ДОКТРИНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ЗАВДАННЯ, ПРИНЦИПИ РЕАЛІЗАЦІЇ

Коминар Назар Михайлович - здобувач кафедри адміністративного права і процесу, фінансового права, інформаційного права юридичного факультету Приватного вищого навчального закладу «Львівський університет бізнесу та права» (Україна)

УДК 342.127

В статті досліджено завдання та принципи реалізації Доктрини інформаційної безпеки України. Вказано, що як інструмент державного впливу на процеси в сфері забезпечення інформаційної безпеки слід більш активно використовувати взаємодію суб'єктів забезпечення інформаційної безпеки, що становить відкриту систему дворівневої конструкції з централізовано-сегментарним поділом владної компетенції між її основними елементами – суб'єктами забезпечення інформаційної безпеки, визначених Доктриною інформаційної безпеки України.

Ключові слова: інформація, інформаційна безпека, Доктрина інформаційної безпеки, суб'єкти забезпечення інформаційної безпеки.

В статье исследованы задачи и принципы реализации Доктрины информационной безопасности Украины. Указано, что как инструмент государственного влияния на процессы в сфере обеспечения информационной безопасности следует более активно использовать взаимодействие субъектов обеспечения информационной безопасности, которое составляет открытую систему двухуровневой конструкции с централизованно-сегментарным разделением властной компетенции между ее основными элементами – субъектами обеспечения информационной безопасности, определенных Доктриной информационной безопасности Украины.

Ключевые слова: информация, информационная безопасность, Доктрина информационной безопасности, субъекты обеспечения информационной безопасности.

The article deals with the tasks and principles of the implementation of the Doctrine of Information Security of Ukraine. It is specified that as a tool of state influence on processes in the field of information security should be more actively use the interaction of information security actors, which is an open system of two-tier design with a centralized-segmental division of power between its main elements – the subjects of information security, defined by the Doctrine of Information Security of Ukraine.

Key words: information, information security, Doctrine of information security, subjects of providing information security.

Постановка проблеми. Сьогодні, в епоху активної побудови інформаційного суспільства, майже усі держави починають замислюватися над такою проблемою, як «інформаційна безпека». Враховуючи інтенсивні інформаційні характеристики сучасного суспільства (наприклад, Інтернет), не варто дивуватися, що інформаційна безпека є зростаючим пріоритетом для більшості держав. Така проблема торкнулась усіх сфер життєдіяльності суспільства, посягнувши на приватність людини, і тим самим завдаючи шкоди її правам і свободам.

Отже, нова ера комп'ютерної інформації змінила спосіб життя людини і діяльності державних інституцій, і те, як їм потрібно відноситись до інформаційної безпеки. Насправді, інформаційна безпека стала доволі важливою для сучасного суспільства, що зумовлено багатьма чинниками. Для України особливого значення інформаційна безпека набула в контексті «гібридної» війни, яка проводиться стосовно нашої держави Російською Федерацією і супроводжується масштабним використанням інформаційної зброї та іншими загрозами.

Саме тому ця тематика потребує прискіпливої уваги з боку науковців, практиків, а також органів державної влади, – в контексті побудови ефективного законодавства, яке регулює інформаційні відносини загалом, та питання інформаційної безпеки зокрема.

Аналіз дослідження проблеми. У вітчизняній науковій думці існує доволі значна кількість праць, присвячених окремим питанням забезпечення інформаційної безпеки, з-поміж яких вагоме місце займають роботи І. Арістової, О. Баранова, Д. Беззубова, К. Бєлякова, В. Гавловського, М. Гуцалюка, І. Жиляєва, С. Єсімова, Р. Калюжного, О. Копана, А. Марущака, А. Новицького, Н. Новицької, В. Речицького, Р. Романова, А. Семенченко, О. Фролової, В. Фурашева, В. Цимбалюка, В. Хахановського, Л. Чистоклетова, М. Швеця, А. Яременко та ін.

Метою цієї публікації є аналіз Доктрини інформаційної безпеки України, яка в умовах розвитку інформаційного суспільства і агресії Російської Федерації є одним з основних нормативно-правових актів, спрямованих на забезпечення інформаційної безпеки держави та запобігання впливу особливого виду загроз, які виступають у формі цілеспрямованої або стихійної діяльності в інформаційному середовищі.

