ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 4 (10), 2023

**УДК 340:316.7**

**DOI 10.31732/2708-339X-2023-10-166-174**

# ІНФОРМАЦІЙНА БЕЗПЕКА: СУЧАСНІ РИЗИКИ ТА ЗАГРОЗИ У СФЕРІ ЗБЕРІГАННЯ ТА ОБМІНУ ІНФОРМАЦІЇ

***Биков О. М.,***
*док. юр. наук, професор кафедри теорії та історії держави і права*
*ВНЗ «Університет економіки та права «КРОК»*
*м. Київ, вул. Табірна, 30-32, Україна, 03113,*
*e-mail: oleksandrbm@krok.edu.ua,*
*ORCID: https://orcid.org/0000-0003-4965-696X*

# INFORMATION SECURITY: MODERN RISKS AND THREATS IN THE FIELD OF IFORMATION STORAGE AND EXCHANGE

***Bykov O.M.,***
*Doctor of Laws, Professor of the Department of State and*
*Legal Disciplines of «KROK» University,*
*Kyiv, Tabirna St., 30-32, Ukraine, 03113,*
*e-mail: oleksandrbm@krok.edu.ua,*
*ORCID: https:// orcid.org/0000-0003-4965-696X*

***Анотація.*** *Стаття присвячена аналізу інформаційної безпеки в аспекті основних ризиків та загроз, що виникають під час зберігання та обміну інформацією. Технічний прогрес впливає на всі сфери життя людини, а новації в інформаційній сфері, разом з їх численними перевагами, спричиняють появу безпрецедентних раніше викликів безпеці людини у її найрізноманітніших вимірах.*

*Сучасні інформаційні технології істотно впливають на особу розширенням можливостей доступу до інформації та загальним постійним приростом її об'ємів. Поступово в користувачів поглиблюється розуміння сутності інформаційних процесів, зростає здатність осмислення та узагальнення одержаних знань, розвиваються спеціальні вміння і зростає ступінь компетентності фахівців. Люди з усього світу підтримують зв'язок через Інтернет, вільно публікуючи інформацію про свою діяльність, взаємодію та інші аспекти особистого життя, часто забуваючи при цьому про власну безпеку. Особливо небезпечними є випадки використання недостатньо захищених та вразливих до зовнішніх злочинних посягань ресурсів державними установами та організаціями. Необхідно також враховувати, що надмірне захоплення віртуальним світом загрожує людині втратою її індивідуальності та етнокультурної самобутності, соціальною самоізоляцією, посиленням дегуманізації робочого процесу.*

*У статті констатовано, що перед кожною сучасною державою та численними міжнародними організаціями постає нове завдання щодо необхідності розвитку інформаційної культури суспільства. Оскільки постійно зростає рівень інформаційних потреб сучасного суспільства, науковці повинні зосередити свою увагу на вивченні усіх можливих загроз у сфері зберігання та обміну інформації, напрацювати механізми що дозволять ефективно протидіяти незаконному доступу до інформації, зменшувати ризики її втрати чи пошкодження.*

*В роботі також зосереджено увагу на дослідженні основних форм незаконного доступу до інформації, описано основні ознаки протиправних дій, що загрожують інформаційній безпеці.*

***Ключові слова:*** *безпека, інформаційна безпека, загрози інформаційної безпеки, національна безпека, втрата інформації, кіберзлочинність, інформаційні технології, інформаційне право.*

***Формул****: 0; рис.: 0, табл.: 0, бібл.: 10*

***Abstract.*** *The article is devoted to analyzing information security in the aspect of major risks and threats that arise during information storage and exchange. Technological progress affects all aspects of human life, and innovations in the information industry, along with their numerous advantages, lead to the emergence of unprecedented challenges to human security in its various dimensions.*

