Інформаційна і національна безпека

УДК 341.232

КОВАЛЬОВ К.Є., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1243-3973.

ІНФОРМАЦІЙНА БЕЗПЕКА: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

Анотація. *У статті висвітлені міжнародно-правові аспекти інформаційної безпеки. Представлені результати аналізу міжнародно-правових норм у сфері інформаційної безпеки, а також зарубіжного досвіду у цій сфері. Підкреслено значущість досвіду окремих зарубіжних країн у сфері забезпечення інформаційної безпеки для України. З огляду на глобальний характер мереж зв'язку зроблено висновок, що інформаційна безпека має бути забезпечена лише за умови ефективної міжнародної взаємодії держав. В ході дослідження визначаються пріоритети та проблеми забезпечення інформаційної безпеки у країнах Східної Європи. Виділені пріоритетні напрями правового забезпечення інформаційної безпеки України.*

Ключові слова*: інформаційна безпека, кібербезпека, національна безпека, правовий аспект, міжнародна співпраця.*

Summary. *The article highlights the international legal aspects of information security. The results of the analysis of international legal norms in the field of information security, as well as foreign experience in this field, are presented. The importance of the experience of certain foreign countries in the field of information security for Ukraine is emphasized. Given the global nature of communication networks, it is concluded that information security should be ensured only through effective international cooperation between states. During the research, priorities and issues related to information security in Eastern European countries are determined. Prioritized directions for legal support of information security in Ukraine have been identified.*

Keywords: *information security, cyber security, national security, legal aspect, international cooperation.*

Постановка проблеми. Стрімкий розвиток інформаційно-комунікаційних технологій, тотальна комп'ютеризація, створення глобального інформаційного простору зумовлює послаблення інформаційного суверенітету держави. Глобалізація інформаційного простору не може не впливати на стан інформаційної безпеки будь-якої держави.

Створення інформаційного суспільства зумовило виникнення багатьох новітніх загроз у важливих сферах життєдіяльності суспільства (банківська, воєнна, критична інфраструктура тощо), тому інформаційну безпеку цілком виправдано розглядають як самостійний елемент національної безпеки [1, с. 284].

Захищаючи свої інформаційні інтереси, кожна держава має дбати про інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України повинна формуватися як складова її національної безпеки та частина соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством [2, с. 68].

В умовах сучасного розвитку інформаційних комунікацій кожна держава виробляє власну стратегію поведінки та політики у сфері інформаційної безпеки.

Так, в країнах, які постійно знаходяться у фокусі інформаційного впливу (Китай, США, Ізраїль, Британія, ФРН та ін.), функціонують найбільш розвинуті системи інформаційної безпеки.

Проблема забезпечення інформаційної безпеки не обійшла й Україну. У зв'язку з подіями, що відбулися 24.02.2022 р., введенням в Україні воєнного стану, з боку російської федерації відбувається інформаційна експансія, упереджене та систематичне висвітлення спотворених фактів та явищ, спрямованих на пропаганду національної ворожнечі, насильства та сепаратизму.

Інформаційно-психологічні операції росії спрямовані на руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави тощо. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіа-заходи відбувається вплив не лише на свідомість громадян України, а й на світову спільноту. Мета цих заходів – забезпечити домінування (утримання медійної переваги) як в українському, так і міжнародному інформаційному просторі.

Результати аналізу наукових публікацій. Дослідженням сучасних загроз інформаційної безпеки займалися багато вітчизняних дослідників, серед яких можна виділити роботи Н.М. П.Д. Біленчука [3], О.Р. Вайцеховської [4], М.М. Присяжнюка [5], В.А. Ліпкана [3], М.О. Сенченка [6], О.Л. Гурковського, О.М. Яхно, О.В. Левченко, В.М. Бебика, Г.Г. Почепцова, І.С. Чижа, В.М. Скалацького, О.В. Сосніна, В.М. Абакумова, Є.О. Кирильчука та ін.

Проблематика наукових досліджень не втрачає своєї актуальності, оскільки загрози інформаційній безпеці держави в сучасних умовах розвитку інформаційного суспільства є динамічними та постійно змінюються.

Метою статті є визначення міжнародно-правових аспектів забезпечення інформаційної безпеки держави в контексті удосконалення законодавства у цій сфері.

