

### **Література**

1. Ісмайлов К.Ю. Акти судової влади в системі джерел національного права України: монографія / К.Ю. Ісмайлов. – Донецьк: Вид-во «Ноулідж» (Донецьке відділення), 2014. – 116 с.
2. Костецька Т.А. Джерела інформаційного права України: поняття, система, особливості / Т.А. Костецька // Часопис Київського університету права, 2007. – № 3. – С. 68-73.
3. Письменицький А.А., Гапотій В.Д. Загальна теорія інформаційного права: Монографія. – Мелітополь: ТОВ «Видавничий будинок ММД», 2012. – 300 с.
4. Тополевський Р.Б. Системні зв'язки юридичних джерел права [Текст] : дис. ... канд. юрид. наук : 12.00.01 / Руслан Богданович Тополевський. – К., 2004. – С. 12.
5. Мураховська Т.Є. Формування нових галузей в системі права України [Текст]: дис. ... канд. юрид. наук : 12.00.01 / Тетяна Єгорівна Мураховська; Харк. нац. ун-т внутр. справ. – Х., 2011. – 233 с.

## **ДЕЯКІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ**

**Косаревська О.В.**

*к.пед.н., доцент, доцент кафедри кібербезпеки та інформаційного забезпечення  
Одеський державний університет внутрішніх справ*

**Олексієнко А.О.**

*студент 2-го курсу факультету №4  
Одеський державний університет внутрішніх справ*

В сучасних складних умовах соціально-політичного, економічного, культурного розвитку українського суспільства на шляху спрямування до європейських стандартів, в край необхідним постає проблема боротьби з кіберзлочинністю та правового регулювання кібербезпеки в Україні як одного із загальнодержавного напрямку.

Аналіз сучасної наукової думки стосовно протидії кіберзлочинності та удосконалення нормативно-правового регулювання в сфері кібербезпеки, а саме робіт: І.Р. Березовської, В.М. Бутузова, В.Д. Гавловського, В.П. Горбулінова, І.В. Литовченко, О.Ю. Паливоди, О.М. Петрашева, О.О. Тихомірова В.Г. Хахановського та ін. визначає, що кіберзлочинність слід розглядати як самостійну площину у системі загальної злочинності (здебільш в економічній сфері) у зв'язку з чим дає підставу наголосити на окремі проблемні аспекти.

Кіберзлочинності притаманні такі кримінологічні риси, як: транснаціональність, латентність, динамічність темпів зростання та трансформацій, анонімність, масштабність наслідків, тощо[5, С. 252-259].

Комп'ютерне піратство, шахрайство, хакерство та новітній прояв кіберзлочинності – кібертероризм міцно закріпились у суспільній свідомості як особливо небезпечні явища, перед якими можуть опинитись беззахисними як окремі громадяни так і суспільство та

держава в цілому. Саме тому кіберзлочинність вже набула масштабів загрози міжнародній безпеці і стала одним з головних предметів державної та міжнародної діяльності.

- Проблемами, які ускладнюють боротьбу з кіберзлочинами слід зазначити:

- неврегульованість правового забезпечення Національної державної політики у сфері кібербезпеки;
- не сформованість єдиної державної структури з координації протидії кіберзлочинам.

За останні роки чинне законодавство України у сфері забезпечення кібербезпеки держави являє собою цілу низку нормативних документів різних рівнів, а саме:

- «Конвенція про кіберзлочинність. Конвенція ратифікована із застереженнями і заявами Законом №2824-IV від 7.09.2005 ВВР 2006 №5-6 ст.7»

- Закони України: Про інформацію: закон України від 02.10.1992. № 2658 XII із змін., внес. згідно із законами України : за станом на 25.06.2016 року N 2938-VI.; Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994 року №90/94-ВР станом на 19.04.14 року.; Про державну таємницю: закон України від 21.01.1994 року №3855-XII станом на 09.08.2015 року; «Про Державну службу спеціального зв'язку та захист інформації України»//Відомості Верховної Ради України. – 2006. - №30. – ст.258.; Про основи національної безпеки України: закон України від 19.06.2003 року № 964-IV станом на 07.08.2015 року; Про Доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 року № 514/2009;

Кримінальний кодекс України прийнятий 05.04.2001 року, зі змінами від 08.10.2016 встановлює у розділі XVI кримінальну відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку» (ст.ст. 361-363).

Особливого розгляду потребує рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», яка була затверджена указом Президента України від 15 березня 2016 року, №96/2016.

Мета нової стратегії кібербезпеки в Україні полягає в створенні умов для безпечної експлуатації кіберпростору, його використання в інтересах особистості, суспільства і держави.

Найбільш важливими, на нашу думку, напрямками реалізації вищезазначеної стратегії є:

- розробка та оперативна адаптація державної політики в сфері кібербезпеки, досягнення сумісності з відповідними стандартами ЄС і НАТО;
- забезпечення кіберзахисту критичної інфраструктури до якої входять: енергетичні і транспортні магістральні мережі, лінії нафто- і газопроводів, морські порти і т.д.;
- розвиток потенціалу сектора безпеки та оборони в сфері кібербезпеки;
- створення спеціальних підрозділів у Збройних силах України за рахунок залучення провідних ІТ-фахівців;
- вдосконалення процедурних механізмів збору доказів в електронній сфері (підрозділи: кіберполіції, СБУ); підготовка суддів, слідчих суддів і прокурорів для роботи з електронними доказами;

—створення механізму анти-кібератак проти агресії у віртуальному просторі, з метою «активного кіберзахисту» у воєнно-політичній та воєнно-технічних сферах (СБУ, Служба зовнішньої розвідки, Національний інститут стратегії дослідження).

