УДК 343.9
DOI 10.36919/3041-1149(Print).11.2025.141-147

І. П. Нагірний,
аспірант кафедри права,
ПВНЗ «Європейський університет»
email: i.nagirnui@e-u.edu.ua
ORCID 0009-0007-1161-0946

ЕВОЛЮЦІЯ ПРАВОВОЇ ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ІСТОРИЧНІ ВИТОКИ ТА СУЧАСНІ ВИКЛИКИ

У статті проведено історико-правовий аналіз становлення та розвитку механізмів протидії злочинності у сфері ІТ. Звернуто увагу на основні етапи формування нормативно-правової основи протидії кіберзлочинності на міжнародному та національному рівнях. Зауважено, що в умовах активного розвитку ІТ спостерігається постійне виникнення нових форм злочинності, що за масштабом і способами вчинення значно відрізняються від традиційних видів кримінальних правопорушень. Встановлено, що на міжнародному рівні ключові види кримінальних правопорушень у сфері ІТ врегульовано положеннями Конвенції Ради Європи про кіберзлочинність 2001 року, яку було ратифіковано Україною 2005 року із застереженнями.

Особливу увагу зосереджено на процесах становлення системи нормативно-правового регулювання протидії кіберзлочинності: доповнення положень Кримінального кодексу України 1960 року статтею щодо кримінальної відповідальності за вчинення злочинів, пов'язаних із використанням комп'ютерної техніки, ухвалення нової редакції КК України 2001 року та подальша імплементація міжнародних стандартів. У статті зазначено щодо фрагментарності правового регулювання протидії злочинності у сфері ІТ на національному рівні, а також потреби в удосконаленні нормативно-правової бази, враховуючи виклики сьогодення в цифровій сфері.

Представлено комплексний аналіз змісту та структури розділу XVI Особливої частини КК України, положення якого присвячені врегулюванню кримінальної відповідальності за вчинення кримінальних правопорушень у сфері ІТ. Додатково було розкрито особливості окремих елементів складу кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, зокрема об'єктивних і суб'єктивних ознак, та проблематики законодавчого формулювання. Зауважено, що з метою ефективної протидії кримінальним правопорушенням у сфері ІТ існує потреба не лише в удосконаленні кримінального закону, але й розробці ефективних механізмів імплементації зарубіжного досвіду.

Ключові слова: *інформаційні технології, кіберзлочинність, комп'ютерна злочинність, протидія кіберзлочинності, історико-правовий аспект.*

Постановка проблеми та актуальність. На сьогодні активний розвиток інформаційних технологій (далі – ІТ) відіграє роль не лише вагомим елементом соціально-економічного прогресу, але й своєрідною формою загрози для правових систем і безпеки світових держав. Популярність використання цифрових платформ, перехід до електронного формату документообігу, а також віртуального простору в усіх сферах суспільного життя зумовило виникнення нових форм злочинної поведінки, які називають «кіберзлочини», що за своїм змістом відрізняються від традиційних кримінальних правопорушень за своїм масштабом, способами вчинення та наслідками. Злочини у сфері ІТ вчиняються дистанційно та виходять за межі юрисдикції держав, унаслідок чого національні правові й правоохоронні системи виявляються нездатними до оперативного реагування на нові виклики й загрози.

Правові механізми протидії злочинності у сфері ІТ формувалися впродовж тривалого часу, що потребує детального дослідження особливостей становлення нормативно-правових підходів до протидії кіберзлочинності в різні періоди. Це дає змогу визначити, як саме змінювалися уявлення щодо загроз у віртуальному просторі, які концептуальні підходи були найбільш ефективними чи неефективними в процесі протидії злочинам у сфері ІТ. Водночас до цього часу історично-правові аспекти протидії злочинності у сфері ІТ залишаються малодослідженими, у зв'язку із чим ідеться про існування комплексної проблеми: системному вивченні процесу формування й розвитку механізмів протидії кіберзлочинам, а також урахування сучасного стану й актуальних викликів епохи цифровізації.

