УДК 342.9

СИСТЕМА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ПРОБЛЕМИ ФОРМУВАННЯ ТА ЕФЕКТИВНОЇ ДІЯЛЬНОСТІ

Федченко Д.І.
Інститут прокуратури та кримінальної юстиції
Національного юридичного університету імені Ярослава Мудрого

Дану наукову статтю присвячено дослідженню таких актуальних сучасних явищ як кібербезпека, кіберпростір та кіберзлочинність. У статті проаналізовано наукові підходи до визначення цих понять, встановлено їх характерні ознаки та взаємозв'язок. З огляду на стрімкий розвиток кіберпростору та явищ похідних від нього, досліджено реальність кіберзагроз та розвиток кіберзлочинності, у зв'язку з чим проаналізовано необхідність формування системи забезпечення кібербезпеки. У статті встановлено проблеми створення цієї системи та запропоновано шляхи їх вирішення. В ході наукового дослідження доведено, що на ефективність функціонування системи забезпечення кібербезпеки основний вплив здійснює правове регулювання як на міжнародному, так і на національному рівні, а також рівень взаємодії і узгодженості діяльності відповідних суб'єктів.

Ключові слова: кібербезпека, кіберпростір, кіберзагрози, кіберзлочинність, система забезпечення кібербезпеки.

Постановка проблеми. З огляду на масове впровадження в життя суспільства і держави комп'ютерних, інформаційних та інших телекомунікаційних технологій виникає необхідність правового регулювання їх використання, адже разом із застосуванням корисних властивостей цих об'єктів, виникають і поширюються негативні явища пов'язані з ними. Розглядаючи це питання з філософського аспекту, можна дійти висновку, що основною проблемою розвитку людства в цілому є той факт, що людина здатна перетворити усі свої здобутки на зброю, замість використання позитивних якостей, майже у всьому можна застосовувати негативні, які покликані заподіяти шкоду. Зважаючи на це нагальною стає потреба формування системи забезпечення кібербезпеки, яка буде охоплювати і міжнародний, і національний рівні. Основна проблема полягає в тому, що на сьогоднішній день відсутнє уніфіковане визначення поняття «кібербезпека», кожна держава шукає свій власний підхід до забезпечення кібербезпеки в межах національної безпеки, на міжнародному рівні приймаються акти, які стосуються одного аспекту кібербезпеки, а комплексний – відсутній.

Дане питання різнобічно досліджене у наукових роботах таких вчених як В.А. Ліпкана, І.В. Тімкіна, Н.Є. Новікова, І.В. Діордіци, С.В. Мельника, В.І. Кащука, В.П. Шеломенцева, М.М. Присяжнюка, Є.І. Цифри, В. Маркова, М. Камчатного та інших. **Аналіз останніх публікацій** вказує на те, що в сучасних наукових дослідженнях більше уваги приділяється забезпеченню кібербезпеки на національному рівні. Але досягнення такої безпеки лише всередині держави є неможливим, тому необхідно вести мову про посилення міжнародно-правового регулювання цієї проблеми.

Таким чином, **не вирішеним раніше** залишилося основне питання щодо формування єдиної системи забезпечення кібербезпеки, узгодження та взаємодії її складових частин на міжнародному та національному рівнях, оскільки проблема кібербезпеки є глобальною і окремих зусиль різних суб'єктів для її вирішення буде недостатньо.

Мета даної статті полягає в тому, щоб проаналізувати сучасні визначення таких термінів як «кіберпростір», «кібербезпека», «кіберзагроза» та надати кожному з них уніфіковане тлумачення, дослідити загрози, які виникають у сучасному кіберпросторі, та їх суспільну небезпечність, проаналізувати моделі систем забезпечення кібербезпеки у різних країнах світу та запропонувати єдину, яка охоплюватиме і міжнародний, і національний рівні, вивчити їх структуру, визначити які органи туди входимуть, їх функції, обов'язки, взаємодію.

