УДК 342.951

МАНУІЛОВ Я.С., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: https://orcid.org/0000-0001-8149-2745

ЄВРОПЕЙСЬКИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334153

Анотація. *У статті висвітлюється європейський досвід забезпечення кібербезпеки. Аналізуються ключові тенденції і події, які визначають політику ЄС у сфері забезпечення кібербезпеки. Розглянуто основні нормативні акти ЄС у цій сфері. Звертається увага на європейський досвід застосування режиму "кіберсанкцій". Висвітлені нові стандарти кібербезпеки, які є обов'язковими до виконання на всій території ЄС. Підкреслюється, що застосування найсучасніших технологій штучного інтелекту може кардинально поліпшити роботу команд з кібербезпеки, підвищуючи їх ефективність і зменшуючи існуючі кіберризики. Зроблено висновок, що для досягнення стратегічних цілей у сфері кібербезпеки Україна має посилити спроможності у протидії кіберзлочинності шляхом проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі.*

Ключові слова: *європейський досвід, ЄС, протидія, кібербезпека, кіберзлочинність, кіберстійкість.*

Summary. *The article highlights the European experience in cybersecurity. It analyzes key trends and events that determine the EU policy in the field of cybersecurity. It examines the main EU regulatory acts in this area. It analyzes the European experience in applying the "cyber sanctions" regime. It highlights new cybersecurity standards that are mandatory across the EU. It highlights how the use of cutting-edge artificial intelligence technologies can dramatically improve the work of cybersecurity teams, increasing their efficiency and reducing cyber risks. It is concluded that to achieve strategic goals in the field of cybersecurity, Ukraine must strengthen its capabilities in countering cybercrime by conducting joint measures with the EU aimed at increasing resilience in cyberspace.*

Keywords: *European experience, EU, countering, cybersecurity, cybercrime, cyber resilience.*

Постановка проблеми. Кібербезпека є важливим пріоритетом для України. Сучасні інформаційні та кібертехнології відкривають безмежні можливості, але водночас створюють складні виклики та загрози [1]. Кіберпростір давно визнано одним із можливих театрів воєнних дій. Враховуючи сучасні виклики і тенденції у сфері кібербезпеки, для забезпечення кібербезпеки України доцільно активно використовувати кращі практики з цих питань держав-членів ЄС. У Стратегії кібербезпеки України вказується, що Україна у сфері кібербезпеки має забезпечити поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі [2]. За словами Секретаря РНБО О. Литвиненка: "Надзвичайно важливо зміцнювати кіберстійкість – здатність інформаційних систем функціонувати у складних і надскладних безпекових умовах, відновлювати свої ресурси навіть за умов їхньої обмеженості та активної протидії з боку

ворога” [1]. Він підкреслив важливість поглиблення міжнародної співпраці у цій сфері. Співпраця нашої держави з ЄС є важливим кроком у формуванні сильної кіберспільноти та розбудові екосистеми української і міжнародної кібербезпеки. Наведене свідчить про важливість дослідження європейського досвіду у сфері забезпечення кібербезпеки.

Результати аналізу наукових публікацій. Досвід ЄС у сфері забезпечення кібербезпеки став предметом поглибленого дослідження у роботах Д. Антонюка [3], М. Багве, О. Кузнєцова [4], Т. Сліпченко, О. Федієнка [5], Р. Лук’янчука та ін. Співпраця України та ЄС у сфері кібербезпеки висвітлювалася у працях Я. Костюченка [6].

Довгострокова підтримка ЄС та посилення ролі України як регіонального лідера в сфері кібербезпеки є предметом постійних Міжнародних форумів кіберстійкості, які відбуваються в Україні [1].

Ключові тенденції і події протягом 2023 – 2024 рр. висвітлені у Річному аналітичному огляді, підготовленому за підтримки Агентства США з міжнародного розвитку в рамках Проєкту USAID “Кібербезпека критично важливої інфраструктури України” [7].

