і людини, що вирішується державними структурами і переважно, методами правового регулювання і громадського контролю на підставі їх структурної і функціональної інтеграції, удосконалення нормативно-правової бази (створення інформаційного кодексу), згідно з євроатлантичними стандартами. *По-друге*, це забезпечення кібербезпеки і захист життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, що забезпечується переважно держаними і, частково, громадськими організаціями з розгалуженням відповідальності між суб'єктами за функціонально-структурними ознаками. *По-третє*, це регулювання інформаційних відносин в громадянському суспільстві через активізацію діяльності неурядових, громадських і правозахистних організацій на підставі розвитку і впровадження цінностей інформаційного суспільства, захисту інформаційних прав і свобод людини, формування інформаційної культури та її складової – культури інформаційної безпеки засобами освіти, просвіти, самоосвіти та інтеграції інформаційних відносин в глобальний інформаційній простір.

Аналіз теоретичних здобутків в досліджуваній області, дозволяє визначити інформаційну безпеку в широкому сенсі поняття, як сферу національної безпеки, що характеризується всебічною (правовою, економічною, техніко-технологічною і організаційною) захищеністю усталеного функціонування інформаційного простору, захищеністю інформаційних, інформаційно-технологічних і безпекових інтересів держави і суспільства, інформаційних і прав і свобод людини.

Наведена аргументація вимагає розроблення концептуальних основ забезпечення кібербезпеки як підсистеми інформаційної безпеки, її теоретичного редукування та функціонального розгалуження з урахуванням вимог Євросоюзу і НАТО, удосконалення інститутів її реалізації в Україні.

Генезис кібербезпеки як початок її практичного відокремлення від інформаційної безпеки, а також входження в науковий обіг поняття "кіберпростору", пов'язується з прийняттям у 2000 році Окінавській хартії глобального інформаційного суспільства, яка розглядається світовою спільнотою як "конституція" інформаційного суспільства. У хартії зазначається, що зусилля міжнародного співтовариства, спрямовані на розвиток глобального інформаційного суспільства, мають бути скоординованими, щоб забезпечити *безпечний та вільний від злочинності кіберпростір* [11].

На першому Всесвітньому саміті з питань інформаційного суспільства, забезпечення інформаційної безпеки і безпеки мереж були відзначені як один з принципів побудови інформаційного суспільства. Вперше на світовому рівні поставлено питання про запровадження *глобальної культури кібербезпеки* [12]. Переважно, положення підсумкових документів Всесвітнього саміту впроваджені у Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки", де поряд з іншими стратегічними цілями, проголошено необхідність покращення стану інформаційної безпеки. Але стратегічні

цілі на цьому шляху закріплені у "Стратегії розвитку інформаційного суспільства в Україні", схваленої розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р. Стратегія визначає мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні, завдання, спрямовані на їх досягнення, а також основні напрями, етапи і механізм їх реалізації з урахуванням сучасних тенденцій та особливостей розвитку України в перспективі до 2020 року. Для розвитку інформаційного суспільства Стратегія, поряд з іншими, пропонує застосовування принципів гарантованості права на інформацію, правомірності одержання, використання, поширення, зберігання та *захисту інформації та інформаційної безпеки*. Проте тлумачення, або визначення поняття інформаційної безпеки у Стратегії відсутні.

Відображенням стурбованості світової спільноти ризиком того, що комп'ютерні мережі та електронна інформація може використовуватися для здійснення кримінальних правопорушень, стало прийняття Конвенції про кіберзлочинність (Будапешт, 23 листопада 2001 року), яку ратифіковано Україною у 2005 році. Потрібно зауважити, що у Конвенції, вперше на світовому рівні, окреслено низку небезпек, що виникають безпосередньо у кіберпросторі, хоча дана категорія не застосовувалась. *Це дії, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними.* Загрозами, які кваліфіковані як правопорушення, визначено такі: незаконний доступ до комп'ютерної системи; нелегальне перехоплення технічними засобами комп'ютерних даних, які не є призначеними для публічного користування; втручання у дані (навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це); втручання у комп'ютерну систему; зловживання пристроями, включаючи комп'ютерні програми; шахрайство, пов'язане з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав [13]. Загалом, Конвенція визначила види правопорушень у сфері використання комп'ютерної інформації, визначила повноваження, достатні для ефективної боротьби з такими кримінальними правопорушеннями, як на внутрішньодержавному, так і на міжнародному рівнях, визначила порядок укладення домовленостей щодо швидкого і надійного міжнародного співробітництва.

