УДК 004.056.5
DOI https://doi.org/10.20535/2308-5053.2021.1(49).233023

КІБЕРЗЛОЧИН, КОМП'ЮТЕРНИЙ ЗЛОЧИН ЧИ КІБЕРПРАВОПОРУШЕННЯ? АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ ТЕРМІНОЛОГІЇ

Бараненко Р. В.,
кандидат технічних наук, доцент,
доцент кафедри професійних та спеціальних дисциплін
Херсонського факультету
Одеського державного університету внутрішніх справ
ORCID ID: 0000-0002-5231-6248

Нині кіберзлочинність та комп'ютерний тероризм визначені як одні із загроз національній безпеці України в інформаційній сфері.

Заходи з кібербезпеки включають досягнення та підтримку функцій безпеки в ресурсах установи чи користувачів, спрямованих на запобігання відповідних кіберзагроз.

Кіберзлочинність як сукупність кримінальних правопорушень, вчинених у віртуальному просторі комп'ютерними системами або за допомогою комп'ютерних мереж та інших засобів доступу до кіберпростору, в межах комп'ютерних систем або мереж, а також проти комп'ютерних систем, комп'ютерних мереж та комп'ютерних даних, має сьогодні широке розповсюдження.

У статті розглядаються такі терміни, як «комп'ютерна злочинність», «інформаційна злочинність», «злочинність у сфері комп'ютерної інформації», «злочини в галузі інформаційних технологій».

Проаналізовано наукові праці вітчизняних та зарубіжних дослідників із питань протидії кіберзлочинності. Наведено зв'язок поняття «кібербезпека» з термінами «кіберзлочини», «комп'ютерна злочинність» та «кіберправопорушення»; визначено поняття «кіберправопорушення». У роботі розглянуті їхні основні особливості. Розглянуто різницю у трактуванні понять «кібербезпека» та «інформаційна безпека».

Розглянуто поняття «комп'ютерна віктимність» та його складники.

Із введенням інституту кримінальних проступків до національного кримінального законодавства терміни «кіберзлочинність» та «комп'ютерна злочинність» повинні втратити свою актуальність, про що свідчить зміна назви Розділу XVI Кримінального кодексу України на «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Тому натомість рекомендуємо вживати термін «кіберправопорушення», який пропонуємо розуміти як «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано кримінальним правопорушенням міжнародними договорами України, а кіберзлочинність – сукупність кіберправопорушень». Зрозуміло, що це потребуватиме і внесення відповідних термінологічних змін до Закону України «Про основні засади забезпечення кібербезпеки України» та інших нормативно-правових актів.

Ключові слова: кібербезпека, кіберзлочин, кіберзлочинність, кіберправопорушення, комп'ютерний злочин.

Вступ і постановка завдання. Інформаційні технології заповнили всі сфери діяльності сучасного інформаційного суспільства, що привело до колосальних можливостей для злочинців щодо зловживання цією вразливістю.

З огляду на те, що з кожним днем зростає кількість користувачів мережі Інтернет у світі, поширюється використання персональних комп'ютерів, інформаційно-обчислюваних мереж та інших ґаджетів, проявляються також і негативні наслідки всесвітньої комп'ютеризації, серед яких слід відзначити новий різновид злочинності – кіберзлочинність, яка пов'язана з використанням комп'ютерів, інформаційних технологій та глобальних мереж [1].

Не випадково саме кіберзлочинність і комп'ютерний тероризм визначено однією із загроз національній безпеці в інформаційній сфері згідно зі ст. 7 Закону України «Про основи національної безпеки України», а в Конституції України забезпечення інформаційної безпеки названо справою усього українського народу [2, с. 10].

У зв'язку з цим постає питання визначення відповідної термінології та меж її застосування в національному законодавстві та науковому дискурсі.

Аналіз попередніх досліджень. Дослідженням проблем кіберзлочинності займалися такі вчені, як Д. Азаров, В. Бутузов, В. Голубєв, О. Користін, Т. Тропіна та інші. Окремі питання кримінально-правової охорони інформаційних суспільних відносин розглядали у своїх роботах П. Біленчук, В. Вєхов, В. Гавловський, В. Горбулін, М. Карчевський, Н. Савінова та інші.

