

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СВІТОВИХ ПРАКТИК НА СТАНДАРТИЗАЦІЮ ПРОФЕСІЙ

Розглянуто вплив розвитку інформаційних технологій на процеси стандартизації професій у контексті глобальних змін на ринку праці. Висвітлено основні міжнародні підходи до формування професійних стандартів, зокрема у сфері кібербезпеки, та їх імплементація в Україні. Проаналізовано світові класифікаційні системи, такі як ISCO-08, ESCO, ECSF та NIST NICE, їх структура та значення для гармонізації національних стандартів. Особливу увагу приділено трансформації професійних вимог у галузі інформаційних технологій та кібербезпеки під впливом цифровізації. Розглянуто створення Національної рамки кваліфікацій у сфері кібербезпеки в Україні та впровадження нових професійних стандартів. Окреслено перспективні напрями розвитку систем стандартизації професій з урахуванням динамічних змін у цифровому середовищі та викликів національної безпеки. Досліджено взаємозв'язок між професійними стандартами у сфері кібербезпеки та підвищенням рівня національної інформаційної безпеки в умовах цифрової трансформації. Визначено ключові компетенції фахівців з інформаційних технологій згідно з європейськими та міжнародними фреймворками та їх відповідність потребам українського ринку праці. Обґрунтовано необхідність постійного оновлення професійних стандартів з урахуванням швидких темпів технологічних змін та еволюції кіберзагроз. Запропоновано механізми впровадження адаптивних професійних стандартів, що забезпечать гнучкість реагування освітньої системи на потреби галузі. На основі проведеного дослідження сформульовано стратегічні напрями державної політики щодо розвитку людського капіталу в сфері інформаційних технологій та кібербезпеки як фундаментального елементу цифрової стійкості держави.

Ключові слова: інформаційні технології, стандартизація професій, кібербезпека, професійні стандарти, цифрова трансформація, національна рамка кваліфікацій.

Вступ

Сталий розвиток інформаційних технологій змінює сучасний світ, створюючи нові виклики та можливості для ринку праці. Цифровізація, автоматизація та поширення штучного інтелекту призводять до трансформації традиційних професій і появи нових, які вимагають сучасних навичок та компетенцій. Інтеграція України у світову економіку підвищує потребу в уніфікації професійних стандартів, що забезпечують конкурентоспроможність українських фахівців на міжнародному рівні.

Кібербезпека є однією з найбільш критичних сфер, що зазнала суттєвих змін. Постійні кібератаки, витоки даних та інформаційні війни змушують держави та приватні організації адаптуватися до нових реалій, створюючи ефективні системи захисту інформації. У зв'язку з цим особливо важливим є формування професійних стандартів у сфері кібербезпеки, що базуються на кращих міжнародних практиках і враховують виклики цифрової епохи.

Цифрова трансформація, яка стала визначальним трендом XXI століття, створила безпрецедентний попит на кваліфікованих фахівців у галузі інформаційних технологій та кібербезпеки. За даними дослідження Всесвітнього економічного форуму 2023 року, до 2026 року глобальний ринок праці потребуватиме понад 3,5 мільйона спеціалістів у сфері кібербезпеки, при цьому близько 40% цих вакансій залишаться незаповненими через брак кваліфікованих фахівців.

Україна активно впроваджує європейські та світові підходи до стандартизації професій, адаптуючи міжнародні системи кваліфікацій, такі як американська рамка кваліфікацій NIST NICE Cybersecurity Workforce Framework, ISCO-08 (Міжнародна стандартна класифікація занять), ESCO (Європейська класифікація навичок і професій) та ECSF (Європейська система навичок у сфері кібербезпеки). Впровадження цих стандартів сприяє гармонізації національної системи професійної підготовки, забезпечує відповідність кваліфікацій сучасним вимогам та підвищує рівень захисту інформаційного простору.