Важливим кроком на шляху до створення безпечного кіберпростору стало підписання, під час Лісабонського саміту 19 листопада 2010 року, нової Стратегічної концепції оборони та безпеки країн-членів НАТО, що фактично прирівняла загрози кібератак до військових загроз, що, у свою чергу, передбачає можливість відповіді на масовані кібератаки із застосуванням кіберпідрозділів національних збройних сил. Кібератаки стали одним з найбільш небезпечних викликів безпеці країн-членів Альянсу, а *забезпечення кібербезпеки визначено як пріоритет Альянсу*. Доктрина НАТО "Strategic Concept NATO 2010", у свою чергу, відзначає співробітництво з країнами-партнерами у сфері розбудови системи забезпечення кібербезпеки Альянсу як ключового механізму заходів Організації Північноатлантичного договору із забезпечення кіберзахисту [14]. Знаковою подією на шляху євроінтеграції України, в контексті можливості запозичення досвіду союзників у створенні надійного захисту кіберпростору, стала зустріч глав держав та голів урядів країн – учасниць Північноатлантичного альянсу, що відбулася у 2016 році, де відбулося підписання договору про співпрацю між ЄС та НАТО у сфері *кіберзахисту*.

Але, найбільш важливим і суттєвим кроком, на шляху розв'язання протиріч стосовно об'єкту інформаційної безпеки та створенням умов для безпечного функціонування кіберпростору, стало прийняття Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року, у якій *вперше дається визначення кібербезпеки, окреслено основи Національної системи кібербезпеки, визначені принципи, пріоритети та напрями забезпечення кібербезпеки України, означено загрози кібербезпеці*. Зауважено, що кіберпростір поступово перетворюється на окрему сферу ведення бойових

дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу. Сучасні інформаційно-телекомунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема, шляхом порушення роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває діяльність у кіберпросторі у вигляді атак на урядові та приватні веб сайти в мережі Інтернет. Об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які мають гарантувати безпеку. Новітні технології застосовуються також для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації. У Стратегії вперше конкретизовано пріоритетні напрями забезпечення кібербезпеки України, це: розвиток безпечного, стабільного і надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури; кіберзахист критичної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; боротьба з кіберзлочинністю. З огляду на значущість організаційної і функціональної координації, підкреслено, що національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [2].

Однак, треба розуміти, що на час прийняття документу, відсутнє єдине розуміння і тлумачення понять, що утворюються прикметником "кібернетичний". Відсутність єдиної термінології для будь-якої сфери діяльності є явищем суттєво негативним, до того ж аналіз публікацій, стосовно змісту таких базових понять, як кіберпростір, кібербезпека, свідчить про їх іноді суперечливе розуміння фахівцями. Подібна ситуація є неприпустимою для повноцінного існування та ефективного розвитку сфери кібербезпеки [15].

Прийняття в 2017 році Закону "Про основні засади забезпечення кібербезпеки України" (далі – Закон), дозволило не тільки виокремити в інформаційному просторі інститут кібербезпеки, але і визначити поле розгортання відносин, що функціонують у кіберпросторі, визначити принципові положення, поняття і норми, що регулюють правові відносини у цій сфері. Законом визначено правові та організаційні основи забезпечення захисту життєвоважливих 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.

