УДК 343.34
DOI: https://doi.org/10.18524/2411-2054.2019.33.162068

Г. В. Форос, канд. юрид. наук, доцент, професор
Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
вул. Успенська, 1, Одеса, 65014, Україна

В. С. Жогов, ад'юнкт
Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
вул. Успенська, 1, Одеса, 65014, Україна

ОСОБЛИВОСТІ ТРАКТУВАННЯ ПОНЯТТЯ «КІБЕРБЕЗПЕКА» В СУЧАСНІЙ ЮРИДИЧНІЙ НАУЦІ

Статтю присвячено визначенню особливостей впровадження та удосконалення поняття «кібербезпека» в сучасній юридичній науці, проаналізовано систему джерел національного та міжнародного законодавства, яка регулює правовідносини в кіберпросторі. Проаналізовано різні підходи до поняття «кібербезпека», а також досліджено визначення безпеки як філософської категорії і розкрито її сутність.

Ключові слова: кібербезпека, кіберпростір, кіберзахист, кіберзлочинність.

Постановка проблеми. Стрімкий розвиток людства в XXI столітті, обумовлений розробкою і застосуванням на практиці передових наукових розробок, дозволив в найкоротші терміни прискорити численні життєво-важливі процеси, що протікають в багатьох сферах суспільного життя. З появою і впровадженням в ці процеси комп'ютерних технологій, новітніх засобів і способів передання інформації для людства почався відлік нової реальності – глобальної інформатизації, яка в даний час активно керує існуванням і життєдіяльністю держав світової спільноти.

Так, за даними Internet World Stats (IWS) станом на 30.06.2018, кількість користувачів мережі Інтернет в світі, становить 4 208 571 287, а все населення планети – 7 634 758 428. Інформація Internet World Stats про використання Інтернету заснована на даних, опублікованих Nielsen Online, Міжнародним союзом електрозв'язку, GfK, місцевими органами регулювання ІКТ та іншими надійними джерелами.

У звіті «Global Digital 2018» від We Are Social і Hootsuite повідомляється, що у жовтні 2018 у світі налічується майже 4,2 мільярда користувачів Інтернету (зростання за рік на 7%), біля 3,4 мільярда осіб по всьому світу використовували соціальні мережі (зростання за рік на 10%), більше 5,1 мільярда чоловік користуються мобільним телефоном, більшість з яких смартфон [1].

Однак, кожна з нових сфер нашого життя приносить з собою і нові загрози. Це стосується й віртуального, інформаційного кіберпростору. Відтепер вчинення злочину не потребує попереднього особистого контакту з потенційною жертвою. Кіберпростір одночасно виступає як місце вчинення злочину, так і як знаряддя злочину. Виникла необхідність у забезпеченні доступності, цілісності, автентичності, конфіденційності, захищеності інформації в даному середовищі.

Аналіз останніх досліджень і публікацій. Проблеми дослідження впровадження та удосконалення поняття категорії «кібербезпека» в сучасній юридичній науці, певною мірою розглядалися теоретиками права, державознавцями, адміністративістами, фахівцями у сфері інформаційного права, соціологами, кібернетиками. Особливо слід підкреслити внесок у розробку даної проблеми таких провідних вчених як: В. М. Богуш, В. Л. Бурячок, С. О. Гнатюк, Б. А. Кормич, В. А. Ліпкан, В. М. Сидоренко,

М. М. Присяжнюк, Є. І. Цифра, Л. М. Щербак, а також зарубіжних – C. Lucian, A. Fabian, L. David, B. Matt, J. Stubbs, M. Williams, N. Weaver та інших.

Метою статті є комплексний аналіз впровадження та удосконалення поняття категорії «кібербезпека» в сучасній юридичній науці на підставі аналізу чинного законодавства.

Виклад основного матеріалу. Для того, щоб розкрити зміст поняття «кібербезпека» необхідно визначити природу і деструктивний потенціал інформаційних загроз в кіберпросторі. Вивчивши наукові праці з даного питання, можна навести такі приклади інформаційних загроз, які описуються як в наукових працях, так і у нормативно-правових актах держав.

Під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків [2]. Аргументом щодо даного твердження виступає етимологічне тлумачення двох складових даної правової категорії – кібер та безпека. У Великому тлумачному словнику української мови «кібер» або «кібернетичний» – стосується до кібернетики; який створено, працює на основі принципів, методів кібернетики [3, с. 308]. А «безпека» – стан, коли кому-, чому-небудь ніщо не загрожує [3, с.106], тобто відсутність небезпеки. В запропонованому визначенні абсолютно відсутні ці дві категорії, хоча вони і є його понятійно-категорійним апаратом.