Мета та завдання дослідження

Стаття присвячена аналізу впливу розвитку інформаційних технологій на стандартизацію професій, розгляду основних міжнародних підходів до формування кваліфікаційних вимог та їхньої адаптації в Україні. Особливу увагу приділено викликам кібербезпеки, які потребують комплексного підходу до професійної підготовки фахівців у цій галузі.

Основні проблеми, що досліджуються в статті:

1. Вплив цифрової трансформації на зміну вимог до професійних компетенцій у галузі інформаційних технологій.
2. Аналіз міжнародних систем стандартизації професій та їх адаптація до українських реалій.
3. Виклики у формуванні національної системи кваліфікацій у сфері кібербезпеки.
4. Шляхи подолання кадрового дефіциту в галузі інформаційної безпеки.

Дослідження цих питань має вирішальне значення для створення ефективної системи підготовки фахівців, здатних забезпечити інформаційну безпеку держави та конкурентоспроможність українських спеціалістів на глобальному ринку праці.

Аналіз літератури

З метою подолання кризових явищ притаманних сучасному світу, переходу від індустріального до інформаційного суспільства, зміцнення стійкої конкурентоспроможності в економіці, забезпечення соціальної справедливості з впровадженням на практиці першого принципу Європейської основи соціальних прав: доступ до освіти, професійної підготовки та навчання впродовж життя для кожного та на підтвердження зацікавленості України у реалізації проголошених резолюцією Генеральної Асамблеї Організації Об'єднаних Націй від 25 вересня 2015 року №70/1 глобальних цілей сталого розвитку до 2030 року, в Україні сформовано систему моніторингу основних індикаторів, за якими можна відстежувати та оцінювати хід досягнення цілей сталого розвитку (ЦСР) в окремих сферах життєдіяльності [1].

В свою чергу в Національній доповіді “Цілі Сталого Розвитку: Україна”, яка була презентована урядом в вересні 2017 року, завдання, індикатори та рекомендації щодо адаптації до 2030 року 17-ти глобальних цілей сталого розвитку та 169 завдань з урахуванням специфіки національного розвитку. Ціллю № 9 є створення стійкої інфраструктури, сприяння всеохоплюючій і сталій індустріалізації та інноваціям передбачається вирішення низки завдань, одним з яких є завдання 9.с – Істотне розширення доступу до інформаційно-комунікаційних технологій, прагнути до забезпечення загального і недорогого доступу до Інтернету в найменш розвинених країнах [2].

Згідно з Указом Президента України від 30 вересня 2019 року № 722 Цілі сталого розвитку України на період до 2030 року є орієнтирами для розроблення проєктів прогностичних і програмних документів, проєктів нормативно-правових актів з метою забезпечення збалансованості економічного, соціального та екологічного вимірів сталого розвитку України [3].

Дані ЦСР України ґрунтуються на глобальних Цілях сталого розвитку, прийнятих на Саміті ООН у вересні 2015 року, та адаптовані до національного контексту. Для моніторингу виконання цих завдань Державною службою статистики України розроблено систему із 183 показників, що дозволяє оцінювати прогрес досягнення ЦСР.

Відповідно до Добровільного національного огляду щодо досягнення Цілей сталого розвитку України за 2023 рік, держава продемонструвала певний прогрес у реалізації завдань, незважаючи на складні обставини повномасштабної війни. Особливих успіхів досягнуто у

впровадженні Цілі 4 “Якісна освіта” через розвиток цифрових освітніх платформ та забезпечення доступу до навчання для внутрішньо переміщених осіб, а також Цілі 9 “Промисловість, інновації та інфраструктура” завдяки пришвидшеній цифровій трансформації державних послуг.

