УДК 343
DOI https://doi.org/10.32844/2618-1258.2026.1.54

ВОЛИНЕЦЬ Р.А., ПТАЩЕНКО Д.С.

КВАЛІФІКАЦІЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ КОМП'ЮТЕРНИХ СИСТЕМ У СВІТЛІ СУЧАСНОЇ СУДОВОЇ ПРАКТИКИ УКРАЇНИ

QUALIFICATION OF UNAUTHORIZED INTERFERENCE IN THE OPERATION OF COMPUTER SYSTEMS IN THE LIGHT OF CONTEMPORARY JUDICIAL PRACTICE OF UKRAINE

Актуальність теми зумовлена зростанням кількості кіберінцидентів, що супроводжуються несанкціонованим втручанням у роботу комп'ютерних систем, електронних комунікаційних мереж і баз даних. У сучасних умовах цифровізації суспільства такі дії становлять реальну загрозу не лише інформаційній безпеці, а й стабільності державних інституцій, бізнесу та громадського сектору. Попри наявність кримінально-правової норми, передбаченої ст. 361 Кримінального кодексу України, практика її застосування свідчить про істотні проблеми в тлумаченні елементів складу злочину, визначенні стадій його вчинення, розмежуванні суміжних складів та ідентифікації співучасників. Це вказує на необхідність глибокого наукового осмислення механізму кваліфікації таких правопорушень.

Метою дослідження є комплексний аналіз кваліфікації несанкціонованого втручання в роботу комп'ютерних систем за ст. 361 Кримінального кодексу України у світлі сучасної судової практики, а також формування пропозицій щодо підвищення ефективності кримінально-правового захисту інформаційної безпеки.

Методологічну базу становлять діалектичний, системно-структурний, формально-логічний, порівняльно-правовий та емпіричний методи. Для досягнення мети було проаналізовано положення Кримінального кодексу України і понад п'ятнадцять рішень судів першої, апеляційної та касаційної інстанцій за 2020–2024 роки.

У результаті дослідження було встановлено, що сучасна судова практика демонструє перехід від формального до змістовного підходу у кваліфікації кіберзлочинів: визначальним стає не сам факт доступу, а його наслідки для конфіденційності, цілісності та доступності даних. Найбільш проблемними залишаються питання розмежування підготовки і замаху, визначення повторності, сукупності й співучасті. Виявлено тенденцію до конкуренції норм між ст. 361, 361-1 і 362 Кримінального кодексу України, що зумовлює правову невизначеність.

Сформульовано висновок про необхідність уніфікації методик технічного аналізу цифрових доказів, гармонізації кримінально-правових норм із міжнародними стандартами та розроблення національних рекомендацій щодо кваліфікації кіберзлочинів.

Ключові слова: *несанкціоноване втручання, кіберзлочин, стаття 361 Кримінального кодексу України, судова практика, кваліфікація злочину, цифрові докази.*

The relevance of the topic is due to the growing number of cyber incidents accompanied by unauthorized interference in the operation of computer systems, electronic communication networks, and databases. In the current conditions of

© ВОЛИНЕЦЬ Р.А. – доктор юридичних наук, професор кафедри кримінально-правової політики та кримінального права (Інститут права Київського національного університету імені Тараса Шевченка) https://orcid.org/0000-0002-8134-8572

© ПТАЩЕНКО Д.С. – кандидат юридичних наук, асистент кафедри кримінально-правової політики та кримінального права (Інститут права Київського національного університету імені Тараса Шевченка) https://orcid.org/ 0000-0001-9751-1509

digitalization of society, such actions pose a real threat not only to information security but also to the stability of state institutions, business, and the public sector. Despite the existence of a criminal law provision under Article 361 of the Criminal Code of Ukraine, its application in practice reveals significant problems in interpreting the elements of the crime, determining the stages of its commission, distinguishing between related crimes, and identifying accomplices. This points to the need for a deep scientific understanding of the mechanism for classifying such offenses.

The purpose of the study is to conduct a comprehensive analysis of the classification of unauthorized interference in the operation of computer systems under Article 361 of the Criminal Code of Ukraine in the light of current judicial practice, as well as to formulate proposals for improving the effectiveness of criminal law protection of information security.

The methodological basis consists of dialectical, systemic-structural, formal-logical, comparative-legal, and empirical methods. To achieve the goal, the provisions of the Criminal Code of Ukraine and more than fifteen decisions of courts of first, appeal, and cassation instances for 2020–2024 were analyzed.

The study found that current judicial practice demonstrates a shift from a formal to a substantive approach to the classification of cybercrimes: it is not the fact of access itself that is decisive, but its consequences for the confidentiality, integrity, and availability of data. The most problematic issues remain the distinction between preparation and attempt, the definition of repetition, concurrence, and complicity. A tendency toward competition between Articles 361, 361-1, and 362 of the Criminal Code of Ukraine has been identified, which leads to legal uncertainty.

