УДК 316.6:378:004.056
DOI: https://doi.org/10.24919/2308-4634.2026.356048

Світлана Воронова, *кандидат педагогічних наук,*
доцент кафедри кіберпсихології та реабілітації
Державного університету інтелектуальних технологій і зв'язку
ORCID: https://orcid.org/0000-0003-2753-8049

СОЦІАЛЬНА ІНЖЕНЕРІЯ В ОСВІТІ: ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ РОЗПІЗНАВАННЯ ТА ЗАПОБІГАННЯ СОЦІОІНЖЕНЕРНИМ АТАКАМ

У статті обґрунтовано систему формування у здобувачів вищої освіти компетентностей розпізнавання та запобігання соціоінженерним атакам в умовах цифрової трансформації освіти. Систему побудовано на поєднанні компетентнісного, системного, діяльнісного та ризик-орієнтованого підходів. Її реалізацію структуровано через навчальні теми, формування практичних навичок і блок інформаційної безпеки. Визначено результати підготовки: захист від атак, ефективна протидія маніпулятивному впливу, підвищення індивідуальної та інституційної кібербезпеки.

Ключові слова: *кібербезпека; компетентності; освітнє середовище; соціальна інженерія; соціоінженерна атака.*
Рис. 1. Літ. 13.

Svitlana Voronova, *Ph.D. (Pedagogy), Associate Professor of the Cyberpsychology and Rehabilitation Department,*
State University of Intelligent Technologies and Telecommunications
ORCID: https://orcid.org/0000-0003-2753-8049

SOCIAL ENGINEERING IN EDUCATION: FORMING COMPETENCIES TO RECOGNIZE AND PREVENT SOCIAL ENGINEERING ATTACKS

The article examines the problem of forming competencies in higher education students to recognize and prevent social engineering attacks in the context of the digital transformation of the educational environment. The relevance of the topic is due to the increase in the number of manipulative influences in cyberspace aimed at obtaining confidential information, violating information security, and psychological pressure on the individual. The purpose of the article is to theoretically substantiate the system of forming competencies in higher education students to recognize and prevent social engineering attacks within the framework of studying the discipline "Social Engineering". Conceptually, the system is built on the principle of combining competency-based, systemic, activity-based, and risk-based approaches to organizing the educational process and represents the relationship between content, procedural, and outcome components of training. The system is implemented through four content blocks: educational topics, practical skills, information security, and learning outcomes. The first block, "Educational topics," reflects the theoretical and methodological basis for the formation of competencies. The second block, "Practical Skills," represents the operational and activity component of training. The formation of practical skills is reinforced by the third block "Information Security", the purpose of which is to form a legal, analytical, and technological basis for safe behavior, which ensures conscious recognition of threats and the implementation of effective protection mechanisms. The formation of competencies for recognizing and preventing social engineering attacks is represented by three interrelated results: protection against social engineering attacks, effective counteraction to manipulative influence, and increasing the level of individual and institutional cybersecurity.

The practical significance of the article lies in the possibility of using the proposed system in the development of educational programs, educational and methodological complexes, and training courses on social engineering.

Keywords: *cybersecurity; competencies; educational environment; social engineering; social engineering attack.*

Постановка проблеми. Трансформація вищої освіти в умовах глобального цифрового суспільства супроводжується не лише розширенням можливостей для навчання, а й виникненням нових безпекових викликів. Одним із найнебезпечніших серед них є соціальна інженерія, яка використовує методи маніпуляції психологією людини з метою отримання конфіденційних даних або доступу до закритих ресурсів. Для здобувачів вищої освіти, які є найбільш активною групою користувачів цифрових сервісів, ця загроза набуває особливої гостроти. Сучасний здобувач перебуває в епіцентрі інформаційних потоків, що робить його вразливим до таких атак, наприклад, як фішинг, претекстинг, бейтинг. Проблема полягає в тому, що традиційна підготовка з інформаційної безпеки часто обмежується технічними аспектами, залишаючи поза увагою поведінковий та психологічний компоненти. Виникає нагальна потреба у зміщенні акцентів: від простого інформування про загрози до цілеспрямованого формування компетентностей розпізнавання та запобігання соціоінженерним атакам. Проте на сьогодні в педагогічній теорії та практиці спостерігаються суттєві прогалини: відсутність чіткого теоретичного підґрунтя для інтеграції знань із соціальної інженерії в освітній процес непрофільних та профільних спеціальностей; питання протидії маніпуляціям зазви-

чай розглядаються побіжно, без виділення їх в окрему дидактичну одиницю; освітній процес потребує структурованої педагогічної моделі, яка б об'єднувала когнітивний, діяльнісний та особистісний компоненти підготовки майбутнього фахівця.