Виклад основного матеріалу. Для комплексного проведення даного дослідження, насамперед, необхідно проаналізувати визначення основних понять. На думку І. Діордіци, системою забезпечення кібербезпеки варто розуміти сукупність організаційно об'єднаних органів управління, а саме: державних органів, громадських організацій, посадових осіб та окремих громадян, які спрямовують свою діяльність на створення умов для реалізації національних інтересів у кіберпросторі, а також сил, засобів і методів, які використовуються для досягнення даної цілі відповідно до законодавства [1]. Також можна додати, що система забезпечення кібербезпеки є єдиним державно-правовим механізмом, та всі його суб'єкти діють чітко в межах, визначених законодавством. У вузькому сенсі система забезпечення кібербезпеки – сукупність органічної об'єднаних спільними цілями суб'єктів, які здійснюють свою діяльність у кіберпросторі з метою реалізації національних інтересів. Кожна держава індивідуально визначає сфери, які вона відносить до кібернетичної безпеки, перелік об'єктів і суб'єктів її забезпечення, виходячи зі тих стратегічних цілей і завдань, які стоять перед державою на національному та міжнародному рівнях, та її практичних можливостей реалізації національних інтересів [2, с. 110]. Не можна не погодитись із поданими визначеннями, однак обидва ці тлумачення надаються у прив'язці до норм національного законодавства і побудовані на їх основі. На мою думку, побудова даної системи та подальша її реалізація має виходити не лише

© Федченко Д.І., 2018

з норм національного законодавства та можливостей кожної окремої держави, а й ґрунтуватися на нормах міжнародного права та узгодженості дій суб'єктів даної системи, неухильного виконання взятих на себе зобов'язань.

Також, як система кібернетичної безпеки (система кібербезпеки) розглядається сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються [3, с. 303].

Ще однією науковою думкою є наступна: система кібернетичної безпеки – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі з метою забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Розвиток національної системи кібербезпеки має супроводжуватись відповідними корективами у процесі реформування сфери національної безпеки, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором [4, с. 176].

Таким чином, система забезпечення кібербезпеки – це комплексна та узгоджена діяльність спеціально уповноважених міжнародними та національними нормами суб'єктів забезпечення кібербезпеки, покликана запобігти виникненню та реалізації загроз кіберпростору, а у відповідних випадках – усунути їх негативний вплив.

Для повного розуміння кібербезпеки необхідно проаналізувати визначення терміну «кіберпростір».

Держави та міжнародні установи використовують термін «кіберпростір», але офіційного нормативного його тлумачення не надано. У науковій розробці існує безліч підходів до його визначення.

Якщо розглядати кіберпростір як словосполучення «кібернетичний простір», то кіберпростір – це простір (територія), який створений та працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки інформації) [5, с. 216].

З філософської точки зору, кіберпростір – це сфера віртуального буття людини, де діють інші закони, інші звичаї, де людина перетворюється на громадянина іншої держави, стає «кібернавтом» [6, с. 144].

Відповідно до міжнародного стандарту, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, якого не існує в будь-якій фізичній формі.

Деякі держави все ж надають власне визначення цього поняття. Наприклад, США кіберпростір – це сфера, яка характеризується можливістю використання електронних і електромагнітних засобів для запам'ятовування, модифікування та обміну даними в мережевих системах і пов'язану з ними фізичну інфраструктуру; Великобританія: кіберпростір – це всі форми мережевої цифрової активності, що включають у себе контент і дії, здійснювані через цифрові мережі; Німеччина: кіберпростір – це вся інформаційна інфраструктура, яка доступна через Інтернет поза будь-якими територіальними кордонами. За офіційними документами Євросоюзу, кіберпростір – це віртуальний простір, у якому циркулюють електронні дані світових персональних комп'ютерів [7, с. 62].