Виклад основного матеріалу. Переважна більшість дослідників вважає, що під інформаційною безпекою слід розуміти стан захищеності національних інтересів України в інформаційній сфері, що складається із сукупності збалансованих інтересів особи, суспільства та держави, від внутрішніх та зовнішніх загроз.

З точки зору П.Д. Біленчука, безпека в інформаційній сфері передбачає забезпечення інформаційного суверенітету; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження сучасних технологій у цій сфері, наповнення інформаційного простору достовірною інформацією; забезпечення конституційного права громадян на свободу слова, доступу до інформації, недопущення протиправного втручання органів державної влади у діяльність засобів масової інформації; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери держави [3, с. 54-55].

Про інформаційний суверенітет також пише і О.Р. Вайцеховська [4, с. 243]. Осмислення сукупності інформаційних процесів щодо забезпечення їх безпеки має велике значення як для окремого суспільства, так і міжнародного співтовариства в цілому.

Інформаційна безпека є не лише складовою національної безпеки, а й невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки,

адже всі типи взаємовідносин між суб'єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією. З цього приводу В.А. Ліпкан зазначає, що національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу [6].

Український учений М. Сенченко справедливо відзначає, що Україні для ефективного протистояння інформаційній війні з боку росії потрібно мати хоча б: 1) ефективну систему ведення інформаційної війни; 2) ефективну правову концепцію інформаційної війни; 3) стратегію ведення інформаційної війни [7]. Лише та держава може розраховувати на лідерство в економічній, військово-політичній чи інших сферах, мати стратегічну й тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби [5].

Інформаційна безпека України передбачає головне стратегічне завдання: створити потужний національний інформаційний простір як головний аспект, що засвідчує присутність країни на світовій інформаційній арені. Реалізація такого завдання зумовлює потребу створення системи протидії будь-якій інформаційній загрозі та захисту власних інформаційних ресурсів, середовища та інфраструктурної складової країни. Застосування росією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України росія використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [8].

Механізми захисту інформаційної безпеки України можна розділити на два рівні – законодавчий та адміністративний. Найважливіше на законодавчому рівні – створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, що може спричинити послаблення інформаційної безпеки.

Адміністративний механізм забезпечення інформаційної безпеки охоплює установи, діяльність яких спрямована на формування та реалізацію інформаційної безпеки. Головне на адміністративному рівні – сформувати програму заходів в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи поточний стан справ.

Сьогодні запорукою створення надійної системи забезпечення охорони інформаційної безпеки може бути тільки зміцнення самої української держави та державних органів, відповідальних за її забезпечення. Реалізація цього завдання зумовлює масштабні завдання, пов'язані з виробленням системи забезпечення інформаційної безпеки, пошуком принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління ризиками та загрозами [9].

Серед основних напрямів забезпечення інформаційної безпеки виділяють: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; зміцнення інформаційної безпеки на державному рівні шляхом

впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг тощо; розвиток міжнародного співробітництва з питань інформаційної безпеки [10].

Інформаційна безпека як поняття розглядається у декількох ракурсах.

У найзагальнішому вигляді – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах особи, суспільства, держави. Інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, юридичних заходів, спрямованих на забезпечення сталого розвитку суспільства і держави [11, с. 64].

Оскільки суспільні відносини, що виникають у зв'язку із забезпеченням інформаційної безпеки регулюються нормами права, є необхідним проаналізувати основні принципи і норми, спрямовані на забезпечення інформаційної безпеки.

Український законодавець за роки незалежності сформував потужну правову базу у сфері національної безпеки, основою для якої є чинна Конституція України. Так, у ч. 1 ст. 3 Конституції України сформульовано концептуальні засади забезпечення безпеки людини: "людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визначаються в Україні найвищою цінністю". У ч. 1 ст. 17 Конституції України передбачено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [12].

Загалом, у Конституції України містяться правові норми, пов'язані із забезпеченням інформаційної безпеки, які становлять основу законодавства у цій сфері і мають вищу юридичну силу. У цих нормах закріплено право на інформацію, передбачена охорона відомостей, що становлять державну таємницю.

Конституційні норми, пов'язані із забезпеченням інформаційної безпеки, вказують на те, що це питання є настільки багатоаспектним та багатогранним, що кожна з зазначених правових норм може стати окремими темами наукових досліджень.

