УДК 343
DOI https://doi.org/10.32782/2524-0374/2020-8/94

ЗАХИСТ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ЧАСТИНА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

INFORMATION PROTECTION AND CYBER SECURITY AS A COMPONENT OF UKRAINE'S NATIONAL SECURITY

Микитенко Д.О., студент ІІ курсу магістратури
Слідчо-криміналістичний інститут
Національного юридичного університету імені Ярослава Мудрого

У статті розглянуті актуальні питання забезпечення кібербезпеки в сучасних умовах, які торкаються широкого кола не лише приватних, але й корпоративних і навіть державних інтересів, та які мають широке розповсюдження і набувають загрозливого характеру. Наведено правовий аспект питань забезпечення кібербезпеки в Україні. Проаналізовано значення таких термінів, як «безпека», «національна безпека України», «інформація», «відомості», «дані», «кібербезпека» не тільки на побутовому, а й на доктринально-правовому і законодавчому рівнях тощо. Виокремлено пріоритетний напрям забезпечення національної безпеки – інформаційна безпека. Проаналізовано два основні підходи до захисту від загроз, що виходять із глобального інформаційного простору, а саме кібербезпека та інформаційна безпека. Проведено аналіз міжнародно-правових актів у сфері кібербезпеки та протидії кіберзлочинності, наприклад, Конвенції ООН про забезпечення міжнародної інформаційної безпеки, Конвенції ООН проти транснаціональної організованої злочинності від 15.11.2000 року, Конвенції про кіберзлочинність. Досліджено діяльність Міжнародного союзу електрозв'язку та Європейської ради, Центру національної кібербезпеки, групи координації безпеки електронної пошти (ESCG). Досліджено принципи забезпечення міжнародної інформаційної безпеки відповідно до Конвенції ООН про забезпечення міжнародної інформаційної безпеки. Виокремлені основні тенденції розвитку кіберзагроз у сучасному інформаційному просторі та заходи, необхідні для їх нейтралізації. Визначені основні проблеми, що виникають у міжнародному регулюванні боротьби з кіберзлочинністю, та основні загрози міжнародному миру і безпеці в інформаційному просторі. Відмічено наявність міждержавних угод Генеральної прокуратури України з головними органами прокуратури інших держав, наприклад, Угоди про співробітництво між Генеральною прокуратурою України та Федеральною прокуратурою Королівства Бельгія у боротьбі з кіберзлочинністю, організованою злочинністю, корупцією і тероризмом. Досліджені такі спеціалізовані органи, як Європейський центр з боротьби з кіберзлочинністю. Створено рекомендації для політики України у сфері забезпечення інформаційної безпеки та кібербезпеки на національному та міжнародному рівні.

Ключові слова: інформаційна безпека, кібербезпека, інформація, кіберпростір, національна безпека, кіберзлочинність, міжнародна інформаційна безпека, міжнародне регулювання боротьби з кіберзлочинністю.

The article considers topical issues of cybersecurity in modern conditions, which affect a wide range of not only private but also corporate and public interests, are widespread and threatening. The legal aspect of cybersecurity issues in Ukraine is presented. The meanings of such terms as "security", "national security of Ukraine", "information", "information", "data", "cybersecurity", etc. are analyzed. The meanings of such terms as "security", "national security of Ukraine", "information", "information", "data", "cybersecurity" are analyzed not only at the domestic, but also at the doctrinal-legal and legislative levels, etc. Information security has been identified as a priority for national security. There are two main approaches to protection against threats emanating from the global information space, cybersecurity and information security. An analysis of international legal acts in the field of cybersecurity and combating cybercrime, for example, the UN Convention on International Information Security, the UN Convention against Transnational Organized Crime of 15.11.2000, the Convention on Cybercrime. Study of the activities of the International Telecommunication Union and the European Council, the Center for National Cyber Security, the ESCG. An analysis of international legal acts in the field of cybersecurity and combating cybercrime. The main trends in the development of cyber threats in the modern information space and the measures needed to neutralize them are highlighted. The main problems that arise in the international regulation of the fight against cybercrime and the main threats to international peace and security in the information space are identified. There are interstate agreements between the Prosecutor General's Office of Ukraine and the main prosecutor's offices of other countries, such as the Agreement on Cooperation between the Prosecutor General's Office of Ukraine and the Federal Prosecutor's Office of the Kingdom of Belgium in combating cybercrime, organized crime, corruption and terrorism. The study includes specialized bodies such as the European Center for Combating Cybercrime. Recommendations for Ukraine's policy in the field of information security and cybersecurity at the national and international levels have been created.

