

В.О.Ткач, науковий керівник - **Л.М.Новак-Каляєва**

Національний лісотехнічний університет України, спеціальність
«Публічне управління та адміністрування», місто Львів, Україна,
ORCID: 0009-0001-6582-0064

ВПЛИВ ЦИФРОВИХ ІНСТРУМЕНТІВ І КІБЕРЗАХИСТУ НА РОЗБУДОВУ УКРАЇНСЬКОЇ ДЕРЖАВНОСТІ ТА ІНТЕГРАЦІЮ В СВІТОВІ ОСВІТНІ І ТЕХНОЛОГІЧНІ ПРОЦЕСИ

У цих тезах досліджується роль цифрових технологій та кіберзахисту у процесі розбудови сучасної української держави та її інтеграції у глобальний освітній та технологічний простір. Розглядаються ключові аспекти цифровізації державних послуг, впровадження електронного урядування, а також виклики та можливості, пов'язані з кібербезпекою в контексті національної безпеки та міжнародного співробітництва. Особлива увага приділяється інтеграції України в світові освітні та технологічні процеси через розвиток цифрових компетенцій та інноваційних екосистем.

Ключові слова: кібербезпека, цифрові інструменти, кіберзахист, освітні процеси.

Інтеграція цифрових інструментів і покращення кіберзахисту можуть суттєво посилити українську державність через кілька ключових аспектів.

По-перше, цифровізація державних послуг спрощує взаємодію між громадянами та владою, підвищуючи прозорість і зменшуючи корупцію. Автоматизація адміністративних процесів економить ресурси і час, а також знижує ймовірність помилок.

По-друге, зміцнення кіберзахисту державних установ і критичної інфраструктури знижує ризики кіберзагроз, що важливо для стабільності країни. Надійний кіберзахист також забезпечує безпеку державних даних.

По-третє, інтеграція цифрових технологій у бізнес-процеси стимулює розвиток цифрової економіки, підвищуючи продуктивність і залучаючи інвестиції. Це створює нові можливості для стартапів і малого бізнесу.

По-четверте, цифрові інструменти забезпечують доступ до якісних освітніх і медичних послуг, покращуючи рівень життя населення. Електронні платформи взаємодії залучають громадян до процесів прийняття рішень.

По-п'яте, залучення людей до електронного урядування підвищує громадянську активність і відповідальність, а публікація державних даних підвищує прозорість.

Наостанок, інтеграція цифрових технологій сприяє співпраці з міжнародними організаціями та адаптації до європейських стандартів, що є важливим для політичної та економічної інтеграції з ЄС.

Для покращення впливу цифрових інструментів на освітні процеси в Україні та забезпечення кібербезпеки необхідно провести кілька ключових досліджень.

1) Варто оцінити рівень цифрової грамотності та доступність інфраструктури в освітніх закладах. Це включає вивчення рівня цифрових навичок учнів і викладачів, а також наявності технічних засобів і доступу до інтернету.

2) Необхідно проаналізувати ефективність використання цифрових платформ, таких як Google Classroom і Zoom, у навчальному процесі. Це дозволить виявити найуспішніші методики навчання та допомогти в розробці національних стандартів.

3) Зосередитися на стані кіберзахисту освітніх установ, вивчаючи вразливі місця і загрози для персональних даних. Це передбачає аудит систем безпеки та опитування ІТ-фахівців.

4) Як кіберзагрози впливають на освітні процеси і національну безпеку, аналізуючи кіберінциденти та їх наслідки.

5) Останнє, важливе дослідження — вивчення міжнародного досвіду впровадження цифрових інструментів і кіберзахисту. Це дозволить адаптувати найкращі практики до українських реалій, що сприятиме покращенню цифровізації освітніх процесів і підвищенню кібербезпеки в країні.

1. Цифрові інструменти в розбудові державності

Цифрові сервіси, зокрема платформа "Дія", стали важливим інструментом у державному управлінні України, забезпечуючи доступ до понад 70 державних послуг онлайн, що спрощує взаємодію між громадянами та урядом та зменшує корупцію. Ці сервіси підвищують ефективність адміністративних процесів і забезпечують доступність послуг у віддалених регіонах.

Громадяни отримують можливість активно брати участь у державному управлінні через системи електронних петицій та громадського бюджету, що зміцнює демократію і залучає молодь до суспільних процесів. Однак зростання цифровізації підвищує ризики кіберзагроз, що робить кібербезпеку критично важливою. Атаки на критичну інфраструктуру вимагають посилення кіберзахисту та підвищення кіберграмотності серед державних службовців [6].

Інтеграція цифрових інструментів у світові технологічні процеси відкриває нові можливості для України, зокрема у сфері міжнародних ІТ-проектів та доступу до освітніх програм. Для успішної цифровізації Україні необхідна стратегія, яка включає розвиток цифрової інфраструктури, підвищення грамотності, посилення кібербезпеки та співпрацю з міжнародними партнерами. Це сприятиме інтеграції в світовий цифровий простір і розвитку країни.

