УДК 340.8
DOI https://doi.org/10.32782/2408-9257-2024-6-31

Лавренюк В. А.,
аспірант кафедри кримінального права та процесу
Державного податкового університету

ІСТОРІЯ ВИНИКНЕННЯ ТА РОЗВИТКУ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ: ВІТЧИЗНЯНИЙ ТА ЗАРУБІЖНИЙ АНАЛІЗ

THE HISTORY OF THE EMERGENCE AND DEVELOPMENT OF COMPUTER CRIMES: DOMESTIC AND FOREIGN ANALYSIS

Протидія комп'ютерним злочинам є однією з найактуальніших проблем сучасності. Їх специфічні особливості та стрімкий розвиток ставлять перед суспільством і міжнародною спільнотою важливі завдання щодо кримінально-правового захисту кіберпростору.

Стаття присвячена дослідженню історичних передумов виникнення та розвитку комп'ютерних злочинів, а також аналізу вітчизняного та міжнародного досвіду боротьби з кіберзлочинністю. У роботі простежується еволюція засобів комунікації, що сприяла трансформації суспільних відносин та обробки інформації. Починаючи з ранніх етапів існування людства, суспільство поступово перейшло до використання писемності й друкарства. У XX столітті значного розвитку набули технології телеграфу, телефону, радіо, кіно та телебачення.

Особлива увага у статті приділяється останнім десятиліттям, коли стрімкий розвиток комп'ютерних технологій радикально змінив усі сфери життя суспільства. Комп'ютеризація дозволила накопичувати та обробляти великі обсяги даних, що значно полегшило роботу з інформацією, але водночас створило нові ризики та загрози. Масштабна цифровізація стала платформою для виникнення та поширення кіберзлочинів.

У статті розглядаються ключові етапи становлення комп'ютерних злочинів як соціального явища, а також їхні сучасні форми, які включають несанкціонований доступ до даних, фінансові шахрайства, атаки на критичну інфраструктуру та поширення шкідливого програмного забезпечення. Дослідники аналізують вітчизняний досвід України у протидії кіберзлочинності, зокрема розробку правових та технологічних механізмів боротьби, а також досліджують міжнародний досвід, наголошуючи на необхідності міжнародної співпраці. Особливу увагу приділено аналізу правових норм щодо кіберзлочинів у законодавстві США, Німеччини та Франції.

Стаття акцентує увагу на сучасних викликах, пов'язаних із кібербезпекою, та окреслює перспективні напрями для подальших досліджень, включаючи удосконалення законодавчої бази, розвиток технологій захисту інформації, підвищення кіберграмотності та посилення міжнародного співробітництва у боротьбі з кіберзлочинами.

Ключові слова: *комп'ютерні злочини; кіберзлочини; кримінальні правопорушення; комп'ютерні технології; інформаційні технології; комп'ютерні мережі.*

Counteraction to computer crimes is one of the most pressing problems of our time. Their specific features and rapid development pose important tasks for society and the international community regarding the criminal and legal protection of cyberspace.

The article is devoted to the study of the historical prerequisites for the emergence and development of computer crimes, as well as the analysis of domestic and international experience in combating cybercrime. The work traces the evolution of communication tools, which contributed to the transformation of social relations and information processing. Starting from the early stages of the existence of mankind, society gradually switched to the use of writing and printing. In the twentieth century, the technologies of the telegraph, telephone, radio, cinema and television underwent significant development.

The article pays special attention to the last decades, when the rapid development of computer technologies has radically changed all spheres of society. Computerization has allowed the accumulation and processing of large volumes of data, which has greatly facilitated work with information, but at the same time has created new risks and threats. Large-scale digitalization has become a platform for the emergence and spread of cybercrime.

The article examines the key stages of the formation of computer crimes as a social phenomenon, as well as their modern forms, which include unauthorized access to data, financial fraud, attacks on critical infrastructure and the spread of malicious software. The researchers analyze Ukraine's domestic experience in combating cybercrime, in particular the development of legal and technological mechanisms for combating it, and also study international experience, emphasizing the need for international cooperation.

Particular attention is paid to the analysis of legal norms regarding cybercrimes in the legislation of the USA, Germany and France.

The article focuses on modern challenges related to cybersecurity and outlines promising areas for further research, including improving the legislative framework, developing information protection technologies, increasing cyber literacy and strengthening international cooperation in the fight against cybercrimes.

