DOI: https://doi.org/10.26642/sas-2025-1(7)-55-62
УДК 351

Грицишен Димитрій
доктор економічних наук, доктор наук з державного управління, професор
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0002-1559-2403

Соха Станіслав
кандидат юридичних наук, докторант
Державний університет «Житомирська політехніка»
https://orcid.org/0009-0004-2606-1263

Корзун Світлана
аспірантка
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0002-8360-6766

Бовсунівський Сергій
аспірант
Державний університет «Житомирська політехніка»
https://orcid.org/0009-0004-0015-0399

Становлення кримінальної відповідальності за кіберзлочини в Україні

Анотація. У статті висвітлюються актуальні питання щодо протидії кіберзлочинам в Україні та досліджується ґенеза становлення кримінальної відповідальності за ці злочини у вітчизняному законодавстві. На сучасному етапі розвитку кіберзлочинність є однією з найбільших глобальних загроз, як для України, так і для усього світу. Саме тому дослідження кримінальної відповідальності за кіберзлочини в Україні набуло особливої актуальності та значного поширення.

Проаналізовано нормативно-правову базу протидії кіберзлочинам та становлення кримінальної відповідальності за ці злочини. Зокрема, розглянуто особливості кримінальної відповідальності за кіберзлочини в умовах повномасштабного вторгнення, а саме посилення заходів щодо інформаційної безпеки України. Детально проаналізовано положення Кримінального кодексу України в частині встановлення кримінальної відповідальності за кіберзлочини. Визначено види кримінальних правопорушень та відповідні види покарань, а саме: штраф, обмеження волі, виправні роботи, пробаційний нагляд, позбавлення волі, позбавлення права обіймати певні посади або займатися певною діяльністю за статтями Кримінального кодексу, враховуючи обтяжуючі обставини. Особливу увагу в роботі зосереджено на аналізі змісту проєктів нового Кримінального кодексу України, зокрема, визначено принципові відмінності від чинного законодавства, а саме види покарань залежно від тяжкості злочину тощо. У статті визначено специфічні особливості кримінальної відповідальності за кіберзлочини відповідно до чинного Кримінального кодексу України (2001 р.). Також здійснено аналіз змісту проєкту Кримінального кодексу України від 01.08.2024 р., розробленого Робочою групою з питань розвитку кримінального права, та порівняння його з чинним законодавством. Це дозволяє визначати особливості реформування кримінального законодавства в сфері кіберзлочинів відповідно до динамічних змін безпекового середовища.

Ключові слова: кіберзлочин; кіберзлочинність; кримінальна відповідальність; Кримінальний кодекс України; штраф; інформаційні системи; комп’ютерні дані.

Постановка проблеми. Питання протидії кіберзлочинам в Україні є досить важливим як з позиції забезпечення інформаційної безпеки держави, так і з позиції інформаційного захисту бізнесу. Адже кіберзлочини можуть здійснюватися в різноманітних сферах суспільного життя й відповідно мати різноманітні наслідки як для держави в цілому, так і для суб’єктів господарської діяльності та громадян. «В умовах гібридної війни, тотального використання засобів масової інформації та її комунікаційних складових частин особливої актуальності набуває попередження основних загроз кіберзлочинності. Як свідчать результати наукових досліджень, проблематика кіберзлочинності хвилює не тільки державу, а й окремих господарюючих суб’єктів, практично кожну особу. Кіберзлочинність є неминучим наслідком глобалізації інформаційних процесів і становить серйозну загрозу для соціогуманітарної сфери та інших компонентів суспільства. Зростаюча кількість кіберзлочинної діяльності на підприємствах, постійна

модернізація інформаційних технологій і нові можливості для «вдосконалення» інструментів щодо їхньої реалізації створюють економічні загрози для глобальних інформаційних мереж» [9].