Мета статті полягає у здійсненні історико-правового аналізу процесу становлення та розвитку підходів щодо протидії злочинності у сфері ІТ, виявлення загальних тенденцій і специфіки окремих різновидів кримінальних правопорушень у зазначеній галузі.

Аналіз останніх досліджень і публікацій. Окремі аспекти та проблематика протидії злочинам у сфері ІТ через призму історично-правового розвитку були предметом дослідження значної кількості науковців. Так, у працях Ю. Батуріна, П. Біленчука, О. Бодунової, А. Войцехівського, М. Діхтяренка, К. Ісмайлова, С. Круля, Т. Тропіної загально проаналізовано історичні витоки та причини поширення злочинності у сфері ІТ, а також визначено особливості створення системи протидії такому виду злочинів. Зі свого боку дослідження О. Бандурки, О, Кришевича, І. Рощиної, М. Сащенка, В. Тулякова тощо присвячені кримінальним правопорушенням у сфері ІТ як однієї з ключових загроз для безпеки держави. Незважаючи на значну кількість досліджень цього питання, донині в науковій літературі не представлено єдиного ґрунтовного вивчення загальних аспектів і специфіки окремих правопорушень у сфері ІТ через призму історично-правового розвитку, що й обумовлює актуальність цієї статті.

Виклад основної частини дослідження. Вперше потреба в нормативно-правовому регулюванні відповідальності за вчинення інформаційних правопорушень виникла в другій половині XX століття, що пов'язано з активізацією розвитку автоматизованих систем управління та обчислювальної техніки. Уявлення щодо так званих «комп'ютерних злочинів» почало формуватися в країнах Західної Європи та Сполучених Штатах Америки (далі – США) у 1970-х роках, у зв'язку із чим виникла потреба в розробці відповідних правових підходів до протидії протиправним діянням такої категорії [1, с. 91].

1986 року в США було ухвалено федеральний закон «Про комп'ютерне шахрайство і зловживання» (Computer Fraund and Abuse Act), який став першим нормативним актом, спрямованим на системне врегулювання проблеми використання ІТ для вчинення злочинів. До того ж ухвалення зазначеного законодавчого акта стало своєрідною формою реагування на зростання кількості вчинених злочинів із використанням комп'ютерних систем. Положеннями цього закону було передбачено настання кримінальної відповідальності за вчинення таких видів протиправних діянь: незаконне віддалене отримання доступу до урядових чи фінансових комп'ютерних систем; вчинення шахрайських дій із використанням комп'ютерної техніки та ІС; умисне втручання в програми з метою пошкодження даних; здійснення торгівлі паролями доступу до інформаційних баз даних [2]. У подальшому положення вказаного законодавчого акта неодноразово змінювалися, у зв'язку із цим 2001 року було значно розширено повноваження правоохоронних органів у сфері кібербезпеки, що пов'язано із поширенням діяльності терористичних груп.

Перші спроби уніфікації правових підходів у країнах Європи відбувалися переважно під егідою Ради Європи. За результатами тривалої роботи 2001 року було підписано Конвенцію про кіберзлочинність, положеннями якої визначено основні різновиди правопорушень у сфері ІТ, процедурні аспекти та форми співпраці щодо протидії кіберзлочинності на міжнародному рівні. Зокрема, до основних видів кримінальних правопорушень у сфері ІТ положеннями міжнародного документа віднесено такі:

1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних систем і даних: незаконний доступ (ст. 2); нелегальне перехоплення (ст. 3); втручання в дані та систему (ст. 4 та 5); зловживання пристроями (ст. 6).

2. Правопорушення, пов'язані з комп'ютерами: підробка чи шахрайство, пов'язані з комп'ютерами (ст. 7 та 8).

3. Правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією (ст. 9).

4. Правопорушення, пов'язані з порушенням авторських і суміжних прав (ст. 10) [3].