В Україні взагалі відсутнє єдине поняття кіберпростору. С. Гнатюк, провівши багатокритеріальний аналіз, запропонував таке узагальнене визначення: кіберпростір – це віртуальний простір, що отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у т.ч. Інтернет) для підтримки та управління процесами перетворення інформації (електронних інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства [8, с. 119].

Підсумовуючи вищенаведене доцільно запропонувати ще одне узагальнене визначення, кіберпростір – це категорія міжнародного права, яка визначає специфічну сферу, що не обмежена жодними кордонами та використовується державами, іншими суб'єктами для досягнення відповідних цілей або настання певних наслідків, шляхом застосування кібернетичних можливостей, новітніх інформаційних технологій.

Наступним елементом даного аналізу є дослідження поняття «кіберзагроза». Стрімке впровадження інформаційних технологій у всі сфери життя, глобалізація інформаційних відносин зумовлюють світову тенденцію до перенесення протиправної діяльності у кібернетичний простір. Сьогодні кіберзлочинність, для якої не існує державних кордонів, загрожує не лише правам та майну громадян, а й посягає на національні інтереси. Спостерігається висока вразливість кібернетичного простору перед кібератаками, діяльністю злочинних угруповань, хакерів, промислово-фінансових груп та осіб, допущених до роботи із системами в порядку здійснення службової діяльності (інсайдерів). Випадки негативного кібервпливу стають частішими, організованішими, більш легкими та дешевими в підготовці і реалізації.

Неконтрольоване поширення та необмежене застосування інформаційного і кіберпросторів протягом останніх десятиріч: 1) призвело до уразливості інформаційної сфери більшості країн світу для стороннього кібернетичного впливу; 2) визначило політичну необхідність контролю і подальшого регулювання відносин у цій царині; 3) дало підстави стверджувати про особливу актуальність: процесів пошуку, збирання й добування інформації у відкритих, відносно відкритих і закритих електронних джерелах; заходів із забезпечення конфіденційності, цілісності та доступності власного IP, а також протидії цілеспрямованому впливу з боку потенційно можливих кібернетичних втручань і загроз. Зважаючи на це та враховуючи постійно зростаючий потенціал використання мережі Internet у військових цілях, провідні країни світу – США, Японія, Франція, Велика Британія, Росія, Китай та багато інших – протягом останніх років активно модернізують власні сектори безпеки, й передусім безпеки кібернетичної, відводячи при цьому головну роль проблемі завоювання інформаційної переваги в управлінні військами (силами) і зброєю, а також удосконаленню нормативно-правової бази [9, с. 107].

Таким чином, загроза з потенційної перетворилася на реальну і тому питання про усунення ймовірності настання таких загроз, їх негативного впливу є надзвичайно актуальним на сьогоднішній день, адже розвиток і вдосконалення інформаційних технологій розширює можливості кіберзлочинів, в тому числі, і для здійснення фізичних вбивств, бо в сфері охорони здоров'я, де багато пристроїв мають вихід в мережу, злочинці, можуть безконтактно здійснювати вбивства, наприклад, відключивши кардіостимулятор або апарат штучної вентиляції легенів, змінивши запропоновану дозу ліків.

Можливості комп'ютерної мережі Інтернет інтенсивно освоює і наркомафія. Наркоторговці і їх клієнти дедалі частіше укладають угоди в «закритих кімнатах» каналів чату, захищених від сторонніх програмними засобами, і відмивають свої незаконні доходи в так званих інтернет-банках. Безумовно, в майбутньому зросте небезпека шахрайств, пов'язаних з кредитними картами, можливими атаками на енергосистеми, що забезпечують електроенергією, військові об'єкти, систему управління безпілотними літальними апаратами і т. д.

Найбільш поширена класифікація кіберзлочинів в даний час ґрунтується на Конвенції Ради Європи про кіберзлочинність, що була відкрита для підписання у листопаді 2001 р. В цьому документі кіберзлочини поділяються на п'ять груп:

- злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему);
- злочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів, а саме – для маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерні підроблення);
- злочини, пов'язані з контентом (змістом даних);
- злочини, пов'язані з порушенням авторського права і суміжних прав;
- акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж [10].

