DOI: https://doi.org/10.26642/sas-2024-2-3(3)-106-111
УДК 351:378(477)



**Слюсар Вадим**
*д.філос.н., доц., завідувач кафедри філософсько-історичних студій та масових комунікацій*
*Державний університет «Житомирська політехніка»*
https://orcid.org/0000-0002-5593-0622

**Яблонська Надія**
*к.пед.н., доц.кафедри філософсько-історичних студій та масових комунікацій*
*Державний університет «Житомирська політехніка»*
https://orcid.org/0000-0002-3368-5929

**Зайко Леся**
*к.філос.н., доц.кафедри філософсько-історичних студій та масових комунікацій*
*Державний університет «Житомирська політехніка»*
https://orcid.org/0000-0001-5009-607X

**Панченко Наталія**
*ст. викл. кафедри педагогічних технологій та мовної підготовки*
*Державний університет «Житомирська політехніка»*
https://orcid.org/0000-0003-3878-5563

# Формування цифрової стійкості у підготовці фахівців з національної безпеки та вчителів «Захисту України»

**Анотація.** У статті розкрито особливості формування цифрової стійкості фахівців національної безпеки та вчителів «Захисту України» як значимого фактору до сучасних викликів і загроз, забезпечення стабільного розвитку суспільства й захисту його цифрового майбутнього. Зазначено, що фахівці повинні виявляти джерела виникнення загроз для інформаційного простору країни і застосовувати механізми їх дискредитації, а також враховувати спрямованість деструктивної дії ворога на вразливих людей через соціальні мережі та таргетовану рекламу. Наголошено, що формування цифрової стійкості доволі результативним може бути під час вивчення освітньої компоненти «Стратегічні комунікації», під час якої майбутні фахівці з національної безпеки та вчителі «Захисту України» вивчають такі ключові елементи цього виду комунікацій, як інформування, вплив та переконування; ефективність інформування; координація та деконфліктизація; «комунікування діями» та зменшення розриву у конструкції say-do. Формування цифрової стійкості у фахівців національної безпеки та вчителів «Захисту України» передбачає оволодіння навичками створювати власні та використовувати профільні критичні платформи й інструменти, необхідні для виявлення і протидії гібридним загрозам. Акцентовано увагу на механізми формування цифрової стійкості як концепції «Суспільство 5.0», яка стала своєрідним теоретичним викликом на соціально-економічні та соціокультурні трансформації, що відбуваються як наслідок тотального упровадження цифрових технологій. Зазначено, що у контексті досліджуваної проблеми є ризик нерівномірності освоєння людьми цифрових медіа, що актуалізує необхідність на державному рівні упроваджувати механізми інтенсифікації адаптативних процесів.

**Ключові слова:** цифрова стійкість; національна безпека; Середня освіта (Захист України); стратегічні комунікації; НАТО; «Суспільство 5.0».

**Актуальність**. Проблема цифрової стійкості актуалізувалася лише останнє десятиліття у контексті процесів глобальної диджиталізації та, відповідно, зростання загроз у кіберпросторі. Вона стає об’єктом дослідження не лише технічних наук, які акцентують на механізмах запобігання кіберзагрозам, а й соціальних, які аналізують їх на рівнях суспільство – організація – особа як здатності протистояти їм, реалізовувати механізми збереження функціональності та відновлення після атак. Спостерігається взаємна детермінація зростання утвердження цифрових технологій та відповідне збільшення кількості втручання сторонніх суб’єктів із власною метою, переважно деструктивної дії. Подальший розвиток цифрових систем та широке їх використання у різних сферах життєдіяльності людини (особливо в умовах пандемії

Covid-19, коли цифрові технології дозволили зберегти комунікативні та деякі соціально-економічні зв'язки) роблять їх потенційними об'єктами для впливу на медіапростір. Це виражається також і в реалізації стратегічних комунікацій через поширення фейкових новин та дезінформації у медіапросторі потенційного чи реального ворога, завдаючи шкоди їх національній безпеці, економіці, політиці, соціальній стабільності загалом. Відтак, перед профільними навчальними закладами, у т. ч. закладами вищої освіти постає завдання формування цифрової стійкості у підготовці фахівців з національної безпеки, а також, у контексті сучасної освітньої реформи, вчителів «Захисту України». Ці професіонали повинні вміти розробляти ефективні стратегії захисту та управління інформаційними ризиками, швидко та ефективно долати соціальні та організаційні наслідки кібератак.