Аналіз основних досліджень і публікацій. Проблематика соціальної інженерії як інструменту маніпулятивного впливу активно досліджується у працях закордонних фахівців із кібербезпеки та прикладної психології. Значний внесок у популяризацію розуміння людського фактора в інформаційній безпеці здійснив K. Mitnick, який у своїх працях обґрунтовує вирішальну роль психологічної складової у структурі кіберзагроз [13]. Практико-орієнтований підхід до дослідження соціальної інженерії представлено у роботах C. Hadnagy, де соціальна інженерія розглядається як міждисциплінарна галузь на перетині психології, комунікації та інформаційної безпеки. Автор систематизує техніки впливу та пропонує моделі навчання протидії соціоінженерним атакам [11]. Психологічні механізми соціального впливу глибоко досліджені R. Cialdini, який визначає базові принципи переконання (авторитет, взаємність, дефіцит, соціальний доказ тощо), що активно використовуються в соціоінженерних сценаріях [10]. У сфері стандартизації управління інформаційною безпекою важливу роль відіграють документи International Organization for Standardization, зокрема стандарт ISO/IEC 27001, що акцентує на підвищенні обізнаності персоналу як складовій системи менеджменту інформаційної безпеки [12].

В українському науковому просторі проблеми кібербезпеки та інформаційної культури досліджуються переважно з технічної або правової позиції (Є. Іосіфов, Н. Казеян, Д. Курбанмурадов, О. Куценко, О. Лоза, Л. Половенко, С. Мерінова, В. Соколов, В. Яковенко). В. Кононович та співавтори підкреслюють, що в епоху інтелектуальних технологій найважливішим "софтом" залишається людський розум, а найефективнішим методом захисту – його освіченість та критичне сприйняття дійсності [7]. Т. Ткач досліджує соціотехнічні аспекти проєктування освітніх середовищ, де навички розпізнавання маніпуляцій стають базовою компетенцією сучасної особистості [8]. О. Цуркан, Р. Герасимов, О. Крук аналізують методи протидії використанню соціальної інженерії; розглядають методи підвищення обізнаності працівників, клієнтів; акцентують на навчанні стосовно вірогідних сценаріїв атак соціальної інженерії [9]. Таким чином, аналіз наукових публікацій свідчить про наявність вагомої теоретичної бази щодо природи соціальної інженерії, однак проблема цілісного формування компетентностей розпізнавання та запобігання соціоінженерним атакам у системі вищої освіти залишається недостатньо розробленою.

Мета статті – теоретично обґрунтувати систему формування компетентностей розпізнавання та запобігання соціоінженерним атакам у здобувачів вищої освіти в межах вивчення дисципліни "Соціальна інженерія".

Виклад основного матеріалу. Формування компетентностей розпізнавання та запобігання соціоінженерним атакам у здобувачів вищої освіти є багаторівневим педагогічним процесом. Його специфіка полягає в тому, що об'єктом захисту виступає не лише інформаційна система, а й психологічна цілісність особистості, її здатність до критичного сприйняття маніпулятивних стимулів. Освітній процес базується на поєднанні теоретичних знань із когнітивної психології, кібербезпеки та практичних вправ/тренінгів із виявлення деструктивного впливу. Компетентність у цьому контексті ми розглядаємо як інтегровану характеристику особистості, що включає три ключові вектори: когнітивний (знання видів соціоінженерних атак (фішинг, вішинг, претекстинг тощо) та розуміння механізмів їхнього впливу); поведінковий (володіння алгоритмами перевірки джерел інформації та навичками безпечної комунікації в цифровому середовищі); ціннісний (відповідальне ставлення до власних цифрових даних та розуміння наслідків соціоінженерних атак для суспільства)

Запропонована система відображає цілісний процес формування у здобувачів вищої освіти компетентностей розпізнавання та запобігання соціоінженерним атакам у межах дисципліни "Соціальна інженерія" (рис. 1).