Водночас, у зв’язку з появою нових гібридних загроз інформаційного характеру, бурхливим розвитком інформаційних технологій, пов’язаних з штучним інтелектом (далі ШІ), останнім часом відбулися істотні зміни у політиці ЄС у сфері кібербезпеки, які потребують подальших досліджень.

Метою статті є аналіз кращих практик ЄС у сфері забезпечення кібербезпеки в контексті поглиблення євроінтеграційних процесів України.

Виклад основного матеріалу. РФ продукує гібридні загрози не тільки для України, але й для інших країн світу, у т.ч. для ЄС. У зв’язку з цим ЄС вживає активні заходи для запобігання цим загрозам в інформаційному просторі. У міру того, як кіберзагрози стають дедалі агресивнішими, а нападники – більш технологічними, досягнення спільного високого рівня кібербезпеки серед установ Європейського Союзу є обов’язковою умовою для забезпечення відкритої, ефективної, безпечної та сталої роботи керівних органів ЄС [8].

Проблема протидії кіберзагрозам давно перебуває у фокусі європейського співтовариства. Перша згадка про суспільно небезпечні прояви кіберзагроз міститься у Будапештській конвенції про кіберзлочинність (2001), яка визначила перелік кіберзлочинів (несанкціонований доступ, перехоплення даних, втручання в роботу системи тощо) та зобов’язала держав-членів криміналізувати їх прояви у національному законодавстві. Ця Концепція є правовою основою для співпраці правоохоронних органів різних країн: спрощення видачі кіберзлочинців, спільні розслідування, обмін електронними доказами[9]. Нині на території європейських держав реалізується проект CyberEast+ (2024–2027) – спільна ініціатива ЄС та Ради Європи, яка сприяє вдосконаленню в Україні політики та законодавства проти кіберзлочинності згідно з вимогами Конвенції [10]. Це підтверджує важливе значення Будапештської конвенції як “золотого стандарту” кібербезпеки, яка залишається базовою основою для протидії кіберзагрозам [6].

Прийнята ще в 2013 році перша Стратегія кібербезпеки ЄС визначала стратегічні цілі та конкретні дії для досягнення кіберстійкості, зменшення кіберзлочинності, розробки можливостей кіберзахисту, розвитку технологічних ресурсів та встановлення послідовної міжнародної політики щодо кіберпростору для ЄС [11].

Ключовим нормативним актом ЄС у сфері протидії кіберзлочинності стала Директива ЄС 2013/40/EU щодо атаки на інформаційні системи [12], яка зобов’язала

країни ЄС запровадити мінімальні стандарти криміналізації кібератак та уніфікувати відповідальність за них. Поряд з основними кримінальними правопорушеннями, пов'язаними з кібератаками, ця Директива запровадила нові склади кримінальних правопорушень – виготовлення чи розповсюдження інструментів для несанкціонованого втручання, встановивши мінімальні та максимальні санкції за такі порушення та механізми обміну інформацією та статистичними даними про кіберінциденти [6]. Для координації транснаціональних операцій діє спільна слідча група J-CAT (Joint Cybercrime Action Taskforce) [13], до складу якої входять представники кіберполіції різних країн під егідою Європи [6].

Однією з основ нормативно-правової бази ЄС стала ухвалена у 2016 році Директива 2016/1148 про безпеку мережевих та інформаційних систем(NIS Directive) [14], яка запровадила нову культуру кібербезпеки в ЄС. Саме нова кіберкультура визначає революційний розвиток кібертехнологій, підтримує і полегшує стратегічне співробітництво і обмін інформацією між державами-членами ЄС. Завдяки цій Директиві держави-члени ЄС обмінюються інформацією про кіберінциденти, а також кращими практиками у сфері боротьби з кіберзлочинністю [15].