*Modern information technologies significantly impact individuals by expanding access to information and continually increasing its volume. Gradually, users deepen their understanding of the essence of informational processes, enhance their ability to comprehend and generalize acquired knowledge, develop specific skills, and increase the level of professional competence. People worldwide stay connected through the internet, freely publishing information about their activities, interactions, and other aspects of personal life, often forgetting about their own security. Cases of insufficiently protected and vulnerable resources being used by governmental institutions and organizations for external criminal purposes are particularly dangerous. It is also necessary to consider that excessive immersion in the virtual world threatens individuals with the loss of their individuality and ethnocultural identity, social self-isolation, and the intensification of dehumanization of the work process.*

*The article notes that each modern state and numerous international organizations face a new task regarding the necessity of developing the information culture of society. As the level of informational needs of modern society constantly grows, researchers should focus their attention on studying all possible threats in the field of information storage and exchange, developing mechanisms to effectively counter illegal access to information, and reducing the risks of its loss or damage.*

*The work also focuses on researching the main forms of unauthorized access to information, describing the key characteristics of unlawful actions that threaten information security.*

***Keywords:*** *security, information security, threats to information security, national security, information loss, cybercrime, information technology, information law.*

***Formulas:*** *0; fig: 0; tabl.: 0; bibl.: 10*

**Постановка проблеми.** Інформація значною мірою впливає на життя сучасної людини. Завдяки вдосконаленому обміну інформацією, швидкій комунікації, у тому числі через мережу Інтернет, життя цивілізації вийшло на новий рівень розвитку. Водночас, не заперечуючи ряд позитивних ефектів від формування так званого «інформаційного суспільства» (з легким обміном даними та неконтрольованими потоками інформації), кіберзлочинність та інші загрози викликають серйозні та обґрунтовані занепокоєння як науковців, так і державних діячів з усього світу. В той час коли онлайн-шахрайство, злами акаунтів, кіберзалякування, фішинг, популяризація мережевих азартних ігор, розповсюдження порнографії та інші незаконні дії ускладнюють життя окремих громадян, такі явища як кібертероризм, витоки даних, Dos-атаки, кібершпигунство є загрозою для національної безпеки, а в окремих випадках навіть для існування держав. В наведених умовах, вагомими є комплексні дослідження викликів та загроз у сфері зберігання та обміну інформацією, від яких сьогодні потерпає значна кількість людей по всьому світу, а також напрацювання дієвих механізмів боротьби із такими загрозами.

**Аналіз останніх досліджень і публікацій.** Загальні питання інформаційної безпеки, окремі загрози для зберігання та обміну інформацією в своїх працях висвітлюють такі зарубіжні науковці та державні діячі як О.Тоффлер, Дж. Фрулінгер, М. Усманов, М. Стемп, М. Вестагрер, Т. Бретон. Вітчизняну наукову думку представлено працями, які насамперед описують сутність та основні характеристики інформаційної безпеки (І.Сопілко, М.Олашин, В. Шемчук), соціально-філософські аспекти (Н. Авер'янова, Т. Воропаєва) а також роботами, в яких увагу зосереджено на дослідженнях правових засад та

правового регулювання інформаційної безпеки України (А. Нашинець-Наумова, П. Біленчук), співвідношення національної та інформаційної безпеки (І. Боднар, І. Жаровська), вивченні ролі міжнародних організацій в системі міжнародної інформаційної безпеки (О. Фролова, В. Кононенко та Л. Новікова), дослідженнях інформаційної безпеки та збереження важливої інформації в контексті російсько-української війни (І. Залєвська і Г. Удренас) тощо.

**Метою статті** є дослідження сучасних ризиків та загроз у сфері зберігання та обміну інформації, наведення основних переваг інформаційного суспільства та висвітлення викликів, які загрожують його існуванню, становлення і розвиток інформаційного права.

**Виклад основних положень.** Чимало користувачів сьогодні використовує Інтернет як платформу для проведення дискусій, становлення своєї популярності або вираження власних почуттів. Для користувачів мережі важливо першими поширити інформацію, викликавши підвищену увагу до неї з боку інших суб'єктів. За допомогою найрізноманітніших платформ таких як Facebook, Telegram, Instagram, Twitter чи YouTube, користувачі мають можливість публікувати власні дописи, відеофайли та фотографії. З кожним наступним роком інформація стає доступнішою. За даними Мінфіну та КМІС лише за останній рік в Україні частка людей, які користуються інтернетом кожного дня зросла з 72% до 80%. офіційні джерела наголошують також на тому, що починаючи з 2021 року загальних показник користувачів Інтернету збільшився на понад 10%.

