

Scientific journal
PHYSICAL AND MATHEMATICAL EDUCATION
Has been issued since 2013.

ISSN 2413-158X (online)
ISSN 2413-1571 (print)

Науковий журнал
ФІЗИКО-МАТЕМАТИЧНА ОСВІТА
Видається з 2013.



<http://fmo-journal.fizmatsspu.sumy.ua/>

Глазунова О.Г., Касаткіна О.М., Корольчук В.І., Саяпіна Т.П., Волошина Т.В. Формування навичок цифрової безпеки у студентів економічних спеціальностей: процедури, інструменти, сервіси. *Фізико-математична освіта*. 2021. Випуск 2(28). С. 34-39.

Glazunova O., Kasatkina O., Korolchuk V., Saiapina T., Voloshyna T. Formation of digital security skills in students of economic specialties: procedures, tools, services. *Physical and Mathematical Education*. 2021. Issue 2(28). P. 34-39.

DOI 10.31110/2413-1571-2021-028-2-006
УДК 004.67-049.5:378-057.87:330

О.Г. Глазунова

Національний університет біоресурсів і природокористування України, Україна
o-glazunova@nubip.edu.ua
ORCID: 0000-0002-0136-4936

О.М. Касаткіна

Національний університет біоресурсів і природокористування України, Україна
olga_kasat@nubip.edu.ua
ORCID: 0000-0002-3952-9046

В.І. Корольчук

Національний університет біоресурсів і природокористування України, Україна
korolchuk@nubip.edu.ua
ORCID: 0000-0002-3145-8802

Т.П. Саяпіна

Національний університет біоресурсів і природокористування України, Україна
t_sayapina@nubip.edu.ua
ORCID: 0000-0001-9905-4268

Т.В. Волошина

Національний університет біоресурсів і природокористування України, Україна
t-voloshina@nubip.edu.ua
ORCID: 0000-0001-6020-5233

ФОРМУВАННЯ НАВИЧОК ЦИФРОВОЇ БЕЗПЕКИ У СТУДЕНТІВ ЕКОНОМІЧНИХ СПЕЦІАЛЬНОСТЕЙ: ПРОЦЕДУРИ, ІНСТРУМЕНТИ, СЕРВІСИ

АНОТАЦІЯ

Формулювання проблеми. В сучасних умовах цифровізації суспільства навичками цифрової безпеки повинні володіти фахівці будь-якої сфери діяльності, у тому числі в галузі економіки. Проблема полягає у тому, що розвиток цифрової економіки висуває перед закладами освіти завдання змінювати програми підготовки та вводити до них вивчення сучасних інформаційних технологій, без володіння якими неможливо стати висококваліфікованим фахівцем зокрема в галузі економіки.

Матеріали і методи. Здійснено класифікацію та систематизацію наукових джерел; проведено аналіз інструментів гібридного хмаро орієнтованого навчального середовища закладу вищої освіти для використання в процесі формування навичок цифрової безпеки майбутніх економістів. Експериментальною базою дослідження є Національний університет біоресурсів і природокористування України, в експерименті взяли участь студенти спеціальності «Економіка» закладу вищої освіти, загальна кількість учасників – 143 особи.

Результати. Запропоновано процедури використання інструментів гібридного хмаро орієнтованого навчального середовища для формування навичок цифрової безпеки майбутніх економістів, а саме: процедура 1. Використання масові відкриті онлайн курси та сервіси цифрової безпеки для формування рівня навичок «Цифрове громадянство»; процедура 2. Використання інструментів для спільної роботи для формування рівня навичок «Цифрова творчість»; процедура 3. Використання сервісів для управління, обліку та аналізу даних для формування рівня навичок «Цифрове підприємництво».

Висновки. За результатами експериментальних досліджень у студентів спеціальності 051 «Економіка» підвищуються навички цифрової безпеки за трьома рівнями: цифровий громадянин, цифровий творець, цифровий підприємець завдяки інтеграції в освітній процес інструментів гібридного хмаро орієнтованого навчального середовища закладу вищої освіти, а саме: масових відкритих онлайн курсів, сервісів цифрової безпеки, інструментів для спільної роботи, сервісів для управління, обліку й аналізу.

