МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені А. С. МАКАРЕНКА

Кваліфікаційна наукова праця на правах рукопису

УДК 378.147:[373.5.011.3-051:004]: 004.056 -028.63 -057.874(043.5)

ДУБИНСЬКИЙ Віталій Олегович

ФОРМУВАННЯ ГОТОВНОСТІ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ ДО РОЗВИТКУ НАВИЧОК ЦИФРОВОЇ БЕЗПЕКИ УЧНІВ НА ЗАСАДАХ ІНФОРМАЦІЙНОГО ПІДХОДУ

01 Освіта
015 Професійна освіта (цифрові технології)

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ В.О. Дубинський

Науковий керівник – Штика Юрій Михайлович, кандидат педагогічних наук, доцент, Сумський державний педагогічний університет імені А.С. Макаренка

Суми 2025

АНОТАЦІЯ

Дубинський В.О. Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 015 Професійна освіта (цифрові технології). – Сумський державний педагогічний університет імені А.С. Макаренка, Суми, 2024.

У дисертації здійснено теоретичне узагальнення й практичне розв'язання проблеми формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

У першому розділі охарактеризовано цифрові загрози і відповідні навички цифрової безпеки молоді та доведено важливість їх розвитку в умовах інформаційного суспільства, а також узагальнено результати аналізу теоретичного і практичного стану розробленості проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.

За результатами термінологічного аналізу понять «цифрові загрози», «цифрові небезпеки» та їх видів, зіставлення понять «кібербезпека» і «цифрова безпека» уточнено поняття навички цифрової безпеки як сукупність знань та умінь для безпечного, відповідального та етичного використання цифрових технологій, яка забезпечує особі захист особистих даних, цифрової ідентичності, пристроїв і мереж від кібератак, а також сприяє свідомому онлайн-спілкуванню.

До основних навичок цифрової безпеки віднесено: розуміння кіберзагроз та способів їх уникнення: ідентифікація основних видів загроз (фішинг, шкідливе програмне забезпечення, атаки програм-вимагачів); використання антивірусного програмного забезпечення та фаєрволів; захист пристроїв від несанкціонованого доступу; *у*правління цифровою ідентичністю

та слідом: контроль над особистими даними, що залишаються в цифровому просторі; налаштування конфіденційності в соціальних мережах; використання безпечних методів аутентифікації (двофакторна автентифікація, надійні паролі); здатність виявляти дезінформацію та критично оцінювати інформацію: аналіз джерел інформації на достовірність; розпізнавання маніпулятивного контенту та фейкових новин; виявлення шкідливих або шахрайських сайтів; розуміння основ функціонування комп'ютерних систем та програмного забезпечення, базові знання про операційні системи, мережеві протоколи, налаштування безпеки; використання захищених каналів зв'язку (VPN, шифрування даних); виявлення підозрілої активності на пристроях та в облікових записах; безпечне цифрове спілкування та культура онлайн-поведінки: дотримання правил етикету в Інтернеті (нетикету); уникнення надсилання конфіденційної інформації через незахищені канали; усвідомлення ризиків онлайн-спілкування та соціальної інженерії; розуміння правових та етичних аспектів цифрової безпеки: ознайомлення з правовими нормами щодо захисту персональних даних (GDPR, українське законодавство); усвідомлення відповідальності за кібербулінг, незаконний обіг інформації та порушення авторських прав; дотримання принципів інформаційної етики; захист здоров'я та добробуту в цифровому середовищі, запобігання цифровій залежності та кібербулінгу; дотримання правил гігієни зору та безпечного використання гаджетів; усвідомлення психологічного впливу цифрових технологій.

На основі аналізу наукової літератури виявлено можливі шляхи модернізації програм підготовки вчителів для розвитку в учнів навичок цифрової безпеки: інтеграція цифрової безпеки в курси з методики навчання інформатики; розробка й упровадження спеціалізованих курсів з цифрової безпеки у освітньо-професійні програми підготовки вчителів; використання цифрових інструментів та симуляції для формування практичних навичок цифрової безпеки; сприяння співпраці та обміну знаннями з професіоналами.

У другому розділі уточнено сутність і структуру готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів, змодельовано процес формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

За результатами термінологічного аналізу ключових понять дослідження («готовність», «готовність до професійної діяльності», «готовність учителя») було уточнено сутність ключової категорії дослідження: готовність учителів інформатики до розвитку навичок цифрової безпеки учнів як інтегративної особистісної здатності майбутнього вчителя інформатики розвивати навички цифрової безпеки учнів, яка поєднує: усвідомлені прагнення такого розвитку; специфічні знання й уміння; навички рефлексії щодо успішності такого розвитку. Виявлена сутність обумовила розгляд поняття «готовність учителів інформатики до розвитку навичок цифрової безпеки учнів» як складного особистісного утворення, яке поєднує в собі три компоненти:

- мотиваційний компонент (прагнення розвитку навичок цифрової безпеки учнів) характеризує усвідомлення студентами потреби розвитку навичок цифрової безпеки учнів і є фундаментом їхньої мотивації діяти в цьому напрямку. Це усвідомлення впливає на їхню професійну діяльність, сприяє особистісному розвитку та забезпечує безпечне освітнє середовище;
- предметно-методичний компонент (специфічні знання й уміння) поєднує в собі предметні знання про цифрову безпеку і методичні знання щодо стратегій розвитку навичок цифрової безпеки учнів. Він характеризується сукупністю предметних знань, знань методичних підходів для розвитку навичок цифрової безпеки та психолого-педагогічних знань та умінь дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки учнів;
- особистісний компонент (навички рефлексії щодо успішності розвитку навичок цифрової безпеки учнів) є важливою складовою готовності

і охоплює рефлексивну діяльність, яка дозволяє аналізувати власний рівень цифрової безпеки, вдосконалювати методики навчання, формувати критичне мислення у школярів та усвідомлювати етичні аспекти цифрової взаємодії.

На основі узагальнення наукових результатів обґрунтовано необхідність використання інформаційного підходу як провідного у формуванні готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів, оскільки саме інформаційний підхід дозволяє майбутнім учителям опанувати принципи безпечної взаємодії в цифровому середовищі, розвинути навички критичного аналізу інформації, захисту персональних даних та етичного використання цифрових ресурсів. Застосування цього підходу в підготовці вчителів інформатики уможливлює формування в них здатності передбачати потенційні ризики цифрового середовища, аналізувати інформаційні загрози та адаптувати освітній процес відповідно до змін у сфері кібербезпеки. Активна взаємодія з цифровими платформами, інструментами управління інформацією та засобами захисту даних дозволяє майбутнім педагогам не тільки опанувати цифрову безпеку особисто, а й ефективно передавати ці знання учням. Інформаційний підхід забезпечує системне розуміння того, як інформація циркулює в цифровому середовищі, які механізми впливають на її безпеку та як навчити учнів захищати себе від можливих загроз.

З використанням методу моделювання було унаочнено процес формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу. Авторська модель базується на дотриманні принципів (науковість та актуальність, системність, компетентісна орієнтованість, практико-орієнтованість, інтеграція та міждисциплінарність) при організації навчання спецкурсу «Цифрова безпека у навчальному середовищі» у традиційній формі (лекції, практичні заняття) з використанням активних і проблемних методів навчання та різних цифрових засобів навчання (цифрові навчальні середовища, цифрові освітні ресурси та програми спеціалізованого спрямування).

У третьому розділі розроблено діагностичний інструментарій дослідження та експериментально перевірено ефективність моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

На основі структурно-логічного аналізу з урахуванням означення категорії «готовність майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів» та характеристики її компонентів було розроблено критерії та показники сформованості мотиваційного, предметно-методичного та особистісного компонентів готовності. У дослідженні використано спонукальний, компетентісний і поведінковий критерії, які увиразнюються чотирма показниками: «ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів»; «знання методичних підходів для розвитку навичок цифрової безпеки»; «уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки в учнів»; «прагнення до професійного розвитку в галузі цифрової безпеки».

У дослідженні з використанням порівняльного аналізу схарактеризовано чотири рівні готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів: початковий, базовий, високий, творчий.

Представлено коротко поетапний перебіг процесу дослідження: на першому етапі було здійснено теоретичний і практичний аналіз та обґрунтування проблеми дослідження, виявлено наявні суперечності для уточнення предмету дослідження, а також розроблено науковий апарат дослідження та відповідний тезаурус; на другому етапі розроблено і обґрунтовано модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу; третій етап визначався експериментальним упровадженням моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу; на заключному, четвертому етапі, проведено статистичний аналіз даних та зроблено якісні висновки.

Педагогічний експеримент як провідний метод науково-педагогічного дослідження використаний для підтвердження теоретичних висновків через статистичні методи. Зібрані в ході педагогічний експерименту емпіричні дані за всіма показниками підтвердили позитивні зрушення середніх для ЕГ по відношенню до КГ: найбільшу динаміку в ЕГ набув предметно-методичний компонент готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів – обидва показники продемонстрували суттєве зростання середніх (9,07 і 2,52 проти 12,22 і 3,59 відповідно). Статистичний аналіз підтвердив основне припущення нашого дослідження про ефективність розробленої моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

Виявлені в ході дослідження проблеми й отримані результати дали підстави для формулювання рекомендацій розробникам та викладачам, які реалізують освітні програми підготовки вчителів інформатики. Зокрема, відсутність послідовної та ефективної політики в галузі цифрової безпеки в освітніх програмах підготовки учителів інформатики може мати відтерміновані негативні наслідки. Інтеграція курсів з цифрової безпеки в освітні програми підготовки вчителів інформатики має вийти за рамки ізольованих вибіркових або факультативних курсів і стати нормативним компонентом освітньої програми, а освітні установи повинні розвивати культуру безперервного навчання для професійного розвитку в галузі цифрової безпеки.