Існує чимало суперечливих теорій, в яких можна виділити як позитивні, так і негативні аспекти інформаційного впливу на особу. Беззаперечно позитивним видається розвиток комп'ютерних технологій, які у багатьох сферах полегшують робочі процеси, забезпечують особі свободу вибору, в окремих випадках підвищують рівень безпеки людини (використання комп'ютерних технологій правоохоронними органами сприяє розкриттю злочинів та інших правопорушень). Комп'ютерні технології допомагають людині виконувати рутинні завдання ефективно та швидко, автоматизують робочі процеси, які раніше вимагали набагато більше часу, інтелектуальних та фізичних зусиль. Інтернет, електронна пошта, соціальні мережі, телеграм канали та інші технології забезпечують швидку і зручну комунікацію між людьми по всьому світу. Всемережжя надає безмежний доступ до інформації, дозволяє користувачам швидко знаходити відповіді на різноманітні запитання, досліджувати нові теми, навчатися новим навичкам.

Розвиток інформаційного середовища має неабияку користь для бізнесу та науки, позаяк комп'ютерні технології стимулюють інновації в бізнесі, сприяють розробці нових послуг та продуктів, оптимізують процеси і покращують способи взаємодії з клієнтами. Ефективний і швидкий обмін інформацією допомагає в наукових дослідженнях, під час аналізу даних та проектування нових можливостей для покращення практичного життя людини.

Новітні інформаційні технології дозволяють ефективніше управляти виробництвом, фінансами та іншими аспектами управління. Стрімінгові платформи, віртуальна реальність, комп'ютерні ігри та інші розважальні ресурси дозволяють людям розважатися та відпочивати. Комп'ютерні технології

мають беззаперечний позитивний влив на медицину, допомагають у діагностиці, під час лікування та моніторингу за станом здоров'я пацієнтів.

Щодо негативних аспектів захоплення комп'ютерними технологіями, варто виокремити такі небезпечні явища як: соціальна ізоляція (зменшення реального спілкування та соціальної взаємодії між людьми), зменшення критичного мислення (втрата здатності самостійно аналізувати інформацію), віддаленість від природи (що може негативно позначатися на фізичному та психічному здоров'ї людини), збільшення ризиків безпеки (включає втручання в приватність особи, через необережне ставлення особи до своїх особистих даних та інформаційної безпеки в цілому).

Інша група ризиків, які мають місце у сфері активного обміну інформацією пов'язана із забезпеченням інформаційної безпеки суб'єктів. За допомогою наукових досліджень необхідно виявляти потенційні загрози та вразливості інформаційної інфраструктури, напрацьовувати стратегію по боротьбі з правопорушеннями в інформаційній сфері, описувати процедури та стандарти, які визначатимуть більш ефективні правила, а також вимоги забезпечення безпеки інформації, розробляти процедури та плани швидкого реагування на загрози з метою швидкого виявлення та відновлення відповідних систем після потенційного порушення безпеки обміну чи зберігання інформації.

Сучасна інформаційна глобалізація та швидке формування інформаційного простору в Україні визначили, що одним з актуальних завдань є забезпечення інформаційної безпеки людини, суспільства та держави від інформаційних загроз. Одним з наслідків злочинних посягань на інформаційну безпеку людини, суспільства та держави М. Олашин називає появу в Україні так званого «тіньового» ринку інформації з обмеженим доступом [6, с. 273]. Дослідниця зосереджує свою увагу на загрозах, які виникають через незаконне розголошення важливої інформації (наприклад, розголошення банківської чи комерційної таємниці), характеризує незаконне розголошення як злочинне діяння, яке може проявлятися як у формі дії, так і у формі бездіяльності.

