УДК 007:351.778.542(477)

В. В. ЛУК'ЯНОВА, А. Ю. ЛАУТАР
Хмельницький національний університет

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Розглянуті окремі питання сутності інформаційної безпеки в умовах розвитку інформаційної системи, основні види, суб'єкти та об'єкти інформаційної системи; виділенні можливі загрози та методи забезпечення захисту інформації. Також розглянута державна система забезпечення інформаційної безпеки країни, оскільки являє собою організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Запропоновані основні форми забезпечення інформаційної безпеки держави.

Ключові слова: *безпека, інформаційне середовище, інформаційна безпека, загрози інформаційній безпеці, інформаційний патронат, інформаційна кооперація, інформаційне протиборство.*

V. V. LUKYANOVA, A. U. LAUTAR
Khmelnitsky National University

INFORMATION SECURITY IN THE DEVELOPMENT OF INFORMATION SYSTEMS

Abstract – The main goal of this work is a theoretical study of information security, its classification and definition of national interests in the field of information, identify threats such interests, their classification, search and providing optimal tools that allow for the creation of a stable system of information security.

The article deals with some issues of the nature of information security in the development of information system, basic types, subjects and objects of the information system, the allocation of possible threats and methods of protection. Also consider the state system of information security, as is the organizational merger of state and capabilities of information security, performing its functions on the basis of the law under the control and protection of the judiciary. The basic form of information security.

Thus, information security is crucial to the future of society, a complex activity that requires special prudent methodology of scientific research. This article reviewed the basic concepts of information security, their classification and possible threats. Information security is an integral part of national security, which is why various public authorities should pay special attention to guaranteeing this security, particularly in the context of steady movement developed societies to comprehensive information in all spheres of life.

Key word: *security, information environment, information security, information security threats, information patronage, information cooperation, information confrontation.*

Постановка проблеми. Проблеми інформаційної безпеки в сучасних умовах є надзвичайно актуальними і вимагають поглибленого вивчення. Характерною ознакою сучасного етапу науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх використання як у повсякденному житті, так і в управлінні державою. Інформація та інформаційні технології все більше визначають розвиток суспільства і слугують новими джерелами національної могутності. Становлення інформаційного суспільства радикально змінює геополітичну обстановку в світі, впливає на формування нових сфер життєдіяльності людства, а відтак і національної безпеки. У свою чергу, основою глобалізації стають інтеграція інформаційних систем різних держав до єдиної загальносвітової інформаційної системи, формування єдиного інформаційного простору, створення глобальних інформаційно-телекомунікаційних мереж, інтенсивне впровадження нових інформаційних технологій в усі галузі суспільного життя. Тому актуальність теми є очевидною, оскільки система інформаційної безпеки відбиває стан захищеності національних інтересів саме в інформаційній сфері від зовнішніх та внутрішніх загроз як для самої держави або суспільства, так і для конкретної людини.

Аналіз останніх досліджень і публікацій. Особливо важливі питання для осмислення інформаційної безпеки як виду соціально важливої діяльності середовища охарактеризовані в працях вітчизняних вчених: М.Б. Левицької, В.А. Ліпкана, В.П. Горбуліна, Г.В. Іващенка, Б.А. Кормича, В.М. Лопатіна, Ю.Є. Максименко, А.І. Марущака, Г.В. Новицького, А.О. Стрельцова та ін.

Мета статті. Головною метою роботи є теоретичне обґрунтування інформаційної безпеки, її класифікацію, а також визначення національних інтересів у інформаційній сфері, виявлення загроз таким інтересам, їхню класифікацію, пошук та надання оптимальних засобів, які дозволяють забезпечити створення стійкої системи інформаційної безпеки держави.

Виклад основного матеріалу дослідження. Поняття інформаційної безпеки, залежно від його використання, розглядається у декількох ракурсах (див. рис. 1).

У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. Під інформаційним середовищем [*information environment*] розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини: створення і розповсюдження вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації та дві забезпечувальні предметні частини: створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення, а також засобів і механізмів інформаційної безпеки.