Наукова новизна дослідження полягає у тому, що

– *вперше розроблено, теоретично обґрунтовано та експериментально перевірено* модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу, яка передбачає дотримання принципів (науковість та актуальність, системність, компетентісна орієнтованість, практико-орієнтованість, інтеграція та міждисциплінарність) при організації навчання спецкурсу

«Цифрова безпека у навчальному середовищі» у традиційній формі (лекції, практичні заняття) з використанням активних і проблемних методів навчання та різних цифрових засобів навчання (цифрові навчальні середовища, цифрові освітні ресурси та програми спеціалізованого спрямування);

– *уточнено* поняття «готовність учителів інформатики до розвитку навичок цифрової безпеки учнів» (інтегративна особистісна здатність майбутнього вчителя інформатики розвивати навички цифрової безпеки учнів, яка поєднує: усвідомлені прагнення такого розвитку; специфічні знання й уміння; навички рефлексії щодо успішності такого розвитку); *охарактеризовано структуру* готовності вчителів інформатики до розвитку навичок цифрової безпеки учнів через тріаду його компонентів (мотиваційний, предметно-методичний, особистісний);
– *розроблено* діагностувальний інструментарій та схарактеризовано рівні (початковий, базовий, високий, творчий) готовності майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів ;
– *подальшого розвитку набули* методи і засоби підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів у закладах вищої освіти, наукові уявлення про структуру готовності майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів, критеріальні та рівневі ознаки готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.

Ключові слова: майбутні учителі інформатики, навички цифрової безпеки, інформаційний підхід, готовність учителя, професійна підготовка

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці,

у яких опубліковані основні наукові результати дисертації

Статті у наукових фахових виданнях України

1. **Dubinsky V.** Information approach in education and its use in the training of computer science teachers to form students' digital safety skills. *Академічні візії, 2024. 38*. https://doi.org/10.5281/zenodo.14594487. Отримано з https://www.academy-vision.org/index.php/av/article/view/1587.

2. **Dubinsky V.** Training of computer science teachers for the formation of cybersecurity skills in students: actualization of problems and their possible solutions. *Освіта. Інноватика. Практика*, 2024. Том 12, № 10. С. 6-11. https://doi.org/10.31110/2616-650X-vol12i10-001.

3. **Dubinsky V. O.** The readiness of computer science teachers to develop students' digital security skills. *Наукові інновації та передові технології» (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»),* 2025. № 2(42). С. 1075-1087. https://doi.org/10.52058/2786-5274-2025-2(42)-1075-1087.

Стаття у закордонному виданні

4. Dubinsky V. Digital security skills of computer science teachers: generalization of the results of scientific papers. *Academia Polonica*. 2024. Vol. 67(6). Pp. 22-29. https://doi.org/10.23856/6703.

Публікації у виданнях, що індексуються у наукометричних базах Scopus та/ або Web of science

5. M. Yachmenyk et al., "Development of Information and Media Literacy in the System "Students-Parents-Teachers": Ukrainian Practice," 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, pp. 430-435, doi: 10.1109/MIPRO60963.2024.10569314 (Scopus)

Наукові праці, які засвідчують апробацію матеріалів дисертації

6. **Dubinsky V. O.**, Shamonia V. G. On the development of information and digital competence of future teachers of vocational education. *Вектори розвитку науки, освіти, технологій і суспільства в умовах глобалізації*: збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 19 жовтня 2023 р.): у 2 ч. Полтава: ЦФЕНД, 2023. Ч. 1. С.17-18.

7. **Дубинський В.**, Шамоня В. Про інформаційно-цифрову компетентність як сучасну педагогічну категорію. *Наукова діяльність як шлях формування професійних компетентностей майбутнього фахівця* (НПК-2023) : матеріали Міжнародної науково-практичної конференції, 7-8 грудня 2023 р., м. Суми. Суми : ФОП Цьома С.П., 2023. С. 26-27.

8. **Дубинський В.** Академічна доброчесність – невід'ємний складник інформаційно-цифрової компетентності майбутніх викладачів ЗП(ПТ)О. *Академічна культура дослідника в освітньому просторі: європейський та національний досвід*: збірник матеріалів VII Міжнародної науково-практичної конференції (м. Суми, 17-18 травня 2024 року) / за ред. О. М. Семеног. Суми : Видавництво СумДПУ імені А. Макаренка, 2024. С. 172-174.

9. **Дубинський В. О.**, Шамоня В. Г. До питання про розвиток інформаційно-цифрової компетентності в умовах неформальної освіти. *Інформаційні технології в соціокультурній сфері, освіті та економіці* : матеріали IIIV Міжнародної науково-практичної конференції студентів і молодих учених. / М-во освіти і науки України; Київ. нац. ун-т культури і мистецтв. Київ : Видавничий центр КНУКіМ, 2024. С.93-95.

10. **Dubinsky V.**, Shamonia V. On the development of students' digital security skills based on the information approach. *Наукова діяльність як шлях формування професійних компетентностей майбутнього фахівця (НПК-2024)* : матеріали Міжнародної науково-практичної конференції (5-6 грудня 2024 р., м. Суми). Суми : СумДПУ ім. А. С. Макаренка, 2024. С. 12-13.

ABSTRACT

Dubinsky V. O. Formation of future computer science teachers' readiness to develop students' digital security skills based on the information approach. - Qualification scientific work on the rights of a manuscript**.**

Dissertation for Doctor of Philosophy degree in specialty 015 Professional Education (Digital Technologies). – Sumy State Pedagogical University named after A.S. Makarenko, Sumy, 2025.

The thesis provides theoretical generalization and practical solution to the problem of forming future computer science teachers' readiness to develop students' digital security skills based on the information approach.

The first chapter characterizes digital threats and relevant digital security skills of youth. It proves the importance of their development in the information society, as well as summarizes the results of the analysis of the theoretical and practical state of the problem of preparing future computer science teachers to develop students' digital security skills.

Based on the results of the terminological analysis of the concepts of "digital threats", "digital hazards" and their types, comparison of the concepts of "cybersecurity" and "digital security", the concept of digital security skills is clarified as a set of knowledge and skills for the safe, responsible and ethical use of digital technologies, which provides a person with the protection of personal data, digital identity, devices and networks from cyberattacks, and also promotes conscious online communication.

The primary digital security skills include: understanding cyber threats and ways to avoid them: identifying the main types of threats (phishing, malware, ransomware attacks); using antivirus software and firewalls; protecting devices from unauthorized access; managing digital identity and trail: controlling personal data that remains in the digital space; setting up privacy in social networks; using secure authentication methods (two-factor authentication); ability to identify disinformation and critically evaluate information: analysis of information sources

for reliability; recognition of manipulative content and fake news; identification of malicious or fraudulent websites; understanding of the basics of computer systems and software, basic knowledge of operating systems, network protocols, security settings; use of secure communication channels (VPN, data encryption); detection of suspicious activity on devices and accounts; safe digital communication and culture of online behavior: observance of rules of etiquette on the Internet (netiquette); avoidance of sending confidential information through unsecured channels; awareness of the risks of online communication and social engineering; understanding of legal and ethical aspects of digital security: familiarization with legal norms on personal data protection (Ukrainian legislation); awareness of responsibility for cyberbullying, illegal circulation of information and copyright infringement; adherence to the principles of information ethics; protection of health and well-being in the digital environment, prevention of digital addiction and cyberbullying; compliance with the rules of visual hygiene and safe use of gadgets; awareness of the psychological impact of digital technologies.

Based on the analysis of scientific literature, possible ways to modernize teacher training programs to develop students' digital security skills are identified: integration of digital security into courses on computer science teaching methods; development and implementation of specialized courses on digital security in educational and professional teacher training programs; use of digital tools and simulations to develop practical digital security skills; promotion of cooperation and knowledge exchange with professionals.

The second chapter clarifies the essence and structure of future computer science teachers' readiness to develop students' digital security skills, and models the process of forming the readiness of future computer science teachers to develop students' digital security skills based on the information approach.

Based on the results of the terminological analysis of the key concepts of the study ("readiness", "readiness for professional activity", "teacher's readiness"), the essence of the key category of the study was clarified: computer science teachers' readiness to develop students' digital security skills as an integrative personal ability

of a future computer science teacher to develop students' digital security skills, which combines: conscious aspirations for such development; specific knowledge and skills; skills of reflection on the success of such development. The identified essence led to the consideration of the concept of "computer science teachers' readiness to develop students' digital security skills" as a complex personal formation that combines three components:

- the motivational component (the desire to develop students' digital security skills) characterizes students' awareness of the need to develop them. It is the foundation of their motivation to act in this direction. This awareness affects their professional activities, promotes personal development, and provides a safe educational environment;
- the subject-methodological component (specific knowledge and skills) combines the subject understanding of digital security and methodological understanding of strategies for developing students' digital security skills. It is characterized by a combination of subject knowledge, knowledge of methodological approaches to developing digital security skills, as well as psychological and pedagogical knowledge and skills to select methods/approaches/teaching tools for developing students' digital security skills;
- the personal component (skills of reflection on the success of developing students' digital security skills) is an important component of readiness. It includes reflective activities that allow analyzing one's own level of digital security, improving teaching methods, developing critical thinking in students, and realizing the ethical aspects of digital interaction.

