УДК 343.9
DOI https://doi.org/10.51989/NUL.2025.6.25

КРИМІНАЛІСТИЧНІ ОСОБЛИВОСТІ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З ІНФОРМАЦІЙНИМИ ТЕХНОЛОГІЯМИ, ТА ХАРАКТЕРИСТИКА ОКРЕМИХ ЇХ РІЗНОВИДІВ

Нагірний Іван Петрович,
orcid.org/0009-0007-1161-0946
аспірант
Приватного вищого навчального закладу
«Європейський університет»

У статті представлено дослідження особливостей злочинів у сфері інформаційних технологій, які виступають одним із найбільш динамічних і небезпечних видів злочинності в сучасному світі. Акцентовано увагу на особливостях злочинів у сфері інформаційних технологій, зокрема на високому рівні латентності, транснаціональному характері, складнощах у процесі виявлення та ідентифікації злочинців. Визначено основні різновиди та вчинення злочинів у сфері інформаційних технологій, аналіз яких демонструє рівень технічної обізнаності кіберзлочинців та їхню здатність до оперативної адаптації в нових умовах цифрового розвитку.

Особливу увагу звернуто на нормативно-правове регулювання злочинності в галузі інформаційних технологій в Україні. Проаналізовано зміст розділу XVI Особливої частини Кримінального кодексу України, в якому законодавцем передбачено настання кримінальної відповідальності за використання комп'ютерів, електронно-обчислювальних машин, мереж і систем зі злочинними цілями. Наголошено на існуванні нагальної потреби в модернізації нормативно-правової бази, з урахуванням новітніх інформаційних викликів і цифрових загроз.

За результатами проведеного дослідження акцентовано увагу на важливості підвищення ефективності діяльності правоохоронних органів у процесі розслідування злочинів у сфері інформаційних технологій, розширенні міжнародної та міжвідомчої співпраці у сфері боротьби з кіберзлочинністю, підвищенні кваліфікації працівників правоохоронних структур, а також формуванні культури цифрової безпеки в суспільстві. Зроблено висновок, що натепер наявна нагальна потреба у використанні комплексного підходу до виявлення, розслідування, протидії та боротьби зі злочинами у сфері інформаційних технологій, що потребує не лише забезпечення ефективного кримінального переслідування винних осіб, але й реалізації превентивних заходів протидії кіберзлочинності на рівні розроблення та запровадження окремих кроків державної політики, а також позитивних змін громадянської свідомості.

Ключові слова: *інформаційні технології, кіберзлочини, комп'ютерна злочинність, протидія кіберзлочинності, кіберзлочинність, несанкціоноване втручання, криміналістична характеристика.*

Nahirnyi Ivan. Forensic features of crimes related to information technologies and characteristics of their individual varieties

The article presents a study of the features of IT crimes, which are one of the most dynamic and dangerous types of crime in the modern world. The focus is on the features of IT crimes, including a high level of latency, transnational nature, and difficulties in the process of detecting and identifying criminals. The main types and types of IT crimes are identified, the analysis of which demonstrates the level of technical awareness of cybercriminals and their ability to quickly adapt to new conditions of digital development.

Special attention is paid to the regulatory and legal regulation of crime in the IT industry in Ukraine. The content of Section XVI of the Special Part of the Criminal Code of Ukraine is analyzed,

in which the legislator provides for the onset of criminal liability for the use of computers, electronic computers, networks and systems for criminal purposes. The urgent need to modernize the regulatory and legal framework is emphasized, taking into account the latest information challenges and digital threats.

The results of the study emphasize the importance of increasing the effectiveness of law enforcement agencies in the process of investigating IT crimes, expanding international and interagency cooperation in combating cybercrime, improving the skills of law enforcement officers, and forming a culture of digital security in society. It was concluded that today there is an urgent need to use an integrated approach to detecting, investigating, countering and combating IT crimes, which requires not only ensuring effective criminal prosecution of perpetrators, but also implementing preventive measures to combat cybercrime at the level of developing and implementing individual steps of state policy, as well as positive changes in civic consciousness.