В науковій літературі кібербезпека визначається як безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

Для забезпечення кібербезпеки надзвичайно важливо розуміти загрози кіберпростору. Кібернетичні загрози (кіберзагрози) – наявні та/ або потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [4].

При цьому можна виділити таку типологію кібернетичних загроз: кібервійна; кібертероризм; кібершпигунство; кіберзлочинність [5, с. 130].

В «Стратегії національної безпеки України» надається розмежування понять кібербезпека та інформаційна безпека, шляхом визначення загроз інформаційній безпеці та загроз кібербезпеці і безпеці інформаційних ресурсів [6]. Так, до загроз інформаційній безпеці віднесено ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Загрози кібербезпеці і безпеці інформаційних ресурсів визначаються в уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а також у фізичній і моральній застарілості системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

На думку аналітика лондонського Королівського інституту закордонних справ (Chatam House) П. Корніша, до інформаційних загроз слід віднести:

- діяльність хакерів-одинаків;
- організовану злочинність, яка діє в глобальних інтернет-мережах;
- ідеологічний і політичний екстремізм (кібертероризм);
- інформаційну агресію, яку проводить одна держава по відношенню до іншої (кібервійна).

На його думку, на сьогоднішній день тільки перші два різновиди загроз з класифікації знайшли практичне втілення в світовій політиці. Він стверджує, що кібертероризм і кібервійна між державами в даний час є скоріше уявними загрозами, ніж реальність і можуть бути реалізовані через десятиліття [7].

На наш погляд, дана позиція є недостатньо вірною, так як в даний час кібертероризм, як один із способів ведення протиборства між державними, громадськими та іншими суб'єктами широко представлений на міжнародній арені, а кібервійна як один з видів і типів сучасних війн має стрімкий науковий розвиток і все зростаючі за своєю кількістю епізоди практичного застосування.

Тому на даний історичний момент найбільш актуальним стає не тільки подальший розвиток практичної діяльності в кіберпросторі суб'єктів світового політичного процесу, організацій, груп, окремих громадян, але і правове забезпечення цієї діяльності, яке виражається в прийнятті на державному і міждержавному рівнях різних за своєю юридичною силою нормативно-правових документів.

Науковцями в рамках своїх досліджень для об'єднання явищ пов'язаних з умовами забезпечення захищеності від політичних, фізичних, духовних, емоційних, освітніх, професійних, психологічних та інших видів впливів, а також аварійних наслідків, помилок, нещасних випадків, пошкоджень, шкоди та інших подій, що відбуваються в кіберпросторі, що визнаються небажаними, запропоновано використання терміну «кібербезпека», що й відповідно закріплено в Міжнародній організації стандартизації під кодом «ISO/IEK 27032 2012» [8].

У цьому стандарті не варто шукати відвертостей чи вселенської мудрості. Однак він дає чітке розуміння зв'язку терміна cybersecurity (кібербезпека) з network security (мережевою безпекою), application security (прикладної безпекою), Internet security (Інтернет-безпекою) та critical information infrastructure protection (безпекою критичних інформаційних інфраструктур) з точки зору західних фахівців. У стандарті наводиться ось така схема, яка візуалізує зв'язок різних термінів.

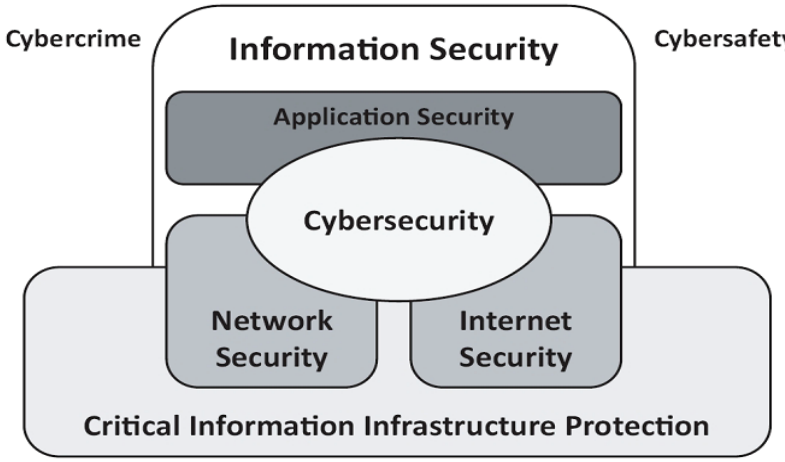

Figure 1 — Relationship between Cybersecurity and other security domains

І відразу стає зрозуміло, що кібербезпека, і так нам звична інформаційна безпека – це зовсім не одне і теж. І безпека критичних інформаційних інфраструктур, хоч і пов'язана з кібербезпекою (так як її розуміють в усьому світі), але тільки частково.

