УДК 65.012.8:339.9

Федорук О.В.

КОНЦЕПТУАЛЬНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті розкрито сутність та значення системи забезпечення інформаційної безпеки, досліджено особливості реалізації державної інформаційної політики, проаналізовано базові концепції забезпечення інформаційної безпеки та вдосконалення інформаційної політики з метою гарантування реалізації національних інтересів та інформаційного забезпечення державної соціально-економічної політики.

The article discloses the nature and significance of information security management system for, investigates features of the implementation of state information policy, analyzes the basic concepts of information security and perfecting of the information policy to ensure the implementation of national interests and information supply of the state social and economic policy.

Постановка проблеми у загальному вигляді. Сьогодні до побудови глобального та європейського інформаційного суспільства залучено значну частину інтелектуальної, політичної й економічної еліти провідних світових держав. Інформаційні технології та інформаційно-комунікативні системи за нинішніх умов глобального цивілізаційного розвитку є ключовими ресурсами суспільства та держави й необхідною передумовою їх конкурентоспроможності на глобальних ринках. Саме інформаційна сфера здатна виступати провідним фактором реалізації найважливіших суспільних проектів динамічного розвитку, становлення громадянського суспільства, а також входження до світової спільноти.

Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки в інформаційній сфері при мінімумі відповідних витрат. Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення рівноважного функціонування системи державного управління. Підкреслимо, що інформаційна безпека виступає як характеристика стабільного, стійкого стану системи державного управління, яка при впливі внутрішніх та зовнішніх загроз і небезпек зберігає суттєво важливі характеристики для власного функціонування та розвитку.

Аналіз досліджень і публікацій останніх років. Значний внесок у розвиток концептуальних засад формування системи забезпечення інформаційної безпеки як невід'ємного компонента економічної складової національної безпеки зробили такі відомі вчені, як: С. Авсейков, Д. Андерсон, В. Антипенко, Б. Барбер, Є. Бойцова, Ш. Вайн, В. Василенко, Г. Вейман, Е. Герман, А. Гуцал, Д. Деннінг, К. Еверетт, Дж. Істон, Є. Камінський, М. Кастельс, О. Леонов, В. Ліпкан, Є. Лісіцин, Є. Макаренко, Г. Міхелс, К. Нейл, М. Ожеван, С. Расторгуєв, М. Руденко, М. Уфарєв, К. Шеннон, Г. Шіллер та ін.

Виділення невирішених раніше частин загальної проблеми. Водночас аналіз минулої та сучасної наукової думки засвідчив відсутність комплексного підходу щодо формування системи забезпечення інформаційної безпеки, яка б охоплювала сучасні теоретичні концепції інформаційної безпеки в контексті протидії інформаційним загрозам. Тому системне дослідження базових засад зазначеної наукової проблеми є важливим для розвитку вітчизняної економічної науки, а також є основою формування інформаційного забезпечення державної соціально-економічної політики.

Постановка завдання. Метою статті є розкриття сутності та значення системи забезпечення інформаційної безпеки, дослідження особливостей реалізації державної

інформаційної політики, аналіз базових концепцій забезпечення інформаційної безпеки та вдосконалення інформаційної політики з метою гарантування реалізації національних інтересів та інформаційного забезпечення державної соціально-економічної політики.

Виклад основного матеріалу дослідження. Значимість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне із глобальних і пріоритетних завдань політики національної безпеки, вирішенню якого мають бути підпорядковані політична, економічна, культурна та інші види діяльності системи державного управління. Під системою забезпечення інформаційної безпеки варто розуміти систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення [1, с.158]. Об'єктами системи забезпечення інформаційної безпеки України є інтереси органів державного управління в інформаційній сфері; система органів державного управління, а також їх компетентні особи та відносини між ними – суспільні відносини в інформаційній сфері; власне система забезпечення інформаційної безпеки України.

Основна мета функціонування системи забезпечення інформаційної безпеки полягає в створенні необхідних економічних і соціокультурних умов, правових й організаційних механізмів формування, розвитку та забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах діяльності громадянина, суспільства та держави. До важливих завдань системи забезпечення інформаційної безпеки належать: створення умов для забезпечення інформаційного суверенітету держави; участь в удосконаленні державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією; створення умов для активного залучення засобів масової інформації до боротьби з корупцією; забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації; забезпечення інформаційної безпеки усіх складових системи державного управління; забезпечення інформаційно-аналітичного потенціалу країни; реалізація державної політики інформаційної безпеки; моніторинг стану інформаційної безпеки; забезпечення збереження державної таємниці тощо.