В Україні правове осмислення проблеми поширення кіберзлочинності розпочалося значно пізніше. У 1990-х роках було зроблено перші кроки в напрямі криміналізації окремих діянь, пов'язаних із використанням комп'ютерних систем. Так, 1994 року положення Кримінального кодексу України 1960 року було доповнено ст. 198[1] «Порушення роботи автоматизованих систем», якою встановлено кримінальну відповідальність за вчинення умисного втручання в роботу автоматизованих систем, унаслідок чого було допущено знищення чи викривлення інформації або носіїв інформації, а також поширення технічних і програмних засобів, призначених для протиправного проникнення до автоматизованих систем, що може призвести до вказаних наслідків [4].

Лише після набрання чинності Кримінальним кодексом України (далі – КК України) 2001 року було введено в дію статті, які безпосередньо стосуються кримінальних правопорушень у сфері ІТ, зокрема ст. 361–363 кримінального закону [5]. Незважаючи на численні зміни та доповнення положень розділу XVI Основної частини КК України, на думку О. Бодунової, законодавче регулювання кримінальної відповідальності за вчинення правопорушень у сфері ІТ донині має переважно фрагментарний характер [6, с. 442].

У зв'язку із поширенням злочинних посягань у сфері ІТ 7 вересня 2005 року Україною було ратифіковано Конвенцію про кіберзлочинність 2001 року, положення якої фактично покладено в основу процесу приведення норм національного законодавства у відповідність до міжнародних стандартів кібербезпеки. Водночас положеннями Закону України «Про ратифікацію Конвенції про кіберзлочинність» передбачено певні застереження та заяви щодо виконання нашою державою вказаного міжнародного договору. Зокрема, Україна залишає за собою право щодо декриміналізації діянь, пов'язаних із виготовленням, придбанням для використання, наданням для використання комп'ютерних програм, паролів чи кодів доступу, що має на меті вчинення кримінального правопорушення [7].

У березні 2016 року Указом Президента України було введено Стратегію кібербезпеки України, ключовою метою якої є створення ефективної системи протидії кіберзлочинності на національному рівні [8]. Положення зазначеної Стратегії було переглянуто 2021 року, за результатами чого Указом Президента України від 26 серпня 2021 року затверджено нову Стратегію кібербезпеки України. Як зазначено в положеннях нового стратегічного документа, спостерігається поширення кіберзагроз на всі сфери життя, а також удосконалення інструментарію їхньої практичної реалізації, що потребує підвищення ефективності стратегій і тактики протидії їхньому негативному впливу [9].

З метою повноцінної реалізації положень Стратегії кібербезпеки України 2017 року Верховною Радою України було ухвалено Закон України «Про основні засади забезпечення кібербезпеки України». Положеннями зазначеного законодавчого акта врегульовано ключові правові й організаційні аспекти захисту основоположних прав та інтересів людини й громадянина, суспільства та держави, а також національних інтересів у кіберпросторі. До того ж норми цього Закону визначають основні напрями, цілі та принципи реалізації державної політики у сфері кібербезпеки, повноваження органів державної влади й місцевого самоврядування, юридичних і фізичних осіб, а також ключові аспекти координації їхньої діяльності щодо забезпечення безпеки в кіберпросторі [10].

Отже, в Україні сформовано достатньо значну базу нормативно-правового регулювання сфери забезпечення кібербезпеки. Як зазначають І. Рощина та О. Кришевич, це зумовлено тим, що сфера ІТ займає одне із найважливіших місць в економічній системі, а фахівці ІТ-галузі визнаються одними із найбільш кваліфікованих у цій сфері, працюючи в різноманітних компаніях усього світу. Водночас дослідниками зауважено, що нормативно-правове регулювання сфери ІТ в Україні до сьогодні є дещо застарілим, оскільки не відповідає темпам розвитку технологій, унаслідок чого проблема кіберзлочинності постає особливо гостро [11, с. 120].

Нині склади кримінальних правопорушень у сфері ІТ закріплено в розділі XVI Особливої частини КК України, що має назву «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», що складається із шести статей. Усі кримінальні правопорушення, що містяться в цьому розділі, є винними суспільно небезпечними, протиправними діяннями, які спрямовані проти суспільних відносин у сфері контрольованого використання комп'ютерних даних, а також нормального функціонування комп'ютерної техніки, автоматизованих систем чи мереж комунікації [12, с. 4].

