УДК 340.13:351.746.1+004.9

ДОВГАНЬ Олександр Дмитрович

ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ І РОЗВИТКУ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми. Необхідність протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо є одним із основних завдань забезпечення інформаційної безпеки і вкрай важливим для української держави на сучасному етапі. Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері.

Аналіз останніх досліджень і публікацій. Інформаційна безпека особистості, суспільства і держави аналізується в різних аспектах. Методологічні аспекти інформаційної безпеки розглядають І. Бінько, Г. Костенко, О. Литвиненко, В. Потіха, Г. Феоктистов, Г. Шевченко. Інформаційно-психологічне протиборство в сучасних умовах аналізують Г. Грачов, Є. Коротченко, Е. Макаренко, А. Поздняков. Проблемі інформаційних воєн присвячують свої роботи І. Панарін, Г. Перепелиця, А. Поздняков, Г. Почепцов, С. Расторгуєв, В. Роговець. Питання інформаційних загроз і шляхів їх нейтралізації висвітлювались М. Ожеваном, О. Зарицьким, О. Вусатюком, Б. Зінчуком, В. Петровим та іншими. Розвиток українського суспільства в умовах впливів, визначальних для забезпечення інформаційної безпеки, розглядалися І. Лукіновим, С. Соколенком, В. Гейцем, В. Семиноженком, О. Сосніним та іншими. Ю. Батурін, В. Кузнєцов, А. Жодзишський вивчають інформаційну безпеку з погляду криміналізації суспільства, росту комп'ютерної злочинності.

Водночас проблемам формування і розвитку дієвої системи забезпечення інформаційної безпеки та її складових, у тому числі визначення об'єктів і суб'єктів забезпечення інформаційної безпеки та правових засад їх діяльності, приділено недостатньо уваги в науковій літературі, що зумовлює актуаль-

ність подальших досліджень у цьому напрямі.

Метою статті є визначення правових засад формування і розвитку системи забезпечення інформаційної безпеки України.

Виклад основного матеріалу. Зараз в Україні значно зросла кількість законодавчих колізій, пов'язаних з інформаційними правовідносинами. Зокрема, з'являються раніше невідомі праву суб'єкти та об'єкти, методи інформаційно-правового регулювання, перебудовуються загальновизнані й виникають нові суспільні відносини і зв'язки. Разом з тим існує досить багато недоліків та прогалин в правовому регулюванні інформаційних процесів, що завдає чималої шкоди структурам інформаційного суспільства, діяльності всіх суб'єктів інформаційного простору.

Так, на сьогодні правову основу інформаційної безпеки становлять Конституція України, Закон України «Про основи національної безпеки України» та інші закони країни, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Стратегія Національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015, а також видані на виконання законів інші нормативно-правові акти України.

Забезпечення інформаційної безпеки відповідно до Конституції України [1] є однією із найважливіших функцій держави і справою усього Українського народу. Державна політика у сфері інформаційної безпеки визначається Верховною Радою України, яка також формує законодавчу базу в інформаційній сфері.

На жаль, до цього часу не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно в країні не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже і забезпечення інформаційної безпеки.

Про таку ситуацію зазначали учасники постійно діючого форуму всеукраїнського об'єднання «Просвіта» [2]. Зокрема, увага акцентувалася на тому, що «в Україні фактично відсутня цілісна системна інформаційна політика. …не мають єдиної узгодженої стратегії розвитку інформаційної галузі, плану консолідованих дій та спільного бачення засобів реагування на серйозні загрози й виклики».

