УДК 342.951:323:004.056.5

# ІНФОРМАЦІЙНА БЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: СУЧАСНІСТЬ І ПЕРСПЕКТИВИ

**Євген КОБКО,**
кандидат юридичних наук, доцент,
доцент кафедри адміністративного права і процесу
Національної академії внутрішніх справ

**АНОТАЦІЯ**

У статті з позицій науки адміністративного права досліджено проблеми забезпечення інформаційної безпеки в системі національної безпеки. Наголошено, що у XXI ст. в системі національної безпеки інформаційна безпека посідає провідне місце. Акцентовано, що інформаційна безпека є комплексним утворенням з різнорівневими зв'язками та системою суб'єктів і має дворівневе значення: 1) національне; 2) міжнародне. Визначено, що інформаційну безпеку можна розглядати в таких аспектах: 1) самостійне суспільно-державне явище; 2) основа для розвитку політичного, соціального, економічного, культурного складників суспільства; 3) політична та економічна стабільність у державі є засобом (ресурсом) розвитку інформаційної системи суспільства. Наголошено, що створення сучасної системи цінностей (інформаційної культури) та інтеграція її в суспільство є фундаментом для забезпечення інформаційної безпеки людини й держави.

**Ключові слова:** національна безпека, інформаційна безпека, кібербезпека, національні інтереси, інформаційна безпека держави, суспільства й особи.

## INFORMATION SECURITY IN THE NATIONAL SECURITY SYSTEM: PRESENT STATE AND PERSPECTIVE

**Yevhen KOBKO,**
PhD in Law, Associate Professor,
Associate Professor of the Department of Administrative Law and Procedure
of the National Academy of Internal Affairs

**SUMMARY**

The paper analyses the problems of providing information security in the national security system from the standpoint of the science of administrative law. It is emphasised that in the 20th century information security occupies a leading position in the national security system. It is highlighted that information security is a complex formation with diverse links and a system of subjects and has two-level significance: 1) national; 2) international. It is determined that information security can be considered in the following aspects: 1) an independent social and state phenomenon; 2) the basis for the development of the political, social, economic, cultural components of society; 3) political and economic stability in the state acts as a means (resource) for the development of the information system of society. It was stressed that the creation of a modern system of values (information culture) and its integration into society will serve as the basis for ensuring information security of man and the state.

**Key words:** national security, information security, cybersecurity, national interests, information security of the state, society and man.

**Постановка проблеми.** Інтенсивність глобалізаційних процесів у світі, утвердження позицій транснаціональних корпорацій, їх політичних, економічних, інформаційних систем зумовлюють кожну державу світу, у тому числі й Україну, створювати власний інформаційний простір, який був би спроможний інтегруватися та взаємодіяти з інформаційними системами інших країн і міжнародними утвореннями, мати надійну систему захисту. Тому нині кожна країна світу одним зі своїх пріоритетних завдань установлює гарантування та забезпечення інформаційної безпеки особи, суспільства й держави.

**Актуальність теми** дослідження. Теоретична важливість і практичність теми не може викликати жодних сумнівів, проте все ж як однин із низки наявних аргументів варто зазначити, що воєнний конфлікт, який продовжується на частині території України, та анексія іншої її частини вимагають не лише розвивати національні збройні сили, а й потужно працювати в напрямі захисту приватної та державної й особливо воєнної інформації, що в умовах радикальних світових інформаційно-комунікаційних трансформацій стає все складніше. Так, державні програми, державна інформаційна політика загалом, системи захисту (у технічному аспекті), які ще не так давно характеризувалися як ефективні, нині вже є застарілими й у більшості випадків потребують не оновлення, а надійної заміни. Створення нових знань, упорядкування наявних сфер діяльності людини є найбільш результативним процесом в умовах взаємодії суспільства, держави та наукової сфери. Саме через такий підхід нове знання зможе отримати практичне застосування для покращення життєдіяльності суспільства. У зв'язку з цим питання інформаційної безпеки має отримати доктринальний супровід і стати фундаментом для захисту національних інтересів, зокрема, в інформаційній сфері, на міжнародній арені в умовах глобалізаційних викликів.