Key words: information security, cybersecurity, information, cyberspace, national security, cybercrime, international information security, international regulation in the fight against cybercrime.

Постановка проблеми. Глобальна інформатизація сьогодні активно впливає на існування і життєдіяльність держав світової спільноти, інформаційні технології застосовуються у вирішенні завдань забезпечення національної, військової, економічної безпеки тощо. Разом із тим одним із фундаментальних наслідків глобальної інформатизації державних і військових структур стало виникнення принципово нового середовища протиборства конкуруючих держав – кіберпростору, яке не є географічним у загальноприйнятому сенсі цього слова, але, тим не менш, у повній мірі є міжнародним. І якщо сьогодні між провідними у військовому та економічному відношенні світовими державами склався в тій чи іншій мірі певний паритет у галузі застосування звичайних озброєнь і зброї масового ураження, а в міжнародному праві зафіксовані основні принципи взаємовідносин цих держав у межах таких просторів, як наземне, морське, повітряне, космічне, то питання про міждержавний паритет і взаємини в кіберпросторі натепер продовжують залишатися відкритим.

Вказане питання стало предметом дослідження таких науковців, як С.А. Буяджи, А.В. Войціховський, І.В. Гринчак, О.О. Грицун та інших.

Мета і завдання дослідження. Метою даної роботи є комплексний аналіз проблем захисту інформації та кібербезпеки як складової частини національної безпеки України.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1) розкрити сутність основних понять у сфері захисту інформації та кібербезпеки;

2) проаналізувати національне та міжнародне законодавство з питань кібербезпеки та протидії кіберзлочинності.

Виклад основного матеріалу. Поняття «безпека» в сучасному світі відіграє чи не найголовнішу роль у всіх життєвих процесах: біологічних, політичних, економічних, соціальних, технічних, територіальних тощо. Тому важливо не тільки коректно визначати це поняття і його

похідні, а й правильно застосовувати їх за призначенням. Натепер вітчизняне законодавство не містить загальної дефініції поняття «безпека». В юридичній літературі під безпекою розуміється рівень захищеності життєво важливих інтересів людини, а також суспільства, держави, навколишнього природного середовища від реальних або потенційних загроз, що їх створюють антропогенні чи природні фактори. При цьому виокремлюють воєнну, екологічну, економічну, інформаційну, пожежну політичну, продовольчу, радіаційну, соціальну, технічну, транспортну, фінансову, ядерну безпеку. Ключовим чинником політики будь-якої держави виступає національна безпека [6, с. 385].

Відповідно до ст. 1 Закону України «Про національну безпеку України» національною безпекою України визнається захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [16, с. 241].

Вивченням теоретичних підходів до інтерпретації поняття «національна безпека» з'ясовано, що існують різні підходи до сутності та змісту даної категорії, проте загалом вони відповідають легальній дефініції.

Одним із пріоритетних напрямів забезпечення національної безпеки є інформаційна безпека, оскільки сьогодні важливим стратегічним пріоритетом України є розвиток інформаційного суспільства та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя і в діяльність органів державної влади.

Відповідно до ст. 1 Закону України «Про інформацію» під інформацією розуміються будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [15, с. 650]. У ст. 1 Закону України «Про захист економічної конкуренції» вказано, що інформація являє собою відомості в будь-якій формі й вигляді, збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості [14, с. 64].