Концептуально система побудована за принципом поєднання компетентнісного, системного, діяльнісного та ризик-орієнтованого підходів до організації освітнього процесу і репрезентує взаємозв'язок змістових, процесуальних і результативних компонентів підготовки. Компетентнісний підхід визначає результат навчання як інтегровану характеристику особистості, що поєднує знання, уміння, навички, цінності та готовність до практичної діяльності. У контексті соціальної інженерії це означає не лише обізнаність щодо типів атак, а й здатність критично оцінювати інформаційні впливи, протидіяти маніпулятивним стратегіям та приймати відповідальні рішення в умовах цифрових ризиків. Системний підхід дозволяє розглядати процес формування компетентностей як взаємодію змістових, процесуальних і результативних компонентів, що перебувають у логічній та функціональній єдності. Діяльнісний підхід акцентує на практичному засвоєнні моделей поведінки через тренінги, симуляції, аналіз кейсів тощо. Ризик-орієнтований підхід передбачає формування навичок оцінювання й управління інформаційними загрозами відповідно до міжнародних стандартів інформаційної безпеки.

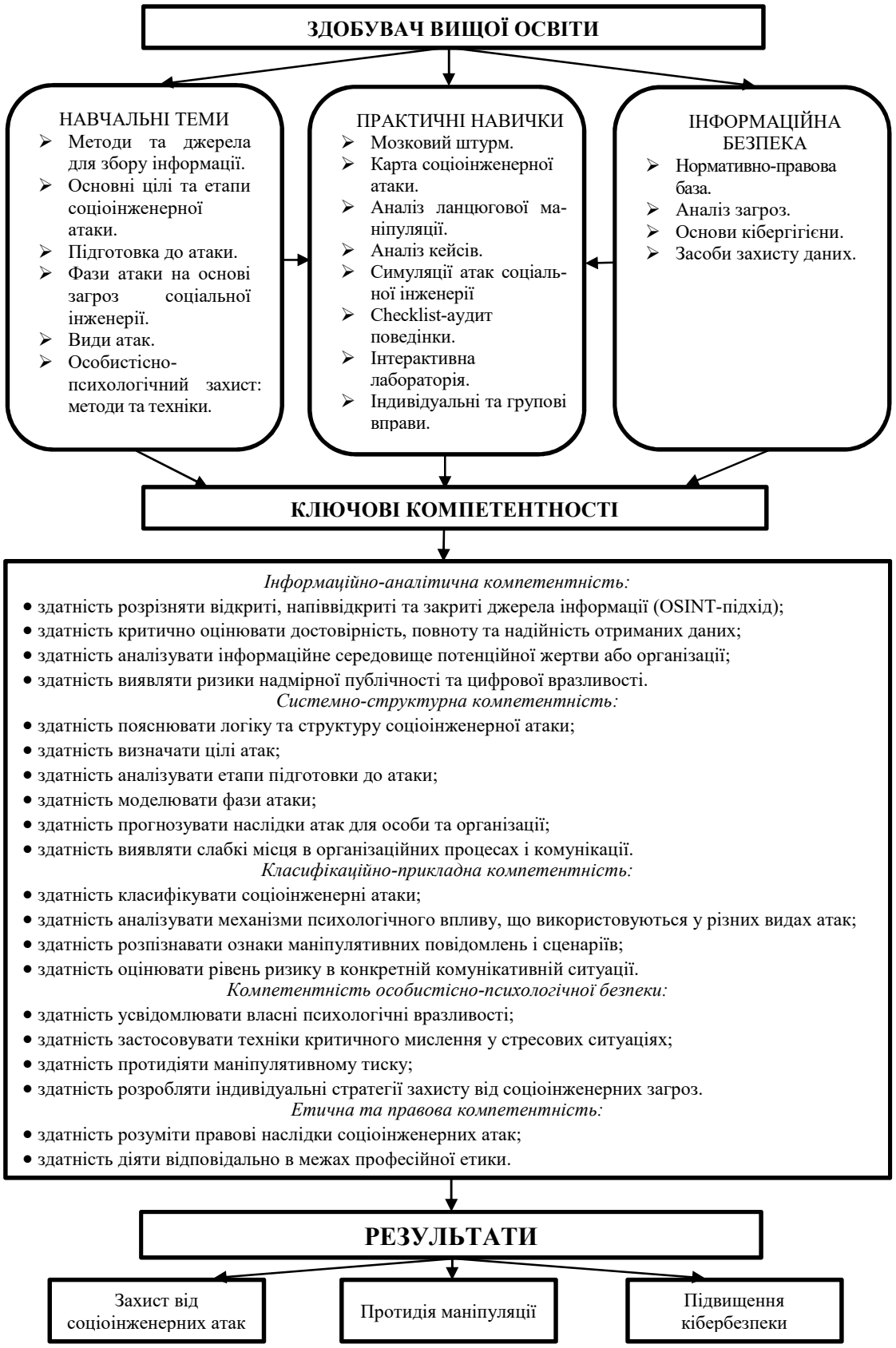

Рис. 1. Система формування у здобувачів вищої освіти компетентностей розпізнавання та запобігання соціоінженерним атакам

Центральне місце займає суб'єкт освітнього процесу – здобувач вищої освіти, що підкреслює студентоцентрований характер навчання. Далі маємо три взаємопов'язані структурні блоки: навчальні теми, практичні навички та інформаційна безпека.

Перший блок "Навчальні теми" відображає теоретико-методологічну основу формування компетентностей. Зміст цього блоку забезпечує формування когнітивного компонента компетентності, що включає знання про методи та джерела для збору інформації; основні цілі та етапи соціоінженерної атаки; підготовку до атаки; фази атаки на основі загроз соціальної інженерії; види атак; методи та техніки особистісно-психологічного захисту.

Другий блок "Практичні навички" репрезентує діяльнісний компонент підготовки. Його мета – сформувати прикладні вміння і поведінкові алгоритми розпізнавання маніпуляцій, оцінки ризиків та безпечного реагування в умовах реальної або змодельованої загрози. Він реалізується через мозкові штурми, створення карти соціоінженерної атаки, аналіз ланцюгових маніпуляцій та кейсів, симуляції атак, Checklist-аудит