Протягом 2002–2010 років було три спроби ухвалити концепцію державної інформаційної політики. 11 січня 2011 року черговий проект концепції прийняли у першому читанні за основу закону і направили на доопрацювання Комітету Верховної Ради України з питань свободи слова та інформації. Після чого у другому читанні проект закону про Концепцію державної інформаційної політики був розглянутий на засіданні Верховної Ради України і від-

хилений [3]. Однак такий нормативно-правовий акт вкрай необхідний і повинен бути розроблений та прийнятий. У ньому, на нашу думку, у рамках державної політики у сфері інформаційної безпеки мають бути закладені основи для вирішення завдань щодо захисту прав і свобод людини і громадянина, свідомості населення, інформаційного суверенітету України, збереження духовних і культурних цінностей Українського народу, убезпечення сталого розвитку його національної самоідентичності та цивілізаційної єдності, створення в Україні розвиненого інформаційного суспільства, національного інформаційного простору, цілеспрямованого набуття Україною статусу інформаційно розвиненої держави і рівноправного членства у європейській та міжнародній спільноті.

Світ змінюється, виникають принципово нові суспільні відносини в інформаційній сфері, економіці й виробництві. Все це відбувається завдяки глобальному розвитку дистанційних комунікацій, інформаційних технологій та продуктів, ресурсів і послуг. Інформація та інформаційні ресурси стають стратегічним потенціалом і найважливішим чинником розвитку людини, суспільства і держави, про що нами неодноразово наголошувалося.

Процесам, що відбуваються в глобальному інформаційному просторі, притаманні певні тенденції та особливості, які, на наш погляд, можемо охарактеризувати наступним чином. По-перше, уроки інформаційної агресії, які пережила і переживає Україна, змінюють традиційні уявлення про символи могутності й способи досягнення світового панування. Розвиток інформаційної сфери не визнає національно-державних меж і веде до утворення глобальних інформаційних мереж та інформаційних ресурсів, що нав'язують свої стандарти поведінки й мислення. По-друге, як показує практика, інформаційна перевага надає можливість випередити суперника у прийнятті рішень, у тому числі військово-політичних, і є запорукою успіху у воєнних діях. Оскільки, як зазначалося вище, завдяки глобальному розвитку в перспективі виникне нове протистояння у світі за контроль над інформаційним простором і «транспортуванням інформації», що в свою чергу порушить проблему будівництва нової системи європейської та міжнародної безпеки. По-третє, самі по собі геополітичні трансформації нинішнього століття зумовлюють характер відносин співробітництва і протиборства. Однією із головних сфер такого суперництва виступатиме інформаційний простір на різних його рівнях (глобальному, регіональному, можливо, субрегіональному і національному). В умовах інформаційної глобалізації жодна держава світу, незалежно від рівня економічного, воєнного чи інформаційного потенціалу, нездатна самостійно за-

безпечити власну інформаційну безпеку. По-четверте, володіння інформаційними ресурсами стає одним із головних факторів геополітичної конкуренції. Формування глобальної інформаційної інфраструктури на основі мережі Інтернет може привести до посилення просторової взаємозалежності держав. У сучасному інформаційному просторі посилюються процеси, пов'язані з розвитком відносин партнерства і суперництва. Все це є наслідком трансформації інформаційної сфери в сучасних умовах. По-п'яте, у різних країнах світу активно розробляються технології та психологічні засоби ведення інформаційної війни й інформаційного протиборства, спрямовані на використання інформації проти людського інтелекту. І насамкінець, по-шосте, поряд із відомими засобами впливу (дезінформація, чутки, пропаганда, агітація, міфи тощо) на перший план виходять засоби одержання й доставки інформації. Це насамперед системи глобального телерадіомовлення, за допомогою яких реальні події з відповідними коментарями та спеціально підібрані факти й аргументи стають доступними аудиторії в багатьох країнах світу.

