СИСТЕМНИЙ ПІДХІД ДО ФОРМАЛІЗАЦІЇ ПОНЯТТЯ «ІНФОРМАЦІЙНА БЕЗПЕКА»

SYSTEMATIC APPROACH TO THE FORMALIZATION OF THE «INFORMATION SECURITY» DEFINITION

УДК 004.056.5

Яровенко Г.М.
к.е.н., доцент,
доцент кафедри економічної кібернетики
Сумський державний університет

Стаття присвячена дослідженню питання визначення інформаційної безпеки, що пов'язано з існуванням різних підходів до його трактування, яке породжує невизначеності стосовно розуміння її сутності. Так, в роботі було проведено аналіз етапів розвитку інформаційної безпеки. Його результати дозволили визначити такі її характеристики, як багатосуб'єктність, різноманіття сфер діяльності, існування можливостей правового регулювання з боку держави. Також було проведено узагальнення підходів до визначення інформаційної безпеки з позиції властивостей функціонування та виявлено, що її розглядають як стан, процес та сфера діяльності. Аналіз літератури дозволив сформувати також й другий напрям визначення інформаційної безпеки з позиції суб'єктів – держави, економічних агентів та особистості. Представлені підходи дозволяють трактувати інформаційну безпеку з урахуванням тільки одного її аспекту. Застосування системного підходу у роботі дозволило сформулювати визначення інформаційної безпеки, яке враховує всі її особливості, як багатоаспектної системи, а також дозволяє уникнути вузького підходу до її розуміння.
Ключові слова: *багатоаспектність, інформаційна безпека, мета функціонування, об'єкт інформаційної безпеки, системний підхід, суб'єкт інформаційної безпеки, сфера інформаційної безпеки.*

Статья посвящена исследованию вопроса определения информационной безопасности, что связано с существованием различных подходов к его трактовке, что порождает неопределенности относительно понимания ее сущности. Так, в работе был проведен анализ этапов развития информационной безопасности. Его результаты позволили определить такие ее характеристики, как многосубъектность, многообразие сфер деятельности, существование возможностей правового регулирования со стороны государства. Также было проведено обобщение подходов к определению информационной безопасности с позиции свойств ее функционирования и обнаружено, что ее рассматривают как состояние, процесс и сфера деятельности. Анализ литературы позволил сформировать также и второе направление для определения информационной безопасности с позиции субъектов – государства, экономических агентов и личности. Представленные подходы позволяют трактовать информационную безопасность с учетом только одного ее аспекта. Применение системного подхода в работе позволило сформулировать определение информационной безопасности, которое учитывает все ее особенности, как многоаспектной системы, а также позволяет избежать узкого подхода к ее пониманию.
Ключевые слова: *многоаспектность, информационная безопасность, цель функционирования, объект информационной безопасности, системный подход, субъект информационной безопасности, сфера информационной безопасности.*

The article is devoted to the study of the definition of information security, which is associated with the existence of different approaches to its interpretation, which creates uncertainty about the understanding of its essence. Thus, the analysis of the stages of information security development was carried out in the work. Its results allowed to determine such its characteristics as multi-subjectivity, diversity of spheres of activity, the existence of opportunities for legal regulation by the state. It was also generalized approaches to the definition of information security from the standpoint of the properties of functioning and found that it is considered as a state, process and area of activity. The analysis of the literature also allowed to form the second direction of determining information security from the standpoint of the subjects – the state, economic agents and individuals. The presented approaches allow to interpret information security taking into account only one of its aspects. The application of a systems approach in the work allowed to formulate a definition of information security, which takes into account all its features as a multifaceted system, and also avoids a narrow approach to its understanding.
Key words: *multidimensionality, information security, purpose of functioning, information security object, system approach, information security subject, information security sphere.*

