УДК 378.147.011.3-051:004

**Бондаренко Володимир Іванович**
доктор педагогічних наук, доцент,
завідувач кафедри загальнотехнічних дисциплін, безпеки життєдіяльності та автосправи
ДВНЗ «Донбаський державний педагогічний університет», м. Слов'янськ, Україна
ORCID ID 0000-0002-8359-884X
*vibondarenko1287@gmail.com*

# УМОВИ ТА ЗАСОБИ ФОРМУВАННЯ НАВИЧОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МАЙБУТНІХ УЧИТЕЛІВ

**Анотація.** Статтю присвячено дослідженню умов та засобів формування навичок інформаційної безпеки, яке є актуальним у сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій. Проведений аналіз наукової літератури доводить: збільшення об'єму та способів передачі інформації, полегшення доступу до різних інформаційних джерел, а також зростання інтересу до застосування ІКТ в освітньому процесі обумовлює актуальність досліджуваної проблеми. У статті представлено докладний аналіз понять «кібербезпека», «е-безпека», «цифрова безпека», на основі яких визначено зміст дефініції «інформаційна безпека». Особливу увагу приділено змісту навичок інформаційної безпеки, які розподілено на три групи: функціональні, комунікативні та навички критичного мислення. Зазначено, що умовами формування інформаційної безпеки є сукупність змісту інформаційної підготовки та аспектів інформаційної безпеки, а також інформаційних форм і засобів її реалізації в освітньому процесі. Автором доведено, що ефективним засобом формування навичок інформаційної безпеки є створення навчального середовища у ВНЗ. Представлено досвід упровадження навчального курсу, створеного на базі системи Moodle, яка є найбільш поширеною у вишах країни, безпечною та легко інтегрується з хмарними сервісами, що дозволяє створити репозиторій навчальних матеріалів. Під час розробки навчального модуля для формування навичок інформаційної безпеки особливу увагу сфокусовано на такому аспекті: формування навичок інформаційної безпеки є складовою частиною фахової компетентності майбутніх учителів, що вимагає залучення життєвого і професійного досвіду студентів для вирішення навчальних завдань. У статті представлено дані експериментальної перевірки впроваджуваного модуля, які підтверджують його ефективність.

**Ключові слова:** інформаційна безпека; цифрова грамотність; безпека життєдіяльності; майбутні вчителі, система Moodle.

## 1. ВСТУП

**Постановка проблеми.** Стрімкий розвиток інформаційних технологій має значний вплив на всі сфери життєдіяльності людини та змінює свідомість громадян. Процеси інформатизації в галузі освіти є визначальними для подальшого розвитку економіки, науки і культури країни. В умовах стрімкого поширення інформації особливого значення набувають питання захисту громадян від небезпечних інформаційних впливів, адже вони здатні трансформувати свідомість як окремої людини, так і суспільства в цілому. Інформаційним захистом громадян на сьогодні опікується держава, що відображено в таких нормативно-правових документах: Доктрина національної безпеки від 29 грудня 2016 року, «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Забезпечення інформаційної безпеки не може реалізовуватися лише фахівцями в галузі безпеки. До процесів забезпечення належного рівня інформаційної безпеки в усіх сферах життєдіяльності, разом з освітньою, слід безпосередньо залучати фахівців, які виконують професійну інформаційну діяльність

(збір, передачу, зберігання, обробку та використання інформації), що вимагає певних знань та навичок забезпечення інформаційної безпеки широкого кола користувачів сучасних інформаційно-комунікаційних технологій. Тому ефективне вирішення проблем інформаційної безпеки вимагає підготовки висококваліфікованих фахівців різних спеціальностей, які володіють необхідними знаннями та навичками забезпечення інформаційної безпеки своєї професійної діяльності, зокрема в галузі освіти та педагогіки. Отже, у вищих педагогічних навчальних закладах у межах навчальної дисципліни «Безпека життєдіяльності» відповідно до навчальної програми слід проводити цілеспрямоване формування навичок інформаційної безпеки в системі професійної підготовки майбутніх учителів, бо саме в сучасних реаліях тривають процеси формування інтелектуального потенціалу нашої країни, а широке застосування новітніх Інтернет-технологій вимагає підвищення якості сучасної освіти та оволодіння майбутніми спеціалістами навичками ефективного та безпечного користування ІКТ.

**Аналіз останніх досліджень і публікацій.** Дослідження в сфері інформаційної безпеки до недавнього часу проводилися лише у військових навчальних закладах, а інформація про такі дослідження і педагогічний досвід формування навичок інформаційної безпеки не оприлюднювалась. Питання інформаційної безпеки в сфері освіти почали привертати увагу педагогів у другій половині ХХ століття, коли збільшився об'єм та способи постачання інформації до людини, полегшився доступ до різних інформаційних джерел, а також збільшився інтерес до застосування ІКТ в освітньому процесі.

Аналіз закордонних та вітчизняних літературних джерел з питань інформаційної безпеки дозволяє стверджувати, що вчені вважають її складовою інформаційної культури особистості (І. Теплицький, С. Семеріков та ін.). Питання формування інформаційної культури вчителя висвітлено в працях В. Бикова, О. Данильчука, М. Жалдака, А. Коломієць, Л. Гаврілової, І. Смирнова та ін. [3; 4; 5]. Так, М. Жалдак, наголошуючи на необхідності використання комп'ютерної техніки та засобів зв'язку, стверджує, що таке користування має бути педагогічно виваженим і доцільним. На думку науковця, інформаційна культура майбутніх учителів має формуватися під час навчання в педагогічних вишах при вивченні дисциплін професійного та загального циклів.