Тому, з урахуванням тих процесів, що відбуваються в глобальному інформаційному просторі і мають певні тенденції та особливості, на наше переконання, слід визначити основні проблеми інформаційної безпеки, які постають на сучасному етапі, про що було зазначено вище. До таких, враховуючи всі тенденції, що мають місце в глобалізованому інформаційному просторі, необхідно віднести: відчутні, подекуди революційні, зміни в інформаційному суспільстві, які трансформують системи соціальних цінностей і активізують нові глобальні можливості, у тому числі інформаційні виклики і загрози; ескалацію кібертероризму, кіберзлочинності й інші невирішені питання інформаційної безпеки, з якими зіштовхнулася більшість країн світу; поширення та постійний приріст інформаційної агресії і насилля, що спостерігається протягом останніх десятиліть; поширення маніпуляції свідомістю людини, інформаційно-психологічних операцій, моделювань і провокацій поведінкових конфліктів; здійснення розробок інформаційної зброї або її елементів у різних країнах світу; реальну шкоду національній безпеці, яка завдається шляхом застосування інформаційних впливів; необхідність перегляду систем інформаційної безпеки на міжнародному, регіональному (субрегіональному), національному, груповому та індивідуальному рівнях.

Вивчення та аналіз великого масиву проведених науковцями досліджень й результати практики свідчать про те, що загрози мають широкий спектр класифікацій і носять характер багатоманітності та неоднаковості, багатошаровості й певної

нескінченності загроз та небезпек інформаційній безпеці. При цьому є адекватними часу і простору, темпам розвитку суспільства.

Тому, з урахуванням зазначеного, постає питання щодо можливості на підставі теоретичних розробок і практичних даних формувати адекватну систему моніторингу та управління загрозами і небезпеками в інформаційній сфері.

На законодавчому рівні було звернуто увагу на порушені питання. Так, в Законі України «Про основи національної безпеки України» [4] однією з основних загроз інформаційній безпеці названо «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації». До інших загроз віднесено: прояви обмеження свободи слова та доступу до публічної інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерну злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави.

Питання забезпечення інформаційної безпеки та розробки складових державної політики у цій сфері на системному рівні вперше були визначені у рішенні Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» [5], введеному в дію Указом Президента України від 23 квітня 2008 року № 377/2008, та у Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 8 липня 2009 року № 514/2009 (втратила силу на підставі Указу Президента України від 6 червня 2014 року № 504/2014). Водночас вказані напрацювання не були своєчасно реалізовані, а система забезпечення інформаційної безпеки, як засвідчив стан протидії інформаційній агресії РФ, залишилась неефективною і такою, що не відповідає національним інтересам України.

Таким чином бачимо, що з боку держави робляться спроби створення повноцінної системи забезпечення інформаційної безпеки. Про що свідчить і Указ Президента України від 1 червня 2014 року № 449/2014 [6], яким уведено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Вказаним документом передбачено вдосконалення нормативно-правового забезпечення та попередження й нейтралізація потенційних і реальних загроз національній безпеці в інформаційній сфері, зокрема, запропоновано

розробити та внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України («Про основи національної безпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України») щодо приведення національного законодавства у відповідність із міжнародними стандартами з питань інформаційної й кібернетичної безпеки, вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України тощо.

На сьогодні єдиним чинним стратегічним документом в межах цієї проблематики є Стратегія національної безпеки України [7]. Вона визначила як основні загрози *інформаційній безпеці*: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства; *кібербезпеці і безпеці інформаційних ресурсів*: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом; *безпеці критичної інфраструктури:* критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення.

У зв'язку з цим для вжиття адекватних заходів на загальнодержавному рівні пріоритетами забезпечення інформаційної безпеки є:

– забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;

– розробка і реалізація скоординованої інформаційної політики органів державної влади;

– виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

– створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав – членів НАТО;

– удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу.

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів Стратегією визначено:

– розвиток інформаційної інфраструктури держави;

– створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);

– моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;

– розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

– забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;

– реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС;

– створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;

– розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

За таких умов актуальним постає завдання формування і розвитку дієвої системи забезпечення інформаційної безпеки та її складових, у тому числі визначення об'єктів і суб'єктів забезпечення інформаційної безпеки та правових засад їх діяльності, і як наслідок – побудова моделі забезпечення інформаційної безпеки (див. рис. 1).