A conclusion has been formulated on the need to unify the methods of technical analysis of digital evidence, harmonize criminal law provisions with international standards, and develop national recommendations on the classification of cybercrimes.

Keywords: *unauthorized interference, cybercrime, Article 361 of the Criminal Code of Ukraine, judicial practice, classification of crimes, digital evidence.*

Постановка проблеми. Стрімка цифровізація суспільства, зростання обсягів обробки даних і розширення мережевих інфраструктур зумовлюють підвищення рівня кіберзагроз та появу нових форм протиправного втручання в роботу інформаційних систем [1]. У таких умовах особливого значення набуває ефективність кримінально-правових механізмів протидії кіберзлочинності. Стаття 361 Кримінального кодексу (КК) України [2], що встановлює відповідальність за несанкціоноване втручання в роботу комп'ютерних систем або мереж, є центральною нормою у сфері кіберзахисту. Водночас правозастосовна практика демонструє наявність значних труднощів у кваліфікації таких діянь, що пов'язані з розмежуванням складів злочинів, визначенням стадій їх вчинення, повторності, співучасті та конкуренції норм. Відсутність уніфікованих методичних підходів до аналізу цифрових доказів і технічних аспектів правопорушень створює ризики неоднакового тлумачення норм, що знижує ефективність кримінально-правового реагування [3, с. 810]. Таким чином, дослідження особливостей кваліфікації злочинів, передбачених ст. 361 КК України, у світлі сучасної судової практики є актуальним і має важливе наукове та практичне значення.

Аналіз останніх досліджень і публікацій. У наукових працях останніх років простежується посилена увага до проблем боротьби з кіберзлочинністю, удосконалення кримінально-правових механізмів та адаптації системи доказування до викликів цифрової доби. Так, у дослідженні Н. Хадам (N. Khadam) та співавторів розглянуто питання ефективність покарань за атаки шкідливого програмного забезпечення в різних юрисдикціях, зокрема у Великій Британії, США, Китаї, Ефіопії та Пакистані, що дало змогу виявити розбіжності у правозастосуванні та вплив санкцій на рівень кіберзлочинності [4]. У цьому контексті Ф. Касіно (F. Casino) та колеги, аналізуючи проблеми транскордонних кримінальних розслідувань, наголошують на складнощах обміну цифровими доказами між державами та необхідності гармонізації процедур міжнародної взаємодії [5]. Розвиваючи цей напрям, М. Думчиков (M. Dumchikov) із колегами акцентував на використанні віртуальних активів як об'єкта й засобу вчинення кіберзлочинів в українських реаліях воєнного стану, виявивши нормативні прогалини в правовому регулюванні таких діянь [6, p. 919]. Натомість М. Бада (M. Bada) та Дж. Нерс (J. Nurse) у систематичній праці представили типові профілі кіберзлочинців, визначивши головні категорії правопорушників і психологічні чинники,

що зумовлюють девіантну поведінку в цифровому середовищі [7, p. 2]. Подібної думки дотримуються В. Стратонов (V. Stratonov) і співавтори, які дослідили найпоширеніші види кіберзлочинів в Україні та підкреслили потребу імплементації міжнародного досвіду у сфері кримінального переслідування таких діянь [8, p. 191]. Водночас І. Зозуля проаналізувала роль Національної поліції в протидії кіберзлочинам, наголосивши на доцільності інтеграції положень Конвенції про кіберзлочинність до вітчизняного законодавства [9, с. 17]. Вагомий внесок у розвиток кримінально-правової доктрини зробили М. Красько та А. Цевух, які обґрунтували необхідність адаптації кримінального права до цифрової епохи, окресливши виклики транскордонності, юрисдикції та появи нових об'єктів злочину, зокрема криптовалют і цифрових доказів [10]. Наукову цінність становлять і результати С. Корзуна, який розробив понятійно-категоріальний апарат державної політики у сфері протидії кіберзлочинності та запропонував класифікацію кіберзлочинів з урахуванням їх технічної природи [11, с. 131]. У цьому ж контексті Г. Тютюннікова зі співавторами, досліджуючи цифровізацію управлінських процесів, показали потенціал автоматизації облікових і контрольних процедур, що має прикладне значення для підвищення ефективності кіберслідчих дій [12, с. 984]. У науковому доробку П. Галушко досліджено правову природу кіберзлочинності у співвідношенні національного та міжнародного права, обґрунтовано її подвійний характер – як цифрової форми традиційних злочинів і як самостійного кримінально-правового феномену [3, с. 808].