Based on the generalization of scientific results, the necessity of using the information approach as a leading one in shaping future computer science teachers' readiness to develop students' digital security skills is substantiated since it is the information approach that allows future teachers to master the principles of safe interaction in the digital environment, develop skills in critical analysis of information, protection of personal data and ethical use of digital resources. The application of this approach in the training of computer science teachers makes it

possible to develop their ability to anticipate potential risks of the digital environment, analyze information threats, and adapt the educational process to changes in cybersecurity. Active engagement with digital platforms, information management tools, and data protection tools allows future educators not only to master digital security personally but also to pass this knowledge on to students effectively. The information approach provides a systematic understanding of how information circulates in the digital environment, what mechanisms affect its security, and how to teach students to protect themselves from possible threats.

Using the modeling method, the process of forming future computer science teachers' readiness to develop students' digital security skills based on the information approach was illustrated. The author's model is based on the principles (scientificity and relevance, systematicity, competence orientation, practice orientation, integration and interdisciplinarity) in organizing the teaching of the special course "Digital Security in the Learning Environment" in the traditional form (lectures, practical classes) using active and problem-based learning methods and various digital learning tools (digital learning environments, digital educational resources, and specialized programs).

In the third section, the diagnostic tools of the study are developed, and the effectiveness of the model of forming future computer science teachers' readiness to develop students' digital security skills based on the information approach is experimentally tested.

Based on the structural and logical analysis, taking into account the definition of the category "future computer science teachers' readiness to develop students' digital security skills" and the characteristics of its components, criteria, and indicators of the formation of motivational, subject-methodological, and personal components of readiness were developed. The study used motivational, competence, and behavioral criteria, which are expressed by four indicators: "the degree of awareness of the need to develop digital security skills in students"; "knowledge of methodological approaches to developing digital security skills"; "ability to select

methods/approaches/teaching tools for developing digital security skills in students"; "desire for professional development in the field of digital security".

The study uses comparative analysis to characterize four levels of future computer science teachers' readiness to develop students' digital security skills: initial, basic, high, and creative. The article presents a briefly phased course of the research process: at the first stage, theoretical and practical analysis and substantiation of the research problem were carried out, existing contradictions were identified to clarify the subject of the study, and the scientific apparatus of the research and the corresponding thesaurus was developed; at the second stage, the model of formation of future computer science teachers' readiness to develop students' digital security skills based on the information approach was developed and substantiated; the third stage was determined by the experimental implementation of the model of formation of future computer science teachers' readiness to develop students' digital security skills based on the information approach; at the final, fourth stage, statistical analysis of data was carried out, and qualitative conclusions were drawn.

As a leading method of scientific and pedagogical research, the pedagogical experiment is used to confirm theoretical conclusions through statistical methods. The empirical data collected during the pedagogical experiment for all indicators confirmed the positive changes in the average for the EG compared to the CG: the subject-methodological component of future computer science teachers' readiness to develop students' digital security skills acquired the most significant dynamics in the EG – both indicators showed a significant increase in the average (9.07 and 2.52 vs. 12.22 and 3.59, respectively). The statistical analysis confirmed the primary assumption of our study about the effectiveness of the developed model of forming future computer science teachers' readiness to develop students' digital security skills based on the information approach.

The problems identified in the study and the results obtained gave grounds for formulating recommendations for developers and teachers who implement educational programs for training computer science teachers.

In particular, the lack of a consistent and effective digital security policy in computer science teacher education programs may have delayed negative consequences. Integrating digital security courses into computer science teacher education programs should go beyond isolated elective or optional courses and become a normative component of the curriculum. Education institutions should develop a culture of lifelong learning for professional development in digital security.

The scientific novelty of the study is that

– for the first time, a model of forming future computer science teachers' readiness to develop students' digital security skills based on the information approach was developed, theoretically substantiated and experimentally tested, which provides for compliance with the principles (scientificity and relevance, systematicity, competence orientation, practice orientation, integration and interdisciplinarity) in organizing the teaching of the special course "Digital Security in the Learning Environment" in the traditional form (lectures, practical classes) using active and problem-based learning);
– the concept of "computer science teachers' readiness to develop students' digital security skills" (the integrative personal ability of a future computer science teacher to develop students' digital security skills, which combines conscious aspirations for such development; specific knowledge and skills; skills of reflection on the success of such development) is clarified; the structure of computer science teachers' readiness to develop students' digital security skills is characterized through the triad of its components (motivational, subject-methodological, personal);
– diagnostic tools have been developed, and the levels (initial, basic, high, creative) of the future computer science teacher's readiness to develop students' digital security skills have been characterized;
– the methods and means of training future computer science teachers to develop students' digital security skills in higher education institutions, scientific ideas about the structure of future computer science teachers' readiness to develop

students' digital security skills, criterion and level signs of future computer science teachers' readiness to develop students' digital security skills were further developed.

Key words: future computer science teachers, digital security skills, information approach, teacher readiness, professional training.

Scientific works,
in which the main scientific results of the dissertation are published

Articles in scientific professional publications of Ukraine

1. **Dubinsky V.** Information approach in education and its use in the training of computer science teachers to form students' digital safety skills. *Академічні візії, 2024. 38*. https://doi.org/10.5281/zenodo.14594487. Отримано з https://www.academy-vision.org/index.php/av/article/view/1587.

2. **Dubinsky V.** Training of computer science teachers for the formation of cybersecurity skills in students: actualization of problems and their possible solutions. *Освіта. Інноватика. Практика*, 2024. Том 12, № 10. С. 6-11. https://doi.org/10.31110/2616-650X-vol12i10-001.

3. **Dubinsky V. O.** The readiness of computer science teachers to develop students' digital security skills. *Scientific Innovations and Advanced Technologies" (Series "Management and Administration", Series "Law", Series "Economics", Series "Psychology", Series "Pedagogy"),* 2025. № 2(42). С. 1075-1087. https://doi.org/10.52058/2786-5274-2025-2(42)-1075-1087.

Research work which publishes the main scientific results in international publications

4. Dubinsky V. Digital security skills of computer science teachers: generalization of the results of scientific papers. *Academia Polonica*. 2024. Vol. 67(6). Pp. 22-29. https://doi.org/10.23856/6703.

Articles in periodical scientific journals of foreign countries and publications included into the world's scientometric databases Scopus and Web of Science

5. M. Yachmenyk et al., "Development of Information and Media Literacy in the System “Students-Parents-Teachers”: Ukrainian Practice," 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, pp. 430-435, doi: 10.1109/MIPRO60963.2024.10569314 (Scopus)

Scientific works certifying the approbation of the dissertation materials

6. **Dubinsky V. O.**, Shamonia V. G. On the development of information and digital competence of future teachers of vocational education. *Vectors of Development of Science, Education, Technology and Society in the Context of Globalization: Collection of Abstracts of the International Scientific and Practical Conference (Poltava, October 19, 2023): in 2 parts: CFEMS*, 2023. Part 1. P.17-18.

7. **Dubinsky V. O.**, Shamonia V. G. On information and digital competence as a modern pedagogical category. Scientific activity as a way of forming professional competencies of a future specialist (SPC-2023) : Materials of the International Scientific and Practical Conference, December 7-8, 2023, Sumy. Sumy : FOP Tsioma S.P.,2023. P. 26-27.

8. **Dubinsky V.** Academic integrity is an integral component of the information and digital competence of future teachers of VET. The academic culture of the researcher in the educational space: European and national experience: a collection of materials of the VII International Scientific and Practical Conference (Sumy, May 17-18, 2024) / edited by O. Semenog. Sumy : Sumy Makarenko State Pedagogical University, 2024. P. 172-174.

9. **Dubinsky V. O.**, Shamonia V. G. On developing information and digital competence in non-formal education. Information technologies in the socio-cultural sphere, education, and economy: materials of the III International Scientific and Practical Conference of Students and Young Scientists. Kyiv : KNUKiM Publishing Center, 2024. P.93-95.

10. Dubinsky V., Shamonia V. On the development of students' digital security skills based on the information approach. *Scientific activity as a way of forming professional competencies of a future specialist (SPC-2024) : Materials of the International Scientific and Practical Conference (December 5-6, 2024, Sumy). Sumy : Sumy State Pedagogical University named after A. S. Makarenko, 2024. P*. 12-13.

ПЕРЕЛІК СКОРОЧЕНЬ

CS – computer science (комп’ютерні науки, інформатика)

DDoS - атаки типу «відмова в обслуговуванні»

IoT – інтернет речей

MR - змішана реальність

OECD - Organisation for Economic Co-operation and Development (Організація економічного співробітництва та розвитку).

VR - віртуальна реальність

ЕОР - електронні освітні ресурси

ЗВО – заклади вищої освіти

ІКТ - інформаційно-комунікаційні технології

ІТ - інформаційні технології

ОПП - освітньо-професійні програми

ПЗ - програмне забезпечення

ЦТ – цифрові технології

ШІ – штучний інтелект

ЗМІСТ

ВСТУП

Стрімкий розвиток цифрових технологій змінив суспільства в усьому світі, створивши взаємопов’язане глобалізоване «інформаційне суспільство». Цифрова трансформація забезпечила широкі можливості для спілкування, співпраці та економічного зростання і водночас спровокувала значні виклики, у т.ч. цифрову безпеку членів суспільства. Цифровий ландшафт постійно розвивається, і тому із загрозливою швидкістю з’являються нові технології та вразливості. Кіберзлочинці стають все більш витонченими, використовують передові методи для використання слабких місць не лише у системах і мережах, а й у суспільстві в цілому. Фішингові атаки, розповсюдження шкідливого програмного забезпечення, витоки даних та атаки типу «відмова в обслуговуванні» (DDoS) стали руйнівними чинниками як для окремих осіб, бізнесу, так і для урядів, призвели до фінансових і репутаційних втрат та, навіть, компрометації національної безпеки.