Об'єктом дисертаційних досліджень А. Коломієць та І. Смирнової є формування інформаційної культури майбутніх учителів початкової школи, у яких особливу увагу зосереджено на доведенні багатокомпонентного змісту поняття «інформаційна культура майбутнього вчителя» та на створенні цілісної методичної системи формування фахової компетентності майбутнього вчителя, яка поєднує в собі гуманітарні та технічні знання в професійно важливих предметних галузях. Своєю чергою, О. Данильчук вважає, що поняття «інформаційна культура» складається з двох компонентів – загальнокультурного та професійно-педагогічного (прояв інформаційної культури під час вирішення професійних завдань та формування інформаційної культури учнів) [4].

Звернувшись до сучасних освітніх дефініцій «цифрова культура», «цифрова грамотність», «цифрова компетентність», Л. Гаврілова вважає, що навички безпечної роботи в мережі є складовими більш складного поняття «цифрова грамотність» [5]. Дефініція «цифрова грамотність» є популярною та широковживаною в педагогічних дослідженнях західних учених Д. Белшоу (D. Belshaw), Н. Хоклі (N. Hockly), Н. Сонк (N. Sonck), С. Лівінгстоун (S. Livingstone), Е. Купер (E. Kuiper). За їхнім визначенням, цифрова грамотність – це здатність знаходити, упорядковувати, розуміти, оцінювати і перетворювати інформацію, використовуючи ІКТ. У більш вузькому значенні, стосовно освітнього процесу, цифрова грамотність передбачає не лише роботу з джерелами

інформації та застосування комп'ютерної техніки і можливостей мережі Інтернет, а й майбутню якісну освіту, яка є доступною та відповідає індивідуальним особливостям та інтересам тих, кого навчають.

Т. Тейлор (T. Taylor) та І. Вард (I. Ward) розрізняють два види цифрової грамотності: інструментальну грамотність (уміння працювати з комп'ютерною технікою) та презентаційну грамотність (використання інструментальної грамотності для досягнення певних цілей). Учені стверджують, що студенти почасти мають високий рівень сформованості технічних умінь, але їм бракує вмінь та досвіду використовувати їх на практиці. На думку Т. Тейлора і І. Варда, на навчальні заклади покладається обов'язок формування цифрової грамотності студентів, зокрема особливу увагу слід приділяти е-безпеці, е-навчанню та створенню е-портфоліо [6].

Вітчизняна дослідниця О. Радзієвська вивчає шляхи вдосконалення цифрової грамотності й вважає, що одним з головних принців, на яких має базуватися державна політика в інформаційній сфері, є вміння громадян створювати власний безпечний інформаційний простір. Дослідниця також констатує незадовільний стан модернізації системи освіти, а також той факт, що навчально-виховний процес не охоплює того обсягу інформації, який учні або студенти отримують у позанавчальний час. Тому забезпечення цифрової грамотності передбачає убезпечення власного інформаційного простору, уміння виокремити необхідну інформацію із загальної кількості, опрацьовувати й трансформувати її в знання та навички, користуватися ними.

В. Кудлай також стверджує, що формування цифрової компетентності студентів є необхідною умовою ефективної взаємодії викладача та студента, підвищення інтересу до дистанційного навчання, збільшення цінності творчості та інновації. Прагнучи розвивати цифрову компетентність студентів, важливо встановити прямий зв'язок із інформаційною безпекою. Щодо загроз цифрових технологій у сфері освіти вчена розглядає їх у двох аспектах: техніко-технологічному та соціогуманітарному. Небезпеки соціогуманітарної сфери, за В. Кудлай, пов'язані з недотриманням норм поведінки в мережі Інтернет, зокрема розміщення компрометуючої інформації, провокування інших осіб, кіберзалежність. Техніко-технологічний аспект інформаційної безпеки передбачає вміння користуватися програмами захисту інформації, усвідомлення небезпеки збереження інформації з мережі тощо [7].

Дослідженню інформаційних загроз у контексті роботи людини з ІКТ присвячено праці українських та зарубіжних науковців Є. Архипової, А. Бєгуна, В. Голубєвої, С. Кавуна, А. Сахарова та ін. Однак з-поміж значної кількості наукових досліджень, які висвітлюють питання інформаційної безпеки, відсутні праці, у яких узагальнено зміст поняття «навички інформаційної безпеки», а також представлено умови та засоби формування цих навичок.

**Мета статті** полягає в детальному аналізі змісту поняття «інформаційна безпека» й окресленні умов та засобів формування навичок інформаційної безпеки студентів вищих педагогічних навчальних закладів.

## 2. МЕТОДИ ДОСЛІДЖЕННЯ

Дослідження проблеми формування інформаційної безпеки майбутніх учителів зумовлює використання теоретичних та емпіричних методів, а саме теоретичний аналіз наукової літератури з питань інформатизації освіти та забезпечення інформаційної безпеки [4; 5; 8; 9; 10]; вивчення нормативних документів, що визначають зміст навичок інформаційної безпеки та критеріїв оцінювання захищеності інформації в комп'ютерних системах [1; 2]. Для дослідження ефективності розробленого модуля та запропонованої системи засобів із формування навичок інформаційної безпеки

майбутніх учителів було використано метод тестування, методи інтерпретації, узагальнення і репрезентування власних результатів дослідження.