Узагальнення зазначених джерел свідчить про міждисциплінарний характер сучасних досліджень у сфері кібербезпеки – від кримінально-правових аспектів до технологічних рішень, спрямованих на збір та аналіз цифрових доказів, що формує наукове підґрунтя для оновлення підходів до кваліфікації, розслідування та запобігання кіберзлочинам в Україні.

Попри значний масив досліджень і практичних напрацювань, низка важливих питань залишається відкритою: відсутність уніфікованих критеріїв для розмежування підготовки, замаху та фактичного втручання; дефіцит стандартизованих процедур фіксації й оцінки цифрових доказів; конкуренція норм і невизначеність при кваліфікації сукупності дій (ст. 361, 361-1, 362, 176 КК України); проблеми ідентифікації повторності та триваючого характеру кібердій; проблеми встановлення співучасті в умовах транснаціональних мереж; наявність нормативних прогалин щодо віртуальних активів і механізмів трансграничного обміну доказами. Ці проблеми вимагають цілеспрямованого наукового аналізу, що поєднає правову доктрину з технічною експертизою.

Формулювання цілей статті. Метою дослідження є системний аналіз проблем кваліфікації несанкціонованого втручання в роботу комп'ютерних систем відповідно до ст. 361 КК України та узагальнення сучасної судової практики з метою визначення головних тенденцій, суперечностей і напрямів удосконалення правозастосування у сфері кіберзлочинів. Для досягнення поставленої мети передбачено: 1) з'ясувати теоретико-правові засади складу злочину, передбаченого ст. 361 КК України, та його місце в системі кіберзлочинів; 2) проаналізувати судову практику 2020–2024 рр. і виявити ключові проблеми кваліфікації несанкціонованого втручання; 3) сформулювати пропозиції щодо вдосконалення законодавства, методичного забезпечення та судово-експертної практики у сфері кваліфікації кіберзлочинів.

Матеріали та методи дослідження. Емпіричну базу дослідження становлять положення чинного кримінального законодавства України, зокрема ст. 361, 361-1, 362 КК України, а також узагальнені судові рішення міських та районних судів за 2020–2024 роки. Для забезпечення об'єктивності аналізу використано близько п'ятнадцяти рішень, що репрезентують різні підходи до тлумачення складу злочину, доказування та розмежування суміжних складів.

Методологічну основу становлять загальнонаукові та спеціальні методи пізнання: діалектичний – для виявлення взаємозв'язку між нормою та практикою її застосування; формально-логічний – для аналізу правових конструкцій складу злочину; системно-структурний – для виокремлення елементів і взаємозалежностей у механізмі правової кваліфікації; метод судового аналізу – для узагальнення тенденцій практики та формулювання висновків щодо її впливу на розвиток доктрини кримінального права.

Виклад основного матеріалу. Стаття 361 КК України [2] займає ключове місце в системі кіберзлочинів, що передбачені розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». Її норми спрямовані на охорону суспільних відносин, які забезпечують безпечне функціонування інформаційних технологій, автоматизованих і комунікаційних систем. Умови цифрової трансформації, зростання обсягів обробки даних, активне використання мережевих сервісів і дистанційних форм управління призводять до суттєвого збільшення кількості посягань на інформаційну безпеку.

У системі складів злочинів цього розділу саме ст. 361 КК України [2] є базовою нормою, від якої походять інші кримінально-правові склади: створення чи розповсюдження шкідливих програм (ст. 361-1); несанкціоновані дії з інформацією (ст. 362); порушення правил експлуатації систем (ст. 363). Вона формує концептуальний фундамент правової охорони інформаційного простору, визначаючи межу між технічно можливим доступом і кримінально караним втручанням.

Зміст ст. 361 КК України [2] розкривається через систему елементів складу злочину, які утворюють цілісну правову конструкцію. Безпосереднім об'єктом правопорушення є суспільні відносини, що забезпечують належне функціонування інформаційних (автоматизованих) та електронних комунікаційних систем і мереж, спрямованих на обробку, зберігання, передавання та захист інформації. Порушення цих відносин підриває стабільність інформаційного середовища та створює загрозу безпеці держави й користувачів цифрових ресурсів [14].

Об'єктивна сторона злочину виражається у діях, спрямованих на незаконне втручання у функціонування систем, що спричиняють наслідки у вигляді витоку, втрати, блокування чи підробки інформації, спотворення процесів її обробки чи маршрутизації. Такі дії можуть мати різні технічні форми – від несанкціонованого доступу до облікових записів до використання шкідливого програмного забезпечення (ПЗ). Обов'язковою ознакою є наявність причиново-наслідкового зв'язку між діянням і наслідками [14]. У ст. 361-1 КК України цей елемент має активний прояв, а саме: створення, розповсюдження або збут програмних і технічних засобів, які здатні порушити роботу інформаційних систем [2].

