

*Голда М.,*

*аспірант, Західноукраїнський національний університет*

*Суп В.,*

*студентка 3-го курсу юридичного факультету,*

*Західноукраїнський національний університет*

## **ДО ПИТАННЯ ПРО ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

Інформаційна безпека є невід'ємною частиною сучасного світу, де обмін даними є основою багатьох аспектів життя: від економіки до науки, від політики до особистих відносин. Поняття інформаційної безпеки виникло з появою перших комп'ютерів та мереж в середині 20 століття. Одним з перших піонерів цієї галузі був американський математик Клод Шеннон, який в 1948 році представив основні поняття теорії інформації.

У 1960-х роках з появою перших комп'ютерних мереж виникла необхідність захисту даних від несанкціонованого доступу, що призвело до активного розвитку криптографічних алгоритмів та систем захисту. Сьогодні інформаційна безпека відіграє вирішальну роль у забезпеченні стабільності та безпеки. У сфері бізнесу вона допомагає захищати конфіденційність комерційних даних та забезпечує надійність фінансових транзакцій. Для суспільства інформаційна безпека гарантує захист особистих даних, свободу слова та права на приватність. У багатьох країнах вона є ключовим аспектом національної безпеки, захищаючи важливі інфраструктури від кібератак та витоків інформації.

Інформаційна безпека стала однією з найбільш актуальних тем у сучасному світі, де обмін інформацією став необхідністю для розвитку бізнесу, науки, технологій та суспільства в цілому. По суті, інформаційна безпека - це забезпечення захищеності інформації від неправомірного доступу, руйнування, викрадення чи модифікації, а також забезпечення цілісності, конфіденційності та доступності цієї інформації. У цій доповіді

ми розглянемо ключові аспекти інформаційної безпеки, її важливість та вплив на різні сфери життя.

Інформаційна безпека базується на трьох основних складових: конфіденційності, цілісності та доступності інформації. Конфіденційність означає, що інформація доступна лише тим особам, які мають право на неї. Цілісність передбачає, що інформація захищена від несанкціонованої модифікації. Доступність гарантує, що інформація доступна тим, хто має на неї право у визначений час.

Загрози інформаційній безпеці постійно зростають у зв'язку з швидким розвитком технологій та появою нових методів кібератак. Загрози можуть бути як зовнішніми (наприклад, хакерські атаки), так і внутрішніми (наприклад, витік інформації від співробітників). Боротьба з цими загрозами потребує постійного вдосконалення заходів захисту та усвідомлення ризиків.

Одним із найбільших викликів для інформаційної безпеки є постійно зростаюча кількість кібератак та хакерських загроз. Зловмисники постійно вдосконалюють свої методи, що вимагає постійного вдосконалення захисту та розробки нових стратегій боротьби. Серед таких стратегій можна виокремити застосування сучасних криптографічних алгоритмів, впровадження механізмів багаторівневого захисту та підвищення кіберграмотності серед користувачів.

Інформаційна безпека є сукупністю заходів та стратегій, спрямованих на захист інформації від неправомірного доступу, викрадення, руйнування чи модифікації. Поняття інформаційної безпеки виникло у зв'язку зі зростанням ролі інформації в сучасному суспільстві та з потребою її захисту від різноманітних загроз. Одним з піонерів в цій сфері вважається Клод Шеннон, американський математик, який запропонував основні поняття теорії інформації в 1948 році.

Заснуванням сучасної системи інформаційної безпеки вважається поява перших комп'ютерних мереж у 1960-х роках, коли стало очевидним, що потрібно захищати дані від несанкціонованого доступу та зловживань. У 1970-х і 1980-х роках відбулася інтенсивна розробка криптографічних алгоритмів та стандартів безпеки, що поклало початок розвитку сучасної інформаційної безпеки як науки та галузі практичного застосування.

Значимість інформаційної безпеки в сучасному суспільстві важко переоцінити. Вона впливає на всі сфери життя, від захисту особистих даних громадян та забезпечення безпеки електронних платежів до захисту національних інформаційних систем від кібератак з боку іноземних агентів. Успіх у боротьбі зі загрозами інформаційної безпеки напряду впливає на стабільність економіки, політичну стабільність та забезпечення прав та свобод громадян. Тому розвиток ефективних систем захисту інформації є однією з найважливіших завдань для урядів, корпорацій та громадянського суспільства в цілому.

Отже, інформаційна безпека є однією з найважливіших галузей сучасного світу, яка впливає на всі сфери життя. Її розвиток і вдосконалення є вирішальним завданням для забезпечення стабільності, безпеки та приватності. Заснована на принципах конфіденційності, цілісності та доступності інформації, інформаційна безпека відіграє ключову роль у сучасному світі і вимагає постійного уваги та вдосконалення.

#### **ЛІТЕРАТУРА:**

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>

2. ОСОБЛИВОСТІ РОЗУМІННЯ ПОНЯТЬ «ІНФОРМАЦІЙНА БЕЗПЕКА» ТА «БЕЗПЕКА ІНФОРМАЦІЇ». URL: [https://ktpu.kpi.ua/wp-content/uploads/2016/02/st14\\_AA\\_Osoblivosti-rozuminnya-IB\\_BI.pdf](https://ktpu.kpi.ua/wp-content/uploads/2016/02/st14_AA_Osoblivosti-rozuminnya-IB_BI.pdf)

3. Закони України [zakon.rada.gov.ua]: Закон України «Про інформацію» від 02.10.1992 № 2657-XII.

*Яворський І.,*

*аспірант, Західноукраїнський національний університет*

*Красовська А.,*

*студентка 3-го курсу юридичного факультету,*

*Західноукраїнський національний університет*

## **АНАЛІЗ РОЗМІРУ КОМПЕНСАЦІЇ В СИСТЕМІ ЗАХИСТУ**

### **АВТОРСЬКИХ ПРАВ: НАЦІОНАЛЬНІ ТА ІНОЗЕМНІ ПРАКТИКИ**

Отримання компенсації за порушення авторських прав в системі захисту авторських прав може відрізнитися залежно від національного законодавства та практики. Національні закони можуть встановлювати різні механізми визначення розміру компенсації, а також фактори, які враховуються при її визначенні.

В багатьох країнах, в тому числі і в Україні, розмір компенсації може бути визначений на основі різних критеріїв, таких як:

Величина збитків, заподіяних порушенням авторських прав.

Прибуток, отриманий порушником в результаті незаконного використання авторського твору.

Ринкова вартість використання авторського твору.

Ступінь невідповідності використання авторського твору умовам ліцензії чи договору.