Постановка проблеми. Наслідки четвертої промислової революції призвели до зростання інформатизації та цифровізації різних процесів та сфер життєдіяльності. З іншого боку, це сприяло виникненню можливостей щодо порушення цілісності, конфіденційності та доступності інформації по відношенню до різних суб'єктів – держави, економічних агентів, окремих індивідів. Для забезпечення попередження подібних інцидентів й з'явилася потреба у формуванні та впровадженні системи інформаційної безпеки на різних рівнях функціонування суспільства, для різних сфер життєдіяльності та суб'єктів. Особливо дана проблематика є актуальною для економіки, оскільки зараз спостерігається тенденція її стрімкої цифровізації, тому більшість загроз, що виникають, спрямовані на отримання персональної фінансової інформації та інформації суб'єктів господарювання, що врешті призводить до її втрат та здійснення додаткових витрат на її відновлення та відшкодування. Тому формування та впровадження дієвих превентивних заходів для захисту

інформації та даних є важливою задачею для інформаційної безпеки. Але це можливо тільки тоді, коли є чітке розуміння її сутності, що виражається через формулювання поняття. Оскільки тільки в останнє десятиліття зросла активність щодо здійснення наукових досліджень з проблем інформаційної безпеки, то за часту в науковій літературі спостерігається існування різних підходів та напрямів щодо її трактування, які мають певні недоліки, що сприяють некоректному розумінню досліджуваного об'єкта. Для їх усунення та формалізації поняття інформаційної безпеки й буде присвячене дане дослідження.

Аналіз останніх досліджень і публікацій. Проблематикою інформаційної безпеки в науковій літературі почали займатися з 1967 року, коли було опубліковано першу публікацію, індексовану у базі даних Scopus, у матеріалах 1-го симпозіуму з принципів операційних систем, який було проведено Асоціацією обчислювальних машин. За період з 1967 року по 2017 рік було опубліковано 16543 дослідження, які було присвячено питанням інформаційної безпеки, при чому найбільше зростання їх кількості відбулося тільки з 2000 року [1]. Найбільший науковий внесок у вирішення проблематики інформаційної безпеки належить таким закордонним науковцям, як: Р. Вон Солмс, А. Ахмад, Н. Милославська, Х. Рао, Дж. Ченг, Р. Аміртраджан, Дж. Елофф, Х. Пен, С. Фенц та інші [1].

Слід відмітити, що вітчизняні науковці також приділяють увагу вивченню різних аспектів інформаційної безпеки. Так, її правовий базис досліджували Б. Кормич [2], В. Петрик [3]; її психологічний вплив на окремих індивідів та державу в цілому – У. Ільницька [4]; її проблеми, вплив, наслідки та шляхи вирішення для суб'єктів підприємницької діяльності – Т. Микитенко, І. Петровська, П. Рогов, А. Гаркуша [5]; М. Зубок [6]; її формування як основа національної безпеки – І. Боднар [7]; її понятійний апарат – В. Остроухов, В. Петрик [8], та інші. Хоча питання інформаційної безпеки є досить актуальним та досліджується для різних сфер життєдіяльності суспільства, але в наукових публікаціях існує ряд невизначеностей, пов'язаних із відсутністю єдиних підходів до трактування її поняття, що впливає на подальше розуміння її сутності. Саме цей аспект потребує уточнення та ретельного вивчення.

Метою даного дослідження є аналіз етапів розвитку інформаційної безпеки та підходів до її визначення задля формалізації та розробки власного поняття на основі системного підходу.

Виклад основного матеріалу дослідження. Зростання рівня інформатизації та комп'ютеризації суспільства призвело до необхідності появи інформаційної безпеки. Вважається, що це було пов'язано із потребою захисту інформації про торгові угоди, майно, фінансові операції, тощо, яка фіксувалася на офіційних паперах до початку 19 сторіччя. Тобто її необхідно було вберегти від фізичних пошкоджень та викрадення злочинцями. Із розповсюдженням радіо- та електрозв'язку з'явилась необхідність у захисті даних, які передавалися, від сторонніх впливів. Особливо це було важливо в умовах ведення країнами військових дій, в результаті чого почали вдаватися до кодування та декодування сигналів. Починаючи із 1935 року, коли активно розроблялися та використовувалися засоби радіолокації та гідроакустики, акцент безпеки змістився на підвищення їх захисту шляхом створення маскувально-імітувальних перешкоджальних засобів. Впровадження перших електронно-обчислювальних комп'ютерів у практичну діяльність на при кінці 40-х та на початку 50-х років 20-го сторіччя, сприяли формуванню нових завдань інформаційної безпеки, пов'язаних із розробкою заходів, що обмежували на фізичному рівні доступ до пристроїв збору, обробки та виведенням інформації [9; 10].

