DOI: https://doi.org/10.26642/jen-2024-2(108)-198-203
УДК 004.056.5:339.924(477)

С.О. Савчук, здобувач
Державний університет «Житомирська політехніка»

Виклики та можливості інтеграції України в систему кібербезпеки ЄС

(Представлено: д.е.н., д.держ.упр., проф. Грицишен Д.О.)

У статті висвітлено ключові аспекти розвитку системи кіберзахисту в Європейському Союзі та його значення для стійкості електронної комерції та комунальних структур. Розглянуто директиви NIS і NIS2, які встановлюють стандарти щодо норм кібербезпеки, а також Закон про кібербезпеку, який визначає процеси сертифікації IT-товарів і послуг. Визначено функції спеціалізованих європейських органів, таких як ENISA, CERT-EU та EU-CyCLONE, щодо організації реагування на протидію кіберзагрозам, методам посилення міжнародної співпраці та обміну розвідданими. В статті представлено скориговану структуру механізму цифрового захисту національної держави, яка об'єднала принципи, характерні для європейського режиму утвердження цифрових гарантій. Запропонована модель передбачає унікальні обов'язки органів державного управління, які розроблені відповідно до запропонованої в статті стратегії та сприяють як найму експертів, так і державно-приватній співпраці. Результатом втілення моделі є зміцнення критичної інфраструктури, підвищення рівня реагування на надзвичайні ситуації та надання національного характеру. В статті наголошується на важливості європейської інтеграції України в контексті зміцненні захисту від сучасних кібернебезпек і збереженні довіри в кіберсередовищі. Отримані висновки та поради можуть слугувати основою для продовження вивчення та практичного розгортання структури кібербезпеки, яка б узгоджувалася з національними та міжнародними протоколами.

Ключові слова: *державне управління; інтеграція; кіберзагрози; кібербезпека; критична інфраструктура; сертифікація.*

Постановка проблеми. Директива NIS2 є ключовим кроком до створення гармонізованого та стійкого середовища кібербезпеки в ЄС. Вимагаючи створення добре забезпечених ресурсами та спроможних органів з управління кіберкризами, директива гарантує, що держави-члени спроможні реагувати на складні сучасні кіберзагрози. Ці органи відіграватимуть вирішальну роль у захисті цифрової інфраструктури та сприянні безпеці та стабільності цифрової економіки та суспільства ЄС. Для ефективного виконання своїх завдань Директива вимагає, щоб ці органи державного управління з кібербезпеки були забезпечені відповідними ресурсами. Підхід стосується не лише фінансових ресурсів, а й доступу до передових технологій, кваліфікованого персоналу та операційної підтримки. Адекватне забезпечення ресурсами має вирішальне значення для того, щоб органи могли підтримувати ситуаційну обізнаність, керувати звітністю про інциденти та координувати заходи реагування в широкому діапазоні секторів, враховуючи критичну інфраструктуру, державне управління та постачальників цифрових послуг. Очікується, що органи управління кіберкризою працюватимуть у більш широких європейських межах. Їм доручено робити внесок у загальноєвропейські ініціативи, такі як Європейський кіберщит і Мережа організацій зв'язку з кіберкризами (CyCLONe). Інтегруючи свої зусилля з цими транснаціональними механізмами, орагни влади посилюють колективну стійкість Союзу проти кіберзагроз. Інтеграція включає обмін розвідувальними даними про загрози, участь у спільних навчаннях і узгодження національних протоколів зі стандартами ЄС.

На додаток до своїх оперативних функцій органи влади відіграють ключову роль у впровадженні та забезпеченні політики кіберзахисту. Вони контролюють застосування правил кібербезпеки в межах своєї юрисдикції, забезпечуючи дотримання організаціями вимог щодо управління ризиками та звітування про інциденти. Подвійна роль як координатора та виконавця покладає на ці організації значну відповідальність за досягнення балансу між проактивною підтримкою та регулятивним наглядом.

Серед проблем у створенні органів управління кіберкризою є те, що держави-члени повинні усунути розбіжності в можливостях, ресурсах і досвіді в різних регіонах. Забезпечення узгоджених стандартів і зміцнення довіри між заінтересованими сторонами є важливими для ефективного функціонування органів влади. Динамічний характер кіберзагроз вимагає постійної адаптації, інновацій та нарощування потенціалу в цих організаціях.

