11. Про Рахункову палату : Закон України від 02.07.2015 № 576-VIII (із змінами і доповненнями. URL: http://zakon3.rada.gov.ua

12. Методичні рекомендації з проведення Рахунковою палатою фінансового аудиту : затверджені рішенням Рахункової палати від 22.09.2015 № 5-5. URL: http://consultant.parus.ua

13. Методичні рекомендації щодо здійснення Рахунковою палатою контролю у сфері державних закупівель : затверджені постановою Колегії Рахункової палати від 21.07.2014 № 15-5. URL: www.ac-rada.gov.ua/doccatalog/document/.../Zvit_11-6.pdf

14. Рекомендації з управління і контролю якості контрольних заходів, що проводяться Рахунковою палатою : затверджені рішенням Рахункової палати від 10.1.2015 № 8-5. URL: http://zakon3.rada.gov.ua

15. Положення про Державну аудиторську службу України : затв. постановою Кабінету Міністрів України від 3 лютого 2016 р. № 43. URL: http://zakon3.rada.gov.ua

16. Про затвердження Порядку оформлення протоколів про адміністративні правопорушення та внесення приписів Національним агентством з питань запобігання корупції : рішення Національного агентства з питань запобігання корупції від 09.06.2016 № 5 (із змінами і доповненнями). URL: http://zakon3.rada.gov.ua

17. Про основні засади здійснення державного фінансового контролю в Україні : Закон України від 26.01.1993 № 2939-XII (із змінами і доповненнями). URL: http://zakon3.rada.gov.ua

18. Назар Ю.С., Проць І.М. Суб'єкти застосування заходів адміністративної та фінансово-правової відповідальності за порушення бюджетного законодавства. *Науковий вісник Львівського державного університету внутрішніх справ.* 2016. № 4. С. 222–234.

* ***Мороз Євген Степанович – аспірант Університету сучасних знань.***

Стаття надійшла до редакції 6 серпня 2018 р.

УДК 340.1; 342.7

Віктор Шемчук *

ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті розкрито принципи правового регулювання і забезпечення інформаційної безпеки, засади розвитку інформаційного суспільства, національного інформаційного простору. Приділено увагу відповідності цих основоположних засад існуючим нормам і принципам міжнародно-правового регулювання у сфері інформаційної безпеки тощо.

***Ключові слова**: інформаційне суспільство, інформаційно-комунікаційні технології, інформаційна безпека, принципи, засади, правова основа, забезпечення.*

Шемчук В. В. Принципы обеспечения информационной безопасности.

В статье рассмотрены принципы правового регулирования и обеспечения информационной безопасности, основы развития информационного общества, национального информационного пространства. Уделено внимание соответствию данных фундаментальных принципов существующим нормам и принципам международно-правового регулирования в этой сфере и т.д.

***Ключевые слова**: информационное общество, информационно-коммуникационные технологии, информационная безопасность, принципы, правовая основа, обеспечение.*

Shemchuk V. V. The principles of ensuring of the information security.

The article reveals the principles of legal regulation of and ensuring of information security, fundamentals the development of the information society, the national information space. Attention of compliance data of fundamental principles of the existing norms and principles of international legal regulation in this sphere, etc.

Keywords: information societies, information and communications technology, information security, principles, basis, legal foundation, ensuring.

Актуальність дослідження. Активне використання у різноманітних сферах життєдіяльності людини й суспільства та останнім часом і в науковому обігу інформаційно-комунікаційних технологій передбачає відповідні позитивні й негативні наслідки. Так, відбуваються системні зміни та доповнення до чинного законодавства, прийняття якісно нових законів та інших нормативно-правових актів України 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 та ресурсне забезпечення інформаційного суспільства здатне гарантувати інформаційну безпеку людини, держави та суспільства, тим паче світової спільноти загалом. Кібератаки у різних куточках світу лише це підтверджують.