Початком формування інформаційної безпеки, як окремого самостійного напряму розвитку інформаційних систем, є шістдесяті роки 20-го сторіччя, оскільки саме в той час у суспільстві та фінансово-господарській діяльності компаній масово стали траплятися випадки втрати інформації через зовнішні та внутрішні джерела, що було обумовлено створенням локальних мереж (рис. 1). Множина таких інцидентів призвела до того, що більшість підприємств почали впроваджувати нові інструменти захисту. Основним із них було створення паролів доступу користувачів у відповідності із їх функціональними обов'язками.

Сімдесяті роки 20-го сторіччя пов'язані із появою перших хакерських атак, що стало можливим за рахунок використання телефонних ліній, за допомогою яких великі організації з'єднували комп'ютери (рис. 1). Також в ці роки відбувався розвиток проекту ARPANET (Мережа агентства з перспективних дослідницьких проектів), що сприяло появі першого комп'ютерного хробака "CREEPER" (розробники Боб Томас та Рей Толінсон) та першого антивірусного програмного забезпечення "Reaper" (розробник Рей Толінсон) [11; 12].

Вісімдесяті роки 20-го сторіччя характеризуються активізацією комп'ютерних мереж, розповсюдженням ARPANET, який перетворився на світову мережу Інтернету (рис. 1). Хакерство почало охоплювати різні сфери діяльності людини. Найбільшою подією, яка отримала назву «414-ті», було зламування більше 400 військових комп'ютерів, що було виконано російськими спецслужбами з метою викрадення американських військових таємниць. Це був початок застосування кіберзброї однією державою проти іншої. Саме тоді уряди країн почали залучатися до вирішення питань інформаційної безпеки. Також протягом