Key words: *computer crimes; cybercrimes; criminal offenses; computer technologies; information technologies; computer networks.*

Актуальність теми дослідження. З моменту виникнення людського суспільства спілкування завжди було невід'ємною потребою людей. Спочатку обмін інформацією відбувався за допомогою жестів, знаків, міміки та нерозділеними звуків. Згодом виникла людська мова, писемність і друкарство. У XX столітті значного розвитку набули такі засоби комунікації, як телеграф, телефон, радіо, кіно та телебачення. Останні десятиліття характеризуються стрімким прогресом комп'ютерних технологій, які стали активно впроваджуватися в усі сфери життя суспільства. Завдяки цьому величезні обсяги даних у вигляді комп'ютерної інформації значно спростили їх обробку та використання.

Інформаційні мережі локального характеру, а також мережа Інтернет дозволяють створити єдиний інформаційний простір, миттєво обмінюватися інформацією та оперативно координувати дії різних служб, органів, підрозділів та організацій. Впровадження комп'ютерних технологій дозволило автоматизувати різні виробничі та управлінські процеси, що сприяло збільшенню продуктивності праці.

У XXI столітті з появою комунікаторів, смартфонів, планшетів, комп'ютер із колись дорогого, громіздкого стаціонарного пристрою перетворився на доступний переважній кількості жителів планети мобільний гаджет, що володіє великим функціоналом. Разом з тим, поява ЕОМ та подальший розвиток комп'ютерних технологій призвело до виникнення абсолютно нового виду злочинності – комп'ютерної.

Аналіз досліджень і публікацій з проблеми. Дослідження історичних аспектів виникнення та розвитку комп'ютерних злочинів в Україні та інших країнах проводили різні вітчизняні науковці, які спеціалізуються на кримінології, правознавстві, кібербезпеці та інформаційних технологіях. Серед найбільш відомих українських науковців, які досліджували цю тему, можна виділити таких авторів: О. Бантишев, О. Волобуєв**,** Г. Дідківська, О**.** Фролова. Науковці публікували роботи, присвячені історії, розвитку та правовим аспектам протидії кіберзлочинам, а також співпраці України з іншими країнами у цій сфері.

Попри значний прогрес у дослідженні проблем комп'ютерних злочинів, залишаються актуальні питання, які потребують подальшого вивчення та розробки. Основні напрями для подальших досліджень у цій сфері включають: еволюція методів скоєння комп'ютерних злочинів, правові прогалини в законодавстві, проблеми міжнародної співпраці. Постійно з'являються нові форми та методи кіберзлочинів, такі як атаки із застосуванням штучного інтелекту, глибоких фейків (deepfakes) та блокчейн-технологій. Потрібно досліджувати, як розвиваються технології злочинців, щоб вчасно розробляти ефективні механізми протидії. Законодавство України та інших країн часто не встигає за технологічними змінами. Важливо розробляти більш гнучкі правові норми, здатні регулювати нові види злочинів, пов'язаних із використанням квантових обчислень, криптовалют та метавсесвітів.

Метою статті є аналіз історичних передумов виникнення та еволюції комп'ютерних злочинів, а також дослідження вітчизняного та міжнародного досвіду протидії кіберзлочинності**.**

Виклад основного матеріалу. Сьогодні кіберзлочинці становлять загрозу не лише для окремих осіб, а й для цілих держав. Хоча новітні технології значно підвищують комфорт і якість життя, водночас вони створюють нові можливості для здійснення протиправної діяльності. З поширенням комп'ютерних мереж та Інтернету кількість кіберзлочинів невпинно зростає. За даними Інтерполу, злочинність у кіберпросторі демонструє найшвидші темпи зростання порівняно з іншими видами кримінальних правопорушень [1].

Розвиток комп'ютерних технологій відкрив нові можливості не лише для суспільного про-

гресу, але й для злочинної діяльності. Тому важливо звернутись до історичного аспекту даної проблематики.

Батьківщиною терміна «комп'ютерна злочинність» вважається США, де у 60-х роках минулого століття подібне словосполучення вперше з'явилося у ЗМІ у зв'язку з виявленням перших злочинів, скоєних з використанням ЕОМ. Перші випадки кіберзлочинів мали місце ще в кінці 1970-х років. Одним із перших інцидентів стало пограбування банку Security Pacific у 1970-х роках, у результаті якого було викрадено понад 10 мільйонів доларів. У 1979 році в СРСР відбулося розкрадання комп'ютерів у Вільнюсі на суму 79 тисяч карбованців [2].

1980-ті роки ознаменувалися появою перших комп'ютерних вірусів. У 1984 році був винайдений перший у світі вірус, хоча збитки від нього не були зафіксовані. У 1985 році за допомогою вірусу вдалося зірвати голосування в Конгресі США, а у 1986-1988 роках вірус вперше з'явився на радянській території. Водночас відбулися гучні кібератаки, такі як блокування тисяч комп'ютерів у Пентагоні у 1989 році, здійснене американським студентом [2].

