МІНІСТЕРСТВО ОСВІТИ І НАУКИУКРАЇНИ

ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет менеджменту, адміністрування та права

Кафедра права та європейської інтеграції

СЛОВНИК ТЕРМІНІВ ТА ПОНЯТЬ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНЕ ПРАВО»

для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання

Харків 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет менеджменту, адміністрування та права

Кафедра права та європейської інтеграції

СЛОВНИК ТЕРМІНІВ ТА ПОНЯТЬ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНЕ ПРАВО»

для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання

Затверджено

рішенням НМР факультету МАП ДБТУ

Протокол № 6 від 18.02.2025 р

Харків 2025

УДК 342.951(038)
П 73

Інформаційне право / словник термінів та понять для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання***; упоряд.: В.В.Брулевич** – **Харків: ДБТУ, 2025 – 23 с.***

*Словник термінів та понять призначений для надання допомоги здобувачам у засвоєнні основних понять з навчальної дисципліни «**Інформаційне право**» що охоплюють питання правового регулювання інформаційних відносин у сучасному цифровому суспільстві. Він спрямований на розкриття взаємозв'язку інформаційного права з процесами цифровізації, розвитком електронного врядування, захистом персональних даних, кібербезпекою та інформаційними правами громадян в умовах глобалізації та інтеграції України у європейський правовий простір.*

Призначений для здобувачів денної та заочної форми навчання

РЕЦЕНЗЕНТИ:

Дуюнова Т.В, – канд. юрид. наук, д-ка економ. наук, завідувачка кафедри права та європейської інтеграції Державного біотехнологічного університету.

Остапенко Ю.І. – д-р юрид. наук, доцент, доцент кафедри асистент кафедри господарського права Національного юридичного університету імені ЯрославА Мудрого.

Відповідальний за випуск:
Кандидат юридичних наук В.В. Брулевич
права та європейської інтеграції

ВСТУП

Інформаційне право є однією з ключових галузей сучасного права, що регулює суспільні відносини у сфері створення, збирання, обробки, зберігання, поширення та захисту інформації. Воно визначає правові механізми функціонування інформаційного суспільства, забезпечує дотримання прав людини на доступ до інформації та її захист, а також встановлює правила взаємодії між державою, юридичними особами та громадянами у цифровому середовищі.

У контексті європейської інтеграції України, розвитку цифрової економіки та електронного врядування особливо важливим є чітке розуміння основних понять і категорій інформаційного права. Це необхідно для ефективного застосування норм, що регулюють персональні дані, кібербезпеку, свободу вираження поглядів, медіа-сферу, штучний інтелект, цифрові платформи та правовий режим інформаційних технологій.

Цей словник термінів та понять створений для здобувачів вищої освіти з метою систематизації та пояснення ключових юридичних термінів, що використовуються в інформаційному праві та інформаційному процесі. Він сприятиме формуванню належного рівня правової культури, розумінню законодавчих актів, судової практики, а також засвоєнню механізмів правового регулювання інформаційних відносин.

У словнику представлено основні поняття, що стосуються правового статусу суб’єктів інформаційного права, правових режимів інформації, процедур доступу до публічної інформації, цифрової трансформації, електронного документообігу, захисту персональних даних, боротьби з кіберзлочинністю, а також питань дезінформації, цифрових прав людини та регулювання штучного інтелекту.

Сподіваємося, що цей словник стане корисним ресурсом для здобувачів, викладачів, науковців та всіх, хто цікавиться інформаційним правом, допомагаючи їм у навчанні, дослідницькій діяльності та практичному застосуванні отриманих знань.

1. **Адаптація законодавства** – процес приведення національного законодавства у відповідність до міжнародних та європейських правових норм у сфері інформаційного права.

2. **Адміністративна відповідальність у сфері інформаційного права** – вид юридичної відповідальності за порушення законодавства, що регулює відносини в інформаційній сфері (наприклад, за порушення прав на доступ до публічної інформації або розповсюдження фейкових новин).

3. **Анонімність в Інтернеті** – здатність користувача здійснювати інформаційну діяльність без розкриття своєї особи.

4. Авторське право – сукупність правових норм, що регулюють створення, використання та захист авторських творів у цифровому середовищі.

5. **Аутентифікація** – процес перевірки особи користувача для надання доступу до інформаційних ресурсів.

6. **Агрегація даних** – процес збору та об'єднання даних із різних джерел для подальшого аналізу або обробки.

7. **Альтернативні факти** – інформаційні твердження, що подаються як правдиві, але насправді є спотвореними або маніпулятивними.