**Мета** – визначити особливості формування цифрової стійкості в сучасній вищій школі на прикладах майбутніх фахівців з національної безпеки та вчителів «Захисту України».

**Ступінь дослідження проблеми**. У соціально-гуманітарному дискурсі дослідження цифрової стійкості є складовою воєнних наук, зокрема у контексті вивчення стратегічних комунікацій. У контексті управління національною безпекою України значимою є аналітична довідка, підготовлена фахівцями «Microsoft», в якій здійснено огляд кібератак росії в Україні у перші шість тижнів широкомасштабного вторгнення та описано досвід підтримки цифрової стійкості нашої країни цією компанією [6]. Згодом виходить Звіт «Цифрова стійкість» за редакцією Рут Харланд, у якому здійснено спробу дати уявлення про обсяг, масштаби та методи використання росією кіберпотужностей як частини широкомасштабної «гібридної» війни в Україні, відзначити роботу організацій в Україні, які захищаються від наполегливих супротивників, а також надати стратегічні рекомендації організаціям у всьому світі [4]. Формуванню системи взаємодії між приватним технологічним сектором та державним сектором для формування цифрової стійкості, де перший відповідає за розробку технологій та розбудови цифрової інфраструктури, а другий – за прийняття інституційних рішень, присвячена праця «Цифрова передова. 15 заходів для підвищення цифрової стійкості Європи» [7]. У ній наголошується, що цифрова стійкість є механізмом подолання сучасних викликів для національної безпеки, адже війна в Україні є першою гібридною війною, яка розмиває межі між фізичними та нефізичними загрозами.

Також проблема формування відповідних навиків є складовою педагогічних і психологічних наук. Філософське осмислення тенденцій змін суспільного розвитку у контексті взаємовідносин «людина – техніка» дозволяє розкривати динаміку цифрової стійкості відповідно до характеру та інтенсивності диджиталізації. Аналізуючи цифрову стійкість у контексті вивчення ролі інформаційних технологій у забезпеченні безперервності підготовки фахівців в кризових умовах, Олена та Костянтин Левчук акцентують на таких компонентах цифрової стійкості як надійна онлайн-інфраструктура, засоби зв'язку, безпечне керування даними та адаптивні методи навчання [11]. Значимим доробком у філософсько-педагогічному зрізі дослідження цієї проблеми є наукова праця Петра та Ірини Саух «Суспільство 5.0». Архітектоніка освіти в умовах П'ятої промислової революції: виклики та перспективи», в якій автори розкривають характер трансформації освіти як синтезу найкращих досягнень цифрового й людського світу та синергію людини і штучного інтелекту [15]. Вітчизняні науковці Валентина Воронкова та Віталіна Нікітенко розкрили специфіку становлення цифрової людини і цифрового суспільства у філософській парадигмі. Зокрема вони наголошують на необхідності утвердження цифрових парадигм освіти, культури та людини, які формуватимуть індекси креативності, інноваційності, зростання патентної активності, легкості ведення бізнесу, національної та енергетичної безпеки промислових підприємств [9].

**Викладення основного матеріалу.** Однією із вихідних точок системного застосування механізмів цифрової стійкості у системі національної безпеки стала хвиля кібератак на державні служби Естонії у 2007 році, яка тривала протягом трьох тижнів. Але джерелом формування цифрової стійкості є не лише кібератак, а будь-яка дія, яка потребує застосування цифрових технологій для подолання її наслідків. У цьому контексті найбільш повним за змістом та обсягом є визначення поняття «цифрова стійкість», яке подане у праці «DigitalEurope. Цифрова лінія фронту. 15 дій для підвищення цифрової стійкості Європи». Автори його тлумачать як «розбудова нашої здатності як суспільства використовувати потужний потенціал цифрових технологій для підготовки та захисту від низки нинішніх і майбутніх викликів та загроз. Це можуть бути кібератаки, дезінформаційні кампанії, стихійні лиха, нові інфекційні захворювання або … війна» [7, с. 7]. При цьому актуалізується саме досвід російсько-української війни з її гарячою фазою, яка триває з 2022 року.