Відповідно до окресленої мети та завдань можна визначити такі функції системи забезпечення державної інформаційної безпеки: розроблення та прийняття законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами; розроблення та реалізація фінансово-економічних засад регулювання процесів формування і використання інформаційних ресурсів; здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів; забезпечення ефективного використання інформаційних ресурсів у діяльності органів державного управління; оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних й організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку й ефективного використання інформаційних ресурсів; забезпечення розробки та застосування правових, організаційних й економічних механізмів стосовно форм і засобів обігу інформаційних ресурсів держави; регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного та взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну, здійснення єдиної державної політики наукової підтримки

системи державного управління формуванням, розвитком і використанням національних інформаційних ресурсів; кадрове забезпечення функціонування системи державного управління національними інформаційними ресурсами; інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами.

Світовий досвід розвитку інформаційного ринку показує, що управлінська та підприємницька діяльність потребує постійного отримання економічної інформації, а також інформації соціального характеру. Зростання впливу та значущості інформаційної складової суспільства, а також психологічних і технічних можливостей для маніпулювання масовою свідомістю вимагають переходу до прогностичної випереджувальної моделі інформаційного забезпечення, яка передбачає ефективний захист від технологій інформаційно-психологічного впливу, а також задовольняє зростаючу потребу суспільства в одержанні необхідного обсягу достовірної та корисної інформації [2, с.545].

У рамках інформаційного забезпечення національної безпеки, захисту особистої інформації є боротьба з кіберзлочинністю, оскільки це особливо актуальна проблема для країн Європи, що обумовлено високим рівнем комп'ютерної оснащеності. Базовим міжнародним нормативно-правовим документом, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю, є Конвенція Ради Європи «Про кіберзлочинність». У більшості європейських країн прийняті закони, що дають можливість притягнути до відповідальності провайдерів за розміщення на їхніх сайтах інформації незаконного змісту, крім того, деякі правила обмежують доступ провайдерів до таких джерел інформації. Мережеві оператори не можуть бути притягнуті до відповідальності за зміст інформації, яка передається мережами, однак вони зобов'язані на умовах виданих ліцензій вжити необхідних заходів щодо користувачів і клієнтів, які використовують мережі для передання інформації незаконного змісту. У Великій Британії, Німеччині та Нідерландах прийняті кодекси поведінки, а також створені незалежні органи, які розробляють етичні стандарти для змісту інформації та класифікації незаконної інформації.

З метою підвищення ефективності боротьби з кібертероризмом в Україні доцільно реалізувати таку систему заходів: розробити державну стратегію, концепцію та доктрину по боротьбі з кібертероризмом; організувати ефективне співробітництво в інформаційній сфері з державами світу, їх правоохоронними органами, а також міжнародними організаціями; ініціювати підписання регіональних угод як одного з найефективніших інструментів по боротьбі з кібертероризмом; необхідно мати національний підрозділ для боротьби з кіберзлочинністю та міжнародний контактний пункт для допомоги в умовах здійснення або попередження кібератаки; відповідно до існуючих законів про боротьбу з кіберзлочинністю та кібертероризмом, згідно з чинними міжнародними стандартами і Конвенцією Ради Європи про боротьбу з кіберзлочинністю сьогодні в Україні необхідно ухвалити закони про електронну безпеку [3, с.280–281].

Забезпечення інформаційної безпеки представляє безперервний процес, що полягає в обґрунтуванні та реалізації найбільш раціональних методів і шляхів вдосконалення та розвитку системи захисту, контролі її стану, виявленні резервів, а також протиправних дій в інформаційній сфері. Інформаційна безпека може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту у всіх структурних елементах виробничої системи та на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі використовувані засоби, методи та заходи об'єднуються в єдиний цілісний механізм – систему захисту інформації. При цьому функціонування системи має контролюватися, оновлюватися та доповнюватися в залежності від зміни зовнішніх і внутрішніх умов. Варто наголосити, що система захисту інформації не може забезпечити

необхідного рівня безпеки інформації без належної підготовки користувачів і дотримання ними всіх встановлених правил, спрямованих на її захист. З позицій системного підходу до захисту інформації пред'являються такі вимоги: захист інформації повинен бути безперервним, плановим, цілеспрямованим, конкретним, активним, надійним, універсальним і комплексним [4].