Взаємопов’язаний характер інформаційного суспільства означає, що успішна атака на одну сутність (уряд, бізнес, фінансова система, фізична особа тощо) може мати каскадні наслідки для багатьох систем і організацій. Розвиток сьогодні штучного інтелекту та машинного навчання ще більше ускладнює ландшафт загроз, оскільки такі технології можуть бути використані для автоматизації атак та ускладнення їх виявлення чи пом’якшення. Наслідки порушень цифрової безпеки виходять за рамки безпосередньої фінансової та репутаційної шкоди, вони впливають на приватність і благополуччя окремої особистості, що підкреслює важливість профілактичних заходів у сфері цифрового захисту.

Ефективна цифрова безпека ґрунтується не лише на технологічних рішеннях, а й на знаннях та навичках кожної особи. Навички цифрової безпеки передбачають розуміння загроз в Інтернеті, звичку безпечного перегляду Інтернет-джерел, розпізнавання спроб фішингу, використання надійних паролів та впровадження відповідного програмного забезпечення для безпеки даних. Такі навички мають важливе значення для зниження суспільних

ризиків та захисту суспільства від цифрових загроз, і тому саме суспільство має приділяти першочергову увагу формуванню й постійному розвитку навичок цифрової безпеки. Забезпечення цифрової безпеки дітей є відповідальністю всього суспільства, а підготовка компетентних учителів є ключовим фактором успіху в цьому напрямку.

В Україні прийнято низку нормативно-правових документів, які спрямовані на підвищення цифрової грамотності та забезпечення інформаційної безпеки громадян: Концепція розвитку цифрових компетентностей (2021), затверджена розпорядженням Кабінету Міністрів України, визначає стратегічні напрями розвитку цифрових навичок населення; Стратегія інформаційної безпеки (2021), затверджена Указом Президента України, визначає актуальні виклики та загрози національній безпеці в інформаційній сфері, а також стратегічні цілі та завдання, спрямовані на протидію таким загрозам (документ підкреслює важливість розвитку цифрових навичок та кіберобізнаності громадян для забезпечення інформаційної безпеки держави); Закон України "Про основні засади забезпечення кібербезпеки України" (2017 зі змінами) визначає правові та організаційні основи захисту життєво важливих інтересів людини, суспільства та держави у кіберпросторі, встановлює обов’язки державних органів щодо забезпечення кібербезпеки та підкреслює необхідність формування навичок цифрової безпеки серед населення; Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" (2021) акцентує увагу на тому, що цифрові навички та кіберобізнаність щодо сучасних кіберзагроз і методів протидії їм повинні стати невіддільними елементами освіти кожного громадянина України; Рекомендації Міністерства освіти і науки України щодо безпеки дітей у цифровому просторі (2021) для педагогічних працівників та батьків щодо забезпечення безпеки дітей в інтернеті, підкреслюючи спільну відповідальність за підтримку та навчання дітей безпечному використанню цифрового середовища. Перелічені та інші нормативні документи створюють

основу для формування та розвитку навичок цифрової безпеки молоді в українському суспільстві, забезпечують правові та організаційні умови для підвищення цифрової грамотності молоді.

Узагальнення низки наукових досліджень свідчить про актуальність проблеми цифрової грамотності вчителів (І. Воротнікова, Р. Гуревич, Л. Коношевський, М. Носкова, O. Stoika та ін.) або конкретних технологічних інструментів для забезпечення цифрової безпеки (М. Біличенко, Н. Касьянова, Ю. Кірпічніков, А. Рибидайло, А. Севериненко та ін.). Низка досліджень актуалізують поточні проблеми підготовки вчителів до використання інформаційних технологій (ІТ) (В. Биков, В. Осадчий, М. Шишкіна, О. Семеніхіна, О. Спірін та ін.) та вчителів інформатики до ефективної професійної діяльності в умовах НУШ (П. Бабіч, Н. Дегтярьова, І. Шишенко, А. Юрченко та ін.), не торкаючись безпосередньо навичок цифрової безпеки. Водночас активно піднімаються питання медіаінформаційної грамотності (О. Семеног, М. Ячменик та ін.) та інформаційної гігієни молоді (М. Друшляк, Ю. Руденко, О. Семеніхіна та ін.).

Вивчення доробку науковців показує, що незважаючи на зростаючу важливість освіти в галузі цифрової безпеки, у підготовці вчителів інформатики наявна низка викликів і прогалин, серед яких ми виділяємо:

- відсутність належної підготовки вчителів інформатики в галузі цифрової безпеки (І. Іванюк, О. Овчарук) - наявні освітні програми не завжди враховують еволюційний характер цифрових загроз і важливість опанування учителями конкретних педагогічних підходів, необхідних для ефективного навчання;

- обмежений доступ до ресурсів і технологій (Т. Вдовичин, А. Яцишин) - ефективна освіта в галузі цифрової безпеки вимагає доступу до відповідних ресурсів і технологій, однак прослідковується нестача необхідних ресурсів (фінансових, адміністративних, освітніх тощо) для своєчасного придбання й оновлення програмного забезпечення, надання надійного доступу до мережі Інтернет, що може серйозно обмежити здатність учителів

ефективно здійснювати професійну діяльність. Швидкий розвиток технологічного ландшафту ускладнює вчителям своєчасне оновлення їхніх знань та вмінь щодо розвитку навичок цифрової безпеки учнів. Вчителям може не вистачати наявних результатів професійної підготовки для коректної оцінки навчальних досягнень учнів у галузі цифрової безпеки тощо.

Перелічені та інші виклики свідчать про наявність суперечностей:

- між швидким розвитком інформаційних технологій, який спричинює появу цифрових загроз, та вразливістю членів суспільства через фрагментарну освіченість суспільства у галузі цифрової безпеки, недостатній розвиток у членів суспільства навичок цифрової безпеки;
- між суспільним запитом на безпечне використання молоддю ІТ та недостатньою увагою закладів освіти до відповідної підготовки вчителів інформатики щодо розвитку навичок цифрової безпеки молоді ;
- між потенціалом закладів вищої освіти щодо якісної підготовки вчителів інформатики та відсутністю ефективних моделей професійної підготовки вчителів інформатики, орієнтованих на формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.

Актуальність проблеми, її практична значущість та недостатня теоретична й практична розробленість, а також необхідність вирішення суперечностей визначили тему дослідження **«Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу»**.

Об’єкт дослідження – процес професійної підготовки майбутніх учителів інформатики закладах вищої освіти.

Предмет дослідження – формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

Мета дослідження – теоретично обґрунтувати та експериментально перевірити ефективність модулі формування готовності майбутніх учителів

інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

Для досягнення поставленої мети було визначено такі **завдання дослідження.**

1. Охарактеризувати цифрові загрози і відповідні навички цифрової безпеки молоді та довести важливість їх розвитку в умовах інформаційного суспільства.
2. Оцінити стан розробленості проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.
3. Уточнити сутність і структуру готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.
4. Розробити і теоретично обґрунтувати модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.
5. Розробити діагностичний інструментарій дослідження та експериментально перевірити ефективність моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

Для розв'язання завдань використано такі **методи дослідження:**

теоретичні:

– *аналіз, систематизація, узагальнення* нормативних та науково-методичних джерел для виявлення стану розробленості проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів;

– *термінологічний аналіз* – для уточнення сутності поняття «готовність майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів» та *структурно-логічний аналіз* для виділення структури цього поняття і характеристики критеріїв їх сформованості;

– *моделювання* для унаочнення процесу формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу;

емпіричних:

– *педагогічне спостереження* за освітнім процесом, *анкетування* для виявлення практичного стану розробленості проблеми дослідження;

– *педагогічний експеримент* для перевірки ефективності формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу;

статистичні:

– *методи математичної статистики* – для статистичного аналізу результатів експериментальної роботи (методи описової статистики та критерій Стьюдента оцінки середніх).

Наукова новизна дослідження полягає у тому, що

– *вперше розроблено, теоретично обґрунтовано та експериментально перевірено* модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу, яка передбачає дотримання принципів (науковість та актуальність, системність, компетентісна орієнтованість, практико-орієнтованість, інтеграція та міждисциплінарність) при організації навчання спецкурсу «Цифрова безпека у навчальному середовищі» у традиційній формі (лекції, практичні заняття) з використанням активних і проблемних методів навчання та різних цифрових засобів навчання (цифрові навчальні середовища, цифрові освітні ресурси та програми спеціалізованого спрямування);

– *уточнено* поняття «готовність учителів інформатики до розвитку навичок цифрової безпеки учнів» (інтегративна особистісна здатність майбутнього вчителя інформатики розвивати навички цифрової безпеки учнів, яка поєднує: усвідомлені прагнення такого розвитку; специфічні знання й уміння; навички рефлексії щодо успішності такого розвитку); *охарактеризовано структуру* готовності вчителів інформатики до розвитку навичок цифрової безпеки учнів через тріаду його компонентів (мотиваційний, предметно-методичний, особистісний);

– *розроблено* діагностувальний інструментарій та схарактеризовано рівні (початковий, базовий, високий, творчий) готовності майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів ;

– *подальшого розвитку набули* методи і засоби підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів у закладах вищої освіти, наукові уявлення про структуру готовності майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів, критеріальні та рівневі ознаки готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.

Практичне значення одержаних результатів полягає в розробці та впровадженні у процес професійної підготовки майбутніх учителів інформатики: методичного супроводу спецкурсу «Цифрова безпека у навчальному середовищі»; діагностичного інструментарій для визначення рівнів готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів (авторські завдання для комп'ютерного тестування за показником «знання методичних підходів для розвитку навичок цифрової безпеки», компетентнісні практико-орієнтовані завдання за показником «уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки в учнів», анкетування за показниками «ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів» і «прагнення до професійного розвитку в галузі цифрової безпеки»).