Окремим завданням постають питання внесення змін до правового регулювання щодо заходів відповідальності за порушення у сфері кіберпростору (захист даних) та підготовка високо кваліфікованих спеціалістів у сфері протидії кіберзлочинності.

Згідно статистичних даних сьогодні в Україні близько 18 млн. громадян є постійними користувачами мережі Інтернет. З кожним роком злочинів в інтернеті збільшується приблизно на 25-30%, але разом з тим збільшуються і можливості держави.

За даними спецслужб, за останній рік українські хакери вкрали з кредитних карт у всьому світі близько сотні мільйонів доларів. За кількістю спроб зараження комп'ютерними вірусами Україна випереджає країни не тільки Східної та Західної Європи, а також Центральної Азії і США, як показало дослідження «Лабораторії Касперського» [3].

Українською проблемою є як недостатня кількість державних експертів в області комп'ютерно-технічної експертизи, так і складності з введенням в правове поле досліджень фахівців комерційних організацій. Середній термін проведення комп'ютерно-технічних експертиз становить від півроку і вище через високу завантаженість профільних державних установ. Для проведення розслідування таких злочинів необхідні кваліфіковані фахівці, що володіють не тільки технічними навичками, але й знаннями в галузі права [6].

На підставі вище викладеного аналізу нормативно-правової бази у сфері запобігання кіберзлочинності та наукових досліджень у сфері забезпечення кібербезпеки в Україні ми дійшли наступних висновків.

1. Стрімкий розвиток інформаційних технологій створюють серйозну загрозу для національної і міжнародної безпеки у всьому світі.

2. Поточний рівень кібербезпеки в Україні є досить низьким, що приводить до збільшення кількості випадків незаконного збирання, зберігання, використання, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства.

3. Розвиток потенціалу сектора безпеки та оборони має включати реалізацію здійснення державного стратегічного планування та програмно-орієнтованого, програмного забезпечення у сфері електронних комунікацій, інформаційних технологій, захисту інформацій та кіберзахисту.

4. Запорукою дієвої боротьби з кіберзлочинністю виступає консолідація зусиль ОБСЄ в боротьбі з сучасними викликами і загрозами безпеці, такими як: тероризм, торгівля людьми, кіберзлочинність, організована транскордонна злочинність

### **Література**

1. Конвенція про кіберзлочинність. Конвенція ратифікована із застереженнями і заявами Законом №2824-IV від 7.09.2005 ВВР 2006 №5-6 ст.7

2. Про Стратегію кібербезпеки України: Указ Президента України від 27 січня 2016 року №96/2016 [Електронний ресурс]. — Режим доступу: <http://zakon0.rada.gov.ua/laws/show/96/2016>

3. Киберпреступность в Украине набирает обороты [Електронний ресурс]. — Режим доступу: <http://ru.golos.ua/social.problem/>.

4. Хахановський В. Г. Проблеми реалізації в Україні положень Конвенції про кіберзлочинність у контексті міжнародної співпраці / В. Г. Хахановський, Є. М. Ращенко // *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. – К. : МНДЦ, 2014. – № 22. – С. 208-215

5. О.О. Тихомиров «Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки» // *Право України: Юрид. журн.* 2011. – № 4 – с. 252 – 259

6. Устенко А. Страна становится эпицентром киберпреступности [Електронний ресурс] / А. Устенко. — Режим доступу: <http://focus.ua/society/210275/>

### **Порушення авторських прав у кіберпросторі та шляхи їх рішення**

**Кузьмініх А.Ю.**

*студент факультету №4*

*Одеського державного університету внутрішніх справ*

**Даниленко С.К.**

*старший викладач кафедри цивільно-правових дисциплін*

*Одеського державного університету внутрішніх справ*

У сучасну епоху, яку називають «інформаційним суспільством», ми є свідками бурхливого розвитку інтелектуальної діяльності людини. Ця діяльність має значення не тільки для людини, але і для соціального й економічного розвитку будь-якої держави. Вона є складовою частиною безпеки держави, оскільки недостатній інтелектуальний потенціал, що є, як правило, наслідком недостатнього розвитку нормативно-правової бази, яка веде до неконкурентоспроможної економіки, отже до слабкої держави. Змінюються суспільні процеси, в наше життя давно міцно увійшли такі поняття, як комп'ютер, програмне забезпечення, Інтернет. Бібліотеки та архіви поступаються місцем електронним бібліотекам. Електронні банки даних, що містять величезну кількість творів літератури, науки, мистецтва, цілком уміщаються на жорсткому диску комп'ютера або web-сайті. Обслуговуються вони, як правило, однією людиною. Інтернет - поняття глобальне не тільки в географічному, а й у соціально-правовому сенсі цього слова. Він, в тій чи іншій мірі, зачіпає самі різні сфери життєдіяльності сучасної людини, в тому числі і цивільно-правові відносини.

Актуальність теми визначається тим, що захист авторських прав в мережі Інтернет до цих пір не отримала достатнього висвітлення в юридичній літературі. Захист же авторських прав в мережі Інтернет за допомогою сучасних комп'ютерних технологій, перш за все, залежить від того, наскільки грамотно використовуються їхні можливості. В даний час гостро стоїть необхідність регулювання питань захисту в Глобальній мережі, регламентації Інтернету, як найбільш важливого елемента нових інформаційних технологій. Серйозну увагу на дану проблему теоретики і, особливо, практики стали звертати відносно недавно, коли Інтернет міцно увійшов у життя людини. Таким чином, слід відзначити, що дана проблема практично не досліджена, хоча в останні роки і теорія, і практика визнають необхідність її врегулювання.