МАЗУРЕНКО СВІТЛАНА ВІКТОРІВНА

Національний університет «Одеська юридична академія»,
доцент кафедри права інтелектуальної власності та корпоративного права,
кандидат юридичних наук, доцент

ПРАВОВІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

У Великому тлумачному словнику української мови терміни «кібер» або «кібернетичний» трактуються як такий, що походить від терміну «кібернетика», який створено та працює на основі принципів та методів кібернетики. А термін «безпека» описує стан, коли кому та/або чому-небудь ніщо не загрожує, тобто характеризує відсутність небезпеки [1]. Підґрунтям запровадження терміну «кібербезпека» стало розуміння необхідності вирішення проблеми нейтралізації або мінімізації сукупності кіберзагрози. З технологічної точки зору кібербезпека є складовою частиною інформаційної безпеки, оскільки сутність загроз, методів, засобів і заходів є однаковою та кібербезпека стосується лише кіберпростору. З іншої точки зору термін «Кібербезпека» розглядається як окремий випадок інформаційної безпеки, введення якого обумовлене використанням комп'ютерних систем і мереж (КСМ) та/або телекомунікаційних мереж (ТКМ). «Кібербезпека» як безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує, передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам. Аналіз основних факторів, що негативно впливають на функціонування комп'ютерних систем і мереж та/або телекомунікаційних мереж показав, що існує низка чинників, які спричиняють ризики кіберзагрози їх функціонуванню та потребу їх захищеності від кібератак [2].

О.А. Баранов пропонує під кібербезпекою розуміти окремий випадок інформаційної безпеки, поява якого обумовлена використанням комп'ютерних систем та/або телекомунікаційних мереж. В розгорнутому стані автор пропонує під цим терміном розуміти «такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації» [3].

Важливість проблем кібербезпеки спричинила прийняття в Україні Закону «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження

державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Згідно з ст. 1 цього закону кібербезпека розуміється як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [4].

В законі також дається визначення таким термінам, як: «кіберзагроза» – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів; «кіберзахист» – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем; «кіберзлочин» (комп'ютерний злочин) – 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.

У п. 14 доповіді комітету II десятого конгресу ООН 2000 р. з попередження злочинності і поводження з правопорушниками зазначено, що існує дві категорії інформаційних злочинів: кіберзлочини у вузькому розумінні («комп'ютерні» злочини) – будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних; кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) – будь-яке протиправне діяння, що вчинюється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [5].

На думку Н.М. Дімітрова, на відміну від традиційних видів злочинів, історія яких налічує століття, таких як вбивство або крадіжка, кіберзлочинність явище відносне молоде і нове, яке виникло з появою мережі Інтернет. Специфіка даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється, практично не відходячи від «робочого місця», злочини є доступними, оскільки комп'ютерна техніка постійно дешевшає, злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу [6].

До основних видів кіберзлочинів Н.М. Дімітров відносить: порушення авторського права і суміжних прав; шахрайство; ухилення від сплати податків, зборів (обов'язкових платежів); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ввезення, виготовлення, збут і розповсюдження порнографічних предметів; незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

В цілому можна визначити такі основні ознаки, які відрізняють кіберзлочини від інших кримінальних правопорушень: вчинення таких злочинів не вимагає фізичного зближення суб'єкта злочину та жертви; завдяки автоматизованості, кількість об'єктів злочину може вимірюватись тисячами, як наслідок одного злочинного діяння; такі злочини вчиняються «моментально», тому потрібне швидке реагування відповідних органів; відсутність сталого алгоритму вчинення дій, які призводять до протиправних наслідків, через недостатню дослідженість.

На сьогодні не до кінця з'ясованою слід вважати термінологічне співвідношення кіберзлочинів зі злочинами в мережі Інтернет. Сфера вчинення Інтернет-злочинів – так званий віртуальний простір, який можна визначити як модельований за допомогою комп'ютера інформаційний простір, де містяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді і що перебувають у процесі руху по локальних і глобальних комп'ютерних мережах, або ж відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі.

Специфіка злочинності в мережі Інтернет полягає у такому: відносній комфортності, тобто готування та скоєння злочину здійснюється практично не відходячи від «робочого місця»; доступності – у зв'язку з тенденцією постійного зниження цін на комп'ютерну техніку; широкій географії скоєння злочинів, але враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає «левова частка» злочинності; віддаленості об'єкта злочинних посягань – він може перебувати за тисячі кілометрів від місця скоєння злочину; складності виявлення, фіксації і вилучення криміналістично-значущої інформації (слідової картини злочину) при виконанні слідчих дій для використання її в якості речового доказу і т. ін.; широкому використанні злочинцями засобів шифрування інформації [7].

Головною умовою припинення правопорушень, що вчинюються із використанням мережі Інтернет, є встановлення особи злочинця. Після налагодження контакту зі злочинцем та отримання протиправної пропозиції, за допомогою технічних можливостей мережі здійснюється встановлення його місце перебування та комп'ютера, яким він користувався.

