УДК 342.9
DOI: 10.33098/2078-6670.2022.13.25.133-140

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ

Шопіна Ірина Миколаївна,
доктор юридичних наук, професор,
професор кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ,
вул. Городоцька 26, м. Львів, Україна, 79000
e-mail: uaftp@ ukr.net,
ORCID: https://orcid.org/0000-0003-3334-7548

Мета. *Метою дослідження є систематизація наявних підходів до побудови дефініції інформаційної безпеки та характеристика їх сутності.* ***Методика.*** *Методологічну основу дослідження склав комплекс загальнонаукових та галузево-правових методів, об'єднаних комплексним підходом, завдяки якому вдалося розглянути феномен інформаційної безпеки у різних аспектах. Методи аналізу та синтезу, дедукції та індукції, формально-правовий метод, а також метод моделювання дозволили побудувати систему концептуальних підходів до проблеми інформаційної безпеки.* ***Результати.*** *Виокремлено та охарактеризовано десять концептуальних підходів до інформаційної безпеки: статусний, диференційний, реляціоналістський, інструментальний, протекціоністський, збережувально-забезпечувальний, процесуальний, концептуальний підхід, за якого інформаційна безпека ототожнюється зі спроможностями, діяльнісний та екзистенційний підходи. Акцентовано увагу на міждисциплінарності дослідження проблем інформаційної безпеки, яка, з одного боку, сприяє багатоаспектному її розумінню, але, з іншого боку, не дозволяє спрямувати всі зусилля на створення належного правового та нормативного підґрунтя досліджуваного феномену.* ***Наукова новизна.*** *Систематизовано існуючі у теоретичних джерелах методологічні підходи до інформаційної безпеки, охарактеризовано їх сутність, обґрунтовано думку щодо негативного впливу відсутності нормативного підходу до досліджуваного феномену на розвиток і правове закріплення цієї категорії.* ***Практична значимість.*** *Результати дослідження можуть бути використані у подальших інформаційно-правових дослідженнях як методологічна база подальшого опрацювання проблем інформаційної безпеки, а також у навчальному процесі.*

Ключові слова: *інформаційна безпека, концептуальні підходи, діяльнісний підхід, статусний підхід, диференційний підхід, інструментальний підхід, процесуальний підхід.*

Iryna Shopina
Doctor of Law, Professor, Professor of Department of Administrative and Legal Disciplines of Lviv State University of Internal Affairs,
26 Horodotska Street, Lviv, Ukraine, 79000
e-mail: uaftp@ ukr.net,

THE CONCEPT OF INFORMATION SECURITY: CONCEPTUAL APPROACHES TO DEFINITION

Purpose. *The purpose of the study is to systematize approaches to building a definition of information security and characterize their essence.* ***Methods.*** *The methodological basis of the study was a set of general scientific and industry-legal methods, united by an integrated approach, thanks to which it was possible to consider the phenomenon of information security in different aspects. The methods of analysis and synthesis, deduction and induction, the formal legal method, as well as the modeling method made it possible to build a system of conceptual approaches to the problem of information security.* ***Results.*** *Ten conceptual approaches to information security are identified and characterized: status, differential, relational, instrumental, protectionist, savings-providing, procedural, conceptual approach, in which information security is identified with opportunities, activity and efficiency. Attention is focused on the interdisciplinary of the study of information security problems. Interdisciplinary promotes a multidimensional understanding of information security, but does not allow all efforts to be directed towards creating an appropriate legal and regulatory framework.* ***Scientific novelty.*** *The methodological approaches to information security that exist in theoretical sources are systematized, their essence is characterized, the idea is substantiated by the negative impact of the lack of a normative approach to the phenomenon under study on the development and legal consolidation of this category.* ***Practical significance****.*

The results of the study can be used in further information and legal research as a methodological basis for further processing of information security problems, as well as in the educational process.