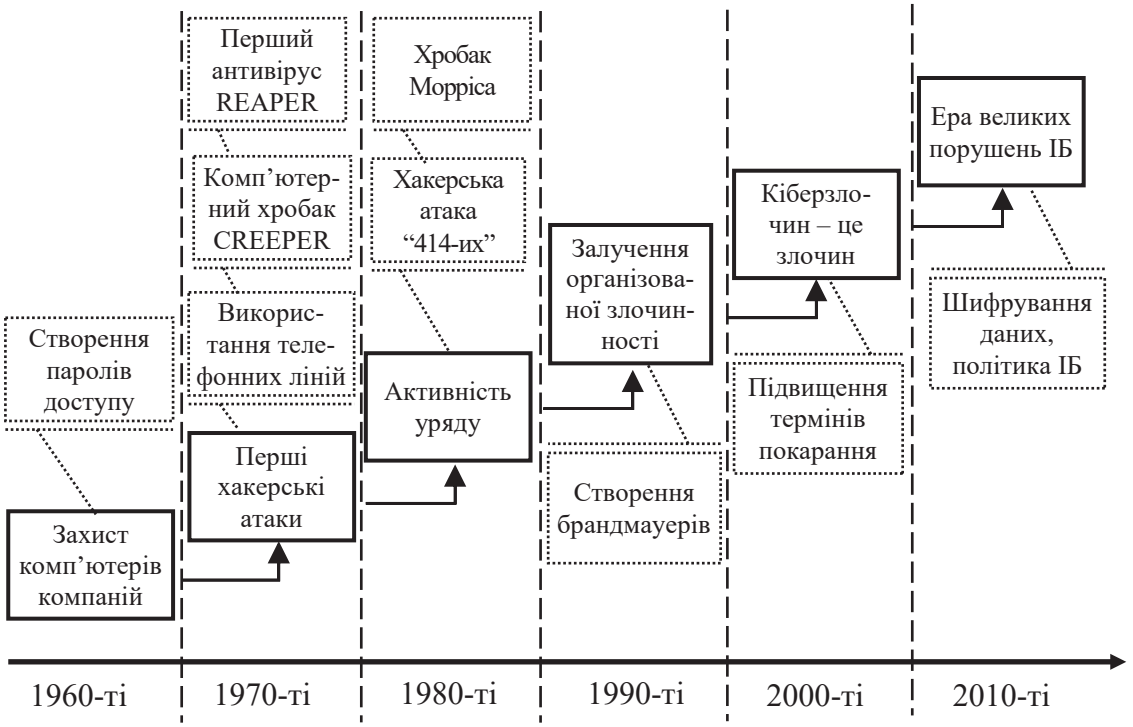

Рис. 1. Етапи розвитку інформаційної безпеки

Джерело: складено автором на основі [11; 12]

даного десятиліття Робертом Моррісом було створено комп'ютерного хробака, від дій якого було завдано серйозні збитки великої кількості компаній, в результаті чого до винахідника вперше застосували правову відповідальність та висунули звинувачення згідно розробленого та впровадженого «Закону про комп'ютерне шахрайство та зловживання» [11; 12].

Після того, як Інтернет набув масового розповсюдження та став доступним для будь-яких груп користувачів, масово з'явились випадки шахрайств, пов'язаних із викраденням особистої інформації, що відбувалось організованими злочинними групами. В результаті для захисту були створені брандмауери, які знижали кількість хакерських атак (рис. 1). Це призвело до зміни законодавства, згідно з яким кібрзлочини каралися на рівні із іншими видами тяжких злочинів, тобто з'явилася кримінальна відповідальність. Але починаючи з 2010 року, кількість кіберзлочинів тільки зростає, при чому відбувається ускладнення технологій, які застосовуються для їх здійснення.

Тобто інформаційна безпека існувала в різні епохи розвитку суспільства, починаючи від паперових технологій та завершуючи програмно-технічними комплексами; вона стосується різних сфер діяльності та впроваджується з метою попередження втрат інформації та кіберзлочинності, а також порушення якої пов'язано із кримінальною відповідальністю. Отримані знання щодо історичного розвитку інформаційної безпеки дозволили провести аналіз існуючих підходів до його визначення. Можна виділити два напрями.

Перший стосується підходів, які визначають інформаційну безпеку, виходячи з її властивостей функціонування, як стану, процесу та сфери діяльності. Результати його узагальнення наведені у таблиці 1. Перший підхід пов'язує інформаційну безпеку із станом захищеності, що не зовсім вірно, оскільки вона забезпечує його, використовуючи різні засоби. Тобто подібні визначення роблять акцент на мету функціонування інформаційної безпеки. Другий підхід передбачає те, що інформаційна безпека є процесом, який включає застосування різного роду програмних, технічних, правових, інформаційних та організаційних інструментів для забезпечення функціонування її основної мети. Також некоректним буде вважати інформаційну безпеку тільки процесом, тобто послідовністю виконання дій щодо захисту, оскільки вона може передбачати реалізацію ряду взаємопов'язаних процесів, спрямованих на виявлення та попередження загроз. Третій підхід є досить широким, оскільки наголошує, що інформаційна безпека є мультидисциплінарною сферою. Хоча можна погодитися із тим, що вона є саме сферою діяльності, але такий підхід робить її тільки певним різновидом надання послуг. Тобто представлені поняття тільки відображають один аспект інформаційної безпеки, пов'язаний з її функціонуванням, та не розкривають інші, які є досить важливими для розуміння її сутності.

Оскільки наслідки інформаційних загроз, попередження яких є головною задачею інформаційної безпеки, є суттєвими для суспільства, то не погоджуємося із такими трактуваннями в повній мірі, оскільки вони знижують цінність інформаційної безпеки для суспільства.

Другий напрям відображає підходи, які акцентують увагу на суб'єктах інформаційної безпеки, які її забезпечують, а саме держави, економічних агентів, особистості (див. табл. 2).