У тому ж році була презентована Глобальна стратегія зовнішньої політики та політики безпеки ЄС. У розділі "Кібербезпека" цієї Стратегії зазначається, що стратегічною метою для Євросоюзу залишається посилення інституційних спроможностей інституцій ЄС та держав-членів у протидії кіберзагрозам, при цьому має зберігатися відкритий, вільний та безпечний кіберпростір [11].

Водночас Європейська комісія прийняла Пакет з кібербезпеки, покликаний забезпечити досягнення кількох цілей: здійснити заходи для забезпечення кіберстійкості, розробити механізм кіберстримування та кібероборони [11]. При цьому наголошується на важливості удосконалення механізмів кримінальної відповідальності за кіберзлочини, що має спонукати розвиток міжнародної співпраці між державами ЄС.

У 2018 році Європейський парламент увалив резолюцію "Боротьба з кіберзлочинами", в якій зазначається, що Росія і Китай через державні та недержавні інституції займаються плануванням та реалізацією кібератак на критичну інфраструктуру держав-членів ЄС [11]. Сьогодні країни по всьому світу уважно спостерігають за цими змінами у динаміці кіберпротистояння і змінюють власну політику щодо посилення своїх військових кіберпідрозділів. Так, керівництво ЄС розпочало обговорення створення європейських кіберсил, що будуть мати наступальні можливості. Німеччина планує створити окремий рід військ – кіберсили для того, щоб швидше реагувати на нові загрози та посилити свою кібероборону [7].

У травні 2019 року Рада ЄС ухвалила рішення про запровадження обмежувальних заходів проти осіб та організацій, які здійснюють кібератаки [11]. Таким чином, народився новий санкційний режим, який вперше запрацював у 2020 році, коли кіберсанкції було накладено на 8 фізичних та 4 юридичних осіб з РФ, КНР та Північної Кореї. Режим кіберсанкцій являє собою дію правових рамок адресних обмежувальних заходів проти особи або установ, які залучалися до скоєння кібернетичних атак, що завдали значної шкоди та представляють зовнішню загрозу для ЄС або його держав-членів, а кінцевою метою запровадження цих заходів є стримування та реагування на кібернетичні атаки, при цьому санкції можуть включати заборону на подорожі до держав ЄС, заморожування фінансових активів осіб та установ [4, с.110].

З метою захисту критичної інфраструктури, комунікацій, державних інформаційних ресурсів, гарантуючи безпеку онлайн-суспільства та економіки, ЄС 15 вересня 2022 року було ухвалено Закон ЄС про кіберстійкість (The Cyber Resilience Act

(CRA) [16], який передбачає законодавче забезпечення покращення стану кібербезпеки за допомогою удосконалення відповідних стандартів, що передбачає створення на теренах ЄС нової європейської кібер-екосистеми, яка буде більш безпечною для усіх громадян незалежно від того, наскільки вони освічені у питаннях цифрової безпеки[5].

7 січня 2024 року у Євросоюзі набули чинності нові регуляторні правила, що мають на меті підвищити кібербезпеку європейських організацій, установ та інституцій[8]. Ці правила встановлюють нові норми внутрішнього менеджменту для ризиків у сфері кібербезпеки, управління та контролю для кожного суб'єкта ЄС, а також передбачають запровадження Міжвідомчої ради з кібербезпеки (IICB) для здійснення моніторингу їх виконання та сприяння у їх імплементації[8]. Нові правила також містять додаткові повноваження груп з надзвичайного реагування для інституцій, установ, офісів та агенцій ЄС (CERT-EU). Зокрема, це стосується додаткових можливостей із проведення оцінки загроз, створення координаційного штабу для обміну інформацією та реагування на інциденти. Інституції та установи ЄС у терміни, визначені в регуляторних правилах, зобов'язані організувати процеси з внутрішньої кібербезпеки та проводити оцінку наявних ризиків, а Міжвідомча рада з кібербезпеки (IICB) надаватиме їм допомогу у цій роботі та здійснюватиме контроль за дотриманням нових правил [8].