Кабінет Міністрів України у березні 2022 року створив Координаційну раду з питань відновлення України, яка розробила План відновлення України, що узгоджується з ЦСР та включає стратегічні напрями для післявоєнної відбудови з акцентом на принципах сталого розвитку. Зокрема, План передбачає інтеграцію екологічних стандартів ЄС у процеси відбудови інфраструктури (в рамках Цілі 11 “Сталий розвиток міст і громад”) та впровадження енергоефективних технологій (Ціль 7 “Доступна та чиста енергія”).

Прийнятий 15 липня 2022 року Закон України “Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій” визначає сталий розвиток як основний принцип політики відновлення та розбудови країни, що безпосередньо пов’язує процеси післявоєнного відновлення з реалізацією ЦСР.

Важливим кроком у імплементації ЦСР стало також підписання Угоди про асоціацію між Україною та ЄС, а також надання Україні статусу кандидата на вступ до ЄС у червні 2022 року, що створює додаткові стимули для прискорення впровадження принципів сталого розвитку та відповідних реформ. Згідно з Планом дій з реалізації Стратегії екологічної безпеки та адаптації до зміни клімату на період до 2030 року, затвердженим розпорядженням Кабінету Міністрів України від 13 жовтня 2021 року № 1363-р, передбачено інтеграцію екологічних вимог до всіх сфер державної політики згідно з принципами Європейського зеленого курсу.

Відповідно з чинним Законом України № 537-V “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” від 9 січня 2007 року визначено, що одними з основних стратегічних цілей розвитку інформаційного суспільства в Україні є: забезпечення комп’ютерної та інформаційної грамотності населення, насамперед шляхом створення системи освіти, орієнтованої на використання новітніх інформаційно-комунікаційних технологій у формуванні всебічно розвиненої особистості; захист інформаційних прав громадян, насамперед щодо доступності інформації, захисту інформації про особу, підтримки демократичних інститутів та мінімізації ризику “інформаційної нерівності”; вдосконалення законодавства з регулювання інформаційних відносин; покращення стану інформаційної безпеки в умовах використання новітніх інформаційно-комунікаційних технологій [4].

Досягнення всього вище зазначеного можливо завдяки вирішенню низки завдань по створенню повнофункціональної інформаційної інфраструктури держави та забезпеченню захисту її критичних елементів;

підвищенню рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобіганню таким загрозам та забезпеченню ліквідації їх наслідків, здійсненню міжнародного співробітництва з цих питань;

вдосконаленню нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп’ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

розгортанню та розвитку Національної системи конфіденційного зв’язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [4].

Досягнення всього вище зазначеного можливо завдяки вирішенню низки завдань по створенню повнофункціональної інформаційної інфраструктури держави та забезпеченню захисту її критичних елементів;

підвищенню рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпеченню ліквідації їх наслідків, здійсненню міжнародного співробітництва з цих питань;

вдосконаленню нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

розгортанню та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [4].

Ефективна реалізація зазначених завдань набуває особливого значення в умовах війни та післявоєнного відновлення, коли інформаційний простір України зазнає постійних атак та потребує підвищеного захисту. Згідно з Стратегією кібербезпеки України, визначено п'ять стратегічних цілей, спрямованих на створення національної системи кіберстійкості, що безпосередньо пов'язані з вирішенням вищезазначених завдань. [5].

Відповідно до щорічного звіту Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України за останні роки, кількість кібератак на об'єкти критичної інфраструктури зросла на 45%, що підтверджує необхідність посилення заходів із захисту інформаційної інфраструктури держави. Особливо вразливими залишаються інформаційні системи у сферах енергетики, фінансів та державного управління.

У рамках міжнародного співробітництва Україна у 2022-2024 роках підписала низку меморандумів про взаєморозуміння у сфері кібербезпеки з країнами ЄС та НАТО, що дозволяє використовувати передовий досвід та технології для розбудови національної системи кіберзахисту. Зокрема, Україна долучилася до Центру передового досвіду НАТО з питань кіберзахисту (CCDCOE) як країна-контрибутор, що суттєво розширює можливості для обміну знаннями та підвищення кваліфікації українських фахівців.