За характеристиками об'єктивної сторони для кримінальних правопорушень у сфері ІТ є притаманна двозначна структура. Так, одні сконструйовані як злочини із формальним складом (наприклад, ст. 361[1] КК України «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»), об'єктивна сторона яких передбачає виключно вчинення суспільно небезпечного діяння. Інші кримінальні правопорушення у сфері ІТ передбачають обов'язкового настання негативних наслідків (наприклад, ст. 363 КК України «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 оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію») [5].

Суб'єктом кримінальних правопорушень, відповідальність за які встановлено в розділі XVI Особливої частини КК України, може бути як загальний, тобто будь-яка фізична осудна особа, яка досягла 16-річного віку, так і спеціальний – особа, яка має доступ до комп'ютерної інформації чи на яку покладено відповідальність щодо безпечної експлуатації систем, мереж і комп'ютерів. За характеристиками суб'єктивної сторони переважна більшість кримінальних правопорушень у сфері ІТ вчиняються із умисною формою вини, крім ст. 363 КК України, для якої є притаманною необережна форма вини [12, с. 5].

Так, до кримінальних правопорушень у сфері ІТ законодавцем віднесено діяння, передбачене ст. 361 КК України, а саме несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [5]. Водночас у диспозиції статті не деталізовано, що саме потрібно розуміти під категорією «несанкціоноване втручання». Як зазначає О. Басараб, під поняттям «несанкціоноване» варто розуміти таке діяння, що вчиняється без дозволу відповідних інстанцій і спрямоване на використання даних, які не перебувають у вільному доступі. За цих обставин несанкціоноване втручання може проявлятися в різноманітних діях, що супроводжуються порушенням порядку доступу до інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, а також електронних комунікаційних мереж, встановленого положеннями чинного законодавства [13, с. 320].

Варто звернути увагу на те, що диспозиції чч. 1 та 2 ст. 361 КК України не містять обов'язкового посилання на настання негативних наслідків. Така позиція законодавця може бути обґрунтована тим, що навіть сам факт несанкціонованого втручання до інформаційних систем є суспільно небезпечним і протиправним діянням, а також наслідком реалізації злочинного умислу, спрямованого на порушення інформаційної безпеки громадян, суспільства та держави загалом, унаслідок чого формує самостійний склад кримінального правопорушення у сфері ІТ. Водночас кваліфікуючими ознаками діяння, передбаченого ст. 361 КК України, є такі: вчинення повторно чи за попередньою змовою групою осіб; спричинення витоку, втрати, підробки чи блокування інформації, викривлення процесу обробки даних чи порушення встановленого порядку маршрутизації інформації; заподіяння значної шкоди або створення небезпеки настання тяжких технологічних аварій чи екологічних катастроф, загибелі або масового інфікування населення чи інших тяжких наслідків; вчинення діяння під час дії правового режиму воєнного стану [5].

Ч. 5 ст. 361 КК України передбачено кримінальну відповідальність за вчинення несанкціонованого втручання в комп'ютерні мережі, вчинено в умовах воєнного стану за умови, що це призвело до тяжких та особливо тяжких наслідків. Варто зауважити, що зазначену норму

було внесено законодавцем до ст. 361 КК України 24 березня 2022 року, тобто вже після початку повномасштабного вторгнення проти України [14]. Потреба в посиленні міри відповідальності за вчинення кримінальних правопорушень у сфері ІТ є цілком обґрунтованою та вагомою ще з часів активізації інформаційної пропаганди проти України в 2013–2014 роках. Отже, посилення санкцій і криміналізація діянь, що загрожують інформаційній безпеці України, дадуть змогу частково стримувати потенційних порушників від скоєння кримінальних правопорушень у сфері ІТ.

Висновки. За результатами історико-правового аналізу становлення системи протидії злочинності у сфері ІТ встановлено, що зазначене питання викликає значні труднощі як на національному, так і на міжнародному рівнях. У міжнародній практиці вагому роль у процесі формування основоположних підходів до криміналізації діянь, пов'язаних із використанням ІТ, відіграли США та країни Західної Європи. Водночас в Україні становлення національного законодавства з питань кримінальної відповідальності за вчинення протиправних посягань із використанням ІТ відбувалося в більш пізній період. Попри це, сьогодні на законодавчому рівні закріплено ряд кримінально-правових норм, які враховують переважну більшість видів кримінальних правопорушень у сфері ІТ.