Аналіз вітчизняної правової доктрини свідчить, що більшість науковців дублюють законодавче визначення «інформація» через поняття «відомості», «дані»: зокрема, під інформацією розуміють: 1) відомості, що передаються усним, письмовим або іншим способом, зокрема за допомогою умовних сигналів, технічних засобів і т.п. [19, с. 24]; 2) відомості (а не дані) про події та явища, які можуть бути пізнані особою та передані іншій особі у вигляді, придатному для сприйняття [12, с. 9]; 3) відомості про об'єктивно існуючі явища, які використовуються більш ніж однією особою, незалежно від форми та способу надання в суспільних відносинах [13, с. 7] тощо.

Таким чином, поняття «інформація», «дані», «відомості», «повідомлення», «знання» не тільки на побутовому, а й на доктринально-правовому і законодавчому рівнях визначаються одне через одного та є синонімами.

Особливістю поняття «інформація» є його універсальність. Воно використовується в усіх без винятку сферах людської діяльності, водночас визначення категорії «інформація» передусім залежить від конкретної галузі знань, в якій ведеться дослідження. Виходячи з наведених вище визначень, ми можемо говорити про те, що з правової точки зору інформація – це дані, які є об'єктом комунікації, і посягання на інформацію слід розглядати у двох площинах: як посягання безпосередньо на інформацію і як посягання на можливості її безперешкодної передачі (комунікації). Таким чином, інформація, будучи засобом комунікації, стає об'єктом правового захисту вже в момент її появи, незалежно від того, в якій формі вона надана і незалежно від її подальшого поширення.

Упродовж останніх десятиліть інформація набуває властивостей потужного засобу впливу на суспільно-політичні, ідеологічні та соціально-економічні процеси, стає свого роду зброєю, яке вимагає створення системи протидії, захисту інформаційних ресурсів, що належать державним органам і становлять державну, лікарську, особисту таємницю.

Існує два основні підходи до захисту від загроз, що виходять із глобального інформаційного простору, – кібербезпека та інформаційна безпека. Ці підходи не є взаємовиключними. Проте вони відображають соціально-культурні, економічні та політичні особливості держав і спрямовані на реалізацію відповідних національних інтересів.

У звіті «Global Digital 2018» від We Are Social і Hootsuite повідомлялося, що в жовтні 2018 р. у світі налічувалось майже 4,2 мільярда користувачів Інтернету (зростання за рік – 7%), біля 3,4 мільярда осіб по всьому світу використовували соціальні мережі (зростання за рік – 10%), більше 5,1 мільярда чоловік користувалися мобільним телефоном, більшість з яких – смартфон [23].

Нині визначення поняття «кібербезпека» закріплено на законодавчому рівні, а саме у ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», де 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 в кіберпросторі [17, с. 103]. У цій же статті надається визначення поняттю «кіберпростір», яким визнається 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.

Із зазначених вище дефініцій убачається, що інформаційна безпека ширше кібербезпеки і крім питань, пов'язаних з технічним забезпеченням безпеки інфраструктури та безпеки інформації, розглядає проблеми захисту особистості й суспільства від деструктивного інформаційного впливу. У свою чергу визначення терміна «кібербезпека» базується на понятті «кіберпростір» та являє собою сукупність умов, за яких всі складники кіберпростору захищені від максимально можливої кількості загроз і впливів з негативними наслідками.

Натепер сформована правова основа у сфері кібербезпеки України, яка, крім Законів України «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України», «Про інформацію», включає також Доктрину інформаційної безпеки України (введена в дію 25.02.2017 року) [18], а також інші законодавчі та підзаконні нормативно-правові акти.

Вивчення даних законодавчих актів з'ясувало, що кібербезпека та інформаційна безпека визначаються як одні з головних пріоритетів у протидії загрозам національній безпеці.