**Стан дослідження.** Розгляду питань інформаційної безпеки приділяли увагу в дослідженнях із позицій різних наук (філософії, соціології, історії, політології, управління, психології, юриспруденції тощо) Х. Андерсен, І. Арістова, В. Артемов, Є. Архипова, І. Бачило, З. Бжезинський, І. Березовська, К. Бєлякова, Л. Браун, В. Брижка, В. Гавловський, В. Горбуліна, Ю. Грицюк, В. Демиденко, О. Дзьобань, О. Довгань, В. Домарєв, Д. Домарєв, І. Забара, І. Залєвська, О. Золотар, І. Івченко, Н. Камінська, Р. Калюжний,

Л. Карвалікс, О. Кирилюк, В. Кір'ян, Г. Кіссінджер, Б. Кормич, Дж. Крік, В. Ліпкан, А. Марущак, В. Мунтіян, Л. Наливайко, М. Ніелс, Г. Новицький, А. Пазюк, В. Пилипчук, В. Пікард, В. Сідак, Є. Скулиша, І. Сопілко, О. Соснін, О. Степко, М. Стрельбицький, О. Тихомиров, Т. Ткачук, Т. Умесао, Ч. Флавін, Х. Френч, В. Харченко, В. Цимбалюк, М.-Дж. Шварц та ін. Виклики, які нині постали перед інформаційною безпекою України, мають усе більш динамічний характер, до того ж системно модифікуються. Тож питання інформаційної безпеки як складника національної безпеки стає ще актуальнішим, незважаючи на вже наявний внесок науковців і публічних інституцій у цьому напрямі.

Метою й завданням статті є дослідження сучасних проблем забезпечення інформаційної безпеки людини, суспільства та держави в системі національної безпеки й визначення подальших перспектив у цьому напрямі з позицій науки адміністративного права.

**Виклад основного матеріалу.** Відповідно до ст. 17 Конституції України, захист інформаційної безпеки нарівні із захистом суверенітету й територіальної цілісності України є провідною функцією держави і справою всього Українського народу [1]. Тому інформаційна безпека, безсумнівно, є одним із найважливіших складників національної безпеки України. Оскільки інформаційна сфера має своїм змістом знання про інші сфери життєдіяльності суспільства, вона водночас існує як самостійно, так і у взаємозв'язку з іншими сферами життєдіяльності суспільства, адже здійснює їх «інформаційне обслуговування» за допомогою інформації [2, с. 90].

Аналіз нормативних документів розвинутих демократичних країн з інформаційної безпеки, які прийняті ще в 90-х рр. XX ст., показав, що американські та європейські уряди вже тоді розуміли складність інформаційних систем, а з тим і складність забезпечення інформаційної безпеки [3, с. 134]. Україна в цьому напрямі активізувалася значно пізніше, оскільки в 90-х рр. XX ст., й навіть на початку 2000-х рр. наша держава та українське суспільство перебувало на початковому етапі інформатизації в широкому розумінні цього поняття. Так, більшість громадян і чиновників не могла навіть уявити існування інформаційних загроз і необхідності вироблення засобів їх подолання через інформаційно-комунікаційні технології.

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігається заподіяння шкоди через неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації [4]. Звісно, цей законодавчо передбачений перелік можливих загроз на практиці є значно ширшим і детальнішим, про що буде йтися далі.

Інформаційна безпека є важливим чинником з боку маніпуляторів, хто хоче так чи інакше захопити вплив над людиною, групою людей, корпорацією чи країною. Якщо раніше для того, щоб захистити країну, потрібна була сильна та численна армія з різними видами озброєння, то нині необхідно декілька висококваліфікованих спеціалістів, які вміють керувати інформацією, подати її так, як потрібно, спрямувати її в потрібне русло з тією чи іншою метою [5, с. 94]. Такими особами можуть бути спеціалісти в інформаційних технологіях, журналісти, які володіють на високому рівні своєю спеціальністю, та ін.

Інформаційна безпека посідає особливе місце в системі національної безпеки, тому загрози інформаційного характеру можуть спрямовуватись до будь-яких складників національної безпеки, однак їх негативний вплив завжди опосередковуватиметься завданням шкоди інформаційній безпеці держави [6, с. 162]. Відповідно, в умовах розвитку інформаційного суспільства інформаційна безпека виступає як: 1) самостійне суспільно-державне явище; 2) основа для розвитку політичного, соціального, економічного, культурного складників суспільства; 3) політична та економічна стабільність у державі є засобом (ресурсом) розвитку інформаційної системи суспільства, сприяє розвитку виготовлення ефективного інформаційного продукту, який першочергово зможе захистити інтереси власної країни, а також стати цікавим комерційним об'єктом для інших суб'єктів міжнародного права.

