

ІНФОРМАЦІЙНА БЕЗПЕКА: СУТНІСТЬ ТА ПОРЯДОК РЕАЛІЗАЦІЇ

Світлична В.Ю.

Харківський національний університет міського господарства імені О.М. Бекетова

Досліджуються питання сутності інформаційної безпеки. Висвітлюється сутність поняття «загрози інформаційній безпеці». Аналізуються джерела загроз інформаційній безпеці. Деталізуються аспекти інформаційного протиборства та інформаційної зброї. Вивчаються основні складові системи забезпечення інформаційної безпеки.

Ключові слова: інформація, інформаційна безпека, національна безпека, загрози, промисловий шпідіаж.

Постановка проблеми. В сучасних умовах інформаційної ери ХХІ ст. інформаційна безпека грає все більш вагомую роль, а питання її забезпечення стають дедалі гострішими. Стрімке впровадження інформаційних, комп'ютерних технологій у всі сфери життєдіяльності суспільства та розвиток економіки актуалізує питання визначення обґрунтованих та ефективних шляхів забезпечення інформаційної безпеки.

Процеси всеохоплюючої інформатизації розвитку країни обумовлюють активний вплив інформаційної безпеки на економічну, соціальну, політичну та інші складові її національної безпеки. Такий нерозривний зв'язок інформаційної та національної безпеки пояснюється так: «захищеність інформації та її повнота впливають на стабільність у суспільстві, забезпечення прав і свобод громадян, правопорядок і, навіть, на збереження цілісності держави» [18, с. 221].

Аналіз результатів останніх досліджень і публікацій. У наукових працях вітчизняних та зарубіжних вчених-економістів представлено численні дослідження інформаційної безпеки [6; 8; 11; 13; 15-16].

Виділення невирішених раніше частин загальної проблеми. Однак питання побудови ефективної політики забезпечення інформаційної безпеки залишаються все ще маловивченими.

Мета статті. Метою роботи є дослідження основних аспектів забезпечення інформаційної безпеки підприємств.

Викладення основного матеріалу. Динамічний розвиток економічних, політичних, соціальних подій ХХІ століття сформулювали нове уявлення про інформацію, як одного із факторів (ресурсів) виробництва. На макрорівні інформація впевнено займає позиції головного фактора могутності держави, адже здатність держави мати у своєму розпорядженні найсучасніші інформаційні технології дозволяє ефективно управляти інформацією. Володіння державою такою здатністю – шлях до подальшого нарощування своєї економічної міцності [8, с. 2].

На мікрорівні обсяг, достовірність, цілісність, якість обробки інформації визначає ефективність дій менеджменту підприємства, а, отже, актуалізує використання інформаційних технологій в управлінні грошово-кредитними, фінансовими, соціально-економічними процесами даного підприємства. «Без необхідного обсягу та якості інформації неможливо забезпечити розвиток суб'єкта господарювання на основі високотехнологічного виробництва, ефективних методів організації праці» [16, с. 34].

На сьогоднішній день існує багато підходів до визначення терміну «інформація». Так, наприклад:

– інформація – це документовані або публічні відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі [1, с. 1];

– інформація – представляє собою результат відображення та обробки в людській свідомості різноманіття навколишнього світу, відомостей про предмети, що оточують людину, явища природи, діяльність інших людей і т. п. [13, с. 23].

Всеосяжні процеси інформатизації суспільства держав світу та широке запровадження інформаційних технологій (як характерні риси нинішнього століття), їх вплив на всі сфери розвитку цих держав, висуває на перший план питання забезпечення інформаційної безпеки. Від виваженої політики інформаційної безпеки, від ступеня захищеності і достовірності інформації у сучасному світі залежить стабільність соціально-економічної ситуації держави, збереження правопорядку, забезпечення прав її громадян.