У аналітичній доповіді «Цифрова передова. 15 заходів для підвищення цифрової стійкості Європи» визначаються чотири складові цифрової стійкості, які визначають характер управління національною безпекою країни. До них належить кібербезпека та кіберуправління; цифрова інфраструктура; стійкість ланцюгів постачання; гнучкі механізми закупівель для нових та проривних технологій (EDT) [7, с. 3]. Вважаємо, що одним з ключових компонентів цифрової інфраструктури у цьому контексті має цифрова освіта, яка передбачає формування відповідних навиків застосовувати цифрові технології для відповідей на актуальні виклики, а також протидіяти деструктивному впливові, який діє через цифрові медіа.

Інша класифікація, запропонована С. Кавалліні, Р. Солді, Г. Казаліні, Г. Верді, А. Грассо, містить три компоненти: комплексна законодавча база, яка встановлює мінімальні вимоги до кібербезпеки та кіберстійкості; міцна та надійна критична інфраструктура (як зовнішня інфраструктура, необхідна для надання державних послуг та цифрова інфраструктура (мережі зв'язку та інформаційні системи з їхнім апаратним та програмним забезпеченням); належні навички цифрової та кібербезпеки для розуміння та подолання ризиків, управління наслідками інцидентів, стримування шкоди та поширення зовнішніх атак в органах місцевої та регіональної влади [4, с. 6]. Оволодіння цими навичками є передумовою професійного становлення сучасного фахівця з національної безпеки, а також педагога, який здатен сформувати відповідні навички в учнів (це, передусім, вчитель «Захисту України»). Щодо останніх, то у попередніх дослідженнях ми уже акцентували на необхідності формування лідерських soft skills в закладах вищої освіти (на прикладі підготовки вчителів «Захисту України») як відповідність освітній реформі щодо викладання цієї дисципліни [16].

Підвищення цифрової стійкості, як визначають Ш.К. Шанділя, А. Датта, Я. Картік, А. Нагар, передбачає застосування наступних «кроків»: оцінка поточного стану щодо існуючих заходів кібербезпеки та наявність вразливих місць; управління ризиками; навчання та обізнаність (упровадження навчальних програм, щоб усі працівники розуміли свою роль у підтримці цифрової стійкості); регулярне оновлення технологій та інструментів, які підвищують безпеку та стійкість; планування реагування на інциденти; створення та підтримка функціонування системи постійного моніторингу цифрових активів, щоб виявляти загрози та реагувати на них у режимі реального часу; співпраця та обмін інформацією [5]. Тобто окрім проведення відповідних навчальних занять у закладах вищої освіти, на яких відбувається формування цифрової стійкості, повинна функціонувати система освіти впродовж життя, в якій професіонали підвищуватимуть рівень обізнаності особливостей оновлення цифрових технологій.