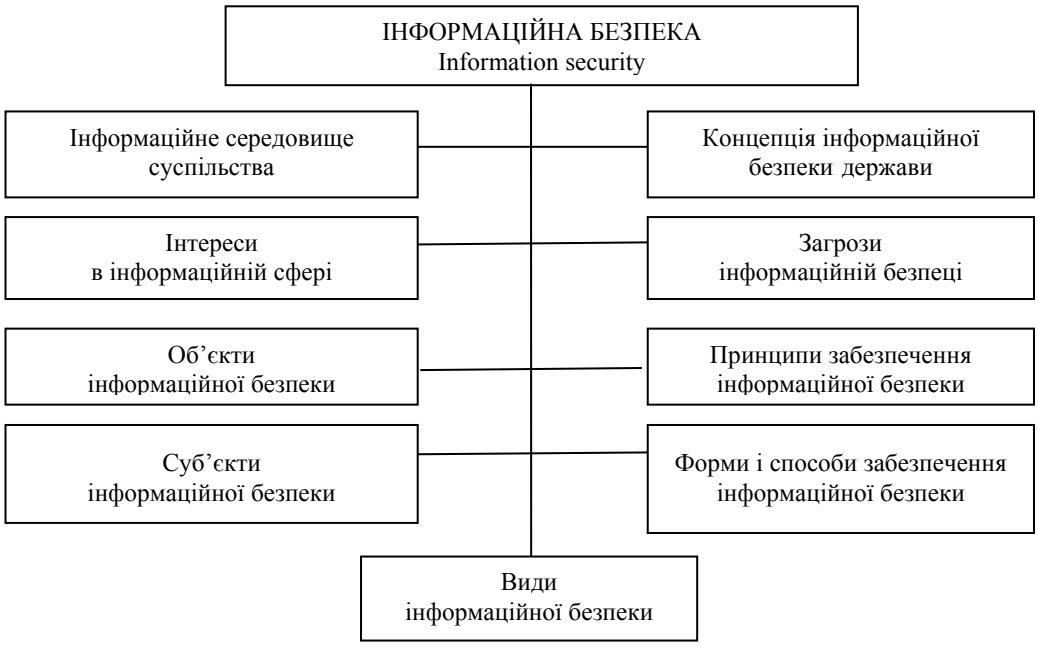

Рис. 1. Основні поняття інформаційної безпеки

Більш розгорнуте формулювання інформаційної безпеки – це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обгрунтованість рішень та дій, що приймаються [2, с. 46–48].

Залежно від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформацію та інформаційні ресурси від неправомірного впливу сторонніх осіб; інформаційні права і свободи людини і громадянина. В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [5, с. 47–49].

Об'єктами інформаційної безпеки [*information security object*] можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство.

До суб'єктів інформаційної безпеки [*information security subject*] відносяться: держава, що здійснює свої функції через відповідні органи; громадяни; суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства (рис. 2).

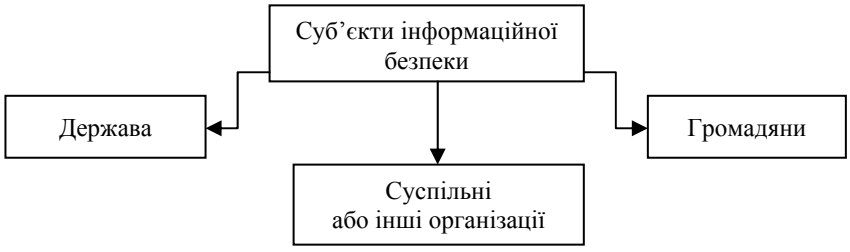

Рис. 2. Суб'єкти інформаційної безпеки

Інформаційна безпека особистості – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо.

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В концепції інформаційної безпеки держави проводиться системна класифікація дестабілізуючих факторів і інформаційних загроз безпеці особистості, суспільства і держави; обґрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції по способах і формах забезпечення інформаційної безпеки [4, с. 24–25].