Проте низка важливих питань у сфері протидії кіберзлочинності залишилися без достатньої уваги дослідників.

Метою роботи є аналіз термінів «кіберзлочин», «комп'ютерний злочин», «злочин у сфері комп'ютерної інформації», «злочини у сфері використання інформаційних технологій», «кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» відповідно до положень чинного національного законодавства та наукових праць вітчизняних і зарубіжних дослідників у галузі права та інформаційної безпеки.

Основний матеріал. О.А. Баранов трактує поняття «кібербезпека» як деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об'єктів, на які можуть впливати будь-які загрози з кіберпростору, це визначення терміну дає змогу врахувати наявність якихось загроз функціональності систем більш високого порядку, до яких як складові елементи входять інформаційні системи. Це положення має важливий методологічний зміст у розумінні місця і ролі проблеми кібербезпеки в контексті інших видів безпеки [3, с. 55].

На відміну від нього В.М. Фурашев визначає кібербезпеку як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, насамперед – несвідомого, негативного впливу (управління) інформації [4, с. 162–169]. Подібно до нього кібербезпеку трактує і В.М. Бутузов: як стан захищеності життєво важливих прав та інтересів людини, суспільства, держави в кіберпросторі від внутрішніх і зовнішніх протиправних посягань та загроз таких посягань [5, с. 176].

Український вчений В.Л. Бурячок визначає кібербезпеку більш широко як стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним або національним інтересам та запобігання їм [6, с. 3–4].

У цьому контексті позиціонує кібербезпеку і професор А.В. Мовчан: як важливу складову частину національної безпеки, що дає змогу протистояти протиправним діям у кіберпросторі, уникнути або зменшити негативні наслідки від реалізації кіберзагроз [7, с. 162].

На нашу думку, кібербезпека – це безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам. Залежно від виду загроз кібербезпеку можна розглядати як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб; інформаційних прав і свобод людини й громадянина [8, с. 108–110].

В інформаційному праві розглядається категорія «інформаційна безпека» – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства, з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [9, с. 47–49].

Насамперед загрози інтересам держави також можуть проявлятися у вигляді отримання протиправного доступу до відомостей, що становлять державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки державі [8, с. 108–110]. Ці дії містять ознаки кримінальних правопорушень, що регулюються Кримінальним Кодексом України.

Кіберзлочинність – це злочинність у так званому віртуальному просторі – кіберпросторі, який можна визначити як модельований за допомогою комп'ютера інформаційний простір, у якому знаходяться відомості про осіб, предмети, факти, події, які представлені в математичному, символьному або будь-якому іншому вигляді, що знаходяться у процесі руху локальними і глобальними комп'ютерними системами, або відомості, які зберігаються у пам'яті будь-якого фізичного чи віртуального пристрою, а також іншого носія, який спеціально пристосований для їх зберігання, обробки та передачі [10].

Дослідники розглядають поняття кіберзлочину у двох значеннях: 1) у вузькому сенсі (комп'ютерний злочин) – будь-яке протиправне діяння, вчинене за допомогою електронних операцій, об'єктом посягання якого є безпека комп'ютерних систем і оброблюваних ними даних; 2) у широкому розумінні (як злочин, пов'язаний з комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння і пропозицію або розповсюдження інформації за допомогою комп'ютерних систем або мереж [11; 12, с.49; 13, с.146].

Проте кіберзлочинність включає в себе не тільки діяння, вчинені в глобальній мережі Інтернет. Вона поширюється на всі види кримінальних правопорушень, вчинені в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати (бути) предметом (метою) злочинних посягань, середовищем, у якому відбуваються правопорушення, і засобом або знаряддям кримінального правопорушення [14].

К.В. Тарасюк під «кіберзлочинами» розуміє суспільно-небезпечні діяння, які так чи інакше пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами. Такі діяння характеризуються такими особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказування в суді подібних справ, транснаціональною складовою частиною в основному з використанням інформаційної мережі Інтернет, високим збитком навіть від одиничного кримінального правопорушення [15, с. 178].

