4. The University of Baltimore. The economic cost of bad actors on the internet Fake News | 2019. Baltimore : CHEQ, 2019. 17 p. URL: https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf (date of access: 28.04.2024).

5. Онищенко С. В., Маслій О.А. Ризики та загрози в умовах цифровізації: безпековий аспект. II International Scientific Conference Development of Socio-Economic Systems in a Global Competitive Environment: Conference Proceedings, May 24th, 2019. Le Mans, France. P.54-56.

6. Onyshchenko S., Yanko A., Hlushko A., Maslii O., Cherviak A. Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association*. 2023. 29(5). pp. 818–835

УДК 316.774

Глушко Аліна Дмитрівна,
кандидат економічних наук, доцент
Корсакас Богдан Олексійович
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

СПІВПРАЦЯ УКРАЇНИ ТА ЄС У СФЕРІ КІБЕРБЕЗПЕКИ

У сучасному світі, де цифрові технології пронизають всі сфери життя, кібербезпека стає питанням національної безпеки. Україна, яка з 2014 року перебуває під постійною загрозою кібератак з боку рф, особливо зацікавлена у співпраці з Європейським Союзом для посилення кіберстійкості та захисту своїх інтересів у кіберпросторі. Зростання кіберзагроз, таких як APT-атаки, дезінформаційні кампанії та викрадення даних, робить співпрацю України та ЄС у цій сфері більш актуальною, ніж будь-коли [1]. Сьогодні Україна стоїть на передовій боротьби з агресією рф й у

кіберпросторі, і наша держава прагне ділитися досвідом з Європейським Союзом. Ефективні заходи запобігання кібератакам, посилення кіберстійкості та взаємодія з партнерами є ключовими інструментами. Зустріч із представниками ЄС є важливим кроком поглиблення співпраці та зміцнення обороноздатності обох сторін. Співпраця має на меті підвищення кіберстійкості, тобто спільними зусиллями сторони прагнуть зміцнити стійкість своїх кіберсистем до кібератак та інших кіберзагроз [2]. Кібератаки можуть завдати шкоди критичній інфраструктурі, такій як енергетика, транспорт та телекомунікації. Тим самим співпраця може бути спрямована на захист цих систем від кібернебезпек. Забезпечення безпеки громадян. Кібератаки можуть призвести до крадіжки особистих даних, фінансових втрат та інших негативних наслідків для громадян. Спільними зусиллями сторони прагнуть захистити своїх громадян від кіберзагроз. Кібербезпека є ключовим фактором для розвитку цифрової економіки. Співпраця сприяє створенню безпечного та сприятливого середовища для розвитку цифрових технологій [3].

Україна з ЄС може обмінюватись інформацією про кіберзагрози, методи їх виявлення та нейтралізації, а також про кращі практики кібербезпеки. Фахівці з кібербезпеки можуть брати участь у спільних навчаннях та тренінгах, де вони діляться досвідом та підвищують свою кваліфікацію. ЄС може надавати технічну допомогу у вигляді обладнання, програмного забезпечення та експертної підтримки для модернізації систем кібербезпеки. Сторони працюють над гармонізацією свого законодавства у сфері кібербезпеки, що полегшить співпрацю та обмін інформацією [4, 5]. Спільні дослідження та розробки в сфері кібербезпеки сприяють розробці нових методів та технологій для протистояння кіберзагрозам.

Це історичні кроки для нашої держави, та, безумовно, важливі кроки на шляху вступу України до Європейського Союзу. Співпраця з Європейським агентством з кібербезпеки (ENISA) відкриває нові можливості для зміцнення взаємодії у сфері кібербезпеки та обміну найкращими практиками з країнами ЄС [6]. Це особливо важливо зараз, коли Україна знаходиться на передовій світової кібервійни, яку веде рф. Об'єднання зусиль укріпить європейську систему кібербезпеки, а Україна братиме участь у формуванні стратегічних підходів та виробленні нових політик у сфері кібербезпеки та кібероборони на міжнародному рівні. Національний координаційний центр кібербезпеки (НКЦК) при РНБО України та Адміністрація Державної служби спецзв'язку та захисту інформації України (ДССЗЗІ) уклали Угоду про співпрацю з Агентством Європейського Союзу із мережевої та інформаційної безпеки (ENISA), спрямовану на розбудову спроможностей, обмін найкращими практиками та підвищення рівня обізнаності щодо ситуації в кібербезпеці [7]. Ця угода включає як короткострокові структуровані заходи співпраці, так і відкриває шлях до довгострокового узгодження політики кібербезпеки та підходів до її реалізації.