Дестабілізуючі фактори [*destabilizing factor*] – явища та процеси природного і штучного походження, що породжують інформаційні загрози. Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їх об'єднання. До найбільш сильних із них відносяться ворожі держави або коаліції ворожих держав, в яких для формування інформаційних загроз створюються і функціонують спеціальні органи і служби.

Особливу групу джерел складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей і інших причин. Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації; фабрикування, розповсюдження і впровадження дезінформації [6, с. 72–73].

Загрози інформаційній безпеці [*information security threat*] – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:

− впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

− несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

− інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації тощо).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні (рис. 3) [4, с. 15].

Рис. 3. Класифікація загроз інформаційній безпеці

Під політичними факторами загроз інформаційній безпеці розуміють:

− зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;

− інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;

− становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;

− знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;

− прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;

− низька загальна правова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці інформації є:

– перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних і зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації і захисту інформації, включення інформаційної продукції в систему товарних відносин;

– критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;

– розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

– недостатня нормативно-правова база у сфері інформаційних відносин, у т.ч. в галузі забезпечення інформаційної безпеки;

– недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;

– широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;

– зростання обсягів інформації, яка передається відкритими каналами зв'язку;

– загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері [7, с. 16–17].

Державна система забезпечення інформаційної безпеки країни [*government system of national information security*] являє собою організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі. Основними завданнями такої системи є виявлення і прогнозування дестабілізуючих факторів і інформацій них загроз життєво важливим інтересам особистості, суспільства та держави; здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення; створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

На сьогодні окремі елементи системи інформаційної безпеки створені та функціонують (органи зовнішньої розвідки, інформаційні служби різноманітних міністерств, система технічного та криптографічного захисту інформації держави тощо). Проте для їх функціонування ще недостатня правова база. Зміст діяльності органів інформаційної безпеки також ще не в повній мірі відповідає покладеним на них завданням. Це пояснюється в першу чергу недостатнім опрацюванням питань, що стосуються форм і способів забезпечення інформаційної безпеки [3, с. 2–3].

Найважливіша вимога до обґрунтування способів, форм і механізмів їх реалізації полягає в абсолютному верховенстві права у будь-якій, в тому числі і політичній діяльності. У свою чергу, кожний суб'єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, добре уявляти наслідки свої дій для інших суб'єктів та міру відповідальності на випадок порушення їхніх життєво важливих інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється відповідно у формах інформаційного патронату та інформаційної кооперації, у другому – у формі інформаційного протиборства (рис. 4).

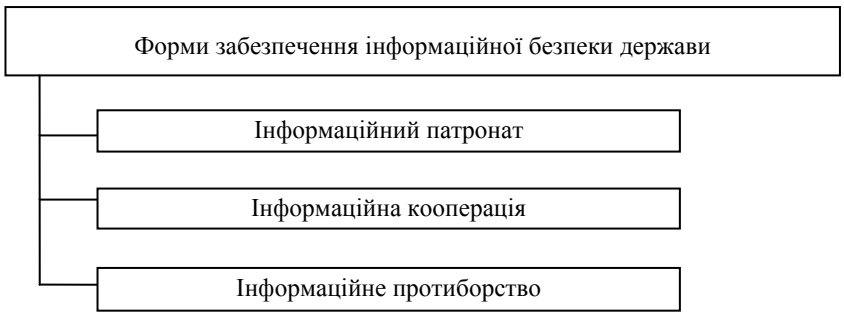

Рис. 4. Основні форми забезпечення інформаційної безпеки держави

Інформаційний патронат [*information patronage*] (лат. *patronatys* від *patronys* – захисник) – форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) і власне захист життєво важливих інтересів цих осіб від інформаційних загроз або, як ще кажуть, – інформаційний захист [1, с. 41–42]. При цьому інформаційне забезпечення інформаційної безпеки [*information support of information security*] включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхню обробку, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки. Його основу складає збір (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контр розвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

Інформаційний захист [*infosecurity*] досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційна кооперація [*information cooperation*] (лат. *cooperatio*, від *coopero* – співробітничаю) – форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі і інформаційні загрози та захист від них доступними законними способами і засобами.

