**НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СУСПІЛЬСТВІ**

**Кривешко І.В.1, Міхайліна Т.В.2,\***

*1**Донецький національний університет імені Василя Стуса, м. Вінниця, Україна*

*2 Донецький національний університет імені Василя Стуса, м. Вінниця, Україна*

\*…

[mihaylina@donnu.edu.ua](mailto:mihaylina@donnu.edu.ua)

Стрімка діджиталізація, що характеризує сучасне суспільство, принесла не лише позитивні зміни, а й загострила численні проблеми, серед яких порушення прав інтелектуальної власності, конфіденційності, втручання у приватне життя особи тощо, що разом охоплюються ємним поняттям інформаційної безпеки, досягнення якої стало одним із найсуттєвіших викликів сучасності.

На думку К.Ю. Ісмайлова, термін «інформаційна безпека» на даний момент часу не є коректним по своїй суті. Замість нього він пропонує вживати термін «інформаційна захищеність» – захист конфіденційності, цілісності та доступності інформації [1, c. 32-33]. Хоча навряд чи доцільно це робити, оскільки термін «інформаційна безпека» у праві України є легалізованим, тобто визначеним у законодавстві. Запровадження ще одного терміну не принесе сутнісних змін, а лише призведе до плутанини та необгрунтованого ускладнення поняттєвого апарату. Д.В. Дубов та М.А. Ожеван ототожнюють кібербезпеку з інформаційною безпекою [2, c. 4; 3, с. 356], що також не визнається вірним, оскільки інформаційна безпека являє собою більш широке поняття та охоплює стан захищеності суспільних відносин, як у власне інформаційному, так і інформаційно-технічному середовищі. Якщо ж мова йде про кібербезпеку, то вона виступає частиною інформаційної безпеки і опосередковує стан захищеності суспільних відносин лише в інформаційно-технічному середовищі.

Як стверджують Ю. Луценко та А. Тарасюк, система інформаційної безпеки, особливо на рівні її вихідних компонентів, може бути структурована за різними критеріями. У тому числі, як структурний компонент інформаційної безпеки, автори виділяють кібернетичну безпеку. Законом України «Про основні засади забезпечення кібербезпеки України» вона визначена як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Виокремлення кібербезпеки зумовлене специфікою середовища, у якому функціонують інформаційні системи, здійснюється обіг інформації, реалізуються законні інтереси суб’єктів інформаційних процесів. Тож «кібернетичний вимір» властивий усім складовим інформаційної безпеки [4, с. 322]. Останнє видається досить сумнівним, оскільки навіть у сучасному світі, з його підвищеними темпами інформатизації та технологізації, ці процеси все одно відбуваються досить нерівномірно у різних суспільствах та державах, а отже, не завжди технологічна інфраструктура певної держави є такою, щоб переводити будь-які фактичні інформаційні відносини у кібернетичні (тобто, з інформаційно-технічним компонентом).

Отже, інформаційна інфраструктура може бути як власне інформаційною (способи, шляхи, засоби, правила передачі інформації, її зберігання, використання тощо), так і інформаційно-технічною, тобто опосередкованою, у тому числі, засобами комп’ютерної техніки. На підставі цього можна зробити висновок, що інформаційна безпека являє собою стан захищеності усіх інформаційних відносин у певному суспільстві. Натомість, кібербезпека – стан захищеності інформаційних відносин, інформаційна інфраструктура яких характеризується технічним компонентом, тобто є інформаційно-технічною. Таким чином, у Законі України «Про основні засади забезпечення кібербезпеки України» її визначальні характеристики сформульовані досить вдало, у той час, як у наукових дослідженнях нерідко відбувається змішування понять інформаційна безпека та кібербезпека.

Для забезпечення, як власне інформаційної, так і кібербезпеки, необхідні відповідні засоби, з-поміж яких виділяється правове регулювання інформаційних відносин, закріплення правових приписів поводження з інформацією. Проте у сучасному динамічному світі правове регулювання не завжди встигає за стрімким розвитком інформаційних систем та відносин, внаслідок чого нормативна основа функціонування інформаційних систем потребує доповнення. Одним з таких елементів стають корпоративні норми, які формально чи неформально встановлюються соціальними мережами, транснаціональними корпораціями (у аспекті поводження з певною, у тому числі службовою, інформацією). Як не дивно, але у сучасному суспільстві саме корпоративні норми нерідко виявляються більш ефективними у впорядкуванні інформаційних відносин, аніж норми правові (як національні, так і наднаціональні). Це забезпечується транснаціональністю соціальних мереж, спільними правилами поводження у кожній з них, стрімкою реакцією на виклики інформаційного суспільства, суворістю наслідків (у вигляді, наприклад, повного блокування акаунтів). Хоча, з іншого боку, недоліком цього є складність оскарження накладення корпоративних санкцій, внаслідок технологізації процесу (нерідко оскарження відбувається через чат-ботів відповідних компаній, які слідують лише формальним правилам та процесам, не враховуючи сутність та особливості скарги), а також відсутності офіційного представництва певних соціальних мереж на території певних держав (наприклад, в Україні відсутнє офіційне представництво Фуйсбуку).

У такому разі інколи єдиним способом, який може забезпечити інформаційну безпеку, залишається підвищення інформаційної культури суб’єктів, яка також включається до нормативної основи інформаційних відносин. Як зазначають науковці, інформаційна безпека в контексті інформаційної культури, з одного боку, слугує вектором її розвитку, а з іншого сама є результатом розвитку [5, с. 42; 6, с. 38], чим, по-перше, підкреслюється циклічність досліджуваних явищ і процесів, а, з-іншого боку, їхній функціональний взаємозв’язок.

На підставі викладеного, стверджується, що забезпечення інформаційної безпеки має грунтуватися на поєднанні, як юридичних, так і неюридичних засобів [7, с. 45], а нормативна основа інформаційних відносин та забезпечення інформаційної безпеки складатися з таких компонентів, як: 1) правові норми (національного та міжнародного рівня); 2) корпоративні норми; 3) інформаційна культура.

**Список використаних джерел:**

1. Ісмайлов К.Ю. Поняття «кібезбезпека та «інформаційна безпека». *Типологія безпеки. Актуальні проблеми автоматизації та управління*: міжнародна науково-практична конференція. Луцьк, 2016. С. 32-33.
2. Дубов Д.В., Ожеван М.А. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців: аналітична доповідь. НІСД. 2012. 28 с.
3. Кононенко В.П., Новікова Л.В., Копицька П.О. Політика міжнародних організацій з питань інформаційної безпеки. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2021. Вип. 65. С. 353-358.
4. Луценко Ю.В., Тарасюк А.В., Денисенко М.М. Кібербезпека та інформаційна безпека: співвідношення понять. *Юридичний науковий електронний журнал*. 2022. №8. С. 320-323.
5. Француз-Яковець Т.А. Інформаційно-правова культура як необхідний елемент формування сучасного інформаційного суспільства. *Часопис Київського інституту інтелектуальної власності та права*. 2022. Вип. 2. С. 41-45.
6. Панченко О.А., Панченко Л.В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*. 2015. №2 (46). С. 32-38.
7. Кривешко І.В. Інформаційна культура як правовий феномен. *Правничий часопис Донецького національного університету імені Василя Стуса*. 2022. №1-2. С. 42-46.