Метою статті є аналіз сучасної системи кібербезпеки Європейського Союзу, вивчення її ключових нормативно-правових актів, механізмів координації та інституційної структури, а також розробка адаптованої моделі інтеграції України в європейську екосистему кіберзахисту.

Аналіз останніх досліджень та публікацій. Дослідження кібербезпеки в Європейському Союзі привертає значну увагу науковців. Українські дослідники, такі як В.Бойко, М.Василенко,

С.Кухаренко [17] та інші, аналізують вплив європейських директив на національне законодавство України, підкреслюючи важливість гармонізації стандартів. Інші автори, зокрема Р.Муді [5], Л.Стрельцов [15], Л.Керулус [4] і Е.Грінберг [12], розглядають кібербезпеку в глобальному та регіональному контекстах, акцентуючи увагу на сучасних викликах, таких як кібервійна та вплив транснаціональних загроз. Дослідження свідчать, що ефективна кібербезпека базується на комплексному підході, який включає технічні, правові та організаційні заходи, а також тісну міжнародну співпрацю. Водночас існує потреба в актуалізації досліджень з урахуванням сучасних цифрових викликів.

Викладення основного матеріалу. Агентство Європейського Союзу з кібербезпеки – ENISA займає центральне місце в ініціативах ЄС щодо створення послідовної та ефективної структури кібербезпеки [10]. ENISA було засновано в 2004 році та розташовано в Греції. Повноваження Агентства з часом значно розширилися, в першу чергу з прийняттям Закону про кібербезпеку 2019 року, який надає Агентству розширені права та обов'язки [14]. Як спеціалізована агенція, ENISA зосереджується на зміцненні потенціалу кібербезпеки в державах-членах, координації транскордонного реагування на кіберінциденти та розробці загальних стандартів і практик, які можуть бути прийняті в усьому Союзі. Роль ENISA передбачає створення мереж співпраці між національними групами реагування на інциденти комп'ютерної безпеки, підтримку розробки та впровадження законодавства, першочергово Директива NIS та NIS2 [6, 7], а також сприяння діалогу між державними та приватними заінтересованими сторонами. Координаційна функція поширюється на управління загальноєвропейськими навчаннями з кібербезпеки, розробленими для перевірки колективної готовності та механізмів реагування на інциденти кіберзагроз. Шляхом імітації великомасштабних кібератак ці навчання виявляють вразливі місця та операційні прогалини, які інакше могли б залишитися непоміченими, спонукаючи держави-члени вдосконалювати свої стратегії виявлення, пом'якшення та звітування про загрози.

Ключовою сферою впливу ENISA є створення та розповсюдження найкращих практик і технічної документації. Звіти Агентства про загрози, які публікуються щорічно, відстежують нові вектори атак і зловмисників, надаючи державам-членам, установам ЄС і приватним організаціям консолідований огляд середовища кібербезпеки [9]. Консолідовані оцінки базуються на даних про інциденти, висновках експертів і транскордонному обміні розвідувальними даними, щоб висвітлити вразливі місця в критичній інфраструктурі, ланцюгах постачання і мережевих системах. Завдяки розвідувальній функції ENISA слугує основоположним регулятором та координатором для національних органів влади, зменшуючи дублювання та фрагментацію в зусиллях зі збору інформації та забезпечуючи більш синхронізовану відповідь на нові кіберзагрози.

Роль ENISA виходить за межі консультативних функцій і включає сприяння обміну інформацією та стимулювання гармонізації стандартів кібербезпеки. У співпраці з приватними підприємствами, державними адміністраціями та науковими установами ENISA сприяє впровадженню найкращих практик у сфері управління ризиками, реагування на інциденти та схем сертифікації. Завдяки цій взаємодії з багатьма заінтересованими сторонами Агентство підтримує більшу частину політично орієнтованої структури ЄС, перетворюючи Директиви NIS/NIS2 та Закон про кібербезпеку у практичні заходи, які можуть бути прийняті як на національному, так і на галузевому рівнях.