Проаналізуємо термінологію щодо інформаційної безпеки. Основні визначення сутності інформаційної безпеки продекларовано у ряді нормативно-правових актів. Так, в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 р.р.» цей термін трактується як: «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [3, с. 103]. Численні дослідники пропонують наступні точки зору щодо аналізованого терміну:

– під інформаційною безпекою підприємства пропонуємо розуміти суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [16, с. 33];

– інформаційна безпека – стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації [17, с. 23];

– інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [5, с. 54];

– інформаційна безпека – представляє собою 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 [6, с. 45];

– під інформаційною безпекою слід розуміти одну із сторін розгляду інформаційних відносин у межах інформаційного законодавства [12, с. 48].

Заслуговує на окрему увагу дослідження сутності аналізованого терміну авторами навчального посібнику «Інформаційна безпека України в умовах євроінтеграції» [11, с. 27]. Вони пропонують виді-

лити наступні три аспекти визначення сутності «інформаційна безпека» (таблиця 1).

Аналіз перелічених підходів до трактування терміну «інформаційна безпека» дозволяє виокремити її наступні сутнісні характеристики. Отже, інформаційна безпека – це: по-перше, стан захищеності інформаційного простору; по-друге, стан захищеності національних інтересів України в інформаційному середовищі; по-третє, захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі; по-четверте, суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства і держави від реальних та потенційних загроз в інформаційному просторі; по-п'яте, невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки [11, с. 36].

Отже, інформаційна безпека є однією із складових стійкого розвитку всієї держави, а процес забезпечення інформаційної безпеки необхідно розуміти як: «...одне з глобальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління» [11, с. 6].

В процесі дослідження інформаційної безпеки важливим питанням виступає моніторинг загроз та ризиків, що можуть загрожувати її ефективності.

Інформаційні загрози становлять небезпеку для індивіда, суспільства та держави. «Реалізація загроз і переростання їх у небезпеки свідчить про неефективність функціонування системи державного управління інформаційною безпекою» [11, с. 34]. Управління загрозами і небезпеками сприяє їх усуненню.

Загрози інформаційній безпеці можна трактувати як сукупність внутрішніх та зовнішніх умов, які можуть нанести шкоду інтересам особистості та суспільства через небажані інформаційні атаки на відповідні об'єкти інформаційної інфраструктури держави. Актуальність вивчення загроз інфор-

маційній безпеці підтверджує у своїй роботі і [6, с. 47]: «...Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план впливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, та вироблення механізмів протидії їм у всіх напрямках».

Виходячи з численних досліджень [5-6; 8; 11] можна виділити наступні види загроз інформаційній безпеці:

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

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

3) збої в роботі обладнання (може виникнути при блокуванні доступу до одного або декількох ресурсів інформаційної системи);

4) загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.).

Зупинимось більш детальноше на понятті «інформаційна війна». Вона представляє собою найвищий ступінь інформаційного протистояння, спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних конфліктів між державами, народами, націями та соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційної зброї. Інформаційна війна включає наступні дії:

Таблиця 1

Існуючі аспекти визначення категорії «інформаційна безпека»

Аспект	Пояснення
1. Нормативно-правовий (ґрунтується на аналізі нормативно-правових актів)	Закон України «Про Концепцію Національної програми інформатизації» інформаційну безпеку розглядає як невід'ємну частину політичної, економічної, оборонної та інших складових національної безпеки [2, с. 54]. В Законі України «Про основи національної безпеки України» поняття «інформаційна безпека» не розкривається, увага фокусується на інформаційній сфері національної безпеки, при чому, не дається визначення навіть і даного поняття, а лише перераховуються загрози та напрями державної політики у вищезазначеній сфері [4, с. 54].
2. Доктрильний (виходячи з аналізу трактувань терміну в роботах дослідників, фахівців у цій галузі)	а) під інформаційною безпекою розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [14, с. 45]; б) інформаційна безпека – безпека об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошення даних про той чи інший об'єкт, що є державною таємницею [9, с. 23]; в) інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави [10, с. 12]; г) національна інформаційна безпека України – це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних та матеріальних цінностей нації, прогресивного розвитку України, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [7, с. 10].
3. Енциклопедичний (в основі – аналіз визначень, наведених у словниках, енциклопедіях)	Інформаційна безпека означає: законодавче формування державної інформаційної політики; гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України; створення і впровадження безпечних інформаційних технологій; охорону державної таємниці, а також інформації з обмеженим доступом; захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення інформаційної продукції [19, с. 714].