Кіберзлочинність (cybercrime) ж взагалі стоїть окремо і не має ніякого відношення ні до інформаційної безпеки, ні до кібербезпеки. Також як і поняття cybersafety, яке в Україні не має прямого і ємного перекладу, але сенс його такий – безпечна поведінка в кіберпросторі і, в першу чергу, захист дітей від негативної інформації в мережі Інтернет.

В рекомендації Міжнародного Союзу Електрозв'язку X.1205 MCE-T «кібербезпека» визначена як набір засобів, стратегій, принципів забезпечення безпеки, заходів щодо забезпечення безпеки, керівних принципів, підходів до управління ризиками, дій, професійної підготовки, практичного досвіду, страхування і технологій, які можуть бути використані для захисту кіберпростору, ресурсів організації і користувача [9].

Обстановка, яка складається в сучасному світовому кіберпросторі навколо України вимагає прийняття адекватних заходів протидії, щоб потенційні конкуренти не могли завоювати та отримати інформаційну перевагу над Україною як в мирний, так і у воєнний час.

У зв'язку з цим, виникла потреба негайно виробити основні принципи тлумачення поняття категорії «кібербезпека» в юридичній науці, що допоможе забезпечити захист прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі, запобігання, виявлення, припинення та розкриття кіберзлочинів, шляхом, вдосконалення існуючих та створення нових відповідних нормативно-правових актів. На нашу думку, вироблення необхідних правових механізмів нейтралізації кібераграсії, кібервпливів та кіберзлочинів, які можуть проводиться потенційним правопорушниками, допоможе правоохоронним органам створювати і розвивати сили та засоби забезпечення кібербезпеки критично важливої інфраструктури держави.

Поняття «кібербезпека» з'явилося відносно нещодавно і розглядалося в концептуальних рамках. Значна частина досліджень категорій «кіберзахист», «кібербезпека» носили теоретичний характер, оскільки вважалося, що, перш за все, ця діяльність пов'язана з технічно-прикладним станом захищеності: створенням відповідних програмних комплексів, діяльності певних корисних моделей, ноу-хау, інтегральних мікросхем тощо.

Тому виникає необхідність вивчення даної категорії крізь призму аналізу норм права, зокрема Конституції України, тим більше зміни в суспільстві, що відбулися за останнє десятиліття, внесли свої корективи в обговорювану проблему. Все це обумовлює доцільність подальшого вдосконалення поняття і питань забезпечення кібербезпеки. Якісні зміни адміністративної практики, зокрема правопорушень, що посягають на кібербезпеку, привели до значної зміни змістовного значення категорії «кібербезпека».

Найважливішим методологічним підґрунтям дослідження в юриспруденції є науково-практична ідея, яка ґрунтується на прагненні людини зрозуміти, пояснити досліджуване явище. Це, в свою чергу, вимагає системного аналізу його становлення і розвитку.

У Конституції України 1996 року конкретні поняття «кібербезпека», «кіберзлочинність» відсутні. Крім того, в конституційному законодавстві більшості зарубіжних країн дефініцій даної категорії також не вказано. І це недивно. Оскільки, одним з перших нормативно-правових актів в даній сфері можна вважати Конвенцію про кіберзлочинність, яка була підготовлена в контексті Ради Європи лише 23 листопада 2001 р. Але якщо провести аналіз даного міжнародного нормативно-правового документа, можна зробити висновок, що ключовим завданням, яке постає перед державами-підписантами є забезпечення основних прав людини, як це передбачено відповідними міжнародними угодами, які підтверджують право кожного безперешкодно дотримуватись поглядів, а також право на свободу слова, включаючи право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на кордони, а також права на повагу до приватного життя, зокрема і в кіберпросторі [10].

Тому якщо зіставити вищезазначене з 2 розділом Конституції України, то можна дійти висновку, що поняття «кібербезпека» все таки позначено, але на пряму не розшифровується, що закономірно. В силу цього виникла необхідність конституційного роз'яснення даного терміну, вказати його відмінні риси від схожих категорій і інститутів [11].

З метою імплементації відповідних правових норм у національне законодавство, 5 жовтня 2017 року Верховна Рада України прийняла Закон України «Про основні засади забезпечення кібербезпеки України». В даному Законі під кібербезпекою розуміється захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [12].