Щодо захисту бізнесу варто зазначити, що «трьома країнами з найбільшою кількістю кіберзлочинів є США, Китай та Німеччина. І проблема полягає не в слабкому захисті зі сторони уряду, а саме в зацікавленості злочинців, оскільки вказані країни мають велику кількість зареєстрованих компаній, що є дуже цінними для зловмисників. Незважаючи на усі законодавчі ініціативи та створені агентства (Federal Bureau of Investigation, National Cyber Investigative Task Force, National Security Agency у США, Cyberspace Administration у Китаї, European Cybercrime Centre в ЄС), про захист компанії передусім повинні пам'ятати її власники. Адже кібератаки призводять до колосальних репутаційних та фінансових втрат, причому від них не застрахований ані малий, ані великий бізнес» [6]. Це вказує на незахищеність бізнесу й, відповідно, економічної системи держави. Внаслідок кіберзлочинів з'являються значні ризики, що стосуються як інформаційної безпеки держави, так і національної безпеки загалом. Адже кібератаки на критично важливу інфраструктуру загрожують воєнній, економічній, продовольчій та іншим видам безпеки. «Існування кіберзлочинності є досить серйозною проблемою в умовах глобального процвітання інноваційно-технологічних ресурсів. Це впливає абсолютно на всіх: як на окремих фізичних та юридичних осіб, так і на об'єкти критичної інфраструктури й державні органи. Окрім безпосередньої шкоди, кіберзлочинність є величезною загрозою для цифрової довіри, значною мірою підриваючи переваги кіберпростору» [3]. Відповідно, для України в умовах війни нагальною є потреба в посиленні кримінальної відповідальності за кіберзлочини. Це вимагає дослідження еволюції державницьких підходів до кримінальної відповідальності за кіберзлочини та визначення основних пріоритетів та векторів розвитку державної політики.

Аналіз останніх досліджень та публікацій. Питання кримінальної відповідальності за кіберзлочини в Україні стали об'єктом наукового дослідження багатьох вітчизняних вчених у сфері юридичних, економічних, політичних наук та наук державного управління. Зокрема, варто наголосити на працях таких вчених: Д.О. Грицишена, К.В. Малишева, С.О. Савчука, В.В. Євдокимова, Т.В. Барановської, А.П. Дикого, В.О. Кучменка, О.В. Кравчука, Т.С. Ярового, М.О. Думчикова, І.В. Каріх, Т.П. Яцик, К.О. Кислої, Т.М. Пушкарьової, Н.А. Загребельної, І.Д. Казанчук, А.В. Котелевець, О.М. Будонової, М.О. Будакового, В.М. Бутузова, М.М. Галамбо, Р.А. Калюжного, Н.В. Камінської, В.В. Коваленко, Я.Ю. Кондратьєва, Б.А. Кормичема, Ю.Є. Максименка, А.І. Марущака, Г.В. Новицького та інших.

Мета статті – дослідити питання кримінальної відповідальності за кіберзлочини в Україні.

Викладення основного матеріалу. «Інтернет зруйнував бар'єри між країнами, спільнотами та громадянами, дав можливість взаємодіяти та обмінюватися інформацією й ідеями у всьому світі. Щоб кіберпростір залишався відкритим, вільним та безпечним, в Інтернеті повинні застосовуватися ті самі норми, принципи та цінності, що існують в офлайн-режимі. У сучасному світі розвиток інформаційних технологій відкриває нові можливості для комунікації, бізнесу та науки. Однак поряд з позитивними аспектами цифровізації зростає рівень кіберзлочинності, яка стає однією з найсерйозніших загроз для безпеки держав, організацій та окремих осіб. Кіберзлочинність охоплює широкий спектр кримінальних правопорушень: від крадіжки особистих даних і фінансових шахрайств до атак на критичні інфраструктури. Незважаючи на зусилля урядів та міжнародних організацій щодо створення ефективних заходів протидії кіберзлочинності, кількість та складність таких кримінальних правопорушень продовжує зростати. Це вимагає постійного вдосконалення правових, технологічних та організаційних механізмів захисту» [1].

«Сьогодні кіберзлочинність є, напевно, однією з найбільших глобальних загроз як для України, так і для усього світу. За даними всесвітнього огляду економічних злочинів Pricewater house Coopers (PWC) за 2021 р., кримінальні правопорушення у кіберпросторі досягли найвищого рівня за весь період публікаційних оглядів. Так рівень злочинності збільшився з 24 % у 2014 р. до 39 % у 2021 р., тим самим посівши друге місце серед економічних кримінальних правопорушень у світі, залишивши позаду злочини, пов'язані з легалізацією грошових коштів, отриманих незаконним шляхом, та різні корупційні кримінальні правопорушення. Однак вказані дані значною мірою не відповідають дійсності, адже кримінальні правопорушення, вчинені в кіберпросторі, є дуже латентними за своєю ознакою, тому реальна картина та статистика мають інший вигляд. Це зумовлено насамперед відсутністю чітких методів збирання даних про вчинення кримінальних правопорушень у кіберпросторі та певними характерними особливостями зазначеного виду кримінальних правопорушень» [2].