В даному випадку акцент робиться тільки на тому, хто впроваджує її, регулює та використовує. Також дані поняття не враховують спільні риси безпеки для різних суб'єктів, які дозволяють використовувати загальні підходи та інструменти в процесі організації захисту інформації. Все це обмежує розуміння даного поняття тільки на рівні окремого суб'єкта чи окремої сфери.

Виходячи із проведеного аналізу та синтезу отриманої інформації, узагальненої в таблицях 1 та 2, застосуємо системний підхід, які дозволить сформувати поняття інформаційної безпеки з урахуванням недоліків окремих підходів. З цією метою виділимо риси, характерні для більшості визначень інформаційної безпеки, та представимо їх у вигляді схеми (рис. 2).

Тобто системний підхід передбачає розгляд та дослідження будь-яких систем з позиції мети їх функціонування, суб'єктів, які приймають участь у її забезпеченні, об'єктів, які функціонують у певній сфері діяльності, та на яких направлено інструменти впливу, а також механізмів, які забезпечують виконання та регулювання системи. Згідно із цим, на рисунку 2 представлені основні компоненти інформаційної безпеки, як системи, що дозволило сформулювати власне поняття інформаційної безпеки: інформаційна безпека – це комплексна система, мета функціонування якої – захист об'єктів (інформація, знання, інформаційні системи), що належать до фінансово-господарської, політичної, військової, технологічної сфер діяльності, від різного роду загроз (несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення) із застосуванням програмних, технічних, методичних, інформаційних та правових засобів, що використовують окремі особи або спе-

Таблиця 1

Узагальнення підходів до визначення інформаційної безпеки з позиції властивостей функціонування

Зміст підходу	Автор або джерело	Визначення інформаційної безпеки
Інформаційна безпека, як стан	Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [13]	Це «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»
	Кормич Б.А. [2, с. 109]	Це «стан захищеності встановлених законодавством норм, параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини, суспільства як суб'єктів процесів та відносин»
	Петрик В. [3, с. 122]	Це «стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток, технічний, інтелектуальний, соціально-політичний, морально-етичний, за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди»
Інформаційна безпека, як процес	ISO/IEC 27000:2009 [14]	Це «збереження конфіденційності, цілісності та доступності інформації. Примітка. Крім того, можуть бути задіяні й інші властивості, такі як достовірність, підзвітність, відмова та надійність»
	SNSS [15]	Це «захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації, знищення для забезпечення конфіденційності, цілісності та доступності»
	ISACA [16]	Вона «забезпечує таким чином, що лише авторизовані користувачі (конфіденційність) мають доступ до точної та повної інформації (цілісність), коли це потрібно (наявність)»
	SANS Institute [17]	Вона «відноситься до процесів та методологій, які розроблені та впроваджені для захисту друкованої, електронної чи будь-якої іншої форми, приватної та конфіденційної інформації, чи даних від несанкціонованого доступу, використання, розкриття, зловживання, знищення, модифікації чи порушення»
Інформаційна безпека, як сфера діяльності	Cherdantseva Y., Hilton J. [18]	Це «мультидисциплінарна сфера вивчення та професійної діяльності, яка займається розробкою та впровадженням усіх доступних типів механізмів безпеки (технічних, організаційних, орієнтованих на людину, юридичних) з метою збереження інформації у всіх її місцях (усередині та поза периметром організації) і, отже, в інформаційних системах, де інформація створюється, обробляється, зберігається, передається та знищується, вільна від загроз»