КЛЮЧОВІ СЛОВА: цифрова безпека, «цифрове громадянство», «цифрова творчість», «цифрове підприємництво», майбутні фахівці з економіки.

ВСТУП

Постановка проблеми. Цифрова безпека є предметом вивчення у закладі вищої освіти (ЗВО) для студентів технічних спеціальностей. Але на сьогодні навички цифрової безпеки необхідні фахівцю будь-якої галузі, у тому числі в галузі економіки. Проблема полягає у тому, що розвиток цифрової економіки висуває перед закладами освіти завдання змінювати програми підготовки та вводити до них вивчення сучасних інформаційних технологій, без володіння якими неможливо стати фахівцем в галузі економіки. Саме цифрова безпека відноситься до таких технологій, які надзвичайно важливі у підготовці сучасного економіста. На даний час недостатньо обґрунтовано зміст навчання та процедури використання ресурсів і сервісів е-середовища ЗВО для вивчення технологій цифрової безпеки при підготовці майбутніх економістів.

Аналіз актуальних досліджень. Визначення поняття «цифрова безпека» та формування навичок інформаційної (цифрової) безпеки у майбутніх фахівців різних галузей розглянуто у працях таких дослідників: М. Доделя (M. Dodel) та Г. Меш (G. Mesch), Дж. Достала (J. Dostal), Х. Ванга (X. Wang), В. Штейнгартнера (W. Steingartner), П. Нуангчалерма (P. Nuangchalerm), В. Олексюка та О. Олексюк (формування компетентностей з інформаційної безпеки майбутніх учителів інформатики), В. Бондаренко (формування навичок інформаційної безпеки майбутніх учителів).

Дж. Достал (J. Dostal), Х. Ванг (X. Wang), В. Штейнгартнер (W. Steingartner), П. Нуангчалерм (P. Nuangchalerm) трактують поняття «цифрова безпека» як здатність виявляти кіберзагрози (наприклад, злом, шахрайство, шкідливі програмні забезпечення) та використовувати відповідні інструменти безпеки для захисту даних.

Серед останніх досліджень формуванню цифрових навичок майбутніх економістів з використанням сервісів і ресурсів інформаційно-освітнього середовища присвячені праці: В. Зінченко, Р. Манна, О. Кравченко та І. Ганжали, В. Бондаренко.

Р. Манном, О. Кравченко та І. Ганжалою запропоновано доступні для використання в освітньому процесі мобільні додатки, які спрямовані на підвищення якості та ефективності оволодіння економічними знаннями для забезпечення їх подальшого працевлаштування за спеціальністю (Манн, Кравченко, Ганжала, 2020). В. Бондаренко зазначає, що процес формування навичок інформаційної безпеки здебільшого орієнтований на виявлення інформаційних загроз та оволодіння прийомами безпечної поведінки в професійній діяльності (Бондаренко, 2019).

Сутність поняття та можливості використання хмаро орієнтованого навчального середовища у своїх дослідженнях розглядають такі вчені: В. Биков, Т. Вакалюк, О. Глазунова, С. Литвинова, А. Salam, N. Sardar, O. Saad, M. Rana, M. Шишкіна та ін. У статті розглянуто поняття хмарно-орієнтованого освітнього наукового середовища ЗВО (Глазунова, Шишкіна, 2018). У нашому подальшому дослідженні під гібридним хмаро орієнтованим навчальним середовищем (ГХОНС) будемо розуміти ІКТ-середовище, що функціонує на основі технологій хмарних обчислень та поєднує дидактично обґрунтоване використання навчальних ресурсів і сервісів академічної хмари закладу освіти та загальнодоступних хмар (Волошина, 2018). Таке ГХОНС ЗВО спроектовано в Національному університеті біоресурсів і природокористування України (НУБіП України), у якому інтегровано різні ресурси та сервіси, які використовують для підготовки фахівців різних галузей (Глазунова, Волошина, Корольчук 2020; Волошина 2018)

Мета статті. Обґрунтувати процедури використання інструментів ГХОНС з використанням масових відкритих онлайн курсів (МВОК) і сервісів цифрової безпеки; інструментів для спільної роботи; сервісів для управління, обліку та аналізу даних, що сприятиме формуванню навичок цифрової безпеки майбутніх економістів.