8. **База даних** – організована сукупність інформації, яка зберігається у структурованому вигляді й доступна для обробки за допомогою комп’ютерних технологій.

9. **Блокування інформаційних ресурсів** – тимчасове або постійне обмеження доступу до певного веб-ресурсу відповідно до рішення суду або уповноваженого органу.

10. **Блокчейн** – технологія децентралізованого зберігання даних, що забезпечує прозорість, незмінність та безпеку інформації.

11. **Біометрична ідентифікація** – процес розпізнавання особи на основі фізичних чи поведінкових характеристик (відбитки пальців, розпізнавання

обличчя тощо).

12. **Відкриті дані –** інформація, що є у вільному доступі та може бути використана, змінена й поширена без обмежень.

13. **Віртуальна реальність** – штучно створене середовище, що моделює реальний світ та взаємодію користувача з ним.

14. **Впливові цифрові платформи** – великі онлайн-ресурси (наприклад, Google, Facebook, TikTok), які мають значний вплив на інформаційний простір.

15. **Віртуальна приватна мережа (VPN)** – технологія, що забезпечує захищене з'єднання між пристроєм користувача та мережею Інтернету

16. **Громадська інформація** – інформація, що знаходиться у володінні органів державної влади та місцевого самоврядування й повинна бути доступною громадянам.

17. **Гібридні загрози в інформаційному просторі** – комплексні інформаційні атаки, спрямовані на маніпулювання свідомістю, дестабілізацію суспільних процесів і підрив довіри до державних інститутів.

18. **Глибокі фейки (Deepfake)** – технологія штучного інтелекту, яка дозволяє створювати реалістичні фальсифіковані зображення, відео або аудіозаписи.

19. **Гібридна цензура** – комбіновані методи обмеження доступу до інформації, що включають як правові, так і технологічні інструменти.

20. **Дезінформація** – свідоме поширення неправдивих або маніпулятивних відомостей з метою впливу на громадську думку або прийняття рішень.

21. **Державна таємниця** – інформація, що охороняється державою та розголошення якої може завдати шкоди національній безпеці.

22. **Доступ до інформації** – право фізичних і юридичних осіб отримувати, використовувати та поширювати інформацію, що є у відкритому доступі.

23. **Дезінформаційні кампанії** – організовані дії з поширення неправдивої або маніпулятивної інформації з метою впливу на суспільство.

24. **Діджиталізація державного управління** – процес переведення державних послуг та управлінських функцій у цифровий формат.

25. Електронний документообіг – система створення, обміну, зберігання та використання електронних документів із застосуванням цифрових технологій.

26. **Електронний підпис** – технологічний засіб підтвердження автентичності електронного документа та особи, яка його підписала.

27. **Електронна демократія** – використання цифрових технологій для розширення участі громадян у політичних процесах.

28. **Етичний штучний інтелект** – підхід до розробки та використання ШІ, який враховує принципи прозорості, відповідальності та справедливості.

29. **Зловмисне програмне забезпечення (Malware)** – різні типи шкідливих програм, призначених для несанкціонованого доступу або пошкодження інформаційних систем.

30. **Зашифрований трафік** – передача даних у мережі Інтернет у зашифрованому вигляді для захисту від несанкціонованого перехоплення.

31. **Інформаційне право** – галузь права, що регулює суспільні відносини у сфері збору, обробки, зберігання, передачі та захисту інформації.

32. **Інформаційна безпека** – захист інформації та інформаційних систем від несанкціонованого доступу, модифікації, знищення або інших загроз.

33. **Інформаційна війна** – використання інформаційних технологій для досягнення стратегічних цілей у політичній, економічній або військовій сферах.

34. **Інформаційні ресурси** – сукупність документованої інформації, що має суспільну, економічну або правову цінність.

35. **Інформаційна етика** – сукупність моральних норм і принципів, що регулюють поведінку суб'єктів в інформаційному просторі.

36. **Інтернет речей (IoT)** – концепція, що передбачає взаємодію фізичних пристроїв через мережу Інтернет.

К к

37. **Кібербезпека** – заходи щодо захисту інформаційних систем, мереж та даних від кібератак.

38. **Кіберзлочинність** – протиправна діяльність у цифровому середовищі, спрямована на незаконний доступ до інформації, шахрайство, злам систем тощо.

39. **Криптографія** – методи шифрування інформації для її захисту від несанкціонованого доступу.

40. **Кібергігієна** – комплекс заходів, спрямованих на безпечне користування інформаційними технологіями та захист особистих даних.

41. **Кібертероризм** – використання інформаційних технологій для здійснення атак на критично важливу інфраструктуру держави чи бізнесу.