Прийняття даної Конвенції ще у 2001 році і її ратифікація 29 державами свідчить про те, що поширення кіберзагроз та використання кіберпростору у злочинних цілях розпочалося вже досить давно, а тому нагальна потреба регламентації діяльності у цій сфері, створення єдиного узгодженого механізму контролю за такою діяльністю залишається відкритою.

Спроби нормативного регулювання кіберпростору розпочалися з 1998 року. Кожного року Генеральна Асамблея готує резолюції «Досягнення в сфері інформатизації і телекомунікацій у контексті міжнародної безпеки». Ці документи сприяють підвищенню уваги держав необхідності врегулювання відносин між ними у кіберпросторі, яка посилюється. Окрему увагу питанням кібербезпеки приділяє і Організація Об'єднаних Націй (далі – ООН). У липні 2000 року в Японії президенти восьми провідних країн світу підписали Хартію глобального інформаційного суспільства з метою (також відома як «Окінавська Хартія») розвитку світової економіки та переходу до нового етапу розвитку суспільства. В Хартії було наголошено , що «Інформаційно-комунікаційні технології є одними з найбільш важливих чинників, що впливають на формування суспільства двадцять першого століття. Їх революційна дія стосується способу життя людей, їх освіти і роботи, а також взаємодії уряду і самого суспільства» [11, с. 794]. 20 грудня 2002 року резолюцією 57/239 Генеральної Асамблеї були прийняті «Елементи для створення глобальної культури кібербезпеки». Як вказується у документі «глобальна культура кібербезпеки буде вимагати від усіх учасників врахування 9 основних взаємодоповнюючих елементів: обізнаність, відповідальність, реагування, етика, демократія, оцінка ризику, проектування та впровадження засобів забезпечення безпеки, управління забезпеченням безпеки, переоцінка». Також у 2012 році Всесвітньою асамблеєю зі стандартизації електрозв'язку Міжнародного союзу електрозв'язку було прийнято Резолюцію 50 «Кібербезпека», якою, серед іншого, було підкреслено, що всім зацікавленим сторонам необхідно разом працювати над розробкою стандартів та принципів в цілях захисту від кібератак та полегшення виявлення джерел атак. Крім того, варто сприяти глобальним узгодженим та сумісним процесам обміну інформацією, що стосується реагування на інциденти. Також в 2012 році ООН було підготовлено Доповідь групи урядових експертів з досягнень у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки. Група, серед іншого, погодилася, що заходи по зміцненню довіри, такі як контакти на високому рівні і своєчасний обмін інформацією, можуть підвищити довіру і впевненість серед усіх країн і сприяти зниженню ризику виникнення конфлікту завдяки підвищенню передбачуваності та усунення хибних уявлень. Важливим є те, що за результатами Доповіді було підтверджено, що на кіберпростір поширюється дія міжнародного права, зокрема, Статуту ООН [12, с. 321].

Серед органів, які здійснюють регулювання кіберпростору, варто зазначити такі: у Європейському Союзі функціонує Агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA), у Сполучених Штатах Америки кібербезпекою займається Агентство Національної Безпеки, у НАТО створений Комітет з кібернетичної оборони (The Cyber Defence Committee), а також Спільний центр з кібернетичної оборони (Cooperative Cyber Defence Centreof Excellence), Спеціалізований центр з оборони в сфері кібербезпеки НАТО (CCDCOE), Міжнародний альянс із забезпечення кібербезпеки (ICSPA), Інтерпол (INTERPOL), Міжнародне багатостороннє товариство проти кіберзагроз (IMPACT) та ін. Саме вони мають здійснювати регулювання діяльності у кіберпросторі.

