

## СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В ПЕРІОД ГЛОБАЛЬНОЇ КРИЗИ

*In the article was observed different approaches to the creation of the system of informational security in the researches of national scientists, was analyzed basic directions of national politic of Ukraine in the informational sphere in time of global crisis.*

Початок нового тисячоліття характеризується глобалізацією світових економічних і політичних процесів, невід'ємною складовою яких є інтенсивне використання досягнень сучасних інформаційних технологій. Після вибору Україною шляху до інтеграції в Європу, яка сьогодні активно розбудовує інформаційне суспільство, гостро постала проблема ефективного забезпечення інформаційної безпеки молодій державі.

У сучасному світі інформація є найціннішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності і т. ін. Тому Конституція України забезпечення інформаційної безпеки відносить до найважливіших функцій держави.

Згідно Доктрини інформаційної безпеки України, за сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку [6].

Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки. Завдяки унікальному геополітичному розташуванню України, багатству духовної та історичної спадщини Українського народу, керуючись ідеями розвитку національного самоусвідомлення та цивілізаційної єдності української нації, Україна має стати інформаційно розвинутою державою, повноправним і впливовим учасником європейського життя, посісти гідне місце у глобалізованому світі. Основною метою реалізації положень Доктрини інформаційної безпеки України є створення в Україні розвинутого національного інформаційного простору і захист її інформаційного суверенітету.

Забезпечення інформаційної безпеки України має здійснюватися за такими принципами [6]:

- свобода збирання, зберігання, використання та поширення інформації;
- достовірність, повнота та неупередженість інформації;

---

\* аспірантка кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка  
Науковий керівник: проф. Рижков М.М.

- обмеження доступу до інформації виключно на підставі закону;
- гармонізація особистих, суспільних і державних інтересів;
- запобігання правопорушенням в інформаційній сфері;
- економічна доцільність;
- гармонізація українського законодавства в інформаційній сфері з міжнародним;
- пріоритетність національної інформаційної продукції.

Інформаційний суверенітет та інформаційна безпека України гарантуються і забезпечуються Конституцією України, Законом України «Про Інформаційний суверенітет та інформаційну безпеку України», Законами України «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про авторське право та суміжні права», «Про державну таємницю», «Про захист інформації в автоматизованих системах». «Про національний архівний фонд та архівні установи», «Про охорону і використання пам'яток історії та культури», «Про інформаційні агентства», «Про зв'язок», «Про рекламу», «Про видавничу справу», «Про професійних творчих працівників та творчі спілки», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про кінематографію», «Про Національну раду України з питань телебачення і радіомовлення», «Про систему Суспільного телебачення і радіомовлення України», Основами законодавства України про культуру, іншими законодавчими актами, а також міжнародними договорами і конвенціями в галузі свободи слова та інформаційної діяльності, ратифікованими Україною.

Основні задачі забезпечення інформаційної безпеки України:

- виявлення, оцінка та прогнозування джерел загроз інформаційній безпеці;
- розробка державної політики забезпечення інформаційної безпеки та комплексу заходів і механізмів її реалізації;
- створення нормативно-правових засад забезпечення інформаційної безпеки, координація діяльності органів державної влади та управління, установ та підприємств по реалізації політики інформаційної безпеки;
- розвиток системи забезпечення інформаційної безпеки, вдосконалення її організації, форм, методів і засобів запобігання загрозам інформаційній безпеці та ліквідації наслідків її порушення;
- забезпечення участі України в процесах створення і використання глобальних інформаційних мереж та систем [5].

Як свідчать наукові дослідження, система забезпечення інформаційної безпеки України не виконує окремих важливих функцій. Зокрема, неефективними є управління її діяльністю, організаційні зміни, що здійснюються в рамках адміністративної реформи, мають несистемний характер, проводяться без попереднього функціонального дослідження органів державної влади. Негативні тенденції розвитку національного інформаційного простору, кризовий стан економіки України та інші чинники зумовлюють ескалацію загроз, що може призвести (і призводить) до значних втрат політичного, економічного, воєнного та іншого характеру, завдання шкоди юридичним особам та громадянам України.