Доцільно зауважити, що інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, адекватних загрозам та небезпекам національним інтересам особи, суспільства та держави в інформаційній сфері. Для створення і підтримання належного рівня національної безпеки в інформаційній сфері розробляється система правових норм, що регулюють відносини в інформаційній сфері, визначаються основні напрями діяльності органів державного управління, формуються органи забезпечення державної інформаційної безпеки, а також механізми контролю та нагляду за їх діяльністю.

У сучасних умовах забезпечення інформаційної безпеки досягається на основі реалізації системи заходів, спрямованих на попередження загроз, – це превентивні заходи щодо забезпечення інформаційної безпеки шляхом попередження можливості виникнення загроз; на виявлення загроз, що виражається в систематичному аналізі та контролі можливості появи реальних або потенційних загроз і своєчасних заходах щодо їх попередження; на виявлення загроз, що передбачає визначення реальних загроз і конкретних злочинних дій; на локалізацію злочинних дій і вжиття заходів щодо ліквідації загрози або конкретних злочинних дій; на ліквідацію наслідків загроз і злочинних дій, а також відновлення статус-кво.

Розрізняють юридичні, організаційно-економічні й технологічні заходи із забезпечення інформаційної безпеки. Ці заходи базуються на таких принципах: нормативно-правова база інформаційних відносин у суспільстві чітко регламентує механізм забезпечення права громадян вільно одержувати, створювати та поширювати інформацію будь-яким законним способом; інтереси власників і розпорядників інформаційних ресурсів охороняються законом; засекречування (закриття) інформації є виключенням із загального правила на доступ до інформації; відповідальність за збереження інформації, її засекречування та розсекречення персоніфікується; важливим завданням держави є розвиток сфери інформаційних послуг, що надаються населенню та фахівцям на основі сучасних комп'ютерних мереж, системи загальнодоступних баз і банків даних, котрі містять довідкову інформацію соціально-економічного, культурного та побутового характеру, право доступу до яких гарантується й регламентується законодавством [5, с.100–101].

Системна цілеспрямована інформаційна політика покликана насамперед забезпечити реалізацію таких стратегічних напрямів розвитку суспільства і держави, як: захист конституційних прав і свобод громадян в інформаційній сфері, свободи висловлювання й права на поінформованість; протидія структурам міжнародної організованої злочинності, що зловживають прозорістю світових інформаційних потоків; інформаційно-аналітичне забезпечення діяльності ЗМІ, владних, наукових, господарчих та інших структур; входження України до європейського та світового інформаційного простору; розв'язання протиріч між національною нормативно-правовою базою й європейським та міжнародним законодавством в інформаційній сфері; реалізація бюджету розвитку, який би стимулював примноження людського капіталу; формування інтелектуальної економіки на засадах нормативно-правової бази, спрямованої на ефективний захист в Україні інтелектуальної власності, інтелектуальних продуктів і боротьбу із проявами піратства [3, с.332–333].

У зв'язку з масовою комп'ютеризацією інформаційних процесів, збільшенням цінності та значимості інформаційних ресурсів особливої гостроти набуває проблема надійного захисту інформації, що циркулює в інформаційних системах,

тобто попередження її спотворення та знищення, несанкціонованої модифікації, незаконного отримання й використання [6, с.191]. Забезпечення інформаційної безпеки повинно здійснюватись передусім шляхом проведення виваженої та з балансованої політики держави в інформаційній сфері, яка характеризується трьома основними векторами: захист інформаційних прав і свобод людини; захист державної безпеки в інформаційній сфері; захист національного інформаційного ринку, економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції. Основною метою державної влади в період глобальної інформаційної революції є розробка та реалізація концептуальних основ державної інформаційної політики шляхом прийняття адекватних нормативно-правових актів щодо регулювання інформаційних відносин.