Правові засади національної безпеки України також регламентуються Законом України "Про національну безпеку України" від 21 червня 2018 р. [13].

У різних державах розроблені основні принципи та інструментальні засоби формування ефективного інформаційного захисту національного простору. Застосовуючи різні засоби, країни-лідери достатньо ефективно здійснюють національну політику інформаційної безпеки.

Відповідно до національної специфіки й унікальної ролі нашої держави в сучасній геополітиці, необхідно постійно аналізувати та застосовувати закордонний досвід.

Наразі йдуть активні процеси формування міжнародного досвіду у сфері забезпечення інформаційної безпеки в рамках діяльності таких міжнародних організацій, як ООН, Ради Європи, Європейського Союзу та інших.

Основні принципи законодавчого регулювання суспільних відносин у сфері міжнародної інформаційної безпеки сформульовані в основних міжнародних документах, їх потрібно постійно вивчати та аналізувати, а головне робити висновки та постійно удосконалювати законодавство України.

Враховуючи масштаби глобального інформаційного виклику, неможливість вирішення зазначених проблем зусиллями однієї або навіть декількох держав, слід усвідомити необхідність розвитку міждержавного співробітництва в сфері забезпечення міжнародної інформаційної безпеки в межах Організації Об'єднаних Націй, здатної комплексно вирішувати будь-які політичні проблеми, при найширшому представництві і

максимально враховуючи інтереси всієї світової спільноти. Ідея забезпечення міжнародної інформаційної безпеки вперше отримала практичну реалізацію в Резолюції Генеральної Асамблеї ООН A/RES/53/70 "Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки" від 4 грудня 1998 р. Цей документ започаткував спільне обговорення питань створення абсолютно нового міжнародно-правового режиму, структурним елементом якого в перспективі стали інформація, інформаційна технологія і методи її використання [14].

Отже важливу участь у безпекових заходах традиційно бере ООН. Її діяльність у сфері інформаційної безпеки спрямована на розробку міжнародно-правової бази та вироблення документів для протидії протиправному використанню науково-технологічного прогресу терористичними угрупованнями та організованою злочинністю. Проблема інформаційної безпеки в контексті формування глобального інформаційного суспільства стала актуальною для діяльності спеціалізованих установ ООН, зокрема, ЮНЕСКО та МСЕ, враховуючи гуманітарні та технічні програми та проекти організацій [15].

Невизначеність на глобальному рівні та відсутність єдиних підходів змушує керівництво держав формувати політику кібербезпеки на національному рівні.

Серед міжнародних організацій, основною метою яких є саме безпека, НАТО найбільш ефективно модернізувала політику щодо інформаційної безпеки. Організація заснувала центри у країнах-членах як багатонаціональні інститути для розробки доктрини кібербезпеки, вдосконалення міждержавної взаємодії, впровадження теоретичних напрацювань у практиці протидії кіберзагрозам, обміну досвідом кіберзахисту представників країн-членів і країн-партнерів. Наразі Центр кібербезпеки НАТО функціонує в Естонії, він не є підрозділом військового командування або структури збройних сил НАТО, а персонал та фінансування забезпечуються державами-спонсорами та державами-учасниками [16].

Активну політику щодо забезпечення інформаційної безпеки проводить і Європейський Союз. Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки стало одним із пріоритетних напрямів діяльності ЄС.

У 2001 р. Європейською Комісією було представлено перший документ під назвою "Мережева та інформаційна безпека: європейський політичний підхід", в якому була представлена концепція вирішення проблеми інформаційної безпеки. У документі використовується термін "мережева та інформаційна безпека", який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [17].

Усвідомлюючи той факт, що ефективність забезпечення інформаційної безпеки в європейському кіберпросторі також залежить від розвитку співпраці держав у рамках міжнародних органів у 2013 р. в структурі Європейського поліцейського офісу (Європол) був утворений Європейський центр боротьби з кіберзлочинністю.

До пріоритетних напрямів діяльності Центру відноситься розслідування шахрайства через Інтернет-мережі, а також розслідування злочинів, що посягають на безпеку критично важливої інфраструктури та інформаційних систем ЄС [18].

З метою протидії інформаційним загрозам, таким як кібертероризм та кіберзлочинність, Україна враховує стандарти ЄС та НАТО, постійно співпрацює та переймає досвід багатьох країн Східної Європи щодо приведення національного законодавства у відповідність до вимог вказаних міжнародних стандартів.