У цьому аспекті своєчасним та дійовим (важливим) нормативно-правовим документом став Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 31 жовтня 2001 р., «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 р. № 1193/2001 [4]. Указом було передбачено розробку Концепції національної інформаційної політики та інформаційної безпеки України, здійснення заходів щодо оптимізації системи державних органів, які реалізують інформаційну політику, забезпечивши чітке розмежування повноважень і налагоджен-

ня їх взаємодії та координації, створення організаційної структури системи забезпечення інформаційної безпеки, аналіз програм в інформаційній сфері, які фінансуються з Державного бюджету України, вжиття заходів стосовно першочергової реалізації та повноцінного фінансування найактуальніших з них та інші важливі заходи для забезпечення інформаційної безпеки.

З огляду на зазначене, варто зупинитися на одному з найважливіших аспектів забезпечення належного захисту інформаційної безпеки – на координації діяльності державних органів, приватного сектору, громадських організацій та окремих громадян. Згідно зі статтею 17 Конституції України забезпечення інформаційної безпеки – справа усього українського народу [2].

Проблема координації є важливою сама по собі та набуває значення у зв'язку з тим, що, на відміну від багатьох інших галузей, у сфері інформаційних технологій постійно змінюється термінологія, ламаються традиційні уявлення про методи та засоби передачі, отримання, обробки та зберігання інформації, хоча часом за зміною вже сталих термінів простежується тільки робота маркетологів з просування власних проектів. Це призводить до того, що одне й те саме поняття описується завдяки різним термінам, і, навпаки, один і той самий термін несе різне значення навантаження.

Питання забезпечення інформаційної безпеки сьогодні для України стоять на одному рівні із захистом суверенітету і територіальної цілісності, забезпеченням її економічної безпеки. Роботи над концепцією інформаційної безпеки України спрямовані на систематизацію питань, які поєднані в проблему забезпечення інформаційної безпеки країни, на визначення методів та засобів захисту життєво важливих інтересів особистості, суспільства, держави в інформаційній сфері, на створення засад для формування державної політики інформаційної безпеки, розвитку інформаційного простору країни. Інформаційний простір – середовище, де здійснюється формування, збір, зберігання та розповсюдження інформації. Інформаційний простір України – це інформаційний простір, на який розповсюджується юрисдикція України.

Метою забезпечення інформаційної безпеки в Україні є створення розгалуженого та захищеного інформаційного простору, захист національних інтересів України в умовах формування світових інформаційних мереж, захист економічного потенціалу держави від незаконного використання інформаційних ресурсів, реалізація прав громадян, установ та держави на отримання, поширення та використання інформації [6].

Стан інформаційного простору України характеризується наявністю протиріччя між потребами суспільства в розширенні вільного обміну інформацією і необхідністю окремих обмежень на її поширення. Необхідно відзначити, що порушенню інформаційної безпеки сприяє безсистемність захисту інформації і слабка координація дій по захисту інформації в загальнодержавному масштабі.

Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз - це нанесення шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо.

На сучасному етапі в Україні немає реальних гарантів інформаційної безпеки країни, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Процес інформатизації має стихійний, некерований характер, з переважним ухилом у бік використання засобів інформатизації іноземного виробництва.

Безсистемність процесів формування інформаційної інфраструктури України обумовлює складність вирішення проблеми інформаційної безпеки, захисту інформаційних ресурсів. Специфіка цих проблем полягає в тому, що об'єктивно достатній рівень захищеності інформаційної інфраструктури та інформаційних ресурсів може бути досягнутий тільки у результаті чіткого визначення об'єктів ін-

формаційної безпеки України, забезпечення надійного функціонування державних та суспільних інститутів для реалізації практичних заходів забезпечення інформаційної безпеки [1].

