

Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Тези

**77-ї наукової конференції професорів,
викладачів, наукових працівників,
аспірантів та студентів університету**

ТОМ 2

16 травня – 22 травня 2025 р.

ПРАВОВЕ ПОЛЕ КІБЕРПРОСТОРУ УКРАЇНИ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ

В умовах розвитку ІТ-сфери, кіберпростір стає важливим аспектом в житті кожного громадянина. А захист цього кіберпростору - це нагальна тема для держави. Багато зроблено в Україні з цього приводу. Це імплементація міжнародних правових актів, створення особливих структур з кіберзахисту, об'єднання їх в правове поле та інше. Фахівці з питань кібербезпеки мають розробляти та впроваджувати засоби з безпеки протидії загрозам, враховуючи появи як нових, так і зміни існуючих загроз.

Надаючи правову оцінку тому, як реалізована система кіберзахисту в Україні, слід зазначити, що в основному ця сфера обумовлена вимогами євроатлантичної інтеграції держави, і виходить з тих доктрин та стратегій принципів НАТО та Європейського Союзу. У Стратегії воєнної безпеки України визначені об'єкти критичної інфраструктури, і відповідно для реалізації державної політики у цій сфері необхідно реалізувати національні стандарти, які будуть побудовані на основі європейських стандартів та конвенції про кіберзлочинність. Це є запорукою створення глобальної системи протидії кіберзагрозам, про що визначається в резолюції генеральної асамблеї ООН [2].

У Законі «Про національну безпеку України» до загроз в інформаційній сфері віднесли обмеження свободи слова та доступ громадян до інформації, поширення культу та пропаганди насильства, жорстокості, тероризм комп'ютерний, розкриття інформації, що містить державну та іншу таємницю, та конфіденційну інформацію, яка знаходиться у власності держави або іде на забезпечення потреб національних інтересів суспільства та держави, маніпуляція свідомістю шляхом поширення інформації завідомо помилкової, неповної або необ'єктивної [1].

Це було зазначено на стратегічному рівні, тому що комп'ютерні правопорушення та комп'ютерний тероризм не повністю відображає такі загрози. Надали увагу впровадженню новітніх та конкурентно спроможних інформаційних технологій, а саме сучасних програмних продуктів. Необхідно забезпечити безпеку в інформаційних та телекомунікаційних системах, які діють в інтересах держави, відповідають потребам оборони, кредитному та банківському сектору, в системах критичної інфраструктури, необхідно створити національну систему кібербезпеки. До

загроз віднесли інформаційну війну, яку ведуть проти України, відсутність комунікативної політики держави в цьому напрямку, необхідність підвищення рівня медіакультури. Вразливість об'єктів критичної інфраструктури: державні інформаційні ресурси вразливі до кібератак, причиною цього є нові цифрові технології, розвиток штучного інтелекту та інше [1].

Таблиця 1. Дії з боку держави в сфері кіберзахисту

Інформація	Деталі	Примітка
Термінологія	Кібербезпека, кібератака, кіберзагрози, кібероборона, кіберпростір, та інше	Запроваджено
Основні суб'єкти забезпечення кібербезпеки, та їх завдання	Міністерство оборони України, РНБО, ДСЗІ, СБУ, CERT-UA, Національна поліція України, Національний банк, розвідувальні органи України	Сформовано
Відповідальність	Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361 - 362)	Запроваджено
Відповідність до міжнародних стандартів	Україна ратифікувала конвенцію Ради Європи про кіберзлочинність, Стратегія кібербезпеки України	Запроваджено

В Законі України «Про основні засади забезпечення кібербезпеки України» визначено терміни з цієї сфери. Це і індикатори кіберзагроз, інцидент кібербезпеки, кібератака, кібербезпека, кіберзагрози, захист, злочин, кібероборона, кіберпростір, кібертероризм інші. Визначились із тим, на що буде поширюватись закон, на які відносини та діяльність. Ця діяльність пов'язана як із захистом інформації, так і з державною таємницею, це й соціальні мережі, приватні електронні інформаційні ресурси, комунікаційні системи тощо [3].

До правових основ відносимо Конституцію України, конвенції про кіберзлочинність, Укази Президента України, Кабінету Міністрів України, інші нормативно-правові акти. Визначено також об'єкти кібербезпеки та кіберзахисту, критичної інфраструктури, принципи забезпечення кібербезпеки, а також особливості національної системи кібербезпеки [3].

Тобто можемо констатувати, що в Україні створено нормативно-правову базу для розвитку національної системи кіберзахисту, вдосконалюючи її правову основу, вона впроваджує систему інформаційної безпеки на об'єкти критичної інфраструктури, створює

галузеві центри, які мають реагувати на атаки, а також працює в полі міжнародного співробітництва в сфері протидій кібератакам, підготовки кадрів в сфері кібербезпеки, підвищення цифрової грамотності громадян, впроваджує системи захисту інформації, створюючи довірчі відносини між державою та суспільством.

Зважаючи на динамічний розвиток кіберзагроз та зростаючу цифровізацію всіх сфер суспільного життя в Україні, перспективи розвитку нормативно-правових актів у сфері кібербезпеки є надзвичайно важливими. Очікується подальше удосконалення законодавства, спрямоване на посилення захисту критичної інформаційної інфраструктури, персональних даних громадян та державних інформаційних ресурсів. Варто розробити нормативні акти, що регулюватимуть використання штучного інтелекту в контексті кібербезпеки, протидію дезінформації в кіберпросторі та відповідальність за кіберзлочини, в тому числі з урахуванням міжнародного досвіду та стандартів. Крім того, важливим напрямком має стати гармонізація національного законодавства з європейським у сфері кібербезпеки задля забезпечення інтеграбельності та спільного реагування на транскордонні кіберінциденти.

Література:

1. *Про національну безпеку України: закон України від 21 червня 2018 року № 2469-VIII.* URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
2. *Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України».* URL: <https://zakon.rada.gov.ua/laws/show/121/2021#Text>
3. *Про основні засади забезпечення кібербезпеки України: закон України від 5.10.2017 р. № 2163-VIII.* URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 05.05.2025).

УДК 340.1:342.2

А.О. Кунатенко, студентка групи 401 – П

Науковий керівник:

О.О. Скрильник., к.ю.н., доцент

Національний університет

«Полтавська політехніка імені Юрія Кондратюка»

СУЧАСНІ ТЕНДЕНЦІЇ РЕАЛІЗАЦІЇ ПРАВА НА ЖИТТЯ ТА ПОВАГУ ДО ГІДНОСТІ

Право на життя та повагу до гідності людини є фундаментальними цінностями, що лежать в основі міжнародної системи прав людини. Вони визнаються такими, що не можуть бути обмежені навіть у надзвичайних обставинах, зокрема під час воєнного стану, що є найбільш актуальним