Key words: *information security, conceptual approaches, activity approach, status approach, differential approach, instrumental approach, procedural approach.*

Постановка проблеми. Повномасштабна збройна агресія Російської Федерації проти України актуалізувала проблеми зміцнення інформаційної безпеки держави і громадянського суспільства. Разом з тим будь-яка діяльність, спрямована на удосконалення певних явищ та процесів, може бути ефективною лише за умови усвідомлення їх сутності.

Однак, не зважаючи на наявність легального і численних доктринальних визначень інформаційної безпеки, розуміння цього феномену відрізняється у досить широкому діапазоні у різних авторів. За таких умов, для напрацювання теоретико-методологічного підґрунтя означеної проблематики, уявляється доцільним систематизація наявних підходів до сутності інформаційної безпеки у вітчизняній і зарубіжній науковій літературі.

Аналіз останніх досліджень і публікацій. Проблематика, пов'язана із визначенням дефініції інформаційної безпеки, була предметом наукових досліджень таких авторів, як І. Арістова, К. Бєляков, О. Довгань, О. Дзьобань, О. Золотар, Р. Калюжний, О. Качан, В. Клочко, Б. Кормич, Є. Магда, А. Марущак, О. Мартин, А. Мащенко, О. Олійник, Є. Скулиш, О. Соснін, М. Требін, Н.Тульба, В. Цимбалюк та ін. Разом з тим, з огляду на складність та багатоаспектність питань визначення сутності інформаційної безпеки, вказана проблематика потребує подальшого розвитку.

Постановка завдання. Систематизувати наявні підходи до побудови дефініції інформаційної безпеки та охарактеризувати їх сутність.

Виклад основного матеріалу дослідження. Вважається, що одне із перших визначень поняття інформаційної безпеки було сформульовано у 1980 році Л. Дж. Хоффманом. Автор вважав, що інформаційна безпека – це стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації [1, с.34]. Вказана дефініція, сформульована ще у доцифрову епоху, виявилася надзвичайно стійкою – не зважаючи на активний розвиток інформаційного права та його термінологічної бази, сприйняття інформаційної безпеки як стану інформації або стану захищеності цієї інформації є найбільш поширеним з-поміж інших підходів до сутності досліджуваного феномену. Так, на думку Б.А. Кормича, інформаційна безпека – це стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин [2, с. 109]. Поняття інформаційної безпеки як стану знайшло своє відображення у чинній Стратегії інформаційної безпеки, відповідно до якої інформаційна безпека України - складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [3]. Додамо, що, відповідно до ч.4 ст.3 Закону України

«Про національну безпеку України», державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо [4]. З цього законодавчого положення ми можемо зробити висновок, що інформаційна безпека є видом національної безпеки. Отже, як перше за часом виникнення, так і легальне визначення поняття інформаційної безпеки базуються на статусному підході, за якого досліджуваний феномен розуміється як актуальний стан інформації (відомостей, ресурсів) або актуальний стан захищеності останніх.

Близьким до статусного підходу є концептуальний підхід, за якого інформаційна безпека сприймається як рівень захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від зовнішніх та внутрішніх загроз [5, с.223]. Якщо статусний підхід обмежується констатацією певного становища інформаційної безпеки, то сприйняття її як рівня передбачає певне оцінювання, диференціацію. Це дає змогу виокремити диференційний підхід до визначення інформаційної безпеки, сутність якого полягає у визначенні її рівнів у певних суб'єктів та у певні проміжки часу.

Досить поширеним у теоретичних джерелах є підхід, за якого досліджуване явище розуміється як суспільні (соціальні) відносини. Так, Р. Калюжний та В. Цимбалюк вважають, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації [6, с.110]. О. Крюков формулює визначення інформаційної безпеки як суспільних правовідносин щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільних правовідносин, пов'язаних з організацією технологій створення, розповсюдження, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави [7, с.3]. На нашу думку, обидва визначення мають надзвичайно широкий характер, відносячи до складу інформаційної безпеки явища, які скоріше охоплюються категорією «інформаційна діяльність». Разом з тим, оскільки право, відповідно до класичного підходу, регулює саме суспільні відносини, розуміння інформаційної безпеки саме як відносин уточнює предмет правового регулювання, полегшуючи завдання як науковця, так і нормотворця. Так, виходячи із положень вказаного підходу, А. Ландіна досить вдало, на нашу думку, формулює поняття інформаційної безпеки як об'єкта злочинного посягання – це врегульований нормами права порядок суспільних відносин у частині реалізації інформаційної потреби фізичних та юридичних осіб, суспільства, держави, проти якого спрямоване суспільно небезпечне діяння [8, с.359]. Отже, реляціоналістський (від англ. relationalism – юридичний реалізм) підхід обумовлює сприйняття інформаційної безпеки як виду суспільних правовідносин, що виникають в інформаційній сфері на основі актів інформаційного законодавства з метою приведення об'єктів інформаційної безпеки у бажаний для держави і суспільства стан.