МЕТОДИ ДОСЛІДЖЕННЯ

Для вирішення поставленої мети використовувалися такі методи дослідження: аналіз і узагальнення науково-педагогічної літератури з метою розкриття основних понять досліджуваної проблеми; класифікація та систематизація теоретичних даних; аналіз інструментів ГХОНС ЗВО для використання в процесі викладання дисципліни «Інформаційні системи та технології в економіці» з метою формування навичок цифрової безпеки майбутніх економістів; статистичні методи опрацювання результатів оцінювання рівня цифрової безпеки студентів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Суть методики полягає у використанні інструментів ГХОНС для формування навичок цифрової безпеки майбутніх економістів відповідно до визначених процедур.

Процедура 1. Використання МВОК і сервісів цифрової безпеки для формування рівня навичок «Цифрове громадянство» (ЦГ) (здатність розпізнавати та ліквідувати технічні та програмні кіберзагрози на рівні операційної системи, роботи у мережі, роботи з персональними даними та авторським контентом).

Процедура 2. Використання інструментів для спільної роботи для формування рівня навичок «Цифрова творчість» (ЦТ) (здатність планувати та впроваджувати засоби захисту кібербезпеки при створенні цифрового контенту, організація безпеки даних та робочих інформаційних систем).

Процедура 3. Використання сервісів для управління, обліку та аналізу даних для формування рівня навичок «Цифрове підприємництво» (ЦП) (здатність організувати безпечне інформаційне середовище для організації бізнесу).

Процедури методики інструментів ГХОНС, що формують навички цифрової безпеки майбутніх економістів наведено на рис. 1.

Перша процедура передбачає інтеграцію МВОК і сервісів цифрової безпеки у електронний навчальний курс (ЕНК) з дисципліни «Інформаційні системи та технології в економіці». Для самостійного опрацювання в межах змістовного модуля «Цифрова безпека: захист у цифровому середовищі» студентам рекомендуються відібрані академічні онлайн ресурси, такі як: Cisco Acsdemy, Prometheus, Udemy, Academy Khana; фахові інтернет-ресурси: блоги, форуми, сайти фахового спрямування, соціальні мережі, публічні платформи, офіційні джерела інформації та сервіси для цифрової безпеки, а саме: безпека мереж: сканери вразливості мережі Wireshark, Cain&Avel; онлайн сканери портів Nmap, File2rcar; безпека програм: сервіси для аналізу шифрування файлів і даних PE-SIG, TeslaCrypt Description Tool; антивірусні програми Windows Defender, AVG, Comodo, NOD32; безпека вебдодатків: онлайн інструменти для сканування вразливості вебсайту Sucuri, Qualys, UpGuard; онлайн тест на сервер SSL OnlineServer SSL Test, SSL Labs by Qualys, SSL Checker.