Результати дослідження можна використовувати вченим та викладачам для імплементації теоретичного і практичного доробку в освітньо-професійні програми підготовки вчителів інформатики, розширення переліку вибіркових дисциплін, розробки програм підвищення кваліфікації вчителів у системі післядипломної освіти, а також здобувачам освіти при написанні кваліфікаційних робіт.

Результати дослідження **апробовані** у таких ЗВО України: Сумський державний педагогічний університет імені А.С. Макаренка (довідка про впровадження № 542/1 від 21.02.2025), Харківський національний

педагогічний університет імені Григорія Сковороди (довідка про впровадження № 01/10-244 від 17.03.2025), Уманський державний педагогічний університет імені Павла Тичини (довідка про впровадження № 470/01 від 14.03.2025).

Публікації. Основні наукові результати подано у 10 публікаціях автора (із них 5 – одноосібні): 3 статті у фахових виданнях України, 1 стаття в закордонному виданні, 5 матеріалів апробаційного характеру, 1 стаття додатково відбиває результати наукового пошуку та індексується наукометричною базою Scopus.

Особистий внесок здобувача у роботах, написаних у співавторстві (за списком публікацій, що подані в додатку Є), полягає: у підборі аналітичних матеріалів [5]; узагальненні результатів термінологічного аналізу [6; 7]; обґрунтуванні доцільності неформальної освіти для професійного розвитку вчителів у галузі ІТ [9]; обґрунтуванні інформаційного підходу для розвитку навичок цифрової безпеки [10].

Апробація результатів дисертаційного дослідження. Основні положення та результати дисертаційної роботи доповідалися та отримали позитивну оцінку на наукових, науково-методичних і науково-практичних конференціях та семінарах різних рівнів:

міжнародних: «Вектори розвитку науки, освіти, технологій і суспільства в умовах глобалізації» (Полтава, 19 жовтня 2023 р.); «Наукова діяльність як шлях формування професійних компетентностей майбутнього фахівця» (Суми, 7-8 грудня 2023 р., 5-6 грудня 2024 р.); «Академічна культура дослідника в освітньому просторі: європейський та національний досвід» (м. Суми, 17-18 травня 2024 р.); «Інформаційні технології в соціокультурній сфері, освіті та економіці» (Київ, 2024).

Матеріали дисертаційного дослідження доповідалися й обговорювалися на засіданнях кафедри інформатики, науково-методичних семінарах Лабораторії використання інформаційних технологій в освіті Сумського державного педагогічного університету імені А. С. Макаренка (2023-2025 рр.).

Структура та обсяг дисертації. Дисертація складається з анотацій, переліку умовних позначень, вступу, трьох розділів, висновків, списку використаних джерел (200 найменувань) та 8 додатків. Дисертація містить 11 таблиць, 30 рисунків.

Загальний обсяг дисертації становить 237 сторінок, із них основний текст – 159 сторінок.

РОЗДІЛ 1.
ПІДГОТОВКА МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ ДО РОЗВИТКУ НАВИЧОК ЦИФРОВОЇ БЕЗПЕКИ УЧНІВ ЯК ПЕДАГОГІЧНА ПРОБЛЕМА

1.1. Навички цифрової безпеки та важливість їх розвитку в умовах інформаційного суспільства

Сучасне суспільство стрімко змінюється під впливом цифрових технологій, які стали невід'ємною частиною повсякденного життя. Люди користуються інтернетом для спілкування, навчання, роботи, фінансових операцій та розваг. Хмарні сервіси, мобільні додатки, соціальні мережі та електронна комерція відкрили нові можливості для розвитку, але водночас зробили користувачів більш вразливими до загроз цифрового середовища.

Із поширенням цифрових технологій зростає і потреба у забезпеченні безпеки інформації. Витоки персональних даних, несанкціонований доступ до облікових записів, фінансові шахрайства та кібератаки стали серйозними викликами для як окремих користувачів, так і цілих організацій. У таких умовах цифрова безпека вже не є питанням вибору — це необхідність, без якої неможливо гарантувати захист особистої інформації та конфіденційності даних.

Важливим аспектом забезпечення цифрової безпеки є формування відповідних навичок у членів суспільства. Навіть найсучасніші технологічні рішення залишаються вразливими, якщо користувачі не вміють ними правильно користуватися. Загалом навички цифрової безпеки сьогодні асоціюють здатність розпізнавати потенційні загрози, захищати персональні дані, створювати надійні паролі, користуватися двофакторною автентифікацією та критично оцінювати інформацію в цифровому просторі. Проте перед тим, як говорити про конкретні навички, варто зрозуміти, які саме

загрози існують у цифровому середовищі та яким чином вони можуть впливати на безпеку користувачів і організацій.

Сучасні цифрові загрози є різноманітними та постійно еволюціонують, створюючи нові виклики для інформаційної безпеки.

Цифрові загрози – це широкий спектр загроз, пов'язаних з використанням цифрових технологій. Вони можуть впливати на індивідів, організації та навіть цілі держави, завдаючи значних економічних, соціальних та політичних збитків. Розуміння природи цих загроз є критично важливим для розробки ефективних стратегій захисту. Цифрові загрози можна класифікувати за різними критеріями, включаючи їхню природу, ціль та метод атаки (рис.1.1). Деякі з найпоширеніших типів включають:

Рис.1.1. Класифікація цифрових загроз (за [181])

Зловмисне програмне забезпечення (Malware) – це будь-яка програма, розроблена для пошкодження комп'ютерних систем або крадіжки даних [168]. До поширених типів malware належать віруси, трояни, черв'яки, шкідливі програми-вимагачі (ransomware) та spyware [168]. Віруси розмножуються, заражаючи інші файли, тоді як трояни маскуються під легітимні програми та не є очевидними відразу. Черв'яки поширюються самостійно через мережу, без потреби в зараженні інших файлів. Шкідлива програма Ransomware блокує доступ до даних, вимагаючи викуп за їх розблокування. Інша програма Spyware стежить за активністю користувача та збирає конфіденційну інформацію [181]. Ефективність захисту від malware сьогодні залежить від використання надійного антивірусного програмного забезпечення та регулярного оновлення програмного забезпечення [**Ошибка! Источник ссылки не найден.**].

Кібератаки – це цілеспрямовані атаки на комп'ютерні системи або мережі з метою отримання несанкціонованого доступу, крадіжки даних або пошкодження системи. Ці атаки можуть бути здійснені різними методами, включаючи phishing, SQL injection, DDoS атаки та інші [168].

Phishing – це вид соціальної інженерії, який використовує підроблені електронні листи або веб-сайти для отримання конфіденційної інформації, такої як паролі або номери кредитних карток [181].

SQL injection – це метод атаки, який використовує вразливості в базах даних для отримання несанкціонованого доступу до даних[181].

DDoS атаки – це розподілені атаки на відмову в обслуговуванні, які перевантажують цільову систему запитами, роблячи її недоступною для легітимних користувачів [137]. Захист від кібератак вимагає комплексного підходу, включаючи використання брандмауерів, систем виявлення вторгнень та систем запобігання вторгненням, а також навчання співробітників щодо безпеки в інтернеті [181].

Соціальна інженерія (Social Engineering) – це метод маніпулювання людьми для отримання конфіденційної інформації або доступу до систем.

Зловмисники використовують психологічні методи, такі як обман або шантаж, щоб переконати жертву розкрити свої паролі або інші важливі дані [168]. Соціальна інженерія може включати phishing, pretexting (створення правдоподібного приводу для контакту), baiting (заманювання жертви на шкідливий ресурс) та інші методи. [181] Навчання співробітників розпізнавати та уникати методів і підходів соціальної інженерії є важливим і дієвим інструментом захисту від цього типу загроз. [137].

Внутрішні загрози – це загрози, що виникають зсередини організації, наприклад, від незадоволених співробітників або зловмисників, які мають доступ до внутрішніх систем безпеки [166]. Такі загрози можуть включати крадіжку даних, саботаж або несанкціонований доступ до інформації [168]. Тому ефективний контроль доступу та моніторинг активності співробітників є важливими заходами для мінімізації внутрішніх загроз [181].

Джерела цифрових загроз можуть бути різними (рис.1.2) [168; 181].

Рис.1.2. Джерела цифрових загроз та їх наслідки

Вони включають*:* хакерів, кіберзлочинців та інших зловмисників, які прагнуть отримати несанкціонований доступ до даних або систем; віруси, трояни, черв'яки та інші типи malware, які можуть заражати системи та красти

дані; помилки в програмному забезпеченні, які можуть бути використані зловмисниками для отримання несанкціонованого доступу; людські помилки співробітників або користувачів, які можуть призвести до витоку даних або зараження систем; державні органи, які можуть використовувати кібератаки для досягнення політичних або економічних цілей.

Наслідки цифрових загроз можуть бути серйозними та включати [166; **Ошибка! Источник ссылки не найден.**] різні види втрат, серед яких відзначимо фінансові втрати коштів внаслідок крадіжки даних, викупу або пошкодження систем, репутаційні втрати (людини або організації) через пошкодження репутації внаслідок витоку даних або кібератак; юридичні проблеми, зокрема, штрафи та судові позови внаслідок порушення законів про захист даних. Також можливі перебої в роботі систем або сервісів внаслідок кібератак або збоїв та витік конфіденційних даних, що може призвести до значних особистих наслідків. Тому для пом’якшення ризиків, пов’язаних з цифровими загрозами, рекомендують вжити комплексних заходів [168; 181;137], які включають захист даних (використання шифрування, резервного копіювання та інших методів захисту даних), захист мереж (використання брандмауерів, систем виявлення вторгнень та систем запобігання вторгненням), оновлення програмного забезпечення для усунення вразливостей; навчання співробітників щодо безпеки в інтернеті та розпізнавання цифрових загроз. Також використовуються моніторинг та аналіз систем і мереж для вчасного виявлення та реагування на загрози. Дієвими вважається попереднє планування реагування на можливі інциденти (план реагування на інциденти безпеки для швидкого та ефективного усунення наслідків атак).