Надзвичайно важливу роль у сфері захисту інформації та кібербезпеки відіграє міжнародно-правове регулювання [1, с. 78]. Міжнародне співтовариство на різних рівнях виробило ряд актів, що мають значення для захисту інформації та кібербезпеки, причому особливу роль відіграють регіональні акти, оскільки універсальний документ натепер створити важко. Разом із тим не можна не відзначити спроби держав поширити норми глобальних міжнародних договорів на боротьбу з кіберзлочинністю або укласти нові договори. Наприклад, оскільки в кіберпросторі поряд з окремими особами можуть діяти й орга-

нізовані злочинні групи, існує можливість застосування до них міжнародних договорів, спрямованих на боротьбу з організованою злочинністю, зокрема Конвенції ООН проти транснаціональної організованої злочинності від 15.11.2000 року [9, с. 1056].

Крім того, розроблено концепцію Конвенції ООН про забезпечення міжнародної інформаційної безпеки [8]. У ст. 4 Конвенції закріплені основні загрози міжнародному миру і безпеці в інформаційному просторі, з яких виділено 11 базових і 4 додаткових. Серед базових названі, наприклад, використання інформаційних технологій і засобів для здійснення ворожих дій і актів агресії; цілеспрямований деструктивний вплив у інформаційному просторі на критично важливі структури іншої держави; транскордонне поширення інформації, яка суперечить принципам і нормам міжнародного права, а також національним законодавствам держав. Знову ж у документі не вказані такі реальні загрози міжнародній безпеці, як вчинення кіберзлочинів, розповсюдження наркотичних і психотропних засобів, їхніх аналогів, а також порнографії, в тому числі й дитячої.

Крім цього, концепція Конвенції містить ст. 5, присвячену основним принципам забезпечення міжнародної інформаційної безпеки. Аналіз представлених принципів дозволяє зробити висновок про те, що їх можна розділити на чотири групи: принципи участі держави в системі міжнародної інформаційної безпеки як члена міжнародного співтовариства; принципи, які дозволяють державі зберегти свій суверенітет у процесі міжнародного співробітництва в боротьбі з кіберзлочинністю; принципи забезпечення вільного інформаційного обміну між країнами. Четверта група принципів установлює характер взаємодії держави і приватних суб'єктів у розглядуваних відносинах. Разом із тим знову ж доводиться констатувати, що в концепції Конвенції детально не прописані принципи міжнародного співробітництва в боротьбі з кіберзлочинами, крім спрямованого проти дій терористичного характеру [8].

Таким чином, положення концепції Конвенції ООН про забезпечення міжнародної інформаційної безпеки носять достатній, але компромісний характер і орієнтовані насамперед на попередження інформаційних війн, тероризму.

Важливі питання співробітництва держав у боротьбі зі злочинним використанням інформаційно-комунікаційних технологій було покладено на Міжнародний союз електрозв'язку. Результатом діяльності стало прийняття вказаним суб'єктом Глобальної програми кібербезпеки [3, с. 174], яка визначила цілі, принципи і стратегії розробки моделей законодавства у сфері боротьби з комп'ютерною злочинністю.

Не можна не відзначити, що більшу частину спеціалізованих актів з боротьби з кіберзлочинами становлять акти Європейського союзу, який має одну з найбільш розвинених у світі систем забезпечення інформаційної безпеки. Так, у жовтні 1999 року в ході Тамперської наради Європейської ради ЄС було прийнято рішення про доцільність включення злочинів у сфері високих технологій (high-tech crime) у число злочинів, за якими необхідне вироблення загального європейського підходу в частині криміналізації і санкцій [21, с. 267].

У 2001 році Європейська комісія представила спеціальне повідомлення «Створення безпечного інформаційного суспільства за допомогою підвищення захищеності інформаційної інфраструктури і боротьби зі злочинами з використанням комп'ютерних засобів», у якому містилися пропозиції правового та організаційного характеру щодо боротьби з кіберзлочинністю в Європейському союзі.

Як для Європейського союзу, так і для всієї світової спільноти принципове значення має Конвенція про кіберзлочинність, яка регламентує глобальні заходи боротьби з кіберзлочинністю й була прийнята Радою Європи у 2001 році (ратифікована Україною 07.09.2005 року) [10].