Досить цікавим є інструментальний підхід, за якого інформаційна безпека сприймається як сукупність засобів забезпечення інформаційного суверенітету України, захисте інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз [9, с.63]. Додамо, що він також знайшов відображення у правових актах, так, у Положенні про

організацію системи внутрішнього контролю в банках України та банківських групах інформаційна безпека розуміється як комплекс організаційних, програмних і техніко-технологічних засобів, що функціонують на всіх організаційних рівнях банку та забезпечують захист інформації від випадкових та/або навмисних загроз, наслідком реалізації яких може стати порушення доступності, цілісності, конфіденційності інформації щодо діяльності банку або його клієнтів [10].

У зарубіжних теоретичних джерелах досить розповсюдженим є протекціоністський підхід, у межах якого інформаційна безпека ототожнюється із захистом. Так, інформаційна безпека визначається як захист інформації, системи та апаратного забезпечення, які використовують, зберігають і передають інформацію, для забезпечення цілісності, конфіденційності та доступності даних, а також захищені операційні процедури [11]. Інформаційна безпека визначається також як ступінь захисту, інтеграції та доступності інформації та засобів її обробки [12, с.108]. На думку українських вчених О. Дзьобаня та Є. Мануйлова, яких також можна віднести до прихильників протекціоністського підходу, інформаційна безпека – це і захист інформації, і захист від інформації [13, с.50.]. Отже, протекціоністський підхід до сутності інформаційної безпеки обумовлює сприйняття останньої як захисту інформації (інформаційних ресурсів, систем, засобів забезпечення) та захисту людини та суспільства від деструктивних інформаційних впливів.

Слід також відмітити наявність збережувально-забезпечувального підходу, за якого інформаційна безпека визначається як збереження конфіденційності, цілісності та доступності інформації; а також інших її властивостей, таких, як автентичність, підзвітність, невідмовність [14, с.1]. На думку О. Литвиненка під інформаційної безпекою слід розуміти єдність трьох елементів: забезпечення захисту інформації; забезпечення захисту й контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [15]. На нашу думку, у Положенні про захист інформації та кіберзахист у платіжних системах, затвердженому Постановою Національного банку України від 19 травня 2021 року №43, також знайшов своє відображення вказаний підхід («інформаційна безпека - збереження конфіденційності, цілісності та доступності інформації» [16] – визначено у згаданому нормативно-правовому акті). Отже, збережувально-забезпечувальний підхід формує уявлення про інформаційну безпеку як про збереження і забезпечення істотних властивостей інформації, зокрема, її цілісності, доступності, автентичності, конфіденційності.

Процесуальний підхід представляє інформаційну безпеку як процес або сукупність процесів, які виникають і протікають в інформаційних та соціальних системах і призначені для досягнення цілей публічного управління в інформаційній сфері. Так, О.Шумейко вважає, що інформаційна безпека – це одна з характеристик інформаційної системи, тобто інформаційна система на певний момент часу володіє деяким станом (рівнем) захищеності, а захист інформації – це процес, який повинен виконуватися неперервно на всьому протязі життєвого циклу інформаційної системи [17, с.2].

У межах концептуального підходу, за якого інформаційна безпека ототожнюється зі спроможностями, акцент робиться на можливості соціальних та інформаційних систем ефективно функціонувати за умов активізації зовнішніх та внутрішніх загроз. Так, К. Захаренко визначає інформаційну безпеку як спроможність системи протистояти випадковим або навмисним внутрішнім і зовнішнім загрозам [18, с.212].