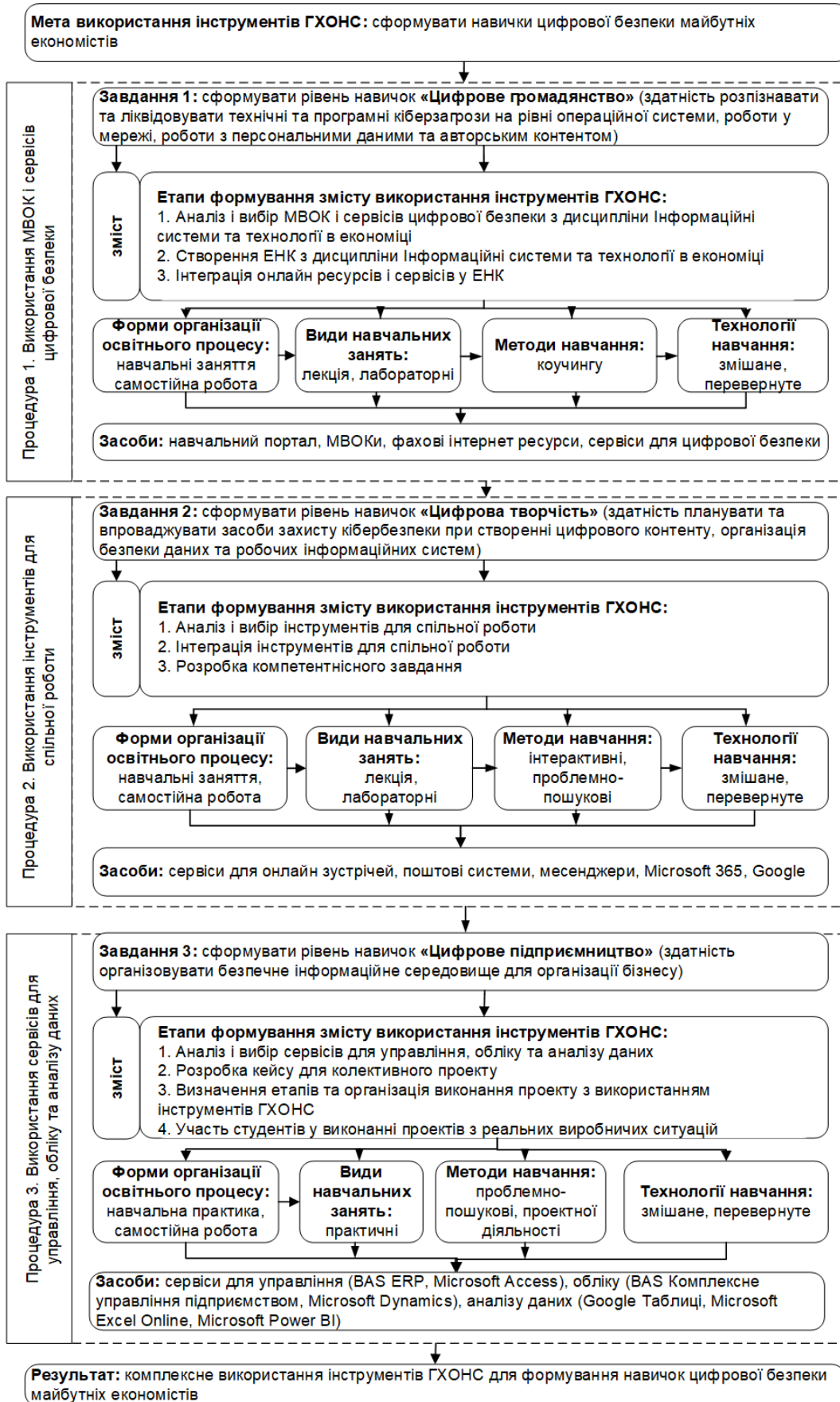


Рис. 1. Структура методики використання інструментів ГХОНС для формування навичок цифрової безпеки майбутніх економістів

В результаті у студентів формується здатність розпізнавати та ліквідувати технічні та програмні кіберзагрози на рівні операційної системи, роботи у мережі, роботи з персональними даними та авторським контентом. При цьому формування змісту навчання здійснюється відповідно до таких етапів:

1. Аналіз і вибір онлайн ресурсів і сервісів з дисципліни Інформаційні системи та технології в економіці (НПП, який відповідає за викладання навчальної дисципліни, аналізує додаткові онлайн курси, обирає фахові інтернет-ресурси та сервіси для цифрової безпеки для включення до робочої програми дисципліни).

2. Створення ЕНК з дисципліни Інформаційні системи та технології в економіці (НПП створює ЕНК відповідно до робочої програми дисципліни).

3. Інтеграція онлайн ресурсів і сервісів у ЕНК (під час лекцій та лабораторних робіт студентів знайомлять з різними фаховими інтернет-ресурсами та зміст лабораторних робіт передбачає виконання завдань з використанням відповідних сервісів для цифрової безпеки, у завданнях для самостійної роботи розміщується посилання на відповідні онлайн курси та визначається максимальна кількість балів для оцінювання результатів з його проходження).

Для організації навчальної діяльності використовуються технології змішаного та перевернутого навчання. Додатковий навчальний матеріал вивчається студентами під час самостійної роботи. При цьому активно застосовується метод коучингу, оскільки здійснюється персоналізоване навчання кожного студента. Викладач консультує з приводу вибору наступних курсів, фахових інтернет-ресурсів та сервісів для цифрової безпеки, які можуть бути корисними для студента та надалі у професійній діяльності.