Важливо наголосити, що основна частина розробок у галузі інформаційної безпеки донедавна здійснювалась виключно в інтересах держави. Її історичне коріння сягає IV тис. до н. е., саме так історики датують першу згадку про засоби шифрування [7, с. 30]. Початок історії захисту інформації вчені пов'язують із появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю. Практично одночасно з появою писемності виникли перші методи захисту інформації – шифрування та приховування. Історія охорони й захисту інформації на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто [8; 9, с. 140].

В аспекті комплексного й усебічного розгляду проблематики відзначимо, що лише з 40-х рр. XX ст. у світі набув розвитку власне напрям інформаційної безпеки людини. Це питання почало формуватись не «згори» – від владних органів, а «знизу» – в контексті боротьби за реалізацію інформаційних прав людини, зокрема свободи слова, таємниці приватного життя тощо [10, с. 97]. Відповідно, інформаційну безпеку помилково розглядати виключно в контексті держави, як це можна спостерігати в різних авторських дослідженнях, хоча вже й значно рідше. Інформаційна безпека – багатофакторне явище, що передбачає захист держави та суспільства загалом, людини (об'єднань громадян) у певному секторі функціонування.

У 1946 р. Генеральна Асамблея Організації Об'єднаних Націй ухвалила одну зі своїх перших резолюцій, де зазначено, що свобода інформації є фундаментальним правом людини і критерієм для всіх свобод, яким присвячено Організацію Об'єднаних Націй [11, с. 19]. Тому в нинішніх умовах розвитку інформаційного суспільства, активних глобалізаційних процесів інформаційна безпека людини, що, по суті, є її природним правом, та інформаційна безпека держави є рівномірними, взаємопов'язаними та взаємозумовленими явищами. Розгляд проблематики інформаційної безпеки людини, суспільства й держави в системному взаємозв'язку уможливить створення ефективних засобів її забезпечення.

Зі зростанням попиту населення на інформацію держава повинна прораховувати виклики та проблеми, швидко проводити модернізацію в стратегічних сферах державного сектору. Отже, в сучасному суспільстві, яке здійснює модернізацію, виникає потреба переглянути наявні економічні, політичні, соціально-культурні концепції розвитку та інформувати суспільство про ці зміни. Водночас розвиток інформаційних технологій, що необхідні для накопичення й ефективного використання інформаційних ресурсів, стає стратегічним чинником забезпечення національної безпеки [3, с. 134]. Формування та розвиток інформаційної системи й інформаційно-комунікаційних технологій є чинником національної конкурентоспроможності тощо.

Інформаційно-комунікаційні технології є одним із найбільш важливих факторів стимулювання економічного зростання та розвитку громадянського суспільства, зайнятості населення, розширення конкуренції, як наслідок, сприяння подоланню «цифрового розриву». Проте саме рівень технологічного розвитку визначає не лише економічний потенціал країни та якість життя її громадян, а й роль і місце цієї країни в глобальному суспільстві, масштаби та перспективи її економічної й політичної інтеграції з усім світом [12]. Особлива роль мережі Інтернет у житті держави та суспільства відкриває нові можливості для формування соціально-економічного сектору, розвитку особистості й низки інших позитивних чинників. Але разом із тим виникають загрози різного рівня (від електронного пограбування громадян до злому державної інформаційної системи, що може вплинути на економіку всієї країни), яким далеко не завжди можна запобігти чи які швидко вирішити.

Донедавна питання захисту особистої інформації не викликало жодного зацікавлення з боку громадян, проте останніми роками воно становить безумовний інтерес, що пов'язано з різними чинниками, такими як розвиток інформаційно-комунікаційних технологій; бажання вплинути на людину через отримання незаконним шляхом її особистої інформації тощо. Однак більш негативні наслідки з'являються, коли такий вплив здійснюється на державних службовців, органи державної влади загалом, оскільки в такому випадку може бути порушено інтереси значно більшої групи осіб чи взагалі інтереси всієї країни (національні інтереси).