Суб'єктом правопорушення є фізична осудна особа, яка досягла 16-річного віку. Хоча закон не визначає спеціального суб'єкта, на практиці найчастіше такі злочини вчиняють особи з фаховими знаннями у сфері інформаційних технологій (ІТ), адміністрування мереж або програмування. Ця обставина має важливе значення для з'ясування умислу та рівня суспільної небезпеки діяння [1; 14].

Суб'єктивна сторона характеризується прямим умислом: особа усвідомлює протиправність дій, передбачає наслідки й бажає їх настання. Для ст. 361-1 КК України обов'язковою є наявність мети – протиправного використання, розповсюдження або збуту шкідливих засобів. Цей критерій дає змогу відмежувати кримінально карані дії від легітимної діяльності у сфері кіберзахисту чи тестування ПЗ [1; 14].

Для систематизації зазначених характеристик і відображення типових прикладів із судової практики узагальнені результати представлено в табл. 1, яка демонструє взаємозв'язок між структурними елементами складу злочину, їх юридичним змістом і фактичними обставинами, встановленими в судових справах.

Наведені дані демонструють, що змістова структура складу злочину є складною системою, у якій технічні дії, мотиви та наслідки перебувають у тісному взаємозв'язку. Саме цей взаємозв'язок визначає межу між адміністративним порушенням, етичним зловживанням і кримінально караним втручанням.

У цьому контексті судові рішення останніх років є практичним індикатором еволюції правозастосування: вони не лише конкретизують зміст окремих елементів складу злочину, а й відображають поступову адаптацію кримінального законодавства до цифрової реальності. Аналіз рішень судів за 2020–2024 рр. (табл. 2) дає змогу простежити трансформацію підходів до тлумачення об'єкта та предмета злочину, визначити критерії, які суди вважають визначальними для встановлення факту втручання, та оцінити суспільну небезпеку діяння в умовах стрімкого технологічного розвитку.

Огляд судових рішень 2020–2024 рр. засвідчує перехід від формального до змістовного тлумачення поняття «втручання» – з урахуванням технічної сутності діяння, його наслідків і ролі цифрових доказів. Суди дедалі частіше підкреслюють, що сам факт доступу до облікового запису (акаунта) чи ресурсу не утворює складу злочину без доведених наслідків – витоку, блокування чи спотворення інформації. Такий підхід підтверджено в рішеннях Івано-Франківського міського суду (2021) та Приморського районного суду міста Одеси (2020), де відсутність шкоди стала підставою для закриття кримінальних проваджень.

Водночас у справах, де доведено використання шкідливого ПЗ або віддалених засобів контролю, дії кваліфікують за ч. 2 ст. 361 КК України, що передбачає реальні наслідки та обтяжуючі обставини. Так, у рішеннях Печерського (2021) та Шевченківського (2023) районних судів міста Києва наголошено на важливості логів (журналів подій) і висновків технічних експертиз для підтвердження факту втручання, тоді як їх відсутність часто стає підставою для виправдувальних вироків.

Таблиця 1

Характеристика складу злочину, передбаченого ст. 361 КК України

Елемент складу	Змістова характеристика	Типові приклади судової практики (2020–2024 рр.)
Об'єкт	Суспільні відносини у сфері належного функціонування інформаційних (автоматизованих) систем, мереж і комунікацій	Викрадення чи блокування облікових записів державних або корпоративних поштових систем; втручання у внутрішні бази даних компаній
Предмет	Інформаційні системи, електронні комунікаційні мережі, дані	Несанкціонований доступ до корпоративної пошти або персональних кабінетів користувачів онлайн-сервісів
Об'єктивна сторона	Дії, спрямовані на несанкціоноване втручання, що призводять до витоку, блокування, підробки або спотворення інформації	Використання програм для підбору паролів, впровадження шкідливого коду, надання стороннім особам доступу до мережі Wi-Fi організації
Суб'єкт	Осудна особа від 16 років; найчастіше – користувач або фахівець з IT, який має технічні знання чи доступ до систем	Працівники технічних відділів або адміністратори, які використовували службові доступи не за призначенням
Суб'єктивна сторона	Прямий умисел; для ст. 361-1 – наявність мети протиправного використання, розповсюдження чи збуту шкідливих програмних засобів	Створення та продаж шкідливих програм, використання «кряків» для обходу захисту, збут інструментів хакінгу в мережі

Джерело: укладено за [1; 14; 15; 16].

