5. *Т. Волошанівська. Застосування судами України практики Європейського суду з прав людини щодо забезпечення права на ефективний захист у кримінальному провадженні.* Науково-практичний журнал «Підприємництво, господарство і право». *12/2017. С. 258-262.*

6. *Цебенко С.Б., Красько С.А. Проблематика застосування практики Європейського суду з прав людини під час здійснення правосуддя.* Науковий вісник Ужгородського національного університету, *2020. Серія ПРАВО. Випуск 61 том 1. С. 43-47.*

DOI https://doi.org/10.36059/978-966-397-359-3-48

ЩОДО ПОСИЛЕННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Гуцалюк Михайло Васильович
кандидат юридичних наук, доцент,
провідний науковий співробітник
Міжвідомчого науково-дослідного центру з проблем боротьби
з організованою злочинністю при РНБО України
м. Київ, Україна

Клименко Ольга Анатоліївна
кандидат юридичних наук
м. Київ, Україна

8 листопада 2023 року Європейська комісія у своєму щорічному звіті про розширення рекомендувала країнам-членам ЄС розпочати з Україною офіційні переговори про її приєднання до Євросоюзу.

Приєднання України до Євросоюзу означатиме входження до єдиного цифрового ринку ЄС, що потребує імплементації низки європейських норм, серед яких важливе місце посідають нормативні документи у сфері кібербезпеки.

Єдиний цифровий ринок – це ринок, на якому забезпечується вільний рух товарів, осіб, послуг та капіталу та де окремі особи й підприємства можуть безперешкодно отримувати доступ і здійснювати діяльність в Інтернеті за умов чесної конкуренції та високого рівня захисту споживачів і персональних даних. Стратегію побудови європейського цифрового ринку було прийнято у 2014 році [1].

Через зростання загроз та інцидентів, що впливають на безпеку інформаційних систем і необхідність прийняття спільних норм та механізмів протидії у липні 2016 року в ЄС було прийнято Директиву (ЄС) 2016/1148 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива NIS [2]). У документі визначено основні положення щодо посилення безпеки в інформаційному просторі та надано відповідні рекомендації.

Уже через шість років у відповідь на зростаючі загрози, спричинені цифровізацією, у грудні 2022 року прийнято Директиву про заходи для високого спільного рівня кібербезпеки в Союзі (переглянута Директива NIS або «NIS 2» [3]). NIS 2 посилює вимоги до безпеки, які висуваються до компаній і стосується зокрема ланцюгів постачання та відносин з постачальниками, оптимізує зобов'язання щодо звітності, запроваджує більш вимогливі заходи нагляду щодо національних органів влади та посилює вимоги до виконання заходів кібербезпеки та спрямована на гармонізацію режимів санкцій у державах-членах. NIS 2 допоможе покращити обмін інформацією і співпрацю з управління кіберкризою на рівні ЄС.

Згідно з даною директивою держава-член призначає або створює один або більше компетентних органів, відповідальних за управління великомасштабними інцидентами та кризами кібербезпеки (органи управління кіберкризами). Держави-члени забезпечують наявність у цих органів відповідних ресурсів для ефективного та дієвого виконання покладених на них завдань. Також утворюється Європейська мережа організації зв'язку з кіберкризами (EU-CyCLONe) – тобто мережа співпраці для національних органів держав-членів, які відповідають за управління кіберкризами. Мережа була запущена в 2020 році та офіційно оформлена 16 січня 2023 року з набранням чинності NIS 2.

Мета створення такої мережі полягає у розвитку своєчасного обміну інформацією та ситуаційної обізнаності на основі інструментів і підтримки, наданих Агентством ЄС з кібербезпеки, що виконує функції Секретаріату CyCLONe.

Для подальшого посилення кібербезпеки та виявлення кіберінци-дентів та реагування на них в ЄС Європейська комісія 18 квітня 2023 року запропонувала Акт ЄС про кіберсолідарність – The EU Cyber Solidarity Act [4].

Закон ЄС про кіберсолідарність спрямований на зміцнення потенціалу в ЄС для виявлення, підготовки й реагування на значні і масштабні загрози кібербезпеці та кібератаки. Пропонується впровадити Європейський щит кібербезпеки і комплексний механізм реагування на надзвичайні ситуації у сфері кібербезпеки. Європейський кіберщит складатиметься з операційних центрів безпеки (Security Operations Center, SOC) по всьому ЄС, об'єднаних

у кілька платформ SOC у кількох країнах. Завдання Cyber Shield – покращити виявлення, аналіз і реагування на кіберзагрози. При цьому SOC використовуватимуть передові технології, такі як штучний інтелект (ШІ) та аналітику даних, щоб виявляти й ділитися попередженнями про кіберзагрози з органами влади у своїй країні та за кордоном.