У Конвенції про кіберзлочинність кіберзлочини класифікуються так:

1) злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (offences against the confii dentiality, integrity and availability of computer data and systems): протизаконний доступ (illegal access); неправомірне перехоплення (Illegal interception); вплив на дані (data interference); вплив на функціонування системи (system interference); протизаконне використання пристроїв (Misuse of devices);

2) правопорушення, пов'язані з використанням комп'ютерних засобів (Computer-related offences): фальсифікація з використанням комп'ютерних технологій (computer-related forgery); шахрайство з використанням комп'ютерних технологій (computerrelated fraud);

3) злочини, пов'язані з утримуванням даних (content-related offences); злочини, пов'язані з дитячою порнографією (Offences related to child pornography);

4) правопорушення, пов'язані з порушенням авторського права і суміжних прав (offences related to infringements of copyright and related rights) [10].

Додатковий протокол до Конвенції про кіберзлочинність включає в зазначений перелік такі види злочинів: 1) поширення расистських і ксенофобських матеріалів за допомогою комп'ютерних систем (dissemination of racist and xenophobic material through computer systems); 2) мотивована загроза расизму і ксенофобії (racist and xenophobic motivated threat); 3) расистська і ксенофобська мотивована образа (Racist and xenophobic motivated insult); 4) невизнання, надзвичайна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства (denial, gross minimisation, approval or justifii cation of genocide or crimes against humanity) [4].

Конвенція передбачає також і розвиток кримінального процесуального законодавства, наприклад, необхідність законодавчого закріплення оперативного забезпечення збереження накопичених комп'ютерних даних, процедури проведення обшуку і виїмки збережених комп'ютерних даних.

Основні проблеми, що виникають у міжнародному регулюванні боротьби з кіберзлочинністю, полягають у відмінності національних стандартів у сфері кібербезпеки; відсутності чіткого уніфікованого категоріального апарату; недостатньому рівні координації діяльності правоохоронних органів під час розслідування кіберзлочинів, низькому рівні обміну інформацією про кіберінциденти між державами; недостатньому рівні державно-приватного співробітництва [20, с. 99].

Також варто відмітити наявність міждержавних угод Генеральної прокуратури України з головними органами прокуратури інших держав. Зокрема, у 2015 році було укладено Угоду про співробітництво між Генеральною прокуратурою України та Федеральною прокуратурою Королівства Бельгія в боротьбі з кіберзлочинністю, організованою злочинністю, корупцією і тероризмом [22]. Подібні угоди були укладені, зокрема, і з Національною прокуратурою Королівства Нідерланди [11] та державами пострадянського простору.

На міжнародному рівні з метою захисту інформації та кібербезпеки створюються також спеціалізовані органи. Оскільки інформаційна безпека держави пов'язана з її суверенітетом, то створення єдиного органу, який би координував взаємодію держав щодо боротьби з кіберзлочинами, ускладнено, проте створюються допоміжні органи, які додержуються єдиних стандартів діяльності, узагальнюють практику різних країн з питань боротьби з кіберзлочинами [5, с. 65].

Велике значення у взаємодії держав – учасників Європейського союзу має діяльність Європолу та Євроюсту,

які беруть безпосередню участь у боротьбі з кіберзлочинністю на просторі Європейського союзу [21, с. 268]. У роботі Європолу використовується система аналітичних робочих картотек (analys work fiiles), що формуються шляхом зосередження в його інформаційних системах даних з метою аналізу, що визначається як обробка або використання даних для підтримки кримінальних розслідувань. Система діючих аналітичних картотек включає картотеки з кіберзлочинності Cyborg і дитячої порнографії Twins [2, с. 110].