поведінки, інтерактивні лабораторії, індивідуальні та групові вправи. Мозкові штурми сприяють розвитку навичок виявлення потенційних загроз, генерації ознак соціоінженерних атак, формуванню критичного мислення. Результат – здобувачі здатні швидко ідентифікувати ризикові ситуації та пропонувати варіанти захисту. Створення карти соціоінженерної атаки (візуалізація структури атаки: ціль – канал – техніка – тригери – наслідки) формує у здобувачів системне бачення механізму атаки, розуміння етапності та логіки маніпуляції, допомагає виявити "точки втручання". Результат – здатність деконструювати атаку та прогнозувати її розвиток. Аналіз ланцюгових маніпуляцій допомагає визначити послідовність психологічних впливів, розпізнати ескалацію довіри та поступок, усвідомити механізми втягування. Результат – здатність перервати маніпуляцію на ранніх етапах. Аналіз кейсів (реальні або змодельовані ситуації) забезпечує перенесення теоретичних знань у практичний контекст, розвиває аналітичні та оціночні вміння, формує алгоритм безпечного реагування. Результат – здатність аргументовано оцінювати ризики та приймати рішення. Симуляції соціоінженерних атак (рольові ігри, сценарії фішингу, вішингу, претекстингу тощо) забезпечує відпрацювання моделей поведінки у стресовій ситуації, формування автоматизованих реакцій безпеки, розвиток емоційної стійкості. Результат – готовність діяти безпечно в умовах реального тиску. Checklist-аудит поведінки (індивідуальний або командний самоаналіз) сприяє формуванню навичок самоконтролю, виявленню поведінкових вразливостей, закріплює стандарти інформаційної гігієни. Результат – розвиток метакогнітивної компетентності та відповідальної поведінки. Інтерактивні лабораторії (цифрові інструменти, тестування, моделювання кіберсередовища) допомагають інтеграції технічних і психологічних аспектів безпеки, відпрацюванню навичок розпізнавання фішингових повідомлень, фейкових сайтів, розвивають цифрову грамотність. Результат – комплексна безпекова компетентність. Індивідуальні та групові вправи сприяють формуванню особистої відповідальності, розвитку командної взаємодії, тренуванню аргументації та безпечної комунікації. Результат – здатність застосовувати навички як автономно, так і в колективному середовищі. Отже, зазначений блок забезпечує перехід від знання "що таке соціоінженерна атака" до вміння "як розпізнати і як діяти".