В Україні, попри значний прогрес у розвитку цифрових інструментів, існують суттєві слабкі сторони, які заважають досягти європейських стандартів. По-перше, доступ до інтернету залишається проблемою, особливо у віддалених районах, що створює цифровий розрив між містами і селами. В Європі, навпаки, доступ до швидкісного інтернету є універсальним, навіть у віддалених зонах.

По-друге, недостатній рівень цифрової грамотності, зокрема серед старшого населення, перешкоджає ефективному використанню цифрових

інструментів. У країнах ЄС реалізовані масштабні програми підвищення цифрової грамотності для різних груп населення, що допомагає людям адаптуватися до нових технологій.

Кібербезпека в Україні залишається критично важливою проблемою через постійні кібератаки, які підкреслюють вразливість державних установ. У Європі ж існують комплексні системи кіберзахисту, що включають координацію між урядовими та приватними секторами, а також регулярне навчання кіберграмотності.

Недостатня інтеграція цифрових технологій в освіту також є проблемою: багато шкіл не мають належного обладнання та підготовлених викладачів. В Європі цифрові технології стали невід'ємною частиною освітнього процесу, акцентуючи увагу на індивідуалізованому навчанні та використанні штучного інтелекту.

В ЄС уже функціонують чіткі стандарти, такі як GDPR (Загальний регламент захисту даних), що регулюють захист персональних даних і діяльність цифрових платформ [4].

2. Кіберзахист як складова національної безпеки

За даними звіту CrowdStrike 2024, кіберзагрози в Україні значно зросли з початку війни в 2022 році. Найбільш поширеними типами атак залишаються зловмисний програмний забезпечення, фішинг та атаки на доступність (DDoS). В Україні зафіксовано різке збільшення кібератак на критичну інфраструктуру, особливо в енергетичному секторі, де зловмисники намагаються зупинити або порушити роботу важливих об'єктів [2].

У Європі, відповідно до звіту ENISA, у 2023 році кіберзагрози зосереджувалися на атаках з використанням програм-вимагачів (60% постраждалих організацій могли заплатити викуп) та зловмисного програмного забезпечення. Зокрема, в Європі в 2022 році стався найбільший напад типу DDoS, який стався у липні, в результаті якого було знищено багато інфраструктур [1].

DDoS (Distributed Denial of Service) атаки — це спроби порушити роботу цільового сервера або мережі, завантажуючи їх величезною кількістю запитів з Інтернету. Основні аспекти DDoS атак:

Механізм: Атакуючий часто використовує ботнет — мережу інфікованих комп'ютерів, які надсилають численні запити до цільового сервера. Це може призвести до уповільнення або повного падіння сервера, роблячи його недоступним для легітимних користувачів.

Типи атак:

- Атаки на обсяги: Наприклад, UDP-флуди, що насичують пропускну спроможність.
- Протокольні атаки: Як SYN-флуди, які використовують вразливості протоколів.

- Атаки на прикладному рівні: Спрямовані на конкретні програми з метою споживання ресурсів. Вплив: DDoS атаки можуть спричинити фінансові втрати, пошкодження репутації та перерви в обслуговуванні. Вони також можуть використовуватись як димова завіса для інших злочинних дій.

Стратегії захисту: Організації можуть використовувати фільтрацію трафіку, обмеження швидкості та спеціалізовані послуги для захисту від DDoS атак. Важливою є обізнаність та готовність до таких загроз. Кіберзагроза від програм-вимагачів (ransomware) — це тип шкідливого програмного забезпечення, яке блокує доступ до системи або даних, зазвичай шляхом шифрування файлів, і вимагає викуп (ransom) для їх відновлення. Основні аспекти програми-вимагачів:

1. Механізм дії: Програмне забезпечення проникає в систему, зазвичай через фішинг (в електронних листах) або вразливості в програмному забезпеченні. Після успішного вторгнення програма шифрує файли на комп'ютері жертви, на екрані з'являється повідомлення з вимогою викупу.

2. Фінансова вигода: Кіберзлочинці часто вимагають плату в криптовалюті, щоб ускладнити відстеження транзакцій. Це може призвести до великих фінансових втрат для жертв, включаючи бізнеси та організації.

3. Вплив: Атаки програм-вимагачів можуть зупинити роботу організацій, призводити до втрати важливих даних, порушення конфіденційності та завдати шкоди репутації компаній. Відомі атаки, такі як WannaCry, показали, як сильно можуть постраждати організації, якщо їх системи не захищені.

Стратегія кібербезпеки України є важливим документом, що визначає основні напрямки для забезпечення національної кібербезпеки у відповідь на зростаючі загрози, особливо з боку росії. Основні аспекти стратегії включають створення єдиної національної системи кібербезпеки, яка об'єднує державні органи, приватний сектор і громадянське суспільство. Основна увага приділяється захисту критичної інфраструктури, такої як енергетичний сектор та фінансові установи, де вже проведено оцінки ризиків і розроблено рекомендації щодо захисту.

