

shcho-robiti-yakshcho-pd-chas-vyni-znishcheno-zastavne-mayno-poradi-yurista (дата звернення: 26.02.2025).

DOI <https://doi.org/10.30525/978-9934-26-558-7-25>

EVOLUTION OF THE CONCEPT OF "INFORMATION SYSTEM" IN THE CONTEXT OF ARTICLE 361 OF THE CRIMINAL CODE OF UKRAINE: MODERN CHALLENGES AND PROSPECTS

ЕВОЛЮЦІЯ ПОНЯТТЯ "ІНФОРМАЦІЙНА СИСТЕМА" В КОНТЕКСТІ СТАТТІ 361 КК УКРАЇНИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Dryzhakova D. Yu.

Postgraduate Student at the Department of Criminal Policy and Criminal Law, Taras Shevchenko National University of Kyiv, Ukraine
<https://orcid.org/0009-0004-7585-5860>

Дрижакова Д. Ю.

аспірантка кафедри кримінально-правової політики та кримінального права Київський національний університет імені Тараса Шевченка м. Київ, Україна
<https://orcid.org/0009-0004-7585-5860>

Стаття 361 Кримінального кодексу України, що передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, є ключовою нормою у сфері кібербезпеки. Проте, з розвитком інформаційних технологій, поняття "інформаційна система" зазнало суттєвих змін, що вимагає переосмислення та адаптації кримінально-правових норм до сучасних реалій.

Інформаційна система (англ. Information system) – сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

За ДСТУ 2392-94: Інформаційна система – комунікаційна система, що забезпечує збирання, пошук, оброблення та пересилання інформації [1].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» визначає інформаційну (автоматизовану) систему як організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [2].

В українському законодавстві встановлено такі визначення терміна:

– Інформаційна система – автоматизована система, комп'ютерна мережа або система зв'язку[3].

– Інформаційна система – організаційно-технічна система обробки інформації за допомогою технічних і програмних засобів [4].

– Інформаційна система – система, призначена для одержання, обробки, зберігання, відображення та/або реєстрації даних про технічний стан конструкцій, систем, елементів, їх властивості та/або функціонування [5].

На момент прийняття КК України у 2001 році, поняття "інформаційна система" переважно асоціювалося з локальними комп'ютерними мережами та серверами. З розвитком Інтернету, хмарних технологій, Інтернету речей (IoT) та інших цифрових інновацій, межі інформаційних систем стали розмитими.

Сьогодні "інформаційна система" може включати:

– Класичні комп'ютерні мережі: Локальні та глобальні мережі, сервери, робочі станції.

– Хмарні обчислення: Інфраструктура, платформи та програмне забезпечення, що надаються через Інтернет.

– Інтернет речей (IoT): Мережа фізичних пристроїв, що обмінюються даними через Інтернет.

– Мобільні пристрої: Смартфони, планшети, інші портативні пристрої, що підключені до мережі.

Бази даних: Системи зберігання та управління інформацією.

Крім позитивних соціальних наслідків широке впровадження інформаційних технологій спричинило також появу нових видів посягань. При цьому їх небезпечність визначається важливістю суспільних процесів в інформаційній сфері, яке постійно зростає. Тому можна стверджувати, що очевидно є необхідність правового регулювання й охорони означеної сфери [6].

Дотепер у науці кримінального права не вирішеними є питання щодо визначення поняття "інформаційна безпека", формулювання критеріїв суспільної небезпечності посягань на неї, меж застосування та змісту кримінально-правових засобів її захисту. Дискусійними залишаються питання про ознаки й сутність інформації як предмета злочину, зміст інших ознак складів так званих "комп'ютерних" злочинів (ст.ст. 361–363-1 КК України), напрями вдосконалення відповідних законів про кримінальну відповідальність. Україна ратифікувала Конвенцію про кіберзлочинність, що вимагає відповідної роботи щодо гармонізації українського та міжнародного законодавства [6].

На сьогодні можна виділити основні виклики:

1. Розмитість меж: складність визначення меж інформаційної системи у хмарних середовищах та IoT.

2. Транскордонність: кіберзлочини часто мають транскордонний характер, що ускладнює розслідування та притягнення до відповідальності.

3. Швидкість розвитку технологій: законодавство не завжди встигає за темпами розвитку технологій, що створює прогалини у правовому регулюванні. На сьогодні внесено законопроект народними депутатами України: І. М. Стойком (реєстр. № 390), О. І. Кузьмуком (реєстр. № 041), Ю. М. Сиротюком (реєстр. № 214) «Про засади інформаційної безпеки», який дає наступне визначення інформаційній сфері – сукупність інформаційних технологій, ресурсів, продукції і послуг, інформаційної інфраструктури, суб'єктів інформаційної діяльності та системи регулювання суспільних інформаційних відносин, а інформаційну безпеку визначає як – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [7].

4. Складність доказування: доведення факту несанкціонованого втручання в інформаційну систему вимагає спеціальних знань та навичок.

5. Кібервійна: збройна агресія РФ проти України актуалізувала проблему захисту критичної інформаційної інфраструктури, що вимагає посилення кримінально-правових заходів.

З урахуванням реалій сьогодення можна виділити основні перспективи розвитку:

Удосконалення законодавства: необхідно внести зміни до статті 361 КК України, уточнивши поняття "інформаційна система" та врахувавши сучасні технологічні реалії.

Міжнародна співпраця: посилення міжнародної співпраці у сфері боротьби з кіберзлочинністю, обмін інформацією та досвідом.

Підвищення кваліфікації: підвищення кваліфікації правоохоронних органів, суддів та прокурорів у сфері кібербезпеки.

Розвиток цифрової криміналістики: впровадження сучасних методів та технологій для виявлення та доказування кіберзлочинів.

Інформаційна просвіта: підвищення рівня обізнаності громадян щодо кібербезпеки та захисту персональних даних.

Висновки. Еволюція поняття "інформаційна система" вимагає постійного аналізу та адаптації кримінально-правових норм до сучасних реалій. Тільки шляхом удосконалення законодавства, посилення міжнародної співпраці та підвищення рівня обізнаності суспільства можна ефективно протидіяти кіберзлочинності та забезпечити кібербезпеку держави.

Література:

1. ДСТУ 2392-94 Інформація та документація. Базові поняття.
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР (Редакція від 19.04.2014). *Архів оригіналу за 22 червня 2017*. Процитовано 8 вересня 2017.
3. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.1999 № 1229/99. *Архів оригіналу за 14 вересня 2017*. Процитовано 8 вересня 2017.
4. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, затверджений постановою Кабінету Міністрів України від 16.11.2002 р. № 1772. *Архів оригіналу за 28 серпня 2017*. Процитовано 23 серпня 2017.
5. Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій, затверджені Наказом Державної інспекції ядерного регулювання України від 22.07.2015 № 140. *Архів оригіналу за 23 серпня 2017*. Процитовано 23 серпня 2017.
6. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС Ук- раїни, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с., с. 8.
7. Проект Закону України «Про засади інформаційної безпеки». <https://zakon-pro.ligazakon.net/document/JG3TH00A?land=UA&context=UA&an=3>