Поряд з ENISA Європейська мережа організації зв'язку з кіберкриз (EU-CyCLONe) [11] більш вузько зосереджується на оперативних аспектах кібербезпеки та врегулюванні криз, особливо під час масштабних або транскордонних кіберзагроз. Спираючись на підтримку галузевих центрів обміну та аналізу інформації (ISAC), EU-CyCLONe допомагає координувати відповіді стейкхолдерів, гарантуючи, що приватний сектор, державні органи та спеціалізовані агентства оперативно обмінюються розвідувальною інформацією про загрози та узгоджують свої зусилля зі стримування та пом'якшення. Секторальні ISAC представляють критичні точки взаємодії для таких галузей, як енергетика, фінанси чи транспорт, що дозволяє установам та організаціям у цих сферах обмінюватися спеціальними галузевими даними та найкращими практиками в режимі реального часу. EU-CyCLONe працює під егідою ENISA, але має власний окремий мандат на подолання розриву між політичними рамками та реагуванням на кризи, сприяючи комунікації між національними органами держав-членів, коли кіберінцидент досягає порогу, який ризикує каскадними ефектами через кордони.

CERT-EU забезпечує ще один ключовий елемент структури, що слугує спеціальною групою реагування на комп'ютерні надзвичайні ситуації для установ, органів і агенцій ЄС [3]. На практиці CERT-EU координує роботу з національними центрами кібербезпеки держав-членів, пропонуючи оперативну підтримку, аналіз інцидентів і рекомендації щодо захисту цифрової інфраструктури на рівні ЄС. Взаємодія між CERT-EU та національними центрами дозволяє швидше розголошувати критичні інциденти та більш однорідну позицію реагування. Паралельно співпраця зі спеціалізованими організаціями, враховуючи Спільний центр передового досвіду кіберзахисту НАТО (CCDCOE), сприяє певній узгодженості між ЄС і НАТО, особливо в аналізі загроз і технічних дослідженнях [2]. Хоча CCDCOE формально є афілійованим центром НАТО, результати його досліджень і навчань з кіберзахисту можуть інформувати про політику ЄС і зміцнювати трансатлантичні норми кібербезпеки.

Європейське оборонне агентство (EDA), яке в основному зосереджено на військовій співпраці між державами-членами, співпрацює з ENISA щодо ініціатив, які мають як цивільне, так і оборонне застосування. Оперативна мережа військової комп'ютерної команди реагування на надзвичайні ситуації (MICNET) [8], що працює під егідою EDA, об'єднує національні військові CERT (milCERT) з кількох країн [13]. Встановивши цю паралельну, але оперативну структуру для інцидентів, пов'язаних з обороною, ЄС може протидіяти специфічним воєнним загрозами або передовим постійним загрозами (APT), які можуть бути спрямовані на оборонну інфраструктуру, водночас координуючи роботу з цивільною владою, у ситуації, де кібератаки охоплюють кілька доменів.

Вказана взаємодія між цивільною та військовою сферами – MICNET, CERT-EU та ENISA, підкреслює зростаюче визнання в ЄС того, що кіберінциденти не завжди обмежуються інституційними кордонами. Військові системи, державні установи, оператори критичної інфраструктури та приватні компанії можуть скоординовано стати ціллю зловмисників. Таким чином, система ЄС передбачає сумісність: ресурси та досвід ENISA керують встановленням стандартів, EU-CyCLONe та CERT-EU координують управління кризовими ситуаціями для широкого цивільного сектора, тоді як EDA та MICNET займаються специфікою оборонних операцій. Водночас національні центри кібербезпеки залишаються базовими органами системи для місцевого правозастосування, реагування на кіберінциденти та впровадження політики, при цьому центри кожної держави-члена зберігають остаточну відповідальність за національну інфраструктуру та процедури транскордонного співробітництва.

Результатом є багаторівнева та взаємопов'язана екосистема, розроблена для функціонування як горизонтально, коли агенції та національні центри співпрацюють, так і вертикально, коли приватний сектор і академічні установи передають інформацію вгору, отримуючи вказівки та підтримку від органів на рівні ЄС. На практиці ефективність системи залежить від бажання та спроможності держав-членів використовувати ці канали, обмінюватися своєчасною інформацією та інвестувати в розширення можливостей національних CSIRT і milCERT. Крім того, система спирається на певний ступінь довіри та взаємну співпрацю з транснаціональними та міжнародними партнерами, враховуючи глобальний характер кіберзагроз. Тим не менш, окресливши конкретні ролі для мереж ENISA, EU-CyCLONe, CERT-EU та EDA, орієнтованих на військову діяльність, ЄС інституціоналізував структуру, яка прагне досягти узгодженості між кількома рівнями управління та різноманітними операційними контекстами.