У квітні 2024 року Європарламент ухвалив Акт про кіберсолідарність, який має на меті не тільки зміцнити загальні можливості ЄС щодо виявлення, ситуаційної обізнаності та реагування, але й фокусується на двох важливих аспектах: створення кіберрезерву на рівні ЄС (через інструменти залучення допомоги від надійних приватних постачальників); впровадження інструментів тестування безпеки ОКІ[6]. Акт кібернетичної солідарності ЄС передбачає координацію між державами-членами за трьома головними напрямками: створення європейської системи раннього попередження; створення так званого надзвичайного кібернетичного механізму; резерв кібернетичної безпеки, який надаватиме резервні послуги в разі серйозних порушень, на запит держав-членів, євроінституцій, або асоційованих третіх країн[17]. Ці напрямки багато в чому пов'язані із рефлексією ЄС щодо українського досвіду ведення кібервійни.

В жовтні 2024 року Європейський Союз прийняв Акт про кіберстійкість (Cyber Resilience Act), який створює нові рамки функціонування для IT сектору та виробників IT обладнання, вимагаючи від них більше уваги до заходів кібербезпеки. Очікується, що імплементація цього акта буде складною й такою, що буде відбуватись з різною швидкістю в європейських країнах, оскільки більшість новацій є реакцією на зміни у ландшафті кіберзагроз, з яким стикається ЄС [6].

Також внесені Актом про кіберстійкість зміни кореспондуються із довгостроковими оцінками кіберзагроз, які регулярно оприлюднює Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (далі ENISA).

Оприлюднений ENISA у березні 2024 року Звіт "Передбачення загроз кібербезпеці до 2030 року" якраз вказує на загрози ланцюжкам поставок, застарілу цифрову інфраструктуру, що може піддаватись додатковим кіберризикам та загрозам з боку нецільового використання ШІ [6].

Намагаючись створити більш гнучкі механізми реагування на інциденти, у травні 2024 року Європейська Рада схвалила Керівні настанови, що сприятимуть створенню гібридних груп швидкого реагування. Такі групи потрібні для підготовки та протидії гібридним загрозам і кампаніям впливу у сьогоднішньому світі. Вони будуть орієнтовані на протидію дезінформації, кібератакам, атакам на критичну інфраструктуру тощо. Гібридні групи мають стати одним із ключових інструментів для підтримки держав-

членів ЄС і країн-партнерів у протидії гібридним загрозам у рамках EU Hybrid Toolbox [6].

12 липня 2024 року набув чинності ключовий регуляторний документ ЄС у сфері штучного інтелекту (ШІ) – Акт про Штучний Інтелект (Artificial Intelligence Act), зміст якого охоплює, зокрема, тематику кібербезпеки. Остання висвітлюється в контексті використання перевірених наборів даних, можливих атак на легітимний ШІ, метою яких є невиведення системи з ладу, а наповнення її "отруєними" наборами даних. Відповідно цей Акт вимагає, щоб розроблені алгоритми ШІ були кіберстійкими, належно захищеними, а ключовим органом з кібербезпеки ШІ стане ENISA [6].