Таблиця 2

Судова практика (2020–2024 рр.): тенденції кваліфікації несанкціонованого втручання

Джерело / дата	Короткий зміст / факти	Кваліфікація / положення КК України	Рішення / результат	Примітки
1	2	3	4	5
Заводський районний суд міста Миколаєва, 16.01.2020 р.	Угода про визнання вини: встановлення вірусної програми для «нейтралізації» паролів	ч. 1/ч. 2 ст. 361	Затверджено угоду про визнання вини	Приклад досудового врегулювання/ угода
Приморський районний суд міста Одеси, 03.04.2020 р.	Несанкціонований доступ до акаунта у Facebook, зміна пароля	ч. 1 ст. 361 (поставлено питання про втручання в систему)	Виправдання	Суд відмежував «доступ до сторінки» від втручання в роботу інформаційно-телекомунікаційних систем
Чернігівський апеляційний суд, 14.04.2021 р.	Неавторизовані дії проти комп'ютерних систем, пов'язані з крадіжкою	ч. 2/інші частини ст. 361 (залежно від справи)	Первинно – 2 роки позбавлення волі; апеляція – посилила покарання	Приклад: апеляція посилила вирок
Печерський районний суд міста Києва, 17.06.2021 р.	Злам корпоративної електронної пошти з використанням шкідливого ПЗ	ч. 2 ст. 361	Визнано винним, штраф	Цифрові докази прийняті

Продовження таблиці 2

1	2	3	4	5
Жовтневий районний суд міста Маріуполя, 19.07.2021 р.	Інсталяція зламаного ArchiCAD 22; обхід захисту «кряком» (Trojan); відтворення ПЗ	ч.1 ст. 361 (втручання в автоматизо-вану систему, спотворення обробки) + ст. 361-1 ч. 1; (суміжно ст.176 ч.1)	Штраф 17 000 грн (за сукупністю); витрати – 6 864 грн; носії – знищити	Показовий перетин ст. 176/361/361-1 (піратство ↔ кібер)
Івано-Франківський міський суд, 09.09.2021 р.	Доступ до бази даних через TeamViewer	ч. 1 ст. 361	Закрито – відсутність наслідків (витоку)	Суд: сам факт доступу без наслідків – не завжди утворює склад злочину
Коропський районний суд Чернігівської області, 15.09.2021 р.	Встановлення шкідливої програми → витік службової інформації	ч. 1/ч. 2 ст. 361	Штраф (вирок) – частково виправдання за іншими епізодами; в апеляції – питання декриміналізації термінології	Ця справа також переглядалася у Верховному Суді (2024) – див. табл. 1
Приморський районний суд міста Одеси, 08.10.2021 р.	Держреєстратор несанкціоновано змінив дані в Державному реєстрі речових прав на нерухоме майно: зареєстрував рухоме майно як цілісний майновий комплекс, включив чуже нерухоме майно; шкода 612 345 грн	ч. 3 ст. 362 (зміна інформації в автомати-зованій системі особою з доступом, за змовою, значна шкода)	Угода; штраф 68 000 грн (ст. 69)	Межа між ст. 361 (втручання) і ст. 362 (зміна даних уповноваженим)
Шевченківський районний суд міста Києва, 12.10.2021 р.	Пособництво: підключення до Wi-Fi компанії, надання віддаленого доступу; несанкціоновані дії з корпоративною поштою	ч. 5 ст. 27 + ч. 2 ст. 361	3 роки позбавлення волі + заборона – 1 рік; іспитовий термін – 1 рік; витрати 10 983,04 грн	Роль доступу до Wi-Fi; систематичність
Заводський районний суд міста Кам'янське, 18.01.2022 р.	Brute-force доступ до облікового запису hotmail через «All-in-one-checker-cracked», витік персональних даних	ч. 2 ст. 361 (за попередньою змовою, витік)	3 роки позбавлення волі + заборона – 1 рік; іспитовий термін – 1 рік; конфіскація ноутбука; витрати 1 716,20 грн	Угода про визнання; використання шкідливого ПЗ
Соборний районний суд м. Дніпра, 19.01.2022 р.	Податківець збував конфіденційні реєстри з інформаційно-телеко-мунікаційних систем «Податковий блок» стороннім особам	ч. 1 ст. 361-2 (збут інформації з обмеженим доступом із систем)	1 рік позбавлення волі; іспитовий термін – 1 рік; витрати – 5 000 грн	Інсайдерське зловживання доступом; повернення ноутбуків