## 3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Здійснення професійної діяльності особами будь-яких спеціальностей, передусім учителів, пов'язане зі знаходженням та опрацюванням значної кількості інформаційних джерел, особливо тих, які розміщено в мережі Інтернет. У реаліях сьогодення важливого значення набуває сформованість навичок інформаційної безпеки, які, як доводить аналіз наукової літератури, є складовою частиною інформаційної (цифрової) грамотності. Звернемося до аналізу дефініцій (комп'ютерна грамотність, кіберграмотність, інтернет-грамотність, інформаційна грамотність, технічна грамотність, електронна грамотність, цифрова грамотність) задля визначення змісту вмінь інформаційної безпеки в межах професійної діяльності майбутніх учителів. У тлумачних словниках поняття «грамотність» традиційно визначалося як уміння читати та писати. Однак у ході економічного, соціального, культурного та технологічного розвитку значення поняття «грамотність» було розширено, і в сучасних джерелах його детерміновано як уміння здобувати знання із застосуванням технологій і можливість надавати оцінку складному матеріалу. Подальше ґрунтовне дослідження закордонними науковцями змісту поняття «грамотність» доводить, що воно є комплексним поняттям і передбачає сформованість цілої низки вмінь [11]. До сьогодні в педагогічній науці не вироблено уніфікованого визначення поняття грамотність, у нашому дослідженні ми виходимо з того, що грамотність – це вміння оволодіти професійними знаннями та навичками роботи в умовах інформатизації суспільства.

Ми поділяємо думку В. Кудлай, яка, проаналізувавши ряд новітніх понять, зокрема «комп'ютерна грамотність», «кіберграмотність», «інтернет-грамотність», «інформаційна грамотність», «технічна грамотність», «електронна грамотність», «цифрова грамотність», вилучає з наукового обігу перші чотири, тому що вони мають вузьку сферу застосування і не завжди корелюють з цифровими технологіями. З-поміж зазначених термінів, зауважує дослідниця, саме поняття цифрової грамотності охоплює як уміння застосовувати сучасні комп'ютерні технології, так і вести обмін інформацією в онлайн середовищі, критично осмислюючи цифрові технології з точки зору соціальних, культурних, політичних та освітніх аспектів своєї професійної діяльності [7].

Цифрова грамотність майбутнього фахівця є цілісною системою, що складається з таких компонентів (за В. Поляковим):

- Аксіологічний – визначення на особистому рівні гуманістичної цінності інформаційної діяльності людини;
- комунікативно-етичний, який характеризується культурою спілкування та моральною поведінкою в сфері інформаційних стосунків;
- когнітивно-інтелектуальний, що передбачає компетентність та вільну орієнтацію в сфері ІКТ, гнучкість та адаптивність мислення;
- прогностичний, який сприяє передбаченню можливих наслідків інформаційної діяльності, пофесійно-соціальній адаптації майбутніх спеціалістів в умовах постійного оновлення ІКТ;
- прикладний, що дозволяє використовувати інформаційно-комунікаційні технології для ефективного вирішення навчальних та професійних завдань;
- правовий, який передбачає знання «інформаційного права» й усвідомлення відповідальності за дії, які виконуються з інформаційними ресурсами;

- морально-етичний, що реалізує принципи комп'ютерної етики в інформаційній сфері;
- сек'юритологічний, орієнтований на забезпечення інформаційної безпеки корпоративних й індивідуальних ресурсів, захист інформації і захист від інформації [12, с. 62].

Відповідно до принципів системного підходу всі компоненти забезпечують цілісність функціонування інформаційно-цифрової грамотності, однак В. Поляков наголошує, що саме сек'юритологічний компонент є системоутворювальним. Оскільки сек'юритологічний компонент домінує в інформаційній підготовці спеціалістів різних сфер життєдіяльності, інформаційна безпека має розглядатися як обов'язкова складова професійної компетентності спеціаліста [12, с. 62-63].

Зазначимо, що визначення змісту вміння інформаційної безпеки, а також умов та засобів їх формування, вимагає докладного аналізу поняття інформаційна безпека. Щодо цього поняття, воно також є неоднозначним. У сучасній науковій літературі широковживаними є поняття кібербезпека, е-безпека та цифрова безпека. Деякі західні науковці вважають, що поняття «кібербезпека» (cyber safety) пов'язане з використанням інформаційних технологій та комп'ютерів. Вони визначають кібербезпеку як формування кібербезпечної поведінки, яка базується на відповідальному користуванні Інтернетом та мобільними технологіями, а також застосування заходів, що долають ризики негативного або шкідливого впливу цих технологій. Серед кіберзагроз, яким постійно протистоять студенти й особливо учні, західні вчені значну увагу приділяють кіберцькуванню (cyberbullying), яке здійснюється через соціальні мережі, текстові повідомлення або електронне листування.

Поняття «е-безпека» (e-safety) або «цифрова безпека» (digital safety) охоплює не лише використання Інтернет-технологій, а й комунікацію через мобільні телефони, ігрові консолі та технології бездротового зв'язку. Е-безпека передбачає формування в молоді розуміння переваг, ризиків та відповідальності щодо застосування інформаційно-комунікаційних технологій. У межах проєкту «ІКТ у школі» (ICT in Schools http://ictinschools.org/teachers/) команда науковців на чолі з М. Хамільтоном (M. Hamilton) та С. Робертом (S. Robert) визначили зміст е-безпеки для учнівської та студентської молоді: уміння розуміти та ефективно використовувати інноваційні технології, уміння визначати переваги та ризики ІКТ, уміння безпечної онлайн поведінки в аудиторній та позааудиторній діяльності.

Аналіз понять «кібербезпека», «е-безпека» та «цифрова безпека» доводить, що всі вони передбачають використання запобіжних заходів, яких слід дотримуватись під час використання мережі Інтернет, щоб забезпечити власну безпеку та збереження особистої інформації.