В контексті досліджуваної проблеми, варто розглянути деякі положення змістовного боку Закону. У Законі наведено 21 нове або уточнене поняття, що мають важливе значення для побудови системи кібербезпеки, серед них, такі як кібербезпека, кіберзагроза, кіберзахист, кібероборона, кіберзлочин, кіберпростір. Введені законом у обіг поняття, утворюються на підставі поєднання з прикметником – "кібернетичний", похідним від дав.-грец. "кібернетика", за яким розуміється мистецтво управління, керування складними кібернетичними системами різної природи походження. Але, власно в інформаційному контексті, визначення кібернетики сформульовано одним з її засновників академіком Віктором Глушковим – як науки про загальні закони одержання, зберігання, передавання й перетворення інформації у складних системах управління. Проте і це визначення не відокремлює технічні та електронні системи управління від соціальних і природних систем. Це один з термінологічних чинників, що зумовлює різні підходи до розуміння всіх понять, що походять від слова кібернетика. *Тому, потрібно відрізняти розуміння кібернетики в широкому сенсі слова, що охоплює собою всі можливі інформаційні системи управління та у*

вузькому сенсі, що традиційно застосовується для розуміння тільки електронних систем управління – кіберсистем. Але виходячи з наявності базової суперечності у поняті "кібернетика", в розумінні поняття "кіберсистема" також зберігається двозначність, що потребує визначень за сферою, чи простором функціонування. На цій підставі дослідниками пропонується підхід, згідно з яким, поняття інформаційного простору розуміється як сфера функціонування будь яких інформаційних систем, зокрема, й кібернетичних, а кіберпростір, є більш вузькім поняттям, що є сферою функціонування кіберсистем [15]. Однак, визначення "кіберпростору", наведене у Законі, є більш широким і містить низку конкретних ознак, що розширюють значення поняття.

Однак, і цей підхід не вирішує однозначно межі розведення інформаційного і кібернетичного просторів у розумінні поняття "кібербезпека". Прикладами можуть бути публікації матеріалів в Інтернет виданні, що містять ознаки порушення прав на інтелектуальну власність, образи, приниження честі й гідності людини або інші ознаки порушення вимог національної безпеки і норм права. Постає питання – на скільки оправданим відносити такі порушення до проблем кібербезпеки? *Розведення сфер з інформаційної і кібербезпеки має базуватись, не лише на просторовій підставі, але і на підставі предметної ознаки порушення – стосовно чого воно скоєно. Якщо немає протиправного втручання в інформаційно-телекомунікаційну систему, то злочин, скоєний за допомогою електронних засобів, відносити до загроз кібербезпеці не варто.* Але визначення кібербезпеки, що сформульовано в Законі, не дає підстав для чіткого розмежування питань, що стосуються власне проблеми несанкціонованого втручання в інформаційно-телекомунікаційну систему, що створює загрозу кібербезпеці і таких, що стосуються порушень, скоєних в кіберпросторі, але без несанкціонованого втручання в систему. Дану проблему забезпечення кібербезпеки, можна розв'язати завдяки застосуванню поняття "кіберзагроза", але визначення, наведене в Законі, є на стільки широким, що також не дає такої можливості. *Доцільно розрізняти поняття "загрози кібербезпеці", тобто загрози функціонуванню системи забезпечення кібербезпеки, з одного боку, та інформаційні безпекові загрози, що виникають у кіберпросторі, або "кіберзагрози" у широкому сенсі поняття, з іншого боку*. Врахування запропонованого підходу може бути плідним в контексті розподілу функціональної відповідальності між державними структурами, призначеними для забезпечення кібербезпеки.

З огляду на наведені аргументи, важливим, є чітко визначене Законом, поняття "кіберзахисту" як сукупності організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [16]. Наведене в Законі визначення "кіберзахисту" дозволяє розмежувати, не тільки технічні і гуманітарні аспекти у понятті кібербезпеки, розподілити відповідальність, але і відокремити "кіберзагрози" від злочинів, скоєних у кіберпросторі. Теоретичною підставою для розмежування поля відповідальності у кіберпросторі, є розрізнення об'єкта захисту, що наведений у визначенні інформаційної безпеки – *"життєво важливі інтереси людини, суспільства і держави"* в інформаційному просторі, з одного боку, і об'єкта захисту, згідно з визначенням "кіберзахисту" як *"криптографічного та технічного захисту інформації"*, з іншого. Тобто, в другому випадку захист інформації в кіберпросторі є умовою захисту інтересів в інформаційному просторі.

Іншим є питання відповідності об'єктів кібербезпеки та кіберзахисту, наведених у Законі, обмеженням дії Закону, а також визначенню "національної системи кібербезпеки". Тобто, не доцільно виключати із сфери впливу Закону "діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення" [16], оскільки це стосується національних інтересів держави і національної системи кібербезпеки.