У межах діяльнісного підходу інформаційна безпека ототожнюється з діяльністю або комплексом дій з інформаційними ресурсами або системами. Так, польські дослідники

поняття інформаційної безпеки визначають як сукупність дій, методів і процедур, здійснюваних уповноваженими особами і спрямованих на забезпечення цілісності збирання, зберігання та обробки інформаційних ресурсів шляхом їх захисту від небажаного, несанкціонованого поширення, модифікації або знищення [19].

Екзистенційний підхід зосереджує увагу на внутрішньому суб'єктивному сприйнятті інформаційної безпеки, породжуючи поняття «відчутна інформаційна безпека», яка визначається як суб'єктивна ймовірність, з якою споживачі інформації вважають, що їхня особиста інформація не буде переглядатися, зберігатися або змінюватися неналежними сторонами під час транспортування або зберігання у спосіб, що відповідає їхнім впевненим очікуванням [20].

Як можна побачити, серед описаних підходів відсутній нормативний. Слід звернути увагу на міждисциплінарність дослідження проблем інформаційної безпеки, яка, з одного боку, сприяє багатоаспектному її розумінню, але, з іншого боку, не дозволяє спрямувати всі зусилля на створення належного правового та нормативного підґрунтя досліджуваного феномену.

Висновки. На підставі викладеного вище можна констатувати, що перше за часом виникнення визначення поняття інформаційної безпеки базуються на статусному підході, за якого досліджуваний феномен розуміється як актуальний стан інформації (відомостей, ресурсів) або актуальний стан захищеності останніх. Диференційний підхід до визначення інформаційної безпеки дає змогу визначити рівні її розвитку у певних суб'єктів та у певні проміжки часу. Реляціоналістський підхід обумовлює сприйняття інформаційної безпеки як виду суспільних правовідносин, що виникають в інформаційній сфері на основі актів інформаційного законодавства з метою приведення об'єктів інформаційної безпеки у бажаний для держави і суспільства стан. У межах інструментального підходу інформаційна безпека сприймається як сукупність засобів, застосування яких дозволяє досягти поставлених у системі публічного управління інформаційною сферою цілей. Протекціоністський підхід до сутності інформаційної безпеки обумовлює сприйняття останньої як захисту інформації (інформаційних ресурсів, систем, засобів забезпечення) та захисту людини та суспільства від деструктивних інформаційних впливів. Збережувально-забезпечувальний підхід формує уявлення про інформаційну безпеку як про збереження і забезпечення істотних властивостей інформації, зокрема, її цілісності, доступності, автентичності, конфіденційності. Процесуальний підхід представляє інформаційну безпеку як процес або сукупність процесів, які виникають і протікають в інформаційних та соціальних системах і призначені для досягнення цілей публічного управління в інформаційній сфері. У межах концептуального підходу, за якого інформаційна безпека ототожнюється зі спроможностями, акцент робиться на можливості соціальних та інформаційних систем ефективно функціонувати за умов активізації зовнішніх та внутрішніх загроз. У межах діяльнісного підходу інформаційна безпека ототожнюється з діяльністю або комплексом дій з інформаційними ресурсами або системами. Екзистенційний підхід зосереджує увагу на внутрішньому суб'єктивному сприйнятті інформаційної безпеки.

Список використаних джерел

1. Хоффман Л. Дж. Современные методы защиты информации / пер. с англ. Москва: Советское радио, 1980. 57 с.

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

3. Стратегія інформаційної безпеки: затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7

4. Про національну безпеку України: Закон України 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19

5. Форос А. В. Інформаційна безпека як складова національної безпеки України. *Правова держава*. 2019. №2. С.222-226.

6. Калюжний Р.А., Цимбалюк В.С. Координація діяльності органів влади у боротьбі з організованою кіберзлочинністю. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2002. №6. С. 105–111.