Незважаючи на сформованість нормативно-правової основи, на рівні національного законодавства існують певні прогалини, зокрема щодо чіткого визначення складів злочинів та застарілості способів вчинення кримінальних правопорушень у сфері ІТ, що зумовлено активним розвитком кіберзлочинності. Це потребує своєчасної та повноцінної адаптації правових норм до реалій сьогодення, коли кіберзлочинність є однією з найбільших загроз для безпеки особи, суспільства й держави загалом. У цьому зв'язку існує потреба в подальшому вдосконаленні механізмів протидії та боротьби із кіберзлочинністю на нормативному й інституційному рівнях, враховуючи міжнародну практику, показники технічного прогресу та динаміку змін у сфері ІТ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бєлєнький В. П. Кіберзлочини за законодавством США. *Науковий вісник Міжнародного гуманітарного університету.* 2015. № 17, т. 2. С. 91–93.

2. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, United States of America. WIPO Lex. URL : https://www.wipo.int/wipolex/en/legislation/details/5768

3. Конвенція про кіберзлочинність від 23.11.2001. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text

4. Кримінальний кодекс України від 28.12.1960. URL : https://zakon.rada.gov.ua/laws/show/2002-05#Text

5. Кримінальний кодекс України від 05 квітня 2001 р. № 2341-ІІІ. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text

6. Бодунова О. М. Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2023. № 4. С. 441–445.

7. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. URL : https://zakon.rada.gov.ua/laws/show/2824-15#Text

8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. URL : https://zakon.rada.gov.ua/laws/show/96/2016#n2

9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text

11. Рощина І. О., Кришевич О. В. Кримінально-правова протидія кіберзлочинності як один із елементів інформаційної безпеки в Україні. *Київський часопис права.* 2023. № 4. С. 116–122.

12. Созанський Т. І., Бурда С. Я., Скиба А. Я. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку у схемах : посібник для підрозділів Національної поліції. Львів : Львівський державний університет внутрішніх справ, 2019. 20 с.

13. Басараб О. Т., Басараб О. К. Кримінально-правовий аналіз несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж. *Юридичний науковий електронний журнал.* 2024. № 2. С. 319–322.

14. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24 березня 2022 року № 2149-IX. URL : https://zakon.rada.gov.ua/laws/show/2149-20#Text

REFERENCES

1. Bielienkyi, V. P. (2015). Kiberzlochyny za zakonodavstvom SShA [Cybercrimes under US law]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu*, 17(2), 91–93.

2. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (1986) (United States). URL : https://www.wipo.int/wipolex/en/legislation/details/5768

3. Convention on Cybercrime (2001). URL : https://zakon.rada.gov.ua/laws/show/994_575#Text

4. Verkhovna Rada of Ukraine. (1960). Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine] (Law No. 2002-05). URL : https://zakon.rada.gov.ua/laws/show/2002-05#Text

5. Verkhovna Rada of Ukraine. (2001). Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine] (Law No. 2341-III). *Vidomosti Verkhovnoi Rady (VVR),* 25–26, art. 131.

6. Bodunova, O. M. (2023). Istoryko-pravovi aspekty vynyknennia zlochynnosti u sferi informatsiinykh tekhnolohii [Historical and legal aspects of the emergence of crime in the field of information technology]. *Analitychno-porivnialne pravoznavstvo*, (4), 441–445.

7. Verkhovna Rada of Ukraine. (2005). Pro ratyfikatsiiu Konventsii pro kiberzlochynnist [On ratification of the Convention on Cybercrime] (Law No. 2824-IV). *Vidomosti Verkhovnoi Rady (VVR),* 5–6, art. 71.