Аналіз останніх досліджень та публікацій. Значна увагу приділялася й продовжує приділятися вивченню таких категорій, як «інформація», «інформаційно-комунікаційні технології», «інформаційне суспільство», «інформаційний простір», «інформаційна цивілізація», «інформаційна безпека», «державна інформаційна політика» тощо. Прикметно, що така увага спостерігається у різних галузях сучасної науки – технічній, природничій, суспільних тощо. Представники сучасної юридичної науки також не стоять осторонь процесів в інформаційній сфері. Тому слід виокремити певний науковий інтерес до теоретичних, адміністративно-правових, філософсько-правових, кримінально-правових, міжнародно-правових та інших аспектів становлення й розвитку інформаційного суспільства.

У цьому контексті доцільно відзначити праці таких учених, як В. Гавловський, І. Забара, В. Демиденко, О. Дзьобань, Р. Калюжний, Н. Камінська, О. Кирилюк, В. Кір'ян, А. Марущак, І. Мищак, О. Олійник, А. Пазюк, І. Сопілко, В. Цимбалюк, Л. Карвалікс, Б. Кормич, К. Курокави, В. Пилипчук, В. Пікард, О. Тихомиров, Т. Умесао та ін. При цьому іноді до певної міри відбувається ототожнення інформаційного суспільства та інформаційного простору, інформаційної цивілізації, а також інформаційної безпеки, кібербезпеки й національної безпеки, принципів регулювання та принципів забезпечення інформаційної безпеки тощо.

Таким чином, *мету статті* становить дослідження природи принципів забезпечення інформаційної безпеки, особливостей їх законодавчого закріплення та відповідності існуючим міжнародно-правовим стандартам.

Виклад основного матеріалу дослідження. Якщо природа і сутність інформаційного суспільства як узагальненої категорії суспільних трансформацій вивчається в юридичній та інших науках протягом тривалого часу, то категорія «інформаційна безпека» потребує ґрунтовного дослідження.

Згідно з положеннями п. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» 2007 р. «інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [1].

Залежно від об'єкту впливу інформаційну безпеку поділяють на:

- інформаційну безпеку особи;
- інформаційну безпеку суспільства;
- інформаційну безпеку держави [2].

Інформаційну безпеку особи важливо розуміти як стан захищеності безпосередньо здоров'я людини в контексті наслідків негативного впливу інформації, у тому випадку, коли остання може мати деструктивний вплив на сприйняття дійсності в результаті зловживань. Інформаційна безпека суспільства знаходить своє відображення переважно в конституційних положеннях. Так, ст. 17 Конституції України, визначає інформаційну безпеку як одну з найважливіших функцій держави та покладає обов'язок її захисту на весь

народ України; ч. 2 ст. 34 Конституції України зазначає, що «кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір» [3]. Згадане положення в цілому відповідає п. 2 ст. 19 Міжнародного пакту про громадянські та політичні права ООН, а також деталізується Конституційним Судом України у рішенні від 20.01.2012 р. № 2-рп/2012 [4].

Інформаційна безпека держави розглядається з точки зору наданих відповідним суб'єктам державної влади, необхідної для здійснення законом передбаченої діяльності, компетенції. Зазначений вид безпеки кореспондується здебільшого з поняттям національної безпеки, яке відображалося у ст. 1 Закону України «Про основи національної безпеки України» 2003 р. та означає «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у відповідних сферах» [5].

Наразі у ст. 3 нового Закону України «Про національну безпеку України» 2018 р. закріплено, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. Загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки й оборони, які схвалюються Радою національної безпеки і оборони України та затверджуються указами Президента України [6].

Виходячи з мети нашого дослідження, змушені акцентувати увагу насамперед на основоположних засадах, певних концептуальних ідеях, що становлять основу регулювання й забезпечення інформаційної безпеки на цьому етапі.

Не дивлячись на те, що чітко на законодавчому рівні такі принципи не регламентовані, ґрунтовне вивчення національного законодавства дозволяє підкреслити таке.