Однак вітчизняний дослідник О. Баранов, зіставивши результати аналізу проблем визначення термінів «кібербезпека», «онлайн безпека», «е-безпека», наголошує, що вони є окремими випадками інформаційної безпеки в умовах використання комп'ютерних систем та телекомунікаційних мереж. Отже, у своєму дослідженні ми надаємо перевагу терміну «інформаційна безпека», тому що він є ширшим за визначені вище й означає стан захищеності життєво важливих інтересів особистості, за якого не допускається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [8].

У глобальному розумінні щодо захисту молоді інформаційна безпека змінила головний акцент від ідей захисту до ідей формування вмінь та навичок цифрової

грамотності та інформаційної безпеки, які дають їм можливість приймати раціональні рішення, щоб захистити себе від можливого негативного впливу інформаційно-комунікаційних технологій під час навчання, спілкування або виконання в професійній діяльності.

Аналіз праць західних дослідників К. Хаг (C. Hague) та С. Пейтон (S. Payton) дозволив визначити зміст навичок інформаційної безпеки, розподіливши їх на три групи: функціональні, комунікативні та вміння критично мислити. До складу функціональних належать уміння:

- безпечно зберігати дані та отримувати доступ до них;
- архівувати та резервувати документи;
- визначати характер загроз інформаційної безпеки в комп'ютерній системі;
- розуміти та визначати авторські права, вивантажуючи власні документи в мережу Інтернет;
- реєструватися на сайтах, які вимагають особистої ідентифікації через використання дебетових карт тощо.

До змісту комунікативних умінь увійшли:

- уміння оцінювати та обирати між електронними засобами комунікації (e-mail, месенджер, соціальні мережі, форуми, блоги, вікі тощо) та традиційними засобами спілкування, цифрові засоби комунікації завжди порушують питання відкритості інформації;
- уміння ефективно використовувати можливості телекомунікації для досягнення особистих або професійних цілей [13].

На думку К. Ферсон (K. Pherson), Дж. Бенет (J. Bennett), є чотири ключових уміння критичного мислення, які дозволяють студентам оцінювати проблемні ситуації щодо їх інформаційної безпеки, передбачувати несподівані ситуації та уникати катастрофічних помилок, а саме:

- уміння застосовувати знання та розуміти хід виконання завдання;
- уміння аналізувати альтернативну інформацію та судження;
- уміння синтезувати різні джерела інформації;
- уміння оцінювати інформацію щодо її актуальності і безпечності [13].

Формування вмінь та навичок інформаційної безпеки майбутніх фахівців здійснюється здебільшого під час вивчення дисциплін інформаційного циклу, однак підготовка студентів гуманітарних спеціальностей, зокрема в галузі освіти, має обмежене коло таких дисциплін. Тому в курсі безпеки життєдіяльності один модуль присвячено вивченню питань інформаційної безпеки з огляду на широкомасштабну інформатизацію суспільства та розвиток сучасних інформаційних та комунікаційних технологій.

Умовами формування інформаційної безпеки є сукупність змісту інформаційної підготовки та аспектів інформаційної безпеки, а також інформаційних форм і засобів її реалізації в освітньому процесі. Під час навчання інформаційної безпеки застосовуються традиційні та інноваційні технології, в основі яких лежить створення сучасного інформаційно-освітнього середовища, яке є сукупністю умов, що забезпечують роботу студентів з інформаційними ресурсами. Серед інноваційних технологій, на основі яких у ВНЗ створюється навчальне середовище, де студенти можуть отримати доступ до навчальних матеріалів, здійснювати обмін інформацією, комунікувати, є технології електронного (дистанційного) навчання, використання яких робить навчальний процес більш гнучким, ефективним й безпечним. Перевагою такого середовища є передусім можливість реалізації головної умови успішного опанування професією – перенесення теоретичних знань в практико-орієнтовану площину.

ВНЗ здебільшого використовують систему електронного навчання Moodle, яка має багатомовний інтерфейс надає можливість організувати освітній процес, забезпечуючи його засобами навчання, системою контролю й оцінювання навчальної діяльності студентів.

Продовжуючи дослідження інформаційної безпеки майбутніх учителів, здійснимо аналіз системи Moodle за такими ознаками: 1) за способом доступу – обмеженого доступу, загальнодоступні, гібрідні; 2) за способом комунікації – синхронні, асинхронні, змішані; 3) за рівнем вимог до безпеки – загального використання, корпоративні, спеціальні; 4) за способом обміну даними – SCORM (навчальний матеріал подається окремими невеликими блоками, які можуть об'єднуватись у різні курси та використовуватись незалежно від того, ким, де та за допомогою яких засобів вони були створені) або AICC (описує спосіб обміну даними між навчальними матеріалами і системою управління навчанням, правила створення метаданих).

Враховуючи досвід запровадження системи електронного навчання в Україні, а також можливість застосування інноваційних технологій навчання, які дозволяють забезпечити захист інформації, дистанційне (електронне) навчання, в ДВНЗ «Донбаський державний педагогічний університет» також здійснюється на базі Moodle. Moodle – це середовище для створення дистанційних курсів, яке забезпечує студентам доступ до навчальних ресурсів і вважається безпечним. Рівень інформаційної безпеки та рівень захищеності систем дистанційного навчання має визначатися державними стандартами. Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України розроблено «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [15].