Основна частина

Стрімкий розвиток новітніх інформаційно-комунікаційних технологій та його динамічне інтегрування у різні види економічної діяльності вимагає суттєвого покращення сучасної структури ринку праці та врахування тенденцій його подальшого розвитку. Ринок праці постійно перебуває під впливом тих процесів, які властиві сучасній економіці, і, зрозуміло, під впливом змін, пов'язаних з активним впровадженням інформаційно-комунікаційних технологій.

Цифрова трансформація значно впливає на структуру зайнятості у всьому світі. За даними Всесвітнього економічного форуму, близько 85 мільйонів робочих місць можуть бути витіснені автоматизацією, водночас можуть з'явитися 97 мільйонів нових ролей, адаптованих до нового розподілу праці між людьми, машинами та алгоритмами.

Основними тенденціями, що впливають на трансформацію ринку праці, є:

1. Автоматизація рутинних процесів та заміна їх штучним інтелектом.
2. Зростання потреби у спеціалістах з кібербезпеки, аналізу даних та хмарних технологій.
3. Виникнення гібридних професій, що поєднують технічні навички з галузевими знаннями.
4. Зміна формату роботи з традиційного офісного на віддалений або гібридний.
5. Скорочення життєвого циклу навичок та необхідність постійного навчання.

Так, ще в 2006 році, експерт Статистичного бюро International Labour Organization (Міжнародної організації праці), Девід Хантер констатував наявність суттєвих змін у

структурі попиту на робочу силу під впливом збільшення потреб на працівників, які володіють знаннями та навичками в галузі інформаційно-комунікаційних технологій. Аналізуючи зайнятість працівників у галузі інформаційно-комунікаційних технологій, він виявив наступні проблеми [6]:

- дефіцит кваліфікованих кадрів;
- високі темпи зміни професійної діяльності;
- стрімке зростання зайнятості;
- глобалізацію, міграцію робочої сили, «офшоринг»;
- появу нових технологій, що вимагають нових компетенцій;
- конвергенцію інформаційних технологій та технологій електрозв'язку.

Ці тенденції не тільки зберігаються, але й посилюються в сучасних умовах. За даними LinkedIn, попит на фахівців з кібербезпеки зріс на 30% за останні три роки, а спеціалісти з хмарних обчислень та штучного інтелекту стали одними з найбільш затребуваних на ринку праці.

Враховуючи це, експерти з International Labour Organization, яка об'єднує представників урядів, організацій працівників та роботодавців задля спільної розробки Міжнародної стандартної класифікації занять (The International Standard Classification of Occupations (ISCO-08)), на постійній основі здійснюють нагляд за їх дотриманням, відстежують зміни, які відбуваються зокрема у професійній діяльності фахівців галузі інформаційно-комунікаційних технологій. Так, визначено нові категорії професій. Ними було запропоновано систему тематичних груп як додаток до основної структури ISCO-08 [7].

Сама ж структура Міжнародної стандартної класифікації занять, містить розгорнуту інформацію про заняття, які включені до кожної групи, пов'язуючи фактичні (реальні) назви професій та робіт що застосовуються в світі з групами в класифікаційній структурі.

Класифікаційна структура може також служити в якості моделі (зразка) при розробці або адаптації (оновлені) національних класифікаційних структур занять в випадку, якщо абсолютна відповідність найменувань класифікаційних груп з Міжнародної стандартної класифікації занять (ISCO-08) не вимагається (не забезпечується).

Міжнародна стандартна класифікація занять (ISCO-08) спрямована на полегшення міжнародних зіставлень по зайнятості, забезпечуючи статистиків інструментарієм для здійснення міжнародних порівнянь даних що стосуються професійної зайнятості, а також надає можливість проводити такі зіставлення в форматі, зручному та продуктивному, як з точки зору пошуку конкретних рішень та організаційних заходів (дій), так і з точки зору проблем міжнародної міграції або працевлаштування.