Н.В. Савчук дає таке визначення поняття «кіберзлочинності» (англ. Cybercrime): це поняття, яке охоплює комп'ютерну злочинність (де комп'ютер – предмет кримінального правопорушення, а інформаційна безпека – об'єкт кримінального правопорушення) та інші посягання, де комп'ютер є знаряддям або способом кримінального правопорушення проти власності, авторських прав, громадської безпеки, моралі тощо [16, с. 338–342].

О.Є. Користін та інші визначають кіберзлочинність як сукупність кримінальних правопорушень, що здійснюються в кіберпросторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до кіберпростору, в межах комп'ютерних систем або мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [17, с. 46].

До комп'ютерної ж злочинності, на погляд одних учених, відносяться всі протизаконні дії, за яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом [18, с.14], або всі протизаконні діяння, предметом і засобом здійснення яких є процедури і методи, а також процес комп'ютерного опрацювання даних [19, с. 72].

Російський правознавець В.А. Бессонов як ознаку комп'ютерної злочинності наводить «комп'ютерну віктимність» [20], під якою розуміє здатність персонального комп'ютера з інформацією, що в ньому зберігається, бути самим по собі віктимним, в силу своїх технічних, споживчих властивостей.

В. Лісовий визначає цю ознаку інакше: «електронна обробка інформації» – незалежно від того, на якій стадії кримінального правопорушення вона застосовувалася [21, с. 87].

«Комп'ютерні злочини» – це передбачені законом суспільно-небезпечні дії, вчинені з використанням засобів електронно-обчислювальної техніки. Більшість науковців розуміють терміни «кіберзлочинність» та «комп'ютерні злочини» як синоніми. Проте на їх відмінності наголошують В.А. Намоконов та Т.Л. Тропіна, стверджуючи, що перше є ширшим та більш точно відображає сутність такого явища, як злочинність в інформаційному просторі. До того ж Рада Європи у листопаді 2001 року, приймаючи Конвенцію про кіберзлочинність, застосувала саме термін «cybercrime», а не «computer crime» [2, с. 34]. Проте у вітчизняній юридичній літературі перевага віддається поняттю «комп'ютерна злочинність».

В. Бутузов вважає, що «комп'ютерні злочини» та «кіберзлочини» є різними видами кримінальних правопорушень у сфері високих інформаційних технологій, класифікація яких відбувається за такими ознаками:

– ознакою віднесення певних кримінальних правопорушень до «комп'ютерних злочинів» є знаряддя вчинення кримінального правопорушення – комп'ютерна техніка. Автор зазначає, що об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації;

– ознакою віднесення кримінальних правопорушень до «кіберзлочинів» є специфічне середовище вчинення цих правопорушень – кіберпростір (середовище комп'ютерних систем та мереж) [5, с. 119].

А. Музика та Д. Азаров визначають тотожність понять «кіберзлочини» та «злочини у сфері комп'ютерної інформації» та наголошують, що «кіберзлочини» треба визначати як «злочини у сфері комп'ютерної інформації» [22, с. 5], проте з цим не можна погодитися, оскільки предметом деяких кримінальних правопорушень, передбачених Розділом XVI КК України, є не тільки комп'ютерна інформація, а й об'єкти авторського права, комп'ютерні програми, носії інформації, платіжні картки тощо.

М.В. Карчевський взагалі пропонував використовувати в національному законодавстві поняття «злочини у сфері використання інформаційних технологій», розуміючи під ним «один із видів злочинів у сфері інформаційної безпеки, які передбачені КК України, є суспільно небезпечними, винними, вчиненими суб'єктом злочину діяннями, які заподіюють шкоду забезпеченим засобами обчислювальної техніки відносинам у сфері реалізації інформаційної потреби». Аналіз чинного КК дає змогу дійти висновку, що до таких злочинів слід відносити посягання, передбачені ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1 КК [23, с. 11]. М.М. Дмитрук не погоджується з М.В. Карчевським, наводячи як приклад порушення авторських та суміжних прав, яке здійснюється шляхом втручання в роботу ЕОМ, заподіює шкоду «відносинам у сфері реалізації інформаційної потреби» і вчиняється за допомогою саме «засобів обчислювальної техніки». Проте М.В. Карчевський у своїй роботі цей склад кримінального правопорушення не розглядає в цьому контексті. Інші доводи з боку вказаного вченого наведено на користь позначення кримінальних правопорушень, передбачених у Розділі XVI Особливої частини КК України, як «злочинів у сфері використання ІТ» [24, с. 16].