Функціональні критерії захисту інформації від певного виду загроз розділено на чотири групи. Загрози щодо несанкціонованого ознайомлення з інформацією становлять загрози конфіденційності; загрози щодо несанкціонованої модифікації інформації – загрози цілісності; загрози щодо порушення можливості використання комп'ютерних систем або оброблюваної інформації – загрози доступності. Ідентифікація і контроль за діями користувачів становлять предмет послуг спостереженості і керованості [10]. З огляду на зазначені критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу можна зауважити, що система дистанційного навчання Moodle має достатній рівень захищеності інформації, що представлено в таблиці 1.

*Таблиця 1*

**Рівень інформаційної захищеності системи Moodle**

| Об'єкт | Послуги конфіденційності | | | |
|---|---|---|---|---|
| | Довірча конфіденційність | Адміністративна конфіденційність | Повторне використання об'єктів | Конфіденційність при обміні |
| Інтерфейс користувача | - | - | - | - |
| Засоби адміністрування LCMS | + | + | + | + |
| Репозиторій навчальних об'єктів | + | + | + | + |
| Управління подіями | + | + | - | - |
| Система тестування/оцінювання | + | + | + | + |
| Поштовий сервіс | + | + | - | + |
| Сервіс миттєвих повідомлень | + | + | - | + |
| Сервіси передачі голосу і відео | + | + | - | + |

| | | | | |
|---|---|---|---|---|
| Сервіс дошки оголошень | + | + | + | + |

Щодо безпеки самої системи дистанційного навчання можна стверджувати, що вона є захищеною від зовнішніх загроз, спама та хакерських атак. Щоб не піддавати сайт ризику, достатньо заборонити доступ до начального сервісу незареєстрованим користувачам, а також заборонити самореєстрацію в курсі.

Структура системи дистанційного навчання складається з: інтерфейсу користувача (студента); системи управління навчальним контентом, яка здійснюється адміністратором; системи комунікації. Система Moodle легко інтегрується з хмарними сервісами (Google, Amazon, Dropbox, OneDrive), що дозволяє, зберігати та змінювати файли великого об'єму (більше 20 Мб). Інтегрування з хмарними сервісами відбувається через репозиторії, зокрема через інтерфейс адміністратора, та надає можливість студентам завантажувати файли різних форматів із зовнішніх ресурсів. На офіційному сайті системи Moodle (https://docs.moodle.org/24/en/Repositories) розміщено загальну інформацію хмарних сервісів та інформацію щодо їх підключення.

Модуль «Основи інформаційної безпеки» розроблено в межах навчальної дисципліни «Безпека життєдіяльності» для підготовки майбутніх учителів, які не спеціалізуються в цій галузі, у навчальному середовищі Moodle. Методика навчання основам інформаційної безпеки, що відповідає цілям сучасної освіти в галузі інформаційних та комунікаційних технологій ґрунтується на інтегративному підході, який поєднує в собі характеристики системного, інформаційного та діяльнісного підходів. Тому під час розробки навчального модулю для формування навичок інформаційної безпеки особливу увагу акцентовано на таких аспектах:

1) формування навичок інформаційної безпеки є складовою частиною фахової компетентності майбутніх учителів;
2) залучення життєвого і професійного досвіду студентів для вирішення навчальних завдань;
3) сприяння міжпредметній інтеграції навчальних дисциплін;
4) посилення зв'язку теорії з практикою;
5) розширення сфери прикладних умінь за рахунок інтеграції з дисциплінами фахового циклу навчального плану.

Змістовий компонент навчальної дисципліни «Безпека життєдіяльності» в межах модуля «Основи інформаційної безпеки» містить теми, пов'язані із забезпеченням інформаційної безпеки та професійної підготовки майбутніх учителів. Зокрема цілі навчального модуля «Основи інформаційної безпеки» полягають в:

- ознайомленні студентів з формами та методами інформаційного впливу та інформаційного тиску;
- формуванні уявлення про нерозривну єдність ефективної професійної діяльності з вимогами безпеки та захищеності особистості.

Вивчення кожної теми відбувається через забезпечення студентів інструктивними матеріалами у форматі відеофайлів або інформаційних сторінок, після ознайомлення з цими матеріалами обов'язковою є участь у дискусії щодо актуальних питань обговорюваної теми, наприклад, під час вивчення теми «Управління ризиками» студентам пропонують долучитися до такої дискусії: «Управління ризиком вимагає визначення ефективних заходів для його уникнення. Які дії Ви оберете: уникнення ризику, зниження ймовірності атаки, користування допомогою фахівців у сфері інформаційної безпеки у випадку виникнення ризику?». Виконавши всі завдання, студенти проходять тестування для визначення рівня сформованості навичок інформаційної безпеки.

Для перевірки ефективності розробленого модуля в системі Moodle, а також рівня сформованості навичок інформаційної безпеки майбутніх учителів було проведено експериментальне дослідження рівня сформованості навичок інформаційної безпеки серед студентів першого курсу рівня вищої освіти «Магістр». Загалом у дослідженні взяли участь 117 студентів факультету початкової, технологічної та професійної підготовки. Експериментальна перевірка містила два зрізи – передекспериментальний та контрольний, які складалися з двох блоків запитань, перший блок стосовно можливих інформаційних ризиків, другий – інформаційна безпека, безпека персональних даних та прийоми безпечної поведінки. Відповіді на запитання вимагали не лише сформованості навичок інформаційної безпеки, а й залучення критичного мислення, тобто студенти, відповідаючи на питання тесту, мали проаналізувати можливі ризики та вказати причини, чому саме вони вважають представлені в запитанні факти або дії шахрайством або тим, що несе в собі загрози [15].

Визначення рівня сформованості навичок інформаційної безпеки студентів відбувалося за двома критеріями, представленими в таблиці 2.