З 18 жовтня 2024 року набула чинності нова директива ЄС із кібербезпеки — Директива NIS 2 "Мережева та інформаційна безпека" (далі Директива NIS 2) [18], яка встановлює стандарти кібербезпеки на всій території Європейського Союзу і змушує компанії з різних секторів документувати свою стратегію безпеки. За допомогою цієї Директиви ЄС запровадив суворі правила кібербезпеки для своїх держав-членів. Ця Директива є вдосконаленою версією Директиви NIS 2016 року [14], яка вже покликана забезпечити високий рівень безпеки мережевих та інформаційних систем в Європейському Союзі, але мала деякі недоліки. На відміну від попередньої Директиви NIS 2016 року нова Директива NIS 2: охоплює більше секторів і компаній, які мають важливе значення для суспільства й економіки, тобто таких галузей, як енергетика, охорона здоров'я, транспорт і цифрова інфраструктура; вимагає від відповідних компаній і організацій здійснювати ефективне управління ризиками й повідомляти про серйозні або значні кіберінциденти компетентним державним органам для вжиття необхідних заходів; передбачає більш жорсткі санкції для держав-членів, які можуть становити до 20 мільйонів євро або чотирьох відсотків світового обороту, якщо відповідні компанії та організації не впроваджують необхідних заходів безпеки або не повідомляють про серйозні або значні кіберінциденти компетентним державним органам; підкреслює особисту відповідальність керівництва за кібербезпеку й передбачає, що виконавчі віце-президенти компаній будуть нести відповідальність своїми особистими активами у разі недотримання вимог законодавства [19]. Держави-члени ЄС повинні вжити необхідних заходів для дотримання Директиви NIS й застосовувати ці заходи з 18 жовтня 2024 року.

Заслуговує на окрему увагу внесена у лютому 2025 року Єврокомісією пропозиція щодо забезпечення дієвої та ефективної реакції на масштабні кіберінциденти. Запропонований Єврокомісією план оновлює комплексну структуру ЄС для управління кризою в сфері кібербезпеки та відображає відповідних учасників ЄС, окреслюючи їхні ролі протягом усього життєвого циклу кризи. Це включає готовність і спільну обізнаність про ситуацію для передбачення кіберінцидентів, а також необхідні можливості виявлення для їх ідентифікації, включаючи інструменти реагування та відновлення, необхідні для пом'якшення, стримування та стримування цих інцидентів[20]. Запропонований план базується на існуючих інструментах, таких як комплексне реагування на політичну кризу, План критичної інфраструктури і мережевий кодекс щодо кібербезпеки для електроенергетики ЄС [21]. Запропонований план містить заходи для зміцнення співпраці між цивільними та військовими структурами, включаючи НАТО, одночасно відображаючи цілі майбутньої стратегії готовності ЄС.

З цього приводу виконавчий віце-президент із технічного суверенітету, безпеки та демократії Єврокомісії Х.Віркунен зауважила: "Запропонований план кібербезпеки відображає наше прагнення забезпечити скоординований підхід, використовуючи

існуючі структури для захисту внутрішнього ринку та підтримки життєво важливих суспільних функцій. Це Рекомендація є важливим кроком у зміцненні нашої спільної кіберстійкості" [21].

Основним концептуальним документом в ЄС, який регулює сферу кіберзахисту, залишається оновлена Стратегія кібербезпеки на 2021 – 2027 роки, яка передбачає: використання регуляторних та інвестиційних механізмів, політичних ініціатив за такими напрямами: забезпечення стабільності, технологічного суверенітету та лідерства; здатність попереджувати, стримувати та адекватно реагувати на кібератаки; розвиток міжнародного співробітництва з метою формування глобального та відкритого кіберпростору; запровадження механізму "кіберсанкцій" [4].

З огляду на появу нових інформаційних загроз набувають розповсюдження квантові технології. Так, в січні 2024 року, НАТО прийняло свою першу квантову стратегію, а ЄС готується до впровадження постквантової криптографії для запобігання появі нових кіберзагроз [6]. Єврокомісія вже випустила рекомендації для держав-членів, які вказують на необхідність розробки відповідних дорожніх карт для цього переходу.

Нещодавно стало відомо, що Європейська комісія виділить 1,3 млрд євро на розгортання критично важливих технологій, які є стратегічно важливими для майбутнього Європи та технологічного суверенітету континенту. Йдеться про впровадження штучного інтелекту (ШІ) та його використання бізнесом і державним управлінням, у хмарних технологіях і даних, кіберстійкості та цифрових навичках[22]. Також пріоритетами залишається розвиток потенціалу освітніх і навчальних закладів ЄС у сфері цифрових навичок; сприяння створенню нової архітектури цифрового гаманця ЄС та Європейської інфраструктури довіри, а також сприяння її впровадженню в державах-членах; стимулювання трансформації державного сектору шляхом розвитку ефективних, високоякісних, інтероперабельних цифрових державних послуг [22]. Інновації також прискорюються завдяки використанню технологій ШІ. До речі, нещодавно уряд Швеції запропонував надати дозвіл поліції використовувати технологію розпізнавання обличчя за допомогою штучного інтелекту в режимі реального часу для боротьби зі злочинністю.