М м,

42. **Метавсесвіт** – віртуальний простір, що поєднує елементи віртуальної та доповненої реальності, забезпечуючи інтерактивний досвід користувачів.

43. **Медіаграмотність** – здатність критично оцінювати, аналізувати та використовувати інформацію з цифрових джерел.

О о,

44. **Оператори персональних даних** – суб’єкти, які здійснюють збір, зберігання та обробку персональних

даних.

45. **Онлайн-цензура** – обмеження або контроль за поширенням інформації в Інтернеті, здійснюваний державними органами або платформами.

46. **Омічна приватність (Omnichannel Privacy)** – принцип захисту персональних даних у середовищах, де інформація циркулює між кількома платформами та каналами.

47. **Опенсорс-розвідка (OSINT)** – метод збору інформації з відкритих джерел у цифровому просторі.

48. **Персональні дані** – будь-яка інформація, що дозволяє ідентифікувати фізичну особу (ПІБ, номер телефону, IP-адреса тощо).

49. **Публічна інформація** – відомості, що містяться в офіційних документах органів влади та є відкритими для громадян.

50. **Право на забуття** – право особи вимагати видалення її персональних даних з публічного доступу (наприклад, з пошукових систем).

51. **Програмний алгоритмічний контроль** – автоматизовані системи модерації контенту, що використовуються соціальними мережами та платформами.

52. **Постправда** – ситуація, коли емоції та особисті переконання мають більший вплив на суспільну думку, ніж об'єктивні факти.

53. **Розповсюдження інформації** – процес передавання інформації широкому загалу через ЗМІ, Інтернет або інші засоби комунікації.

54. **Розумний контракт (Smart contract)** – програмний алгоритм, що автоматично виконує умови угоди у блокчейн-мережі.

55. **Ретрансляція інформації** – передача новин або повідомлень через

різні платформи та медіа без зміни змісту.

56. **Свобода слова** – конституційне право особи вільно висловлювати свої думки, погляди та поширювати інформацію.

57. **Соціальні мережі** – онлайн-платформи, що дозволяють користувачам обмінюватися інформацією та комунікувати.

58. **Система розпізнавання обличчя** – технологія аналізу біометричних даних для ідентифікації особи.

59. **Соціальний інжиніринг** – методи маніпулювання людьми для отримання конфіденційної інформації.

60. **Телекомунікаційне право** – підгалузь інформаційного права, що регулює діяльність у сфері зв’язку та Інтернету.

61. **Тіньовий Інтернет (Dark Web)** – частина Інтернету, доступ до якої здійснюється за допомогою спеціальних засобів шифрування та анонімності.

62. **Таргетована реклама** – реклама, що орієнтується на користувачів на основі їхніх уподобань та поведінкових даних.

63. **Технологія Deep Learning** – метод машинного навчання, що дозволяє комп'ютерним системам аналізувати та розпізнавати складні патерни в даних.

34. Фейкові новини – неправдива або маніпулятивна інформація, поширена з метою введення в оману

Фішинг – метод кібершахрайства, що передбачає виманювання особистих даних шляхом видачі себе за довірену особу чи організацію.

Функція цифрового контролю – можливість держави чи компаній регулювати діяльність користувачів у мережі.

35. Цифрові права – права людини у сфері цифрових технологій, що включають право на доступ до інформації, приватність та безпеку в Інтернеті.

36. Цифрова ідентичність – сукупність електронних даних, що дозволяють ідентифікувати особу в цифровому середовищі.

37. Цифрова автономія – можливість особи контролювати власні цифрові дані та самостійно визначати рівень своєї онлайн-присутності.

38. Цифровий тіньовий слід – сукупність цифрової інформації, яку залишає користувач під час використання Інтернету.

39. Штучний інтелект – система, здатна до самостійного аналізу інформації та прийняття рішень на основі алгоритмів машинного навчання.

40. Штучний інтелект у праві – використання алгоритмів ШІ для автоматизації юридичних процесів (аналіз контрактів, прогнозування рішень суду тощо).

41. Шифрування кінцевих точок – метод захисту інформації, що забезпечує її доступність лише для відправника та отримувача.

Навчальне видання

ІНФОРМАЦІЙНЕ ПРАВО

Словник термінів і понять

для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання

Автори-укладачі:
БРУЛЕВИЧ Володимир Віталійович

Формат б0х84/1б Гарнітура Time New Roman
Папір для цифрового друку. Друк ризографічний.
ум. друк. арк. 0,75
Тираж 25 пр.
Державний біотехнологічний університет
б1002, м. Харків, вул. Алчевських ,44