Література:

1. Бізнес зберіг стримані оцінки результатів своєї діяльності – підсумки опитування підприємств у листопаді. Національний банк України. Індекс очікувань ділової активності підприємств у листопаді 2023 року. 01.12.2023. URL: https://bank.gov.ua/ua/news/all/biznes-zberig-strimani-otsinki-rezultativ-svoyeyi-diyalnosti--pidsumki-opituvannya-pidpriyemstv-u-listopadi (дата звернення: 02.12.2023).
2. Про затвердження Критеріїв визначення підприємств, установ і організацій, які мають важливе значення для галузей національної економіки: наказ Міністерства економіки України від 17.02.2023 № 952. Дата оновлення: 10.08.2023. URL: https://zakon.rada.gov.ua/laws/show/z0396-23#Text (дата звернення: 10.11.2023).
3. Про реалізацію експериментального проекту щодо надання на конкурсних засадах фінансової підтримки стартапам в Україні, у тому числі в сфері інформаційних технологій: постанова Кабінету Міністрів України від 24 червня 2022 р. № 736. Дата оновлення: 01.07.2022. URL: https://zakon.rada.gov.ua/laws/show/736-2022-п#Text (дата звернення: 10.11.2023).
4. Деякі питання надання грантів бізнесу: постанова Кабінету Міністрів України від 21 червня 2022 р. № 738. Дата оновлення: 16.11.2023. URL: https://zakon.rada.gov.ua/laws/show/738-2022-п#Text (дата звернення: 17.11.2023).
5. Деякі питання надання грантів для переробних підприємств: постанова Кабінету Міністрів України від 24 червня 2022 р. № 739. Дата оновлення: 15.11.2023. URL: https://zakon.rada.gov.ua/laws/show/739-2022-п#n14 (дата звернення: 16.11.2023).

DOI https://doi.org/10.36059/978-966-397-351-7-101

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВНІ ЄС ТА ОКРЕМИХ ДЕРЖАВ-ЧЛЕНІВ

Недохлєбов Іван Іванович
здобувач кафедри конституційного та адміністративного права Запорізького національного університету

В умовах євроінтеграції, досвід забезпечення інформаційної безпеки на рівні ЄС та її окремих держав-членів є достатньо цікавим для нашої держави. Відзначимо, що на рівні ЄС сформовано систему заходів

забезпечення інформаційної безпеки, до якої включено: підвищення медіакультури та медіаграмотності населення; створення системи попередження інформаційних загроз; технологічна підтримка новітніх розробок у галузі захисту інформації; міжнародна співпраця у сфері інформаційної безпеки; боротьба з кіберзлочинністю; протидія російській пропаганді; захист користувачів від онлайн-загроз [1, с. 119]. Вбачається, що ці заходи окреслюють окремі сфери діяльності держав-членів ЄС та мають ціннісно-орієнтовний характер.

Також в рамках ЄС існує практика індивідуалізації окремих сфер інформаційної безпеки, яка дозволяє деталізувати загрози та розробити адаптовані до них засоби та способи протидії. У якості прикладу наведемо Фінальний звіт дослідження кібербезпеки в енергетиці від 2019 року, який був підготовлений компанією Blueprint Energy Solutions GmbH на замовлення Секретаріату Енергетичного Співтовариства ЄС. В документі наголошено на існуванні геополітичних аспектів, які впливають на рівень кібербезпеки в енергетиці. Також зазначається, що для мінімізації цих ризиків необхідне усунення прогалин у нормативно-правових актах, а також прогалин в інституційних структурах, пов'язаних з кібербезпекою в енергетичному секторі [2]. Для України така індивідуалізація без сумніву є позитивним досвідом, оскільки вона дає змогу диференціювати загрози та напрями протидії.

В основі політики інформаційної безпеки ЄС є низка нормативно-правових актів, які впливають на національне законодавство окремих держав-членів, зокрема:

– Конвенція Ради Європи від 23 листопада 2001 року «Про кіберзлочинність» (регламентує систему заходів, які повинні вживатися на національному рівні задля протидії кіберзлочинності) [3];

– Конвенція Ради Європи від 28 січня 1981 року «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (містить механізми захисту приватного життя, зокрема персональної інформації особи) [4];

– Директива Європейського парламенту і Ради ЄС 2016/1148 від 06 липня 2016 року «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» (деталізовані питання захисту інформаційних систем та забезпечення якості відповідних послуг) [5] та інші акти.

