5. Willard, N. E. (2007). Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Center for Safe and Responsible Internet Use.

6. Hinduja S., Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, 14(3), 206–221.

7. Законодавчі акти України: Кодекс України про адміністративні правопорушення, Кримінальний кодекс України, Закон України «Про освіту».

Саінчин Олександр Сергійович,
професор кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор юридичних наук, професор

КРИМІНАЛІСТИЧНІ ЗАСАДИ ПРОТИДІЇ КРИМІНАЛЬНОГО ПРАВА В КІБЕРПРОСТОРІ

Стратегія інформаційної безпеки України – це державний документ, що визначає загрози, стратегічні цілі та завдання для захисту інформаційної сфери держави. Її головна мета – забезпечити захист життєво важливих інтересів громадян, суспільства та держави, протидіяти загрозам, забезпечувати суверенітет, територіальну цілісність та права громадян. Документ затверджений указом Президента № 685/2021 від 28 грудня 2021 року, реалізація якого розрахована до 2025 року [1; 2].

Згідно з затвердженим Кабінетом Міністрів плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року визначні наступні стратегічні цілі, на деяких аспектах реалізації яких в контексті служби безпеки України, ми вважаємо доцільно зупинитися окремо [3]:

1. Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини і громадянина.

На Службу безпеки України [4] та Службу зовнішньої розвідки покладено реалізації наступних заходів: а) проведення моніторингу спеціальними методами і способами вітчизняних та іноземних медіа, Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері; б) здійснення добування, аналітичного опрацювання, оброблення та надання розвідувальної інформації в установленому Законом України «Про розвідку» порядку її споживачам, відповідальним за формування і реалізацію державної інформаційної політики та здійснення заходів стратегічних комунікацій; в) проведення офіційного моніторингу телерадіопрограм українських телерадіоорганізацій та іноземних мовників, які ретранслюють свої програми на території України; г) підготовка проведення систематичного узагальнюючого моніторингу національного інформаційного простору на предмет виявлення дезінформації, що містить загрози для національної безпеки України; д) підготовка проведення систематичного узагальнюючого моніторингу іноземного інформаційного простору (окремі країни) на предмет виявлення дезінформації, що містить загрози для національної безпеки України [5; 6].

Крім цього на Адміністрацію Держспецзв'язку, Мінцифри МКІП, Центр протидії дезінформації, Національний інститут стратегічних досліджень, наукові та науково-дослідні установи, які забезпечують науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики, покладені наступні обов'язки:

а) створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози;

б) вжиття заходів до запобігання та протидії поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України;

в) розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі;

г) підготовка та проведення складовими сил оборони інформаційно-психологічних операцій та інших заходів, спрямованих на запобігання, стримування та відсіч збройної агресії Російської Федерації проти України;

д) посилення відповідальності за поширення недостовірної інформації (дезінформації) [7–9].

Стратегія інформаційної безпеки є рамковим документом і поки що не дає можливості оцінити, наскільки її впровадження вплине на реалізацію цифрових прав. Тим не менш, при розробці плану дій та законодавства, спрямованих на впровадження Стратегії, варто враховувати такі застереження:

– будь-які законодавчі заходи, спрямовані на протидію дезінформації та обмеження доступу до шкідливого контенту в Інтернеті можуть обмежувати право на свободу вираження поглядів виключно за умови відповідності вимогам законності та пропорційності;

– діяльність державних органів, залучених в імплементацію Стратегії має бути прозорою та з чітким розподілом повноважень, зокрема, слід більш чітко визначити орган, відповідальний за реалізацію Стратегії, що аналізуватиме та звітуватиме перед суспільством про ефективність заходів, вжитих на її виконання;

– План дій на виконання Стратегії має передбачати чіткі індикатори вимірювання ефективності її впровадження;

– при реалізації положень Стратегії та розробці Плану дій на її виконання має бути забезпечена повноцінна, а не формальна залученість громадськості.

Список використаних джерел

1. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

2. План реалізації Стратегії кібербезпеки України : Указ Президента України від 01.02.22 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

3. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : Розпорядження Кабінету Міністрів України від 30.03.23 р. № 272-р. URL: https://zakon. rada.gov.ua/laws/show/272-2023-%D1%80#Text

4. Про Службу безпеки України : Закон України від 25 березня 1992 року № 2229-XII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/ show/2229-12#Text

5. Про розвідку : Закон України від 17 вересня 2020 р. № 912–IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/912IX#Text

6. Про Національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

7. Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/main/56/2022.#Text

8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19.03.2022 № 152/2022. URL: https://zakon.rada.gov.ua/laws/show/152/2022#Text

Сердечна Анастасія Романівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Смаглюк О. В., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

КЛАСИФІКАЦІЯ ТА ТИПОЛОГІЧНІ ПІДХОДИ ДО ДОСЛІДЖЕННЯ ОСОБИ ПОТЕРПІЛОГО В КІБЕРПРОСТОРІ

Станом на початок 2025 року в Україні інтернетом користувався 31,5 млн людей, а рівень проникнення доступу до мережі склав 82,4 %. Для порівняння зазначимо, що в Східній Європі цей показник складає 90,6 %. З січня 2024 року до січня