Більш широкий погляд на систему кібербезпеки ЄС вказує на те, що її стратегічна основа кодифікована через законодавчі акти, такі як Закон про кібербезпеку та Директива NIS, які визначають обов'язки та передбачають співпрацю між державами-членами. Роль ENISA у керуванні технічними стандартами посилюється завдяки створенню загальноєвропейської системи сертифікації кібербезпеки, тоді як циклічні оцінки загроз і широкомасштабні навчання підкреслюють постійну адаптацію до мінливих ризиків. Поєднуючи нормативні цілі з готовністю на місцях, система кібербезпеки ЄС прагне зменшити ризики в спосіб, який є гнучким і надійним, визнаючи, що кіберзагрози розвиваються з тривожною швидкістю, і їм неможливо ефективно протистояти за допомогою ізольованих, нескоординованих ініціатив.

Закон про кіберсолідарність демонструє значний прогрес у підході ЄС до кібербезпеки [16]. Розвиваючи солідарність, посилюючи можливості виявлення та реагування, а також розглядаючи мінливість кіберзагроз, регламент підкреслює відданість ЄС захисту свого цифрового суверенітету та забезпеченню безпечної та стійкої цифрової екосистеми для всіх стейкхолдерів.

Концепція транскордонних кіберхабів є критично важливим компонентом стратегії ЄС щодо посилення архітектури кібербезпеки, як це сформульовано в Законі про кіберсолідарність [1]. Кіберхаби передбачаються як платформи для співпраці, які виходять за межі національних кордонів, сприяючи співпраці в реальному часі та обміну інформацією між державами-членами. Виконуючи роль вузлів у ширшому Європейському кіберщиті, транскордонні кіберхаби відіграють ключову роль в уніфікації підходу ЄС до виявлення та подолання кіберзагроз.

Однією з основних функцій цих центрів є підвищення обізнаності ЄС щодо ситуації щодо загроз кібербезпеці. Завдяки інтеграції передових технологій, враховуючи штучний інтелект і машинне навчання, хаби обладнані для обробки та аналізу величезних обсягів даних, що дозволяє раннє виявлення аномалій і потенційних загроз. Проактивна здатність відіграє важливе значення для боротьби зі зростаючою складністю кібератак, які часто використовують вразливі місця в кількох юрисдикціях.

Транскордонні кіберхаби діють як координаційні центри під час кіберкриз. Пов'язуючи національні центри безпеки (SOC) та інші критично важливі об'єкти, центри сприяють швидкому розповсюдженню розвідувальних даних про загрози та координованої реакції на них. Така координація особливо важлива у випадках, коли кіберінциденти мають транскордонні наслідки, наприклад, атаки на взаємопов'язану інфраструктуру чи ланцюги поставок. Хаби забезпечують синхронізовану реакцію, мінімізуючи збої та забезпечуючи безперервність основних послуг. На додаток до своїх операційних функцій транскордонні кіберхаби слугують інноваційними центрами та центрами нарощування потенціалу. Вони надають

державам-членам платформу для обміну передовим досвідом, розробки гармонізованих протоколів і проведення спільних навчань. Такий спільний підхід не тільки зміцнює індивідуальні національні можливості, але й сприяє розвитку культури взаємодопомоги та довіри між членами ЄС.

Директива NIS2 [7] підкреслює важливість надійних механізмів управління кіберкризами в Європейському Союзі. Як частина комплексної основи для посилення кібербезпеки в державах-членах Директива зобов'язує кожну державу-члена призначати або створювати один або кілька органів управління кіберкризою. На ці органи влади покладено критичні обов'язки щодо забезпечення скоординованої та ефективної відповіді на загрози та інциденти кібербезпеці.

