

3. Карчевский В. П. Человек и робот. Развитие процессов обучения. Искусственный интеллект. 2012. № 4. С. 43–52.
4. Ларина О. С., Овчинский В. С. Штучний інтелект. Етика і право. Москва : Книжный мир, 2020. 192 с.
5. Понкін І. В., Редькіна А. І. Искусственный интеллект с точки зрения права. *Вестник Российского университета дружбы народов. Серия : Юридические науки*. 2018. Т. 22. № 1. С. 91–109.
6. Резолюция Европарламента от 16 февраля 2017 года 2015/2013(INL) P8_TA-PROV(2017)0051. URL: https://roboправо.ru/riezoliutsiia_ies
7. Willick, S., 1983. “Artificial Intelligence: Some Legal Approaches and Implications”. *AI Magazine*, 4(2). P. 5–16.
8. Марценко Н., Кучарська Х. Перспективи визнання нових суб'єктів цивільних прав (правовідносин). *Актуальні проблеми правознавства*. 2020. Вип. 3. С. 146–152.
9. Martsenko N. Determining the place of artificial intelligence in civil law. *Studia Prawnoustrojowe*. 2020. (47). <https://doi.org/10.31648/sp.5279/>

Науковий керівник: к.ю.н., доцент кафедри Марценко Н. С.

ТОЩАКОВА АННА СЕРГІЙВНА

Національний університет «Одеська юридична академія»

ПРОБЛЕМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ: МІЖНАРОДНИЙ ДОСВІД

Питання боротьби з кіберзлочинністю актуальне, впродовж багатьох років. Це питання обговорюються в роботах українських та зарубіжних політичних та громадських діячів, наприклад: А. Войціховський, Н. Савчук, О. Островий, І. Нуруллаєв, В. Овчинський, О. Балусева, К. Шахбазян, А. Segura-Serrano.

Із запровадженням новітніх інформаційних технологій розвиток науково-технічного прогресу спричинив появі нових видів злочинів, і в тому числі до протиправного втручання в роботу електронно-обчислювальних машин, комп'ютерних мереж та систем, крадіжок, привласнення, маніпуляції комп'ютерної інформації, а тому це підсумовується як небезпечне антисоціальне явище під назвою «кіберзлочинність».

Стрімкий розвиток інформаційно-комунікаційних технологій сприяв формуванню кібернетичного простору, який здійснює значний вплив на соціально-економічне становище держав та їх національну безпеку. Однак, інформаційні технології не тільки відкривають певні можливості для розвитку країни, але й створюють ряд викликів та загроз, які активізуються з поширенням таких технологій у політичній, соціальній та

економічних сферах, а тому протидія кіберзлочинності є однією з актуальних проблем в сучасному світі.

В сучасних умовах, для яких є характерним збільшення кількості кібератак та кіберінцидентів, що призводять до фінансових втрат, порушення функціонування інформаційно-телекомунікаційних систем, впливають на стан національної безпеки і оборони країн.

До головних чинників, що ускладнюють узгодження позицій держав щодо боротьби з кіберзлочинністю треба виділити наступні:

- невизначеність правового режиму кіберпростору, зокрема Всесвітньої мережі Інтернет;
- не вирішеність проблеми поширення державного суверенітету на кіберпростір та відповідне розмежування юрисдикцій;
- різноманітність понять, що використовуються у національних законодавствах;
- різні підходи до криміналізації та кваліфікації протиправних діянь у кіберпросторі;
- протилежні підходи щодо визначення процедурних понять розслідування вчинених злочинів.

На цьому етапі спеціальні міжнародні угоди такі як Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, колективний проект Європейського союзу та Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону, проект ООН для розроблення законодавства в області кіберзлочинності для африканських країн, проте вони не є універсальними міжнародними документами за своєю природою, хоча деякі поширюються далеко за межі регіонів, де вони були прийняті, а тому це є ще однією проблемою на шляху подолання кіберзлочинності.

Його поширення спричинило використання державами та регіональними організаціями заходів для протидії та боротьби з проявами цього негативного явища. Однією з регіональних ініціатив щодо вдосконалення співробітництва у сфері протидії та боротьби з кіберзлочинністю, учасницею якої є й Україна, є Конвенція про кіберзлочинність, яка передбачала груп, з метою надання негайної допомоги у розслідуванні чи переслідуванні кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними, та з метою збору доказів в електронній формі до кримінального правопорушення, крім цього є Закон України «Про основні засади забезпечення кібернетичної безпеки України» від 2017 року. Більш того, проблема залучення та оптимізації технічних, фінансових та організаційно-управлінських ресурсів, необхідних для ефективного подолання кіберзлочинності в Україні, на сьогоднішній день стає одним із головних завдань державної політики забезпечення

кібернетичної безпеки та є невід'ємною складовою політики національної безпеки.

Оскільки жодна країна не може діяти лише на національному рівні, щоб захистити себе, комплексна боротьба з кіберзлочинністю вимагає:

- гармонізувати кримінальне законодавство щодо кіберзлочинності на міжнародному рівні;

- розроблення на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, з метою ефективного розслідування злочинів у глобальній інформаційній мережі, отримання, розслідування та надання електронних доказів з урахуванням транскордонного характеру цього питання;

- налагодити співпрацю на оперативному рівні правоохоронних органів при розслідуванні кіберзлочинів;

- механізми вирішення питань юрисдикції у кіберпросторі.

Отже, навряд чи хтось в двадцять першому столітті стане заперечувати, що кіберзлочинність виступає суспільною небезпекою, але на відміну від шахрайства та традиційних крадіжок, вона безперервно удосконалюється, що у свою чергу обтяжує протидію та виявлення цієї незаконної діяльності. У порівнянні з існуючими заходами боротьби з будь-якою іншою формою транснаціональної злочинності, продуктивний контроль за кіберзлочинністю потребує більш глибокої міжнародної співпраці.

Список використаних джерел

1. Конвенція про кіберзлочинність від 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 13.11.2021).
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 01.08.2021. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 13.11.2021).
3. Войцеховський А. В. Міжнародне співробітництво у боротьбі з кіберзлочинністю. Право і Безпека. 2011. 112 с.
4. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. Видавничо-поліграфічний центр «Київський університет». 2009. 342 с.
5. Островий О. В. Формування державної політики забезпечення кібернетичної безпеки в Україні : дисертація. Маріуполь, 2019. 239 с. URL: <https://dsun.edu.ua/storage/documents/nauka/specrada/Островий/дисертація.pdf> (дата звернення: 13.11.2021).

Науковий керівник: к.ю.н., доцент, доцент кафедри Грушко М. В.