Країна активно співпрацює з міжнародними організаціями, такими як НАТО і ЄС, для обміну інформацією про кіберзагрози та найкращі практики. Підвищення обізнаності та навчання населення про кібербезпеку є важливими складовими стратегії, включаючи програми для державних службовців та підприємств. Стратегія також передбачає вдосконалення законодавства у сфері кібербезпеки, зокрема регулювання діяльності операторів критичної інфраструктури [5].

Щодо порівняння з європейськими стандартами, в ЄС діє Директива NIS, що вимагає від держав-членів створення національних стратегій кібербезпеки та визначення відповідальних органів. Українська стратегія базується на європейських принципах, але ще не досягла необхідного рівня деталізації і обов'язковості [3].

В ЄС кожна країна має національний орган, відповідальний за кібербезпеку, тоді як в Україні цю роль виконує Державна служба спеціального зв'язку та захисту інформації, але існують питання координації між різними органами. Фінансування кібербезпеки в Україні залишається обмеженим, на відміну від європейських країн, які отримують значні кошти через програми, як-от Horizon Europe.

У ЄС створено централізовані платформи, такі як ENISA, для обміну інформацією про кіберзагрози, в той час як в Україні система реагування на інциденти потребує більшої інтеграції та узгодженості.

3. Інтеграція в світові освітні процеси

Інтеграція України в світові освітні процеси є важливим кроком для модернізації національної освітньої системи, підвищення її якості та доступу до міжнародних стандартів. Основні аспекти цього процесу включають участь у міжнародних освітніх програмах, таких як Erasmus+, що дозволяє українським студентам навчатися в європейських університетах, а викладачам обмінюватися досвідом з колегами з інших країн. Наприклад, програма Erasmus+ забезпечує можливості для навчання та стажування, що сприяє розвитку міжнародних зв'язків і культурної обізнаності.

Визнання українських дипломів і академічних кредитів в інших країнах стає можливим завдяки адаптації системи освіти до європейських стандартів, зокрема в рамках Болонського процесу. Болонська система передбачає створення спільних критеріїв оцінки якості освіти та впровадження кредитної системи ECTS (European Credit Transfer and Accumulation System). В Україні відбувається поступова адаптація освітніх програм до цих принципів, проте їх впровадження все ще потребує вдосконалення, щоб відповідати вимогам європейських університетів.

Співпраця з міжнародними університетами в спільних наукових дослідженнях і академічних програмах є важливим аспектом інтеграції. Такі партнерства допомагають Україні залучати нові знання та технології, підвищуючи науковий потенціал країни та інтегруючи українських дослідників у міжнародну наукову спільноту. Водночас, на відміну від європейських університетів, які мають більш розвинені механізми міжнародної співпраці, українські вищі навчальні заклади тільки починають формувати ці зв'язки.

Цифровізація освіти є важливим елементом модернізації освітньої системи. Україна прагне впроваджувати цифрові інструменти та електронні навчальні платформи, але рівень інтеграції цих технологій у навчальний процес поки що відстає від європейських стандартів, де цифрові технології використовуються для індивідуалізованого навчання.

У висновку можна підсумувати, що розвиток кіберзахисту та інтеграція України в світові освітні процеси є критично важливими для забезпечення національної безпеки та модернізації освіти. Незважаючи на прогрес у цих сферах, Україні слід звернути увагу на ряд проблем, таких як недостатній рівень кіберграмотності, вразливість критичної інфраструктури, брак координації між державними органами, обмежене фінансування, слабка правова база, проблеми з обміном інформацією та кадровий дефіцит.

Для ефективного реагування на сучасні виклики важливо реалізувати системні заходи, спрямовані на підвищення обізнаності про кіберзагрози, залучення інвестицій, удосконалення законодавства та покращення співпраці між усіма учасниками процесу. Крім того, інтеграція в міжнародні освітні програми, визнання дипломів, розвиток онлайн-освіти та підвищення цифрової грамотності сприятимуть покращенню якості освіти в Україні.

Список використаних джерел :

1. ENISA. "Threat Landscape Report 2023." European Union Agency for Cybersecurity, 2023. <https://www.enisa.europa.eu/publications>.
2. CrowdStrike. "Global Threat Report 2024." CrowdStrike Holdings, Inc., 2024, стор. 45-78. <https://www.crowdstrike.com/resources>.
3. Директива (ЄС) 2016/1148 Європейського Парламенту та Ради про заходи для забезпечення високого загального рівня безпеки мережевих і інформаційних систем (NIS Directive). <https://eur-lex.europa.eu/legal-content>.
4. GDPR (Загальний регламент захисту даних). Регламент (ЄС) 2016/679 Європейського Парламенту та Ради. <https://eur-lex.europa.eu/eli/reg/2016/679>.
5. "Українська стратегія кібербезпеки: напрями розвитку та інтеграція з міжнародними стандартами." Міністерство цифрової трансформації України, 2023, стор. 18-33. <https://mits.gov.ua/cybersecurity-strategy>.
6. OECD. "Digital Transformation of the Public Sector: Innovations in Digital Governance." OECD Publishing, 2022, стор. 92-110. <https://www.oecd.org/gov>.