Підтримуючи напрацювання різного роду нормативних актів в інформаційній сфері, передбачуваних загроз та пріоритетів забезпечення інформаційної безпеки, приходимо до глибокого переконання, що до об'єктів інформаційної безпеки слід віднести: конституційні права і свободи людини і громадянина, фізичне та психологічне здоров'я населення, захищеність людини від деструктивного та маніпулятивного інформаційних впливів; інформаційне забезпечення, гарантії інформаційних прав та права на розвиток населення всіх регіонів України; інформаційний суверенітет, безпека національного сегмента глобального інформаційного простору, інформаційної інфраструктури, захищеність, цілісність, доступність та безпечність інформаційних ресурсів продукції і послуг.

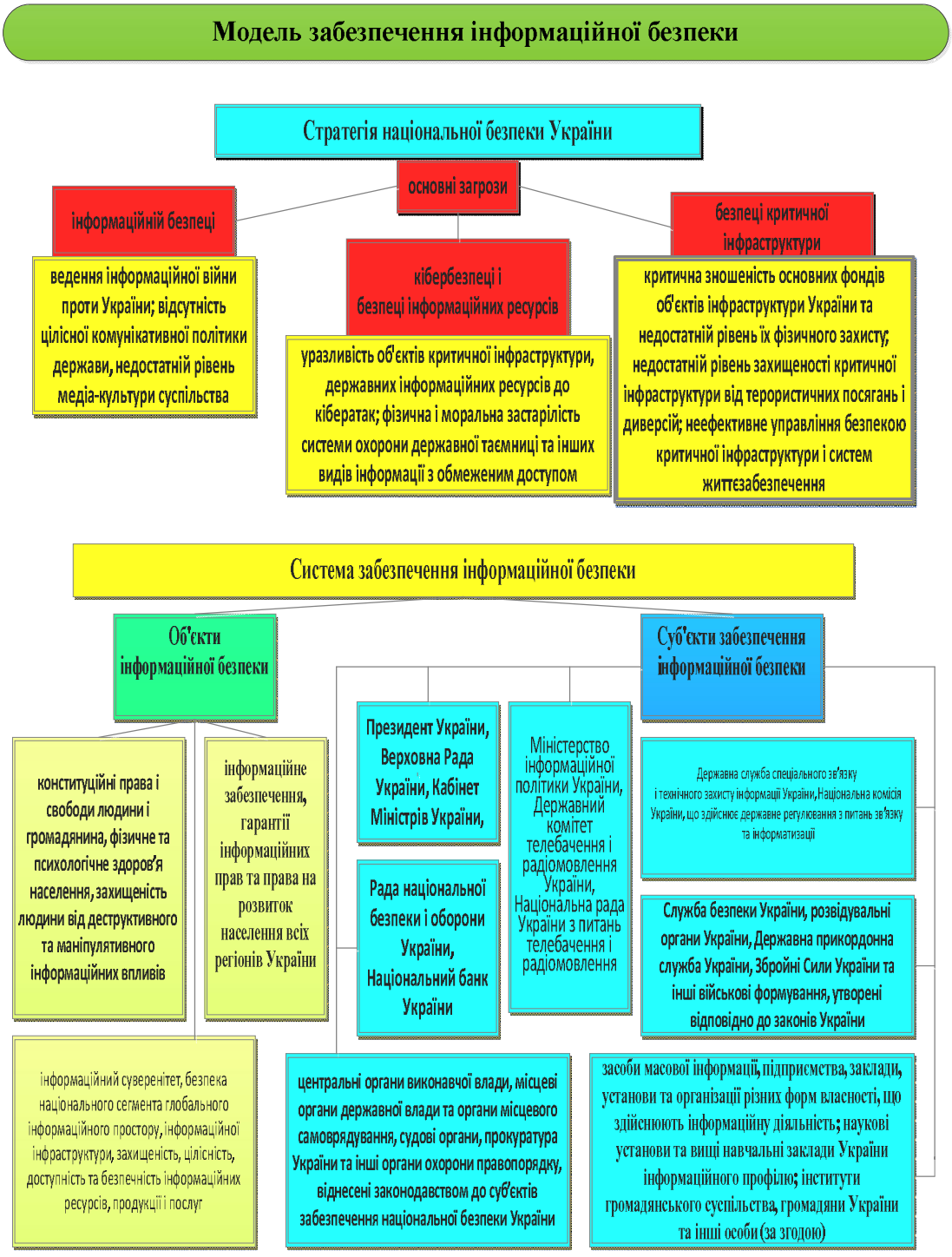

Рис. 1 Модель забезпечення інформаційної безпеки

З урахуванням положень Конституції України й інших законів та нормативно-правових актів України, якими визначаються повноваження, права й обов'язки, до суб'єктів забезпечення інформаційної безпеки пропонуємо віднести: Президента України, Верховну Раду України, Кабінет Міністрів України, Раду національної безпеки і оборони України, Національний банк України, центральні органи виконавчої влади, місцеві органи державної влади та органи місцевого самоврядування, судові органи, Прокуратуру України та інші органи охорони правопорядку, віднесені законодавством до суб'єктів забезпечення національної безпеки України. Також Міністерство інформаційної політики України, Державний комітет телебачення і радіомовлення України, Національну раду України з питань телебачення і радіомовлення, Державну службу спеціального зв'язку і технічного захисту інформації України, Національну комісію України, що здійснює державне регулювання з питань зв'язку та інформатизації; Службу безпеки України, розвідувальні органи України, Державну прикордонну службу України, Збройні Сили України та інші військові формування, утворені відповідно до законів України. Крім того, засоби масової інформації, підприємства, заклади, установи й організації різних форм власності, що здійснюють інформаційну діяльність; наукові установи та вищі навчальні заклади України інформаційного профілю; інститути громадянського суспільства, громадяни України та інші особи (за їх згодою).