Ще один важливий елемент забезпечення кібербезпеки – протидія кіберзлочинності. Основним міжнародним документом у цій сфері є Конвенція про кіберзлочинність, прийнята у 2001 році і ратифікована Україною у 2005 році. Зважаючи на те, що кіберпростір не має кордонів і більшість кібератак здійснюється з інших країн, у травні 2022 року було прийнято Другий додатковий протокол до конвенції, який стосується посилення міжнародного співробітництва [5]. Зокрема даним протоколом передбачається спрощена процедура для отримання відповідних даних компетентними органами безпосередньо у провайдерів інших країн. Україна підписала даний протокол і сьогодні необхідно прийняти закон щодо його ратифікації.

Отже, протягом останніх років Україна значно посилила свою кібербезпеку. Про це свідчить належне функціонування вітчизняної інформаційної, у тому числі критичної, інфраструктури під час кібервійни з рф. Водночас тенденція зростання кількості кіберінцидентів та їх складності стосується як усього світу, так і України. Тому необхідно продовжувати зміцнювати кібербезпеку, використовуючи при цьому міжнародний і насамперед європейський досвід та імплементувати у вітчизняне законодавство європейські норми кібербезпеки.

Література:

1. A Digital Single Market Strategy for Europe. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0192

2. ДИРЕКТИВА ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

3. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/ 2555/oj

4. The EU Cyber Solidarity Act. URL: https://digital-strategy.ec. europa.eu/en/policies/cyber-solidarity

5. Ахтирська Н., Гуцалюк М. Правові засоби боротьби з кіберзагрозами під час воєнного стану в світлі використання механізмів Другого додаткового протоколу до Конвенції про кіберзлочинність.

Актуальні питання розвитку юридичної науки та практики: матеріали Міжнародної наук.-практ. конференції (12 травня 2022 р.) / за заг. ред. д.ю.н., акад. НАПрН України О. П. Орлюк, к.ю.н., доц. Г. З Остапенко, к.ю.н. А. В. Айдинян. Київ, 2022. С. 283–286.

DOI https://doi.org/10.36059/978-966-397-359-3-49

РІВЕНЬ ЖІНОЧОЇ ЗЛОЧИННОСТІ ТА ЇЇ ПРИЧИНИ

Дубович Олеся Валеріївна
кандидатка юридичних наук,
доцентка кафедри підприємництва і права
Полтавського державного аграрного університету
м. Полтава, Україна

Жіноча злочинність є однією з найбільш актуальних тем кримінології. За останнє десятиліття кількість жінок, які потрапляють до системи кримінального правосуддя значно зросла в усьому світі. Як і загальна злочинність населення, жіноча злочинність залежить від певних історичних подій. Оскільки світ постійно змінюється і соціальний статус жінки в ньому теж зазнає змін, то змінюється і жіноча злочинність. Сучасний світ прагне рівноправності чоловіків і жінок. І багато в чому жінки зараз мають рівні права з чоловіками, починаючи від особливостей працевлаштування та закінчуючи особистими відносинами між людьми. Наразі у загальній масі жіноча злочинність становить близько 12% від усієї злочинності. Як свідчить практика, вчинені жінками злочинні діяння завжди викликають більший суспільний резонанс, аніж злочини, вчинені чоловіками. Тому вивчення проблеми жіночої злочинності є на разі актуальним у зв'язку із необхідністю врахування у соціальній, кримінологічній та кримінально-правовій політиці держави ґендерної складової, ролі та впливу соціальних та військових конфліктів на жінок і чоловіків [1, с. 2].

Жіночу злочинність від загальної злочинності можна відрізнити за характером злочинів, їх масштабом, наслідками, способами вчинення та багато іншого. Жінка обирає іншу жертву через відсутність грубої сили, вчиняє злочин у дещо інших сферах, ніж чоловіки.

Теоретична значимість дослідження, яка полягає в кримінологічній характеристиці злочинності жінок, а саме у її детермінації, структурних та статистичних показниках жіночої злочинності, може надати допомогу в розробці найбільш ефективних заходів щодо профілактики злочинів з боку