Другою процедурою є використання інструментів для спільної роботи, що доступні у межах IT-інфраструктури університету (хмарні сервіси Google та Microsoft 365 в межах корпоративного акаунту @it.nubip.edu.ua). Розробляючи компетентнісне завдання для спільної роботи студентів, викладач рекомендує використовувати та знайомить їх з можливостями різних сервісів і платформ, що доступні в межах ГХОНС ЗВО. Таким чином, у майбутніх економістів формується здатність планувати та впроваджувати засоби захисту кібербезпеки при створенні цифрового контенту, організація безпеки даних та робочих інформаційних систем. Зміст навчання формується за такими етапами:

1. Аналіз і вибір інструментів для спільної роботи (НПП, який відповідає за викладання навчальної дисципліни, аналізує доступні хмарні сервіси в межах ліцензійних угод для включення до робочої програми дисципліни).

2. Інтеграція інструментів для спільної роботи (НПП інтегрує хмарні сервіси Google та Microsoft 365 відповідно до робочої програми дисципліни)

3. Розробка компетентнісного завдання (НПП розробляє завдання для виконання групового проєктного завдання розміщуючи у завданнях для лабораторної роботи посилання на хмарну платформу або ж сервіс та визначається максимальна кількість балів для оцінювання результатів з його виконання).

Під час цієї процедури використовуються інтерактивні та проблемно-пошукові методи навчання, які дають можливість співпрацювати зі студентами та формувати у них здатність планувати та впроваджувати засоби захисту кібербезпеки при створенні цифрового контенту, організація безпеки даних та робочих інформаційних систем.

Третьою процедурою забезпечується використання сервісів для управління, обліку й аналізу даних з використанням інструментів ГХОНС, а саме: сервісів для управління (ERP-системи, Microsoft Access, обліку (1С:Підприємство, Microsoft Dynamics) та аналізу даних (Google Таблиці, Microsoft Excel Online, Microsoft Power BI). Таким чином, у студентів формується рівень навичок «Цифрове підприємництво» (здатність організувати безпечне інформаційне середовище для організації бізнесу). Щоб сформувати зміст навчання під час організації цієї процедури методики, необхідно здійснити такі етапи:

1. Аналіз і вибір сервісів для управління, обліку й аналізу даних (НПП, який відповідає за викладання навчальної дисципліни, аналізує відповідні інструменти та включає до робочої програми дисципліни Інформаційні системи та технології в економіці).

2. Розробка кейсу для колективного проєкту (НПП спільно з стейкхолдерами розробляє кейс з реальних виробничих ситуацій для виконання колективного проєкту відповідно до робочої програми дисципліни).

3. Визначення етапів та організація виконання проєкту з використанням інструментів ГХОНС (НПП визначає етапи виконання проєкту відповідно до запропонованого студентам завдання, організовує та супроводжує його виконання з використанням інструментів ГХОНС).

4. Участь студентів у виконанні проєктів з реальних виробничих ситуацій (студент обирає та долучається до фахових інтернет-ресурсів, а саме: блогів, форумів, сайтів фахового спрямування, соціальних мереж, публічних платформ та офіційних джерел інформації).

Основними методами навчання під час цієї процедури будуть проблемно-пошукові та проєктної діяльності.

ОБГОВОРЕННЯ

Педагогічний експеримент проходив на базі економічного факультету НУБіП України протягом 3 років, засвідчив позитивні зміни у рівні формування навичок цифрової безпеки у майбутніх економістів. В процесі дослідження було висунуто припущення про те, що використання компонентів ГХОНС протягом трьох етапів впливає на формування навичок цифрової безпеки.

На кожному етапі методики формування навичок цифрової безпеки відповідно до розробленої методики пропонувалося вирішити відповідне завдання. В результаті до експерименту та після кожного етапу було визначено кількість студентів, які не можуть виконати жодного завдання з запропонованих рівнів, кількість студентів з рівнем сформованості «цифровий громадянин», «цифровий творець» та «цифровий підприємець».