Крім зазначених органів, які мають юрисдикційну компетенцію в розглядуваній сфері, Європейським союзом створюються і допоміжні органи. Так, 18.01.2013 року в Гаазі офіційно відкритий Європейський центр з боротьби з кіберзлочинністю. Цілями його створення є збір і обробка даних стосовно кіберзлочинів, проведення експертних оцінок інтернет-загроз, розроблення і впровадження передових методів профілактики і розслідування кіберзлочинів, підготовка нових кадрів, надання допомоги правоохоронним і судовим органам, а також координація спільних дій зацікавлених сторін, спрямованих на підвищення рівня безпеки в європейському кіберпросторі [7, с. 85].

Особливої уваги заслуговують системи протидії кіберзлочинам на рівні окремих держав. Наприклад, у США поряд з уже функціонуючим Центром національної кібербезпеки (National Cyber Security Center) у складі Збройних сил сформовано Об'єднане кібернетичне командування (Unified US Cyber Command), яке в глобальному масштабі має координувати зусилля всіх структур Пентагону в ході ведення бойових дій, надавати відповідну підтримку цивільним федеральним установам, а також взаємодіяти з аналогічними за завданнями відомствами інших країн.

У Великобританії реалізуються програми зі створення кіберзброї, які забезпечать здатність влади протистояти зростаючим загрозам з кіберпростору. В Австралії створено групу координації безпеки електронної пошти (ESCG). Основним завданням цієї групи є створення безпечного і надійного електронного оперативного простору як для суспільного, так і для приватного секторів [3, с. 36].

Висновки. Наслідком активного використання інформації у всіх сферах людської діяльності є виникнення залежності особистості, суспільства і держави від безперебійного і надійного функціонування інформаційно-комунікаційних систем. Залежність у свою чергу призводить до появи якісно нових загроз, заснованих на використанні властивих інформаційно-комунікативним системам вразливостей, що в ряді випадків є несумісним із завданнями підтримки національної і міжнародної стабільності і безпеки. На міжнародному рівні визнано, що джерелами загроз можуть бути терористи, кіберзлочинці, а також держави.

Існує два основні підходи до захисту від загроз, що виходять із глобального інформаційного простору – кібербезпека та інформаційна безпека. Ці підходи не є взаємовиключними. Проте вони відображають соціально-культурні, економічні та політичні особливості держав і спрямовані на реалізацію відповідних національних інтересів. Інформаційна безпека ширше кібербезпеки і крім питань, пов'язаних з технічним забезпеченням безпеки інфраструктури та безпеки інформації, розглядає проблеми захисту особистості й суспільства від деструктивного інформаційного впливу.

Аналіз міжнародних нормативно-правових актів, законодавства України й ряду зарубіжних держав показує, що багато законів уже включають елементи, необхідні для обмеження деструктивного інформаційного впливу на особистість, суспільство і державу. Зокрема, у багатьох державах існують закони, що дозволяють здійснювати фільтрацію шкідливого контенту. Інтернет повинен, безсумнівно, залишатися простором свободи і загальнолюдським надбанням; кожен повинен мати право на доступ до інформації та право на свободу самовираження. Водночас не можна заперечувати той факт, що свобода не має на увазі вседозволеність, а навпаки, має на увазі відповідальність за свої дії як у фізичному світі, так і у віртуальному просторі.

У числі рекомендацій для політики України у сфері забезпечення інформаційної безпеки та кібербезпеки на національному та міжнародному рівні необхідно продовжити і розширити діяльність зі створення умов для формування системи міжнародної інформаційної безпеки на основі загальновизнаних принципів і норм міжнародного права. Важливо розвивати співробітництво в цій сфері. На рівні ООН необхідно підготувати й ухвалити міжнародно-правові акти, що регламентують застосування принципів і норм міжнародного гуманітарного права у сфері використання інформаційних та комунікаційних технологій.

З урахуванням усієї складності й небезпеки кіберзлочинів необхідне вироблення спільних дій учених-юристів, передусім законодавців і, звичайно ж, фахівців у галузі комп'ютерних інформаційних технологій, спрямованих на боротьбу зі злочинами в глобальних інформаційних мережах. Оскільки впровадження нормативних актів як національного, так і міжнародного характеру – недостатній крок на шляху вирішення проблеми боротьби з кіберзлочинністю, в даному випадку необхідні спеціальні знання у сфері інформаційних технологій і програмного забезпечення. Єдиного глобального акта, який регламентує порядок протидії кіберзлочинам, не вироблено, проте міжнародне співтовариство в межах регіонального співробітництва вживає заходів стосовно законодавчого врегулювання дій суб'єктів у кіберпросторі й боротьби з кіберзлочинами.