Активне використання в різноманітних сферах життєдіяльності людини й суспільства та все частіше й у науковому обігу інформаційно-комунікаційних технологій передбачає відповідні позитивні та негативні наслідки. Так, відбуваються системні зміни й доповнення до чинного законодавства, прийняття якісно нових нормативно-правових актів у цій сфері, розвиток відповідної міжнародно-правової бази, спрямовані на забезпечення розвитку інформаційного суспільства, національного та світового інформаційного простору. Водночас не завжди правове, інституційне, організаційне й ресурсне забезпечення інформаційного суспільства здатне гарантувати інформаційну безпеку людини, держави та суспільства, тим більше світової спільноти загалом. Кібератаки в різних куточках світу стають тому підтвердженням [13, с. 51]. Тож, незважаючи на всі позитивні аспекти розвитку інформаційно-комунікаційних технологій, варто констатувати, що паралельно із цим відбувається й розвиток кіберзлочинності, яка використовує у своїх протизаконних діях вразливі сторони інформаційних систем [14, с. 64]. Забезпечення доступності, цілісності й конфіденційності кіберпростору стало однією з глобальних проблем XXI ст., метою ефективного функціонування держави, економіки та суспільства загалом [5, с. 95].

Під впливом інформаційних атак можуть змінюватися світогляд і мораль як окремих осіб, так і суспільства загалом, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності й форм виявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і суперечать інтересам національної безпеки [15]. Низький рівень захищеності інформації викликає кібератаку з боку інших держав чи недержавних суб'єктів – організацій, приватних осіб (хакерів) та ін. Як наслідок, відбувається негативний вплив на політичну, соціальну, економічну системи держави, дезорієнтація громадян. Створення сучасної системи інформаційної безпеки є підґрунтям для забезпечення національних інтересів як в інформаційній сфері, так і в інших галузях життєдіяльності суспільства.

Наголосимо, що нині в Україні нормативно-правовим підґрунтям у напрямі забезпечення кібербезпеки є Конвенція про кіберзлочинність [16]; Закони України «Про національну безпеку України» [17]; «Про захист персональних даних» [18]; Кримінальний кодекс України [19]; Стратегія кібербезпеки України [20] і низка інших. Однак, як і майже будь-яка сфера, питання забезпечення кібербезпеки потребувало галузевого законодавчого акта. Тому в жовтні 2017 р. прийнято Закон України «Про основні засади забезпечення кібербезпеки України», який набрав чинності 9 травня 2018 р. [21]. Важливо наголосити, що каталізатором прийняття цього Закону стала атака вірусу на державні та приватні структури України (сайти органів публічної влад, енергетичні компанії, банки, аеропорт Харкова тощо), наприкінці червня 2017 р. До цього часу Закон перебував на розгляді Парламенту України з 2015 р. Хоча відомим фактом є те, що питання правового регулювання в кіберпросторі вимагають свого термінового вирішення.

Незважаючи на вказане, справедливо підкреслити, що можливості України з протидії загрозам в кіберпросторі перебувають на початковому етапі формування й усе ще не мають комплексного характеру, а Закон про кібербезпеку є лише одним із перших кроків у цьому напрямі [22]. Так, ще до прийняття цього документа громадськість, експерти висловлювали низку зауважень до Законопроекту.

Нині серед недоліків і прогалин Закону називають такі: за кібербезпеку в рамках своїх повноважень відповідальні міністерства, місцеві держадміністрації, органи місцевого самоврядування, правоохоронні органи, розвідка й контррозвідка, суб'єкти оперативно-розшукової діяльності тощо, проте не визначено єдиного органу, який здійснює оперативне командування всіма суб'єктами забезпечення кібербезпеки; надмірні повноваження Державної служби спеціального зв'язку та захисту інформації України з аудиту об'єктів критичної інфраструктури, що перебувають у приватній власності, тощо. До того ж фахівець з інтернет-безпеки Д. Снопченко вважає, що Закон досить узагальнений і до якихось безпосередніх дій не призведе. А ось закони й постанови, які будуть на його основі написані та реалізовані, мають бути більш конкретні. У свою чергу, І. Рудь зазначає, що, незважаючи на тривалі дискусії й побоювання певних експертів щодо можливості появи надмірного контролю від держави в кіберсфері, цей Закон дає змогу в перспективі перевести розвиток вітчизняного інформаційного простору на якісно новий рівень [23, с. 43; 24]. Отже, Закон України «Про основні засади забезпечення кібербезпеки України», з одного боку, закрив прогалину, що існувала у відповідній сфері, з іншого – з'явилася низка інших питань, що знов ж таки потребують вирішення.