По-перше, у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» 2007 р. є розділи «Законодавче забезпечення розвитку інформаційного суспільства» та «Національна політика розвитку інформаційного суспільства в Україні», де зазначено, що при створенні інформаційного законодавства слід керуватися загальними принципами Конституції України, а також базуватися на принципах свободи створення, отримання, використання та розповсюдження інформації; об'єктивності, достовірності, повноти і точності інформації; гармонізації інтересів людини, суспільства та держави в інформаційній діяльності; обов'язковості публікації інформації, яка має важливе суспільне значення; обмеження доступу до інформації виключно на підставі закону; мінімізації негативного інформаційного впливу та негативних наслідків функціонування ІКТ; недопущення незаконного розповсюдження, використання і порушення цілісності інформації; гармонізації інформаційного законодавства та всієї системи вітчизняного законодавства. Розділ «Організаційно-правові основи розвитку інформаційного суспільства в Україні» згаданого закону передбачає, що організаційно-правові основи розвитку інформаційного суспільства в Україні включають: інституційне, організаційне та ресурсне забезпечення; відповідні об'єднання громадян; механізми інтеграції України у світовий інформаційний простір та механізми реалізації Основних засад розвитку інформаційного суспільства в Україні на 2007-2015 роки [1].

По-друге, у Стратегії розвитку інформаційного суспільства в Україні, затвердженій Розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р для розвитку інформаційного суспільства передбачено застосовувати принципи:

- рівноправного партнерства державних органів, громадян і бізнесу;
- прозорості та відкритості діяльності державних органів;
- гарантованості права на інформацію, вільного отримання та поширення інформації, крім обмежень, установлених законом;
- свободи вираження поглядів і переконань;

- правомірності одержання, використання, поширення, зберігання та захисту інформації;
- інформаційної безпеки;
- постійного навчання;
- підконтрольності та підзвітності державних органів громадськості;
- сприяння пріоритетному розвитку інформаційно-комунікаційних технологій;
- чіткого розмежування повноважень і скоординованої взаємодії державних органів;
- гарантованості повного ресурсного забезпечення національних програм та проектів розвитку інформаційного суспільства [7].

По-третє, Закон України «Про основні засади забезпечення кібербезпеки України» закріпив положення, за яким застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень здійснюються з додержанням принципів:

1) мінімально необхідного регулювання;

2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

6) недискримінації;

7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури. Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань Закону [8].

По-четверте, Законом України «Про національну безпеку України» встановлено такі основні принципи, що визначають порядок формування державної політики у сферах національної безпеки і оборони:

1) верховенство права, підзвітність, законність, прозорість та дотримання засад демократичного цивільного контролю за функціонуванням сектору безпеки і оборони та застосуванням сили;

2) дотримання норм міжнародного права, участь в інтересах України у міжнародних зусиллях з підтримання миру і безпеки, міждержавних системах та механізмах міжнародної колективної безпеки;

3) розвиток сектору безпеки і оборони як основного інструменту реалізації державної політики у сферах національної безпеки і оборони [6].

Можна зустріти в літературі й інші дещо дискусійні підходи до визначення основних принципів інформаційної безпеки (на прикладі відкритих систем). Йдеться про: 1) забезпечення інформаційної безпеки виконується відповідно до політики управління інформаційними ризиками; 2) архітектура системи управління інформаційними ризиками забезпечує оптимальний (раціональний) баланс витрат на управління інформаційними ризиками і загального збитку від інформаційних ризиків; 3) система управління інформаційними ризиками є централізованою і реалізує єдину політику управління; 4) безпека інформації досягається за рахунок комплексного використання нормативних, економічних та організаційних заходів, технічних, програмних і криптографічних засобів; 5) система управління повинна бути багаторівневою і рівно захищеною у всіх ланках; 6) повинна бути забезпечена безперервність функціонування на всіх життєвих циклах системи; 7) повинно бути забезпечено розмежування та обмеження доступу персоналу до інформації; 8) система повинна бути здатна до розвитку й адаптації до зміни умов

функціонування; 9) наявність системи безперервного моніторингу за виконанням **усім** персоналом встановлених правил роботи в інформаційній системі; 10) моніторинг і аудит ефективності системи і своєчасна її модернізація [9].