ЛІТЕРАТУРА

1. Буяджи С.А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. … здоб. наук. ступ. канд. юрид. наук. 12.00.01. Київ, 2018. 203 с.
2. Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. *Право і безпека*. 2011. № 4 (41). С. 107–112.
3. Грицун О.О. Регулювання питань міжнародної інформаційної безпеки в межах міжнародних організацій. *Вісник Запорізького національного університету. Юридичні науки*. 2014. № 4 (1). С. 172–180.
4. Демедюк С.В. Міжнародний досвід протидії кіберзлочинності. *Вісник Харківського національного університету внутрішніх справ: збірник наукових праць.* Харків. 2014. № 4 (67). С. 65–75.
5. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: міжнародний документ від 28.01.2003 р. *Офіційний вісник України* 2010. № 56 ;. 2006. № 31. Ст. 2202. С. 73. 1920 с.
6. Енциклопедія сучасної України. Київ, 2003. Т. 2. 695 с.
7. Кобилянська Л. Правові засади міжнародного співробітництва у сфері боротьби з кіберзлочинністю. *Матеріали регіональної науково-практичної конференції «Європейські та міжнародні підходи до захисту прав людини»*, Київ. С. 83–88.
8. Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.scrf.gov.ru/documents/6/112.htm (дата обращения: 28.10.2020).
9. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності: міжнародний документ від 15.11.2000 р. *Офіційний вісник України*. 2006. № 14. 1056 с.
10. Конвенція про кіберзлочинність: міжнародний документ від 23.11.2001 р. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 28.10.2020).

11. Меморандум про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом: Міжнародний документ від 09.09.2009 р. *Офіційний вісник України.* 2009. № 76. 2601 с.

12. Петров Є.В. Інформація як об'єкт цивільно-правових відносин : автореф. дис. … канд. юрид. наук. 12.00.03. Харків, 2003. 19 с.

13. Правова охорона як складова інформаційної безпеки цивільної авіації : автореф. дис. … канд. юрид. наук : 12.00.03 ; Держ. НДІ МВС України. Київ, 2010. 20 с.

14. Про захист економічної конкуренції : Закон України від 11.01.2001 року № 2210-III**.** *Відомості Верховної Ради України*. 2001. № 12. 64 с.

15. Про інформацію : Закон України від 02.10.1992 року № 2657-XII. */Відомості Верховної Ради України*. 1992. № 48. 650 с.

16. Про національну безпеку України : Закон України від 21.06.2018 року № 2469-VIII/ *Відомості Верховної Ради*. 2018. № 31. 241 с.

17. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 року № 2163-VIII/*Відомості Верховної Ради*. 2017. № 45. 403 с.

18. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 року № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 28.10.2020).

19. Синєокий О.В. Інформаційне право України та електронне право високих технологій : електронний курс лекцій українською мовою. Запоріжжя : ЗНУ, 2010. 215 с.

20. Скулиш Є.Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право*. 2014. № 1 (10). С. 93–100.

21. Смирнов А.А. Система борьбы с киберпреступностью в Европейском Союзе. *Библиотека криминалиста*. 2012. № 2 (3). С. 262–274.

22. Угода про співробітництво між Генеральною прокуратурою України та Федеральною прокуратурою Королівства Бельгія у боротьбі з кіберзлочинністю, організованою злочинністю, корупцією і тероризмом: міжнародний документ від 15.10.2015 р. *Офіційний вісник України.* 2015. № 90. С. 443. 3083 с.

23. Internet World Stats (IWS). URL: https://www.internetworldstats.com/stats.htm (дата звернення: 28.10.2020).