Викликають питання й інші обмеження сфери дії Закону, якщо співвідносити змістовну і сутнісну сторони визначення кібербезпеки з обмеженнями, але це питання – відповідальності за кібербезпеку між державними, приватними і міжнародними суб'єктами, згідно з розумінням сфери охоплення державного, національного і глобального кіберпростору. *Тобто, необхідно розрізняти розуміння кібербезпеки, що стосується сфери державних інтересів, згідно з наведеними обмеженнями, в державному кіберпросторі, з одного боку, і більш широкій зміст цього поняття, наведений, що розповсюджується загалом на національний кіберпростір, з іншого боку.* Але в Законі дається визначення кіберпростору тільки в його глобальному розумінні – як "середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних" [16].

Таким чином, виникає проблема теоретичного і правового розгалуження кіберпростору на підставі відокремлення сфер відповідальності державних, громадських, приватних та міжнародних структур кібербезпеки, (або власності телекомунікаційних систем) і, пов'язане з нею, питання узгодження і вдосконалення норм національного і міжнародного законодавства у сфері регулювання інформаційних відносин у національному, регіональному і глобальному кіберпросторі, особливо в умовах на шляху до євроатлантичної інтеграції України. *В якості провідних ознак конкретизації видів кіберпростору пропонується застосовувати, як сфери відповідальності за кібербезпеку, загальні безпекові та геополітичні інтереси суб'єктів кібербезпеки (національні, регіональні, міжрегіональні і глобальні), так і форми власності на телекомунікаційні мережі.* Розв'язання цього питання надає підстави для подальшого вдосконалення технічного і криптографічного захисту інформації в інформаційно-телекомунікаційних системах, як однієї з найважливіших функцій захисту кіберпростору і базової функціональної відмінності забезпечення кібербезпеки в контексті її відокремлення від інформаційної.

Звертаючись до проблеми розгалуження сфер функціонального охоплення інформаційної і кібербезпеки необхідно звернутись до офіційного визначення поняття "система інформаційної безпеки", що наведено у Постанові КМУ "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19 червня 2019 р. № 518 [17]. Це визначення, за своїм змістом, стосується лише кіберзахисту об'єктів критичної інфраструктури, тобто кіберпростору, але наведено воно під більш широким, за змістом, поняттям – "система інформаційної безпеки", яке має охоплювати загалом весь інформаційний простір – як сферу функціонування мас-медіа, просвіти, освіти, пропаганди і мистецтва. Це можна розглядати як зневагу да формально логічного правила пропорційності дефідента і дефініції. Але назва Постанови надає підстави для адекватного розуміння поняття "система інформаційної безпеки" – в його вузькому сенсі, що стосується тільки кіберпростору.

Висновки. Комплексна захищеність сталого функціонування інформаційної сфери в інтересах людини, суспільства і держави потребує удосконалення теоретичних, правових і організаційних основ надійного захисту національного кіберпростору.

Проблема визначення і обґрунтування теоретичних засад відокремлення кібербезпеки як підсистемного утворення інформаційної безпеки України, згідно з вимогами структурно-функціонального аналізу, вимагає вивчення і класифікації інформаційних і кіберзагроз, з'ясування багатофункціональності і багатовимірності предметного поля інформаційної і кібернетичної безпеки на підставі розгалуження їх функцій, класифікації і визначення об'єктів, що потребують захисту, стосовно державного, загальнонаціонального, регіонального і глобального інформаційного і кібернетичного простору.

Теоретичне розв'язання цієї проблеми надає підстави для подальшого вдосконалення технічного і криптографічного захисту і завадостійкісті інформації в інформаційно-телекомунікаційних системах, як однієї з найважливіших функцій захисту кіберпростору, поряд з іншими.

У перспективах подальших досліджень питання розробки науково-теоретичних, правових, організаційних питань забезпечення кібербезпеки, є одним з найважливіших завдань теорії і практики, особливо в умовах на шляху до євроатлантичної інтеграції України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] М.М. Присяжнюк, та Є.І. Цифра, "Особливості забезпечення кібербезпеки", *Експертні системи та підтримка рішень, Реєстрація, зберігання та обробка даних*, т. 19, № 2, 2017. [Електронний ресурс]. Доступно: https://nbuv.gov.ua/UJRN/rzod_2017_19_2_B. Дата звернення: Черв. 21, 2019.