Таблиця 2

Узагальнення підходів до визначення інформаційної безпеки з позиції суб'єкту

Зміст підходу	Автор або джерело	Визначення інформаційної безпеки
Інформаційна безпека держави	Ільницька У. [4, с. 28]	Це «інтегрована складова національної безпеки і її розглядають як пріоритетну функцію держави»
	Боднар І.Р. [7, с. 69]	Це «сукупність засобів забезпечення інформаційного суверенітету України, які забезпечують захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз та ефективну протидію сукупності інформаційних загроз»
Інформаційна безпека економічних агентів	Микитенко Т.В., Петровська І.О., Рогов П.Д., Гаркуша А.О. [5, с. 25]	Це «одна із складових частин економічної безпеки, яка формує модель захищеності підприємства. Забезпечення (у тому числі і гарантія) безпеки підприємства пов'язана з інформаційною безпекою внаслідок широкого використання інформаційних технологій в його діяльності»
	Зубок М.І. [6, с. 78]	«Інформаційну безпеку підприємницької діяльності можна розуміти, як стан інформаційної роботи суб'єктів підприємництва за якого забезпечується ефективне інформаційне супроводження їх діяльності, надійний захист інформаційного ресурсу та результативна протидія негативному інформаційно-психологічному впливу на них»
Інформаційна безпека особистості	Остроухов В., Петрик В. [8, с. 136]	«Інформаційна безпека особистості – це: 1) належний рівень теоретичної і практичної підготовки особистості, при якому досягається захищеність і реалізація її життєво важливих інтересів і гармонійний розвиток незалежно від інформаційних загроз; 2) здатність держави створити можливості для гармонійного розвитку і задоволення потреб особистості в інформації, незалежно від інформаційних загроз; 3) гарантування, розвиток і використання інформаційного середовища в інтересах особистості; 4) захищеність від різного роду інформаційних небезпек»

ціалізовані підрозділи та фахівці державних органів, економічних агентів.

Висновки з проведеного дослідження. Таким чином, проблематика інформаційної безпеки стала досить актуальною у наш час, що пов'язано із зростанням ризиків втрат інформації для економічних агентів, держави, особистостей, а також збільшенням кіберзлочинів та хакерських атак в різних системах. Саме тому для ефективної її організації з метою попередження різного роду інформаційних та кіберзагроз виникає потреба у розумінні її сутності через чітко сформульоване

