Микитенко Інеса Андріївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Козачина А. М., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор філософії

ІМПЛЕМЕНТАЦІЯ ПОЛОЖЕНЬ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ У НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО

Імплементація положень Конвенції про кіберзлочинність у національне законодавство України є важливим етапом у розвитку державної політики та сфері інформаційної безпеки. З кожним роком роль інформаційних технологій у житті суспільства зростає, а разом із тим – і кількість правопорушень, пов'язаних із використанням комп'ютерних систем, мереж і даних. Саме тому виникла потреба у створенні єдиних міжнародних стандартів, які б регулювали питання протидії таким злочинам. Першим кроком у цьому напрямі стала Конвенція Ради Європи про кіберзлочинність, ухвалена 23 листопада 2001 року в Будапешті. Її головна мета – забезпечити спільну політику держав щодо криміналізації діянь, які вчиняються за допомогою комп'ютерних технологій, а також створити ефективні механізми міжнародного співробітництва.

Україна підписала Конвенцію одразу після її прийняття – 23 листопада 2001 року, а у 2005 році ратифікувала її Законом № 2824-IV. Це означало, що держава взяла на себе зобов'язання забезпечити своє законодавство у відповідності до положень цього міжнародного документа. Імплементація Конвенції полягає не лише у формальному закріпленні її норм у правовій системі, а й у практичному впровадженні міжнародних стандартів боротьби з кіберзлочинами у повсякденну діяльність правоохоронних органів та судової системи.

Передусім, виконання положень Конвенції вплинуло на оновлення кримінального законодавства України. До нього було введено норми, які передбачають відповідальність за несанкціоноване втручання в роботу комп'ютерних систем і мереж, створення та поширення шкідливого програмного забезпечення, незаконне використання або зміну інформації, що обробляється в електронних системах, а також за порушення правил їх експлуатації. Такі нововведення відтворюють основні положення Конвенції та створюють правові механізми для ефективного переслідування осіб, які вчиняють злочини у сфері кібербезпеки.

Окрім змін до кримінального законодавства, значну увагу було приділено удосконаленню кримінального процесу. Конвенція містить положення, що зобов'язують держави забезпечити можливість оперативного доступу до комп'ютерних даних, проведення обшуків і вилучення інформації в електронній формі, а також збереження даних для подальшого розслідування. Україна внесла відповідні зміни до Кримінального процесуального кодексу, що дозволило слідчим використовувати нові форми доказування – електронні листи, файли, записи з мережі Інтернет, дані з мобільних пристроїв.

Реалізація Конвенції про кіберзлочинність також сприяла створенню спеціальних органів, які займаються боротьбою з кіберзлочинами. У структурі Національної поліції України діє Департамент кіберполіції, який координує роботу з виявлення, розслідування та попередження кіберзлочинів. Крім того, створено Національний контактний пункт, який забезпечує цілодобовий обмін інформацією з правоохоронними органами інших країн для швидкого реагування на кіберінциденти.

У 2017 році Верховна Рада України ухвалила Закон «Про основні засади забезпечення кібербезпеки України». Цей закон визначив ключові принципи та напрями державної політики у сфері кібербезпеки, а також перелік суб'єктів, які відповідають за захист кіберпростору – Службу безпеки України, Національну поліцію, Міністерство оборони, Державну службу спеціального зв'язку та захисту інформації. Важливо, що закон передбачає активне міжнародне співробітництво, адже кіберзлочинність не має кордонів і ефективна боротьба з нею можлива лише спільними зусиллями.

Як на міжнародному, так і на національному рівні кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед правоохоронними органами. До цього часу не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці [1, с. 129].

Разом з тим, імплементація положень Конвенції стикається з низкою проблем. По-перше, в Україні все ще не вистачає висококваліфікованих фахівців, здатних професійно працювати з цифровими доказами. По-друге, технічне забезпечення правоохоронних органів часто не відповідає сучасним викликам. По-третє, судова практика у справах про кіберзлочини перебуває на стадії становлення, тому існують труднощі з доказуванням та кваліфікацією таких правопорушень.

У 2022 році Україна підписала Другий додатковий протокол до Конвенції про кіберзлочинність, який спрямований на вдосконалення процедур міжнародного обміну електронними доказами. Це дозволить швидше отримувати необхідну інформацію з-за кордону, а також спростить співпрацю між правоохоронними органами різних країн.

Стрімкий розвиток інформаційних технологій створює умови для появи нових ризиків та кіберзагроз. Незважаючи на позитивний вплив на всі сфери людського життя, цей розвиток зумовив зростання й поширення кіберзлочинів. З упевненістю можна сказати, що кіберзлочини – це одна з основних проблем XXI ст., вирішення якої потребує сучасних методів, активних, рішучих заходів і своєчасного нормативного реагування [1, с. 129].

Оскільки заходи, передбачені Законом України «Про оперативно-розшукову діяльність», можуть бути застосовані і під час кримінального провадження, а зібрана інформація може бути використана як доказ, необхідно узгодити ці положення з Кримінальним процесуальним кодексом, у тому числі і умови та запобіжні заходи, що передбачені ним.