Розуміючи актуальність проблеми забезпечення інформаційної безпеки як складової системи національної безпеки, більшість держав світу почали здійснювати внутрішньодержавні комплексні заходи з забезпечення безпеки в кіберпросторі.

Європейські країни активно модернізують власні сектори безпеки у кіберпросторі у відповідності до викликів сучасності.

Цей процес відбувається шляхом:

- впорядкування нормативної бази, що має забезпечити цілісність державної політики в даній сфері;
- вироблення європейських керівних принципів щодо забезпечення інформаційної безпеки;
- збільшення чисельності підрозділів, що забезпечують інформаційну безпеку;
- посилення контролю за національним інформаційним простором;
- зміцнення захисних механізмів для критичної інформаційної інфраструктури ЄС тощо.

Ці заходи пов’язані, перш за все, з розробкою і вдосконаленням національного законодавства в даній галузі і створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі.

На сьогодні кібербезпека є стратегічною проблемою державного значення, яка зачіпає всі верстви населення. Державна політика з кібербезпеки служить засобом посилення національної безпеки і надійності інформаційних систем держави. Стратегії з кібербезпеки були прийняті такими державами як США, Швеція, Естонія, Фінляндія, Чехія, Франція, Німеччина, Литва, Великобританія, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія тощо. Список країн наочно показує, що проблема кібербезпеки визнається актуальною в усьому світі.

Україна схвалила Стратегію кібербезпеки України [21]. Цей документ визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики інформаційної безпеки, яка відповідатиме світовому рівню.

На основі вивчення міжнародних правових актів, що стосуються протидії новим викликам та загрозам в інформаційній сфері, а також впливу глобалізації на визначення національної стратегії розвитку інформаційного суспільства, очевидним є висновок про необхідність подальшої імплементації положень міжнародних правових актів та гармонізації з законодавствами іноземних держав.

Заходи щодо забезпечення інформаційної безпеки України повинні здійснюватися шляхом: забезпечення інформаційного суверенітету України; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України тощо [21].

Отже, в умовах сучасного розвитку інформаційного суспільства, захист національного інформаційного простору та забезпечення інформаційної безпеки вже стали пріоритетними стратегічними завданнями багатьох держав світу.

Інформаційна безпека визнається невід'ємним елементом системи національної безпеки. При цьому, інформаційна безпека як складова національної безпеки держави може розглядатися як її самостійна частина. Міжнародний характер загроз інформаційної безпеки зумовлює необхідність вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва в рамках міжнародних організацій у зазначеній сфері. Питання забезпечення інформаційної безпеки є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України. Зважаючи на те, що стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, то завданням для української влади повинен стати розвиток ефективного діалогу з ЄС у питаннях забезпечення інформаційної безпеки [1].

На нашу думку, використання взаємодоповнюючих та скоординованих заходів на регіональному та міжнародному рівнях дозволить успішно протистояти сучасним викликам та загрозам безпеці в інформаційній сфері, що можуть порушити доступність, цілісність і конфіденційність інформації, що зберігається або передається за допомогою мережі або інформаційної системи.

Інтенсивний розвиток інформаційних технологій призводить до появи нових загроз національній безпеці, а тому використання скоординованих та взаємодоповнюючих заходів на двосторонньому, регіональному та міжнародному рівнях дозволить адекватно протистояти сучасним викликам та загрозам безпеці в інформаційній сфері.

Інформаційна безпека в силу глобального характеру мереж зв'язку може бути забезпечена лише при міжнародній взаємодії. У зв'язку з цим необхідно посилити взаємодію України із закордонними країнами, міжурядовими організаціями з питань правового забезпечення інформаційної безпеки. Аналіз зарубіжного законодавства, що регулює інформаційну сферу, дозволяє стверджувати, що в сфері правового регулювання права на інформацію, доступу до інформації, ЗМІ, а також обмеження свободи інформації відбулися істотні зміни. Аналіз міжнародних і зарубіжних правових актів в інформаційній сфері свідчить про те, що є значний і різноманітний досвід правового регулювання як на міжнародному, так і на національному рівнях. Зарубіжні державні органи відіграють вирішальну роль в координації дій суб'єктів у сфері забезпечення інформаційної безпеки. Пріоритетним напрямком стає вдосконалення законодавства, що встановлює відповідальність за правопорушення, розробка та законодавче закріплення переліку правопорушень та видів відповідальності в сфері інформаційної безпеки [10].