Key words: *information technology, cybercrime, computer crime, countering cybercrime, cybercrime, unauthorized intervention, forensic characteristics.*

Постановка проблеми. В умовах сьогодення інформаційні технології (далі – ІТ) успішно інтегровані в різноманітні сфери людської діяльності, зокрема в економіку, освіту, оборону та систему національної безпеки держави. Це зумовлює не лише позитивні зміни в суспільному житті, але й різноманітні загрози, пов'язані з використанням цифрових ресурсів у злочинних цілях. Кримінальні правопорушення, які вчиняються у сфері ІТ, з використанням інтернету, комп'ютерної техніки та спеціалізованого програмного забезпечення, нині можна вважати однією з форм злочинності, що найбільш динамічно зростає, у світі.

Злочинам у сфері ІТ притаманні своєрідні особливості, що ускладнюють процес їх виявлення, документування, кваліфікації та розслідування. Зокрема, для кримінальних правопорушень у сфері ІТ характерні транснаціональний масштаб, використання складних систем анонімізації та шифрування даних, здатність до миттєвої модифікації чи знищення цифрового сліду, а також низький рівень підготовки працівників органів досудового розслідування щодо використання кіберпростору. Традиційний криміналістичний інструментарій розслідування кримінальних правопорушень може виявитися неефективним у сфері ІТ, що потребує створення спеціалізованих методик, які враховують технологічні, організаційні та правові аспекти досліджуваної категорії протиправних діянь.

Мета статті полягає у проведенні аналізу криміналістичних особливостей кримінальних правопорушень у сфері ІТ, зокрема специфіки їх вчинення, способів приховування слідів злочину, доказів і обставин, що встановлюються в рамках розслідування.

Аналіз останніх досліджень і публікацій із проблеми. Окремі криміналістичні особливості злочинів, пов'язаних з ІТ, а також їх різновиди виступали предметом дослідження багатьох вітчизняних науковців. Зокрема, праці Г. Авдєєва, А. Баянова, Р. Бєлкіна, І. Васильковського, М. Гвоздецької, В. Стратонова, В. Танасевича, В. Чванкіна, М. Яблокова й інших присвячені загальній кримінологічній характеристиці злочинів, пов'язаних із використанням комп'ютерної техніки та комп'ютерних систем. У дослідженнях К. Ісмайлова, О. Бородай, О. Самойленка, С. Шапочки, В. Голубєва, О. Мотлях, О. Миколенко й інших акцентовано увагу на особистості злочинців, методичних аспектах розслідування, а також на питаннях правової підготовки фахівців, які здійснюють розслідування кримінальних правопорушень у сфері ІТ. Незважаючи на велику кількість наукових праць, присвячених криміналістичним особливостям злочинності у сфері ІТ, дотепер обмежена кількість досліджень окремих різновидів таких видів кримінальних правопорушень.

Виклад основної частини дослідження. Злочинність у сфері ІТ є специфічним різновидом кримінальних правопорушень, які безпосередньо пов'язані із протиправним використанням інформаційних систем і комп'ютерної техніки для досягнення злочинної мети. Така категорія кримінальних правопорушень

характеризується власними особливостями, що зумовлено переважно високим рівнем латентності, оскільки потерпілі не завжди повідомляють правоохоронні органи щодо вчинених проти них протиправних посягань, оскільки впевнені в нездатності до ефективного розслідування такої категорії кримінальних правопорушень та притягнення винних осіб до відповідальності. До того ж користувачі мережі «Інтернет», які стають жертвами інформаційних атак, не завжди готові публічно визнавати факти викрадення своїх особистих даних, оскільки побоюються засудження з боку оточення. У цьому зв'язку М. Гвоздецькою та К. Ісмайловим виділено ключові ознаки кримінальних правопорушень у сфері ІТ, якими є такі:

– високі показники латентності комп'ютерної злочинності, що пов'язано з поширенням інформаційних і комп'ютерних технологій, а також можливістю вчинення протиправних діянь із території іноземної держави;

– відносна легкість учинення кримінальних правопорушень у сфері ІТ зумовлена доступністю комп'ютерних технологій необмеженому колу людей, постійним удосконаленням шахрайського програмного забезпечення;

– інтелектуальний характер злочинності у сфері ІТ, оскільки хоча вчинення кіберзлочинів і не потребує високого соціального статусу від злочинця, проте передбачає опанування специфічних знань;

– відсутність будь-яких вікових обмежень і можливість змінювати свої дані у віртуальному просторі [1, с. 53].