Їхня діяльність по забезпеченню інформаційної безпеки повинна базуватися лише на нормах права, правовідносини будуватися у правовому полі і зосереджуватися на захисті життєво важливих інтересів людини, суспільства і держави в інформаційній сфері та конструктивному поєднанні діяльності держави і всього Українського народу. При цьому необхідно перевагу віддавати наступним пріоритетним напрямам: дотриманню в Україні конституційних прав і свобод людини і громадянина; забезпеченню безпеки спілкування і захисту свідомості населення країни від деструктивних маніпулятивних інформаційних впливів; захисту інформаційного суверенітету, конституційного ладу і територіальної цілісності України; правовому, науковому і науково-технічному забезпеченню формування та розвитку інформаційного суспільства в Україні та його трансформації в суспільство знань; утвердженню в національному інформаційному просторі загальнолюдських і національних цінностей, збереженню і розвитку духовних та культурних традицій Українського народу; формуванню вітчизняної індустрії високотехнологічної інформаційної продукції, розробці і впровадженню новітніх інформаційних технологій та програмної продукції; становленню та інноваційному оновленню

національної інформаційної інфраструктури, національних інформаційних ресурсів, продукції та послуг на засадах стимулювання вітчизняних виробників; забезпеченню захисту права приватності особи, персональних даних, інформації з обмеженим доступом і технічного захисту інформації; розвитку міжнародного співробітництва з питань інформаційної безпеки (див. рис. 2).

Рис. 2 Структура системи забезпечення інформаційної безпеки

Висновки. На сьогодні, у переважній більшості, система працює на протидію загрозам, тобто на пасивну складову, хоча на наше переконання з урахуванням практики країн Європейського Союзу інформаційна безпека повинна бути побудована на моделі стратегічного мислення: вжиття заходів для захисту цілей, їх утримання й забезпечення безпеки на основі принципів демократії, прав людини, захищеного Інтернету тощо.