[2] Президент України. (2016, Бер. 15). *Указ № 96/2016. Про рішення Ради національної безпеки і оборони України від 27 січ. 2016 р. "Про Стратегію кібербезпеки України"*. [Електронний ресурс]. Доступно: http://zakon.rada.gov.ua/laws/show/96/2016. Дата звернення: Черв. 21, 2019.

[3] О.В. Климчук, Інформаційна та кібербезпека в сучасному світі: досвід СБУ, 2018. [Електронний ресурс]. Доступно: https://ua-news.liga.net/politics/opinion/informatsiyna-ta-kiberbezpeka-v-suchasnomu-sviti-dosvid-sbu. Дата звернення: Черв. 21, 2019.

[4] С.Л. Гнатюк, Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України, *Національний інститут стратегічних досліджень, Аналітичні матеріали* 2019. [Електронний ресурс]. Доступно: https://niss.gov.ua/doslidzhennya/analitichni-materiali/informaciyni-strategii/. Дата звернення: Черв. 21, 2019.

[5] Верховна Рада України. V скликання, 2 сесія. (2007, січ. 9). *Закон України № 537-V. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки*. [Електронний ресурс]. Доступно: http://zakon.rada. gov.ua/laws/show/537-16. Дата звернення: Черв. 21, 2019.

[6] В.В. Горлинський, *Філософія безпеки і сталого людського розвитку: ціннісний вимір*: *монографія*. Київ, Україна: Парапан, 2011.

[7] І. Діордіца, "Система забезпечення кібербезпеки: сутність та призначення", *Підприємство, господарство і право. Інформаційне право* 7/2018. [Електронний ресурс]. Доступно: https:// phd.znu.edu.ua/page//aref/07_2018/Diorditsa_aref.pdf. Дата звернення: Черв. 21, 2019.

[8] Ю. Кожедуб, "Організаційна парадигма забезпечення інформаційної безпеки", *Information Technology and Security*, vol. 6, iss. 1 (10). pp. 26-36. July-December 2018. doi: 10.20535/2411-1031.2018.6.1.153133.

[9] Ю. Даник, та О. Корнейко, "Основи методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони України", *Information Technology and Security*, vol. 6, iss. 2 (11). pp. 105-123. July-December 2018. doi: 10.20535/2411-1031.2018.6.2. 153495.

[10] Ю. Лапаєв, та В. Петров: "Я не знаю жодного випадку витоку інформації саме із захищених урядових мереж", *Суспільство, Український тиждень* № 48 (628), 28 лист, 2019. [Електронний ресурс]. Доступно: https:// https://m.tyzhden.ua/Society/238132. Дата звернення: Лист. 30, 2019.

[11] "Окінавська хартія глобального інформаційного суспільства" у М. З. Згуровський, *Розвиток інформаційного суспільства в Україні: правове регулювання у сфері інформаційних відносин*. Київ, Україна: НТУУ "КПІ", 2006.

[12] Всесвітня зустріч на найвищому рівні з питань інформаційного суспільства. Женева, 2003 – Туніс, 2005 р. Декларація принципів. Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті у М. З. Згуровський, *Розвиток інформаційного суспільства в Україні: правове регулювання у сфері інформаційних відносин*. Київ, Україна: НТУУ "КПІ", 2006.

[13] Верховна Рада України. IV скликання, 8 сесія. (2005, Верес. 7). *Закон № 2824-IV (2824-15). Конвенція про кіберзлочинність*. [Електронний ресурс]. Доступно: https://zakon5.rada.gov.ua/ laws/show/994-789. Дата звернення: Черв. 21, 2019.

[14] Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation. Active Engagement, *Modern Defence* / NATO. [Online]. Available: http: //www. nato. int/lisbon2010/strategic-concept-2010-eng.pdf. Accessed on: June 21, 2019.