Закінчення таблиці 2

1	2	3	4	5
Соснівський районний суд міста Черкас, 14.02.2022р.	Фішинг – доступ до банківських рахунків	ч. 2 ст. 361; ч. 2 ст. 190	Визнано винним	Розмежування втручання (система) та шахрайства (майно)
Шевченківський районний суд міста Києва, 22.03.2023 р.	Доступ до серверу через віддалене ПЗ	ч. 2 ст. 361	Виправдано (недостатньо логів)	Важливість технічної експертизи
Житомирський районний суд, 11.07.2023 р.	Підключення до FTTB «Київстар», роздача інтернету, використання викраденого логіна	ч. 2 ст. 361	Виправдано – суд вирішив, що не доведено «витік» у правовому сенсі	Суд зазначив, що інтернет-трафік є загальнодоступним
Верховний Суд (касація), 19.09.2024 р.	Чи означає «інформаційна (автоматизована) система» декриміналізацію втручань у ПК?	Тлумачення об'єкта злочину в ст. 361	Ухвалу апеляції скасовано, справу повернено апеляції	Справа стала орієнтиром для подальшого формування судової практики щодо меж кримінальної відповідальності за втручання у комп'ютерні системи

Джерело: побудовано за [15; 16; 17; 18].

Окремі судові рішення демонструють розмежування втручання від суміжних складів злочинів, зокрема шахрайства (ст. 190 КК України) чи службових зловживань (ст. 362 КК України). Показовим є рішення Соснівського районного суду міста Черкас (2022), де суд одночасно застосував ст. 361 і 190 КК України, чітко визначивши об'єкти посягання – інформаційну систему та майнові права потерпілих.

Загалом практика свідчить про активне використання угод про визнання вини (зокрема, у містах Миколаєві та Кам'янському), що зумовлено складністю технічного доказування та прагненням оптимізувати кримінальне провадження. Призначення іспитових строків і штрафів підтверджує переважно превенційний характер покарання, спрямований на ресоціалізацію винних.

Показовим орієнтиром стало рішення Верховного Суду від 19.09.2024 р., у якому наголошено, що зміна терміна «комп'ютер» на «інформаційна система» не змінює сутності складу злочину, підтверджуючи послідовність і стабільність кримінально-правового захисту інформаційного середовища. Це рішення стало логічним підсумком еволюції судової практики, що поступово переходить від формального до змістовного підходу у кваліфікації несанкціонованого втручання.

Визначальним у правозастосуванні стають не самі дії з доступу, а їхні наслідки для конфіденційності, цілісності та доступності даних, що свідчить про зміщення акценту з факту проникнення на ступінь заподіяної шкоди. Саме крізь призму цих критеріїв формується баланс між криміналізацією діяння та дотриманням прав людини у цифровому середовищі. Водночас кваліфікація таких правопорушень залишається складним процесом, який поєднує технічні, доказові та нормативні аспекти, тоді як головні труднощі зумовлені технологічною природою злочинів і відсутністю уніфікованих методичних підходів для слідчих та експертів.

Аналіз судової практики 2020–2024 рр. підтверджує складність кваліфікації несанкціонованого втручання, оскільки суди застосовують різні підходи до тлумачення складу злочину. Зокрема в справах Приморського районного суду міста Одеси (2020) та Івано-Франківського міського суду (2021) розмежовано поняття «доступ до інформації» та «втручання»: сам факт входу до акаунта не визнавався злочином без встановлення наслідків. Натомість у справах, де доведено використання шкідливого ПЗ або витік даних (Печерський районний суд міста Києва, 2021;

Коропський районний суд Чернігівської області, 2021), дії кваліфікували за ч. 2 ст. 361 КК України з акцентом на доказовій ролі цифрових експертиз і технічних логів. Водночас відсутність єдиних технічних стандартів фіксації цифрових доказів нерідко стає причиною виправдувальних вироків (Шевченківський районний суд міста Києва, 2023), що свідчить про методичну неврегульованість експертної діяльності. Додаткові труднощі виникають через конкуренцію норм між ст. 361, 361-1, 362 і 176 КК України (Жовтневий районний суд міста Маріуполя, 2021), коли одні й ті самі дії охоплюють створення, застосування шкідливого коду та порушення авторських прав, що ускладнює визначення об'єкта посягання. Проблемним залишається також визначення повторності та співучасті. У рішеннях Чернігівського апеляційного суду (2021) та Шевченківського районного суду міста Києва (2021) застосовано різні підходи до оцінки триваючих або каскадних кібердій, а також виявлено відсутність критеріїв розмежування ролей учасників – організаторів, виконавців, пособників, особливо у транснаціональних справах.

Отже, окреслені проблеми мають правовий, доказовий і методологічний характер, що ускладнює забезпечення єдності судової практики. Їх систематизація дала змогу виокремити основні напрями вдосконалення кримінально-правового регулювання та практики застосування ст. 361 КК України. Узагальнення результатів представлено в табл. 3, яка відображає ключові науково-практичні підходи до вдосконалення кваліфікації кіберзлочинів.