Формування практичних навичок підсилюється третім блоком "Інформаційна безпека", мета якого сформувати правову, аналітичну та технологічну основу безпечної поведінки, що забезпечує усвідомлене розпізнавання загроз і впровадження ефективних механізмів захисту. Зазначений блок складається з опанування нормативно-правової бази, аналізу загроз, вивчення основ кібергігієни та визначення засобів захисту даних.

Опанування нормативно-правової бази починається з Конституції України як базового правового рівня, на якому ґрунтується все подальше законодавство про інформацію і дані. Документ гарантує право на приватність та захист персональних даних як невіддільну складову прав і свобод людини [2]. Закон України "Про захист персональних даних" регулює порядок обробки, використання і захисту персональних даних в Україні. Його положення встановлюють обов'язки контролерів даних і права суб'єктів даних (право на доступ до своїх даних, право на виправлення, обмеження обробки) та акцентують, що обробка даних без згоди особи заборонена, окрім випадків, прямо передбачених законом (національна безпека, правосуддя тощо) [6]. Закон України "Про електронні комунікації" визначає правові та організаційні основи діяльності у сфері електронних комунікацій, мереж і послуг, права й обов'язки учасників цього ринку та механізм державного регулювання [4]. Хоч він не є спеціальним актом про кібербезпеку чи захист інформації, його норми мають прямий вплив на інформаційну безпеку в мережах зв'язку. Закон забезпечує конфіденційність електронних комунікацій, встановлює обов'язок оператора застосовувати необхідні технічні та організаційні заходи захисту мереж та інформації, що передається чи зберігається в мережах електронних комунікацій. Зазначений Закон працює разом із Законом "Про захист інформації в інформаційно-комунікаційних системах", який встановлює вимоги до технічного

та організаційного захисту інформації в ІТ-середовищах [5]. Кримінальний кодекс України містить статті, що передбачають кримінальну відповідальність за несанкціонований доступ до інформації, витік даних, кіберзлочинність, що прямо стосується порушень інформаційної безпеки [3]. Кодекс України про адміністративні правопорушення передбачає адміністративну відповідальність за порушення правил обробки або захисту персональних даних (наприклад, за неправомірне використання чи розголошення) [1]. Таким чином, вивчення нормативно-правової бази з інформаційної безпеки забезпечує наступні компетентнісні результати: розуміння правових наслідків соціоінженерних атак, здатність діяти відповідно до норм і регламентів, формування культури відповідальності.

Аналіз загроз спрямований на формування в здобувачів освіти здатності системно оцінювати ризики соціоінженерних атак та приймати обґрунтовані рішення щодо їх мінімізації. Він включає такі складові як вразливості людини та організації, оцінка ймовірності та наслідків, моделювання сценаріїв ризиків. Вразливості людини та організації розглядаються через людський фактор як ключову ланку ризику (довірливість, неуважність, низький рівень цифрової грамотності, емоційна вразливість, схильність до маніпуляцій); психологічні механізми впливу, що використовуються у соціоінженерних атаках; організаційні вразливості (відсутність політик безпеки, слабкий контроль доступу, неналежне резервне копіювання, недостатній рівень навчання персоналу); технічні слабкі місця інфраструктури (незахищені мережі, застаріле програмне забезпечення, відсутність оновлень). Здобувачі освіти навчаються ідентифікувати типові “точки входу” загроз як на рівні особистості, так і на рівні установи. Оцінка ймовірності та наслідків здійснюється через визначення ймовірності реалізації загрози (частота атак, привабливість об’єкта, рівень захищеності); аналіз масштабу потенційних наслідків (фінансові втрати, репутаційні ризики, юридична відповідальність, витік персональних даних); використання якісних і кількісних підходів до оцінювання ризиків (матриця ризиків, шкала впливу, ранжування загроз). Здобувачі освіти вчаться співвідносити ризик із ресурсами захисту та визначати пріоритетність реагування. Моделювання сценаріїв ризику реалізується через побудову типових сценаріїв розвитку атаки (наприклад, фішинг → компрометація облікового запису → витік даних); аналіз ланцюга подій від виникнення загрози до її наслідків; визначення критичних точок, де можливе переривання сценарію; розроблення превентивних та реактивних заходів. Моделювання допомагає здобувачам не лише теоретично розуміти природу загроз, а й практично прогнозувати їх перебіг та планувати ефективні механізми запобігання. Таким чином, аналіз загроз соціоінженерних атак забезпечує такі компетентнісні результати як здатність ідентифікувати потенційні загрози, прогнозувати наслідки порушень безпеки, приймати рішення в умовах невизначеності, навички ризик-орієнтованого мислення.