Директива визнає, що інциденти кібербезпеки часто мають широкомасштабні наслідки, впливаючи на численні сектори та, у деяких випадках, перетинаючи національні кордони. Очікується, що для вирішення цих проблем органи управління кіберкризами будуть виконувати функції центральних координаційних органів у відповідних державах-членах. Їх основні функції включають нагляд за підготовкою до серйозних кіберінцидентів, реагуванням на них і відновленням після них. Реалізація цих функцій передбачає тісну співпрацю з державними та приватними організаціями, установами для забезпечення узгодження зусиль і ресурсів.

Система органів взаємодії Європейського Союзу у сфері кібербезпеки має вагомий потенціал впливу на трансформацію української національної системи кіберзахисту, оскільки демонструє комплексний підхід, де кожен інститут виконує чітко окреслені функції та водночас тісно співпрацює з іншими структурами. Екосистема ЄС включає спеціалізовані установи на кшталт Європейського агентства з кібербезпеки (ENISA), мережі обміну оперативною інформацією (CERT-EU, EU-CyCLONe) та секторні платформи (ISACs), а також військові та оборонні елементи у межах Європейського оборонного агентства чи відповідних мереж (MICNET). Така модель стає прикладом, за яким Україна може оптимізувати розподіл відповідальності між державними органами, військовими структурами, приватними компаніями та громадськими інституціями.

Насамперед українські відомства, які відповідальні за виявлення, оцінку й реагування на кібератаки, отримають зразок ефективного функціонування, де вертикальна ієрархія поєднується з горизонтальними контактами та взаємною підтримкою між різними ланками. Це сприятиме активнішому залученню України в загальноєвропейські механізми обміну інформацією про загрози і у взаємні навчальні ініціативи. Запровадження більш тісної інтеграції з ENISA та іншими структурами ЄС дозволить отримувати оновлені аналітичні дані щодо вразливостей і методів зловмисників, а також впроваджувати найкращі практики щодо протидії сучасним кіберзагрозам.

Окрім взаємодії з європейськими партнерами, українська держава зіткнеться з необхідністю внутрішньої реорганізації та оновлення нормативної бази, аби забезпечити сумісність з координаційними механізмами ЄС. Інституції, які відіграють роль Національних центрів кібербезпеки, а також військові комп'ютерні групи реагування (milCERT), імовірно, об'єднають зусилля для спільного відстеження складних багатоетапних кібератак. У такій системі держава отримує більш повну «оперативну картину» кіберзагроз і може оперативно ухвалювати рішення, у тому числі з урахуванням міжнародних рекомендацій. Гармонізація процедур із системою ЄС також позитивно вплине на рівень довіри між різними секторами й іноземними партнерами. Коли приватний бізнес бачить, що уряд слідує чітким європейським стандартам і приєднується до міжнародних ініціатив з обміну досвідом, це стимулює компанії впроваджувати власні програми безпеки та брати участь у секторальних ISACs. Такий обмін інформацією і найкращими практиками, зокрема, дозволяє краще розуміти специфіку атак на конкретні галузі та швидше розгортати ефективні заходи захисту.

У межах проведеного дослідження нами запропоновано потенційну структуру системи кібербезпеки України, яка враховує необхідність інтеграції в європейську систему кібербезпеки (рис. 1). Структура базується на адаптації європейських стандартів, передбачених Директивою (EU) 2022/2555 (NIS2), а також інших ключових нормативно-правових актів ЄС, таких як GDPR, Cybersecurity Act та Cyber Resilience Act.

Запропонована модель включає три основні рівні: стратегічний, операційний та секторальний. На стратегічному рівні передбачено функціонування таких органів, як Офіс Президента, Кабінет Міністрів та Рада національної безпеки і оборони, які забезпечуватимуть координацію та розробку загальної стратегії кібербезпеки. Операційний рівень представлений Національним центром управління кіберкризами, Центром сертифікації кібербезпеки та Національним кіберрезервом, що забезпечуватимуть реагування на інциденти, сертифікацію IT-продуктів та послуг, а також готовність до масштабних кібератак. На секторальному рівні пропонується створення локальних офісів кібербезпеки, підтримка публічно-приватних партнерств і функціонування Академії кібернавичок для підготовки кваліфікованих кадрів. Модель орієнтована на зміцнення національної стійкості до кіберзагроз, ефективну координацію з європейськими органами кібербезпеки, а також дотримання високих стандартів кіберзахисту в усіх секторах економіки та державного управління.

