DOI: https://doi.org/10.32782/PPSS.2023.1.91

ДЕЯКІ АСПЕКТИ ВИЗНАЧЕННЯ МЕХАНІЗМУ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Владислава Олександрівна МОРОЗ,

курсант 2 курсу навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ (м. Дніпро, Україна)
https://orcid.org/0009-0001-6841-9751

Науковий керівник: *Хашев В. Г., канд. юрид. наук, доц., доцент кафедри кримінального права та кримінології, Дніпропетровського державного університет внутрішніх справ*

SOME ASPECTS OF DEFINING THE CYBERCRIME PREVENTION MECHANISM

Cybercrime poses a serious threat to society in today's digital world, with the surge in information and communication technology usage leading to an increase in cyber-attacks, fraud, and crimes against digital systems and personal information. As new societal relations develop, so does criminality. Key elements include legislative regulation, specialized law enforcement agencies, training for investigators and judges, technical means for detection, and international cooperation. Combatting cybercrime requires a dynamic and destructive phenomenon, necessitating improvements in the legal framework for effective control and resistance to this modern form of criminality.

Кіберзлочинність стала серйозною загрозою для суспільства в сучасному цифровому світі. Збільшення використання інформаційно-комунікаційних технологій призводить до збільшення кількості кібератак, шахрайства та інших злочинів, спрямованих проти цифрових систем і особистої інформації.

Кримінально-правовий обсяг поняття "кіберзлочинність" складають кримінально протиправні діяння, відповідальність за вчинення яких передбачено статтями 361, 361-1, 361-2, 362, 363, 363-1 Кримінального кодексу України, що містяться у його Розділі XVI Особливої частини "Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку". Під кіберзлочинністю слід розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [1, с. 19].

Де розвиваються нові суспільні відносини, там з'являється й злочинність. Відповідно до офіційної статистики Офісу Генерального прокурора України, лише за останні 8 років кількість виявлених кіберзлочинів збільшилась майже в 7,5 разів (і це не враховуючи класичні правопорушення з використанням комп'ютерної техніки, а також рівня латентності такої злочинності) [2]. Су-

часні кримінальні механізми протидії кіберзлочинності націлені на ефективне припинення, розслідування та кримінальне переслідування кіберзлочинності. Для досягнення цієї мети впроваджуються наступні ключові елементи:

1. Законодавча регламентація: Національні закони повинні визнавати кіберзлочини, дати чітке визначення кожного злочину та встановити відповідальність за них. Це включає законодавчу базу для покарань, кримінальних санкцій і компетентних органів, які здатні ефективно боротися з кіберзлочинністю.

2. Спеціалізовані органи правопорядку: необхідно удосконалювати та забезпечувати сучасними технологіями спеціалізовані відділи поліції для розслідування та боротьби з кіберзлочинами. Для того, щоб ці органи працювали ефективно, вони повинні мати ресурси, кваліфікований персонал і сучасні технології.

3. Підвищення кваліфікації слідчих та суддів: Комплексні знання та розуміння цифрових технологій, методів атак та слідчих прийомів є вирішальними для ефективного розслідування та судового розгляду кіберзлочинів. Тому важливо забезпечити підвищення кваліфікації слідчих та суддів у цій сфері, щоб вони були готові до ефективного розгляду кіберсправ.

4. Технічні засоби і методи детекції: Розвиток спеціальних технічних засобів і методів детекції є важливим для протидії кіберзлочинній діяльності. Використання новітніх технологій, таких як “блокчейн”, штучний інтелект та машинне навчання, може допомогти виявити та запобігти кібератакам.

5. Міжнародне співробітництво: Кіберзлочинність не має меж, тому міжнародне співробітництво є необхідним для ефективного протидії цьому явищу. Обмін інформацією, досвідом інших країн, створення спільних розслідувальних груп усувають перешкоди, що заважають розкриттю кіберзлочинів та притягненню злочинців до відповідальності.

Для успішної боротьби з кіберзлочинністю, як явищем динамічним, деструктивним, по своїй суті антисоціальним, актуальним є вдосконалення засад правового регулювання боротьби в зазначеній сфері [3, с. 126].

Кіберзлочинність представляє значну небезпеку для суспільства в сучасному цифровому світі. Збільшення використання інформаційно-комунікаційних технологій призвело до значного зростання кількості кібератак, шахрайства та інших злочинів, спрямованих проти цифрових систем і особистої інформації.

Відповідно кіберзлочинність має чітко визначений кримінальний обсяг, який охоплює різні види злочинів, пов’язаних із використанням електронно-обчислювальних машин, телекомунікаційних систем і комп’ютерних мереж. Даний висновок підкреслює необхідність комплексного підходу до боротьби з кіберзлочинністю, який включає як законодавчі, так і технічні заходи, а також активне міжнародне співробітництво для ефективного контролю і протидії цьому сучасному виду злочинності.

Список використаних джерел:

1. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с. (дата звернення: 22.10.2023).

2. Єрема М., Борисенко А. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *ЮРЛІГА*. Повідомлення від 13.04.2022. URL: https://jurliga.ligazakon.net/

analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 22.10.2023).

3. Ульянов А., Ніколаєв О., Ташматов В. Правове регулювання протидії кіберзлочинності в Україні. 2020. С. 125-135. URL: http://elib.institutemvd.by/handle/MVD_NAM/4631 (дата звернення: 22.10.2023).