Основи кібергігієни спрямовані на формування у здобувачів освіти стійких навичок безпечної поведінки в цифровому середовищі. Йдеться не лише про технічні знання, а й про щоденні практики, які мінімізують ризики соціоінженерних атак. Процеси кібергігієни включають безпечну роботу з паролями, багатофакторну автентифікацію, обережність щодо підозрілих повідомлень, управління цифровим слідом, безпечне використання публічних мереж. У межах безпечної роботи з паролями здобувачі опановують принципи створення складних і унікальних паролів (довжина, поєднання символів, відсутність особистих даних), недопустимості повторного використання одного пароля для різних сервісів, застосування менеджерів паролів, регулярного оновлення облікових даних, небезпечного зберігання паролів у відкритому вигляді або передачі їх третім особам. Формується розуміння, що пароль – це перша лінія захисту цифрової ідентичності. У межах багатофакторної автентифікації здобувачі вивчають принципи багатофакторної автентифікації (MFA) як поєднання щонайменше двох із трьох факторів: знання (пароль), володіння (смартфон, токен), біометрія (відбиток пальця, розпізнавання обличчя). Також розглядаються переваги MFA у запобіганні несанкціонованому доступу навіть у разі компрометації пароля, а також практичні аспекти налаштування таких механізмів у популярних цифрових сервісах. У межах обережності щодо підозрілих повідомлень відбувається розвиток навичок розпізнавання ознак фішингу (помилки в адресі відправника, терміновість, емоційний тиск, вкладення чи посилання невідомого походження), перевірки правдивості джерел інформації, безпечного відкриття файлів і переходу за посиланнями, повідомлення відповідальних осіб або служб про підозрілі інциденти. Акцент робиться на критичному мисленні та психологічній стійкості до маніпулятивних впливів. У межах управління цифровим слідом здобувачі усвідомлюють, що будь-яка активність у мережі формує цифровий профіль. Розглядаються налаштування конфіденційності в соціальних мережах, контроль доступу до персональної інформації, обмеження публікації чутливих даних, видалення застарілих або небажаних матеріалів, репутаційні ризики цифрової присутності. Формується відповідальне ставлення до власного онлайн-іміджу. У межах безпечного використання публічних мереж здобувачі опановують правила: уникнення передачі конфіденційної інформації через відкриті Wi-Fi мережі, використання захи-

щених з'єднань (HTTPS, VPN), вимкнення автоматичного підключення до мереж, перевірка справжності точки доступу, вихід з облікових записів після завершення роботи. Наголошується на тому, що публічні мережі є зоною підвищеного ризику, яка потребує особливої обережності. Таким чином, розуміння основ кібергігієни забезпечує наступні компетентнісні результати: формування щоденних безпечних звичок, зменшення поведінкових вразливостей, підвищення особистої цифрової стійкості.

Вивчення засобів захисту даних спрямоване на формування у здобувачів освіти розуміння технічних і організаційних механізмів забезпечення інформаційної безпеки. Засоби захисту включають: антивірусні рішення та фаєрволи, шифрування, резервне копіювання, системи контролю доступу, захист корпоративних інформаційних систем. Під час вивчення антивірусних рішень та фаєрволів розглядаються принципи роботи антивірусного програмного забезпечення, оновлення антивірусних баз, роль фаєрволів (міжмережевих екранів) у контролі вхідного та вихідного мережевого трафіку, налаштування правил доступу до мережевих ресурсів, інтеграція програмних і апаратних засобів захисту в єдину систему безпеки. Здобувачі усвідомлюють, що ці інструменти є першою технічною лінією оборони від шкідливого програмного забезпечення та несанкціонованих підключень. Тема шифрування формує у здобувачів розуміння, що навіть у разі перехоплення даних їх зміст залишається недоступним без ключа дешифрування. У процесі вивчення питань резервного копіювання здобувачі сприймають резервування як ключовий елемент забезпечення безперервності діяльності. Вивчаючи системи контролю доступу здобувачі вчаться визначати, хто, до яких ресурсів і на яких умовах має право доступу, а також як запобігати його зловживанню. Захист корпоративних інформаційних систем допомагає здобувачам зрозуміти, що такий захист є багаторівневим процесом, який поєднує технічні рішення, організаційні процедури та людський фактор. Таким чином, розуміння теми засобів захисту даних забезпечує наступні компетентнісні результати: розуміння технічних механізмів захисту, здатність обирати адекватні інструменти інформаційної безпеки, розуміння принципів побудови комплексної системи захисту даних в особистому й професійному середовищі.

