В'ячеслав КОРОТКИЙ
аспірант спеціальності міжнародні відносини,
суспільні комунікації та регіональні студії,
Волинський національний університет ім. Лесі Українки.

РОЛЬ ДЕРЖАВ-ЧЛЕНІВ ЄС У ЗАБЕЗПЕЧЕННІ СПІЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасному світі інформація стала однією з найцінніших ресурсів, а її захист - однією з ключових складових національної та міжнародної безпеки. Європейський Союз, як потужне політичне та економічне об'єднання, зіткнувся з численними викликами в інформаційному середовищі: кіберзагрози, дезінформація, втручання у виборчі процеси, гібридні атаки з боку авторитарних держав. У такій ситуації роль держав-членів ЄС у побудові спільної інформаційної безпеки є надзвичайно важливою.

У цьому есе буде розглянуто, як держави-члени ЄС беруть участь у формуванні спільної політики інформаційної безпеки, які механізми взаємодії існують між ними, які ініціативи реалізуються на рівні ЄС, і які виклики ще належить подолати.

Інформаційна безпека як спільний пріоритет ЄС.

Інформаційна безпека у Європейському Союзі охоплює широкий спектр питань: від боротьби з кіберзлочинністю до протидії дезінформації та захисту критичної інфраструктури. В умовах високої інтеграції держав-членів та цифрової трансформації, жодна з країн не може впоратися з цими викликами самостійно. Тому забезпечення інформаційної безпеки стало спільним пріоритетом у рамках політики цифрової Європи (Joint, 2020).

У 2020 році ЄС ухвалив нову Стратегію кібербезпеки, яка передбачає посилення співпраці між державами-членами, розвиток кіберрезильєнтності, створення спільного кіберщита (EU Cyber Shield) та підвищення кіберграмотності населення (Joint, 2020).

Ключова роль національних урядів у реалізації політики інформаційної безпеки.

Попри існування загальноєвропейських стратегій, відповідальність за реалізацію заходів у сфері інформаційної безпеки залишається за державами-членами. Вони зобов'язані адаптувати європейські норми до національного законодавства, створювати власні центри реагування на кіберінциденти (CSIRT), посилювати захист державних ІТ-систем, забезпечувати взаємодію з приватним сектором та громадянським суспільством (European, n.d).

Наприклад, Естонія, після масштабної кібератаки у 2007 році, стала піонером у сфері кібербезпеки в ЄС. Вона заснувала Центр передового досвіду з кібероборони НАТО у Таллінні (The NATO, n.d).

Франція активно працює над захистом свого кіберпростору через агентство ANSSI (Agence, n.d), а Німеччина створила кіберпідрозділи в межах Збройних сил (BSI, n.d.).

Механізми координації між державами-членами.

Однією з найбільших переваг ЄС є розгалужена система координації між країнами-членами. У сфері інформаційної безпеки вона включає такі ключові елементи:

- ENISA - координує національні зусилля, проводить навчання, видає технічні рекомендації та організовує регулярні кібернавчання (European, n.d);
- Мережа CSIRT - команди реагування на інциденти, які обмінюються інформацією про кібератаки;
- East StratCom Task Force - спеціальний підрозділ, що протидіє пропаганді, особливо з боку РФ (EU, n.d.);
- Digital Services Act - правова база, яка зобов'язує онлайн-платформи звітувати перед національними регуляторами (The Digital, 2022).

Завдяки цим інструментам держави-члени не лише мають змогу захищати себе, а й формувати ефективну загальноєвропейську відповідь на виклики цифрової епохи.

Спільна протидія дезінформації та гібридним загрозам

Одним із найнебезпечніших викликів для інформаційної безпеки ЄС є цілеспрямована дезінформація, яку використовують недружні держави для послаблення демократичних інституцій, розколу суспільств і втручання у внутрішні справи країн. Яскравим прикладом є масовані кампанії російської пропаганди проти ЄС та НАТО (EU, n.d.).

У відповідь держави-члени створюють національні центри стратегічних комунікацій, організовують кампанії з медіаграмотності, підтримують незалежні ЗМІ та розслідування впливових онлайн-мереж (Challenges, 2018).

Також у 2022 році було створено Європейський центр протидії гібридним загрозам, у якому країни-члени співпрацюють щодо виявлення, аналізу та нейтралізації інформаційних атак (Hybrid, n.d.).

Країни Балтії, Польща, Фінляндія, Чехія та Словаччина - серед найактивніших учасників цієї роботи. Польща координує заходи через Міністерство цифрових справ (Cybersecurity, n.d.).

Війна в Україні як каталізатор розвитку інформаційної безпеки в ЄС

Повномасштабне вторгнення РФ в Україну в 2022 році радикально змінило європейське уявлення про безпеку. Країни-члени ЄС усвідомили, що інформаційна безпека є частиною колективної оборони. Це призвело до активізації співпраці з НАТО в сфері кібербезпеки, створення аналітичних центрів з виявлення фейкових наративів, санкцій проти пропагандистських ресурсів (EU, (n.d.), а також підвищення інвестицій у кіберкомандування.

Висновки. Інформаційна безпека стала однією з найважливіших складових політики ЄС. Успішне її забезпечення неможливе без активної участі держав-членів. Вони відіграють вирішальну роль у втіленні стратегій, обміні даними, створенні національних структур кіберзахисту, протидії дезінформації та формуванні стійкого інформаційного середовища. Саме завдяки участі кожної з держав-членів вдається вибудувати ефективну систему колективного інформаційного захисту.

Список використаних джерел

Agence nationale de la sécurité des systèmes d'information (ANSSI). (n.d.). *ANSSI official website*. Retrieved from https://www.ssi.gouv.fr/en/

BSI. (n.d.). *German Federal Office for Information Security*. Retrieved from https://www.bsi.bund.de/EN

Challenges facing civil society organisations working on human rights in the EU. (2018). *European Union Agency for Fundamental Rights.* Retrieved from https://fra.europa.eu/en/publication/2018/challenges-facing-civil-society-organisations-working-human-rights-eu

Cybersecurity Department. (n.d.). *Ministry of Digital Affairs of Poland*. Retrieved from https://www.gov.pl/web/cyfryzacja

EU vs Disinfo. (n.d.). *East Stratcom Task Force*. Retrieved from https://euvsdisinfo.eu/

European Union Agency for Cybersecurity. (n.d.). *ENISA official website*. Retrieved from https://www.enisa.europa.eu/

Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade. (2020). *European Commission.* Retrieved from https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Hybrid CoE (n.d.). *Hybrid CoE official website*. Retrieved from https://www.hybridcoe.fi/

The Digital Services Act package. (2022). *European Commission*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. (n.d.). *CCDCOE official website.* Retrieved from https://ccdcoe.org/