Кримінальні правопорушення, пов'язані з ІТ, несуть підвищену небезпеку, що зумовлено спричиненням шкоди не лише процесам використання інформаційно-комунікаційних систем, але й правам і законним інтересам фізичних і юридичних осіб, підривом авторитету держави. Підвищений рівень небезпечності кримінальних правопорушень у сфері ІТ зумовлений особистістю злочинів, а також можливістю використання інформації як способу та засобу вчинення протиправного діяння. Унаслідок цього спостерігається суттєве зниження ефективності кримінально-правової охорони та захисту суспільних відносин у сфері ІТ [2, с. 285–286].

На законодавчому рівні поняття «інформація» закріплено у ст. 1 Закону України «Про інформацію». Відповідно до зазначеної норми, інформацією виступають будь-які дані, що можуть бути збереженими на матеріальних носіях чи відображені в електронному форматі. Згідно зі ст. 5 Закону, кожна особа наділена правом на інформацію, а саме, щодо вільного отримання, поширення, використання, зберігання та захисту інформації, яка є необхідною для реалізації передбачених законом прав, свобод та інтересів. Реалізація такого права не може призводити до порушення громадських, політичних, економічних, духовних, соціальних, екологічних та інших прав, свобод та інтересів фізичних і юридичних осіб [3].

Натепер законодавцем встановлено кримінальну відповідальність за вчинення протиправних діянь у сфері ІТ. До складів кримінальних правопорушень віднесено такі:

– несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361);

– створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1);

– несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2);

– несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж

електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст. 363);

– перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363^1) [4].

Представлений вище перелік кримінальних правопорушень у сфері ІТ закріплено законодавцем в окремому розділі Особливої частини Кримінального кодексу (далі – КК) України – розд. XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». В інших розділах Особливої частини КК України містяться кримінальні правопорушення, які можуть вчинятися шляхом використання ІТ. Прикладом таких злочинних діянь може бути ст. 182 КК України, що встановлює кримінальну відповідальність за незаконне збирання, зберігання, використання, поширення та знищення конфіденційної інформації про особу чи незаконну зміну такої інформації [4].

Одним із ключових елементів криміналістичної характеристики кримінальних правопорушень у сфері ІТ виступає спосіб учинення протиправного діяння, оскільки саме це слугує кваліфікуючої ознаки. Варто зауважити, що ключові засади захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, зокрема й щодо протидії несанкціонованому втручанню, урегульовано положеннями Закону України «Про захист інформації в інформаційно-комунікаційних системах». Зокрема, нормами вказаного законодавчого акта закріплено трактування різноманітних форм порушення захисту інформації в інформаційно-комунікаційних системах [5]. Більш детально такі порушення захисту інформації представлено в таблиці 1.

У науковій літературі представлено більш широку класифікацію способів скоєння кримінальних правопорушень у сфері ІТ, в основу якої покладено методи отримання доступу до інформаційних систем. До таких різновидів способів скоєння кримінальних правопорушень у сфері ІТ віднесено:

1. Вилучення повністю або частини комп'ютерної техніки з метою вчинення кримінального правопорушення. Такій категорії кримінального правопорушення притаманне використання комп'ютерної техніки суто як предмета злочину, а інші технічні механізми, які не належать до комп'ютерних систем, можуть виступати знаряддям учинення злочину [6, с. 141].

2. Несанкціонований перехват даних та інформації, що передбачає використання злочинцями будь-яких засобів та інструментів перехоплення, зокрема шляхом активного (безпосереднього) чи пасивного (електромагнітного) перехвату, аудіо- чи відеоданих, а також використання так званих «інформаційних відходів». У разі активного перехоплення з метою здійснення підключення до баз даних, отримання паролів

Таблиця 1

Форми порушення захисту інформації в інформаційно-комунікаційних системах

Форма порушення	Визначення
Витік інформації	Результат дій чи бездіяльності, унаслідок чого інформація, обробка якої здійснюється в системі чи з використанням пристроїв обробки інформації, стає доступною чи відомою для фізичних або юридичних осіб, які не мають доступу до неї.
Несанкціоновані дії щодо інформації в системі	Будь-які дії, які здійснюються з допущенням порушень порядку доступу до відповідних даних, установлених положеннями чинного законодавства.
Порушення цілісності інформації в системі	Будь-які несанкціоновані дії, учинені щодо інформації в системі, унаслідок чого допущено зміну її вмісту.