Формування компетентностей розпізнавання та запобігання соціоінженерним атакам представлені трьома взаємопов'язаними результатами: захист від соціоінженерних атак, ефективна протидія маніпулятивному впливу, підвищення рівня індивідуальної та інституційної кібербезпеки. Захист проявляється як здатність здобувача освіти своєчасно розпізнати ознаки атаки, припинити взаємодію та мінімізувати можливі наслідки. Ефективна протидія маніпулятивному впливу характеризується не лише технічним захистом, а й психологічною стійкістю здобувачів. Вона забезпечує автономність прийняття рішень і знижує ризик імпульсивної поведінки під впливом зовнішнього тиску. Індивідуальна компетентність трансформується в елемент колективної безпеки де кожен учасник освітнього процесу стає складовою системи протидії загрозам. Таким чином, підвищується рівень довіри, зменшується кількість інцидентів і мінімізуються репутаційні та фінансові втрати.

Висновки. Сучасна освіта має стати простором позитивної соціальної інженерії, спрямованої на розвиток усвідомленої поведінки, аналітичного мислення та цифрової етики. Формування компетентностей розпізнавання соціоінженерних атак потребує інтеграції знань із психології, кібергігієни та педагогіки. Запропонована система є цілісною педагогічною системою формування у здобувачів вищої освіти компетентностей розпізнавання та запобігання соціоінженерним атакам. У сучасному цифровому середовищі ці компетентності стають невіддільною складовою професійної підготовки, елементом громадянської відповідальності та умовою стабільного функціонування освітніх і соціальних інституцій. Система має ієрархічну побудову з вертикальною спрямованістю (від змісту до результату) та горизонтальними міжблоковими зв'язками, що відображають інтеграцію навчального матеріалу, практичного досвіду та безпекових стандартів. Її використання в освітньому процесі забезпечує системність, послідовність і результативність формування компетентностей у сфері протидії соціоінженерним атакам. Загалом запропонована система може бути використана як методологічна основа для розроблення робочих програм дисципліни, критеріїв оцінювання результатів навчання та інструментів моніторингу сформованості відповідних компетентностей у здобувачів вищої освіти.

ЛІТЕРАТУРА

1. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X (редакція від 17.06.2025 № 4496-IX). URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 12.02.2026).

2. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.

3. Кримінальний кодекс України від 05.04.2001 № 2341-III (редакція від 17.07.2025 № 4499-IX). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 12.02.2026).

4. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX (редакція від 15.04.2025 № 4345-IX). URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 12.02.2026).

5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-

ВР (редакція від 27.03.2025 № 4336-IX). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 12.02.2026).

6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI (редакція від 12.02.2025 № 4240-IX). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 12.02.2026).

7. Соціальна інженерія та кіберпсихологія: монографія / авт. кол. : В.Г. Кононович, С.В. Стайкуца, М.М. Тодорова, С.В. Воронова, О.М. Рябуха. Одеса : ДУІТЗ, 2025. 388 с.

8. Ткач Т.В. Системний аналіз та соціальна інженерія як методи проектування освітнього простору. *Збірник наукових праць Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна "Проблеми економіки транспорту".* 2013. № 5. С. 30–36.

9. Цуркан О.В., Герасимов Р.П., Крук О.М. Методи протидії використанню соціальної інженерії. *Information Technology and Security.* 2019. Vol. 7. Iss. 2 (13). С. 161–170. DOI 10.20535/2411-1031.2019.7.2.190563.