Особливості становлення та розвитку державної кримінально-правової політики протидії кіберзлочинам та становлення кримінальної відповідальності за ці злочини досліджено в попередніх працях. У цій статті головна увага зосереджена на сучасному стані кримінальної відповідальності за цей вид злочинів.

«Одним з напрямів боротьби з цим негативним явищем є прийняття на законодавчому рівні нормативно-правових актів, які регулюють відносини у цій сфері. Зокрема, складовими нормативно-правової бази у цій сфері є: Конституція України, Кримінальний кодекс України, закони України: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про основи національної безпеки», Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, затверджені Верховною Радою України як обов'язкові. Також з метою недопущення зростання рівня кіберзлочинності Верховна Рада України прийняла Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах воєнного стану», який набув чинності 24 березня

2022 р. Метою цього закону є забезпечення надійності та безпеки використання цифрових послуг, впровадження дієвих кримінально-правових механізмів протидії кіберзлочинності, оптимізація національної системи кібербезпеки щодо протидії кіберзагрозам. Відповідне посилення санкцій та додаткова криміналізація окремих діянь, на нашу думку, здатні частково стримати потенційних злочинців від вчинення нових кримінальних правопорушень» [3].

Наголосимо на тому, що повномасштабне вторгнення зумовило потребу в підвищенні рівня кримінальної відповідальності за кіберзлочини. Це спонукало законодавців до активності у цьому напрямі, зокрема в першій половинні 2022 р. У цьому контексті рішенням Ради національної безпеки та оборони України, введеним у дію указом президента, було посилено заходи щодо інформаційної безпеки України. Це своєю чергою стало підставою для гармонізації Кримінального кодексу України із законодавством щодо забезпечення кібербезпеки. «Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» набув чинності 03.04.2022 р. (опублікований в «Голосі України» 02.03.2022 р.), згідно з яким: 1) ст. 361 та 361-1 КК України узгоджені з законодавством у сфері кібербезпеки; 2) у ст. 361 КК України розмежована суворість покарання за кібератаку, залежно від наслідків, та посилилось покарання: від штрафу до 15 років ув'язнення; 3) пошук та виявлення вразливостей не є кібератакою (ч. 6 ст. 361 КК України); 4) посилено покарання за ст. 361-1 КК України: від штрафу до 5 років ув'язнення» [8].

Розглянемо більш детально положення Кримінального кодексу України в частинні встановлення кримінальної відповідальності за кіберзлочини. Кримінальний кодекс України було введено в дію у 2001 р., проте протягом більш ніж 20 років він неодноразово піддавався критиці, а станом на 1 січня 2025 р. до нього було внесено понад 800 змін та доповнень. Цим нормативним актом встановлено кримінальну відповідальність за досліджувані злочини. Зокрема, цьому присвячено Розділ XVI Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, який передбачає покарання за такі види кримінальних правопорушень:

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

– створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (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, створеної та захищеної відповідно до чинного законодавства (ст. 361.2);

– несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 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 оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію (ст. 363);

– умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363.1).

Види покарань за зазначеними статтями Кримінального кодексу та обтяжуючі обставини перелічені в таблиці 1.

Відповідно до зазначених в таблиці даних, виділяються такі види покарання за скоєння кіберзлочинів:

– штраф. За кожною із вказаною вище статтею Кримінального кодексу передбачено різну суму штрафу. Загалом зазначена сума може варіюватися від однієї тисячі до чотирьох тисяч неоподатковуваних мінімумів доходів громадян. Якщо йдеться про обтяжуючі обставини, які передбаченні досліджуваним розділом Кримінального Кодексу, то сума штрафу буду варіюватися від трьох тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян, і лише згідно зі ст. 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»;

– обмеження волі. Один із видів покарань за кримінальні правопорушення, що визначається ст. 61 Кримінального кодексу України. Зокрема, у цій статті зазначено: «Покарання у виді обмеження волі полягає у триманні особи в кримінально-виконавчих установах відкритого типу без ізоляції від суспільства в умовах здійснення за нею нагляду з обов'язковим залученням засудженого до праці» [5]. Максимальний строк обмеження волі до п'яти років за кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, і лише згідно зі ст. 361;