Цікава позиція, в якій поняття «комп'ютерний злочин» замінюється на «інформаційний злочин», причому ЕОМ – один із видів засобів для вчинення кримінального правопорушення, а об'єктом є не сам комп'ютер, а дані, які обробляються за допомогою комп'ютера [25, с. 80–81].

Низка російських експертів вважають синонімами «комп'ютерний злочин» і «злочин у сфері комп'ютерної інформації».

Крапку в питанні визначення відповідних термінів і понять мав би поставити Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий у 2017 році, де чітко визначено, що кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України, а кіберзлочинність – сукупність кіберзлочинів [26].

Тобто з погляду цього Закону поняття «кіберзлочин» і «комп'ютерний злочин» є тотожними! Але…

Із запровадженням інституту кримінальних проступків до національного кримінального законодавства терміни «кіберзлочин» і «комп'ютерний злочин» мають втратити свою актуальність, про що свідчить навіть зміна назви Розділу XVI Кримінального кодексу України на «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Тому замість них можна рекомендувати до використання термін «кіберправопорушення», під яким пропонуємо розуміти «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано кримінальним правопорушенням міжнародними договорами України, а кіберзлочинність – сукупність кіберправопорушень». Зрозуміло, що це потребуватиме і внесення відповідних термінологічних змін і до Закону України «Про основні засади забезпечення кібербезпеки України» та інших нормативно-правових актів.

Висновки. Враховуючи необхідність гармонізації українського та європейського законодавства, а також наявну потребу імплементації передового зарубіжного досвіду протидії кіберзлочинності до вітчизняних реалій, необхідно провести велику роботу із впорядкування застосованої термінології у законодавстві України.

Оскільки нині поняття «кіберзлочин» та «комп'ютерний злочин» втратили свою актуальність, то пропонуємо в українському законодавстві використовувати термін «кіберправопорушення». А це означає, що насамперед потребує суттєвого доопрацювання низка Законів України та нормативно-правових актів, що регулюють сферу кіберпростору, інформаційної безпеки та кібербезпеки.

Baranenko R. Cyber crime, computer crime or cyber offense? The analysis of the features of a terminology application

Today cybercrime and computer terrorism are identified as one of the threats to Ukraine's national security in the information sphere.

Cybersecurity measures include achieving and maintaining security features in the resources of an institution or users, aimed at preventing relevant cyber threats.

Cybercrime is a set of criminal offenses committed in cyberspace by computer systems or by using computer networks and other means of access to cyberspace, within computer systems or networks, as well as against computer systems, computer networks and computer data, has been widely developed.

The paper considers such terms as «computer crime», «information crime», «crime in the field of computer information», «crimes in the field of information technology».

Scientific works of domestic and foreign researchers on the issues of countering cybercrime are analyzed. The connection of the concept of «cybersecurity» with the terms «cybercrime», «computer crime» and «cybercrime» the concepts of «cybercrime» was given. The difference in the interpretation of the concepts «cybersecurity» and «information security» was considered. The definitions of «cybercrime», «computer crime» and «cyber offense» were given for comparison. Their main features were considered.

The concept of «computer victimhood» and its components were considered.

With the introduction of the institute of criminal offenses in the national criminal law, the terms «cybercrime» and «computer crime» should lose their relevance, as evidenced by the change of title of Chapter XVI of the Criminal Code of Ukraine to «Criminal offenses in the use of electronic computing machines (computers), systems and computer networks and telecommunications networks». Therefore, instead, we can recommend the use of the term «cyber offense», which we propose to understand as «socially dangerous criminal act in cyberspace and/or using it, liability for which is provided by the law of Ukraine on criminal liability and/or which is recognized as a criminal offense by international treaties of Ukraine, and cybercrime is a set of cyber offences». It is clear that this will require the introduction of appropriate terminological changes in the Law of Ukraine «On the Basic Principles of Cyber Security of Ukraine» and other regulations.