Пропонуємо також звернути увагу на досвід забезпечення інформаційної безпеки окремими країнами ЄС. Досліджуючи досвід Болгарії та Румунії Т. Ю. Ткачук систематизує наступні напрями діяльності: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення

європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення інформаційної безпеки; зміцнення інформаційної безпеки на державному рівні шляхом впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки [6, с. 63]. Очевидно, що вказані держави роблять акцент на глобальних засобах подолання загроз в рамках європейського співтовариства. Означена модель, на наш погляд, не зовсім практична, адже відбувається зміщення акцентів з національного на наднаціональний рівень.

Правовим підґрунтям політики інформаційної безпеки Республіки Польща є низка законодавчих актів, які визначають напрями інформаційної політики, встановлюють технологічні стандарти інформаційного зв'язку, форми залучення іноземних інвестицій, ліцензування інформаційної діяльності. Для боротьби з інформаційними загрозами у Польщі залучають громадянське суспільство. Так, у 2017 році було створено Центр аналізу пропаганди і дезінформації, діяльність якого пов'язана з аналізом і пошуком системного підходу до ідентифікації та протидії російській дезінформації в польському інформаційному просторі [7, с. 515]. Зазначимо, що досвід Польщі дуже схожий з українським, однак його перевагою є активне залучення громадськості, напрацювання механізмів протидії пропаганді та стандартизація інформаційних послуг.

Стратегія забезпечення інформаційної безпеки Федеративної Республіки Німеччина зосереджується на десяти стратегічних напрямах: захист критично важливих інформаційних інфраструктур; захист ІТ-систем у Німеччині; посилення інформаційної безпеки в державному управлінні; створення національної ради з кібербезпеки; проведення ефективного контролю за злочинністю у кіберпросторі; проведення ефективних скоординованих дій для забезпечення інформаційної безпеки в Європі; використання надійних інформаційних технологій; розвиток персоналу у федеральних органах влади; захист особистої інформації громадян під час її обміну засобами електронної пошти [8, с. 35]. На нашу думку, означена стратегія поєднує два ключові напрями: національний та міжнародний. В рамках першого відбувається робота безпосередньо на рівні внутрішніх механізмів протидії інформаційним загрозам, а в рамках другого – співпраця та координація з європейськими інституціями.

Таким чином, досвід держав-членів ЄС у сфері забезпечення інформаційної безпеки може бути корисним для України. Зокрема, слід звернути увагу на такий аспект, як міжнародна співпраця в зазначеній сфері, оскільки він домінує в політиці більшості розвинених та

високотехнологічних країн ЄС. Також варто проаналізувати можливість попередження загроз інформаційній безпеці та активізації практики стандартизації інформаційних послуг. Імплементація позитивного досвіду має відбуватися на основі оцінки його адаптивності до національної правової системи.

Література:

1. Олефір І. В. Особливості забезпечення інформаційної безпеки у провідних країнах світу. *Регіональні студії*. 2018. № 12. С. 118–121.

2. Final Report – Study on cybersecurity in the energy sector of the Energy Community. Blueprint Energy Solutions GmbH. December 2019. URL: https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d90 45ef/Blueprint_cyber_122019.pdf (date of application: 16.01.2024).

3. Про кіберзлочинність: Конвенція Ради Європи від 23 листопада 2001 р. *Офіційний вісник України*. 2007. № 65. стор. 107. стаття 2535.

4. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28 січня 1981 р. *Офіційний вісник України*. 2011. № 1. стор. 1994. стаття 701.

5. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Директива Європейського парламенту і Ради ЄС 2016/1148від 06 липня 2016 р. *Офіційний вісник Європейського Союзу*. 2016. L. 194. стор. 1.

6. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн Східної Європи. *Інформація і право*. 2017. № 4. С. 62–72.

7. Сливка М. М., Лук'янова Г. Ю. Правове забезпечення інформаційної безпеки: досвід країн Європейського Союзу. *Юридичний науковий електронний журнал*. 2021. № 11. С. 514–516.

8. Чернухін І. О. Досвід Федеративної республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. *Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави*. 2014. № 1 (14). С. 27–43.