Інформаційна безпека – це стан захищеності життєво важливих інтересів особи, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність і неправдивість інформації, яка використовується; негативні інформаційні впливи та негативні наслідки застосування інформаційних технологій; несанкціоноване поширення й використання інформації; порушення цілісності, конфіденційності та доступності інформації [1, с. 298]. Під інформаційною безпекою розуміється також набір заходів, спрямованих на забезпечення безпеки інформації [10, с. 5].

Отже, інформаційна безпека передбачає захист інформації насамперед від незаконного доступу, від її втрати, викриття (розголошення) чи пошкодження.

Найпоширенішим та найрізноманітнішим способом впливу на інформаційну систему є несанкціонований доступ. Цей спосіб надає можливість завдати шкоди будь-якій із складових інформаційної безпеки [5, с. 280].

Неуповноважений (несанкціонований, незаконний) доступ до інформації досягається шляхом незаконного підбору паролів, використання крадених (перехоплених) облікових даних користувачів або соціального інженерінгу. Характерною ознакою цієї загрози є отримання зловмисником доступу до даних чи ресурсів без згоди власника чи адміністратора. Небезпечними наслідками неуповноваженого доступу є витік конфіденційної інформації, порушення приватності користувачів, фінансові втрати, пошкодження репутації тощо. У більшості випадків такі діяння носять протиправний характер і тягнуть за собою юридичні наслідки.

Неуповноважений доступ до інформації може мати різні форми. Однією з них є злам комп'ютерних систем або мереж за допомогою використання недосконалостей програмного забезпечення чи внаслідок його недостатньої захищеності. Злам комп'ютерних систем або мереж як правило має місце внаслідок використання користувачем слабких або стандартних паролів, або через виявлення недоліків у конфігурації інформаційних систем.

Відносно самостійною формою неуповноваженого доступу до інформації є фізичний доступ до чужих пристроїв або систем. Характерною рисою такої форми є те, що незаконні користувачі отримують доступ до інформації шляхом фізичного заволодіння чужими комп'ютерами, серверами або іншими електронними пристроями. Обидві з наведених форм незаконного доступу можуть мати ціллю як крадіжку цінної інформації з метою її подальшого використання чи продажу, так і спричинення шкоди або знищення інформації та її носіїв.

Мета зламу визначається мотивацією атакуючого суб'єкта. Такою метою може бути видалення або пошкодження даних, руйнування функціонування комп'ютерних систем або використання систем для запуску інших видів атак. Ціллю викрадення інформації також може бути подальша вимога її викупу власником. В такому разі незаконне заволодіння інформацією як правило супроводжується шифруванням файлів на комп'ютерних системах і вимаганням певної грошової винагороди за їхнє розблокування. Поширеними є злами систем задля вимагання викупу за збереження конфіденційної інформації в таємниці. Ціллю незаконного доступу також може стати розповсюдження шкідливого програмного забезпечення (наприклад, для шпигування).

Злам комп'ютерних систем може призвести не лише до викрадення важливої інформації, але й до її втрати. Збереження інформації є ще одним важливим аспектом інформаційної безпеки. Втрата даних може бути наслідком кібератаки (наприклад внаслідок розповсюдження вірусів чи шпигунського програмного забезпечення), крадіжки або втрати пристроїв, на яких конфіденційна інформація зберігається, пошкодження або втрати носіїв інформації, таких як CD, DVD, USB-накопичувачі, жорсткі диски тощо. Втрата інформації може бути наслідком пожежі, природної катастрофи чи стихійного лиха. Відомості можуть бути втраченими через зміну персоналу (співробітники покидаючи організацію можуть забирати з собою важливі документи, що призводить до втрати цінної інформації). Наведені випадки демонструють, наскільки важливо мати ефективні стратегії збереження та захисту інформації для запобігання

можливим втратам даних. Дублювання важливої інформації може захистити користувача від ризику випадкового видалення або перезапису на носії без можливості відновлення даних.