Ситуація, що склалася в інформаційній сфері України, вимагає невідкладного рішення таких комплексних проблем: 1) розвиток науково-практичних основ інформаційної безпеки, а саме, визначення основних положень стратегії держави в сфері створення і забезпечення умов формування і використання інформаційного ресурсу, підтримка високих темпів його наповнення і заданих критеріїв якості (доступність, достовірність, своєчасність, повнота), розробка сучасних інформаційних технологій і технічних засобів для вирішення задачі захисту інформації в інформаційних системах; 2) створення законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, а саме, нормативно-правової бази щодо розподілу і використання персональної інформації з метою створення умов для інформаційних стосунків між органами державної влади і суспільства, формування передумов досягнення соціального компромісу, створення умов становлення соціального партнерства як основи демократичного розвитку суспільства, розробки регламенту інформаційного обміну для органів державної влади і управління, реєстру інформаційних ресурсів, закріплення відповідальності посадових осіб, громадян за додержання вимог інформаційної безпеки; 3) розроблення механізмів реалізації прав громадян на інформацію загального користування; 4) визначення основних положень стратегії держави у сфері використання засобів масової інформації на засадах досліджень процесів формування суспільної свідомості, удосконалення та розвитку індустрії інформування населення країни, розробка методів і форм інформаційної політики держави; 5) розробка методів і засобів оцінки ефективності систем і засобів інформаційної безпеки та їх сертифікація.

Найдокладніший перелік можливих загроз інформаційній безпеці країни і засобів їх реалізації завжди буде неповним, оскільки зміни в суспільних відносинах, розвиток інформаційних технологій та засобів інформатизації сприяє не стільки усуненню існуючих загроз, скільки виникненню нових. В той же час джерела загроз інформаційній безпеці, як складовій національної безпеки, лишаяються досить сталими. До джерел загроз належать [6]:

- недружня політика іноземних держав в галузі глобального інформаційного моніторингу, поширення інформації та новітніх інформаційних технологій;
- цілеспрямована діяльність іноземних спецслужб, політичних та економічних структур;
  - злочинна діяльність міжнародних угруповань, формувань та окремих осіб;
  - неправомірна чи протиправна діяльність посадових осіб державних органів, структур, формувань, спрямована проти інтересів України;
- стихійні лиха, катастрофи, збройні конфлікти;
- некерований характер процесу створення інформаційної інфраструктури України;
  - недосконалість технічних і програмних засобів й недостатня кваліфікація персоналу інформаційних служб і систем;
  - недосконалість, неповнота і неузгодженість з відповідними міжнародними правовими актами чинного законодавства України в інформаційній сфері;
  - недостатній розвиток лексикографічної бази української мови і національного лінгвістичного забезпечення інформаційних систем;
  - низькі темпи науково-технічного і культурного розвитку суспільства внаслідок економічної кризи або неадекватної внутрішньої політики держави в інформаційній сфері;
  - низька правова, організаційна та програмно-технічна забезпеченість в галузі інформаційної безпеки.

Доктриною інформаційної безпеки України визначено загрози національній безпеці України в інформаційній сфері: невиваженість державної політики та відсутність необхідної інфраструктури в інформаційній сфері; повільність входження України у світовий інформаційний простір; інформаційна експансія з боку інших держав; витік інформації, що становить державну та іншу передбачену законом таємницю [6].

Визначено основні напрями державної політики національної безпеки України в інформаційній сфері, зокрема [6]: вжиття комплексних заходів щодо захисту свого інформаційного простору та входження України до світового інформаційного простору; усунення негативних чинників порушення інформаційного простору; розробка і впровадження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно значимої інформації, створення розвиненої інфраструктури в інформаційній сфері і т. ін.

Засоби впливу загроз на інформаційну безпеку поділяються на інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційно-правові.

До інформаційних засобів належать: порушення адреси і своєчасності інформаційного обміну, протизаконні збір і використання інформації; несанкціонований доступ до інформаційних ресурсів; маніпулювання інформацією (дезінформація, укриття та викривлення інформації); незаконне копіювання інформації в інформаційних системах; використання засобів масової інформації з позицій, які суперечать інтересам громадян, організацій чи держави; викрадення інформації з бібліотек, архівів, банків і баз даних; порушення технології обробки інформації.