Разом з тим, необхідно уточнити значення слова «безпека». В теорії національної безпеки широко використовуються такі поняття: «національна безпека», «безпека особи», «суспільна безпека», «державна безпека», «регіональна безпека», «міжнародна безпека», «інформаційна безпека», «політична безпека», «соціальна безпека», «економічна безпека», «енергетична безпека», «інформаційна безпека», «військова безпека», «технологічна безпека», «екологічна безпека» тощо. Для розуміння їх значення потрібно про-

аналізувати поняття «безпека», оскільки воно включає у себе всі вищеназвані дефініції, є основою їх визначення, які є різновидами безпеки залежно від сфери суспільного та міжнародного життя. Часто дослідники в цій сфері відразу переходять до аналізу національної чи міжнародної безпеки та їх складових, належно не з'ясувавши сутнісно-філософське наповнення поняття «безпека». Це призводить до термінологічного хаосу, різнотлумачень цих понять та дещо спрощеного їх трактування. Ці проблеми зумовлені відсутністю належної методологічної основи, яка дозволила б узагальнити, систематизувати та класифікувати увесь наявний матеріал, виявити закономірності та взаємозв'язок між тими чи іншими поняттями в галузі національної безпеки. У підсумку виникають труднощі в розгляді національної безпеки як системного явища, формування відповідної системи національної безпеки та системи забезпечення національної безпеки.

У академічному тлумачному словнику української мови під безпекою розуміється стан коли кому-, чому-небудь ніщо не загрожує [13]. В.М. Заплатинський позначає безпеку як такі умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень [14].

Необхідно відзначити, що деякі конституціоналісти в своїх науково-навчальних коментарях і посібниках зачіпають поняття кібербезпеки, однак практично ніхто не намагався дати йому докладне визначення, виділити його конституційну основу і зміст.

Разом з тим в науці адміністративного права існують різні точки зору з досліджуваного поняття. Більшість вчених-юристів розглядають кібербезпеку у вузькому і широкому сенсі.

При розгляді кібербезпеки у вузькому значенні необхідно говорити, перш за все про захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кібербезпека являє собою реалізацію заходів професійно підготовленими фахівцями щодо захисту та страхування дій, засобів, технологій, критично важливих об'єктів інфраструктури суспільства та держави від цифрових атак, які використовуються у кіберпросторі. Кібербезпека передбачає збереження та постійне вдосконалення властивостей безпеки, спрямованих проти відповідних кіберзагроз [15].

Такий підхід обґрунтований і використовується в правозастосовчій сфері, в тому числі в юрисдикційної діяльності працівників правоохоронних органів. Кібербезпека забезпечується і підтримується державно-примусовими заходами. Крім того, в більшості нормативних актів правоохоронної сфери законодавець використовує досліджувану категорію саме в такому контексті.

Інша група вчених в своїх працях розглядає кібербезпеку у широкому сенсі. Їхнє бачення полягає в тому, що кібербезпека – це сукупність вольових суспільних відносин, що складаються в процесі свідомого і добровільного дотримання громадянами встановлених в нормах права та в інших нормах неюридичного характеру правил поведінки в кіберпросторі, і тим самим забезпечуються злагоджене, стійке, спільне життя людей в умовах розвинутого суспільства.

У цьому ж спектрі висловлювалися різні точки зору вчених-юристів про структуру і співвідношення «кібербезпеки» та «інформаційної безпеки». Так, на думку деяких вчених, в категорію «інформаційна безпека» входить і «кібербезпека».

Наше бачення полягає в тому, що поняття кібербезпеки у вузькому сенсі може бути використано практичними працівниками задля аналізу сфери правоохоронної діяльності, спрямованої на захист конституційних прав і свобод громадян, а саме при встановленні об'єкта протиправного посягання, що має практичне значення в роботі правоохоронних органів.

У теорії ж адміністративного права оптимальним буде звернення вчених до поняття кібербезпеки в широкому сенсі, так як розуміння даного інституту саме в широкому сенсі є необхідною умовою не тільки для більш поглибленого його вивчення, а й розвитку його розуміння в теорії права.

Висновки. Підбиваючи деякі підсумки аналізу особливостей впровадження та удосконалення поняття категорії «кібербезпека» в сучасній юридичній науці ми можемо говорити, що за останнє десятиріччя в багатьох країнах світу на державному рівні розроблено стратегії кіберпростору. Основний акцент в цих нормативно-правових документах робиться на те, що кібербезпека стає головним завданням держави, економіки і суспільства, але без його чіткого тлумаченя з'являються деякі прогалини та колізії в чинному законодавстві.