Що стосується саме створення системи забезпечення кібербезпеки, то на думку авторитетних науковців, організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкта забезпечення кібербезпеки, пов'язану: – зі створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі; – з упорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень.

Об'єктом даної системи є інформаційний суверенітет, територіальна цілісність, сталий розвиток суспільства та держави, добробут та кібернетичну безпеку громадян, їх права та свободи, адже кіберпростір надзвичайно комплексне явище, із постійним розвитком він вже здатен контролювати майже всі сфери існування держав та життєдіяльності людей.

Дослідження систем забезпечення кібербезпеки у різних державах світу свідчить про те, що на сьогоднішній день відсутня єдина модель такої системи.

Відповідно до прийнятого 25 листопада 2002 р. комплексного нормативно-правового акта у сфері безпеки – закону США «Про внутрішню безпеку» (Homeland Security Act of 2002) – урядові структури, які займались забезпеченням комп'ютерної безпеки, перейшли під контроль цього новоствореного відомства. Вказаний закон також посилив відповідальність за комп'ютерні злочини (включаючи довічне ув'язнення), зобов'язав інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів, розширив їх права щодо можливості перехоплення інформації (прослуховування телефонних переговорів і перлюстрацію електронних повідомлень) без дозволу суду, визначив основні напрями діяльності федеральних органів із підвищення ефективності захисту критичної інфраструктури США від кібератак, зокрема об'єктів стратегічного значення, що перебувають у приватній власності [13, с. 78].

Стратегія кібербезпеки Канади визначає кібертероризм та ворожі дії в кіберпросторі з боку інших країн (кібершпигунство і кібервійну) основними загрозами кібернетичній безпеці держави, а ключовим органом, на який покладена координація та контроль за імплементацією вказаної Стратегії, реалізація державної політики та координація заходів у сфері кібербезпеки та протидії кіберзагрозам, визначене Міністерство громадської безпеки Канади (Public Safety Canada).

Законом ФРН «Про посилення безпеки інформаційних систем» завдання попередження, реагування на інциденти, викликані кібернетичними загрозами, управління й координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема у взаємодії з приватним сектором, покладене на Федеральне відомство безпеки інформаційних систем (BSI) ФРН.

Головним державним органом Великої Британії, на який покладено завдання захисту критичної інфраструктури, мінімізації загроз сталому її функціонуванню, насамперед, від загроз тероризму, є Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI). Крім того, у Великобританії наприкінці березня 2013 р. було створено Центр із протидії кібернетичним загрозам із метою попередження та нейтралізації кібернетичних атак на об'єкти критичної інфраструктури, а також швидкого реагування на скоєні правопорушення у цій сфері.

Стратегією кібернетичної безпеки Австрії національним координатором і центральним органом у сфері кібербезпеки визначено Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ Австрії (Cyber Crime Competence Center (C4) of the Federal Ministry of the Interior). Крім того, на нього покладено головні функції щодо здійснення правоохоронної діяльності у сфері кібербезпеки та боротьби з кіберзлочинністю.

Ключову роль у забезпеченні кібернетичної безпеки Польщі відіграє Агентство внутрішньої безпеки (АВБ) – польський контррозвідувальний орган. Так, у 2013 р. АВБ розробило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони Польщі, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій (активний кіберзахист).

Ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації (РСІ) [13, с. 79].