Крім Міжнародної стандартної класифікації занять існує Європейська багатомовна класифікація навичок, компетенцій, кваліфікацій та професій (European Skills, Competences, Qualifications and Occupations – ESCO). Вона має описовий характер, ідентифікуючи та класифікуючи, навички, компетенції, кваліфікації та професії, актуальні для ринку праці та освіти в ЄС.

ESCO надає детальний опис 3000+ професій та 13500+ необхідних для них навичок, створюючи спільну “мову” для освіти, підготовки та ринку праці. Використання такої структурованої класифікації дозволяє :

1. Покращити узгодження попиту та пропозиції на ринку праці.
2. Полегшити професійну та освітню мобільність.
3. Підтримувати розвиток політики в галузі освіти та працевлаштування.
4. Сприяти інтеграції мігрантів у ринок праці ЄС. [8].

Частиною цієї ESCO є Європейська система навичок у сфері кібербезпеки (ECSF), що надає відкритий європейський інструмент для формування спільного розуміння кваліфікацій та професій у сфері кібербезпеки відповідно до загальних навичок та компетенцій ESCO. ECSF - є практичним інструментом для підтримки визначення та формулювання завдань, навичок, компетенцій та знань, пов'язаних із професіями європейських фахівців у галузі кібербезпеки. ECSF узагальнило професійні заняття, пов'язані з кібербезпекою, у 12 профілів (кваліфікацій), які індивідуально аналізуються з деталізацією їхніх відповідних обов'язків, навичок, поєднання та взаємозалежності.

Вона забезпечує загальне розуміння найнеобхідніших навичок, компетенцій і знань для відповідних професій у сфері кібербезпеки, сприяє визнанню навичок і компетенцій у сфері кібербезпеки та підтримує розробку навчальних програм, пов'язаних із кібербезпекою.

12 професійних профілів, визначених ECSF, включають:

1. Офіцер з кібербезпеки.
2. Аудитор кібербезпеки.
3. Керівник з кібербезпеки.
4. Архітектор кібербезпеки.
5. Спеціаліст з кіберфорензики.
6. Консультант з кібербезпеки.
7. Фахівець з реагування на інциденти.
8. Тестувальник на проникнення.
9. Дослідник кібербезпеки.
10. Аналітик кібербезпеки.
11. Розробник з безпеки.
12. Фахівець з управління ризиками в кібербезпеці.

Стандарти (фреймворк) та відповідний посібник користувача були презентовані під час 1-ї Конференції агенції, що опікується досягненням високого загального рівня навичок з кібербезпеки в Європі (ENISA) у вересні 2022 року.

Поряд з європейськими підходами важливе місце в глобальній системі стандартизації професій у сфері кібербезпеки займає американська рамка NIST NICE (National Initiative for Cybersecurity Education). Цей фреймворк, розроблений Національним інститутом стандартів і технологій США, є детальною класифікацією робочих ролей, завдань, знань, навичок та здібностей, необхідних для ефективної роботи у сфері кібербезпеки.

NIST NICE Cybersecurity Workforce Framework (NCWF) структурує професії у сфері кібербезпеки за сімома категоріями:

1. Надання безпеки (Securely Provision).
2. Експлуатація та обслуговування (Operate and Maintain).
3. Захист і оборона (Protect and Defend).
4. Аналіз (Analyze).
5. Збір та експлуатація (Collect and Operate).
6. Розслідування (Investigate).
7. Нагляд та розвиток (Oversight and Development) [9].

Кожна категорія містить спеціальності, робочі ролі та детальний опис необхідних компетенцій. Загалом фреймворк визначає 52 робочі ролі та понад 1000 знань, навичок та здібностей. Такий детальний підхід дозволяє організаціям розробляти чіткі посадові інструкції, оцінювати персонал та створювати цільові програми навчання.