Джерело: розроблено автором за даними [11, с. 27]

– здійснення впливу на телекомунікації, транспортні мережі тощо;
 – промисловий шпіонаж (порушення прав інтелектуальної власності, проведення конкурентної розвідки, розкрадання патентованої інформації);
 – хакінг (злам і використання особистих даних, інформації з обмеженим доступом) [11, с. 77].

Інформаційна зброя – є основним інструментом здійснення інформаційної війни, і представляє собою сукупність засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу протилежної сторони (руйнування її інформаційної інфраструктури, системи управління державою, зниження духовного потенціалу суспільства).

Серед найбільш серйозних завдань, які можуть вирішуватися за допомогою сучасної інформаційної зброї, можна відмітити: створення атмосфери бездуховності та аморальності; маніпулювання суспільною свідомістю та політичною орієнтацією соціальних груп населення держави з метою створення політичної напруги та хаосу; дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, загострення політичної боротьби; дезінформація населення про роботу державних органів, підірив їхнього авторитету, дискредитація органів управління; провокування соціальних, політичних, національних і релігійних сутичок тощо [5, с. 230].

Вивчення руйнівного впливу загроз інформаційній безпеці висуває на перше місце питання побудови ефективної системи її забезпечення. У сучасному світі забезпечення інформаційної безпеки повинно виступати однією з найважливіших функцій держави.

Зміст, порядок реалізації забезпечення інформаційної безпеки, інструменти, завдання та нормативне регулювання цього процесу полягають у наступному:

1. Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері.

2. Інструментом реалізації державної політики інформаційної безпеки виступає система забезпечення інформаційної безпеки. Остання представляє собою організаційне поєднання заходів (інформаційного, адміністративного, управлінського, методологічного характеру), спрямованих на забезпечення

інформаційної безпеки особистості, суспільства і держави.

3. Завданнями системи забезпечення інформаційної безпеки є:

– моніторинг, прогнозування реалізації дестабілізуючих факторів і інформаційних 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;

– вдосконалення державної політики розвитку інформаційної сфери (створення сприятливих умов розвитку національної інформаційної інфраструктури, впровадження новітніх технологій у цій сфері);

– забезпечення інформаційно-аналітичного потенціалу країни.

4. Нормативно-правове регулювання системи забезпечення інформаційної безпеки України представлено Конституцією України, Законом України «Про основи національної безпеки України», Законом України «Про інформацію», Законом України «Про Концепцію Національної програми інформатизації», Указом Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі», іншими актами.

5. Перелік функцій системи забезпечення інформаційної безпеки України: удосконалення нормативно-правового поля регулювання розвитку інформаційних ресурсів; оптимізація державної політики інформатизації; регулювання інформаційного співробітництва; контроль за встановленим порядком і правилами формування і використання інформаційних ресурсів [11; 15].

Висновки і пропозиції. Таким чином, інформаційна безпека має одне з першочергових значень для соціально-економічного розвитку держави. Україна має продовжити активні кроки на шляху розбудови власної системи інформаційної безпеки. Важливими заходами в цьому процесі мають стати організація і проведення інформаційних операцій, а також розвиток системи сертифікації інформаційних продуктів. Окрім того, система забезпечення інформаційної безпеки повинна гнучко коригуватися відповідно до мінливого характеру зовнішніх та внутрішніх факторів оточення.