Не дивлячись на важливі акценти, сформульовані вище, дозволимо собі не погодитися повною мірою з такими основними науково-практичними принципами забезпечення інформаційної безпеки, це швидше принципи протидії загрозам безпеки та побудови систем управління інформаційними ризиками, інформаційної безпеки у вузькому розумінні.

На нашу думку, система принципів інформаційної безпеки має формуватися й розвиватися на основі ширшого підходу, включаючи співвідношення національних та наднаціональних інтересів в інформаційному просторі, врахування об'єктивних умов чи основ існування інформаційного суспільства (організаційних, економічних; технологічних; правових та ін.).

Тому можна погодитися з такими підходами до визначення принципів інформаційної безпеки [10–19]. Так, Б. Кормич пропонує для визначення принципів забезпечення інформаційної безпеки два комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їх нормативно-правову базу, а саме: це комплекс питань, пов'язаних з інформаційною безпекою людини і суспільства, яка, в першу чергу, вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення; це комплекс питань, пов'язаних з інформаційною безпекою держави, які, навпаки, пов'язані із застосуванням обмежень, заборон, жорсткою регламентацією певних типів відносин в інформаційній сфері і невід'ємним елементом яких є сила державного примусу [12, с. 117].

Ю. Уфімцев, В. Буянов, Е. Єрофеєв важливими принципами визначають: законність заходів із виявлення й запобігання правопорушенням в інформаційній сфері; безперервність реалізації і вдосконалення засобів і методів контролю та захисту інформаційних систем; економічна доцільність, тобто співставлення можливих збитків і витрат на забезпечення безпеки інформації; комплексність використання всього арсеналу засобів захисту на всіх етапах інформаційного процесу [13, с. 53].

А. Стрельцов принципи діяльності із забезпечення інформаційної безпеки розділяє на загальні (гуманізм, соціальну справедливість, об'єктивність, конкретність, ефективність, опора на підтримку й довіру народу, поєднання гласності та професійної таємниці, законність і конституційність) та особливі (насамперед, принцип глобальності та ін.) [14, с. 129–131].

А. Логунов та О. Олійник при визначенні принципів забезпечення інформаційної безпеки виходять з основних принципів міжнародного права, які володіють вищою імперативною юридичною силою. Але виникає питання: чи всі з перелічених таких принципів стосуються сфери інформаційної безпеки?

Загалом поділяємо підхід, відповідно до якого принципи забезпечення інформаційної безпеки включають:

- пріоритет прав, свобод і законних інтересів людини і громадянина;
- верховенство права, рівність усіх суб'єктів правовідносин перед законом;
- відповідальність держави перед людиною за свою діяльність;
- комплексний підхід до вирішення завдань забезпечення інформаційної безпеки;
- єдність і взаємозв'язок напрямів забезпечення інформаційної безпеки;
- розмежування сфер відповідальності й повноважень державних органів і органів місцевого самоврядування з питань забезпечення інформаційної безпеки;
- участь у міжнародних і регіональних системах інформаційної безпеки;
- оперативність, своєчасність, превентивність й адекватність заходів щодо запобігання та захисту від зовнішніх інформаційних загроз і нейтралізації джерел внутрішніх інформаційних загроз [19].

Разом із тим пропонуємо додати низку інших принципів. Наприклад, принципи:

- пріоритету договірних (мирних) засобів у вирішенні інформаційних конфліктів;
- взаємодії державних і недержавних систем інформаційної безпеки;

- громадського контролю за діяльністю органів державної влади, що входять до системи забезпечення інформаційної безпеки України;

- презумпції нетаємності інформації, враховуючи її різновиди конфіденційного, публічного та іншого характеру;

- неперервного захисту, мобільності й динамічності системи інформаційної безпеки, різноманітності захисних засобів і способів;

- адекватності заходів захисту національних інтересів України в інформаційній сфері реальним та потенційним загрозам;

- економічної ефективності;

- створення єдиного цілісного механізму забезпечення національної інформаційної безпеки.