Загрози конфіденційної інформації представляють собою потенційні чи реально можливі дії щодо інформаційних ресурсів, які призводять до неправомірного оволодіння даними, а саме: ознайомлення з конфіденційною інформацією без порушення її цілісності; модифікація інформації у кримінальних цілях; знищення інформації з метою прямого нанесення матеріальних збитків. У підсумку протиправні дії з інформацією спричиняють порушення її конфіденційності, повноти, достовірності та доступності, що, у свою чергу, призводить до порушення режиму та якості управління в умовах помилкової або неповної інформації. Основними загрозами інформації є її розголошення, витік і несанкціонований доступ до джерел інформації:

- розголошення – це умисні або необережні дії з конфіденційною інформацією, що призвели до ознайомлення з нею осіб, не допущених до цієї інформації;
- витік – це безконтрольний вихід конфіденційної інформації за межі організації;
- несанкціонований доступ – це протиправне умисне оволодіння конфіденційною інформацією особою, яка не має права доступу до даної інформації.

До умов, що сприяють неправомірному оволодінню конфіденційною інформацією, відносять: розголошення; несанкціонований доступ шляхом підкупу та схиляння до співпраці з боку конкурентів і злочинних угруповань; відсутність належного контролю та жорстких умов забезпечення інформаційної безпеки; традиційний обмін виробничим досвідом; безконтрольне використання інформаційних систем; наявність передумов виникнення серед співробітників конфліктних ситуацій [4].

З урахуванням сформованої практики забезпечення інформаційної безпеки виділяють такі напрямки захисту інформації:

- правовий захист, що закріплений міждержавними договорами, конвенціями, деклараціями, державними та відомчими актами;
- організаційний захист – це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або послаблює нанесення збитків суб'єктам господарювання;
- інженерно-технічний захист – це використання різних технічних засобів, що перешкоджають нанесенню шкоди господарській діяльності.

Організаційні заходи відіграють важливу роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого використання конфіденційних відомостей значною мірою обумовлюються не технічними аспектами, а зловмисними діями та недбалістю користувачів. На рівні підприємства організаційні заходи повинні реалізовуватися службою безпеки, на яку покладаються такі функції: організація та забезпечення захисту конфіденційної інформації; участь в розробці основоположних документів з метою закріплення в них вимог щодо забезпечення інформаційної безпеки; розробка та реалізація заходів щодо забезпечення роботи з документами, що містять конфіденційні відомості; проведення службових розслідувань за фактами розголошення відомостей, втрат документів, витоку конфіденційної інформації та інших порушень інформаційної безпеки; підтримання контактів із правоохоронними органами та службами безпеки інших підприємств.

Варто наголосити, що розвиток процесів комп'ютеризації, крім незаперечних переваг, спричинив необхідність забезпечення ефективного захисту інформації. Формування системи захисту інформації включає такі етапи:

- аналіз складу та змісту конфіденційної інформації; аналіз цінності інформації з позицій можливих збитків від її одержання конкурентами;
- оцінка доступності інформації для зловмисників;
- дослідження діючої системи захисту інформації; оцінка витрат на розробку нової або вдосконалення діючої системи захисту інформації;
- організація заходів із захисту інформації;
- закріплення персональної відповідальності у сфері захисту інформації;
- реалізація нової системи захисту інформації [7].

Як засвідчує досвід провідних країн світу, великого значення для нормального функціонування інформаційної сфери держави набуває узгоджена діяльність відповідного державно-правового механізму, тобто система взаємопов'язаних державних органів, організацій, установ щодо вироблення та реалізації сукупності норм і принципів права з метою врегулювання суспільних відносин в інформаційній сфері. Під державно-правовим механізмом інформаційної безпеки розуміють систему взаємопов'язаних і взаємоузгоджених державно-правових інституцій, завданнями яких є створення умов для успішної реалізації інформаційної політики.

Під інформаційною політикою розуміють діяльність держави в інформаційній сфері, спрямовану на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору держави та його інтеграції у світовий інформаційний простір з урахуванням національних інтересів й особливостей при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях. Основною метою політики інформаційної безпеки держави є управління реальними та потенційними загрозами і небезпеками з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів.