Джерело: складено автором на основі [5].

чи важливої інформації використовуються кабельні мережі чи мікроволни, отримані через супутникові системи, або наземні радіостанції. Якщо ж ідеться про пасивне перехоплення, то існує можливість для приймання, запису та проведення аналізу даних навіть тоді, коли має місце значна відстань між обладнанням.

Захист інформації в разі аудіоперехоплення є досить складним завданням, оскільки його здійснення потребує наявності вартісного обладнання, що дозволяє прослуховувати розмови. Окрім цього, злочинцями часто використовуються вібраційні й акустичні датчики, що забезпечують перехоплення інформації [6, с. 141–142].

3. Отримання несанкціонованого доступу до інформаційних систем і комп'ютерних мереж. Варто зауважити, що кримінальні правопорушення такої категорії можуть учинятися шляхом використання цілої низки різноманітних способів:

a) «за дурнем», тобто вчинення злочинцем проникнення до інформаційних систем за іншими користувачами;

b) «хвіст», що передбачає підключення до зв'язку конкретного користувача та спрямований на перехоплення сигналу з метою доступу до системи;

c) підбір паролів доступу чи пошук вразливих місць у системі безпеки конкретної мережі чи комп'ютерному обладнанні;

d) використання комп'ютерної системи під виглядом законного користувача чи володільця, а також надання правдивих відповідей на запити власника інформаційних систем;

e) використання програм і засобів, а також поломок, що дозволяють обійти систему безпеки даних [7].

4. Реалізація різноманітних форм злочинної діяльності, що спрямована на здійснення маніпуляцій із даними, їх підробку чи підміну, уведення нових даних чи заміну, що мають на меті досягнення злочинного умислу [7].

Додатково в науковій літературі пропонується виділяти два основні види кримінальних правопорушень у сфері ІТ, якими є такі:

1. Кримінальні правопорушення, які спричиняють шкоду електронно-обчислювальним механізмам, зокрема й шляхом втручання в комп'ютерні мережі та інформаційні системи. Учинення кримінальних правопорушень цієї категорії передбачає реалізацію однієї чи більше таких дій: викрадення програмного забезпечення або даних, які зберігаються на носії, їх псування, перехват, підміна, продаж або поширення. Ключовою метою такої категорії злочинних діянь зазвичай визнається отримання матеріальної вигоди; в окремих випадках, наприклад, у разі викрадення інформації, що становить комерційну таємницю, метою може виступати також шпигунство.

2. Кримінальні правопорушення, в яких ІТ використовуються як знаряддя вчинення злочину. Такими видами кримінальних правопорушень є здійснення комп'ютерного саботажу, шпигунство, вимагання даних, викрадення коштів з рахунків та їх розтрата, умисне введення в оману потерпілого тощо [7].

Як зазначає О. Саморай, найбільшу суспільну небезпеку спричиняють такі кримінальні правопорушення у сфері ІТ, які пов'язані з організованою злочинністю. До цих різновидів кримінальних правопорушень у сфері ІТ автором віднесено такі: комп'ютерний тероризм; різноманітні прояви антагоністичної інформаційної боротьби кримінальних формувань із державними та правоохоронними органами; викрадення інформації, що міститься в базах даних чи комп'ютерних програмах; учинення шахрайських дій, пов'язаних із використанням ІТ, особливо в системах кредитно-фінансових, банківських і міжнародних економічних відносин [8, с. 608].

Кримінальні правопорушення у сфері ІТ натепер досить поширені, що зумовлено відчуттям безкарності та складністю встановлення місцезнаходження злочинців. Такі фактори особливо підвищують суспільну небезпечність досліджуваної категорії кримінальних правопорушень, потребують пошуку ефективних механізмів і заходів проведення розслідування протиправних посягань. Зазвичай у разі вчинення кримінальних правопорушень у сфері ІТ йдеться про комплекс злочинних

посягань, що знаходить своє вираження у протиправному втручанні в комп'ютерні чи інформаційні системи, отриманні доступу до конфіденційних даних, їх перехопленні, викраденні, зміні тощо.