Нам близька думка Дж. Фрулінгера, який зазначає, що інформаційна безпека є набором методів, призначених для захисту даних від несанкціонованого доступу або змін, як під час їх зберігання, так і під час передачі з однієї машини чи фізичного місця в інше. І. Сопілко, досліджуючи співвідношення інформаційної безпеки та кібербезпеки, характеризує кібербезпеку як важливу форму інформаційної безпеки. Водночас обидві категорії безпеки автор вважає самостійними, хоч і тісно пов'язаними, такими, що включають у себе аналогічні й взаємодоповнюючі процеси. Водночас, увага переноситься на наслідки порушення інформаційної безпеки для бізнесу, вчений наголошує на тому, що витік даних, викликаний проломами у кібербезпеці і недоробленістю систем інформаційної безпеки, має руйнівні наслідки для будь-якого бізнесу, підриває репутацію компанії через втрату довіри споживачів і партнерів, позбавляє організацію її конкурентних переваг, і врешті впливає на корпоративні доходи через недотримання правил захисту конфіденційної інформації [8, с. 110].

Ризики інформаційної безпеки науковці оцінюють по різному. Проаналізувавши загрози інформаційної безпеки, М. Делембовський, О. Терентьєв та Є. Шабала вважають, що порушення безпеки функціонування комп'ютерних систем в першу чергу виникає через такі фізичні причини як збій в роботі приладів, природні явища та інше. Друге місце з-поміж загроз дослідники відводять слабкій підготовці фахових спеціалістів, а вже на третю позицію ставлять дії шкідливого програмного забезпечення або навмисні дії зловмисників [2].

І. Залєвська та Г. Удренас аналізуючи роль новітніх інформаційних технологій, застерігають, що інформаційні ресурси та інформаційна структура оборонного потенціалу в наш час є одним із найістотніших об'єктів безпеки в оборонній сфері, адже сучасні засоби озброєння, військової техніки, системи управління військами і зброєю є системами критичних додатків із високим рівнем комп'ютеризації. Ці системи можуть виявитися дуже вразливими з погляду впливу інформаційної зброї як у військовий, так і у мирний час [4, с. 24].

О. Панченко вважає, що на даний час в Україні відсутня чітко виражена організована система вироблення та реалізації єдиної державної політики у сфері забезпечення інформаційної безпеки, яка б визначала пріоритети розвитку єдиного інформаційного простору. Серед причин, які зумовлюють незадовільний стан у сфері забезпечення інформаційної безпеки, автор називає безсистемний розвиток законодавства, яке регулює інформаційну сферу, низький рівень правової та інформаційної культури громадян і суспільства загалом, незадовільне фінансування діяльності із забезпечення інформаційної безпеки, недостатній розвиток інформаційних та комунікаційних технологій у сфері державного управління, неналежний рівень підготовки кадрів у сфері створення і використання інформаційних і комунікаційних технологій [7, с. 59]. Разом з тим, затвердження Доктрини інформаційної безпеки України, (указ Президента

України No47/2017 від 25.02.2017р.) свідчить про позитивні зміни.. У документі перелічено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері, з-поміж яких: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності держави, деморалізацію особового складу Збройних Сил України, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні, проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі. Цей же документ констатує недостатню розвиненість національної інформаційно інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів, неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері та недостатній рівень медіа-культури суспільства.

В. Шемчук підкреслює, що загрози інформаційній безпеці держави виходять за межі географічних кордонів держав, посягають на національний інформаційний простір і можуть мати транскордонні чи глобальні негативні наслідки [9, с. 294.]

Науковці також справедливо вказують на те, що інформаційна стратегія не може існувати окремо від комплексної державної стратегії розвитку. По суті, інформаційна стратегія – це той механізм, який маємо постійно переглядати і вдосконалювати, адже стратегія боротьби з правопорушеннями в інформаційній сфері – це важлива складова частина загальної стратегії національної безпеки. Важливим кроком в українському законодавстві стало введення в дію Стратегії кібербезпеки України (рішення РНБО від 27.01.2016 р.)., метою якої проголошується створення умов для безпечного функціонування кіберпростору, його використання в інтересах окремої особи, суспільства та держави. Водночас, як вірно висловлює побоювання І. Жаровська, ефективній реалізації і цієї стратегії може завадити характерна для більшості сфер правового регулювання проблема реалізації норм права [3, с. 59].

