СТАН ТА ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СВІТІ ТА В УКРАЇНІ

Світлана Федорівна ГУЦУ,

кандидат юридичних наук, доцент,
доцент кафедри права Національного
аерокосмічного університету
імені М. Є. Жуковського
«Харківський авіаційний інститут»

Сучасні технології здійснюють величезний вплив на людську цивілізацію, яка будує глобальне цифрове суспільство. Але соціум і культура, в яких ми живемо, теж впливають на індустріальний світ. І в цьому полягає відмінна характеристика цифрової революції, яка об'єднує різні технології і розмиває кордони між фізичним світом, цифровою і біологічною сферами. Основне завдання Industrial Revolution 4.0 - фактично керувати зближенням цих сфер, мінімізуючи різні ризики, в тому числі і юридичні.

Досягнення в галузі бізнесу та технологій ставлять нові завдання щодо забезпечення їх відповідності нормативним вимогам. Розробка і впровадження нових законодавчих норм у сфері інформаційної безпеки є пріоритетним напрямком законотворчості як в міжнародному праві, так і на національних рівнях. Як показують різні дослідження, проблема інформаційної безпеки однакова актуальна і для держав, і для бізнесу, і для окремої особистості. Так, результати моніторингу компанії PwC у дослідженні «PwC's Global Crisis Survey 2019» показують, що 38% опитаних лідерів і керівників компаній вважають кіберзлочинність найсерйознішою причиною кризових корпоративних ситуацій [1].

Відома Американська компанія Check Point Software Technologies в своєму останньому звіті щодо стану кібербезпеки «The 2020 Cyber Security Report» говорить,що у 2019 році спостерігалася ескалація складних і цілеспрямованих кібер-атак. Нова реальність полягає в тому, що зловмисники витрачають більше часу на збір інформації про своїх жертв, намагаючись нанестиїм максимальноїшкоди та збільшити виплати. Так, у першій половині 2019 року напади зловмисних програм мобільних банків зросли на 50% порівняно з 2018 роком.Зібрані дані свідчать про те, що кібер-атак на мобільні пристрої, зазнали 27% усіх організацій у всьому світі [2].

Проблеми кібербезпеки породжують соціальні проблеми суспільства, а як наслідок і держави. За словами видання Strategy + Business люди втратили віру в здатність установ надавати надійні державні послуги. За даними Edelman Trust, який вимірює рівень довіри в усьому світі, протягом останнього десятиліття менше половини світового населення довіряє урядам, бізнесу або навіть громадянському суспільству. Зростання нерівності, незважаючи на економічну вигоду, є одним з важливих факторів, що змушує людей сумніватися в уряді чи роботодавцеві. Швидкість технологічних змін та безпрецедентний обсяг доступної

інформації - у будь-який час та в будь-якій точці за допомогою смарт-пристроїв - посилює це явище. Сьогодні інформація, яка послаблює нашу віру в суспільство, поширюється швидше, ніж відповіді на неї. Ця тенденція буде тільки зростати, оскільки мобільні мережі 5G збільшують швидкість і розширюють широту підключення [3].

Результати досліджень говорять, що занепокоєння людей має реальні підстави. Витік персональних даних з баз державних установ так само реальний, як і з соціальних мереж або персональних девайсів. Наприклад, нещодавно в Україні поширювалась інформація, що у відкритий доступ викладено персональні данні користувачів додатку «Дія». І хоча кіберполіція не підтвердила цю інформацію, безумовно, вона має вплив на зменшення довіри людей щодо надійності і захищеності інформації в базах державних установ.

Таким чином, проблема інформаційної безпеки потребує комплексного вирішення і спільних зусиль держави, бізнесу і громадських організацій.

Ми стали свідками серйозної законодавчої роботи міжнародних і національних систем в цій сфері. Уряди окремих країн і міжнародні інституції працюють над створенням і вдосконаленням відповідної нормативної бази. (Таблиця 1).

Таблиця 1. **Законодавчі документи в області заборонення кіберзлочинності та захисту персональних даних**

Регіон/країна	**Організація**	**Дата**	**Назва**
Європа	Європейський парламент	16.02.2017	2015/2103 (INL) Civil Law in robotics
		23.11.2001	Convension on Cybercrime
		25.05.2018	GDPR
США	Законодавчий орган штату Каліфорнія	01.01.2020	California Consumer Privacy Act
Бразілія	Конгрес Бразілії	лютий 2020	Law 13.709
Чілі	Національний Конгрес	Січень 2019	Law 19.628/2011
Колумбія	Міністерство торгівлі, промисловості та туризму	27.06.2013	Law 1581/2012
Мексіка	Мексіканський Конгрес	6.07.2010	LFPDPPP
Африка	Африканський Союз	27.06.2014	The African Union Convention on Cyber Security and Personal Data Protection
Сингапур	Комісія із захисту персональних даних	22.05.2019	Guide on Active Enforcement and Guide to Managing Data Breaches 2.0
Україна	Верховна Рада України	05.10.2017	Закон «Про основні засади кібербезпеки України»