Таблиця 1

Кримінальна відповідальність за кіберзлочини в Україні

Злочин	**Покарання**	**Обтяжуючі та/або пом'якшуючі обставини**	
		Обставина	**Покарання**
1	*2*	*3*	*4*
Стаття 361			
Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж	Штраф від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або пробаційний нагляд на строк до трьох років, або обмеження волі на той самий строк	Дії, вчинені повторно або за попередньою змовою групою осіб	Штраф від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеження волі на строк від двох до п'яти років, або позбавлення волі на той самий строк
		Дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації	Штраф від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк від трьох до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого
		Дії заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків	Позбавлення волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого
		Дії вчинені під час дії воєнного стану	Позбавлення волі на строк від десяти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років
Стаття 361.1			
Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років, або позбавлення волі на строк до трьох років	Дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду	Позбавлення волі на строк до п'яти років

Закінчення табл. 1

1	*2*	*3*	*4*
Стаття 362			
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	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років	Дії призвели до витоку інформації	Позбавлення волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк
		Дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду	Позбавлення волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років
Стаття 363			
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	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або пробаційний нагляд на строк до трьох років, або обмеження волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк	Не передбачено	Не передбачено
Стаття 363.1			
Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років	Дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду	Обмеження волі на строк до п'яти років або позбавлення волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років

– виправні роботи. Згідно зі ст. 57 Кримінального кодексу України, передбачено, що «покарання у вигляді виправних робіт встановлюється на строк від шести місяців до двох років і відбувається за місцем роботи засудженого. Із суми заробітку засудженого до виправних робіт провадиться відрахування в доход держави у розмірі, встановленому вироком суду, в межах від десяти до двадцяти відсотків» [5]. Згідно зі ст. 361.1 та 362, передбачено можливість покарання у вигляді виправних робіт до двох років;

– пробаційний нагляд. Регулюється ст. 59.1, згідно з якою: «Покарання у виді пробаційного нагляду полягає в обмеженні прав і свобод засудженого, визначених законом і встановлених вироком суду, із застосуванням наглядових та соціально-виховних заходів без ізоляції від суспільства» [5]. Цією статтею передбачено різносторонні види нагляду;

– позбавлення волі. Це найсуворіший вид покарання за кіберзлочини. Якщо не враховувати обтяжуючі обставини за досліджуваними статтями Кримінального кодексу, то найбільший строк (до трьох років) передбачено згідно зі ст. 361.1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут». В той же час, якщо дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, передбачено позбавлення волі на строк до п'яти років;

– позбавлення права обіймати певні посали або займатися певною діяльністю. «Позбавлення права обіймати певні посади або займатися певною діяльністю може бути призначене як основне покарання на строк від двох до п'яти років або як додаткове покарання на строк від одного до трьох років» [5]. Цей вид покарання на строк до трьох років передбачено згідно зі ст. 361 за таких умов: а) дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації; б) дії заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків; в) дії вчинені під час дії воєнного стану. Таке ж покарання передбачено згідно зі ст. 362 та 363 за умови, якщо дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Щодо реформування кримінального законодавства варто наголосити, що вже протягом декількох років йде робота над розробкою нового Кримінального кодексу України. «Відповідно до Указу Президента України №584/2019 від 07.08.2019 р. було створено Комісію з питань правової реформи, основним завданням якої є сприяння подальшому розвитку правової системи України на основі конституційних принципів верховенства права, пріоритетності прав і свобод людини і громадянина з урахуванням міжнародних зобов'язань України. Частиною цієї Комісії стала Робоча група з питань розвитку кримінального права, до складу якої увійшли одні з кращих представників провідних юридичних шкіл України, та на яку покладено низку завдань, одним з яких є підготовка пропозицій стосовно змін до законодавства України про кримінальну відповідальність. Діяльність цієї групи підтримується Консультативною місією Європейського Союзу в Україні» [7].

Відповідно до сьогоднішнього стану, Робочою групою з питань розвитку кримінального права розроблено декілька проєктів нового Кримінального кодексу України. Так на сайті Робочої групи розміщено черговий проєкт від 01.08.2024 р. [4] Проаналізувавши зміст зазначеного кодексу, необхідно наголосити на розумінні кіберзлочинів як кримінальних правопорушень проти суспільства (книга сьома «Кримінальні правопорушення проти суспільства»). Так кіберзлочини розглядаються як злочини проти безпеки інформаційних систем. Варто зазначити, що проєкт значно відрізняється від діючого Кримінального кодексу, зокрема в частині встановлення покарання за злочини. Так у проєкті визначено ступінь тяжкості злочину, відповідно до якого визначається вид покарання: 1) громадські роботи; 2) штраф; 3) обмеження свободи; 4) строкове ув'язнення; 5) довічне ув'язнення.