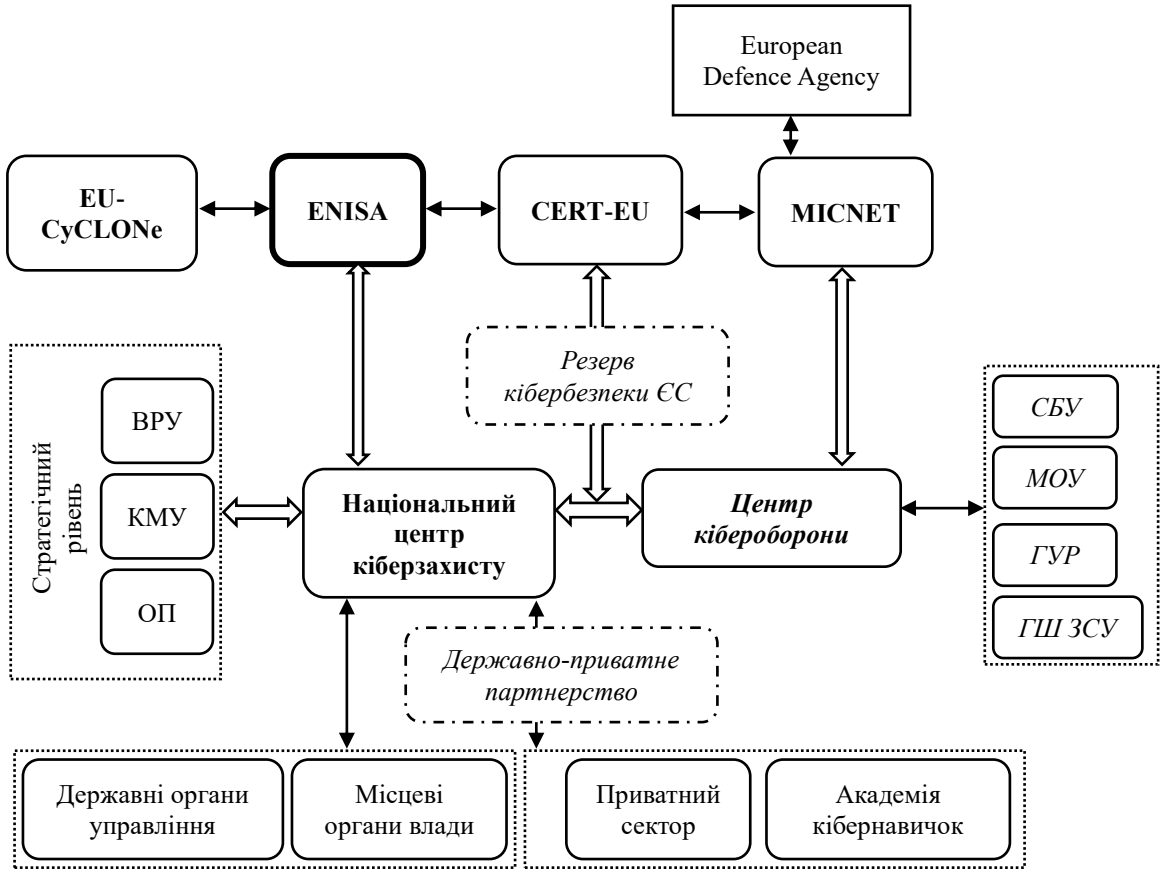

Рис. 1. Модель кібербезпекової системи України інтегрованої до системи ЄС

Висновки та перспективи подальших досліджень. Подальша інтеграція з оборонним сегментом ЄС, зокрема через механізми Європейського оборонного агентства чи подібні мережі, підштовхне реформування військового блоку кіберзахисту України. Це включатиме підвищення кваліфікації військових фахівців та уніфікацію протоколів реагування на гібридні загрози, що охоплюють і військову, і цивільну інфраструктуру. З часом такий процес дозволить уникнути дублювання функцій у різних державних структурах і сприятиме більш оперативному обміну інформацією між цивільними та оборонними відомствами. Загалом система органів взаємодії ЄС у галузі кібербезпеки вплине на трансформацію української системи передусім через демонстрацію прикладу багаторівневого, скоординованого та стандартизованого підходу до захисту цифрового простору. Впровадження споріднених процедур і методологій має на меті не лише підвищити загальний рівень безпеки критичної інфраструктури, але й стимулювати більш тісну інтеграцію України в європейський політико-правовий простір, створюючи умови для сталої співпраці та міжнародного визнання українських компетенцій у сфері кіберзахисту.

