

**ІНСТИТУЦІЙНІ ТА ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ
КІБЕРБЕЗПЕКИ****Пейдж Нікіта Ендрю,***студент 2 курсу факультету кібербезпеки та інформаційних технологій,
Національний університет «Одеська юридична академія»***ДЕРЖАВНО-ПРАВОВА БАЗА ЛЕГІТИМІЗАЦІЇ БОРОТЬБИ З
КІБЕРЗЛОЧИНАМИ**

Розвиток ІТ-технологій та процес глобалізації внесли значні зміни до світового порядку денного. Технологічні розробки у вигляді комп'ютерів, мобільних телефонів, і, особливо Інтернету, збільшили потік особистих даних. Обмін персональними даними між державними та приватними суб'єктами, окремими особами, асоціаціями та компаніями вийшов на якісно інший рівень. Обмін інформацією зробив особисті дані користувачів доступними, що, з одного боку, призвело до значного покращення якості життя людей, збільшило ефективність та продуктивність корисної праці. З іншого боку, неконтрольований потік інформації піддав користувачів потенційним ризикам, таким як шахрайство, фармінг, скімінг, несанкціоноване розкриття інформації, крадіжка особистих даних та багато іншого.

Залежність державних та комерційних організацій від якісного Інтернету зв'язку пропорційно зростає день за днем [1]. За статистикою, до 2000 року користувачі Інтернету обчислювалися 413 мільйонами, а в 2016 році їх кількість збільшилася до 3,4 мільярда. У той самий час кількість підключених до мережі пристроїв зросла з 17,1 млрд до 27,1 млрд 2021 році [2]. Збільшення кількості користувачів зробило Інтернет вразливим для кіберзлочинів. Як наслідок, питання кібербезпеки вийшли на перший план, а боротьбу з кіберзлочинністю очолили кримінальні фахівці провідних країн [3].

Кіберзлочинців важко покарати через абстрактний характер Інтернету та складнощі, пов'язані з встановленням причин кіберзлочину [1]. Однак ця загроза

безсумнівна становить серйозну небезпеку для конфіденційної та приватної інформації не лише окремих осіб чи підприємств, а й країн в цілому. Такі виклики загрожують національній безпеці, соціальному балансу та фінансовому становищу будь-якої країни. По всьому світу держави стикаються з зростаючим числом кіберзлочинів. За даними світових аналітичних та статистичних центрів, у 2018 році від зловмисних витоків даних постраждали Азіатсько-Тихоокеанський регіон (35%), Північна Америка (30%), Європа, Близький Схід та Африка (27%), Латинська Америка та Карибський басейн (8%). Згідно з іншими даними, у 2019 році з кібератаками більшою мірою зіштовхнулися такі країни: США, Індія, Великобританія, Сінгапур, Україна, Саудівська Аравія, Нігерія, Японія, Південна Корея та Іспанія. За оцінками фахівців кібератаки коштували світовій економіці приблизно 5,2 трильйона доларів у період з 2019 по 2021 рік [4]. Отже, кібератаки несуть величезні економічні, і навіть соціальні витрати багатьох держав.

На міжнародному чи глобальному рівні існує дуже мало правових інструментів, за винятком кількох Резолюції ООН, спрямованих на боротьбу з кіберзлочинністю. Для вирішення проблем кібербезпеки задіяні високі технології, відділи, що спеціалізуються на кіберзлочинах, а також юристи.

Однак, через те, що технологічні досягнення розвиваються швидкими темпами, правова база значно відстає [3]. Виникає необхідність легітимізації юридичних організацій із боку зацікавлених осіб. Організаційна легітимність впливають із примусового ізоморфізму за допомогою прийняття відповідних законів, правил, політики стандартизації та вимог відповідності.

Нормативний ізоморфізм пов'язаний із професійними цінностями та нормами, закладеними у правових документах будь-якої організації.

Публічність законів, що приймаються тією чи іншою організацією створює прецедент для інших компаній, які починають застосовувати аналогічні методи боротьби з кіберзлочинністю [5]. Над конструкційна державно-правова база завершує процес легітимізації боротьби з кіберзлочинами на всіх рівнях.

Література

1. Hunton P. A Rigorous Approach to Formalising the Technical Investigation Stages of Cybercrime and Criminality within a UK Law Enforcement Environment. *Journals Digital Investigation*, 2011. p. 105-113.
2. Singh, H. P. E-Commerce Security: Legal and Policy Aspects of Technology Solutions in India. *Mumukshu Journal of Humanities*, 2016. p. 8, 13-19.
3. Ghosh I. This Is the Crippling Cost of Cybercrime on Corporations. *Journal Beijing Law Review*, Vol.11. No.3, 7 November 2019.
4. Alkalbani A., Deng H., Kam B., & Zhang X. (2017). Information Security Compliance in Organizations: An Institutional Perspective. *Journal: Data and Information Management*, №1. p. 104-114. <https://doi.org/10.1515/dim-2017-0006>
5. Cisco. The Zettabyte Era: Trends and Analysis. The document presents some of the main findings of Cisco global IP traffic forecast. 7 June 2017. <https://www.cisco.com/c/en/us/solutions/>