Висновки. Наведені принципи забезпечення інформаційної безпеки є основоположними і вихідними засадами створення, функціонування й розвитку системи інформаційної безпеки у контексті цілісної системи національної безпеки, а також системи міжнародної колективної безпеки. Підкреслимо, що використання інформації, інформаційно-комунікаційних технологій як засобів досягнення мети, що виходить за рамки національної безпеки, потребує застосування дієвих механізмів протидії та встановлення відповідальності за заподіяні збитки в інформаційній сфері. Потребують подальшого вивчення концептуальні науково обґрунтовані взаємоузгоджені принципи, прийоми і засоби, спрямовані на досягнення функціональної рівноваги та забезпечення реально діючої системи інформаційної безпеки людини, держави, суспільства і світової спільноти загалом.

Список використаних джерел:

1. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки Закон України від 09.01.2007 р. № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102. URL: http://zakon2.rada.gov.ua/laws/show/537-16

2. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. № 5. С. 122– 134.

3. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. *Відомості Верховної Ради України*. 1996. № 30. С. 141.

4. Міжнародний пакт про громадянські та політичні права від 16.12.1966 р.. URL: http://zakon5.rada.gov.ua/laws/show/995_043

5. Про основи національної безпеки України: Закон України № 964-IV від 19.06.2003 р. URL: http://zakon3.rada.gov.ua/laws/show/964-15

6. Про національну безпеку України: Закон України № 2469-VIII від 21.06.2018 р. URL: http://zakon2.rada.gov.ua/laws/show/2469-19/page

7. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінет Міністрів України від 15 травня 2013 р. № 386-р. URL: http://zakon5.rada.gov.ua/laws/show/386-2013-р

8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Офіційний вісник України*. 2017. № 91. Ст. 2765.

9. Інформатика для економістів: / під ред. В. П. Полякова. URL: https://stud.com.ua/53288/informatika/informatika_dlya_ekonomistiv

10. Гафнер В.В. Информационная безопасность. URL: http://информационная-безопасность.гафнер.рф/chitat-posobie/glava-1/1-1-ponyatie-informacii-i-informacionnoy-bezopasnosti/principy-obespecheniya-informacionnoy-bezopasnosti/

11. Мамедова К.А. Основные принципы обеспечения информационной безопасности страны. URL: https://cyberleninka.ru/article/n/osnovnye-printsipy-obespecheniya-informatsionnoy-bezopasnosti-strany

12. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посіб. К. : Кондор, 2008. 382 с.

13. Методика информационной безопасности / Ю. С. Уфимцев, В. П. Буянов, Е. А. Ерофеев и др. М. : Экзамен, 2004. 544 с.

14. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / под ред.: В. А. Садовничего и В. П. Шерстюка. М. : МЦНМО, 2002. С. 153–168.

15. Логунов А.Б. Региональная и национальная безопасность: учеб. пос. М. : Вузовский учебник, 2009. 432 с.

16. Демиденко В.О. Принципи застосування органами місцевого самоврядування законодавства України в сфері кібербезпеки. *Юридичний часопис НАВС*. 2018. № 1.

17. Камінська Н.В. Проблеми імплементації міжнародно-правових стандартів у сфері кібербезпеки. Розвиток науки і практики міжнародного права: матеріали міжнар. науково-практ. конфер., присвяченої 25-річчю УАМП. К., 2018.

18. Мищак І.М. Досвід оперативно-організаційної та методичної роботи щодо інформаційного забезпечення управлінських рішень. *Наукові праці Національної бібліотеки України ім. В. І. Вернадського*. Вип. 14 / НАН України. Нац. б-ка України ім. В. І. Вернадського. АБУ; Ред. кол.: О.С.Онищенко (гол.) та ін. К., 2005. С. 67–74.

19. Олійник О.В. Принципи забезпечення інформаційної безпеки України. *Юридичний вісник*. *Повітряне і космічне право*. 2016. № 4. С. 72–78.

* ***Шемчук Віктор Вікторович – кандидат юридичних наук, заступник Голови Кваліфікаційно-дисциплінарної комісії прокурорів***.

Стаття надійшла до редакції 1 серпня 2018 р.