За посередництвом Європейського фонду миру, Європейський Союз підтримує зміцнення кібербезпекового потенціалу Збройних сил України. ЄС профінансував створення кіберлабораторії та кіберкласу, виділивши на цей проєкт 3 мільйони євро [8]. Кіберлабораторія – це онлайн середовище для навчання, проведення тренінгів і досліджень. Технологія кіберлабораторії дає змогу користувачеві створювати реалістичне, переконливе та достовірне віртуальне середовище для відпрацювання належної й своєчасної відрповіді на кібератаки, що передбачає реагування слухачів на симуляції кібератак і захисту в режимі реального часу. У змодельованому середовищі військовослужбовці Збройних сил України мають змогу навчитися краще долати

високий рівень стресу, виявляти й досліджувати вразливості в різних мережевих системах. Кіберклас надає 15 робочих місць і обладнання, потрібне для проведення навчання та виконання вправ із кіберзахисту. У межах проєкту було закуплено, встановлено та налаштовано програмне й апаратне забезпечення системи безпеки для Збройних сил України, а також проведено фахове навчання. Упродовж останніх двох років проєкт очолює Академія електронного управління (eGA). Запуск кіберлабораторії та навчання з кібербезпеки було реалізовано в співпраці з компанією CybExer Technologies.

Таким чином, співпраця України з Європейським Союзом у сфері кібербезпеки набуває виняткової уваги в сучасних умовах, адже вона дає змогу не лише захистити цифрові системи та інфраструктуру обох сторін, але й сприяє євроінтеграції України та зміцнює загальну кібербезпеку в Європі.

Література

1. Маслій О. А., Максименко А. П. Ризики та загрози економічній безпеці України у цифровій сфері в умовах війни. *Ринкова економіка: сучасна теорія і практика управління*, 2023. Том 21 № 3(52). С. 179–199. https://doi.org/10.18524/2413-9998.2022.3(52).275802

2. Україна та ЄС про підписання угоди у сфері кібербезпеки URL: https://armyinform.com.ua/2023/11/13/ukrayina-ta-yes-pidpysaly-ugodu-v-sferi-kiberbezpeky/

3. Україна та Європейський Союз про зміцнення співпраці в боротьбі з кіберагресією URL: https://cip.gov.ua/ua/news/ukrayina-ta-yevropeiskii-soyuz-zmicnyuyut-spivpracyu-v-borotbi-z-kiberagresiyeyu

4. Glushko A.D., Yanko A.S. Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. *Economics and Region*. 2019. № 4 (75). P. 20–28.

5. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V. (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations, 791–803. doi: https://doi.org/ 10.1007/978-3-031-17385-1_67

6. Державна служба з питань звязку та інформатизації України URL: https://cip.gov.ua/ua

7. Національний координаційний центр з кібербезпеки України URL: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky

8. Представництво Європейського Союзу в Україні URL: https://www.eeas.europa.eu/delegations/ukraine_uk?s=232

УДК 657.1.012

Жукова Анжеліка Андріївна,
Слинько Ярослава Володимирівна, *студентки,*
Науковий керівник: Коба Олена Вікторівна,
кандидат технічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

ДІДЖИТАЛІЗАЦІЯ ОБЛІКУ: ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ

У сучасному світі, де технології швидко розвиваються, застосування цифрових рішень у галузі обліку стає все більш важливим і вигідним. Діджиталізація обліку включає в себе використання комп'ютерних програм, хмарних технологій та інших інноваційних інструментів для автоматизації та оптимізації процесів обліку.

До основних тенденцій діджиталізації можна віднести хмарні технології, автоматизацію процесів та галузь кібербезпеки [1]. Розглянемо кожну з них більш детально.