**Висновки.** Перед інформаційною безпекою в сучасному світі постають різноманітні загрози, які можуть призвести до втрати конфіденційності, цілісності та доступності інформації. Такі небезпеки як кібератаки, витоки та втрата даних, «крадіжка ідентичності», різного роду фінансове шахрайство та технічні зброї становлять значні виклики для суспільства та держави. Вироблення ефективної стратегії безпеки має враховувати усю різноманітність загроз безпечному збереженню та обміну інформацією, що дасть можливість вчасно вживати відповідних заходів для запобігання та управління такими загрозами. Водночас, ефективна боротьба з численними порушеннями в інформаційній сфері неможлива без розвитку інформаційної культури суспільства, проведення для користувачів спеціальних навчань та тренінгів для осіб різних вікових груп.

Усі виклики та небезпеки, які протиставляються інформаційній безпеці ми вважаємо взаємопов’язаними і такими, що стають складнішими з кожним днем. Для

зменшення кількості правопорушень в інформаційній сфері у майбутньому будуть необхідні зовсім інші, нові форми, в тому числі міжнародної взаємодії, що спиратимуться на міжнародне право. Це дозволить швидко виявляти, затримувати і притягувати правопорушників до юридичної відповідальності.

***Література:***

1. Авер'янова Н. М., Воропаєва Т. С. Інформаційна безпека України: соціально-філософські аспекти. «Молодий вчений». №10(86), Жовтень. 2020. С. 297-303. URL: https://molodyivchenyi.ua/index.php/journal/article/view/319/308 (дата звернення 29.11.2023).

2. Делембовський М. М., Терентьєв О. О., Шабала Є. Є. Технологія впровадження середовища MATLAB в досліджені моделі загроз інформаційної безпеки. International scientific e-journal ΛΌΓΟΣ. ONLINE. № 15 (November). 2020. URL: https://www.ukrlogos.in.ua/10.11232-2663-4139.15.20.html (дата звернення 29.11.2023).

3. Жаровська І. М. Національна та інформаційна безпека (актуалізація в сучасних умовах). Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки». №3(27). 2020. С.56-61.

4. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах Російської військової агресії. Південноукраїнський правничий часопис. 2022. С. 20- 26. URL: https: //web.archive.org/ web/20220820225319id_/; http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf (дата звернення 29.11.2023).

5. Мосєвніна А. С., Зелінська О. В. Канали несанкціонованого доступу до інформації. Комп'ютерні технології обробки даних. Матеріали III Всеукраїнської науково-практичної конференції. 8 грудня 2022 року. Вінниця. С. 280-282 URL: file: /C:/ Users/User/Downloads/ 13127 - % D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-26086-1-10-20230116.pdf (дата звернення 29.11.2023).

6. Олашин М. Способи незаконного розголошення професійних таємниць. Матеріали Міжнародної науково-практичної конференції «Сучасні напрями розвитку економіки, підприємництва, технологій та їх правового забезпечення». Львів, 18-19 червня 2020 року. Львів. URL: https://www.lute.lviv.ua/fileadmin/www.lac.lviv.ua/data/pidrozdily/Naukovo_Doslidna_Chastyna/Docs/2020_VIKL._ZBIRNIK.pdf#page=273 (дата звернення 29.11.2023).

7. Панченко О. А. Інформаційна безпека в контексті викликів і загроз національній безпеці. Державне управління та місцеве самоврядування. 2020. Вип. 2(45). С. 57-63. URL:https://journals.politehnica.dp.ua/index.php/public/article/view/182/158.

8. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. Юридичний вісник. 2(59). 2021. С. 110-115. URL: https://dspace.nau.edu.ua/bitstream/NAU/53733/1/%d0%86.%20%d0%9c.%20%d0%a1%d0%be%d0%bf%d1%96%d0%bb%d0%ba%d0%be.pdf (дата звернення 29.11.2023)

9. Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та забезпечення. Експерт: парадигми юридичних наук і державного управління. 2020. №1(7). С. 285-296.