Але зусилля, спрямовані на посилення кібербезпеки критичної інфраструктури, включаючи готовність Брюсселю інвестувати в кібербезпеку, слабко корелюються з реальною ситуацією в цій сфері[6]. Звіт ENISA у листопаді 2023 року чітко вказує на те, що хоча кіберчастка ІТ-бюджету ОКІ досягла 7,1% у 2022 році, однак це лише на 0,4% більше ніж у 2021. Крім того, 47% об'єктів критичної інфраструктури не планують наймати фахівців з кібербезпеки протягом наступних двох років, а 83% організацій стверджують, що мають труднощі з наймом принаймні в одній сфері інформаційної безпеки [6].

Враховуючи ці тенденції та загальний характер нормативних змін, до яких вдається ЄС останнім часом, можна передбачити, що європейське законодавство у сфері кібербезпеки буде ставати дедалі більш жорстким та ультимативним, а його порушення буде вести до значних штрафів для компаній. Брак готовності європейських стейкхолдерів витрачати кошти на кібербезпеку змушує ЄС вдаватись до двох стратегій: посилення регуляції та запровадження інструментів фінансової підтримки [6]. Наприклад, у серпні 2024 року оприлюднено нову програму, спрямовану на підвищення рівня кіберзахисту в ЄС, у рамках якої оголошено конкурс для європейських постачальників послуг кібербезпеки, які бажають долучитися до надання послуг країнам ЄС та їхнім об'єктам критичної інфраструктури відповідно до Директиви NIS2. Ця

програма реалізується в межах Програми цифрової Європи (DEP), для реалізації якої планується використати 28,3 млн євро.

Як ми бачимо, ЄС має значний досвід у протидії кіберзлочинності. Для досягнення стратегічних цілей у сфері кібербезпеки Україна має посилити спроможності у протидії кіберзлочинності шляхом проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози [1]. Пунктом 9 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженим розпорядженням Кабінету Міністрів України від 07.03.2025 року №204, передбачено здійснення спільних із державами- членами ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність і реагувати на кіберзагрози [23].

Висновки. Сьогодні європейські країни уважно спостерігають за змінами у динаміці кіберпротистояння РФ, Китаю і США, корегуючи власну інформаційну політику щодо посилення потенціалу кіберстійкості своїх держав. Прийняті останнім часом нормативно-правові акти ЄС з питань запровадження єдиних євростандартів сприяють ефективному співробітництву між європейськими правоохоронними органами у протидії кіберзлочинам. З метою посилення протидії кіберзагрозам стають більш суворими правила кібербезпеки для всіх держав-членів ЄС, недодержання яких тягне відповідальність винних посадових осіб. Отже, законодавство ЄС стає дедалі більш жорстким, а санкції за порушення правил кібербезпеки закономірно посилюються. З огляду на інтеграцію штучного інтелекту (ШІ) з кібератаками, що підвищує їхню небезпеку, слід визнати плідним європейський підхід на випереджання у сфері кібербезпеки із застосовуванням найсучасніших технологій ШІ, які можуть кардинально покращити роботу команд з кібербезпеки, підвищуючи їх ефективність і зменшуючи кіберризики. З огляду на появу нових гібридних загроз в ЄС, набувають поширення квантові технології протидії кібератакам, які надають можливості для аналітики даних, комунікацій і підвищення операційної ефективності.