[15] О. Архипов, та В. Бровко, Кібербезпека – виникнення, формування, розуміння, на *VIII наук.-практ. конф. Актуальні проблеми управління інформаційною безпекою держави*. [Електронний ресурс]. Доступно: http://www.academy.ssu.gov.ua/upload/file/Zbirnyk_ materialiv_konferencii_24. Дата звернення: Черв. 21, 2019.

[16] Верховна Рада України. VIII скликання, 7 сесія. (2017, жовт. 5). *Закон № 2163-VIII. Про основні засади кібербезпеки України*. [Електронний ресурс]. Доступно: http://zakon.rada. gov.ua/laws/show/2163-19. Дата звернення: Черв. 21, 2019.

[17] Кабінет Міністрів України. (2019, черв. 19). *Постанова № 518. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/518-2019-п. Дата звернення: Черв. 21, 2019.

Стаття надійшла до редакції 05.07.2019.

REFERENCE

[1] M.M. Prysyazhnyuk, and E.I. Cifra, "Features of providing cybersecurity", *Expert systems and decision support, registration, Storage and data processing*, 2017, V. 19, № 2, [Online]. Available: https://nbuv.gov.ua/UJRN/rzod_2017_19_2_B. Accessed on: June 21, 2019.

[2] President of Ukraine. (2016, March 15). *Decree no. 96/2016. On the decision of the Council of National Security and Defense of Ukraine dated January 27, 2016 "On the Strategy of Cyber Security of Ukraine"* [Online]. Available: http://zakon.rada.gov.ua/laws/show/96/2016. Accessed on: June 21, 2019.

[3] O.V. Klimchuk, Information and cybersecurity in today's world: the SSU experience, *ua-news*, 2018, [Online]. Available: https:// ua-news.liga.net/politics/opinion/informatsiyna-ta-kiberbezpeka-v-suchasnomu-sviti-dosvid-sbu. Accessed on: June 21, 2019.

[4] S.L. Gnatyuk, Cybersecurity in the Deployment of the Fourth Industrial Revolution (Industry 4.0): Challenges and Opportunities for Ukraine, *National Institute for Strategic Studies, Analytical Materials* 2019, [Online]. Available: https://niss.gov.ua/doslidzhennya/analitichni-materiali/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya. Accessed on: June 21, 2019.

[5] Verkhovna Rada of Ukraine. V convocation, 2nd session. (2007, January 9). *Law of Ukraine no. 537-V. About the basic principles of development of information society in Ukraine for 2007-2015*. [Online]. Available: http //zakon.rada. gov.ua/laws/show/537-16. Accessed on: June 21, 2019.

[6] V.V. Horlynskyi *The philosophy of security and sustainable human development: a value dimension: a monograph.* Kiev, Ukraine: Parapan, 2011.

[7] I. Diordica, Cybersecurity: Essence and Purpose, Enterprise, *Business and Law. Information law* 7/2017. [Online]. Available: https//phd.znu.edu.ua/page//aref/07_2018/Diorditsa_ aref.pdf. Accessed on: June 21, 2019.

[8] Yu. Kojedub, "Organizational paradigm for information security", *Information Technology and Security*, vol. 6, iss. 1 (10). pp. 26-36. July-December 2018. doi: 10.20535/2411-1031. 2018.6.1.153133.

[9] Yu. Danyk, and O. Korneiko, "Basics of methodology of cybercompetence formation in specialists of the security and defense sector of Ukraine", *Information Technology and*

Security, vol. 6, iss. 2 (11). pp. 105-123. July-December 2018. doi: 10.20535/2411-1031. 2018.6.2. 153495.

[10] Yu. Lapayev, and V. Petrov: "I do not know of any case of information leakage from protected government networks", *Society* 2019-11-29, *Ukrainian Week* № 48 (628), 28 Nov. 2019. [Online]. Available: https://m.tyzhden.ua/Society/238132. Accessed on: Nov 30, 2019.

[11] "Okinawa Charter of the Global Information Society", in M. Z. Zgurovskyi, *Development of the Information Society in Ukraine: Legal Regulation in the Field of Information Relations*. Kiev, Ukraine: NTUU "KPI", 2006.