Виклад основного матеріалу. Доводиться констатувати, що інтеграція в міжнародний інформаційний простір, створення основ інформаційного суспільства, що проводиться в нашій державі, мають і позитивні, і негативні наслідки, що зумовлює потребу створення комплексної дієвої системи забезпечення інформаційної безпеки, яка є невід'ємною складовою національної безпеки України.

Відомий український вчений О.А. Баранов зазначає, що безпека – атрибутивний стан будь-якої системи. На всі без винятку системи впливають зовнішні та внутрішні (внутрішньосистемні) дії. Серед усього спектра дій є такі, що спричинюють зниження якості функціонування систем. Це, як правило, призводить до певної шкоди, а в деяких випадках і до загибелі системи [1].

Водночас, слід наголосити, що інформаційна безпека в загальній системі національної безпеки України посідає особливе місце, адже інформація в сучасному світі, зазнаючи постійних якісних і кількісних змін, є найцінішим глобальним ресурсом, а інформаційні відносини є невід'ємною складовою будь-яких процесів у державі. Однак, сьогодення яскраво доводить факт постійного зростання уразливості інформаційного суспільства від потенційних загроз, з-поміж яких, зокрема: недостовірність інформації, несвоєчасне її надходження, найрізноманітніші правопорушення, що вчиняються в інформаційній сфері. Виходячи з того, що посягання на інформаційну сферу можуть завдати значної шкоди життєво важливим інтересам держави, забезпечення інформаційної безпеки є одним із пріоритетних напрямів державної політики України.

Правову основу інформаційної безпеки України становить низка законодавчих актів, з-поміж яких: Конституція України, Закони України: «Про національну безпеку України», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Раду Національної безпеки і оборони України», «Про інформацію», «Про захист суспільної моралі» [2–8] та інші закони, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти.

Особливе місце в системі законодавства щодо забезпечення інформаційної безпеки відведено Доктрині інформаційної безпеки

України, яка затверджена Указом Президента України від 25 лютого 2017 року № 47 [9].

У ній зазначається, що застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація 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 [9].

Доктрина інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Метою цієї Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [9].

Слід підкреслити, що в Доктрині інформаційної безпеки України також визначено пріоритети державної політики в інформаційній сфері. Такі пріоритети мають бути щодо:

– забезпечення інформаційної безпеки;

– забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію;

– відкритості та прозорості держави перед громадянами;

– формування позитивного міжнародного іміджу України [9].

Отже, основними напрямами забезпечення інформаційної безпеки є ті, що найтісніше пов'язані з людиною, суспільством і державою. Саме захист їхніх інтересів, прав, свобод щодо правовідносин в інформаційній сфері потребує особливої уваги, з метою своєчасного визначення існування потенційних загроз.

Якщо ж аналізувати детальніше Доктрину інформаційної безпеки України, в якій під інформаційною безпекою України розуміється стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства та держави, то можна зробити висновок, що основним вектором політики держави щодо забезпечення інформаційної безпеки є дотримання конституційних прав і свобод людини в інформаційній сфері.

На наш погляд, необхідно враховувати і той фактор, що з моменту прийняття основоположних нормативних актів у сфері забезпечення безпеки: Стратегії національної безпеки України (2015 рік), Стратегію кібербезпеки України (2016 рік) і Доктрини інформаційної безпеки України (2017 рік) минув певний проміжок часу [10, с. 3-4]. Для оцінки загроз інформаційній безпеці у світовій практиці використовують спеціальну систему моніторингу, яка може ефективно працювати, застосовуючи відповідні відправні показники системи індикаторів, які необхідно закріпити у законодавчому порядку або на рівні постанови Кабінету Міністрів України, що передбачено Указом Президента України від 26.05.2015 № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», так як індикатори за зазначеним напрямом не включено до Вагових коефіцієнтів елементів інтегрального індексу національної безпеки, як це пропонує представник Національний інститут стратегічних досліджень С. Л. Гнатюк [11, с. 95-101]. У зв'язку з цим потребують конкретизації: загрози інформаційній безпеці, система суб'єктів, які в комплексі забезпечують інформаційну безпеку.