Якщо навички кібербезпеки мають технічну спрямованість, то цифрової безпеки – технологічну, яка передбачає формування в особи здатності розпізнавати в інформаційних потоках шкідливий контент, і навичок відповідним чином реагувати на запобігання його поширення. Звісно, це передбачає освоєння медіаграмотності. Але фахівці з національної безпеки повинні виявляти джерела виникнення загроз для інформаційного простору країни і застосовувати механізми їх дискредитації. Також варто враховувати спрямованість деструктивної дії ворога на вразливих людей, що завдяки соціальним мережам та таргетованій рекламі в них є надзвичайно ефективною. Формування цифрової стійкості доволі результативним може бути під час вивчення освітньої компоненти «Стратегічні комунікації. Майбутні фахівці з національної безпеки та вчителі «Захисту України» вивчають такі ключові елементи цього виду комунікацій, як інформування, вплив та переконування; ефективність інформування; координація та деконфліктизація; «комунікування діями» та зменшення розриву у конструкції say-do [10, с. 13]. Передбачається аналіз інформаційної діяльності одних соціальних структур та організацій, які здатні спричинити ускладнення, а то й деградацію діяльності інших. У цьому контексті вивчення характеристик ведення інформаційних воєн чи спеціальних інформаційно-психологічних операцій дозволяє розуміти механізми дії пропаганди, дезінформації та роль і місце в їх реалізації цифрових технологій.

У словнику «Стратегічні комунікації» автори Т. Попова та В. Ліпкан не подають поняття «цифрова стійкість», але вагомим внеском є визначення близького до нього – «інформаційна стійкість». Воно тлумачиться як «здатність інформаційної системи до збереження суттєво важливих параметрів власного функціонування та розвитку» [14, с. 115]. Це пояснюється актуалізацією зазначеної проблематики лише в останні кілька років уже після видання словника. Але очевидно є тенденція пошуку запобігання діям потенційно ворожих сил щодо їх впливу на інформаційний простір. Тому здобувачі не лише вивчають основи медіаграмотності, а й розуміють тенденцію всеохоплюючого застосування цифрових технологій та ризиків, які воно виявляє. Зазначимо, що наразі здійснюється пошук дієвих програм здійснення стратегічних комунікацій через колективну цифрову стійкість у контексті оновлення змісту діяльності країн НАТО. Зокрема наголошується, що їхнім найбільш потужним засобом пом'якшення криз за допомогою посилення стійкості суспільства залишається довгострокова стратегічна комунікація, яка надає людям можливість діяти задля зменшення ризику, що постає перед ними та іншими людьми, готуючи їх перед наступною надзвичайною ситуацією і допомагаючи їм залишатися у безпеці [1]. Наразі можна стверджувати, що стратегічні комунікації стають дедалі однією з найбільш ефективних інструментів проти ворожих наративів. По суті, Інтернет і масові комунікації поступилися місцем когнітивній війні, яка є цифровою та віртуальною діяльністю, що здійснюється для маніпулювання подразниками навколишнього середовища з метою контролю психічних станів і поведінки ворогів, а також послідовників у війні [13, с. 33]. Але все-таки, вони є дієвими за умови формування колективної цифрової стійкості у громадян, що можливо не лише при наявності відповідних державних програм безпекового характеру, але й наявності достатньої кількості професіоналів, здатних навчати інших.

Водночас є й інші тенденції трансформації сучасної освіти, в т. ч. професійної. Зазначимо, що вища освіта, яка здатна і покликана формувати культурну особистість і громадянина глобального суспільства, спроможного жити і діяти у світі XXI століття з його невизначеністю і ризиком як ключовими