Key words: cyber security, cybercrime, cyber offense, computer crime.

Література:

1. Кириченко В.Д., Бараненко Р.В. Характеристика кіберзлочинності. *Реформування правової системи України під впливом євроінтеграційних процесів* : матеріали ІІІ Всеукраїнської науково-практичної конференції. Херсон : Видавничий дім «Гельветика», 2018. С. 189–191.
2. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнародної науково практичної конференції / за ред. О.В. Манжай. Харків, 2014. / МВС України, Харків.нац.ун-т внутр. справ. Харків : Права людини, 2014. 200 с.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 54–62.
4. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.
5. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КІТ, 2010. 408 с.
6. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ : НАУ, 2013. 432 с.
7. Мовчан А.В. Кібернетична безпека України в умовах глобальної нестабільності. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2015. № 1 (34). С.159–163.
8. Гітрук О.О., Бараненко Р.В. Кібербезпека як один з факторів забезпечення національної безпеки держави. *Кібербезпека в Україні: правові та організаційні питання* : матеріали науково-практичної конференції. Одеса: ОДУВС, 2016. С. 108–110.
9. Литвиненко О. Інформація і безпека. *Нова політика*. 1998. № 1. С. 47–49.
10. Голубєв В.А. «Кибертерроризм» – миф или реальность? *Центр дослідження комп'ютерної злочинності* : веб-сайт. URL: http://www.crime-research.org
11. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Владивосток, 2005. URL: http://www.dissercat.com/content/kiberprestupnost-ponyatie-sostoyanie-ugolovno-pravovye-mery-borby#ixzz43N98D41A
12. Скулиш Є.Д. Теоретико-методологічні засади визначення об'єкта та предмета кіберзлочинів. *Правова інформатика*. 2014. № 2. С. 47–53.
13. Грицун О.О. Кримінальний аспект міжнародної інформаційної безпеки. *Право і суспільство*. 2015. № 6. Ч. 2. С.142–147.
14. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. Москва : Горячая линия-Телеком, 2002.
15. Тарасюк К.В. Прокурорський нагляд при розслідуванні комп'ютерних злочинів. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2012. № 10. С. 178–181.
16. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки*: зб. наук. праць. Київ : Видавничо-поліграфічний центр «Київський університет», 2009. Вип. 19. С. 338–342.
17. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч.посіб. / О.Є. Користін, В.М. Бутузов, В.В. Василевич та ін. Київ : Скіф, 2012.

18. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. …д-ра юрид. наук : спец. 12.00.02 «Государственное право и управление; административное право; финансовое право» / Калюжный Ростислав Андреевич. Київ, 1992. 47 с.
19. Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації. *Право України*. 2000. № 12. С. 69–73.
20. Бессонов Владимир Анатольевич. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации : диссертация ... кандидата юридических наук : 12.00.08. – Нижний Новгород, 2000. 249 с.
21. Лісовий В. Комп'ютерні» злочини: питання кваліфікації. *Право України*. 2002. № 2. С. 86–88.
22. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.08 / НАНУ. Інститут держави і права ім. В.М. Корецького. Київ, 2002. 228 с.
23. Карчевский Н.В. Киберпреступление или преступление в сфере использования информационных технологий? *Кібербезпека в Україні: правові та організаційні питання* : матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса : ОДУВС, 2016. С. 10–15.
24. Дмитрук М.М. Питання термінології у визначенні системи злочинів в сфері ІТ (досвід інших держав). *Кібербезпека в Україні: правові та організаційні питання* : матеріали всеукр. наук.-практ. конф., м. Одеса, 17 листопада 2017 р. Одеса : ОДУВС, 2017. С. 16–18.
25. Черкасов В.Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. Саратов, 1995. С. 80–81.
26. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19.