Отже, цифрові загрози є актуальною проблемою сучасного світу, побудованого на цифрових технологіях. Для ефективного захисту від можливих загроз необхідно використовувати комплексний підхід, який включає технічні, організаційні та людські аспекти, зокрема, розвиток відповідних знань про можливі загрози кіберпростору.

Надалі розглянемо сутність і види цифрових небезпек. Поширення цифрових технологій у суспільстві відкрило еру безпрецедентної можливості для організації якісного зв’язку та комунікації. Однак ця цифрова трансформація також створила новий перелік небезпек, який вимагає від кожного члена суспільства глибокого розуміння їхньої природи.

Цифрові небезпеки можна широко класифікувати. Зокрема, розрізняють навмисні (зловмисні) і ненавмисні небезпеки. Кібератаки як навмисні цифрові ризики охоплюють широкий спектр зловмисних дій, спрямованих на використання вразливостей у цифрових системах для особистої вигоди або збою. Їх класифікація проведена на основі джерел [83; 51; 108; 7; 79; 66; 125; 49].

1. Витік та крадіжка даних. Витоки даних, часто спричинені хакерськими атаками або шкідливим програмним забезпеченням, становлять серйозну цифрову загрозу, до якої відносимо крадіжку конфіденційної особистої інформації, фінансових даних або інтелектуальної власності може мати серйозні наслідки як для окремих осіб, так і для організацій. Масштаби та наслідки витоків даних є значними, а глобальні витрати на їх відповідь сягають сотень мільярдів доларів щорічно.

2. Зловмисне програмне забезпечення та програми-вимагачі. Шкідливе програмне забезпечення, що включає віруси, хробаки, трояни та інше шкідливе програмне забезпечення, становить значну загрозу для цифрової безпеки. Програми-вимагачі, особливо підступні форми шкідливого програмного забезпечення, шифрують дані та вимагають оплату за їх випуск. Фінансові наслідки лише програм-вимагачів складають щорічно мільйони доларів викупу.

3. Фішинг та соціальна інженерія. Фішингові атаки, що включають оманливі електронні листи або веб-сайти, призначені для викрадення облікових даних, є широко поширеною цифровою небезпекою. Соціальна інженерія використовує людську психологію для маніпулювання людьми, щоб змусити людей розголошувати конфіденційну інформацію або виконувати дії,

що ставлять під загрозу їхню безпеку. Ефективність цих атак вимагає постійного навчання користувачів і розробки надійних механізмів аутентифікації. Фінансовий та репутаційні збитки від успішних фішингових кампаній можуть бути значними.

4. Атаки типу «відмова в обслуговуванні» (DDoS). DDoS-атаки наповнюють онлайн-системи трафіком, роблячи їх недоступними для законних користувачів. Ці атаки можуть порушити роботу основних сервісів, спричинивши фінансові втрати та репутаційні збитки компаній. Зростаючий масштаб і складність DDoS-атак вимагають проактивних стратегій пом’якшення наслідків і надійного проєктування інфраструктури інформаційної системи. Вплив на бізнес та критичну інфраструктуру може бути серйозним і призводити до значних простоїв та фінансових втрат.

Ненавмисні цифрові небезпеки, системні збої та помилки включають небезпеки, що виникають внаслідок непередбачених наслідків цифрових систем або людської помилки. Їх класифікація зроблена на основі джерел [83; 125; 37; 98; 56].

1. Помилки та вразливості програмного забезпечення. Програмні баги і вразливості притаманні складним цифровим системам. Ці недоліки можуть бути використані зловмисниками або призвести до системних збоїв. Тому важливою стає потреба в ретельному тестуванні програмного забезпечення та його постійних оновленнях. Наслідки невиявлених помилок можуть варіюватися від незначних незручностей до катастрофічних збоїв системи.

2. Збої в роботі системи. Системні збої можуть бути наслідком збоїв у роботі обладнання, програмних помилок або стихійних лих. Ці події можуть серйозно порушити роботу сервісів і спричинити значні фінансові втрати. Надійний дизайн системи, резервування та планування аварійного відновлення мають важливе значення для пом’якшення цих ризиків. Взаємопов’язаність сучасних систем збільшує потенційний вплив каскадних збоїв.

3. Втрата та пошкодження даних. Втрата або пошкодження даних може бути наслідком апаратних збоїв, програмних помилок або людської помилки. Це може призвести до значних фінансових втрат та значних витрат часу на відновлення. Для зниження цього ризику мають важливе значення регулярне резервне копіювання, надійні методи управління даними та плани відновлення даних. В цьому випадку цифрової небезпеки наслідки особливо серйозні для організацій, які покладаються на критично важливі дані для власної діяльності.

4. Дезінформація. Стрімке поширення дезінформації цифровими каналами теж становить значну загрозу для суспільства. Неправдиві або оманливі наративи можуть негативно впливати на громадську думку, завдавати шкоди репутації та підбурювати до насильства. Боротьба з таким видом цифрової небезпеки вимагає освіти з медіаграмотності, ініціатив з перевірки фактів (факт-чекінгу) та підзвітності платформ.

5. Питання цифрового розриву та доступності. Цифровий розрив, що характеризується нерівним доступом до технологій та різним рівнем цифрової грамотності, створює диспропорції у можливостях та послугах для членів суспільства. Цифровий розрив може посилити існуючу соціальну нерівність та обмежити доступ до важливої інформації та ресурсів. Подолання цифрового розриву вимагає інвестицій в інфраструктуру, інвестицій у медіаосвіту та навчальні програми цифрової грамотності, інформаційної грамотності та цифрової гігієни. Наслідки цифрового розриву особливо відчутні для вразливих груп населення.

В контексті цифрових загроз розглядаються цифрові ризики, які проявляються по-різному в різних секторах економіки і вимагають окремих стратегій для свого пом’якшення. Так, сектор охорони здоров’я дуже вразливий до витоків даних, атак програм-вимагачів і збоїв у роботі важливих Health-систем [83]. Наслідки можуть варіюватися від порушення конфіденційності пацієнтів до збоїв у наданні медичних послуг, тому надійні заходи кібербезпеки й навчання персоналу мають важливе значення для

зниження таких ризиків. Авіаційна промисловість значною мірою покладається на цифрові системи навігації, зв'язку та технічного обслуговування [7]. Кібератаки, спрямовані на ці системи, можуть мати значні негативні наслідки, і тому удосконалені протоколи кібербезпеки, надійні системи управління безпекою та міжнародне співробітництво є важливими для уникнення цифрових ризиків. Фінансовий сектор є основною мішенню для кібератак через значні обсяги фінансових даних [51]. Витік даних, фішингові атаки та програми-вимагачі можуть спричинити значні фінансові втрати та репутаційні збитки, тому важливими є надійні заходи кібербезпеки, зокрема, системи виявлення шахрайства.

Зростаюча автоматизація та цифровізація виробничих процесів в умовах Індустрія 4.0 вносять нові загрози безпеці [54]. Кібератаки можуть порушити роботу, пошкодити обладнання та поставити під загрозу системи безпеки. Надійні заходи кібербезпеки та навчання працівників мають важливе значення для пом'якшення цих ризиків. Інтеграція пристроїв інтернету речей (IoT) та штучного інтелекту також знаходиться у зоні ризику та вимагає ретельного аналізу безпеки й захисту [23]. Ініціативи електронного врядування (цифрове суспільство) роблять уряди й урядові установи вразливими до кібератак, які можуть оприлюднити/ поширити/ модифікувати конфіденційні дані, порушити роботу сервісів і підірвати довіру громадськості до цих установ [12]. Тому важливе значення для суспільства мають надійні заходи кібербезпеки, дотримання правил захисту даних та своєчасне навчання відповідних фахівців.

Отже, цифрові небезпеки створюють значні виклики для всіх секторів сучасного суспільства. У той час як швидкі темпи технологічного прогресу продовжують створювати нові вразливості, всебічне розуміння природи та типів цифрових загроз у поєднанні з впровадженням ефективних стратегій пом'якшення наслідків має важливе значення для побудови стійких і безпечних цифрових екосистем.

Узагальнення пропозицій науковців і фахівців-практиків у галузі безпеки свідчить, що боротьба з цифровими небезпеками вимагає

комплексного підходу, який включає технологічні, процедурні та людські заходи. До технологічних заходів відносять: впровадження надійних брандмауерів, систем виявлення вторгнень та шифрування даних [49]; регулярні оновлення та виправлення програмного забезпечення, підтримка останнього в актуальному стані [37]; багатофакторна автентифікація через додавання рівнів аутентифікації [52]; резервне копіювання та відновлення даних [83]; проактивний моніторинг для виявлення і вчасного реагування на загрози [49]; системи безпеки на основі штучного інтелекту для виявлення загроз та реагування на них [49]; технологія цифрових двійників як моделювання систем і процесів для виявлення вразливостей і тестування стратегій їх пом'якшення [50; 100].

До процесуальних заходів відносять: встановлення чітких політик безпеки та їх послідовне дотримання [49]; навчання про загрози кібербезпеці та опанування кращих практик запобігання кіберзагроз [83]; регулярні аудити та оцінки безпеки для проактивного усунення вразливостей [7] та інші.