Для конкретної особистості такими способами і засобами можуть бути:

− судовий захист прав і свобод у використанні інформації;

− адміністративний захист її життєво важливих інтересів у інформованості з боку територіальних або відомчих органів інформаційної безпеки;

− автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці.

Це ж характерно і для суспільних об'єднань, організацій (підприємств). Разом із тим, при наявності у них власних органів інформаційної безпеки, їхні можливості у сфері автономного захисту суттєво розширюються [8, с. 220–225].

Висновки. Забезпечення інформаційної безпеки є визначальною для майбутнього суспільства, комплексною діяльністю, що потребує особливої виваженості методології її наукових досліджень. У даній статті були розглянуті основні поняття інформаційної безпеки, їх класифікація та можливі загрози. Інформаційна безпека є невід'ємною складовою безпеки національної, саме тому різні органи державної влади повинні приділяти особливу увагу гарантуванню цієї безпеки, особливо в контексті неухильного руху розвинених суспільств до всеохоплюючої інформатизації всіх сфер життєдіяльності.

Література

1. Борсуковский Ю. Подходы и решения: информационная безопасность / Ю. Борсуковський // Мир денег. – 2001. – № 5. – С. 41–42

2. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О. М. Горбатюк // Вісн. Київ. нац. ун-ту ім. Т. Шевченка. – 1999. – Вип. 14: Міжнародні відносини. – С. 46–48.

3. Гуцалюк М. Інформаційна безпека України: нові загрози / М. Гуцалюк // Бизнес и безопасность. – 2003. – № 5. – С. 2–3.

4. Кормич Б. Інформаційна безпека: організаційно-правові основи : навч. посібник / Б. Кормич. – К. : Кондор, 2005. – С. 382.

5. Литвиненко О. Інформація і безпека / О. Литвиненко // Нова політика. – 1998. – № 1. – С. 47–49.

6. Пилипенко О. Формула безопасности: информационная безопасность / О. Пилипенко // CHIP. – 2005. – № 12. – С. 72–74.

7. Система забезпечення інформаційної безпеки України // Національна безпека і оборона. – 2001. – № 1. –С. 16–28

8. Інформаційна безпека України: проблеми та шляхи їх вирішення // Національна безпека і оборона. – 2001. – № 1. – С. 60–69.

References

1. Borsukovskyy Yu. Podkhodu y reshenyya: ynformatsyonnaya bezopasnost' / Yu. Borsukovs'kyy // Myr deneh. – 2001. – № 5. – C. 41–42.

2. Horbatyuk O. M. Suchasnyy stan ta problemy informatsiynoyi bezpeky Ukrayiny na rubezhi stolit'/ O. M. Horbatyuk // Visnyk Kyyivs'koho universytetu imeni T.Shevchenka. – 1999. – Vyp. 14 : Mizhnarodni vidnosyny. – C. 46–48.

3. Hutsalyuk M. Informatsiyna bezpeka Ukrayiny: novi zahrozy / M. Hutsalyuk // Byznes y bezopasnost'. – 2003. – № 5. – C. 2–3.

4. Kormych B. Informatsiyna bezpeka: orhanizatsiyno-pravovi osnovy : navchal'nyy posibnyk / B. Kormych. – K. : Kondor, 2005. – S. 382.

5. Lytvynenko O. Informatsiya i bezpeka / O. Lytvynenko // Nova polityka. – 1998. – № 1. – C. 47–49.

6. Pylypenko O. Formula bezopasnosty: ynformatsyonnaya bezopasnost' / O. Pylypenko // CHIP. – 2005. – № 12. – C. 72–74.

7. Systema zabezpechennya informatsiynoyi bezpeky Ukrayiny // Natsional'na bezpeka i oborona. – 2001. – № 1. –C. 16–28.

8. Informatsiyna bezpeka Ukrayiny: problemy ta shlyakhy yikh vyrishennya // Natsional'na bezpeka i oborona. – 2001. – № 1. – C. 60–69.

Надіслана/Written: 20.05.2013 р.
Надійшла/Received: 22.05.2013
Рецензент: д.е.н., проф. О. О. Орлов