характеристиками, виступає вирішальним чинником реалізації настанов сталого розвитку, втілення їх у спільні соціальні цінності, якими керуються майбутні фахівці як у своїй професійній діяльності, так і в повсякденному житті [8]. Вагомими внеском у наукові розвідки утвердження механізмів формування цифрової стійкості є концепція «Суспільство 5.0». Вона стала своєрідним теоретичним викликом на соціально-економічні та соціокультурні трансформації, які відбуваються як наслідок тотального упровадження цифрових технологій. Розробка концепції, яка ініційована японським урядом у 2016 році, із залученням фахівців з асоціації крупного бізнесу «Кейданрен» стала маніфестом утвердження цифрового суспільства. Сучасний тип суспільства якісно вирізняється від попередніх – суспільства мисливців та збирачів, аграрного, індустріального та інформаційного – орієнтацією на соціальні потреби та запити. Концепція «Суспільство 5.0» вирізняється від інших, які аналізують нинішній стан суспільного розвитку, прагненням прийняття рішень, які сприятимуть створенню спеціальних соціальних умов. Як влучно відзначають Петро та Ірина Саух, перехід до п'ятої промислової революції ставить конкретні вимоги перед суспільством здійснити зміни у цілій низці соціальних сфер щодо розроблення адаптаційних стратегій подолання соціально-економічних наслідків диджиталізації виробництва [15, с. 3]. У розрізі досліджуваної проблеми відзначимо таким ризиком нерівномірність освоєння людьми цифрових медіа, що актуалізує необхідність на державному рівні упроваджувати механізми інтенсифікації адаптативних процесів. Яскравим прикладом є ініційований у лютому 2022 року президентом України О. Зеленським проєкт видачі усім вакцинованим пенсіонерам смартфони. Це передбачає стимулювання певної соціальної спільноти до освоєння диджитал-технологій, особливо у розрізі формування загальнонаціонального сервісу державних послуг та банку документів «Дія». Причиною такої цифрової нерівності може бути відсутність доступу до актуальних цифрових технологій, оскільки динаміка розвитку останніх може суттєво випереджати соціально-економічне забезпечення особи, що виражається у неспроможності як матеріального оволодіння ними, так і вивчення їх застосування.

Формування цифрової стійкості у фахівців національної безпеки та вчителів «Захисту України» передбачає оволодіння навичками створювати власні та використовувати профільні критичні платформи та інструменти, необхідні для виявлення і протидії гібридним загрозам. Як зазначають фахівці «DigitalEurope», наразі дуже мало уваги приділяється пошуку критично важливих талантів у сфері безпеки. За їх даними, як державний, так і приватний сектори повідомляють про труднощі з пошуком людей з потрібним набором навичок, зокрема у 2023 році в Європі не вистачало від 350 000 до мільйона кіберфахівців, а більшість дітей закінчують школу без базових знань з інформатики [7, с. 15]. Тобто, з одного боку, ризиком для будь-якої держави є втрата внаслідок дій агресора цифрових медіа, що паралізує функціонування значної кількості суспільних організацій. Саме приклад України, чия цифрова інфраструктура під час війни, особливо у період від широкомасштабного вторгнення, зазнала значних втрат, став чинником посилення політики по її розбудові та захисту для європейських країн. А з іншого боку – наявність спеціалістів, які здатні не просто використовувати цифрові медіа, а освоювати нові технології, пропонуючи вектори їх удосконалення. Варто враховувати, що сучасна людина може використовувати цифрові технології для посилення своєї стійкості, здатності адаптуватися, пристосовуватися і трансформуватися таким чином, щоб підвищити ймовірність досягнення бажаних результатів [3, с. 45].

Логіка розвитку сучасної освіти у контексті концепції «Суспільство 5.0» передбачає своєрідну синергію цифрових компетентностей у збалансованому поєднанні гуманістичної й технологічної складових. Ті країни, які виявлять неспроможність такої інтеграції, по суті, стагнуватимуть у своєму соціальному розвитку, не пропонуючи адекватні відповіді на виклики національній безпеці. Тобто, «окрім «цифрової грамотності, штучного інтелекту та аналітики даних», «роботи з новими технологіями», «кібербезпеки» та «уважності до даних» особливо важливими мають бути ключові компетентності, пов'язані з творчим, підприємницьким, гнучким і неупередженим мисленням» [15, с. 4]. Нині актуалізуються дослідження за напрямом «цифрова гуманітаристика». Навіть є дискусія щодо створення самостійної спеціальності з «Digital Humanities» та розвитку відповідних програм професійного навчання, щоб навички у цій галузі бралися до уваги при прийомі на роботу та просуванні службовими сходами [9, с. 64]. Цифрова гуманітаристика передбачає освоєння знань з мов і літератури, історії, музики, медіа та комунікації, інформатики та інформаційних досліджень, а також критичні цифрові дослідження, у т. ч. з науки про дані та штучний інтелект [2]. Це сприяє більш комплексному розумінню цифрових загроз і розробці ефективних стратегій їх подолання. Цифрова гуманітаристика актуалізує завдання дослідити соціокультурні наслідки цифрових технологій, здійснити критичний аналіз їх можливостей та обмежень, нові медіа, створення цифрових бібліотек, архівів, баз даних культурного надбання і музейних колекцій, цифрові реконструкції, тобто здійснення діяльності, яка потребує спільних зусиль гуманітаріїв та фахівців з цифрових технологій [12, с. 28]. Усвідомлення особою соціокультурного контексту розвитку цифрових технологій дозволяє не лише розуміти специфіку їх утвердження у різних сферах суспільства, а й надавати їм антропологічних сенсів, тобто «олюднювати» технології, та системно й колективно виявляти