1990-ті роки стали переломними в історії кіберзлочинності. У 1990 році в Голландії відбувся перший міжнародний з'їзд комп'ютерних піратів. У 1991 році було викрадено понад 125 тисяч доларів із «ЗовнішЕкономБанку», а у 1992 році було зафіксовано порушення роботи реакторів Ігналінської АЕС. Одним із наймасштабніших злочинів цього періоду стало шахрайство у Центробанку росії в 1993 році на суму близько 70 мільярдів рублів [3].

На рубежі століть кіберзлочинці почали активно використовувати комп'ютерні віруси. У 1999 році вірус «Melissa», який поширювався через документи MS Word, завдав збитків на 80 мільйонів доларів, а у 2000 році вірус «ILOVEYOU» спричинив збитки у понад 10 мільярдів доларів.

У XXI столітті масштаби кіберзлочинності значно зросли. Віруси, такі як «Slammer» (2003 рік), «Stuxnet» (2010 рік) та «WannaCry» (2017 рік), спричинили багатомільярдні збитки, вражаючи комп'ютерні мережі по всьому світу. У 2013 році відбулася масштабна атака на Yahoo!, унаслідок якої було викрадено дані мільярдів облікових записів. У 2014 році хакерська атака на Sony Pictures Entertainment призвела до збитків понад 100 мільйонів доларів [4].

Останні роки ознаменувалися новими викликами. У 2021 році атака на Colonial Pipeline у США спричинила економічні втрати та викуп у розмірі 4,4 мільйона доларів. У 2022 році масові кібератаки були спрямовані на українські урядові та банківські системи. У 2023 році фішингові атаки на криптовалютні біржі завдали збитків у понад 1,5 мільярда доларів [5].

Серед останніх гучних подій – атака на об'єкти критичної інфраструктури США у 2024 році із збитками у понад 2 мільярди доларів та злом енергетичних компаній у Південній Америці у 2025 році, унаслідок якого було виплачено викуп у 5 мільйонів доларів [6].

Ці події демонструють не лише зростання масштабів кіберзлочинності, але й необхідність посилення міжнародної співпраці та вдосконалення заходів кібербезпеки.

Щодо України, першим зареєстрованим злочином у сфері комп'ютерних технологій вважається випадок 1993 року, коли було зафіксовано незаконне втручання в банківську систему, що призвело до фінансових збитків. Цей інцидент став відправною точкою для усвідомлення важливості кібербезпеки в країні [7].

На підставі викладеного, можна зробити висновок про те, що комп'ютерна злочинність є дуже серйозною загрозою, як для окремих держав, так і для всього світового співтовариства, у зв'язку з чим необхідно розробляти, реалізувати та вдосконалювати на практиці дієві механізми протидії подібним явищам.

Розробка ефективних механізмів протидії кіберзлочинності неможлива без ретельного аналізу зарубіжного досвіду. З огляду на це доцільно розглянути підходи до законодавчої регламентації кримінальної відповідальності за такі дії на прикладі США, Німеччини та Франції.

Як уже зазначалося раніше, перші комп'ютерні злочини були скоєні на території США, тому не дивно, що саме Америка однією з перших законодавчо встановила кримінальну відповідальність за їх вчинення.

Так в 1977 р. у США було розроблено законопроект про захист федеральних комп'ютерних систем. Він передбачав кримінальну відповідальність за такі дії, як: введення свідомо неправдивих даних у комп'ютерну систему; незаконне використання комп'ютерних пристроїв; внесення змін до процесів обробки інформації або порушення цих процесів; розкрадання коштів, цінних паперів, майна, послуг, цінної інформації, скоєні з використанням можливостей комп'ютерних технологій або з використанням комп'ютерної інформації.

На основі цього законопроекту в жовтні 1984 р. було прийнято «Закон про шахрайство та зловживання з використанням комп'ютерів» основний нормативно-правовий акт, який встановлює кримінальну відповідальність за злочини у сфері комп'ютерної інформації. У подальшому він неодноразово (1986, 1988, 1989, 1990, 1994 і 1996 рр.) змінювався і доповнювався, а в даний час він включений у вигляді § 1030 в Титул 18 Зводу законів США [8].

Закон передбачає суворі покарання залежно від тяжкості правопорушення, починаючи від штрафів до значних термінів позбавлення волі. Наприклад, у разі, якщо кіберзлочин призвів до значних фінансових втрат або зачепив національну безпеку, покарання може бути значно суворішим.