Таблиця 3

Головні проблеми кваліфікації несанкціонованого втручання та напрями їх розв'язання

Напрям проблеми	Суть труднощів	Приклади з практики (2020–2024 рр.)	Пропоновані напрями вирішення
1. Межі складу злочину (підготовка ↔ замах)	Відсутність критеріїв визначення моменту фактичного втручання	Приморський районний суд міста Одеси (2020); Івано-Франківський міський суд (2021) – відсутність наслідків	Уніфікація критеріїв стадійності; розроблення індикаторів втручання у системи
2. Доказування втручання	Недостатність цифрових доказів, неуніфікованість експертних підходів	Шевченківський районний суд міста Києва (2023) – виправдання через відсутність логів	Впровадження стандартів цифрової експертизи; підготовка IT-експертів для судів
3. Конкуренція норм і сукупність складів	Перетин ст. 361, 361-1, 362, 176 КК України; невизначеність меж між створенням і застосуванням	Жовтневий райсуд міста Маріуполя (2021); Приморський районний суд міста Одеси (2021)	Роз'яснення Верховного Суду; узагальнення практики на основі типових справ
4. Повторність і триваючий характер	Відсутність технічних критеріїв ідентифікації повторності кібердій	Чернігівський апеляційний суд (2021); Коропський районний суд Чернігівської області (2021)	Розроблення алгоритмів цифрової ідентифікації; запровадження блокчейн-аудиту дій
5. Співучасть у кіберпросторі	Відсутність орієнтирів щодо ролей учасників; складність фіксації змови	Шевченківський районний суд міста Києва (2021) – технічне пособництво	Підготовка методичних рекомендацій Міністерства внутрішніх справ і Офісу Генерального прокурора щодо кваліфікації кіберспівучасті
6. Санкційна практика	Диспропорція між шкодою і покаранням; м'якість санкцій	Заводський районний суд міста Миколаєва (2020); Заводський районний суд міста Кам'янське (2022) – іспитові строки	Диференціація санкцій; обов'язкова оцінка масштабів шкоди та мотивів правопорушення

Джерело: авторська розробка.

Узагальнення наведених аспектів показує, що саме судова практика стала каталізатором переосмислення підходів до кваліфікації несанкціонованого втручання в роботу комп'ютерних систем. Вона виявила низку правових, технічних і доказових прогалин, усунення яких неможливе без міждисциплінарної взаємодії юристів, ІТ-фахівців та слідчих. На сучасному етапі формування кіберправової доктрини ключового значення набуває уніфікація методик технічного аналізу, гармонізація кримінально-правових норм із міжнародними підходами та створення національних стандартів щодо збору й оцінки цифрових доказів.

Систематизація судової практики засвідчує, що ефективність кримінально-правової кваліфікації злочинів, передбачених ст. 361 КК України, визначається не лише нормативною чіткістю формулювань, а й практичним змістом цих положень через конкретні судові рішення. Саме правозастосовна практика демонструє, як теоретичні конструкції об'єктивної та суб'єктивної сторін злочину реалізуються в реальних кейсах і які труднощі виникають під час доведення умислу, повторності, співучасті чи розмежування складів за ст. 361 та 361-1 КК України. Подальший розвиток правового регулювання у сфері кіберзлочинів має ґрунтуватися на інтеграції судових висновків у практику досудового розслідування, експертної діяльності та правотворчості.

Висновки. Кваліфікація несанкціонованого втручання в роботу комп'ютерних систем залишається складним міждисциплінарним завданням, у якому поєднуються технічна природа кібердіянь і правові механізми криміналізації. Судова практика 2020–2024 рр. засвідчила перехід від формального до змістовного підходу: ключовим критерієм визначення складу злочину стають не самі дії з доступу, а їх наслідки для конфіденційності, цілісності та доступності інформації. Такий підхід свідчить про еволюцію правозастосування у сфері кібербезпеки та прагнення судів до балансу між захистом інформаційного середовища та дотриманням прав людини. Найбільші труднощі виникають під час розмежування стадій злочину, визначення повторності, сукупності та співучасті, особливо у випадках, коли дії мають транскордонний або анонімний характер. Конкуренція норм між ст. 361, 361-1, 362 і 176 КК України свідчить про відсутність єдиного підходу до визначення об'єкта посягання та кваліфікації кібердіянь.

Судові рішення відіграють системоутворювальну роль, виявляючи методологічні та доказові прогалини й формуючи практичні орієнтири для правозастосування. Їх аналіз підкреслює потребу в тісній співпраці юристів, ІТ-експертів і слідчих, уніфікації методик технічного аналізу цифрових доказів і гармонізації кримінально-правових норм із положеннями Будапештської конвенції. Ефективність застосування ст. 361 КК України визначається не лише змістом норми, а й практикою її тлумачення судами, що забезпечує розвиток цифрової юстиції, підвищення рівня інформаційної безпеки та зміцнення довіри до правової системи у сфері кіберпростору.