Існують різні методи та способи забезпечення інформаційної безпеки. Завдання забезпечити інформаційну безпеку в країні означає задіяння всіх доступних методів і заходів задля захисту потреб суспільства, окремих особистостей і самої держави в інформації. Найважливіша вимога до обґрунтування способів, форм і механізмів їх реалізації полягає в абсолютному верховенстві права в будь-якій, зокрема політичній, діяльності. Кожний суб'єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, чітко уявляти наслідки своїх дій для інших суб'єктів і ступінь відповідальності в разі порушення їхніх життєво важливих інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється у формах інформаційного патронату й інформаційної кооперації,

у другому – інформаційного протиборства [25, с. 99–101]. Стрімкий розвиток інформаційного суспільства вимагає системного створення нових механізмів забезпечення інформаційної безпеки, що в сучасних умовах є складником національної безпеки кожної держави світу. Фундаментом такої безпеки є захист, цілісність і доступність інформації та інформаційних систем.

**Висновки.** Отже, ретроспективний розгляд, аналіз сучасного стану й визначення перспектив у напрямі забезпечення інформаційної безпеки з позицій адміністративно-правової науки надають підстави констатувати таке:

1. У XXI ст. в системі національної безпеки інформаційна безпека посідає провідне місце. Тривалий історичний період інформаційна безпека першочергово асоціювалася виключно з інтересами держави. Теорія інформаційної безпеки набула іншого змісту і трансформувалася під впливом розвитку інформаційно-комунікаційних технологій. Нині інформаційна безпека всередині країні розповсюджується в таких напрямах: держава, суспільство (або його частина, група людей) і людина. Окремим фундаментальним напрямом є міжнародна інформаційна безпека. Відповідно, інформаційна безпека має дворівневе значення: 1) національне; 2) міжнародне.

2. Інформаційна безпека є комплексним утворенням з різнорівневими зв'язками та системою суб'єктів. Інформаційну безпеку можна розглядати в таких аспектах: 1) самостійне суспільно-державне явище; 2) основа для розвитку політичного, соціального, економічного, культурного складників суспільства; 3) політична та економічна стабільність у державі є засобом (ресурсом) розвитку інформаційної системи суспільства. Загрози інформаційної безпеки є як зовнішніми, так і внутрішніми. Негативний вплив на інформаційну безпеку в більшості випадків становить загрозу для економічної, політичної (особливо в період виборчих процесів) систем суспільства. Лише нещодавно саме останньому напряму почали приділяти більшу увагу науковці та публічна влада (порівняно з питаннями інформаційної безпеки держави), що в тому числі пов'язано з прийняттям профільного законодавства.

3. Створення сучасної системи цінностей (інформаційної культури) та інтеграція її в суспільство стане фундаментом для забезпечення інформаційної безпеки людини й держави. Проте такий підхід ефективний лише в межах держави, оскільки, як відомо, загрози виникають і поза рамками її території. Інформаційна безпека включає два основні напрями: захист інформації (як державної, так і приватної) і захист від інформації (стосується переважно окремих громадян чи групи осіб). Нині пріоритетним завданням Української держави є вироблення стратегій і реалізація єдиної державної політики в цьому напрямі. Від ефективної державної інформаційної політики нині залежить не лише розвиток окремих сфер, а й рівень демократизації суспільства. Відсутність чітко сформульованої державної інформаційної політики та визначення реальних можливостей держави в цьому напрямі ускладнює захист інформаційних інтересів суспільства та сприяє інформаційним атакам від внутрішніх і зовнішніх агресорів.

4. Створення ефективних умов для забезпечення інформаційної безпеки людини потребує викорінення такого явища, як інформаційна дискримінація. Інформаційна дискримінація є багатовекторним явищем, що включає у свій зміст соціально-економічний (відсутність можливості в доступі до передових технологій з метою не лише задовольнити власні інтереси та потреби, а й забезпечити захист, отримати необхідну інформацію своєчасно) складник, що є найбільшою проблемою; віковий (пов'язано з тривалим вихованням у певних ідеологічних умовах, де відсутня мотивація до постійного руху в напрямі отримання нових знань, умінь, навичок, що відображається на частині нинішнього покоління, подекуди людей молодого віку. Це вимагає забезпечити можливості й постійно мотивувати людей до розвитку) складник; мовний (більшість інформаційних програм і контенту в Інтернеті англійською мовою) складник; фізичний (далеко не кожні сайти, програми налаштовані для людей, які мають вади слуху, зору тощо) складник і низку інших складників.