10. Usmonov M. Basic Concepts of Information Security. International Journal of Academic and Applied Research (IJAAR). Vol. 5 Issue 1, January. 2021. P. 5-8 URL: https://scienceweb.uz/publication/6479 (дата звернення 29.11.2023)

***References:***

1. Averianova N. M., Voropaieva T. S. Informatsiina bezpeka Ukrainy: sotsialno-filosofski aspekty. «Molodyi vchenyi». №10(86), Zhovten. 2020. S. 297-303. URL: https://molodyivchenyi.ua/index.php/journal/article/view/319/308 (Accessed 29.11.2023)

2. Delembovskyi M. M., Terentiev O. O., Shabala Ye. Ye. Tekhnolohiia vprovadzhennia seredovyshcha MATLAB v doslidzheni modeli zahroz informatsiinoi bezpeky. International scientific e-journal ΛΌΗΟΣ. ONLINE. № 15 (November). 2020. URL: https://www.ukrlogos.in.ua/10.11232-2663-4139.15.20.html (Accessed 29.11.2023)

3. Zharovska I. M. Natsionalna ta informatsiina bezpeka (aktualizatsiia v suchasnykh umovakh). Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Seriia: «Iurydychni nauky». №3(27). 2020. S.56-61.

4. Zalievska I. I., Udrenas H. I. Informatsiina bezpeka Ukrainy v umovakh Rosiiskoi viiskovoi ahresii. Pivdennoukrainskyi pravnychyi chasopys. 2022. S. 20 – 26. URL: https: //web.archive.org/ web/20220820225319id_/; http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf (Accessed 29.11.2023)/

5. Mosievnina A. S., Zelinska O. V. Kanaly nesanktsionovanoho dostupu do informatsii. Kompiuterni tekhnolohii obrobky danykh. Materialy III Vseukrainskoi naukovo-praktychnoi konferentsii. 8 hrudnia 2022 roku. Vinnytsia. C. 280-282 URL: file: /C:/ Users/User/Downloads/ 13127 - % D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-26086-1-10-20230116.pdf (Accessed 29.11.2023)

6. Olashyn M. Sposoby nezakonnoho rozgholoshennia profesiinykh taiemnyts. Materialy Mizhnarodnoi naukovo-praktychnoi konferentsii «Suchasni napriamy rozvytku ekonomiky, pidpryiemnytstva, tekhnolohii ta yikh pravovoho zabezpechennia». Lviv, 18-19 chervnia 2020 roku. Lviv. URL: https://www.lute.lviv.ua/fileadmin/www.lac.lviv.ua/data/pidrozdily/Naukovo_Doslidna_Chastyna/Docs/2020_VIKL._ZBIRNIK.pdf#page=273 (Accessed 29.11.2023)

7. Panchenko O. A. Informatsiina bezpeka v konteksti vyklykiv i zahroz natsionalnii bezpetsi. Derzhavne upravlinnia ta mistseve samovriaduvannia. 2020. Vyp. 2(45). S. 57-63. URL:https://journals.politehnica.dp.ua/index.php/public/article/view/182/158.

8. Sopilko I. M. Informatsiina bezpeka ta kiberbezpeka: porivnialno-pravovyi aspekt. Yurydychnyi visnyk. 2(59). 2021. S. 110-115. URL: https://dspace.nau.edu.ua/bitstream/NAU/53733/1/%d0%86.%20%d0%9c.%20%d0%a1%d0%be%d0%bf%d1%96%d0%bb%d0%ba%d0%be.pdf (Accessed 29.11.2023)

9. Shemchuk V. V. Zahrozy informatsiinii bezpetsi: problemy vyznachennia ta zabezpechennia. Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia. 2020. №1(7). S. 285-296.

10. Usmonov M. Basic Concepts of Information Security. International Journal of Academic and Applied Research (IJAAR). Vol. 5 Issue 1, January. 2021. P. 5-8 URL: https://scienceweb.uz/publication/6479 (Accessed 29.11.2023)

***Стаття надійшла до друку 06.12.2023***