Для перевірки висунутого припущення було сформульовано нульову гіпотезу, відхилення якої підтвердить ефективність запропонованих технологій навчання: використання компонентів ГХОНС ЗВО не впливає на рівень навичок цифрової безпеки, тобто наявні зміни випадкові.

Для статистичного підтвердження даного припущення, було використано таблицю спряженості та критерій узгодженості Пірсона χ^2 .

В таблиці 1 згруповані результати оцінювання рівня навичок цифрової безпеки за чотирьома рівнями залежно від використання інструментів ГХОНС ЗВО, а також очікувані (теоретичні) частоти при умові відсутності відмінностей між рівнями навичок цифрової безпеки в експериментальних групах.

Таблиця 1

Таблиця спряженості рівнів навичок цифрової безпеки майбутніх економістів

Етап проведення експерименту	Рівень цифрової безпеки	Емпірична частота (f_e)	Теоретична частота (f_t)	$f_e - f_t$	$(f_e - f_t)^2$	$\frac{(f_e - f_t)^2}{f_t}$
До експерименту	Не виконали завдання	91	33,5	57,5	3306,25	98,69
	Рівень ЦГ	24	46,25	-22,25	495,06	10,70
	Рівень ЦТ	19	35,5	-16,5	272,25	7,67
	Рівень ЦП	9	27,75	-18,75	351,56	12,67
I етап	Не виконали завдання	21	33,5	-12,5	156,25	4,66
	Рівень ЦГ	89	46,25	42,75	1827,56	39,52
	Рівень ЦТ	22	35,5	-13,5	182,25	5,13
	Рівень ЦП	11	27,75	-16,75	280,56	10,11
II етап	Не виконали завдання	15	33,5	-18,5	342,25	10,22
	Рівень ЦГ	43	46,25	-3,25	10,56	0,23
	Рівень ЦТ	68	35,5	32,5	1056,25	29,75
	Рівень ЦП	17	27,75	-10,75	115,56	4,16
III етап	Не виконали завдання	7	33,5	-26,5	702,25	20,96
	Рівень ЦГ	29	46,25	-17,25	297,56	6,43
	Рівень ЦТ	33	35,5	-2,5	6,25	0,18
	Рівень ЦП	74	27,75	46,25	2139,06	77,08
Сума		572	572	-	-	338,18

Для розрахунку теоретичної частоти розподілу частот було застосовано формулу $f_t = \frac{f_e f_r}{n}$, де f_e – загальна частота одного рівня за результатами усіх етапів; f_r – загальна частота усіх рівнів за результатами одного етапу експерименту; n – загальна кількість проведених вимірів.

Для статистичної оцінки отриманих результатів було розраховано критерій узгодженості Пірсона за формулою $\chi^2 = \sum \frac{(f_e - f_t)^2}{f_t}$, де f_e – емпірична частота та f_t – теоретична частота. Розрахунковий χ^2 становить 338,18, критичне значення критерію Пірсона χ^2 при числі ступенів свободи 9 дорівнює 21.666. Так як $\chi^2_{\text{розрах}} > \chi^2_{\text{крит}}$, можна зробити висновок, що отримані результати є статистично значущими ($p = 0.01$). Відповідно нами було відхилено нульову гіпотезу та прийнята альтернативна гіпотезу: використання компонентів ГХОНС впливає на рівень навичок цифрової безпеки.

До початку експерименту 16,8% студентів отримали рівень «Цифровий громадянин», 13,3% – рівень «Цифровий творець» та 3,6% – рівень «Цифровий підприємець», інші студенти не змогли виконати компетентнісні завдання. За результатами трьох етапів кількість студентів, які отримали рівень «Цифровий громадянин» зросла на 3,5%, «Цифровий творець» – 9,8%, «Цифровий підприємець» – 45,4%. Проміжні результати отримані після кожного етапу представлені на рисунку 2.