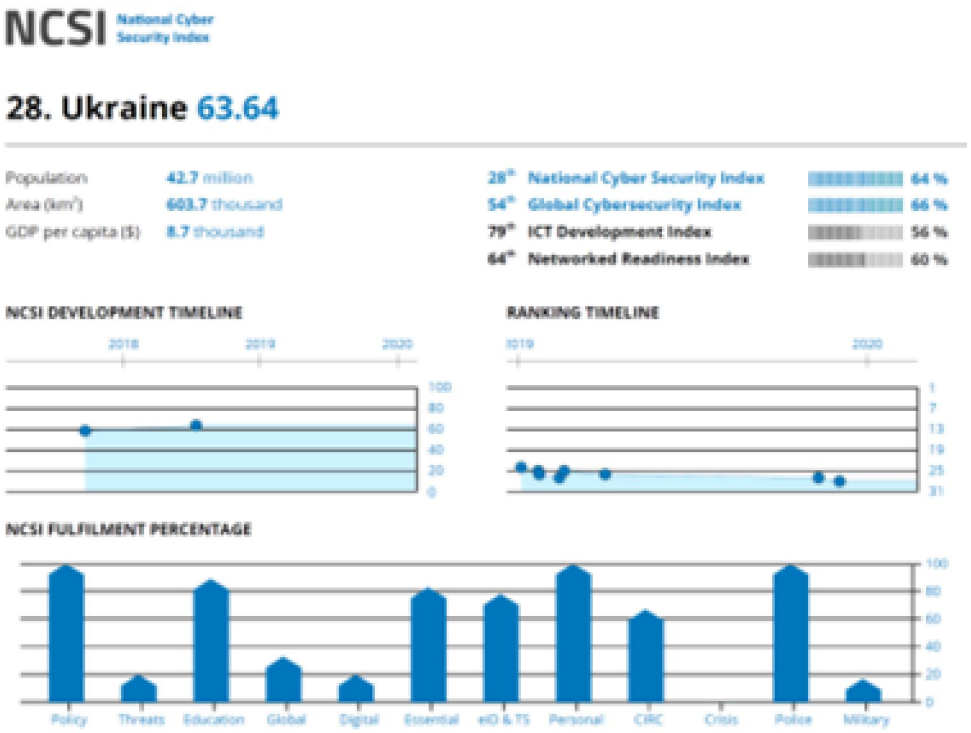
Варто зауважити, що серед правових підходів щодо врегулювання проблем захисту інформації, міжнародна спільнота ще не виробила єдиної позиції. Тому головним правовим завданням у сфері кібербезпеки

залишається розробка загальних міжнародних визначень та стандартів і їх впровадження в національні правові системи.

В Україні з 2018 р. повноцінно запрацювала Стратегія кібербезпекі України і Закон України «Про основні засади забезпечення кібербезпекі України». Також,прийнято Постанову Кабінету Міністрів України від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».

Однак, на сьогоднішній день Україна все ще відстає в плані регуляторної та технічної підтримки кібербезпеки та захисту даних. Національний індекс кібербезпеки за рік знизився на дві позиції (з 26 до 28). Мал. 1

Малюнок 1. **Національний індекс кібербезпеки в Україні** [4]



Захист інформаційної безпеки є однією з функцій держави, національне законодавство повинно визначати ті мінімально необхідні умови та параметри інформаційних процесів, які можна вважати безпечними для існування людини, суспільства та держави. У зв'язку з цим Україні необхідно розробити та впровадити національні стандарти та показники, які б характеризували рівень інформаційної безпеки в різних сферах життя.

Необхідно розділити поняття інформаційної безпеки людини і держави. Інформаційна безпека людини має бути визначена через призму трьох складових: інформаційно-технічної, соціальної і інформаційно-психологічної. Слід законодавчо закріпити і визначити термін «інформаційна безпека людини».

Список використаних джерел:

1. Global Crisis Survey 2019, *PwC*, 2019. [Online]. Available: https://www.pwc.com/globalcrisissurvey. [Accessed: 05- May- 2020].

2. The 2020 Cyber Security Report, *Check Point Software*, 2020. [Online]. Available: https://research.checkpoint.com/2020/the-2020-cyber-security-report/. [Accessed: 10- May - 2020].

3. Sheppard S., Strengthening the foundations of trust in the digital age, *Strategy+Business*, 2019. [Online]. Available: https://www.strategy-business.com/article/Strengthening-the-foundations-of-trust-in-the-digital-age?gko=2e7b2. [Accessed: 11- May - 2020].

4. NCSI : Ukraine, *Ncsi.ega.ee*, 2020. [Online]. Available: https://ncsi.ega.ee/country/ua/. [Accessed: 13- May - 2020].