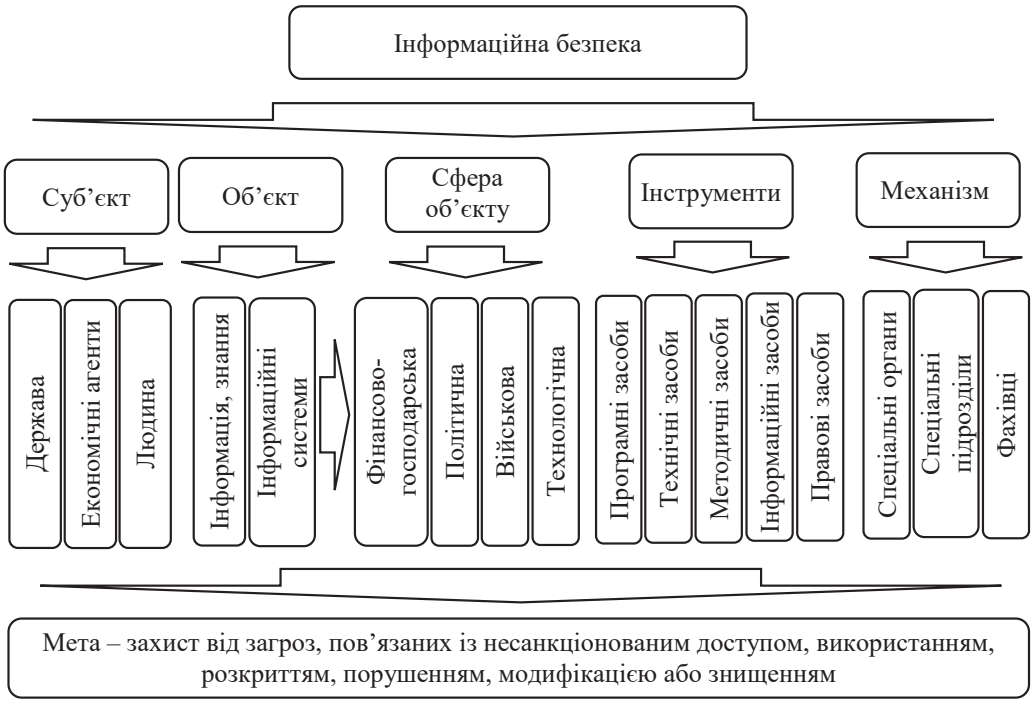

Рис. 2. Риси інформаційної безпеки

Джерело: складено автором самостійно

визначення. Для цього в роботі було проаналізовано історичні аспекти виникнення та формування інформаційної безпеки, що дозволило визначити такі її характеристики, як багатосуб'єктність, різноманіття сфер діяльності, що потребують інформаційного захисту, а також можливості правового регулювання з боку держави.

Проведений аналіз наукових підходів дозволив окреслити два напрямки щодо формулювання визначення інформаційної безпеки - з позиції властивостей функціонування та з позиції суб'єкту. В рамках визначених напрямів також було виділено різні підходи, головним недоліком яких є акцентування уваги тільки на окремій характеристиці інформаційної безпеки, що говорить про вузьке її розуміння та обмеженість щодо використання для інших суб'єктів та видів діяльності. Для уникнення визначених недоліків було запропоноване власне визначення інформаційної безпеки, яке базується на системному підході та враховує всі її особливості, як багатоаспектної системи, а також дозволяє уникнути однобічного підходу до її розуміння.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Analyze search results. Scopus : website. URL: https://www.scopus.com/term/analyzer.uri?sid=70b2c99f9b759b3ceb5320a3eb60f72c&origin=resultslist&src=s&s=TITLE-ABS-KEY%28%22information+security%22%29&sort=plf-f&sdt=b&sot=b&sl=37&count=23772&analyzeResults=Analyze+results&txGid=98de2e10bace52f678610f10474ed450 (дата звернення: 31.12.2017).

2. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. доктора юрид. наук : 12.00.07. Одеса, 2004. 427 с.

3. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Юридичний журнал. 2009. № 5. С. 122–134.

4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Гуманітарні візії. 2016. № 2(1). С. 27–32.

5. Микитенко Т.В., Петровська І.О., Рогов П.Д., Гаркуша А.О. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2014. № 1. С. 24–31.

6. Зубок М.І. Інформаційна безпека в підприємницькій діяльності. К. : ГНОЗІС, 2015. 216 с.

7. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.

8. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. Політичний менеджмент. 2008. № 4. С. 135–141.

9. Артамонова Я.С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения : дис. доктора политических наук / Московский государственный областной университет. М., 2014. 359 с.

10. Петров В.П., Петров С.В. Информационная безопасность человека и общества : учеб. пособ. М. : ЭНАС, 2007. 334 с.

11. Lynett M.A. History of Information Security From Past to Present. Hybrid Document Systems : website. URL: https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present (дата звернення: 31.12.2017).

12. Murphey D. A history of information security. IFSEC GLOBAL : website. URL: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/#:~:text=It%20was%20during%20the%201960s,how%20to%20work%20a%20computer (дата звернення: 31.12.2017).

13. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. № 537-V. Відомості Верховної Ради України. 2007. № 12. Ст. 102.

14. ISO/IEC 27000:2009(en) Information technology – Security techniques – Information security management systems – Overview and vocabulary. ISO : website. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-1:v1:en (дата звернення: 31.12.2017).

15. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010. Center for Homeland Defense and Security : website. URL: https://www.hsdl.org/?abstract&did=7447 (дата звернення: 31.12.2017).

16. Glossary of terms. ISACA : website. URL: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (дата звернення: 31.12.2017)

17. Information Security Resources. SANS : website. URL: https://www.sans.org/information-security (дата звернення: 31.12.2017).

18. Cherdantseva Y., Hilton J. Understanding Information Assurance and Security. In book: F. Almeida, and I. Portela (eds.), Organizational, Legal, and Technological Dimensions of IS Administrator. Publisher: IGI Global Publishing, 2013. P. 32. DOI: https://doi.org/10.4018/978-1-4666-4526-4.ch010