Олександр Онищенко,
аспірант кафедри політичних теорій
Національний університет «Одеська юридична академія»

Науковий керівник – *д. іст. н., проф.* ***Л. І. Кормич***
Національний університет «Одеська юридична академія»

БЕЗПЕКОВИЙ ВИМІР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СУЧАСНОМУ СВІТІ

У сучасному світі процеси глобалізації та інформатизації невпинно змінюють навколишній світ й ту дійсність, в якій наразі відбувається життєдіяльність людства. Ми спостерігаємо повсякденні зміни, що відбуваються у суспільстві, державі, світі – зміни, які беззаперечно пов'язані із науково – технічним прогресом та розповсюдженням інформаційних технологій.

Останнє двадцятиліття знаменувало собою становлення інформаційних суспільств у більшості країн світу, як показника загального прогресу та інформатизації. Разом із появою глобальної Інтернет – мережі, інформація набула нового значення. Завдяки використанню соціальних мереж миттєвий обмін будь-якою інформацією між користувачами став відкритим, зручним та загальнодоступним. Саме тому, сучасні інформаційні технології відкривають нові канали комунікації, що змінюють оточуючий світ, а отже, вимагають подальшого наукового обґрунтування й теоретичного аналізу.

Разом з тим, стрімкий розвиток інформаційних технологій супроводжувався появою нових викликів для людства, а саме: необхідністю подолання нових загроз особистості, суспільству й державі у сфері інформаційної безпеки. Сьогодні поняття «інформаційна безпека» закріплене конституціями більшості держав світу, також й в Україні. Інформаційна безпека являє собою основу будь – якої національної безпеки, яка розглядається крізь призму глобальної проблеми захисту інформації. Інформаційна безпека

держави завжди характеризується ступенем її захищеності, стійкістю основних сфер життєдіяльності стосовно небезпечних інформаційних впливів (4).

Необхідність у конституційному закріпленні «інформаційної безпеки» об'єктивно з'явилась разом із масовим поширенням інформаційних технологій та появою нових каналів комунікації між людьми. Також, із усвідомленням людством нових загроз у сфері порушення конфіденційності інформаційних комунікацій. Сучасні технології намагаються вирішувати поставлені завдання та розробляти якомога ефективніші механізми захисту, передачі та конфіденційності інформації. У XX ст. захист персональних даних та інформації в цілому відбувався шляхом фізичного обмеження щодо засобів добування, переробки і передачі інформації. Сьогодні такі методи не є дієвими, адже людство перейшло у інформаційну епоху, де відбулася технологізація суспільств й держав, де кожен має доступ до телефонів та комп'ютерів, а отже й до каналів поширення інформації. Саме тому, інформація сьогодні є цінним ресурсом, котрий має захищатися державою.

Держава має гарантувати належний захист будь – якої інформації особистості й суспільства, адже це належить до головних державних функцій. Виходячи із головних властивостей інформації (конфіденційність, цілісність, доступність) держава має дбати про її захищеність та запобігати заподіянню шкоди. Виходячи зі сфери застосування інформаційну безпеку можна умовно розподілити на інформаційну безпеку держави, організації та особистості (2).

В контексті розвитку «ІТ – технологій» значно розширилось поняття інформаційної безпеки держави. Зокрема, в науковий обіг було введено поняття «кіберзлочину». Кіберзлочинність – кримінальна діяльність, незаконні дії, спрямовані на злочинне руйнування інформації в інформаційних системах в корисливих цілях. Згідно конвенції Ради Європи усі кіберзлочини можна умовно поділити на 4 групи:

- злочини, спрямовані проти цілісності, конфіденційності та доступності комп'ютерних даних та систем;
- шахрайство та підробка інформаційних даних;

- злочини, пов’язані з розміщенням у мережах протиправної інформації;
- злочини щодо авторських та суміжних прав.

У системі міжнародних відносин питання кіберзлочинності є вкрай важливим та актуальним, адже завдяки сучасним технологіям кіберзлочини можуть здійснюватися з будь – якого куточка світу, хоча жертви таких злочинів фізично будуть знаходитись в іншій державі. Саме тому, для подолання злочинів у сфері інформаційних технологій вагоме місце займає міждержавне співробітництво. Так, Радою Європи була підписана спеціальна конвенція, котра регулює злочини у сфері комп’ютерної інформації від 23 листопада 2001 року. Також, Радою ООН була підписана й прийнята Резолюція щодо міжнародного співробітництва у сфері кібербезпеки задля попередження та розслідування злочинів, спрямованих проти неправомірного використання та фальсифікації персональних даних від 26 липня 2007 року (1, с. 45–50). Задля пошуку найефективніших методів боротьби із кіберзлочинами була створена Міжнародна організація по боротьбі з кібертероризмом – «ІМПАКТ» (1, с. 45 – 50).

З кожним роком кількість міжнародних кіберзлочинів зростає, що вимагає тіснішого міждержавного співробітництва у сфері інформаційних технологій. Наслідком є так звані «кібератаки» на державні й урядові інформаційні системи з боку злочинців. З огляду на це, мають посилюватись державні механізми захисту інформаційних систем. Політика національної безпеки має ґрунтуватися на засадах результативного, послідовного законодавчого забезпечення інформаційної безпеки держави та впроваджуватися шляхом розробки відповідних програм, концепцій, доктрин і стратегій. Адже ефективна інформаційна безпека сприяє розвитку політичної, економічної, соціальної, культурної та іншої державної діяльності.

Отже, сучасна інформаційна безпека держави має бути переглянута в контексті нових світових загроз в умовах посилення кібератак сьогодні. Державою мають бути створені ефективні, дієві механізми захисту

персональних даних та інформації, шляхом впровадження нових програмних засобів безпеки, котрі будуть вбудовані до програмного забезпечення національних систем органів державної влади та органів місцевого самоврядування. Задля сталої інформаційної безпеки держава має узгодити власний стратегічний курс, заснований на розроблених концепціях та доктринах. Має розвиватися державний «ІТ – сектор» як комплекс заходів, покликаний забезпечити чинний інформаційний розвиток в умовах жорсткої, світової конкуренції. Має бути проведений технічний аудит усіх засобів комунікації. На законодавчому рівні мають гарантуватися основні засади забезпечення інформаційної безпеки людини та суспільства.

Таким чином, бурхливий розвиток інформаційних технологій вимагає сьогодні належного державного забезпечення й захисту, а коло проблемних питань, пов’язаних із майбутнім вдосконаленням технологій, буде невпинно зростати, що й надалі потребуватиме наукового обґрунтування.

Список використаних джерел:

1. Ануфрієв М. І., Кісілевич – Чорнойван О. М. Міжнародно – правові засади співробітництва у боротьбі з кіберзлочинами. *Вид. Наше право* (3), 2017. с. 45 – 50

2. Арістова В. І., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг: Монографія. НДІ інформатики і права НАПрН України. К. : Право України. : Право, 2013. 184 с.

3. Голубєв В. О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту* 1997. № 2. С. 39 - 40

4. Князев А. А. Інформаційна війна. Енциклопедичний словник ЗМІ. Бішкек: Вид. КРСУ, 2002. 164 с.