Відповідно до Розділу 7.7 Кримінальні правопорушення проти безпеки інформаційних систем, передбачено такі види кримінальних правопорушень:

– незаконний доступ до інформаційної системи;

– незаконне перехоплення комп'ютерних даних: 1) при їх виході з інформаційної системи, 2) при їх надходженні до інформаційної системи або 3) при операції з ними всередині інформаційної системи;

– незаконне поводження з комп'ютерними даними: 1) знищення комп'ютерних даних, 2) пошкодження комп'ютерних даних, 3) заблокування комп'ютерних даних, 4) порушення цілісності комп'ютерних даних, 5) порушення порядку маршрутизації комп'ютерних даних або 6) спотворення процесу обробки комп'ютерних даних;

– незаконні діяння зі шкідливим програмним чи технічним засобом або шкідливими даними (даними доступу): 1) виготовлення, 2) набуття, 3) переміщення, 4) збут або 5) поширення.

Ознаками, що підвищують тяжкість кіберзлочинів, передбачених цим Розділом, є вчинення умисного злочину:

– у складі простої групи;

– з використанням службових повноважень чи професійних обов'язків або пов'язаних із ними можливостей;

– з використанням шкідливого програмного чи технічного засобу або шкідливих даних (даних доступу);

– в особливий період чи в умовах надзвичайного стану;

– особою, яка має правомірний доступ до інформаційних систем або інформації з обмеженим доступом;

– з метою здійснення переказу грошей, майнових цінностей або віртуальної валюти.

Висновки. Таким чином, у результаті проведеного дослідження визначені специфічні риси кримінальної відповідальності за кіберзлочини відповідно до чинного кримінального законодавства (Кримінальний кодекс України 2001 р.). Аналіз проєкту Кримінального кодексу України від 01.08.2024 р., розробленого Робочою групою з питань розвитку кримінального права, засвідчив наявність низки відмінностей як у частині визначення міри покарання, так і у формулюваннях правових положень. Зокрема, такі поняття, як «автоматизовані системи» та «мережі електрозв'язку» у проєкті не згадуються, а кіберзлочини пов'язані з діями щодо інформаційних систем, комп'ютерних даних та програмних продуктів. Крім того, в умовах війни важливого значення набувають кібератаки на критичну інфраструктуру, про що також не згадується в проєкті нового Кримінального кодексу. Отже, зазначене дослідження є підґрунтям для розробки векторів розвитку кримінального законодавства у сфері протидії кіберзлочинам. Перспективи вдосконалення кримінального законодавства у зазначеній сфері будуть розглянуті у подальших наукових дослідженнях.

Список використаних джерел:

1. *Аніщук В.В.* Проблема протидії кіберзлочинності : порівняльно-правовий аналіз / *В.В. Аніщук, С.Г. Зищик* // Науковий вісник Ужгородського Національного Університету. – 2024. – Вип. 83, Ч. 3. – С. 19–23 [Електронний ресурс]. – Режим доступу : https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4-2.pdf.
2. *Думчиков М.О.* Становлення та генеза кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на теренах України / *М.О. Думчиков, І.В. Карікх* // Юридичний науковий електронний журнал. – 2022. – №5. – С. 476–478 [Електронний ресурс]. – Режим доступу : http://lsej.org.ua/5_2022/113.pdf.
3. «Кіберзлочинність : виклики часу» [Електронний ресурс]. – Режим доступу : https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/.
4. Кримінальний кодекс України : Контрольний текст проекту станом на 01.08.2024 р. [Електронний ресурс]. – Режим доступу : https://newcriminalcode.org.ua/upload/media/2024/08/02/kontrolnyj-tekst-proyektu-kk-stanom-na-01-08-2024.pdf.
5. Кримінальний кодекс України : документ 2341-III **;** *редакція від 01.02.2025, підстава 4200-IX* [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2341-14#Text.
6. *Лугова Є.* Протидія кіберзлочинам : правила корпоративного захисту. [Електронний ресурс]. – Режим доступу : https://eba.com.ua/protydiya-kiberzlochynam-pravyla-korporatyvnogo-zahystu/.
7. «Передумови розробки нового Кримінального кодексу України» [Електронний ресурс]. – Режим доступу : https://newcriminalcode.org.ua/about-us#block1.
8. «Посилено кримінальну відповідальність за кіберзлочини» [Електронний ресурс]. – Режим доступу : https://capital-ukraine.com/posyleno-kryminalnu-vidpovidalnist-za-kiberzlochyny/.
9. *Шемчук В.В.* Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні / *В.В. Шемчук* // Вчені записки ТНУ імені В.І. Вернадського. – 2018. – Том 29 (68), № 6. – С. 119–124 [Електронний ресурс]. – Режим доступу : https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf.