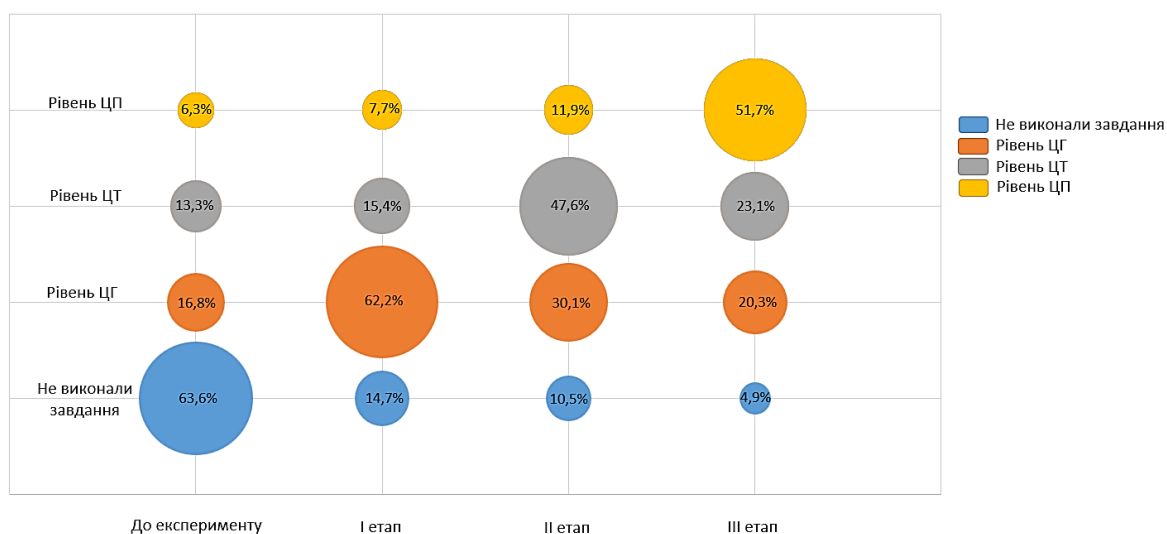


Рис. 2. Діаграма рівнів сформованості навичок цифрової безпеки майбутніх економістів

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШОГО ДОСЛІДЖЕННЯ

Таким чином, обґрунтовані та розроблені процедури базуються на використанні таких інструментів ГХОНС ЗВО для формування навичок цифрової безпеки майбутніх економістів: навчальний портал, МВОКи, фахові інтернет ресурси, сервіси для цифрової безпеки; сервіси для онлайн зустрічей, поштової системи, месенджери, хмарні сервіси Microsoft 365, Google; сервіси для управління (BAS ERP, Microsoft Access), обліку (BAS Комплексне управління підприємством, Microsoft Dynamics), аналізу даних (Google Таблиці, Microsoft Excel Online, Microsoft Power BI). Розглянутий спектр реалізації наведених процедур використання ГХОНС в процесі підготовки майбутніх економістів в рамках викладання дисципліни Інформаційні системи та технології в економіці, їх подальша експериментальна перевірка дає підстави стверджувати про доцільність їх застосування в освітньому процесі для формування навичок цифрової безпеки у студентів спеціальності 051 «Економіка».

Перспективами подальшого дослідження є розробка методики подальшого розвитку навичок цифрової безпеки під час викладання професійно-орієнтованих дисциплін.

Список використаних джерел

1. Бондаренко В.І. Умови та засоби формування навичок інформаційної безпеки майбутніх учителів. *Інформаційні технології і засоби навчання*, 2019. Том 74 (6). С. 294-306.
2. Манн Р., Кравченко О., Ганжала І. Використання інформаційно-комунікаційних технологій як елемент інноваційного навчання фахівців економічного спрямування, *Інформаційні технології і засоби навчання*, 2020. Том 78 (4). С. 145-162. URL: <https://journal.iitta.gov.ua/index.php/itlt/article/view/2810>. (Дата звернення 17.01.2021)
3. Волошина Т.В. Використання гібридного хмаро орієнтованого навчального середовища для формування самоосвітньої компетентності майбутніх фахівців з інформаційних технологій, дис. канд. пед. наук: Інститут інформаційних технологій і засобів навчання НАПН України, Київ, 2018.
4. Glazunova, O., Shyshkina, M.: The Concept, Principles of Design and Implementation of the University Cloud-based Learning and Research Environment, 2018, Vol. 2104. URL: http://ceurws.org/Vol-2104/paper_158.pdf. (Дата звернення 17.01.2021)
5. Glazunova, O., Voloshyna T., Korolchuk V.: Hybrid cloud-oriented learning environment for IT student project teamwork, *Information technology and learning tools*, 2020. Vol. 77 (3). pp. 114-129. URL: <https://journal.iitta.gov.ua/index.php/itlt/article/view/2810>. (Дата звернення 17.01.2021)