7. Крюков О.І. Інформаційна безпека держави в умовах глобалізації. *Державне будівництво*. 2007. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12.

8. Ландіна А. В. Інформаційна безпека як об'єкт злочину. *Правова держава*. 2016. № 27. С. 354-361.

9. Наливайко Л.Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. *Вісник Запорізького державного університету*. 2003. № 1. С. 60–65.

10. Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах: Постанова Національного банку України; Положення, Перелік від 02.07.2019 № 88. URL: https://zakon.rada.gov.ua/laws/show/v0088500-19/ed20190702#n25.

11. Alkhudhayr F., Alfarraj S., Aljameeli B., Elkhdiri S. Information security: A review of information security issues and techniques. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). Pp. 1-6).

12. Kirillova E. A., Yakhutlov U. M., Wenqi X., Huiting G., Suyu W. Information Security in the Management of Personnel in a Modern Organization. *In 2020 International Conference Quality Management, Transport and Information Security, Information Technologies,* pp. 107-109.

13. Дзьобань О. П. Мануйлов Є. М. Інформаційна безпека: екзистенційні аспекти і мережеві практики. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2017. №2 (33). С. 42-54.

14. Mukundan N. R., Prakash Sai L. Perceived information security of internal users in Indian IT services industry. *Information Technology and Management*. 2014. №15(1). Pp.1-8.

15. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. ... канд. політ. наук. Київ, 1997. 18 с

16. Про затвердження Положення про захист інформації та кіберзахист у платіжних системах: Постанова Національного банку України; Положення від 19.05.2021 № 43. URL: https://zakon.rada.gov.ua/laws/show/v0043500-21/ed20210519#n24

17. Шумейко О.О. Інформаційна безпека: навч. посіб. Дніпро: Дніпровський державний технічний університет, 2019. 155 с.

18. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. *Вісник Харківського національного педагогічного університету імені Г.С. Сковороди. Серія Філософія*. 2017. № 48 (1). С. 212-219.

19. Potejko P. Information security in: Wojtaszczyk, K., Materska-Sosnowska, A. (ed.), State security, ASPRA-JR publishing house, 2009.Warsaw, 194 p.

20. Chellappa Ramnath K., Paul A. Pavlou. Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information

Management, 2002. P. 358-368. URL: https://www.emerald.com/insight/content/doi/10.1108/09576050210447046/full/pdf?title=perceived-information-security-financial-liability-and-consumer-trust-in-electronic-commerce-transactions.

References

1. Khoffman, L. Dzh. (1980). *Sovremennye metody zashchyty ynformatsyy* [Modern methods of information protection] / per. s anhl. Moskva: Sovetskoe radyo, 57 p. (in Russian)

2. Kormych, B.A. (2004). *Organizational-Legal Basis of the Information Security Policy of Ukraine*: Thesis for doctor of law. Odesa, 427 p. (in Ukrainian)

3. Information security strategy: Decree of the President of Ukraine № 685/2021 (2021, December 12.). Retrived from: https://zakon.rada.gov.ua/laws/show/685/2021#n7 (in Ukrainian)

4. On the national security of Ukraine: Law of Ukraine № 2469-VIII (2018, June 21). Retrived from: https://zakon.rada.gov.ua/laws/show/2469-19 (in Ukrainian)

5. Foros, A. V. (2019). Informatsiina bezpeka yak skladova natsionalnoi bezpeky Ukrainy. [Information security as a component of national security of Ukraine]. *Pravova derzhava*, 2, pp. 222-226. (in Ukrainian)

6. Kaliuzhnyi, R.A., Tsymbaliuk, V.S. (2002). Koordynatsiia diialnosti orhaniv vlady u borotbi z orhanizovanoiu kiberzlochynnistiu. [Coordination of government activities in the fight against organized cybercrime]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)*, 6, pp. 105–111. (in Ukrainian)

7. Kriukov, O.I. (2007). Informatsiina bezpeka derzhavy v umovakh hlobalizatsii. [Information security of the state in the conditions of globalization]. *Derzhavne budivnytstvo*, 2. Retrived from: http://nbuv.gov.ua/UJRN/DeBu_2007_2_12. (in Ukrainian)