У Німеччині кримінальну відповідальність за комп'ютерні злочини встановлено 1986 року, коли було внесено відповідні зміни до Кримінального кодексу ФРН (Strafgesetzbuch, StGB), спрямовані на адаптацію законодавства до нових викликів у сфері інформаційних технологій. Згідно з Кримінальним кодексом Німеччини, до злочинів у сфері комп'ютерної інформації відносяться наступні дії: Неправомірне отримання даних (§ 202a): особи, які незаконно набувають для себе або інших осіб інформацію, що не є безпосередньо сприйнятною, але може бути відтворена або передана електронним чи магнітним способом. Злочини, пов'язані з майновою вигодою через маніпуляції з даними (§ 263a): намір отримати майнову вигоду шляхом заподіяння шкоди чужому майну через вплив на результат обробки даних за допомогою створення помилкових програм, використання недостовірних даних або неправомірного доступу до даних. Підробка технічних записів (§ 268): підробка або використання підроблених технічних записів, що включають дані, які автоматично фіксуються пристроями. Підробка даних, що мають доказове значення (§ 269): аналогічне підроблення даних, що мають юридичну силу як доказ. Знищення або зміна технічних записів (§ 274): невідомі або навмисні зміни, знищення або приховування технічних записів. Протиправні дії щодо даних (§ 303a): анулювання, знищення, приведення в непридатність або зміна даних без законних підстав. Порушення обробки даних через знищення або пошкодження обладнання (§ 303b): пошкодження, руйнування або приведення в непридатність установок для обробки даних або носіїв інформації [8].

Ці зміни зробили Німеччину однією з перших країн, які на законодавчому рівні адаптувалися до викликів кіберзлочинності. Законодавство продовжує розвиватися з урахуванням появи нових видів загроз і технологій, забезпечуючи високий рівень правового захисту в цифровому середовищі.

Кримінальний кодекс Франції, який вступив в силу навесні 1994 року, також встановлює кримінальну відповідальність за різні комп'ютерні злочини. Зокрема, він передбачає покарання за наступні порушення у сфері комп'ютерної інформації: перехоплення, крадіжка, використання або розголошення повідомлень, що передаються засобами телекомунікацій (ст. 226-15); незаконний доступ до автоматизованої системи обробки даних або незаконне перебування в ній (ст. 323-1); перешкоджання роботі чи порушення функціонування комп'ютерної системи (ст. 323-2); введення у систему обманним шляхом даних або зміна чи знищення інформації в автоматизованій системі (ст. 323-3); введення або зберігання заборонених законом даних в пам'яті комп'ютера (ст. 226-19).

До злочинів, що стосуються інформаційного комп'ютерного простору, згідно з Кримінальним кодексом Франції, також відносяться: здійснення або вказівка на здійснення автоматизованої обробки поіменних даних без дотримання встановлених законом формальностей (ст. 226-16); здійснення або вказівка на обробку даних без забезпечення необхідних заходів безпеки, що гарантують захист даних (ст. 226-17); збирання та обробка даних незаконним спосо-

бом (ст. 226-18); зберігання даних понад встановлений законом термін (ст. 226-20) [8].

Французький Кримінальний кодекс також передбачає суворі покарання за ці злочини, включаючи позбавлення волі та значні штрафи, особливо якщо злочини завдали шкоди національній безпеці, критичній інфраструктурі чи приватним особам. Законодавство Франції постійно оновлюється, щоб враховувати нові кіберзагрози та технологічні виклики, зокрема шляхом імплементації директив ЄС у цій сфері.

Важливим є той факт, що законодавці США, Німеччини і, особливо, Франції виклали чіткіші диспозиції та кваліфікацію комп'ютерних злочинів, що, безсумнівно, сприятливо позначилося на ефективності їх виявлення та розслідування.

В той час Україна суттєво відставала від країн Європи за кількістю засобів обчислювальної техніки, що використовуються як організаціями різних форм власності, і безпосередньо громадянами.

Вперше кримінальну відповідальність за злочини з використанням комп'ютерів було запроваджено в Україні у 2001 році із прийняттям нового Кримінального кодексу України (ККУ). У цьому кодексі було передбачено спеціальні статті, які регулювали кримінальну відповідальність за комп'ютерні злочини, зокрема:

Стаття 361 ККУ: «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». Ця стаття передбачає відповідальність за дії, які порушують роботу комп'ютерних систем.

Стаття 362 ККУ: «Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку».

Стаття 363 ККУ: «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» [9].