Використана література

1. Довгострокова підтримка ЄС та посилення ролі України як регіонального лідера в сфері кібербезпеки: В Києві відбувся Міжнародний форум кіберстійкості 2025. URL:https://www.rnbo.gov.ua/ua/Diialnist/7142.html

2. Стратегія кібербезпеки України: затв. Указом Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

3. Antonyuk, D. The EU imposed sanctions against Russian intelligence officers for cyberattacks against Estonia. URL: https://therecord.media/eu-sanctions-gru-personnel-cyberattack-estonia

4. Кузнєцов О.М. Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. *Інформація і право*. 2021. №1(36). № 2(49). С.106-113.

5. Федієнко О.П. Европейський досвід законодавчого забезпечення посилення кіберстійкості. *Інформація і право*. 2024. № 2(49). С. 178-189.

6. Костюченко Я.М. Співпраця України та ЄС у сфері кібербезпеки: механізми боротьби з кіберзлочинністю URL https://reicst.com.ua/pmtl/article/view/2025-15-01-10/2025-15-01-10.

7. Річний аналітичний огляд. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf?fbclid=IwY2xjawI-fZRleHRuA2FlbQIxMAABHcaZdkgcVIlSJ0eGnBO78x5xRCDcoBwcJ1GKrT4SAVS5reEAtY5u8ssd4w_aem_0xN1oMO3-toIy6vpuA27mA

8. У ЄС набули чинності нові правила кібербезпеки URL: https://www.ukrinform.ua/rubric-technology/3810785-u-es-nabuli-cinnosti-novi-pravila-kiberbezpeki.html.

9. Convention on Cybercrime (ETS No. 185). Budapest 23/11/2001. Council of Europe. Treaty Office. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

10. CyberEast+ (2025). Council of Europe Portal. URL: https://www.coe.int/en/web/cybercrime/cybereast-

11. Кіберстійкість: як досвід ЄС може допомогти Україні. URL: https://www.eurointegration.com.ua/articles/2021/06/11/7124258/

12. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Document 32013L0040. EUR-Lex home. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng

13. International cooperation led to the elimination of a ransomware group in Ukraine against the backdrop of the ongoing war (2024). Europol. URL: https://www.europol.europa.eu/media-press/newsroom/news/international-collaboration-leads-to-dismantlement-of-ransomware-group-in-ukraine-amidst-ongoing-war#:~:text=International%20collaboration%20leads%20to%20dismantlement,apprehend%20in%20Ukraine%20key%20figures

14. Директива Європейського Парламенту (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.

15. Боєр Є. Забезпечення кібербезпеки в європейському союзі: підхід європейської комісії URL:https://ekhnuir.karazin.ua/server/api/core/bitstreams/be158e67-b75b-4bae-aec5-559af490368f/content#:~:text.

16. The Cyber Resilience Act (CRA) 15.09.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454.

17. У ЄС погодили Акт кібернетичної солідарності для боротьби із зовнішніми впливами: для чого це рішення https://rubryka.com/2024/03/07/akt-kibernetychnoyi-solidarnosti/

18. 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) (Text with EEA relevance) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

19. Що таке Директива NIS2? Пояснення правил відповідності URL: https://hideez.com/uk-ua/blogs/news/what-is-nis2.

20. Комісія запускає новий план кібербезпеки для покращення координації ЄС у сфері кіберкризи URL:https://uk.eureporter.co/defence/cyber-security/2025/02/26/commission-launches-new-cybersecurity-blueprint-to-enhance-eu-cyber-crisis-co-ordination/.

21. Єврокомісія інвестує 1,3 млрд євро у штучний інтелект і кібербезпеку. URL: https://www.eurointegration.com.ua/news/2025/03/28/7208270/#:~:text.

22. BDO аналізує кібербезпеку 2025: Головні загрози та вплив новітніх технологій. URL: https://eba.com.ua/bdo-analizuye-kiberbezpeku-2025-golovni-zagrozy-ta-vplyv-novitnih-tehnologij/.

23. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 1 лютого 2022 р. № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~