Документ, підготовлений Офісом Програми з кіберзлочинності Ради Європи за участю експертів Маркко Куннапу та Марка Юріча за фінансової підтримки Європейського Союзу, присвячений аналізу процесу імплементації положень Будапештської конвенції про кіберзлочинність у національне законодавство України. У ньому розглядаються чинні

нормативно-правові акти та проєкти законів, що стосуються боротьби з кіберзлочинністю та використання електронних доказів. Документ визначає відповідність українських норм міжнародним стандартам, надає рекомендації щодо вдосконалення правового регулювання у сфері кібербезпеки та сприяє гармонізації законодавства України з вимогами Ради Європи.

Експерти наводять такі рекомендації, ось кілька з них, які є дійсно перспективними: з метою ефективної протидії розповсюдженню незаконного контенту в мережі Інтернет необхідно ретельно врегулювати питання блокування та вилучення такого незаконного контенту з мережі, оскільки цей захід є дуже суперечливим. Окрему увагу при цьому належить приділяти забезпеченню того, що ордери на блокування не застосовуються щодо досить широкого переліку випадків. Варто передбачити суворе застосування вимог щодо пропорційності. Обміркувати розробку спеціальних правил щодо доступу до електронних даних, що будуть застосовуватись за невідкладних обставин, а також їхнього збирання; особливу уваги потрібно приділити умовам та запобіжним заходам щодо того, коли і за яких обставин варто проводити перевірку заходів [3, с.23]. Звісно це не повний перелік рекомендацій, які є слушними, але питання щодо заходів та спеціального доступу до електронних даних є досить цікавою порадою для втілення положень про кіберзлочинність.

Стратегічним пріоритетом вважається прийняття ефективного законодавства у сфері боротьби з кіберзлочинністю та застосування електронних доказів, яке б відповіло вимогам із забезпечення дотримання прав людини і верховенства закону [4, с. 25].

У наслідок аналізу вітчизняного законодавства та порівняння його положень із нормами Конвенції про кіберзлочинність встановлено ряд напрямків, які потребують опрацювання [4, с. 26].

Вирішення цих питань, як зазначено у Конвенції, буде сприяти підвищенню ефективності кримінальних розслідувань, що стосуються кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі [4, с. 26].

Крім того, проблематика протидії кіберзлочинності набуває особливої важливості в умовах запровадження воєнного стану. Сучасні інформаційні війни здатні завдати шкоди, співмірної або навіть більшої за ту, що спричиняється збройними конфліктами на полі бою. У зв'язку з цим, суб'єкти, відповідальні за протидію кіберзлочинам, повинні вживати всіх можливих заходів для мінімалізації кібератак, здійснюваних противником [2, с. 374].

Підписання, державами, членами Ради Європи «Конвенції по боротьбі з кіберзлочинністю», стало результатом розуміння важливості проведення політики, спрямованої на захист суспільства від кіберзлочинів, необхідності прийняття відповідного законодавства та зміцнення міжнародного співробітництва [5].

Використання та удосконалення сфери інформаційних технологій спричинило появу кіберзлочинності – характерного наслідку глобалізації інформаційних процесів. Кіберзлочинність стала загрозою не лише для окремих осіб, а й для держав, оскільки передбачає руйнування економічної та інформаційної сфер. Характерні ознаки кіберзлочинності приваблюють людство, що означає, у свою чергу, збільшення кількості осіб, що чинять протиправну діяльність. Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто – від дрібних злодіїв до досвідчених кіберзлочинців [6, с. 387].

Отже, імплементація Конвенції про кіберзлочинність стала важливим кроком для України у розвитку правової системи та захисті національного кіберпростору. Вона дала можливість створити сучасне законодавство, яке відповідає міжнародним стандартам, налагодити співпрацю з іншими державами, підвищити рівень захисту інформації та сформувати дієву систему реагування на кіберзагрози. Разом із тим, цей процес потребує подальшого вдосконалення – необхідно посилювати технічні можливості державних структур, підвищувати професійний рівень працівників правоохоронних органів, розширювати освітні програми з кібербезпеки та впроваджувати новітні технології. Лише системна робота у цьому напрямі дозволить Україні ефективно протидіяти кіберзлочинності, забезпечити безпеку громадян та зберегти інформаційну стійкість держави у цифрову епоху.

Список використаних джерел

1. Жеребець О. М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект. *Інформація і право.* 2021. № 4(39). С. 129–134.

2. Захаревич Р. В. Імплементація зарубіжного досвіду в українське законодавство щодо протидії кіберзлочинам. *Аналітично-порівняльне правознавство* : електронне наукове видання. 2025. Вип. 3, ч. 2. С. 372–376.

3. Звіт щодо України. Підготовлено Офісом Програми з кіберзлочинності на основі експертної підтримки незалежних експертів Ради Європи пана Маркко Куннапу і пана Марка Юріча. Про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них. 3 листопада 2016 року. URL: https://share.google/f83dkxYASNhL61Kkn

4. Бердиченко І. О. Імплементації окремих норм конвенції про кіберзлочинність у вітчизняне законодавство, проблеми та шляхи їх вирішення. 2017. С. 25–28. URL: https://share.google/fqpxOpRlmoUgbgTqN

5. Конвенція Ради Європи про кіберзлочинність. URL: https://share.google/jaI2tFm8M6PDEzFSd

6. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету.* Серія ПРАВО. 2021. Вип. 64. С. 386–391. URL: https://doi.org/10.24144/2307-3322.2021.64.71