Перспективи подальших досліджень полягають у розробленні уніфікованих методик технічної експертизи цифрових доказів, поглибленні міждисциплінарного підходу до кваліфікації кіберзлочинів та адаптації національного законодавства до новітніх викликів цифрового середовища й міжнародних стандартів кібербезпеки.

Список використаних джерел

1. Дрижакова Д. Ю., Горішній О. О., Тараненко М. М. Оцінка ефективності правових механізмів запобігання кіберзлочинності в Україні. *Український політико-правовий дискурс.* 2025. № 9. DOI: https://doi.org/10.5281/zenodo.15074665.

2. Кримінальний кодекс України : Кодекс України від 05 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 08.10.2025).

3. Галушко П. П. Кіберзлочинність: поняття та соціально-правова природа. *Вісник Кримінологічної асоціації України.* 2025. Т. 34, № 1. С. 808–817. DOI: https://doi.org/10.32631/vca.2025.1.66.

4. Khadam N., Anjum N., Alam A., Mirza K. A., Assam M., Ismail E. A. A., Abonazel M. R. How to punish cyber criminals: A study to examine goal-based and consequence-based punishment for malware attacks in the UK, USA, China, Ethiopia, and Pakistan. *Heliyon.* 2023. Vol. 9, № 12. Article e22823. DOI: https://doi.org/10.1016/j.heliyon.2023.e22823.

5. Casino F., Pina C., López-Aguilar P., Batista E., Solanas A., Patsakis C. SoK: Cross-border Criminal Investigations and Digital Evidence. *arXiv preprint.* 2022. arXiv:2205.12911. DOI: https://doi.org/10.48550/arXiv.2205.12911.

6. Dumchikov M., Maletova O., Yanishevska K. Virtual assets in cybercrime: a focus on Ukrainian realities. *Journal of Financial Crime.* 2025. Vol. 32, № 4. P. 919–933. DOI: https://doi.org/10.1108/JFC-02-2024-0057.

7. Bada M., Nurse J. R. C. Profiling the cybercriminal: A systematic review of research. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. IEEE, 14–18 June 2021. P. 1–8. DOI: https://doi.org/10.1109/CyberSA52016.2021.9478246.

8. Stratonov V., Slinko D., Slinko S. Some Types of Computer Crime and Cybercrime in Ukraine. *Access to Justice in Eastern Europe.* 2021. Vol. 3, № 11. P. 191–197. DOI: https://doi.org/10.33327/AJEE-18-4.3-n000078.

9. Зозуля І. В. Правове визначення кіберзлочинів і повноваження Національної поліції в їх протидії. *Форум права.* 2025. Т. 81, № 1. С. 17–30. DOI: https://doi.org/10.5281/zenodo.13923163.

10. Красько М. І., Цевух А. І. Еволюція кіберзлочинності: як кримінальне право адаптується до цифрової ери? *Аналітично-порівняльне правознавство.* 2025. Т. 2, № 3. DOI: https://doi.org/10.24144/2788-6018.2025.03.2.63.

11. Корзун С. В. Понятійно-категоріальний апарат державної кримінально-правової політики протидії кіберзлочинам. *Економіка, управління та адміністрування.* 2025. № 1(111). С. 131–145. DOI: https://doi.org/10.26642/ema-2025-1(111)-131-145.

12. Тютюннікова Г. С., Тютюнніков С. В., Балога С. І., Самусь Є. І., Гедеон Г. О., Кіш Н. Ю., Тютюнніков В. С. Optimization of the manufacturing process of controlling machines with CNC. *Наука і техніка сьогодні.* 2025. № 1(42). С. 984–999. DOI: https://doi.org/10.52058/2786-6025-2025-1(42)-984-999.

13. Дрижакова Д. Ю. Визначення предмета та об'єкта несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361, 361-1 КК України). *Інтернаука.* 2023. № 20. DOI: https://doi.org/10.25313/2520-2057-2023-20-9467.

14. Кривенко К. Кіберзлочинність: актуальна судова практика. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika (дата звернення: 08.10.2025).

15. Хавронюк М. Втручання в роботу інформаційно-комунікаційних систем: кримінальна відповідальність. URL: https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist (дата звернення: 08.10.2025).

16. Система пошуку та аналізу судових рішень. URL: https://verdictum.ligazakon.net/analysis (дата звернення: 08.10.2025).

17. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/ (дата звернення: 08.10.2025).

Дата першого надходження статті до видання: 08.01.2026
Дата прийняття статті до друку після рецензування: 27.01.2026
Дата публікації (оприлюднення) статті: 27.05.2026