деструктивні дії як аномальні. Такі атрибути цих дій є своєрідними маркерами небезпеки, які виявляють відповідні реакції на виявлені виклики.

**Висновки.** Цифрова стійкість є багатовимірною проблемою, яка потребує міждисциплінарного підходу та постійного оновлення знань і навичок. Це критично важливо для забезпечення безперервності національної безпеки в умовах швидкого розвитку технологій та нових форм загроз. Цифрова стійкість стає невід'ємною частиною підготовки фахівців, особливо в контексті сучасних викликів, таких як кіберзагрози та гібридна війна. Здатність протистояти цим загрозам є критично важливою для забезпечення національної безпеки. Ефективне формування цифрової стійкості потребує тісної співпраці між приватним технологічним сектором, який відповідає за розробку інноваційних рішень, та державним сектором, який приймає стратегічні рішення на рівні політики. Вивчення стратегічних комунікацій здобувачами освіти допомагають їм зрозуміти природу інформаційних загроз, таких як пропаганда, дезінформація, та маніпуляції, які активно використовуються у кіберпросторі. Це знання дозволяє їм ефективно виявляти та протидіяти цим загрозам.

**Список використаної літератури:**


1. *Aiken A.* The power of information to build resilience in a volatile world / *A.Aiken* // NATO Review. – 2023 [Електронний ресурс]. – Режим доступу : https://www.nato.int/docu/review/articles/2023/05/24/the-power-of-information-to-build-resilience-in-a-volatile-world/index.html
2. *Berry D.M.* What are the digital humanities? / *D.M. Berry* // The British Academy. – 2019. 13.02.2019 [Електронний ресурс]. – Режим доступу : https://www.thebritishacademy.ac.uk/blog/what-are-digital-humanities/
3. *Boh W.* Special Issue Introduction: Building Digital Resilience against Major Shocks, / *W.Boh, P.Constantinides, B.Padmanabhan, S.Viswanathan* // Management Information Systems Quarterly. – 2023. –№ 47 (1). Pp. 343–360.
4. *Cavallini S.* Digital resilience; edited by Ruth Harland. / *S.Cavallini, R.Soldi, G.Casalini, G.Verdi, A.Grasso* // Commission for Economic Policy. – 2023 [Електронний ресурс]. – Режим доступу : http://dx.doi.org/10.2863/5099.
5. *Shandilya S.K.* What Is Digital Resilience? Digital Resilience: Navigating Disruption and Safeguarding Data Privacy / *S.K. Shandilya, A.Datta, Y.Kartik, A.Nagar* // EAI/Springer Innovations in Communication and Computing. – 2024. – Springer, Cham. https://doi.org/10.1007/978-3-031-53290-0_1.
6. Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine // Microsoft. Digital Security Unit. – 2022. April 27. 20 p.