Доктрини в сфері інформаційної безпеки, що реалізуються державою, виступають засобами рішення, перш за все, політичних, а не правових задач, що обумовлюється не вадами проведеної політики, а об'єктивно існуючими закономірностями та тенденціями розвитку права.

Доктрина інформаційної безпеки України визначає національні інтереси в інформаційній сфері: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів; життєво важливі інтереси суспільства і держави [9]. Зміни, що відбуваються в сфері інформаційної безпеки особи, свідчать про те, що вибір реалізованих доктрин не є довільним ні з точки зору її цільової спрямованості, ні з точки зору засобів, використовуваних для її реалізації. Сфера інформаційної безпеки особи є відображенням сутнісних характеристик права. У зв'язку з цим закономірним виявляється те, що цільову спрямованість визначає гуманізація, базова для сфери інформаційної безпеки особи, що характеризує змістовними змінами, які відбуваються в перш за все в європейському праві. Юридизації, яка виступає тенденцією розвитку форм інформаційного права, визначає засоби, за допомогою яких відбувається здійснення гуманізації інформаційної безпеки особи.

Реалізація Доктрини інформаційної безпеки України в контексті гуманізації не може бути забезпечена в умовах подальшої формалізації діяльності ні за допомогою перебудови системи суб'єктів, що реалізують інформаційну політику і забезпечують інформаційну безпеку, ні за допомогою зміни процесуального законодавства, ні за допомогою створення нових, додаткових гарантій забезпечення та захисту прав людини в сфері правосуддя, без зміни нормативно-правової бази технічної складової. Указаний підхід обґрунтовано у аналітичній записці Національного інституту стратегічних досліджень при Президенті України «Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України» (2018 р.) [12].

У контексті реалізації Доктрини інформаційної безпеки стратегічні завдання побудови інформаційного суспільства мають включати в себе:

1. Реалізацію системи заходів щодо створення адекватного нормативно-правового, нормативно-технічного та інституційного забезпечення розвитку інформаційного суспільства із урахуванням світового досвіду.

2. Створення в індустрії інформаційно-комунікаційних технологій (ІКТ) конкурентного середовища із прозорими правилами гри і гарантіями захисту прав інвесторів, що необхідно для залучення інвестицій (з боку як іноземних, так і українських інвесторів).

3. Прискорений розвиток інформаційно-комунікаційної інфраструктури країни шляхом створення належних умов для залучення значного обсягу інвестицій як з боку підприємств індустрії ІКТ, так і з боку споживачів продукції та послуг ІКТ – населення, підприємств, установ та організацій. Зниження собівартості телекомунікацій та доведення цін і тарифів на користування інформаційно-комунікаційною інфраструктурою до рівня європейських країн.

4. Поширення можливостей доступу громадян до інформаційних технологій, Інтернету та інформаційних ресурсів з метою освіти, навчання, спілкування із державними органами у рамках «електронного урядування», розвитку незалежних мас-медіа, створення засад громадянського суспільства. Забезпечення рівних можливостей доступу до інформації, подолання соціальних та регіональних форм інформаційної нерівності. Створення всеукраїнської мережі пунктів колективного доступу (ПКД) населення до ІКТ на основі співпраці між державою та підприємцями, у тому числі малим бізнесом (створення приватних ПКД в комп'ютерних клубах, школах тощо).

5. Створення венчурної індустрії та технологічних кластерів економіки знань (експортно-орієнтована індустрія розробки програмного забезпечення та інші) з метою реалізації інтелектуального та науково-технічного потенціалу України та зайняття нею гідного місця у міжнародному розподілі праці, розвитку освіти, запобігання «відтоку мізків», збільшення валютних надходжень.

6. Вдосконалення захисту інтелектуальної власності на програмне забезпечення та бази даних задля підвищення інвестиційної привабливості індустрії ІКТ.

7. Впровадження концепції «електронного урядування» (надання урядових послуг з використанням ІКТ) з метою підвищення ефективності обслуговування органами державної влади та місцевого самоврядування населення та бізнесу, зменшення корупційного фактору, посилення зв'язку між державою і громадянами, покращання іміджу державних органів серед громадян, створення засад громадянського суспільства.