*Таблиця 2*

**Критерії визначення рівня сформованості навичок інформаційної безпеки**

| **Критерій інформаційної захищеності (КІЗ)** | |
|---|---|
| Низький | – знання про негативні інформаційні впливи є безсистемними та фрагментарними, знання про забезпечення інформаційної безпеки особистості відсутні;<br>– причини виникнення ситуацій негативного впливу пов'язують із незадовільною організацією інформаційної інфраструктури, що заважає усвідомленню власної активної позиції в створенні інформаційного середовища; |
| Середній | – уміння аналізувати і критично оцінювати інформацію;<br>– уміння виявити та нейтралізувати інформаційну загрозу, інформаційну небезпеку;<br>– розуміння особистої відповідальності за розповсюдження інформації в соціальних мережах;<br>– знання правил поведінки особистості в інформаційному суспільстві; |
| Високий | – знання основних законодавчих та нормативних документів щодо забезпечення інформаційної безпеки особистості;<br>– наявність внутрішніх принципів та переконань, які перешкоджають розповсюдженню соціально деструктивної інформації та дезінформації, маніпулюванню свідомістю людей. |
| **Діяльнісний критерій (ДК)** | |
| Низький | – уміння орієнтуватися в інформаційних потоках;<br>– навички методичної роботи з традиційними та нетрадиційними джерелами інформації; |
| Середній | – уміння застосовувати нові інформаційно-комунікаційні технології;<br>– уміння вирішувати професійні завдання за допомогою інформаційно-комунікаційних технологій; |
| Високий | – уміння використовувати прийоми культури інформаційної безпеки в нестандартних ситуаціях для вирішення професійних завдань. |

Обчислювання за кожним критерієм відбувалося за 20-бальною шкалою. Максимальна кількість балів, яку могли отримати студенти, становила 40 балів.

Передекспериментальне опитування проводилося до початку вивчення модуля «Основи безпеки життєдіяльності», середні результати на одного студента за кожним критерієм становлять КІЗ – 7,08, КД – 11, 24. Підсумкове тестування проводилося після вивчення модуля та мало такі середні результати на одного студента: КІЗ –13,2, КД – 15,51. Порівняльні дані за двома критеріями представлено в діаграмі 1.

*Діаграма 1*

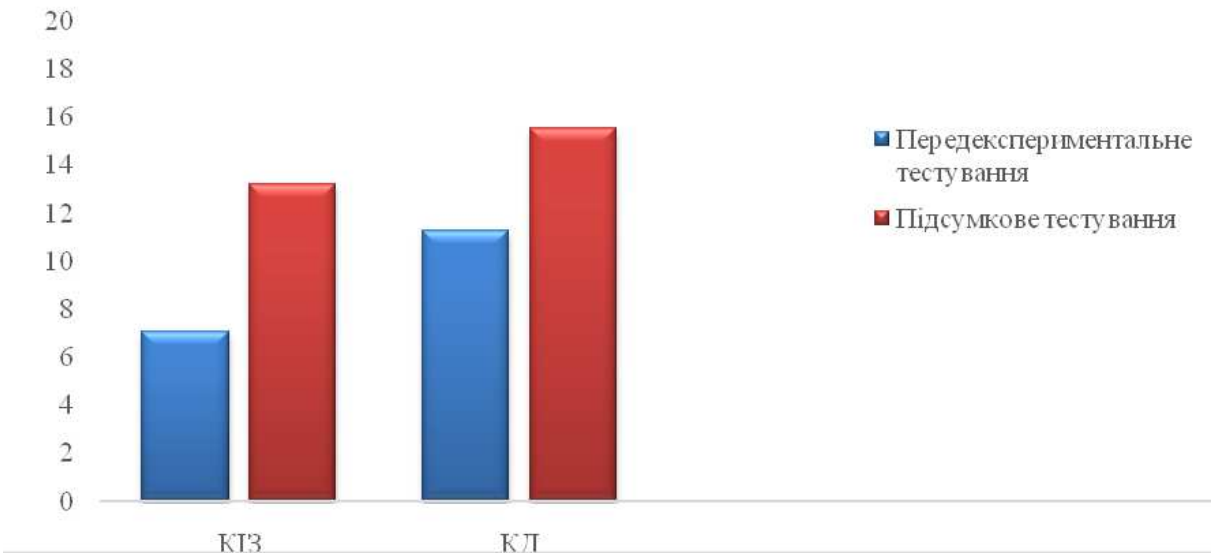


*Рис. 1. Порівняльна діаграма результатів передекспериментального та підсумкового тестування за двома критеріями (на одного студента)*

## 4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, у ході дослідження доведено, що навички інформаційної безпеки є складовою частиною інформаційної грамотності майбутніх учителів. Аналіз цілої низки тлумачень поняття «інформаційна безпека» дозволив визначити його зміст, який передбачає запобігання ризиків негативного інформаційного впливу, негативних наслідків застосування інформаційних технологій, несанкціонованого поширення, використання і порушення цілісності, конфіденційності та доступності інформації. Процес формування навичок інформаційної безпеки здебільшого орієнтований на виявлення інформаційних загроз та оволодіння прийомами безпечної поведінки в професійній діяльності. Головною умовою формування навичок інформаційної безпеки є створення безпечного навчального середовища, а також інтеграція змісту інформаційної підготовки та аспектів інформаційної безпеки, інформаційних форм і засобів її реалізації в освітньому процесі.

Одержані результати передекспериментального та підсумкового тестування перевірки дозволяють стверджувати, що добірка тем та організація навчання на базі системи Moodle у межах дистанційного курсу «Безпека життєдіяльності» є ефективною. Послідовність опрацювання навчальних блоків (теоретичного та практичного), надання переваги завданням, які вимагають інтеграції теоретичних знань та практичного досвіду забезпечують достатній рівень сформованості в студентів навичок інформаційної безпеки.