Все це потребує законодавчого закріплення в найкоротший термін, оскільки нормативним актом буде визначено єдиний понятійно-категоріальний апарат, державну політику забезпечення інформаційної безпеки, об'єкти інформаційної безпеки та суб'єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур із іншими органами

та відомствами, віднесеними законодавством до суб'єктів забезпечення національної безпеки України, та ін.

Прийняття такого нормативного акта, на нашу думку, має задати загальну логіку не лише подальшої нормотворчої діяльності, а й сутнісно сформулювати бачення Україною нових геополітичних умов існування держави передусім щодо її ролі в глобальному та національному інформаційних просторах, стати запорукою вирішення проблем в інформаційній сфері.

Крім того, після прийняття такого акта та створення системи забезпечення інформаційної безпеки, на наше переконання, непогано було б провести вивчення реального стану в інформаційній сфері України і за результатами сформувати відповідний документ з визначенням: ступеня розвитку та основних загроз в інформаційній сфері; сил, які потрібно залучити для вирішення завдань протидії виявленим загрозам та негативним сценаріям розвитку; оцінки наявних можливостей суб'єктів забезпечення інформаційної безпеки щодо протидії виявленим загрозам та негативним сценаріям розвитку; аналізу стану кадрового, фінансового, матеріально-технічного та інших видів їх забезпечення; підходів до формування оптимальної моделі забезпечення інформаційної безпеки з урахуванням реальних можливостей та ресурсів; найбільш перспективних альтернативних моделей та стратегій досягнення поставлених завдань та ін. Це в свою чергу стане джерелом якісного аналізу інформаційної сфери України та своєрідним звітом про ефективність системи забезпечення інформаційної безпеки з урахуванням тих змін, які відбуваються в інформаційному середовищі України.

Список використаних джерел

1 Конституція України від 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 17.

2 Інформаційне протистояння // Голос України. – 2015. – № 212 (6216).

3 Постанова Верховної Ради України «Про відхилення проекту Закону України про Концепцію державної інформаційної політики» від 5 липня 2011 р. № 3590-VI [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/3590-17.

4 Закон України «Про основи національної безпеки України» від 19 червня 2003 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

5 Указ Президента України «Про рішення Ради національної безпеки і оборони України від 21 березня 2008 р. «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» від 23 квітня 2008 р. № 377/2008 [Електронний ресурс]. – Режим доступу :

http://www.uazakon.com/documents/date_b0/pg_gwcewh.htm.

6 Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 1 червня 2014 р. № 449/2014 [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/4492014-17157.

7 Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 р. № 287/2015 // Офіційне інтернет-представництво Президента України [Електронний ресурс]. – Режим доступу : http: //www.president.gov.ua.

Рецензенти:
кандидат юридичних наук, старший науковий співробітник В. Шлапаченко,
кандидат юридичних наук, старший науковий співробітник О. Солодка

Аннотация: В статье исследованы правовые принципы формирования и развития системы обеспечения информационной безопасности Украины. Акцентировано внимание относительно возможности на основании теоретических разработок и практических данных формировать адекватную систему мониторинга и управления угрозами и опасностями в информационной сфере, а также развитии действенной системы обеспечения информационной безопасности и ее составляющих, в том числе определение объектов и субъектов обеспечения информационной безопасности и правовых принципов их деятельности, и как следствие – построение модели обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, обеспечение информационной безопасности, система обеспечения информационной безопасности.

Abstract: The article considers the legal basis of the formation and development of information security ensuring system of Ukraine. The attention is focused on the possibility based on theoretical developments and practical data to form an adequate system of monitoring and management of threats and dangers in the information sector and the development of an effective information security ensuring system and its components as well, including definition of objects and subjects of information security and legal bases of their activities and as a result – building a model of information security.

Key words: information security, information security ensuring, information security ensuring system.