10. Cialdini R. B. Influence: The Psychology of Persuasion. New York : Harper Business, 2006. 320 p.

11. Hadnagy C. Social Engineering: The Science of Human Hacking. Indianapolis : Wiley Publishing, 2011. 416 p.

12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : International Organization for Standardization, 2022. 34 p.

13. Mitnick K.D., Simon W.L. The Art of Deception: Controlling the Human Element of Security. New York : Wiley, 2002. 352 p.

REFERENCES

1. Kodeks Ukrainy pro administratyvni pravoporushennia vid 07.12.1984 № 8073-X (redaktsiia vid 17.06.2025 № 4496-IX) [Code of Ukraine on Administrative Offenses dated 07.12.1984 No. 8073-X (edition dated 17.06.2025 No. 4496-IX)] Available at: https://zakon.rada.gov.ua/laws/show/80731-10#Text (Accessed 12 Feb. 2026). [in Ukrainian].

2. Konstytutsiia Ukrainy : ofits. tekst [Constitution of Ukraine: official text]. Kyiv, 2013. 96 p. [in Ukrainian].

3. Kryminalnyi kodeks Ukrainy vid 05.04.2001 № 2341-III (redaktsiia vid 17.07.2025 № 4499-IX) [Criminal Code of Ukraine dated 05.04.2001 No. 2341-III (edition dated 17.07.2025 No. 4499-IX)]. Available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text (Accessed 12 Feb. 2026). [in Ukrainian].

4. Pro elektronni komunikatsii: Zakon Ukrainy vid 16.12.2020 № 1089-IX (redaktsiia vid 15.04.2025 № 4345-IX) [On electronic communications: Law of Ukraine dated 16.12.2020 No. 1089-IX (edition dated 15.04.2025 No. 4345-IX)]. Available at: https://zakon.rada.gov.ua/laws/show/1089-20#Text (Accessed 12 Feb. 2026). [in Ukrainian].

5. Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: Zakon Ukrainy vid 05.07.1994 № 80/94-VR (redaktsiia vid 27.03.2025 № 4336-IX) [On the protection of information in information and communication systems: Law of Ukraine dated 05.07.1994 No. 80/94-VR (edition dated 27.03.2025 No. 4336-IX)]. Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (Accessed 12 Feb. 2026). [in Ukrainian].

6. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 № 2297-VI (redaktsiia vid 12.02.2025 № 4240-IX) [On the protection of personal data: Law of Ukraine dated 01.06.2010 No. 2297-VI (edition dated 12.02.2025 No. 4240-IX)]. Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Accessed 12 Feb. 2026). [in Ukrainian].

7. Sotsialna inzheneriia ta kiberpsykholohiia : monohrafiia [Social Engineering and Cyberpsychology: monograph] / team of authors : V.H. Kononovych, S.V. Staikutsa, M.M. Todorova, S.V. Voronova & O.M. Riabukha. Odesa, 2025. 388 p. [in Ukrainian].

8. Tkach T.V. (2013). Systemnyi analiz ta sotsialna inzheneriia yak metody proektuvannia osvitnoho prostoru [Systems analysis and social engineering as methods of designing educational space]. *Collection of scientific works of the Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan "Problems of Transport Economics",* No. 5, pp. 30–36. [in Ukrainian].

9. Tsurkan, O.V., Herasymov, R.P. & Kruk, O.M. (2019). Metody protydii vykorystanniu sotsialnoi inzhenerii. *Information Technology and Security.* Vol. 7. Iss. 2 (13). p. 161–170. DOI 10.20535/2411-1031.2019.7.2.190563. [in Ukrainian].

10. Cialdini, R.B. (2006). Influence: The Psychology of Persuasion. New York : Harper Business. 320 p. [in English].

11. Hadnagy, C. (2011). Social Engineering: The Science of Human Hacking. Indianapolis : Wiley Publishing. 416 p. [in English].

12. ISO/IEC 27001:2022 (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : International Organization for Standardization. 34 p. [in English].

13. Mitnick, K.D. & Simon W.L. (2002). The Art of Deception: Controlling the Human Element of Security. New York, 352 p. [in English].

Стаття надійшла до редакції: 18.02.2026
Прийнято до друку:16.04.2026
Опубліковано: 04.05.2026

"Найкраща помилка та, якої допускаються у навчанні".

Григорій Сковорода
український філософ, педагог

"Вміння вести розмову – це талант".

Стендаль
французький письменник