8. President of Ukraine. (2016). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy № 96/2016 [On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cyber Security Strategy of Ukraine": Decree of the President of Ukraine No. 96/2016]. URL : https://zakon.rada.gov.ua/laws/show/96/2016#n2

9. President of Ukraine. (2021). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy № 447/2021 [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cyber Security Strategy of Ukraine": Decree of the President of Ukraine No. 447/2021]. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

10. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cyber security of Ukraine] (Law No. 2163-VIII). *Vidomosti Verkhovnoi Rady (VVR),* 45, art. 403.

11. Roshchyna, I. O., & Kryshevych, O. V. (2023). Kryminalno-pravova protydiia kiberzlochynnosti yak odyn iz elementiv informatsiinoi bezpeky v Ukraini [Criminal law counteraction to cybercrime as one of the elements of information security in Ukraine]. *Kyivskyi chasopys prava*, (4), 116–122.

12. Sozanskyi, T. I., Burda, S. Ya., & Skyba, A. Ya. (2019). Kryminalno-pravova kharakterystyka zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozv'iazku u skhemakh [Criminal and legal characteristics of crimes in the field of using electronic computers (computers), systems and computer networks and telecommunication networks in schemes]. Lviv State University of Internal Affairs.

13. Basarab, O. T., & Basarab, O. K. (2024). Kryminalno-pravovyi analiz nesanktsionovanoho vtruchannia v robotu informatsiinykh (avtomatyzovanykh), elektronnykh komunikatsiinykh, informatsiino-komunikatsiinykh system ta elektronnykh komunikatsiinykh merezh [Criminal law analysis of

unauthorized interference in the work of information (automated), electronic communication, information and communication systems and electronic communication networks]. *Yurydychnyi naukovyi elektronnyi zhurnal*, (2), 319–322.

14. Verkhovna Rada of Ukraine. (2022). Pro vnesennia zmin do Kryminalnoho kodeksu Ukrainy shchodo pidvyshchennia efektyvnosti borotby z kiberzlochynnistiu v umovakh dii voiennoho stanu [On amendments to the Criminal Code of Ukraine regarding increasing the efficiency of the fight against cybercrime under martial law] (Law No. 2149-IX). Ofitsiinyi visnyk Ukrainy, 33, art. 1739.

I. P. Nahirnyi. HISTORICAL AND LEGAL RESEARCH ON COMBATING CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY: GENERAL ASPECTS AND SPECIFICS OF INDIVIDUAL OFFENSES

The article provides a historical and legal analysis of the formation and development of mechanisms for combating crime in the IT sector. Attention is drawn to the main stages of the formation of the regulatory and legal framework for combating cybercrime at the international and national levels. It is noted that in the conditions of active development of IT, there is a constant emergence of new forms of crime, which in terms of scale and methods of commission are significantly different from traditional types of criminal offenses. It is established that at the international level, key types of criminal offenses in the IT sector are regulated by the provisions of the Council of Europe Convention on Cybercrime of 2001, which was ratified by Ukraine in 2005 with reservations.

Particular attention is paid to the processes of formation of the system of regulatory and legal regulation of counteraction to cybercrime: supplementing the provisions of the Criminal Code of Ukraine of 1960 with an article on criminal liability for crimes related to the use of computer technology, adoption of a new edition of the Criminal Code of Ukraine in 2001 and further implementation of international standards. The article notes the fragmentation of legal regulation of counteraction to crime in the IT sector at the national level, as well as the need to improve the regulatory and legal framework, taking into account today's challenges in the digital sphere.

The article presents a comprehensive analysis of the content and structure of Section XVI of the Special Part of the Criminal Code of Ukraine, the provisions of which are devoted to the regulation of criminal liability for committing criminal offenses in the IT sector. Additionally, the features of individual elements of the composition of criminal offenses were revealed.in the field of use of electronic computers (computers), systems and computer networks and telecommunications networks, in particular objective and subjective signs, and the issues of legislative formulation. It was noted that in order to effectively combat criminal offenses in the IT sector, there is a need not only to improve the criminal law, but also to develop effective mechanisms for implementing foreign experience.

Keywords: *information technology, cybercrime, computer crime, counteraction to cybercrime, historical and legal aspect.*