Список літератури:

1. Про інформацію: [закон України: офіц. текст: за станом на 2 жовтня 1992 р., із змінами, внесеними Законом України від 10 січня 2012 р.] – [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/2657-12>
2. Про Концепцію Національної програми інформатизації: [закон України: офіц. текст: за станом на 9 січня 2007 р., із змінами, внесеними Законом України від 7 серпня 2011 р.] // Відомості Верховної Ради України (ВВР). – 2012. – № 7. – Ст. 53.
3. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 р.р.: [закон України: офіц. текст: за станом на 9 січня 2007 р.] // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – Ст. 102.
4. Про основи національної безпеки України: [закон України: офіц. текст: за станом на 19 червня 2003 р., із змінами, внесеними Законом України від 13 жовтня 2012 р.] // Відомості Верховної Ради України (ВВР). – 2012. – № 7. – Ст. 53.
5. Богуш В. Інформаційна безпека держави / В. Богуш, О. Юдін; [Гол. ред. Ю.О. Шпак]. – К.: «МК-Прес», 2005. – 432 с.
6. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О.М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 1999. – Вип. 14: Міжнародні відносини. – С. 46-48.
7. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки / В.І. Гурковський: автореф. дис. канд. юрид. наук: 25.00.02. – К., 2004. – 22 с.
8. Гуцалюк М. Інформаційна безпека України: нові загрози / М. Гуцалюк // Бизнес и безопасность. – 2003. – № 5. – С. 2-3.
9. Данільян О.Г. Національна безпека України: сутність, структура та напрямки реалізації / О.Г. Данільян, О.П. Дзьобань, М.І. Панов. – Х.: «ФОЛІО», 2002. – 296 с.
10. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України / Б.А. Кормич: [монографія]. – Одеса: Юридична література, 2003. – 472 с.
11. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський: [навч. посібник]. – К.: КНТ, 2006. – 280 с.
12. Литвиненко О. Інформація і безпека / О. Литвиненко // Нова політика. – 1998. – № 1. – С. 47-49.

13. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика, 1997. – 125 с.
14. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) / Н.Р. Ситник, Г.П. Ситник, В.Т., В.Т. Білоус: [навч. посібник] / За заг. ред. П.В. Мельника, Н.Р. Нижника. Ірпінь, 2000. – 304 с.
15. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук. – [Електронний ресурс]. – Режим доступу: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php
16. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Економічні науки: Вісник Хмельницького національного університету 2010. – № 2. – Т. 2. – С. 32-35.
17. Хоффман Л.Дж. Современные методы защиты информации / Л.Дж. Хоффман [пер. с англ.]. – М.: Советское радио, 1980. – 57 с.
18. Щербина В.М. Інформаційне забезпечення економічної безпеки підприємств та установ / В.М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220-225.
19. Юридична енциклопедія: в 6 т.: [редкол.: Ю.С. Шемшученко та ін.]. – К.: Укр. енцикл., 1998. – 1999. – Т. 2. – С. 714.

Светличная В.Ю.

Харьковский национальный университет имени А.Н. Бекетова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СУЩНОСТЬ И ПОРЯДОК РЕАЛИЗАЦИИ

Аннотация

Исследуются вопросы сущности информационной безопасности. Освещается сущность понятия «угрозы информационной безопасности». Анализируются источники угроз информационной безопасности. Детализируются аспекты информационного противостояния и информационного оружия. Изучаются основные составные элементы системы обеспечения информационной безопасности.

Ключевые слова: информация, информационная безопасность, национальная безопасность, угрозы, промышленный шпионаж.

Svitlychna V.Yu.

O.M. Beketov National University of Urban Economy in Kharkiv

INFORMATION SECURITY: ESSENCE AND REALIZATION ORDER

Summary

Issues of information security essence are researched. Highlights the essence of the concept of «information security threats». Main treats to information security are analyzed. Detailed aspects of information confrontation and information weapons. Essential components of information security system providing are studied.

Keywords: information, information security, national security, treats, industrial espionage.