

взаємодію приватного та публічного інтересу, що встановлює свій відбиток на протидії різним проявам кіберзлочинності у цій площині з огляду на національне та міжнародне законодавство.

### **Література:**

1. Інформаційні злочини [Електронний ресурс] / Вікіпедія. – Режим доступу: [https://uk.wikipedia.org/wiki/Інформаційні\\_злочини](https://uk.wikipedia.org/wiki/Інформаційні_злочини).
2. Політанський В.С. Обмеження права на доступ до інформації / В.С. Політанський // Державне будівництво та місцеве самоврядування. – 2013. - № 26. – С. 215-227.
3. Рішення Конституційного суду України “У справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” від 30 жовтня 1997 року № 5-зп. [Електронний ресурс] / Офіційний веб-сайт Верховної Ради України. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/v005p710-97/print>.
4. Рішення Конституційного суду України “У справі за поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України” від 20 січня 2012 року № 2-рп/2012. [Електронний ресурс] / Офіційний веб-сайт Верховної Ради України. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/v002p710-12>.
5. Серьогін В.О. Конституційний принцип гласності у діяльності органів державної влади України : автореф. дис. ... канд. юрид. наук : спец. 12.00.02 «Конституційне право» / В.О. Серьогін. – Х., 1999. – 18 с
6. Лист Представника Уповноваженого Верховної Ради України з прав людини від 28 грудня 2015 року № 9-3131/4137-15-73 [Електронний ресурс] / Уповноважений Верховної Ради України. – Режим доступу: <http://www.ombudsman.gov.ua/ua/publication/petition/schodo-pravovix-pidstav-peredachi-personalnix-danix-pravoohoronnim-organam/>.

### **Теоретико-правові аспекти кіберзлочинності в Україні**

**Миронець О.М.**

старший викладач кафедри конституційного і адміністративного права,  
Навчально-науковий Юридичний інститут, Національний авіаційний університет

**Колмиков В.В.**

студент Навчально-науковий Юридичний інститут  
Національний авіаційний університет

У наші дні правопорушення в мережі Інтернет є досить поширеним явищем. Кіберзлочинність у віртуальному просторі становить серйозну загрозу кібербезпеці України, що зумовлює актуальність дослідження її теоретико-правових аспектів.

Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера, інформаційний простір, у якому перебувають відомості про особи, предмети, факти, події, явища і процеси, представлені в математичному, символічному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [1, с.32-34].

Саме віртуальний простір є сприятливим середовищем для злочинних діянь, які називаються комп'ютерними злочинами або кіберзлочинами.

Кіберзлочинність – це проблема, з якою зіштовхнулася планета у 21 столітті, і яка обіцяє рости та поглинати все більше коштів. Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників та зменшуючи вміст кишень пересічних громадян. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців [2].

У наші дні проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кібершахраїв сягнули десятків мільярдів доларів. Для протистояння кібершахраям в світі створюються спеціальні підрозділи і структури. Їхні повноваження постійно розширюються, а технічні можливості посилюються. Останній приклад – Європейський центр боротьби з кіберзлочинністю, який запрацював на початку 2013 року [3].

Специфіка цього виду злочинності полягає у тому, що готування та скоєння таких злочинів 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. Усе це, безумовно, є перевагами для кіберзлочинців [2].

Поняття комп'ютерної злочинності є особливим видом злочинів, які посягають на встановлений в суспільстві порядок інформаційних відносин та скоюються з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Об'єктом злочину виступають інформаційні відносини у суспільстві, що охороняються законом, а предметом – електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі, а також комп'ютерна інформація, що обробляється за їх допомогою. У їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Тому існує необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. Інформаційні відносини, тобто відносини, що виникають при одержанні, використанні, поширенні та зберіганні інформації, регулюються положеннями Конституції України, розділом XVI Кримінального кодексу України, законами від 2 жовтня 1992 р. № 2657-XII «Про інформацію», від 25 червня 1993 р. № 3322-XII «Про науково-технічну інформацію», від 18 листопада 2003 р. № 1280-IV «Про телекомунікації», від 5 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах», а також низкою підзаконних актів, зокрема Положенням про технічний захист інформації в Україні (затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99) та ін. У залежності від виду правопорушення особи, винні у вчиненні «комп'ютерних» злочинів, несуть кримінальну, адміністративну, цивільно-правову, дисциплінарну або матеріальну відповідальність [4].

Останнім часом рівень кіберзлочинності швидко зростає і в нашій державі. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Росією, Бразилією, Китаєм та меншою мірою – Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування. Однак, на думку експертів, кіберзлочинність не є негайною загрозою для українців. Наша країна в особливому становищі, адже має один із найнижчих у Європі рівнів підключення до Інтернету. На сьогодні Україна увійшла до трійки лідерів з DDoS-атак. За даними Лабораторії Касперського, 12% від усіх атак припадає на Україну [2].

У нашій державі до кіберзлочинів відносять порушення авторського права і суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ухилення від сплати податків, зборів (обов'язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографічних предметів, незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю [5].

Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв. За даними НБУ, у 2011 році кількість протиправних операцій за платіжними картами українських банків зросла до 7,6 тис. порівняно з 2,9 тис. роком раніше. Обсяг неправомірно списаних коштів збільшився майже в півтора рази – з 6,3 млн до 9,1 млн грн. І це лише офіційна статистика, до того ж за 2011 рік [3].

Нині кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж ще 5 років тому. Незважаючи на зусилля правоохоронних органів, спрямованих на боротьбу з кіберзлочинами, їх кількість, на жаль, не зменшується, а, навпаки, постійно збільшується. Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері [2].

Отже, вирішення проблеми кіберзлочинності потребує активізації зусиль як на національному, так і міжнародному рівні. Позитивні наслідки протидії інтернет-правопорушенням можуть мати місце лише за умови співробітництва та значної уваги до цього питання з боку всього світового співтовариства. Річ у тім, що саме злочини у віртуальному просторі носять транснаціональний характер, спричиняють значні збитки морального та матеріального характеру, становлять загрозу національній та світовій кібербезпеці.

#### Література:

1. Біленчук Д.П. Кібрешахраї – хто вони? // Міліція України, 1999. №7-8. С.32-34.
2. Довбиш М. Кіберзлочинність в Україні [Електронний ресурс] – Режим доступу: <https://www.science-community.org/ru/node/16132>
3. Кіберзлочинність можна зупинити тільки спільними зусиллями [Електронний ресурс] – Режим доступу: [http://www.ukrbizn.com/vlast\\_biznes/632-kberzlochinnst-mozhna-zupiniti-tlki-splnimiti-zusillyami.html](http://www.ukrbizn.com/vlast_biznes/632-kberzlochinnst-mozhna-zupiniti-tlki-splnimiti-zusillyami.html).
4. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку [Електронний ресурс] – Режим доступу: <http://www.scourt.gov.ua/clients/vsen.nsfh>.
5. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби [Електронний ресурс] – Режим доступу: <https://www.gurt.org.ua/articles/34602/>

### Особливості прояву моральної шкоди через поширення недостовірної інформації в мережі інтернет

**Мороз А.С.**

студентка 2 курсу

факультету № 4 ОДУВС

**Науковий керівник: Сухарєва А.О.**

старший викладач кафедри

цивільно-правових дисциплін ОДУВС

На сьогоднішній день є дуже частими випадками, коли розміщують різноманітну інформацію на інтернет-сайтах, сторінках соціальних мереж, блогах, які своїм змістом порушують права та інтереси фізичної особи, а також ділову репутацію фізичних і юридичних осіб. Це є проявом порушення особистих немайнових прав особи через недостовірну інформацію в мережі інтернет.

Недостовірною вважається інформація, яка викладена не правдиво або не відповідає дійсності. Таким чином, містить різні відомості про явища і події, яких взагалі не існувало, але бувають випадки коли відомості існують, але не відповідають дійсності, тобто не повні. Поширення інформації є демонстрація в громадських місцях плакатів, інших творів, гасел, опублікування у пресі, передання по телебаченні, чи з використанням інших засобів масової інформації, що за своїм змістом, а також формою, порочать та пригнічують гідність та честь фізичної або юридичної особи.

Проблеми захисту честі та гідності розглядали: Можаровська.К.В, Стефанчук. Р.О і Луспенік. Д.Д. Вони зазначали, що в деяких випадках коли інформацію яка порочить честь та гідність сприйняла особа, думка якої є для позивача важливо, тоді позивач має право вимагати від суду обов'язкового спростування інформації перед тією особою за рахунок відповідача, про що повинно бути зазначено у рішенні суду [3,108].

Слід зазначити, що виникнення моральної шкоди тісно пов'язане із обставинами справи, із самої особи, оскільки досить різні протиправні дії тягнуть неоднакові негативні наслідки негативного характеру для різних потерпілих.

Згідно із п.4, ст.23 ЦК України, моральна шкода полягає у приниженні честі та гідності фізичної особи, а також ділової репутації фізичних та юридичних осіб. Моральна шкода може стати наслідком порушення немайнових прав і благ – честі, гідності, свободи. Закріплення за державою важливого обов'язку забезпечення прав, і свобод людини, у випадку їх порушення, дає можливість звернутися до суду з метою захисту та відновлення, а також за компенсацією такої шкоди.

Право на відшкодування матеріальної шкоди дає людині право вимагати від порушника вчиняти певні дії які спрямовані на послаблення та усунення негативних наслідків, які викликані в приниженні гідності.

Моральна шкода підлягає відшкодуванню незалежно від майнової шкоди. Цивільний Кодекс України не встановлює ні мінімального, ні максимального розміру відшкодування. Відшкодування моральної шкоди є компенсація за втрати не майнового характеру, вона відшкодовується одноразово. Але законом чи договором буває передбачено не одноразове право на відшкодування. Розмір відшкодування моральної шкоди визначається судом з урахування змісту, в суті позивних вимог, характеру діяння особи, котра вчинила шкоду.

З аналізу судової практики можна виокремити основних суб'єктів, які найчастіше потребують захисту честі та ділової репутації. ЗМІ уважно пильнують за ними. Такими суб'єктами, зокрема, є