Отже, встановлення особи зловмисника, після отримання інформації про здійснення протиправної діяльності у мережі Інтернет, напряму пов'язане із встановленням: IP-адреси, під якою комп'ютер працював в мережі Інтернет; провайдера Інтернет-послуг, до мережі якого належить IP-адреса, з використанням якої здійснювалася протиправне реалізація порнографічної продукції; встановлення місця знаходження персонального комп'ютера, який мав доступ до Інтернет у вказаний час під встановленою IP-адресою.

Так, інформація щодо розповсюдження або збуту порнографічних предметів, що міститься на відповідному веб-сайті, фізично розміщена на комп'ютерному обладнанні, яке, працюючи в мережі Інтернет, використовує універсальну IP-адресу – ідентифікатор. Крім цього, вебсайт, на якому розміщено подібну інформацію, окрім IP-адреси має вебадресу – алфавітно-цифрове позначення, яка називається доменним ім'ям і також є унікальним в мережі Інтернет.

Таким чином, в останні роки для України особливо актуальною стала проблема кібербезпеки. Поширення кіберзагроз спричинило активізацію законодавця в цій сфері, що вилилось у прийнятті низки нормативно-правових актів, уточнюючих терміни, формуючих системи органів, які відповідають за таку безпеку, посилюють відповідальність за кіберзлочини. Сьогодні під кіберзлочинами слід 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 злочином міжнародними договорами України, а під кібербезпекою – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Список використаної літератури:

1. Бусел В.Т. Великий тлумачний словник сучасної української мови. – К.: ВТФ «Перун», 2003. С. 106, 306.
2. Бистрова Б. Основні поняття дослідження та концептуальні засади професійної підготовки фахівців із кібербезпеки // Педагогічні науки: теорія, історія, інноваційні технології. – 2017. – № 8. – С. 60.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. – 2014. – № 2. – С. 61.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163 -VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.
5. Європіна І.В. види протиправних діянь у сфері новітніх інформаційних технологій // Вісник академії адвокатури України. – 2010. – № 3. – С. 129.
6. Дімітрова Н. М., Н. М. Білик Основні види кіберзлочинів та причини, що їх породжують // Соціально-гуманітарний вісник. – 2018. – Вип. 22. – С. 50.

7. Кіпа О.О. Правопорушення в мережі Інтернет // Часопис Київського університету права. – 2010. – № 4. – С. 347.

Ключові слова: кібербезпека, кіберзлочинність, кіберзагроза, кіберзахист, Інтернет, веб-сайт.
Ключевые слова: кибербезопасность, киберпреступность, киберугроза, киберзащита, Интернет, веб-сайт.
Key words: cybersecurity, cybercrime, cyberthreat, cyber protection, Internet, website.

МАЗІНА ОЛЕНА ОЛЕКСАНДРІВНА

Миколаївський інститут права
Національного університету «Одеська юридична академія»,
доцент кафедри загальнотеоретичної, конституційної
та цивілістичної юриспруденції, кандидат юридичних наук

ПРИВІЛЕЇ В АВТОРСЬКОМУ ПРАВІ ЯК СПОСІБ ЗАХИСТУ ВІД КОНТРАФАКЦІЇ: ІСТОРИКО-ПРАВОВИЙ АСПЕКТ

В історичному аспекті розвитку та становлення авторського права привілеї відігравали значну роль для захисту авторських прав від контрафакції. Протягом тривалого періоду часу до формування законодавства про авторське право наявність привілеїв мала неабияке значення для книговидавців та авторів.

Необхідність охорони видавництв від контрафакції мала наслідком появу привілеїв, які дарувалися тій чи іншій особі на видавництво творів. Привілеї забезпечували за відповідною особою виключне видання та продаж відомої книжки на протязі кілька років, або ж охороняли від контрафакції взагалі всі видання, які здійснювалися даною особою. Поза привілеями не існувало ніякого захисту від контрафакції [1, с. 10-11].

Привілеї видавалися конкретним видавцям на видання певної книги, про що робилася відмітка на примірнику книги.

Загальним привілеєм мав можливість скористуватися кожний, за його відповідності певним умовам. Загальний привілей був ядром усіх останніх законодавчих постанов про авторське право та ним обґрунтовувався погляд на авторське право як на пільгу, як на виняток із законів, який зобов'язаний своїм існуванням мілосердю законодавця. Перший привілей було надано у Венеції 3 січня 1491 року Петру Ровенському на твір Phoenix [2, с. 189]. Надалі доволі часто видавалися привілеї авторам на окремі твори й вони стали нормою існування у авторському праві того часу та формою охорони авторських прав від контрафакції.

На початку XVI століття привілеї з'явилися у Германії та у Франції. Автори самостійних творів або такі, які обробляли рукописи, отримували від видавців єдиноразову винагороду, звичайно помірну, та передавали усі свої права на твір видавцю. Таким чином, хоча з введенням