Список літератури

1. Internet World Stats (IWS) [Електронний ресурс]: https://www.internetworldstats.com/stats.htm.
2. Аналітична записка щодо Законопроекту «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу: www.inau.org.ua/download.php?bd189ae6a731113f59c7d7fcacf193f3.
3. Беляков К. И. Управление и право в период информатизации. Монография. – Киев: Изд-во «КВІЦ», 2001. – 308 с.
4. Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю.О. Розширення термінології сучасного кіберпростору / Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю. О. [Електронний ресурс]. – Режим доступу: mino.esrae.ru/pdf/2014/3Sm/1387.doc.
5. Петров В. В. Щодо формування національної системи кібербезпеки України / В. В. Петров // Стратегічні пріоритети. – Київ: НІСД, 2013. – № 4(29). – С.127-130.
6. Про Стратегію національної безпеки України [Електронний ресурс]: Указ Президента України від 06.05.2015 № 287/2015. – Електрон. дан. (1 файл). – Режим доступу: http://zakon1.rada.gov.ua. – Назва з екрана.
7. Cornish, P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks/ P. Cornish; Directorate-General for External Policies of the Union, Policy Department. – Brussels : European Parliament, 2009. – 34 p.
8. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity [Електронний ресурс]: International Organization for Standardization https://www.iso.org/standard/44375.html.
9. Рекомендація МСЕ-Т X.1205 від 18.04.2008 17-й ДК МСЕ-Т (2005-2008) ст. 8
10. Конвенція про кіберзлочинність [Електронний ресурс]: від 23.11.2001 ратифікована із застереженнями і заявами Законом № 2824-IV від 07.09.2005 – Електрон. дан. (1 файл). – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575 – Назва з екрана.
11. Конституція України [Електронний ресурс]: Закон України від 28.06.1996 р. № 254к/96-ВР із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду: за станом на 30.09.2016 р. – Електрон. дан. (1 файл). – Режим доступу: http://zakon1.rada.gov.ua. – Назва з екрана.
12. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: Закон України від 05.10.2017 № 2163-VIII – Електрон. дан. (1 файл). – Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19 – Назва з екрана.
13. Тлумачення, значення слова «безпека» [Електронний ресурс]: Словник української мови, Академічний тлумачний словник (1970–1980) http://sum.in.ua/s/bezpeka.
14. Заплатинський В. М. Логіко-детермінантні підходи до розуміння поняття «Безпека». Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини. / [редкол.: П. С. Атаманчук (відп. ред.) та ін.]. – Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2012. – Випуск 5. − 336 с. С. 90-98.
15. Что такое кибербезопасность? [Електронний ресурс]: Офіційний портал американської транснаціональної компанії Cisco https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html.

Стаття надійшла 25.02.2019 р.

А. В. Форос, канд. юрид. наук, доцент, профессор
Одесский государственный университет внутренних дел
Кафедра кибербезопасности и информационного обеспечения
ул. Успенская, 1, Одесса, 65014, Украина

В. С. Жогов, адъюнкт
Одесский государственный университет внутренних дел
Кафедра кибербезопасности и информационного обеспечения
ул. Успенская, 1, Одесса, 65014, Украина

ОСОБЕННОСТИ ТРАКТОВКИ ПОНЯТИЯ «КИБЕРБЕЗОПАСНОСТЬ» В СОВРЕМЕННОЙ ЮРИДИЧЕСКОЙ НАУКЕ

Резюме

Статья посвящена определению особенностей внедрения и усовершенствования понятия «кибербезопасность» в современной юридической науке, проанализирована система источников национального и международного законодательства, регулирующая правоотношения в киберпространстве. Проанализированы различные подходы к понятию «кибербезопасность», а также исследованы определения безопасности как философской категории и раскрыта ее сущность.

Ключевые слова: кибербезопасность, киберпространство, киберзащита, киберпреступность.

A. V. Foros, Candidate of Juridical Sciences, Associate Professor, Professor
Odessa State University of Internal Affairs
Department of Cyber Security and Information Support
Uspenskaya Street, 1, Odessa, 65014, Ukraine

V. S. Zhoghov**,** Adjunct
Odessa State University of Internal Affairs
Department of Cyber Security and Information Support
Uspenskaya Street, 1, Odessa, 65014, Ukraine

FEATURES OF TRACKING OF THE CONCEPT «CYBERSECURITY» IN THE CONTEMPORARY LEGAL SCIENCE

Summary

The article is devoted to the definition of the peculiarities of the introduction and improvement of the concept of «cyber security» in modern legal science, analyzed the system of sources of national and international legislation regulating legal relations in cyberspace. Different approaches to the concept of «cybersecurity» are analyzed, and the definition of security as a philosophical category is investigated and its essence is revealed.

Key words: cybersecurity, cyberspace, cyber defense, cybercrime.