До заходів щодо роботи з людиною відносять: своєчасну освіту користувачів про фішинг, соціальну інженерію та інші загрози [66]; дотримання практики надійних паролів [66]; розвиток критичного мислення для виявлення підозрілої активності [125]; створення чітких каналів для повідомлення про інциденти безпеки [83].

Термінологічний аналіз понять «кібербезпека» та «цифрова безпека»

Наступним кроком у дослідженні став термінологічний аналіз понять «кібербезпека» та «цифрова безпека». Ці поняття часто використовуються як синоніми, що призводить до плутанини щодо їхніх точних значень та нюансів взаємозв'язку. Незважаючи на тісний зв'язок між собою, вони представляють різні, хоча й схожі концепції в більш широкій галузі інформаційної безпеки.

Кібербезпека зосереджена на захисті комп'ютерних систем, мереж і даних від несанкціонованого доступу, використання, розкриття, збою, модифікації або знищення [70; 113]. Вона охоплює широкий спектр технологій, процесів і практик, призначених для забезпечення

конфіденційності, цілісності та доступності інформації в цифровій сфері. Кібербезпека часто асоціюється із запобіганням та пом'якшенням наслідків кібератак, включаючи зараження шкідливим програмним забезпеченням, фішингові атаки (часто реалізується через фальшиві електронні листи, сайти або повідомлення, які змушують жертву ввести свої дані), атаки програм-вимагачів та витік даних, який може включати персональні дані, фінансову інформацію, логіни та паролі, що призводить до фінансових збитків, репутаційних втрат і ризику шахрайства.

Ця сфера включає в себе технічні заходи, такі як брандмауери, системи виявлення вторгнень і шифрування, а також нетехнічні заходи, такі як навчання з питань безпеки та планування реагування на інциденти [22; 32]. Фінансовий сектор, наприклад, стикається з викликами кібербезпеки через високу вартість своїх цифрових активів і складність кіберзагроз, спрямованих на фінансові установи [65]. Зростаюча інтеграція штучного інтелекту (AI або ШІ) та машинного навчання (ML або МН) трансформує кібербезпеку, забезпечуючи більш проактивне виявлення загроз та адаптивні механізми захисту [40; 76].

Цифрова безпека, з іншого боку, охоплює більш широку сферу, включаючи кібербезпеку, але виходить за її межі і охоплює додатково захист усіх форм цифрових активів та інформації [3]. Йдеться про безпеку різних цифрових платформ, систем і додатків, для яких важливі конфіденційність даних, управління ідентифікацією та захист інтелектуальної власності [114]. Цифрова безпека розглядає весь життєвий цикл цифрових активів, від їх створення та зберігання до їх передачі та утилізації [86]. Такий підхід включає в себе як технічні, так і нетехнічні заходи, визнаючи *важливість людського фактора* у пом'якшенні ризиків [72]. Перехід від просто фізичної безпеки до цифрової підкреслює еволюцію парадигм безпеки [86], наголошує на необхідності розроблення й упровадження інтегрованих стратегій, спрямованих на боротьбу як з фізичними, так і з цифровими загрозами [8].

Незважаючи на різницю в масштабах, кібербезпека та цифрова безпека мають кілька спільних характеристик. До них відносимо с*пільну мету*, оскільки обидві спрямовані на захист важливих цифрових активів від несанкціонованого доступу, використання, модифікації або знищення. Ця спільна мета обумовлює необхідність впровадження надійних заходів безпеки, незалежно від конкретного контексту [80; 113].

Спільною характеристикою є багаторівневий підхід до реалізації, що включає технічні та нетехнічні заходи: технічні заходи включають шифрування, брандмауери та системи виявлення вторгнень; нетехнічні заходи включають навчання з питань безпеки, планування реагування на інциденти та встановлення сильної організаційної політики [32; 22].

Іншою спільною проблемою є швидкозмінний тип загроз, оскільки самі технології та відповідно безпекові заходи набувають розвитку і нових форм. Зростаюча складність кібератак обумовлює необхідність розробки та впровадження передових технологій і стратегій безпеки [40; 101].

Спільними є важливість проактивного управління ризиками, що включає своєчасне виявлення вразливостей, оцінку ризиків, впровадження відповідних заходів контролю, регулярний моніторинг загроз [9; 94] та розвиток відповідної правової бази, оскільки обидва поняття підпадають під дію різних законодавчих та регуляторних рамок, спрямованих на захист осіб, організацій та національної безпеки. Ці рамки, як правило, часто стосуються конфіденційності даних, інтелектуальної власності та захисту критичної інфраструктури [65].

Маючи спільні цілі та підходи, поняття «кібербезпека» та «цифрова безпека» відрізняються за своїм масштабом та спрямованістю. Кібербезпека, в першу чергу, пов’язана з безпекою комп’ютерних систем, мереж і даних. Цифрова безпека, з іншого боку, охоплює набагато ширший спектр цифрових активів та інформації, включаючи інтелектуальну власність, цифрові ідентичності та фінансові дані.

Кібербезпека зосереджена на запобіганні та пом’якшенні кібератак. Цифрова безпека використовує більш цілісний підхід, що охоплює весь життєвий цикл цифрових активів та інформації, включаючи їх створення, зберігання, передачу та утилізацію.

Кібербезпека часто робить акцент на технічних заходах контролю, таких як брандмауери та системи виявлення вторгнень, тоді як цифрова безпека може приділяти більше уваги дотриманню законодавства, управлінню даними та рамкам управління ризиками.

Кібербезпека часто обговорюється в контексті конкретних технологій або систем, таких як хмарні обчислення, пристрої інтернету речей (IoT) або промислові системи управління. Цифрова безпека розглядає ширший контекст, охоплюючи соціальні, економічні та політичні наслідки поширення цифрових технологій.

У контексті нашого дослідження виділяємо додаткову *важливість нетехнічних заходів з цифрової безпеки, які включають навчання з питань цифрової безпеки та формування навичок цифрової безпеки.*

Загальна характеристика навичок цифрової безпеки

Визначення навичок цифрової безпеки охоплює цілий спектр знань, умінь та поглядів, пов’язаних із захистом себе та своїх даних у цифровому середовищі і включає розуміння різних типів кіберзагроз, таких як крадіжка даних, кібератаки та шахрайство [142], знання того, як виявляти та уникати спроб фішингу, а також впроваджувати безпечні методи паролів [60]. Цифрова безпека поширюється на управління своїм цифровим слідом і репутацією [36], а також на розуміння налаштувань конфіденційності на різних цифрових платформах [60]. Інформаційна грамотність є базовою для цифрової безпеки і передбачає серед іншого здатність виявляти дезінформацію [10; 60]. Це додатково передбачає розуміння природи різних форматів медіа та їх потенційних упереджень [60].

Комп’ютерна грамотність, що включає базове розуміння організації та функціонування комп’ютерних систем і програмного забезпечення, також має

важливе значення для визначення характеристик цифрової грамотності, а тому включає в себе знання операційних систем, додатків і протоколів безпеки. Крім того, цифрова безпека передбачає критичну оцінку джерел інформації в Інтернеті на предмет надійності та упередженості, розуміння правових та етичних наслідків поведінки в Інтернеті та практику відповідальної взаємодії в Інтернеті [2].

Навички цифрового спілкування охоплюють безпечну та відповідальну взаємодію в Інтернеті, включають обізнаність про етикет в Інтернеті та потенціал кібербулінгу. Відповідно, до цифрової безпеки слід віднести розуміння наслідків свого онлайн-спілкування та його потенційних наслідків. Методи цифрової безпеки, такі як управління паролями, звички безпечного перегляду та використання антивірусного програмного забезпечення, мають важливе значення для захисту персональних даних [25]. Для цього потрібно розуміти, як виявляти та уникати спроб фішингу та інших видів шахрайства в Інтернеті. Також важливо сформувати відповідальне та етичне використання цифрових технологій, сприяння безпеці та благополуччю в Інтернеті, а також повагу до прав та конфіденційності інших. Це вимагає розуміння правових та етичних наслідків поведінки в Інтернеті та дотримання її високих стандартів.

Отже, наведені аргументи свідчать про широту навичок цифрової безпеки та підкреслюють важливість їх випереджувального формування. У нашому дослідженні будемо так інтерпретувати поняття «навички цифрової безпеки».

Навички цифрової безпеки – це сукупність знань та умінь для безпечного, відповідального та етичного використання цифрових технологій, яка забезпечує особі захист особистих даних, цифрової ідентичності, пристроїв і мереж від кібератак, а також сприяє свідомому онлайн-спілкуванню (рис.1.3).

Таким чином, навички цифрової безпеки охоплюють технічні, інформаційні, комунікаційні та правові аспекти безпечної взаємодії в

цифровому середовищі, що є важливим для сучасного інформаційного суспільства.

Розуміння кіберзагроз та способів їх уникнення	Управління цифровою ідентичністю та слідом
Ідентифікація основних видів загроз (фішинг, шкідливе програмне забезпечення, атаки програм-вимагачів) Використання антивірусного програмного забезпечення та фаєрволів Захист пристроїв від несанкціонованого доступу	Контроль над особистими даними, що залишаються в цифровому просторі Налаштування конфіденційності в соціальних мережах Використання безпечних методів аутентифікації (двофакторна автентифікація, надійні паролі)
Здатність виявляти дезінформацію та критично оцінювати інформацію	*Розуміння основ функціонування комп'ютерних систем та програмного забезпечення*
Аналіз джерел інформації на достовірність Розпізнавання маніпулятивного контенту та фейкових новин Виявлення шкідливих або шахрайських сайтів	Базові знання про операційні системи, мережеві протоколи, налаштування безпеки Використання захищених каналів зв'язку (VPN, шифрування даних) Виявлення підозрілої активності на пристроях та в облікових записах

Рис. 1.3. Основні *навички цифрової безпеки*

Важливість розвитку навичок цифрової безпеки в інформаційному суспільстві важко переоцінити. Зростаюча залежність від цифрових технологій робить окремих осіб і організації вразливими до широкого спектру кіберзагроз з потенційно руйнівними наслідками. Тому популяризація знань про цифрові загрози, формування навичок цифрової безпеки молоді ще зі школи, відповідна випереджувальна підготовка вчителів різних предметів і особливо вчителів інформатики мають важливе значення для побудови більш безпечного та стійкого цифрового суспільства.