Подальше формування концептуального бачення науковцями питань правового регулювання у сфері інформаційної безпеки як складника національної безпеки, яке б передбачало збалансований підхід до інтересів особи, суспільства й держави, видається одним із першочергових завдань сучасної правової доктрини.

**Список використаної літератури:**

1. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141 (зі змінами, внесеними Законом України «Про внесення змін до Конституції України (щодо правосуддя)» від 2 червня 2016 року. *Відомості Верховної Ради України.* 2016. № 28. Ст. 532).

2. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право.* 2018. № 1. С. 89–103.

3. Еделєва М.А. Забезпечення інформаційної безпеки в контексті реалізації державної інформаційної політики. *Вісник Маріупольського державного університету. Серія «Історія. Політологія»*. 2017. Вип. 19. С. 133–141.

4. Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки: Закон України від 9 січня 2007 року № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

5. Любохинець Л.С., Поплавська О.В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. *Бізнес-навігатор.* 2017. Вип. 4-1. С. 93–97.

6. Цивілізаційний вибір України: парадигма осмислення і стратегія дії: національна доповідь / ред. кол.: С. Пирожков, О. Майборода, Ю. Шайгородський та ін. Київ: НАН України, 2016. 284 с.

7. Потий О. Криптография, прошлое и настоящее. *Служба безопасности*. 2001. № 2–3.

8. Організаційно-правові основи захисту інформації з обмеженим доступом: навчальний посібник / А.Б. Тоцький, О.І. Тимошенко, А.М. Гуз та ін. Київ: Європ. ун-т, 2006. 232 с.

9. Золотар О.О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право*. 2018. № 1. С. 139–148.

10. Кормич Б.Л. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ: Кондор, 2004. 384 с.

11. Свобода інформації: навч. посіб. для держ. служб. / пер. з англ. Р. Тополевського. Київ: Тютюкін, 2010. 128 с.

12. Про Рекомендації парламентських слухань на тему «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України»: Постанова Верховної Ради України. *Відомості Верховної Ради України.* 2016. № 17. Ст. 191.

13. Шемчук В.В. Принципи забезпечення інформаційної безпеки. *Наукові записки Інституту законодавства Верховної Ради України.* 2018. № 4. С. 50–56.

14. Залєвська І. Інформаційна безпека України в сучасних умовах: політичний аспект: дис. … канд. політ. наук. Одеса, 2012. 177 с.

15. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php/.

16. Конвенція про кіберзлочинність від 23 листопада 2001 р. *Відомості Верховної Ради України.* 2006. № 5–6. Ст. 71.

17. Про національну безпеку України: Закон України від 21 червня 2018 року. *Голос України.* 2018. № 122.

18. Про захист персональних даних: Закон України від 1 червня 2010 року. *Відомості Верховної Ради України.* 2010. № 34. Ст. 48.

19. Кримінальний кодекс України від 4 квітня 2001 року (зі змінами і допов.*). Відомості Верховної Ради України.* 2001. № 25. Ст. 131.

20. Стратегія кібербезпеки України: Указ Президента України від 15 березня 2016 року. *Урядовий кур'єр*. 2016. № 52.

21. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

22. Литвин А. Що дасть Україні новий закон про кібербезпеку. URL: https://biz.censor.net.ua/m3069149.

23. Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору. *Україна: події, факти, коментарі*. 2017. № 19. С. 42–48.

24. Янковський О. Закон «Про кібербезпеку» як спроба тотального контролю. URL: https://www.pravda.com.ua/columns/2017/06/10/7146438/.

25. Лук'янова В., Лаутар А. Інформаційна безпека в умовах розвитку інформаційних систем. *Вісник Хмельницького національного університету. Серія «Економічні науки».* 2013. № 2. Т. 3. С. 97–101.

ІНФОРМАЦІЯ ПРО АВТОРА

**Кобко Євген Васильович** – кандидат юридичних наук, доцент, доцент кафедри адміністративного права і процесу Національної академії внутрішніх справ

INFORMATION ABOUT THE AUTHOR

**Kobko Yevhen Vasylovych** – PhD in Law, Associate Professor, Associate Professor of the Department of Administrative Law and Procedure of the National Academy of Internal Affairs

*olga-tregubenko@ukr.net*