На основі проведеного аналізу, можна зробити висновок, що формування єдиної моделі системи забезпечення кібербезпеки є необхідним з огляду на потребу в координації зусиль держав у боротьбі з кіберзлочинністю. Дана потреба повністю обґрунтовується думкою А. В. Войціховського, яку не можна не підтримати. Науковець вказує, що для ефективного запобігання транснаціональним комп'ютерним злочинам необхідний узгоджений міжнародний підхід на різних рівнях. На національному рівні для розслідування кіберзлочинів потрібен добре підготовлений штат співробітників і вдосконалене національне законодавство з метою формування ефективної правової основи для забезпечення слідчої, оперативно-розшукової діяльності правоохоронних органів і спецслужб у боротьбі з подібними злочинами. На міжнародному рівні необхідні оперативні дії, що спираються на координацію зусиль національних центрів із запобігання і розслідування транснаціональних комп'ютерних злочинів з аналогічними міжнародними центрами в інших країнах. У рамках глобальної комп'ютерної мережі кримінально-правова політика окремої держави завдає прямого впливу на міжнародне співтовариство. Кіберзлочинці можуть учиняти свої дії в інформаційному середовищі через певну державу, де такі діяння не криміналізовані, і таким чином вони можуть знаходитися під «захистом» закону такої країни. Отже, забезпечення міжнародної співпраці правоохоронних і судових органів різних держав неможливе без узгодження й ухвалення норм кримінального права відносно кіберзлочинів в окремих державах [14, с. 110].

Тобто, створення даної системи має розпочинатися із укладення єдиного міжнародно-правового договору між максимально можливою кількістю зацікавлених у регулюванні цього питання держав, потім акти щодо кібербезпеки, стратегії кібербезпеки, які були прийняті на національному рівні мають бути приведеними у відповідність умовам договору. Наступним етапом має бути створення уповноважених органів як на міжнародному, так і на національному рівні, причому їх діяльність має бути узгоджена і скоординована таким чином, щоб у випадку виникнення необхідності швидкої реакції на прояв кіберзагрози держави могли надавати одна одній необхідну допомогу, зважаючи на відсутність кордонів кіберпростору. Ще одним елементом ефективної діяльності даних органів є їх співпраця із при-

ватним сектором, тобто відповідними установами приватної форми власності, які мають зацікавленість у протидії кіберзагрозам та зробили це основною метою своєї діяльності.

Висновки. В ході даного дослідження було надано визначення таким поняттям як «кібербезпека», «кіберпростір», «кіберзагрози», а також продемонстровано їх взаємозв'язок, який виявляється у тому, що в кіберпросторі, який за своєю природою немає жодних меж, окрім здійснення правомірної, суспільно-корисної діяльності, поширюються випадки вчинення кіберзлочинів, реалізації інших видів кіберзагроз, які спричинюють шкіливі наслідки як у сфері функціонування держави, так і можуть потягнути за собою реальні людські жертви, тому виникла потреба у здійсненні правової регламентації та контролю за діяльністю у цій сфері. Для реалізації цих завдань створюються системи забезпечення кібербезпеки, але основною їх проблемою є те, що на сьогоднішній день відсутня єдина уніфікована модель такої системи, що об'єднає діяльність уповноважених суб'єктів міжнародного і національного рівня. Тому для вирішення цього питання на практиці необхідне досконале та комплексне його вирішення на науковому рівні.

Список літератури:

1. Поняття та зміст системи забезпечення кібербезпеки [Електронний ресурс]. – Режим доступу : http://goal-int.org.
2. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення / І.В. Діордіца // Підприємництво, господарство і право. – 2017. – № 10. – С. 110–116.
3. Шеломенцев В.П. Сутність організаційного за безпечення системи кібернетичної безпеки України та напрями його удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). Київ: Міжвідом. наук.-дослід. центр з проблеми боротьби з організ. Злочинністю. – 2012. – № 2(28). – С. 299–309.
4. Ліпкан В.А. Національна і міжнародна безпека у визначеннях та поняттях / В.А. Ліпкан, О.С. Ліпкан. – 2-ге вид., доп. і перероб. – К.: Текст, 2008. – 400 с.
5. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності / О.В. Манжай // Право і Безпека. – 2009. – № 4. – С. 215–219.
6. Владленова І.В. Кіберзлочинність як виклик інформаційному суспільству / І.В. Владленова, Е.А. Кальницький // Гілея: науковий вісник : зб. наук. пр. – К., 2013. – Вип. 77. – С. 142–146.
7. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки / М.М. Присяжнюк, Є.І. Цифра // Експертні системи та підтримка прийняття рішень. – 2017. – С. 61–68.
8. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк // Безпека інформації. – 2013. – Т. 19, № 2. – С. 118–129.
9. Бурячок В.Л. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки / В.Л. Бурячок, С.О. Гнатюк, О.Г. Корченко // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К.: Наук.-вид. центр НА СБ України, 2013. – 416 с.
10. Про кіберзлочинність: Конвенція Ради Європи // Офіц. вісник України. – 2007. – № 65. – Ст. 2535. – С. 107. – 10 верес. – Код акту 40846/2007.
11. Лук'янчикова В.Ю. Кіберпростір: загрози для міжнародних відносин та глобальної безпеки / В.Ю. Лук'янчикова // Гілея: науковий вісник. – 2013. – № 72. – С. 793–796.
12. Камчатний М.В. Нормативно-правове закріплення питань кібербезпеки у міжнародному праві / М.В. Камчатний // Актуальні проблеми сучасного міжнародного права : зб. наук. ст. за матеріалами І Харк. міжнар.-прав. читань, присвяч. пам'яті проф. М.В. Яновського і В.С. Семенова, Харків, 27 листоп. 2015 р. : у 2 ч. – Харків, 2015. – Ч. 1. – С. 320–323.
13. Климчук О.О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки / О.О. Климчук, Н.А. Ткачук // Інформаційна безпека людини, суспільства, держави. – 2015. – № 3. – С. 75–83.
14. Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю / А.В. Войціховський // Право і Безпека. – 2011. – № 4. – С. 107–112. – Режим доступу: http://nbuv.gov.ua/UJRN/Pib_2011_4_26.

Федченко Д.И.
Институт прокуратуры и уголовной юстиции
Национального юридического университета имени Ярослава Мудрого

СИСТЕМА ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ: ПРОБЛЕМЫ ФОРМИРОВАНИЯ И ЭФФЕКТИВНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация
Данная научная статья посвящена исследованию таких актуальных современных явлений как кибербезопасность, киберпространство и киберпреступность. В статье проанализированы научные подходы к определению этих понятий, установлены их характерные признаки и взаимосвязь. Учитывая стремительное развитие киберпространства и явлений производных от него, исследованы реальность киберугроз и развитие киберпреступности, в связи с чем проанализирована необходимость формирования системы обеспечения кибербезопасности. В статье установлены проблемы создания этой системы и предложены пути их решения. В ходе научного исследования доказано, что на эффективность функционирования системы обеспечения кибербезопасности основное влияние осуществляет правовое регулирование как на международном, так и на национальном уровне, а также уровень взаимодействия и согласованности деятельности соответствующих субъектов.
Ключевые слова: кибербезопасность, киберпространство, киберугрозы, киберпреступность, система обеспечния кибербезопасности.

Fedchenko D.I.
Criminal Justice and Prosecutors' Training Institute,
Yaroslav Mudryi National Law University

CYBER SECURITY SYSTEM: PROBLEMS OF FORMATION AND EFFECTIVE ACTIVITY

Summary
This scientific article is devoted to the study of such topical contemporary phenomena as cybersecurity, cyberspace and cybercrime. The article analyzes scientific approaches to the definition of these concepts, establishes their characteristic features and interconnection. Given the rapid development of cyberspace and phenomena derived from it, the reality of cyber threats and the development of cybercrime has been explored, in connection with which the necessity of forming a system of cyber security has been analyzed. The article identifies the problems of creating this system and proposes ways of their solution. In the course of the research, it was proved that the legal regulation at the international and national level, as well as the level of interaction and coherence of the activities of the relevant actors, is mainly influenced by the effectiveness of the functioning of the cybersecurity system.
Keywords: cybersecurity, cyberspace, cyber threats, cybercrime, system of cyber security.