References

1. Bondarenko V.I. (2019). Umovy ta zasoby formuvannia navychok informatsiinoi bezpeky maibutnix uchyteliv [Conditions and means of formation of information security skills of future teachers]. *Informatsiini tekhnolohii i zasoby navchannia*, 74 (6), 294-306 [in Ukrainian].
2. Mann R., Kravchenko O., Hanzhala I. (2020) Vykorystannia informatsiino-komunikatsiinykh tekhnolohii yak element innovatsiinoho navchannia fakhivtsiv ekonomichnoho spriamuvannia [The use of information and communication technologies as an element of innovative training of economic specialists]. *Informatsiini tekhnolohii i zasoby navchannia*, 78 (4), 145-162. Retrieved from <https://journal.iitta.gov.ua/index.php/itlt/article/view/2810> [in Ukrainian].
3. Voloshyna T.V. (2018) Vykorystannia hibrydnoho khmaro oriientovanoho navchalnoho seredovishcha dlia formuvannia samoosvitnoi kompetentnosti maibutnix fakhivtsiv z informatsiinykh tekhnolohii [The use of a hybrid cloud-based learning environment for the formation of self-educational competence of future information technology professionals] (Candidate's dissertation). Instytut informatsiinykh tekhnolohii i zasobiv navchannia NAPN Ukrainy [in Ukrainian].
4. Glazunova, O., Shyshkina, M. (2018). The Concept, Principles of Design and Implementation of the University Cloud-based Learning and Research Environment. Retrieved from http://ceurws.org/Vol-2104/paper_158.pdf.
5. Glazunova, O., Voloshyna T., Korolchuk V. (2020). Hybrid cloud-oriented learning environment for IT student project teamwork, *Information technology and learning tools*. 77 (3), 114-129. Retrieved from <https://journal.iitta.gov.ua/index.php/itlt/article/view/2810>.

FORMATION OF DIGITAL SECURITY SKILLS IN STUDENTS OF ECONOMIC SPECIALTIES: PROCEDURES, TOOLS, SERVICES

O.G. Glazunova, O.M. Kasatkina, V.I. Korolchuk, T.P. Saiapina, T.V. Voloshyna
National University of Life and Environmental Sciences of Ukraine, Ukraine

Abstract. Formulation of the problem. Modern digitalization of society, digital security skills must be possessed by specialists in any sphere, including economics. The problem is that the development of the digital economy sets before educational institutions the task of changing training programs and introducing the study of modern information technologies, without which it is impossible to become a highly qualified specialist in particular in the economics.

Materials and methods. Classification and systematization of scientific sources is carried out; the analysis of HCBLE tools of the institution of higher education (HEI) for use in the process of formation of digital security skills of future economists is carried out. The experimental basis of the study is NULES of Ukraine, the experiment was attended by students in specialty "Economics" of higher education, the total number of participants - 143 people.

Results. Procedures for using hybrid cloud-based learning tools for the formation of digital security skills of future economists are proposed, namely: procedure 1. Using mass open online courses and digital security services to develop the level of skills "Digital Citizenship"; procedure 2. Using tools for teamwork to develop the level of skills "Digital Creativity"; procedure 3. Use of services for management, accounting and data analysis to form the level of skills "Digital Entrepreneurship".

Conclusions. According to the results of experimental research, students in specialty 051 "Economics" improve digital security skills at three levels: digital citizen, digital creator, digital entrepreneur through the integration into the educational process of tools hybrid cloud-based learning environment of higher education, namely: mass open online courses, digital security services, collaboration tools, management, accounting and analysis services.

Key words: digital security, "digital citizenship"; "digital creativity"; "digital entrepreneurship"; future specialists in economics.