8. Впровадження інформаційно-аналітичних систем та електронного документообігу в сфері державного управління задля підвищення ефективності управління і створення бази для проведення адміністративної реформи; впровадження систем управління підприємством та електронного документообігу на підприємствах – задля підвищення ефективності управління та продуктивності праці, зменшення собівартості продукції, підвищення конкурентоспроможності, збільшення надходжень до бюджету, створення нових робочих місць.

9. Впровадження систем електронного бізнесу (електронної торгівлі) задля ефективного задоволення потреб споживачів, зменшення витрат на торговельні операції та, як результат, збільшення прибутковості підприємництва, прискорення обігу грошей у банківській сфері, ефективної боротьби із зростанням цін, підвищення рівня прозорості економіки.

10. Впровадження технологій «дистанційного навчання», «телемедицини», «віддаленої роботи» задля підвищення якості освіти та охорони здоров'я, створення нових робочих місць та боротьби з бідністю, запобігання «відтоку мізків» (відтоку висококваліфікованих спеціалістів), проведення ефективної регіональної політики та вирівнювання рівнів соціально-економічного розвитку регіонів.

11. Створення масової системи освіти громадян щодо користування ІКТ та пропаганди науково-технічних знань у цій сфері. Розвиток «електронної довіри» населення до можливостей ІКТ та створення належних умов безпечного користування інформаційними мережами.

12. Реалізація системи заходів, спрямованих на формування іміджу України як країни високих технологій, у якій гармонійно поєднуються духовні, інтелектуальні та науково-технічні надбання із демократичними здобутками помаранчевої революції (як для залучення іноземних інвесторів, так і для виведення на новий рівень експортноорієнтованої індустрії ІКТ, а також для збільшення довіри до українських фінансових інструментів на міжнародних фінансових ринках, протидії негативному інформаційному впливу інших країн, у перспективі – зміни ролі України у міжнародному співтоваристві).

Висновки. Підсумовуючи викладене вище, можемо констатувати, що ефективний захист інформації в умовах, що склались в Україні, може бути досягнутий тільки при створенні системи безпеки інформації, що реалізує державну політику в цій галузі шляхом здійснення управлінської, наукової, адміністративно-господарської й виробничої діяльності, підготовки кадрів та інших видів діяльності.

В основу створення і функціонування цієї системи повинні бути закладені такі принципи: єдина правова, організаційна й матеріально-технічна база, з урахуванням міжнародних норм і правил безпеки інформації, а також чинних у даний час нормативних, організаційних і розпорядчих документів; комплексність рішення проблем безпеки й формування стратегії як складової частини національної безпеки держави в цілому; пріоритетність оснащення системи сертифікованими засобами захисту вітчизняного виробництва й формуванням для цієї мети інфраструктури створення конкурентоспроможних і високоефективних засобів захисту інформації із залученням широкого кола підприємств, установ і організацій як державного, так і недержавного секторів економіки.

Література

1. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика. Київ: Едельвейс, 2014. 497 с.

2. Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. *Bi-*

домості Верховної Ради України, 1996. № 30. С. 141.

3. Про національну безпеку України: Закон України від 21.06.2018 р. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

4. Про державну таємницю: Закон України від 21.01.1994 р. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.

5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. *Відомості Верховної Ради України*. 1994. № 31. Ст. 28.

6. Про Раду Національної безпеки і оборони України: Закон України від 05.03.1998 р. *Відомості Верховної Ради України*. 1998. № 35. Ст. 237.

7. Про інформацію: Закон України від 2 жовтня 1992 р. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

8. Про захист суспільної моралі: Закон України від 20.11.2003 р. *Відомості Верховної Ради України*. 2004. № 14. Ст. 192.

9. 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 р. № 47/2017. URL.: https://www.president.gov.ua/documents/472017-21374.

10. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. Резонанс. 2017. № 18. С. 3–14. URL. http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf.

11. Гнатюк С. Л. Проблеми становлення інформаційного суспільства в Україні. Стратегічні пріоритети, № 1(2), 2007. С. 95-101.

12. Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України. Травень 2018 року. Аналітична записка. *Національний інститут стратегічних досліджень при Президенті України*. URL. http://www.niss.gov.ua/content/articles/files/1_cPPP-standarts_27-04_Gn_var_FIN-732b6.pdf.