

та інстанційності, але з виокремленням і закріпленням на конституційному рівні відповідно до принципу спеціалізації автономної трирівневої системи адміністративних судів: окружні адміністративні суди, апеляційні адміністративні суди і Верховний Адміністративний Суд України, що буде утворений внаслідок злиття Вищого адміністративного суду України з судовою палатою в адміністративних справах Верховного Суду України. Зазначені зміни мають бути відображені у статті 125 Конституції України.

УДК 340. 342.951

**Сопілко І. М.**, д.ю.н, професор,  
директор Навчально-наукового Юридичного інституту,  
Національний авіаційний університет, м. Київ, Україна  
**Зятко Й.**, президент Європейського інституту  
безперервної освіти, Dr.h.mult.JUDr., професор, Словаччина

## **ІНФОРМАЦІЙНІ СКАНДАЛИ ТА ДЕЗІНФОРМАЦІЯ ЯК ЗАГРОЗИ ОСОБИ, СУСПІЛЬСТВУ ТА ДЕРЖАВІ**

Сучасний світ як і Україна з розвитком інформаційних технологій вступили в еру інформаційних загроз, кібератак та, відповідно, інформаційних воєн. Окремі інформаційні війни можуть бути значно результативніші, чим звичайні наземні із використанням людей, території і зброї, так як несуть ураження на невизначені території шляхом використання інформаційних можливостей.

Так, на думку Діордіца І. В., в сучасних умовах зростає загроза використання проти інтересів України кібернетичних засобів як зсередини держави, так і з-за меж її кордонів. Також як загрози в сфері кібернетичної безпеки можна виділити: кіберзлочинність, кібертероризм та кібершпигунство, кібервійна, а самі інформаційні інтервенції і можуть бути складовими перерахованих дій. Злочини із використанням сучасних інформаційно-телекомунікаційних технологій стають все звичнішою практикою в житті українських громадян. Найбільша увага злочинців зосереджена на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів [1].

Важливою тенденцією світового розвитку є зростання ролі гуманітарної безпеки, оскільки вона є складовою національної та міжнародної безпеки й охоплює інтелектуальну, освітньо-виховну, психічну, фізичну, моральну, репродуктивну, духовну, генетичну, майнову, міграційну та культурно-етнічну безпеки [2, с. 124].

Сьогодні однозначно можна констатувати, що дедалі більше розвиток українського законодавства повинен усвідомлювати необхідність

розвитку кібернетичних стратегій, що повинні відігравати ключову роль у захисті комп'ютерних систем. Треба розуміти той факт, що тепер ураження комп'ютерних систем вірусними технологіями можна очікувати не тільки від країн з сильним військовим потенціалом, а також від менших країн, що поставлять собі за мету активно розвивати кібернетичні системи. Усі ці загрози сьогодні стали не лише предметом наукових дискусій, але і елементом нашого інформаційного простору. Так, наприклад, у грудні проти українських компаній – постачальників електроенергії було скоєно низку кібератак, які були спрямовані на виведення підприємств з ладу. Як повідомляє Reuters, мова йде про Прикарпаттяобленерго та ще кілька компаній. «Хоча Прикарпаттяобленерго була єдиною українською компанією з постачання електроенергії, яка заявила про збої в роботі, подібні шкідливі програми були виявлені в мережах ще як мінімум двох інших підприємств», - розповів Роберт Ліповський, старший дослідник шкідливого програмного забезпечення компанії ESET, яка обслуговувала українські підприємства.

Разом з тим, за даними експертів комп'ютерної безпеки з Trend Micro і iSight Partners, атака на Прикарпаттяобленерго може стати першим випадком, коли за допомогою кібератаки вдалося припинити електропостачання. «Вперше ми маємо доказ і можемо пов'язати шкідливу програму і конкретний збій у роботі системи», - підкреслив дослідник Trend Micro Кайл Вілойт. Відзначається також, що хакери отримали доступ до мереж і встановили програму KillDisk, здатну видаляти і перезаписувати файли [3].

Даний факт свідчить про новий рівень інформаційних загроз, які в стані паралізувати великі території держави та завдати значеного збитку економіці. Відповідні дії хакерів потребують належного реагування зі сторони держави шляхом вдосконалення системи захисту програмного забезпечення та унеможливлення відповідних загроз.

Реалізація національних інтересів щодо забезпечення національної безпеки одним з найважливіших напрямів цієї трансформації. Так, в тексті «Доктрини інформаційної безпеки України», яку було прийнято від 28 квітня 2014 року сказано, що за умов швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки [4].

Початок 2016 року ознаменувався рядом подій, що свідчать про зростання інформаційних загроз не лише в Україні, але і в світі. Так, в січні 2016 року набув розголосу інформаційні скандали з приводу замовчування інформації про акти насилля до жінок в Європі в новорічний період. Так, станом на кінець січня 2016 року стало відомо про сексуальні домагання та напади на жінок, що сталися у багатьох європейських містах – ці дані починають оприлюднювати офіційні та

неофіційні джерела. Наймасовіші напади сталися у німецькому Кельні, але менш масштабні напади цієї ж ночі були зафіксовані ще у чотирьох містах Німеччини та в ряді інших країн Європи [5]. Проблемою, в даному випадку є факт замовчування та маніпуляції цією інформацією, яка мала масштабний характер, а тому відповідні дії посадових осіб несуть загрозу не лише приватного але і державного характеру та в цілому являються загрозою стабільності в Європі.

Тому, з метою попередження зловживання інформацією та для захисту інформаційних прав сучасний стан забезпечення національної та інформаційної безпеки України потребує розробки науково обґрунтованої державної політики та стратегії в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах, захисту від інформаційних загроз та реалізації права на отримання достовірної інформації. Паралельно, усе вищевикладене свідчить про потребу прийняття нормативно-правових актів в яких був би передбачений механізм захисту інформаційних прав громадян від протиправних дій третіх осіб щодо інформації та обмеження її впливу на особу. Особливої актуальності заслуговує питання вдосконалення програмного забезпечення діяльності основних державних інституцій, організацій та підприємств.

### *Література*

1. Діордіца І. В. Інформаційні інтервенції як загроза кібернетичній безпеці [Електронний ресурс]. – Режим доступу: <http://goal-int.org/informacijni-intervencii-yak-zagroza-kibernetichnij-bezpeci/>.
2. Новицкий Г. В. Проблемы обеспечения национальной безопасности в условиях глобализации / Г. В. Новицкий // Геополитика – безопасность – терроризм : сб. ст. ; под. ред. Е. А. Вертлиба, Л. М. Бонданца. – Бишкек : Изд-во Бийиктик, 2006. – С. 123–128.
3. Reuters дізналося подробиці кібератаки на українські об'єкти енергетики. // <http://nv.ua/ukr/ukraine/events/reuters-diznalasja-podrobitsi-kiberataki-na-ukrajinski-ob-jekti-energetiki-89667.html>.
4. Доктрина інформаційної безпеки України від 28 квітня 2014 року [Електронний ресурс]. – Режим доступу: [http://comin.kmu.gov.ua/control/uk/publish/article?art\\_id=113319&cat\\_id=61025](http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025).
5. Хвиля насильства новорічної ночі: країни Європи одна за одною визнають напади на жінок [Електронний ресурс]. – Режим доступу: <http://tsn.ua/svit/hvilya-nasillya-novorichnoyi-nochi-krayini-yevropi-odna-za-odnoyu-viznayut-napadi-na-zhinok-567784.html>.