8. Landina, A. V. (2016). Informatsiina bezpeka yak obiekt zlochynu. [Information security as an object of crime]. *Pravova derzhava*, 27, pp. 354-361. (in Ukrainian)

9. Nalyvaiko, L.R. (2003). Informatsiina bezpeka ta informatsiina polityka v Ukraini: konstytutsiino-pravovyi aspekt. [Information security and information policy in Ukraine: constitutional and legal aspect]. *Visnyk Zaporizkoho derzhavnoho universytetu,* 1, pp. 60–65. (in Ukrainian)

10. On approval of the Regulations on the organization of the internal control system in banks of Ukraine and banking groups: Resolution of the National Bank of Ukraine; Regulations, List № 88 (2019, July 02). Retrived from: https://zakon.rada.gov.ua/laws/show/v0088500-19/ed20190702#n25. (in Ukrainian)

11. Alkhudhayr, F., Alfarraj, S., Aljameeli, B., Elkhdiri, S. (2019). Information security: A review of information security issues and techniques. *2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-6. (in English)

12. Kirillova, E. A., Yakhutlov, U. M., Wenqi, X., Huiting, G., Suyu, W. (2020). Information Security in the Management of Personnel in a *Modern Organization. International Conference Quality Management, Transport and Information Security, Information Technologies*, pp. 107-109. (in English)

13. Dzoban, O. P.; Manuilov, Ye. M. (2017). Informatsiina bezpeka: ekzystentsiini aspekty i merezhevi praktyky. [Information security: existential aspects and network practices]. *Visnyk NIuU imeni Yaroslava Mudroho. Seriia: Filosofiia, filosofiia prava, politolohiia, sotsiolohiia*, 2 (33), pp. 42-54. (in Ukrainian)

14. Mukundan, N. R., Prakash, Sai L. (2014) Perceived information security of internal users in Indian IT services industry. *Information Technology and Management,* 15 (1), pp. 1-8. (in English)

15. Lytvynenko, O.V. (1997). Problems of information security in post-Soviet countries (on the example of Ukraine and Russia): PhD thesis abstract, Kyiv, 18. (in Ukrainian)

16. Provisions on information protection and cybersecurity in payment systems] Resolution of the National Bank of Ukraine; Position № 43 (2021, May 19). Retrived from: https://zakon.rada.gov.ua/laws/show/v0043500-21/ed20210519#n24 (in Ukrainian)

17. Shumeiko, O.O. (2019). Informatsiina bezpeka [Informational security]: Navch. posib. Dnipro: Dniprovskyi derzhavnyi tekhnichnyi universytet, 155 p. (in Ukrainian)

18. Zakharenko, K. (2017). Osnovni subiekty ta instytuty informatsiinoi bezpeky. [The main subjects and institutions of information security]. *Visnyk Kharkivskoho natsionalnoho pedahohichnoho universytetu imeni H.S. Skovorody. Seriia Filosofiia*, 48 (1), pp. 212-219. (in Ukrainian)

19. Potejko, P. (2009). Information security in: Wojtaszczyk, K., Materska-Sosnowska, A. (ed.), State security, ASPRA-JR publishing house, Warsaw, 194 p. (in English)

20. Chellappa, Ramnath K., Paul, A. Pavlou (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information Management, pp. 358-368. Retrived from: https://www.emerald.com/insight/content/doi/10.1108/09576050210447046/full/pdf?title=perceived-information-security-financial-liability-and-consumer-trust-in-electronic-commerce-transactions. (in English)

Стаття: надійшла до редакції 27.05.2022
прийнята до друку 03.06.2022
The article: is received 27.05.2022
is accepted 03.06.2022

Бібліографія: Шопіна І. М. Поняття інформаційної безпеки: концептуальні підходи до визначення. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Журнал. Серія Право*. Івано-Франківськ: Редакційно-видавничий відділ Університету Короля Данила, 2022. Вип. 13 (25). С. 133-140. DOI: 10.33098/2078-6670.2022.13.25.133-140.