На нашу думку, подальші розвідки слід спрямувати на дослідження процесу формування інформаційної культури майбутніх учителів у мережевому спілкуванні.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


[1] "Про Доктрину інформаційної безпеки України", №47/2017, 2016 [Електронний ресурс]. Доступно: https://www.president.gov.ua/documents/472017-21374. Дата звернення: Лип. 03, 2018.

[2] "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»", № 96, 2016. [Електронний ресурс]. Доступно: https://www.president.gov.ua/documents/962016-19836. Дата звернення: Лип. 03, 2018.

[3] А. Коломієць, "Інформаційна культура вчителя початкових класів: рівні, критерії, показники", *Педагогічні науки*, Випуск 45, с. 279-285, 2007.

[4] Е. В. Данильчук, *Теория и практика формирования информационной культуры будущего педагога*, Волгоград, Россия: Перемена, 2002.

[5] Л. Гаврілова, Я. Топольник, "Цифрова культура, цифрова грамотність, цифрова компетентність як сучасні освітні феномени", *Інформаційні технології і засоби навчання, 61*(5), с. 1-14, 2017 [Електронний ресурс]. Доступно: https://journal.iitta.gov.ua/index.php/itlt/article/view/1744. Дата звернення: Лип. 09, 2018.

[6] T. Taylor and I. Ward, "*Literacy theory in the age of the Internet*", New York: Colambia UP, 1998.

[7] В. О. Кудлай, "Цифрова грамотність особистості в контексті розвитку інформаційного суспільства", *Вісник маріупольського державного університету*, Вип. 10, с. 97-104, 2015.

[8] О. А. Баранов, "Про тлумачення та визначення поняття «кібербезпека»", *Правова інформатика*, №2 (42), с. 54-62, 2014.

[9] В. Олексюк, О. Олексюк, "Стан сформованості компетентностей з інформаційної безпеки майбутніх учителів інформатики", *Інформаційні технології і засоби навчання, № 62*(6), с. 277-291, 2017 [Електронний ресурс]. Доступно: https://journal.iitta.gov.ua/index.php/itlt/article/view/1906. Дата звернення: Лип. 11, 2018.

[10] В. Ф. Чекурін, О. О. Будік, "Підхід до формування вимог інформаційної безпеки систем електронного навчання", *Вісник Національного університету «Львівська політехніка»,* №695, с. 133-140, 2011.

[11] "Understanding of literacy", *Education for All Global Monitoring Report,* 2006 [Електронний ресурс]. Доступно: http://www.unesco.org/education/GMR2006/full/chapt6_eng.pdf. Дата звернення: Лип. 07, 2018.

[12] В. П. Поляков, "*Аспекты информационной безопасности в информационной подготовке*", Москва, Россия: ФГБНУ «ИУО РАО», 2016.

[13] C. Hague and S. Payton, "Digital literacy across the curriculum", *Curriculum and Leadership Journal*, Vol. 9, Is. 10 [Електронний ресурс]. Доступно: http://www.curriculum.edu.au/leader/default.asp?id=33211&issueID=12380. Дата звернення: Лип. 09, 2018.

[14] L. J. Shannon and J. Bennett, "A case study: Applying critical thinking skills to Computer Science and Technology", *Information Systems Education Journal*, 10 (4), pp. 41-48, 2012.

[15] "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", НД ТЗІ 2.5-004-99, 1999 [Електронний ресурс]. Доступно: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342. Дата звернення: Лип. 11, 2018.


*Матеріал надійшов до редакції 14.08.2018 р.*

## УСЛОВИЯ И СРЕДСТВА ФОРМИРОВАНИЯ НАВЫКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БУДУЩИХ УЧИТЕЛЕЙ

**Бондаренко Владимир Иванович**
доктор педагогических наук, доцент,
заведующий кафедрой общетехнических дисциплин, безопасности жизнедеятельности и автодела
ГВУЗ «Донбасский государственный педагогический университет», г. Славянск, Украина
ORCID ID 0000-0002-8359-884X
*vibondarenko1287@gmail.com*

**Аннотация.** В статье представлено исследование условий и средств формирования навыков информационной безопасности, которое является актуальным в современных условиях стремительного развития информационно-коммуникационных технологий. Проведенный анализ научной литературы доказывает, что увеличение объема и изменение способов

передачи информации, упрощение доступа к разным информационным источникам, а также увеличение интереса к использованию ИКТ в образовательном процессе обусловили актуальность исследуемой проблемы. В статье представлен подробный анализ понятий «кибербезопасность», «е-безопасность», «цифровая безопасность», на основе которого определено содержание дефиниции «информационная безопасность». Особенное внимание уделено содержанию навыков информационной безопасности, которые делятся на три группы: функциональные, коммуникативные и умения критического мышления. Указано, что условиями формирования информационной безопасности является совокупность содержания информационной подготовки и аспектов информационной безопасности, а также информационных форм и средств ее реализации в образовательном процессе. Автор доказывает, что эффективным средством формирования навыков информационной безопасности является создание учебной среды в вузе. Описан опыт внедрения учебного курса, созданного на базе системы Moodle, самой распространенной в вузах страны, безопасной и легко интегрируемой с облачными сервисами, что позволяет создавать репозитарий учебных материалов. При разработке учебного модуля для формирования навыков информационной безопасности был учтен тот факт, что формирование навыков информационной безопасности является составляющей частью профессиональной подготовки будущих учителей, поэтому для решения учебных заданий учитывался жизненный и профессиональный опыт студентов. В статье представлены данные экспериментальной проверки внедряемого модуля, которые подтверждают его эффективность.