Отже впровадження в життя системи професійної стандартизації та атестації кадрів у сфері кібербезпеки та захисту інформації стало одним з стратегічних питань розвитку національної системи кваліфікацій та інтеграції України у європейський та світовий

кваліфікаційний простір. На сьогоднішній день сформована Національна рамка кваліфікації у сфері кібербезпеки з додаванням 27 нових професій у сфері кібербезпеки та захисту інформації до Класифікатора професій України. Окрім розширення списку професій, у провідних закладах вищої освіти країни запроваджені освітні програми, спрямовані на підготовку фахівців у сфері кібербезпеки. Впровадження ініціатив та сертифікаційних програми для державного та приватного сектору дозволить забезпечити високу якість підготовки спеціалістів.

Розроблені професійні стандарти враховують міжнародні стандарти Cyber Workforce Framework (NIST800-181, USA) та European Cybersecurity Skills Framework (ENISA) з урахуванням національних потреб. Зокрема, ініціатива NICE, що базується на NIST SP 800-181, стала ключовим орієнтиром у створенні національної рамки кваліфікацій у сфері кібербезпеки. NICE визначає стандарти для професійних навичок, необхідних спеціалістам у різних доменах кібербезпеки, що дозволяє адаптувати підготовку фахівців до реальних потреб ринку. Затверджено 21 професійний стандарт (46 нових кваліфікацій) у сфері кібербезпеки та захисту інформації.

Створений Кваліфікаційний центр інформаційних технологій та кібербезпеки при Держ.НДІ технологій кібербезпеки та захисту інформації дозволить підвищити ефективність системи кіберзахисту на основі сучасних стандартів, розробки професійних кваліфікацій та впровадження програм атестації для фахівців державного та приватного сектору. Однією з головних переваг цієї системи є підвищення довіри громадян до цифрових послуг та державних онлайн-сервісів. Завдяки впровадженню сучасних стандартів кіберзахисту знижується ризик витоку персональних даних, шахрайства та кібератак на державні ресурси, що особливо актуально в умовах зростаючих загроз у цифровому просторі.

Кваліфікаційний центр виконує наступні функції:

1. Розробка та впровадження професійних стандартів у сфері ІТ та кібербезпеки.
2. Проведення незалежного оцінювання та сертифікації фахівців.
3. Організація професійного навчання та підвищення кваліфікації.
4. Моніторинг потреб ринку праці та актуалізація вимог до фахівців.
5. Співпраця з міжнародними організаціями щодо гармонізації стандартів.

Структура NICE поділяє професії у сфері кібербезпеки на сім ключових доменів, включаючи аналіз загроз, безпеку мереж, управління ризиками та реагування на інциденти. Українська рамка кваліфікацій інтегрує ці підходи, адаптуючи їх до специфіки національної кібербезпеки. Це сприяє гармонізації підготовки фахівців з міжнародними вимогами та забезпечує визнання їхніх навичок на глобальному ринку.

Інтеграція України до європейського та світового кваліфікаційного простору проявляється у конкретних кроках:

1. Адаптація освітніх програм закладів освіти до міжнародних стандартів.
2. Впровадження дуальної освіти, що поєднує теоретичну підготовку та практичний досвід.
3. Розвиток систем незалежної сертифікації, визнаної на міжнародному рівні.
4. Участь українських експертів у розробці міжнародних стандартів.
5. Впровадження єдиної термінології та методології оцінки компетенцій.

Замовником фахівців зі спеціальності F5 (125) Кібербезпека та захист інформації виступає Державна служба спеціального зв'язку та захисту інформації України, яка є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку,

формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону.

Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України [10].