Ці положення стали першими спробами законодавчого врегулювання боротьби з кіберзлочинністю в Україні, враховуючи зростаючу роль комп'ютерних технологій у житті суспільства.

Нині законодавство України щодо кіберзлочинності адаптоване до міжнародних стандартів, зокрема з урахуванням положень Будапештської конвенції про кіберзлочинність, учасником якої Україна є з 2006 року. Кримінальний кодекс України продовжує оновлюватися, враховуючи нові виклики у сфері кібербезпеки, щоб ефективно протидіяти загрозам у цифровому середовищі. На нашу думку, обмежене трактування протиправних діянь, викладених у розділу XVI КК, найчастіше не сприяє їхній вичерпній та правильній кваліфікації

З розвитком суспільно-економічних відносин обсяги оброблюваної інформації постійно зростають. Якщо XX століття багато вчених вважали епохою енергетики, то XXI століття можна назвати епохою інформатики. Інформація стала значним ресурсом, і з розвитком інформаційних технологій вона перетворилася на один з найбільш цінних товарів. Це підтверджується і появою віртуальних платіжних засобів, таких як криптовалюти, кількість яких, за даними різних Інтернет-джерел, сягає від 1,5 до 1,8 тисяч найменувань, кожен з яких має своє котирування відносно традиційних валют. Проте нові технології також сприяють виникненню нових форм злочинності. Останнім часом спостерігається значне зростання комп'ютерних злочинів, особливо у контексті глобальної мережі Інтернет. З'явилася тенденція до атак на мобільні пристрої, оскільки вони набули величезної популярності серед користувачів по всьому світу, а багато з них не звертають увагу на базові заходи безпеки. У великих організаціях зазвичай існують багаторівневі системи захисту, що включають як апаратні засоби, так і спеціалізовані програмні рішення.

На підставі викладеного, можна зробити висновок про те, що комп'ютерна злочинність є однією з найспецифічніших, складно влаштованих і видів злочинності, що динамічно розвиваються. Вона є серйозною загрозою як для окремих держав, так і для всього світового співтовариства. Збитки від дій кіберзлочинців величезні і обчислюються мільярдами доларів. Для ефективної боротьби з цим явищем необхідне вдосконалення законодавства,

що регламентує кримінальну відповідальність за скоєння комп'ютерних злочинів, у тому числі з використанням позитивного досвіду розвинених країн. У вітчизняному законодавстві термін «комп'ютерні злочини» зазвичай охоплюється поняттям «злочини у сфері використання електронно-обчислювальних машин, систем і мереж». Основні положення викладені в Кримінальному кодексі України, зокрема у статтях 361–363. Комп'ютерні злочини є динамічним явищем, що розвивається разом із технологіями, що робить їх вивчення та регулювання важливим завданням сучасного суспільства.

ЛІТЕРАТУРА:

1. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. Вчені записки ТНУ ім. В. І. Вернадського. 2018. Том 29 (68). № 6. С. 121–123.

2. Encyclopedia Britannica. Phreaking. URL: https://www.britannica.com/ topic/phreaking. (дата звернення: 15.12.2024).

3. Концептуальні засади кримінально-правової охорони кіберпростору в Україні: монографія / М. О. Думчиков. Суми : Сумський державний університет, 2023. 413 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/92746/3/Dumchykov_kiberprostir.pdf (дата звернення: 15.12.2024).

4. CYBER DIGEST Огляд подій в сфері кібербезпеки, квітень 2024. URL: https://ufss.com.ua/wpcontent/uploads/2024/05/Cyberdigest_Apr_2024_UA.pdf (дата звернення: 15.12.2024).

5. Рекордні викупи та зломи: хронологія програм-вимагачів у 2024 році. URL: https://www.oksim.ua/2024/12/27/rekordni-vikupi-ta-zlomi-hronologiya-program-vimagachiv-u-2024-roczi/ (дата звернення: 18.12.2024).

6. Енергетична безпека світу: ТОП-25 прогнозів на 2025 рік. URL: https://armyinform.com.ua/2025/01/01/energetychna-bezpeka-svitu-top-25-prognoziv-na-2025-rik/ (дата звернення: 15.12.2024).

7. Довженко О. Ю. Основи методики розслідування кіберзлочинів : автореф. дис. … к-та юр. наук : 12.00.09. Харківський національний університет внутрішніх справ. Харків, 2020. 18 с

8. Міжнародна політика інформаційної (кібер) безпеки. 87 питань і відповідей [Текст]: навч. посіб. / Сергій Валентинович Федонюк. Луцьк : ВежаДрук, 2023.

9. Кримінальний кодекс України (ККУ). Верховна Рада України, 2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 19.12.2024).