References:

1. Anishchuk, V.V. and Zytsyk, S.H. (2024), «Problema protydii kiberzlochynnosti: porivnialno-pravovyi analiz», *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu*, Vol. 83, No. 3, pp. 19–23, [Online], available at: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4-2.pdf
2. Dumchykov, M.O. and Karikh, I.V. (2022), «Stanovlennia ta heneza kryminalnoi vidpovidalnosti za kryminalni pravoporushennia u kiberprostori na terenakh Ukrainy», *Yurydychnyi naukovyi elektronnyi zhurnal*, Vol. 5, pp. 476–478. [Online], available at: http://lsej.org.ua/5_2022/113.pdf
3. «Kiberzlochynnist: vyklyky chasu», [Online], available at: https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/
4. «Kryminalnyi kodeks Ukrainy : Kontrolnyi tekst proektu stanom na 01.08.2024 r.», [Online], available at: https://newcriminalcode.org.ua/upload/media/2024/08/02/kontrolnyj-tekst-proyektu-kk-stanom-na-01-08-2024.pdf
5. Verkhovna Rada Ukrainy (2025), *Kryminalnyi Kodeks Ukrainy*, document 2341-III, redaktsiia vid *01.02.2025*, pidstava – *4200-IX*, [Online], available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text
6. Luhova, Ye. «Protydiia kiberzlochynam: pravyla korporatyvnoho zakhystu», [Online], available at: https://eba.com.ua/protydiya-kiberzlochynam-pravyla-korporatyvnogo-zahystu/
7. «Peredumovy rozrobky novoho Kryminalnoho kodeksu Ukrainy», [Online], available at: https://newcriminalcode.org.ua/about-us#block1

8. «Posyleno kryminalnu vidpovidalnist za kiberzlochyny», [Online], available at: https://capital-ukraine.com/posyleno-kryminalnu-vidpovidalnist-za-kiberzlochyny/
9. Shemchuk, V.V. (2018), «Kiberzlochynnist yak pereshkoda rozvytku informatsiinoho suspilstva v Ukraini», *Vcheni zapysky TNU imeni V.I. Vernadskoho*, Vol. 29 (68), No. 6, pp. 119–124, [Online], available at: https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf

Grytsyshen D., Sokha S., Korzun S., Bovsunivskyi S.

Establishment of criminal liability for cybercrimes in Ukraine

Abstract. This study reveals the current issues of countering cybercrimes in Ukraine and explores the genesis of the establishment of criminal liability for these crimes in domestic legislation. At the current stage of development, cybercrime is one of the biggest global threats, both for Ukraine and for the whole world, which is why the study of criminal liability for cybercrimes in Ukraine has become so relevant and widespread.

The authors of this study analyzed the regulatory framework for countering cybercrimes and the establishment of criminal liability for these crimes. In particular, the features of criminal liability for cybercrimes in the context of a full-scale invasion were considered, namely, the strengthening of measures for the information security of Ukraine. The provisions of the Criminal Code of Ukraine regarding the establishment of criminal liability for cybercrimes were analyzed in detail. Types of criminal offenses and corresponding types of punishments are determined, namely: fine, restriction of liberty, correctional labor, probation supervision, imprisonment, deprivation of the right to hold certain posts or engage in certain activities under the articles of the Criminal Code, taking into account aggravating circumstances. Particular attention in the work was focused on the analysis of the content of the drafts of the new Criminal Code of Ukraine, in particular, the fundamental differences from the current legislation were determined, namely the levels of punishment depending on the severity of the crime and others.

Thus, this article determines the specific features of criminal liability for cybercrimes in accordance with the current Criminal Code of Ukraine (2001), analyzes the content of the draft Criminal Code of Ukraine dated 01.08.2024, developed by the Working Group on the Development of Criminal Law and compares it with the current legislation, which allows determining the features of reforming criminal legislation in the field of cybercrimes in accordance with dynamic changes in the security environment.

Keywords: cybercrime; cybercrime; criminal liability; Criminal Code of Ukraine; fine; information systems; computer data.

Стаття надійшла до редакції 14.01.2025.