**Ключевые слова:** информационная безопасность; цифровая грамотность; безопасность жизнедеятельности; будущие учителя; система Moodle.

# CONDITIONS AND TOOLS FOR DEVELOPING FUTURE TEACHERS' INFORMATION SAFETY SKILLS

**Volodymyr I. Bondarenko**
Doctor of Pedagogical Sciences, Associate Professor, Head of Department of General Technical Disciplines, Safety of Vital Activity and Automotive Engineering
State Higher Educational Establishment "Donbas State Pedagogical University", Sloviansk, Ukraine
ORCID ID 0000-0002-8359-884X
*vibondarenko1287@gmail.com*

**Abstract.** The article is devoted to the research of the conditions and tools for developing information security skills that is relevant in the current conditions of the rapid development of information and communication technologies. The analysis of the scientific literature proves that increased amount of information and means of its transfer, as well as simplification of the access to different information sources and growing interest to using ICT in educational process cause the relevance of the issue. In the article the concepts of "cyber security", "e-security", "digital security" are studied through the detailed analysis that helps define the content of the term "information security". The special attention is paid to the content of the information security skills that are divided into three groups: functional, communicative and critical thinking skills. It is noted that the condition of developing information security is the integrity of the content of information training and the aspects of information security, as well as the forms and means of its realization in the educational process. The author proves that the effective tool of developing information security skills is designing the learning environment in the tertiary institution. The author presents experience of implementing the course on the basis of platform Moodle, which is one of the most widespread in the universities of the country, safe and easily integrated with cloud services that gives an opportunity to create the repository of learning materials. While designing the learning module for developing information security skills, the following fact was taken into account: developing of the information security skills is the constituent element of future teachers' professional training that's why the solving of the learning problems require including students' live and professional experience. In the article the experimental data, which confirm the effectiveness of the implemented module, are represented.

**Keywords:** information security; digital literacy; safety of vital activity; future teachers; platform Moodle.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] "About Doctrine of Information Security of Ukraine", #47/2017, 2016 [Online]. https://www.president.gov.ua/documents/472017-21374. Accessed on: Jul. 03, 2018. (in Ukrainian)
[2] "About Decision of National Security and Defense Council of Ukraine adopted on January, 27, 2016 "About Cyber Security Strategy of Ukraine", #96, 2016. [Online]. https://www.president.gov.ua/documents/962016-19836. Accessed on: Jul. 03, 2018. (in Ukrainian)
[3] A. Kolomiiets, "Information Culture of Primary School Teacher: Levels, Criteria and Indicators", *Pedahohichni nauky*, #45, pp. 279-285, 2007. (in Ukrainian)
[4] Ye. V. Danilchuk, *"Theory and Practice of Developing Future Teacher's Information Culture"*, Volgograd, Russia: Peremena, 2002. (in Russian)
[5] L. Havrilova, Ya. Topolnyk, "Digital Culture, Digital Literacy, Digital Competence as Modern Educational Phenomena", *Information technologies and learning tools,* # 61(5), pp. 1-14, 2017 [Online]. Available: https://journal.iitta.gov.ua/index.php/itlt/article/view/1744. Accessed on: Jul. 09, 2018. (in Ukrainian)
[6] T. Taylor and I. Ward, "*Literacy theory in the age of the Internet*", New York: Colambia UP, 1998. (in English)
[7] V. O. Kudlai, "Digital Literacy of a Personality in the context of Digital Society Development", *Visnyk mariupolskoho derzhavnoho universytetu*, #10, pp. 97-104, 2015. (in Ukrainian)
[8] O. A. Baranov, "About the determination and definition of the concept "cybersecurity", Pravova informatyka, #2, pp. 54-62, 2014. (in Ukrainian)
[9] V. Oleksiuk and O. Oleksiuk, "The Condition of the Development of Information Security Competence of Future Teachers", *Information technologies and learning tools,* #62(6), pp. 277-291, 2017 [Online]. Available: https://journal.iitta.gov.ua/index.php/itlt/article/view/1906. Accessed on: Jul. 11, 2018. (in Ukrainian)
[10] V. F. Cherkun and O. O. Budik, "An Approach to Developing Requirements of the Information Security in the System of E-learning", Visnyk Natsionalnoho universytetu "Lvivska politekhnika", #695, pp. 133-140, 2011. (in Ukrainian)
[11] "Understanding of literacy", *Education for All Global Monitoring Report,* 2006 [Online]. Available: http://www.unesco.org/education/GMR2006/full/chapt6_eng.pdf. Accessed on: Jul. 07, 2018. (in English)
[12] V. P. Poljakov, *"Aspects of Information Security in Information Training"*, Moscow, Russia: FGBNU "IUO RAO", 2016. (in Russian)
[13] C. Hague and S. Payton, "Digital literacy across the curriculum", *Curriculum and Leadership Journal*, Vol. 9, Is. 10 [Online]. Available: http://www.curriculum.edu.au/leader/default.asp?id=33211&issueID=12380. Accessed on: Jul. 09, 2018. (in English)
[14] L. J. Shannon and J. Bennett, "A case study: Applying critical thinking skills to Computer Science and Technology", *Information Systems Education Journal*, 10 (4), pp. 41-48, 2012. (in English)
[15] "Criteria of Assessing the Information Safety in Computer Systems from Unauthorized Access", ND TZI 2.5-004-99, 1999 [Online]. Avaliable: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342. Accessed on: Jul. 09, 2018. (in Ukrainian)