References:

1. CyberHubs, *Analytics*, [Online], available at: https://data.cyberhubs.eu/
2. CCDCOE, «The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise», [Online], available at: https://ccdcoe.org/
3. CERT-EU, *About us*, [Online], available at: https://cert.europa.eu/about-us
4. Cerulus, L., «How Ukraine became a test bed for cyberweaponry», POLITICO, [Online], available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/
5. «Cybersecurity rankings by country: Worst & Best Countries Ranked», *Comparitech*, [Online], available at: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/?fbclid=IwAR2vUYEilDvxl-ktT0WiZ0hRygCw-q0q19IGSnKay-UbVbRbprB5P7jSfDg
6. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, [Online], available at: http://data.europa.eu/eli/dir/2016/1148/oj
7. *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*, [Online], available at: http://data.europa.eu/eli/dir/2022/2555/2022-12-27

8. «EDA-led network of cyber defence teams starts with 18 EU countries», [Online], available at: https://eda.europa.eu/news-and-events/news/2023/02/10/eda-led-network-of-cyber-defence-teams-starts-with-18-eu-countries
9. ENISA (2024), *ENISA Threat Landscape 2024*, [Online], available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
10. ENISA, [Online], available at: https://www.enisa.europa.eu/
11. ENISA, *EU CyCLONe*, [Online], available at: https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone
12. Greenberg, A., «How an Entire Nation Became Russia's Test Lab for Cyberwar», *WIRED*, [Online], available at: https://www.wired.com/story/russian-hackers-attack-ukraine/
13. EDA, *MilCERT Interoperability Conference talks strategy*, [Online], available at: https://eda.europa.eu/news-and-events/news/2021/06/08/milcert-interoperability-conference-talks-strategy
14. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act)*, [Online], available at: http://data.europa.eu/eli/reg/2019/881/oj
15. Streltsov, L. (2017), «The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments», *Eur J Secur Res*, Vol. 2, pp. 147–184, doi: 10.1007/s41125-017-0020-x.
16. «The EU Cyber Solidarity Act», *Shaping Europe's digital future*, [Online], available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity
17. Boiko, V., Vasylenko, M. and Kukharenko, S. (2019), «Kiberbezpeka v YeS ta krainakh-chlenakh: henezys ta problemy yii pidvyshchennia», *Informatsiina bezpeka liudyny, suspilstva, derzhavy*, No. 3 (27), pp. 57–69.

Савчук Сергій Олександрович – здобувач кафедри національної безпеки, публічного управління та адміністрування Державного університету «Житомирська політехніка».

https://orcid.org/0009-0007-7436-0702.

Наукові інтереси:

– державна політика протидії кіберзлочинності.

E-mail: savcukserij4@gmail.com.

Savchuk S.O.

Challenges and opportunities of integration of Ukraine in the EU cyber security system

The article highlights the key aspects of developing the cyber protection system in the European Union and its importance for the sustainability of e-commerce and utility structures. The article examines the NIS and NIS2 directives, which set standards for cyber security norms, and the Cyber Security Law, which defines the certification processes of IT goods and services. Specialized European bodies, such as ENISA, CERT-EU, and EU-CyCLONE, organize responses to countering cyber threats, strengthen international cooperation, and share intelligence. The article presents the adjusted structure of the mechanism of digital protection of the nation-state, which combines the principles characteristic of the European regime of approval of digital guarantees. The proposed model envisages the unique responsibilities of public administration bodies, which are developed by the strategy proposed in the article and promote both the hiring of experts and public-private cooperation. The result of implementing the model is the strengthening of critical infrastructure, increasing the level of response to emergency situations, and providing a national character. The article emphasizes the importance of the European integration of Ukraine in strengthening protection against modern cyber threats and preserving trust in the cyber environment. The conclusions and advice obtained can serve as a basis for further study and practical deployment of a cyber security structure consistent with national and international protocols.

Keywords: public administration; integration; cyber threats; cyber security; critical infrastructure; certification.

Стаття надійшла до редакції 02.05.2024.