Проте, незважаючи на значні досягнення, ще залишається низка викликів. Одним із головних питань є кадровий дефіцит у сфері кібербезпеки, що потребує додаткових освітніх ініціатив та програм перепідготовки. Також важливо продовжувати вдосконалювати нормативно-правову базу для адаптації до сучасних загроз. У перспективі необхідно посилити інтеграцію з міжнародними партнерами для обміну досвідом та впровадження кращих практик у галузі кіберзахисту.

Висновки і рекомендації

У сучасних умовах розвитку інформаційного суспільства та цифрової економіки кібербезпека стала ключовим елементом національної безпеки України. Впровадження міжнародних стандартів у сфері кібербезпеки, створення Національної рамки кваліфікацій, розробка професійних стандартів та відкриття Кваліфікаційного центру інформаційних технологій і кібербезпеки сприяють підвищенню рівня підготовки фахівців. Це забезпечує ефективний захист критичної інформаційної інфраструктури, зміцнює довіру до цифрових послуг та формує стійку, конкурентоспроможну економіку, засновану на сучасних технологіях.

Важливим фактором у розвитку кібербезпеки є міжнародна співпраця, зокрема з ENISA, NIST, ЄС та НАТО, що сприяє інтеграції України у світовий кіберпростір. Однак для подальшого зміцнення кіберзахисту необхідно продовжувати вдосконалювати нормативно-правову базу, впроваджувати сучасні технології моніторингу загроз та підвищувати рівень цифрової грамотності населення. Це дозволить створити безпечне цифрове середовище для громадян, бізнесу та державних установ, зменшити кіберризики та забезпечити стабільний розвиток країни в умовах глобалізованого інформаційного простору.

Перелік посилань

1. Воронцов С., Бурбела Т. М. Сучасний стан та проблеми формування підходів до забезпечення сталого розвитку України. Національний інститут стратегічних досліджень. URL: <http://niss.gov.ua/sites/default/files/2020-07/suchasnyi-stan-zabezpechennya-stalogo-rosvytku-ukrainy.pdf> (дата звернення: 24.02.2025).
2. United Nations General Assembly. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development (A/RES/70/1)*. Retrieved from <https://undocs.org/A/RES/70/1>
3. Український національний комітет сталого розвитку. (2017). Стратегія сталого розвитку України до 2030 року. Організація Об'єднаних Націй. https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/UNDP_Strategy_v06-optimized.pdf
4. Верховна Рада України. (2007). Закон України № 537-V «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Відомості Верховної Ради України (ВВР), 2007, № 12, ст. 102. Отримано з <https://zakon.rada.gov.ua/laws/show/537-16#Text>
5. Указ Президента України від 26 серпня 2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"». Відомості Верховної Ради України (ВВР), 2021. Отримано з <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.
6. Хантер, Д. (2006). Заняття у сфері інформаційно-комунікаційних технологій: Доповідь на п'ятих зборах «Всесвітні показники в галузі електров'язку/ІКТ» (ВПЕ), Женева, Швейцарія, 11-13 жовтня 2006 р. [Електронний ресурс]. Отримано з aritu.org.ua/system/files/ilo-itu10-r.pdf.
7. International Labour Organization. Міжнародні стандарти праці. Сайт: [Електронний ресурс] – Режим доступу: <https://www.ilo.org/international-labour-standards/benefits-international-labour-standards> (дата звернення: 25.02.2025).

8. Офіційний сайт Європейського Союзу: [Електронний ресурс] – Режим доступу: <https://esco.ec.europa.eu/en/about-esco/what-esco> (дата звернення: 25.02.2025).
9. NICE Workforce Framework for Cybersecurity (NICE Framework). Сайт: [Електронний ресурс] – Режим доступу: <https://niccs.cisa.gov/workforce-development/nice-framework> (дата звернення: 25.02.2025).
10. Верховна Рада України. (2006). Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». Відомості Верховної Ради України (ВВР), 2006, № 30, ст. 258. Отримано з <https://zakon.rada.gov.ua/laws/show/3475-15>.

Надійшла 11.02.2025