Як зазначено П. Берназом, більшість кримінальних правопорушень у сфері ІТ вчиняються у віртуальному просторі. У цьому зв'язку складнощі зумовлені відмінностями між місцем скоєння кримінального правопорушення та настанням суспільно небезпечних наслідків. Зокрема, шкідливе програмне забезпечення може бути занесено до інформаційної системи в один час, проте руйнівний вплив стане помітним лише через певний проміжок часу [9, с. 14].

Висновки. За результатами дослідження криміналістичних особливостей злочинів, пов'язаних з ІТ, встановлено, що для них характерні специфічні ознаки: високі показники латентності, доступність технічного інструментарію та обізнаність широкого кола осіб у використанні можливостей віртуального простору, складнощі у процесі пошуку винних і транскордонний характер. Проаналізовані різновиди злочинів у сфері ІТ підтверджують безперебійне вдосконалення механізмів скоєння кіберзлочинів, що потребує оперативної та ефективної реакції з боку правоохоронних органів.

Проблема протидії злочинам у сфері ІТ ускладнюється тим, що більшість таких кримінальних правопорушень учиняються дистанційно, тобто за межами країни, на території якої має місце настання суспільно небезпечних наслідків, через що існують юридичні перепони для притягнення винних осіб до кримінальної відповідальності. Окрім цього, потерпілі від злочинів у сфері ІТ часто приховують факт учинення щодо них протиправного діяння, що може бути пов'язано з низьким рівнем довіри до правоохоронних органів, страхом глузування і втрати репутації тощо.

Отже, підвищення ефективності протидії злочинам у сфері ІТ потребує вдосконалення механізмів нормативно-правового регулювання, а також налагодження міжнародної та міжвідомчої взаємодії, підвищення кваліфікації співробітників правоохоронних органів, інвестування в новітні цифрові технології, призначені для виявлення та протидії кіберзагрозам. До того ж вагому роль відіграє формування культури інформаційної безпеки й цифрової грамотності в суспільстві, оскільки лише за умови об'єднання зусиль громадянського суспільства, бізнесу та держави можна зменшити рівень загроз у сфері ІТ, а також забезпечити високі показники захисту прав і свобод людини та громадянина в епоху цифровізації.

ЛІТЕРАТУРА:

1. Гвоздецька М., Ісмайлов К. Кримінологічна характеристика кіберзлочинності: сучасний стан, структура та специфіка вчинення. *Актуальні задачі та досягнення у галузі кібербезпеки.* 2016. № 2. С. 52–53.

2. Ховпун О., Домбровська О., Муляр Г. Кримінальні правопорушення у сфері інформаційних технологій: особливості розслідування. *Часопис Київського університету права*. 2020. № 3. С. 285–289.

3. Про інформацію : Закон України № 2657–XII від 02.10.1992 р. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.

4. Кримінальний кодекс України : Закон України № 2341–III від 05.04.2001 р. *Відомості Верховної Ради України.* 2001. № № 25–26. Ст. 131.

5. Про захист інформації в інформаційно-комунікаційних системах : Закон України № 80/96-ВР від 05.07.1994 р. *Відомості Верховної Ради України.* 1994. № 31. Ст. 286.

6. Протидія злочинам у сфері використання інформаційних технологій : інтегрований навчально-практичний посібник. Сєвєродонецьк : РВВ ЛДУВС ім. Е.О. Дідоренка, 2019. 187 с.

7. Близнюк І. Проблеми комп'ютерної злочинності – правовий аспект. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/67cd70e9-8b0f-4ee6-9dbb-1604d96f007e/content (дата звернення: 04.07.2025).

8. Саморай О. Особливості кваліфікації організованої комп'ютерної злочинності в Україні. *Аналітично-порівняльне правознавство :* електронне наукове видання. 2023. № 4. С. 603–607. https://doi.org/10.24144/2788-6018.2023.06.106

9. Берназ П. Структура криміналістичної характеристики злочину. *Південноукраїнський правничий часопис*. 2017. № 3. С. 11–14. URL: https://sulj.oduvs.od.ua/archive/2017/3/5.pdf

Стаття надійшла в редакцію: 14.11.2025
Стаття прийнята: 02.12.2025
Опубліковано: 22.12.2025