[12] "World Summit on the Information Society. Geneva, 2003 – Tunisia, 2005. Declaration of Principles. Building an information society is a global challenge in the new millennium", in M.Z. Zgurovskyi. *Development of the Information Society in Ukraine: Legal Regulation in the Field of Information Relations*. Kiev, Ukraine: NTUU "KPI", 2006.

[13] Verkhovna Rada of Ukraine. IV convocation, 8th session. (2005, September 7). *Law of Ukraine no. № 2824-IV 2824-15. The Convention on cybercrime*. [Online]. Available: https //zakon5.rada.gov.ua/laws/show/994-789. Accessed on: June 21, 2019.

[14] *Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation*. Active Engagement_ Modern Defence / NATO. [Online]. Available: http://www. nato. int/lisbon2010/ strategic-concept-2010-eng.pdf. Accessed on: June 21, 2019.

[15] O. Arkhipov, and V. Brovko, *Cyber Security – emergence, formation, understanding.* [Online]. Available: http://www.academy.ssu.gov.ua/upload/file/Zbirnyk_materialiv_konferencii_24. Accessed on: June 21, 2019.

[16] Verkhovna Rada of Ukraine. VIII convocation, 7th session. (2017, October 5). *Law of Ukraine no. № 2163-VIII. On the basic principles of cybersecurity of Ukraine*. [Online]. Available: http//zakon.rada.gov.ua/ laws/show/2163-19. Accessed on: June 21, 2019.

[17] Cabinet of Ministers of Ukraine. (2019, June 19). *Resolution No. 518. On approval of General requirements for cyber security of critical infrastructure facilities*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/518-2019-п. Accessed on: June 21, 2019.

VICTOR HORLYNSKYI,
BORIS HORLYNSKYI

CYBERSECURITY AS A COMPONENT OF INFORMATION SECURITY OF UKRAINE

It is shown that the globalization impact on cyberspace, manifested in the spread of cybercrime, cyberterrorism and information expansion, requires its reliable protection, and ensuring the cyber security of Ukraine in the conditions of the Joint Forces Operation becomes an integral component and a factor of national security. It is proved that the establishment of the established system of information security of the state in the conditions of globalization and development of information technologies and telecommunication systems requires clarification of system-forming bases and basic principles of the system of providing cybersecurity as the most important component of information security of Ukraine. Based on the analysis of scientific publications, it is argued that the study of the problem of information security occurs, as a rule, in two main directions - information-psychological, aimed at protecting consciousness from negative information impact and information-technical, in which the main object of protection are information resources. in information and telecommunication systems. It is substantiated that the methodological basis for addressing this issue is a systematic approach that allows to consider not only certain types of information threats, but also the multifunctionality and multidimensionality of the subject field of information security in understanding information security as a systemic phenomenon. It is proved that on the basis of identification of objects in need of protection, branching of functions and sectors of responsibility of public and private structures, it is expedient to distinguish subject areas of

information and cybersecurity. The definition of information security in the broad sense of the term as a sphere of national security, characterized by comprehensive (legal, economic, technological and organizational) security of the established functioning of the information space, the protection of information, information and technological and security interests of the state and society, information and rights is formulated. and human freedoms. An approach is proposed, according to which it is important, first, to separate the substantive side of the concepts of information and cybersecurity in the broad and narrow sense of the word, and secondly, to differentiate their functional content in the state and national, according to the scope of information and cyberspace and global dimensions. It is concluded that further development of the scientific, theoretical, legal and organizational foundations of cybersecurity is one of the most important tasks of Ukrainian science, especially in the context of the path towards Euro-Atlantic integration of Ukraine.

Keywords: informatization; information threats; informational security; cybersecurity; information space; cyberspace; cyber threats.

Горлинський Віктор Вікторович, кандидат філософських наук, доцент, доцент спеціальної кафедри, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0003-1190-5991.

E-mail: gvv1004@gmail.com.

Горлинський Борис Вікторович, начальник управління, Департамент захисту інформації, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Київ, Україна.

ORCID: 0000-0002-9993-2427.

E-mail: vjzgoxnf@gmail.com.

Horlynskyi Viktor, candidate of philosophical sciences, associate professor, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Horlynskyi Borys, head of the department, department of information protection, Administration of State serves of special communication and information protection of Ukraine, Kyiv, Ukraine.