До основних напрямів державної інформаційної політики належать:

- удосконалення законодавства і правового регулювання в галузі створення та використання інформаційних ресурсів і технологій, реалізації інформаційних прав громадян та прав на результати творчої праці, регулювання діяльності українських сегментів глобальних інформаційних мереж, охорони прав користувачів інформаційних послуг і продуктів, формування системи захисту державної та комерційної таємниці;
- забезпечення інформаційної безпеки та захисту інформації на основі розвитку нормативного регулювання захисту даних в телекомунікаційних мережах;
- покращення та поширення процедур надійної ідентифікації та аутентифікації;
- стимулювання використання систем криптографії операторами мереж, зокрема в галузі супутникового та мобільного зв'язку, розробка превентивних технічних засобів для забезпечення надійності телекомунікацій;
- розширення міжнародного співробітництва й торгівлі в галузі інформаційно-комп'ютерних технологій на основі гармонізації українського законодавства з міжнародним, забезпечення взаємодії українських інформаційних систем із зарубіжними аналогами, створення сприятливих умов для формування єдиного інноваційного та інформаційного простору між країнами на базі загального ринку інформації.

Висновки і перспективи подальших розробок. Таким чином, для реалізації національних інтересів в інформаційній сфері необхідно переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства і забезпечення інформаційної безпеки. Сьогодні актуальним

є створення таких умов для зростання інформаційної індустрії: підтримка розвитку комплексу галузей, які виробляють різноманітні інформаційні продукти та надають послуги в інформаційній сфері шляхом залучення інвестицій приватного сектора, створення збалансованого конкурентного середовища та підтримка розвитку інформаційної інфраструктури українського ринку інформаційно-комунікаційних технологій; покращення доступу населення до інформаційної інфраструктури та мережевих послуг шляхом розвитку бібліотечної мережі, покращення довідково-інформаційного обслуговування населення та створення відповідних сприятливих умов для використання інформаційно-комп'ютерних технологій; розвиток інформаційно-телекомунікаційних систем і формування інформаційних ресурсів в інтересах державного управління шляхом покращення доступу до державної інформації, удосконалення процедур надання послуг, підтримки державних інформаційних центрів, розвитку електронної взаємодії між органами державної влади на центральному, регіональному, місцевому рівнях і створення інтегрованої, орієнтованої на користувача системи державних інформаційних послуг на основі інформаційно-телекомунікаційної системи державних структур, тобто забезпечення доступності інформації через комп'ютерні мережі, створення загальнодоступних сайтів і підключення до мережі відкритих суспільно значущих державних інформаційних ресурсів.

Важливим завданням у сфері вдосконалення інформаційної політики в Україні є формування її стратегії та визначення пріоритетів з метою забезпечення адаптації українського суспільства й держави до реалій глобального та європейського інформаційного суспільства. Ключовим напрямом такої політики має стати підвищення інтелектуального, творчого, технічного рівня вітчизняних виробників інформаційного продукту, зростання їхньої конкурентоспроможності на світовому інформаційному ринку. Лише розвинене конкурентоспроможне на світовому рівні інформаційне виробництво може гарантувати реалізацію національних інтересів в інформаційній сфері, а також вирішити завдання ефективного інформаційного забезпечення державної соціально-економічної політики.

Список використаної літератури

1. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: [навч. посіб.] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К.: КНТ, 2006. – 280 с.
2. Україна у системі міжнародної безпеки: [монографія] / [Я. Б. Базилюк, О. С. Бодрук, Д. Ю. Венцковський та ін.]; заг. ред. О. С. Власюк; Рада національної безпеки і оборони України, Національний ін-т проблем міжнар. безпеки. – К.: Фоліант: Стилос, 2009. – 572 с.
3. Міжнародна інформаційна безпека: сучасні виклики та загрози / [Є. А. Макаренко, М. М. Рижиков, М. А. Ожеван та ін.]. – К.: Центр вільної преси, 2006. – 916 с.
4. Ярочкин В. И. Информационная безопасность: [учеб. для студ. вузов] / В. И. Ярочкин. – 2-е изд. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.
5. Економічна безпека: [навч. посіб.] / [В. І. Франчук, Л. В. Герасименко, В. О. Гончарова та ін.; за ред. В. І. Франчука]. – Л.: ЛьвДУВС, 2010. – 243 с.
6. Экономическая и национальная безопасность: [учеб. для студ. вузов] / [ред. Л. П. Гончаренко]. – М.: Экономика, 2008. – 543 с.
7. Игнатьев В. А. Информационная безопасность современного коммерческого предприятия: [монография] / В. А. Игнатьев. – Старый Оскол: ТНТ, 2005. – 448 с.

Прийнято до друку 25.01.2013