Висновки.

Міжнародний характер загроз інформаційної безпеки зумовлює необхідність вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва в рамках міжнародних організацій у цій сфері. У зв'язку з цим необхідно посилити взаємодію України із зарубіжними партнерами, міжурядовими організаціями з питань правового забезпечення інформаційної безпеки.

Провідні держави в сучасних міжнародних відносинах використовують інформацію як стратегічний ресурс для реалізації своїх геополітичних завдань. Тому інформаційна безпека сьогодні є одним із пріоритетних напрямів національної безпеки України. Могутність країни на зовнішньополітичній арені визначається її можливостями впливати на міжнародне інформаційне поле, а отже, і на інформаційне середовище інших держав.

З метою протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання держави полягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність,

сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, попередження інформаційних конфліктів та оперативне їх подолання [9].

Сучасні інформаційні протистояння засвідчили, що інформаційний простір України потребує додаткового захисту від зовнішніх негативних інформаційно-психологічних впливів. Таким чином, національні інтереси України у сфері інформаційної безпеки повинні полягати у розвитку сучасних телекомунікаційних технологій, у захисті державних інформаційних ресурсів від несанкціонованого доступу.

Саме тому дослідження багатоаспектної проблематики інформаційної безпеки держави, соціуму і людини є сьогодні надзвичайно актуальним і важливим завданням, що постає перед науковою спільнотою нашої країни.

З урахуванням викладеного, можна виділити такі пріоритетні напрями правового забезпечення інформаційної безпеки України:

- удосконалення законодавства України у сфері забезпечення інформаційної безпеки з метою створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі;
- ухвалення нормативно-правових актів, що забезпечують реалізацію концепції електронного уряду, у тому числі надання державних послуг із використанням інформаційно-комунікаційних технологій, розвиток довіреного електронного документообігу на основі використання загальнодоступних інформаційно-телекомунікаційних мереж;
- законодавче закріплення переліку правопорушень та видів відповідальності в сфері інформаційної безпеки;
- вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва у зазначеній сфері.

Використана література

1. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н.Каразіна*. *Серія "ПРАВО"*. 2020. № 29. С. 281-288.

2. Бондар І.Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки.* 2014. № 1. С. 68-75.

3. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

4. Вайцеховська О.Р. Міжнародний фінансовий правопорядок: теоретичні засади та актуальні проблеми в умовах глобалізації: дис. …докт. юрид. наук. Харків, 2020. 472 с.

5. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах. *Вісник національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 32-46.

6. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. Київ: КНТ, 2006. 280 с.

7. Сенченко М.О. Запорука національної безпеки в умовах інформаційної війни. *Вісник книжкової палати*. 2014. № 6. С. 3-9.

8. Доктрина інформаційної безпеки України: Указ Президента України: від 25.02.17 р. № 47/2017. URL: //www.president.gov.ua

9. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. URL: http://journals.maup.com.ua/index.php/political/article/view/2295/2778.

10. Грабар Н.С. Зарубіжний досвід правового регулювання забезпечення інформаційної безпеки. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/12388/1/stGrabar.pdf

11. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

12. Конституція України: Закон України. URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр

13. Про національну безпеку України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355.

14. United Nations. A/RES/53/70 "Developments in the fi eld of information and telecommunications in the context of international security" Resolution Adopted By The General Assembly. 4 January 1999 URL: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_res_53_70.pdf

15. Фролова О.М. Роль ООН в системі міжнародної інформаційної безпеки. URL: http://journals.iir.kiev.ua/index. php/pol_n/article/viewFile/3468/3140

16. NATO Cooperative Cyber Defence Centre (CCDCOE). URL: https://www.cybersecurity intelligence.com/natocooperative-cyber-defence-centre-ccdcoe-395.html

17. Network and information security: proposal for a european policy approach. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN

18. Гассельбах К., Завгородня І. Європейський центр боротьби з кіберзлочинністю починає роботу. URL: http://p.dw.com/p/17HRW

21. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon5.rada.gov.ua/laws/show/96/2016

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~