7. The digital front line. 15 actions to boost Europe's Digital Resilience // DigitalEurope. – 2023 [Електронний ресурс]. – Режим доступу :https://cdn.digitaleurope.org/uploads/2023/03/DIGITALEUROPE-TECHNOLOGY-IN-THE-FACE-OF-HYBRID-THREATS-FINAL-WEB-1.pdf.
8. *Yakovleva O.* New trends in scientific and technological revolution (STR) and transformation of science and education systems in the paradigm of sustainable development / *O.Yakovleva, V.Slyusar, O.Kushnir, A.Sabovchyk* // E3S Web of Conferences. – 2021. – № 277.
9. *Воронкова В.Г.* Філософія цифрової людини і цифрового суспільства: теорія і практика / *В.Г. Воронкова, В.О. Нікітенко*. – Львів-Торунь : Liha-Pres, 2022. – 460 с.
10. *Дубов Д.В.* Стратегічні комунікації: проблеми концептуалізації та практичної реалізації / *Д.В. Дубов* // Стратегічні пріоритети. Серія : Політика. – 2016. – № 4. С. 9–23.
11. *Левчук О.* Цифрова стійкість: оцінка ролі інформаційних технологій у забезпеченні безперервності підготовки фахівців в кризових умовах / *О.Левчук, К.Левчук* // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». – 2024. – Вип. 54. С. 137–145.
12. *Матвієнко О.* Цифрова гуманітаристика як методологічна основа розвитку ІТ-освіти у вищих навчальних закладах культури / *О.Матвієнко, М.Цивін* // Цифрова платформа: інформаційні технології в соціокультурній сфері. – 2018. – Вип. 2. – С. 26–36.
13. *Мойсіяха А.В.* Роль стратегічних комунікацій у зміцненні національної безпеки України: виклики та можливості / *А.В. Мойсіяха* // Публічне управління і адміністрування в Україні. – 2023. – № 37. – С. 30–35.
14. *Попова Т.В.* Стратегічні комунікації : словник / *Т.В. Попова, В.А. Ліпкан*. – Київ : ФОП О. С. Ліпкан, 2016. – 416 с.
15. Саух П.m«Суспільство 5.0». Архітектоніка освіти в умовах п'ятої промислової революції: виклики та перспективи / П.Саух, І.Саух // Вісник Національної академії педагогічних наук України. – 2023. – № 5 (1). С. 1–7. https://doi.org/10.37472/v.naes.2023.5223.
16. *Слюсар В.* Формування лідерських soft skills в закладах вищої освіти (на прикладі підготовки вчителів «Захисту України») / В.Слюсар, Н.Яблонська, О.Мосієнко // International Scientific Journal of Universities and Leadership. – 2024. – № 17. – С. 66–76. https://doi.org/10.31874/2520-6702-2024-17-66-76


**References:**


1. Aiken, A. (2023), The power of information to build resilience in a volatile world. *NATO Review*. [Online], available at: https://www.nato.int/docu/review/articles/2023/05/24/the-power-of-information-to-build-resilience-in-a-volatile-world/index.html
2. Berry, D.M. (2019), What are the digital humanities? *The British Academy*. 13.02.2019, [Online], available at: https://www.thebritishacademy.ac.uk/blog/what-are-digital-humanities/