До програмно-математичних засобів належать: запуск програм-вірусів; установка програмних і апаратних закладних пристроїв; знищення і модифікація даних в інформаційних системах.

Фізичні засоби включають: знищення або руйнування засобів обробки інформації і зв'язку; знищення, руйнування чи викрадення оригінальних носіїв інформації; викрадення програмних чи апаратних ключів і засобів криптографічного захисту інформації; вплив на персонал; поставка «інфікованих» компонентів інформаційних систем.

До радіоелектронних засобів належать: перехоплення інформації в технічних каналах її витоку; будова електронних пристроїв перехоплення інформації в технічних засобах і приміщеннях; перехоплення, дешифрування та подання хибної інформації в мережах передачі даних і мережах зв'язку; вплив на пароліно-ключові системи; радіоелектронне придушення мереж зв'язку і систем керування [3].

До організаційно-правових засобів слід віднести купівлю недосконалих або застарілих інформаційних технологій та засобів інформатизації; невиконання вимог законодавства та затримку прийняття необхідних нормативно-правових положень в інформаційній сфері; неправомірне обмеження доступу, до документів, в яких знаходиться важлива для громадян та організацій інформація.

Реалізація інформаційних загроз на рівні особи призводить до порушення або обмеження доступу громадян до інформації загального користування. Це створює загрозу інформаційній безпеці особистості як з боку органів влади, так і з боку сторонніх осіб або угруповань, порушує баланс стосунків між особистістю, суспільством і державою.

Наслідком впливу інформаційних загроз на соціальну спільноту є ускладнення соціальних процесів, що виявляється у загостренні суперечностей між різними соціальними прошарками, загостренні політичної боротьби, розпалюванні релігійних та етнічних суперечностей, зниженні загальної культури населення, розвитку бездуховності, зростанні злочинності, розповсюдженні антигуманних ідей.

Наслідки інформаційних злочинів в економічній сфері можуть призвести до економічних втрат за рахунок знецінення і втрати товарної частини інформаційного ресурсу - промислових і інформаційних технологій. Вплив інформаційних

загроз на структури державної влади, відповідальні за підготовку та прийняття рішень, реалізація яких безпосередньо впливає на безпеку, може сприяти виникненню надзвичайних ситуацій в державі та суспільстві, значним збиткам через порушення функціонування систем зв'язку, контролю і керування, виток інформації, яка містить державну таємницю [3].

Таким чином, першочергові заходи щодо забезпечення інформаційної безпеки України повинні включати: визначення складу, послідовності і порядку розробки законодавчих і нормативно-правових актів з питань інформаційної безпеки, а також механізмів їх введення в дію (правове забезпечення); розробку державної цільової науково-технічної програми забезпечення інформаційної безпеки, створення інформаційної бази, спрямованої на реалізацію концепції інформаційної безпеки України (науково-технічне забезпечення); розробку і створення організаційної структури системи інформаційної безпеки України; створення вітчизняної системи сертифікації технічних і програмних засобів інформатизації на відповідність вимогам інформаційної безпеки (організаційне забезпечення); забезпечення реальних потреб системи інформаційної безпеки в кадрах, матеріально-технічних і фінансових коштах (ресурсне забезпечення).

#### Список використаних джерел

1. Жданов І. Можливі підходи до визначення основ державної політики забезпечення інформаційної безпеки України // Матеріали до круглого столу «Безпека інформації в інформаційно-телекомунікаційних системах». – К., 2001. – 28 трав. – С.11-19.
2. Конституція України: Прийнята на п'ятій сесії Верховної Ради України 28 черв. 1996 р. – К.: Україна, 1996. – 54 с.
3. Комп'ютерна злочинність: Навч. посіб. – К.: Атіка. 2006 р. – К.: Україна. – 235 с.
4. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України»» від 6 грудня 2001 р. № 1193/2001.
5. Указ Президента України «Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України» від 22 січня 2002 р. № 63/2002.
6. «Указ Президента України « Про доктрину інформаційної безпеки України» від 8 липня 2009 року. N 514/2009