3. Boh, W., Constantinides, P., Padmanabhan, B., Viswanathan, S. (2023), «Special Issue Introduction: Building Digital Resilience against Major Shocks», *Management Information Systems Quarterly*, 47 (1), 343–360.
4. Cavallini, S., Soldi, R., Casalini, G., Verdi, G. & Grasso, A. (2023), "Digital resilience; edited by Ruth Harland, *Commission for Economic Policy*, http://dx.doi.org/10.2863/5099.
5. Shandilya, S.K., Datta, A., Kartik, Y. & Nagar, A. (2024), What Is Digital Resilience? *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy. EAI/Springer Innovations in Communication and Computing*. Springer, Cham. https://doi.org/10.1007/978-3-031-53290-0_1
6. Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. (2022). *Microsoft*. Digital Security Unit. April 27, 2022.
7. The digital front line. 15 actions to boost Europe's Digital Resilience, (2023), *DigitalEurope*. [Online], available at: https://cdn.digitaleurope.org/uploads/2023/03/DIGITALEUROPE-TECHNOLOGY-IN-THE-FACE-OF-HYBRID-THREATS-FINAL-WEB-1.pdf
8. Yakovleva, O., Slyusar, V., Kushnir, O. & Sabovchyk, A. (2021), New trends in scientific and technological revolution (STR) and transformation of science and education systems in the paradigm of sustainable development, *E3S Web of Conferences*. 277.
9. Voronkova, V.H. & Nikitenko, V.O. (2022), Filosofiia tsyfrovoi liudyny i tsyfrovoho suspilstva: teoriia i praktyka, Lviv-Torun : Liha-Pres.
10. Dubov, D.V. (2016), Stratehichni komunikatsii: problemy kontseptualizatsii ta praktychnoi realizatsii, *Stratehichni priorytety. Seriia: Polityka*, 4, p. 9–23.
11. Levchuk, O. & Levchuk, K. (2024), Tsyfrova stiikist: otsinka roli informatsiinykh tekhnolohii u zabezpechenni bezperervnosti pidhotovky fakhivtsiv v kryzovykh umovakh, *Naukovyi zhurnal «Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo»*, 54. P. 137–145.
12. Matviienko, O. & Tsyvin, M. (2018), Tsyfrova humanitarystyka yak metodolohichna osnova rozvytku IT-osvity u vyshchykh navchalnykh zakladakh kultury, *Tsyfrova platforma: informatsiini tekhnolohii v sotsiokulturnii sferi*, № 2, p. 26–36.
13. Moisiiakha, A.V. (2023), Rol stratehichnykh komunikatsii u zmitsnenni natsionalnoi bezpeky Ukrainy: vyklyky ta mozhlyvosti, *Publichne upravlinnia i administruvannia v Ukraini*, № 37, p. 30–35.
14. Popova, T. V. & Lipkan, V.A. (2016), Stratehichni komunikatsii, slovnyk, Kyiv: FOP O.S. Lipkan.
15. Saukh, P. & Saukh, I. (2023), «Suspilstvo 5.0». Arkhitektonika osvity v umovakh piatoi promyslovoi revoliutsii: vyklyky ta perspektyvy, *Visnyk Natsionalnoi akademii pedahohichnykh nauk Ukrainy*, № 5 (1), 1–7, https://doi.org/10.37472/v.naes.2023.5223.
16. Sliusar, V., Yablonska, N. & Mosiienko, O. (2024), Formuvannia liderskykh soft skills v zakladakh vyshchoi osvity (na prykladi pidhotovky vchyteliv «Zakhystu Ukrainy»), International Scientific Journal of Universities and Leadership, № 17, 66–76, https://doi.org/10.31874/2520-6702-2024-17-66-76.

---

**Slyusar V., Yablonska N., Zayko L., Panchenko N.**

**Building digital resilience in the training of national security professionals and teachers of the «Defence of Ukraine»**

**Abstract.** The article reveals the peculiarities of forming digital resilience of national security specialists and teachers of the «Defense of Ukraine» as an important factor in countering modern challenges and threats, ensuring stable development of society and protecting its digital future. It is noted that specialists should identify sources of threats to the country's information space and apply mechanisms to discredit them, as well as take into account the focus of the enemy's destructive actions on vulnerable groups through social networks and targeted advertising. It is emphasized that the formation of digital resilience can be quite effective when studying the educational component «Strategic Communications»", during which future national security specialists and teachers of the «Defense of Ukraine» study such key elements of this type of communication as informing, influencing and persuading; information efficiency; coordination and deconfliction; «communication by action" and reducing the gap in the «say-do» construct. Building digital resilience in national security professionals and teachers of the Defence of Ukraine involves mastering the skills of creating their own and using specialized critical platforms and tools necessary to identify and counter hybrid threats. Attention is focused on the mechanisms of digital resilience formation as a concept of «Society 5.0», which has become a kind of theoretical challenge to the socio-economic and socio-cultural transformations that occur as a result of the total introduction of digital technologies. It is noted that in the context of the problem under study, there is a risk of uneven development of digital media by people, which actualizes the need to introduce mechanisms to intensify adaptive processes at the state level.

**Keywords**: digital resilience; national security; secondary education (Defense of Ukraine); strategic communications; NATO; Society 5.0.

---

Стаття надійшла до редакції 16.05.2024.