1.2. Стан розробленості проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів

У сучасному світі стрімкого розвитку цифрових технологій важливість цифрової безпеки важко переоцінити. Молоде покоління, яке постійно взаємодіє з онлайн-ресурсами, дедалі частіше стикається з ризиками, пов’язаними з кіберзагрозами, шахрайством, булінгом та недостовірною

інформацією [179]. У зв'язку з цим особливого значення набуває здатність учителів інформатики навчати учнів навичок цифрової безпеки, що включає як технічні, так і соціальні аспекти роботи в інформаційному середовищі.

Формування навичок цифрової безпеки у школярів є не лише складовою освітнього процесу, а й запорукою створення безпечного цифрового простору, необхідного для подальшого розвитку суспільства. Готовність учителів інформатики до виконання цієї задачі має комплексний характер і включає професійні компетентності, педагогічну майстерність, знання нормативно-правової бази та гнучкість у впровадженні інноваційних методик.

Формування навичок цифрової безпеки вимагає комплексного підходу [196], який має включати розуміння онлайн-загроз (люди повинні знати про різні типи кіберзагроз, включаючи шкідливе програмне забезпечення, фішинг та атаки соціальної інженерії) і наявність практичного досвіду безпечного перегляду (обережність щодо відвіданих веб-сайтів, уникнення підозрілих посилань та використання надійних паролів), розпізнавання спроб фішингу (фішингові електронні листи та повідомлення як напрям кібератак), використання надійних паролів для захисту облікових записів і даних від несанкціонованого доступу, використання відповідного захисного програмного забезпечення (тобто досвід встановлення антивірусного програмного забезпечення, брандмауерів та інших інструментів безпеки) й оновлення операційних систем для виправлення вразливостей безпеки. При формуванні навичок цифрової безпеки важливо також сформувати навички безпечного використання персональних пристроїв, таких як смартфони й ноутбуки, та навички безпечного поводження у соціальних медіа (налаштування конфіденційності, уникнення ризиків небезпечного спілкування тощо). Особливий акцент варто робити на обізнаності щодо конфіденційності даних - треба розуміти свої права щодо конфіденційності даних та вміти захистити свою особисту інформацію в Інтернеті.

На заваді ефективному формуванню навичок цифрової безпеки стоять кілька факторів. Однією з помітних проблем є швидкий розвиток технологій і

кіберзагроз. Постійно виникають нові проблеми, які швидко призводять до того, що наявні знання та навички застарівають [99]. Це вимагає постійного навчання та адаптації, чого може бути важко досягти за допомогою поширених освітніх моделей, методів і засобів навчання молоді.

Ще одним значним бар'єром є недостатня обізнаність та усвідомлення суспільством важливості цифрової безпеки. Багато людей недооцінюють ризики, пов'язані з діяльністю в Інтернеті, що призводить до недбалої поведінки [36]. Цей брак обізнаності особливо виражений серед певних демографічних груп, таких як люди похилого віку та люди з обмеженою цифровою грамотністю [25]. Також складність концепцій цифрової безпеки може лякати осіб, які не мають технічної підготовки [151]. Використовувана термінологія та технічні деталі можуть створювати перешкоди для розуміння кіберзагроз громадянами та впровадження відповідного захисту або його мінімізації.

Відсутність через швидкий розвиток ІТ усталених програм навчальних дисциплін з кібербезпеки також ускладнює зусилля освітян з формування навичок цифрової безпеки [99]. Непослідовність у підході до відповідної освіти в галузі цифрової безпеки в різних установах та організаціях призводить до фрагментарного та неефективного освітнього результату. Обмеженість ресурсів, включно із доступом до технологій, сучасних засобів навчання та кваліфікованих викладачів, інструкторів, непропорційно впливає на певні групи населення, посилюючи наявну нерівність і розрив у цифровій грамотності та безпеці [25].

Зростаюча залежність від цифрових технологій у всіх аспектах життя вимагає всебічного розуміння цифрової безпеки, починаючи з молоді. Тому саме освітяни, особливо вчителі інформатики, відіграють ключову роль у сприянні розумінню цифрової безпеки. Аналіз досліджень, присвячених підготовці вчителів інформатики формувати в учнів навички цифрової безпеки дозволяє усвідомити поточний стан ситуації та виявити потенційні шляхи для усунення наявних прогалин.

За результатами аналізу та систематизації публікацій ми виявили кілька важливих практичних напрямів розробленості проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів (рис. 1.4).

Сприйняття цифрової безпеки вчителями (оцінка власної компетентності, рівень готовності до навчання цифрової безпеки).

Ми виявили кілька досліджень, які безпосередньо стосуються сприйняття вчителями інформатики та майбутніми вчителями інформатики власних знань та навичок цифрової безпеки. Дослідження [161], присвячене підготовці майбутніх учителів в Іспанії, виявило значну розбіжність у сприйнятті компетентності залежно від статі. Жінки-вчителі, які здобувають освіту, хоча й компетентні з техніко-педагогічної точки зору, відчували, що їм бракує достатньої теоретичної та практичної підготовки з цифрової безпеки. На противагу цьому, чоловіки, майбутні вчителі, сприймали себе як достатньо компетентних, можливо, завдяки попередній підготовці в галузі інформаційно-комунікаційних технологій (ІКТ). Ця невідповідність підкреслює потребу в більш інклюзивних та ефективних навчальних програмах, які враховують різноманітні потреби та досвід вчителів різних предметів.

Рис. 1.4. Практичні аспекти розробленості проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів

Науковці Alazam et al. [41] досліджували готовність вчителів з позицій сформованості знань, грамотності та ставлення до цифрової трансформації в освіті. Хоча вони виявили помірно високий рівень готовності вчителів до формування знань, у дослідженні наголошується на важливій ролі ставлення вчителів до цифрової грамотності учнів та їхньому впливі на ефективність

формування цифрових навичок молоді, включаючи навички цифрової безпеки. Згадане дослідження підкреслило потребу в програмах професійного розвитку вчителів, які не лише надають знання та навички, але й враховують ставлення та переконання вчителів щодо цифрової трансформації суспільства та її важливості для кожного. Зосередження уваги дослідження на вчителях у сільській місцевості також підкреслює необхідність вирішення конкретних проблем, з якими стикаються вчителі в громадах, що мають обмежений доступ до ресурсів (зокрема, Інтернет).

Дослідження Хасескі [42] щодо сформованості навичок кібербезпеки вчителів свідчить про значний взаємозв'язок між компетентністю особистості у сфері кібербезпеки та позитивним ставленням до комп'ютеризованої освіти. У дослідженні підкреслюється усвідомлення майбутніми вчителями важливості формування навичок кібербезпеки як основи для ефективної інтеграції технологій у викладацьку практику та сприяння у створенні ефективного і безпечного освітнього середовища.

Методи навчання цифрової безпеки (інтерактивні підходи, гейміфікація, проєктне навчання, кейси).

Дослідник Олів'є [78] аналізує кейс-метод і піднімає важливі етичні міркування щодо формування потенційно шкідливих навичок, таких як хакерські методи, які є важливими для освіти в галузі кібербезпеки. У статті обґрунтовується важливість впровадження такої освіти у професійні спільноти, які встановлюють етичні принципи та заохочують їх відповідальне використання у професійній діяльності. Дослідження додатково підкреслює потребу в програмах професійного розвитку, які не лише передбачають формування/ розвиток технічних навичок, але й сприяють формуванню сильного почуття професійної етики серед викладачів і вчителів інформатики в галузі цифрової безпеки.

Використання гейміфікації у викладанні кібербезпеки описують Томбре та Веланкар [107]. Науковці досліджують ефективність навчання через підвищення зацікавленості та мотивації здобувачів освіти. Дослідження

показало, що вчителі можуть використовувати активні методи навчання, серед яких - ігрові.

Стаття [165] описує дослідницький метод навчання та присвячена аналізу українських та зарубіжних відкритих освітніх ресурсів як інструменту професійного розвитку педагогів у контексті навчання школярів безпечному використанню мережі Інтернет. У статті акцентовано увагу на ключовій ролі вчителів у формуванні в учнів навичок цифрової безпеки, зокрема керування особистими даними, критичної оцінки цифрового контенту, правил комунікації в соціальних мережах та безпечної поведінки в онлайн-середовищі.

У статті [74] демонструється ефективність науково обґрунтованих програм професійного розвитку для ефективного навчання в галузі цифрової безпеки і підкреслюється важливість інтерактивних методів професійного розвитку з акцентом на активному навчанні та співпраці. Навчання з кібербезпеки можна покращити шляхом інтеграції цифрових інструментів і технологій, таких як віртуальні лабораторії, симуляції та онлайн-платформи. Програми підготовки вчителів повинні надавати освітянам можливість брати участь у постійному навчанні через різні канали, про що зазначено у [169].

Дослідження Liesaputra et al. [57] підтверджує ефективність науково-популярних заходів для популяризації цифрової безпеки. Автори описують семінар, який включає цифрову безпеку як частину міждисциплінарного підходу до освіти з інформатики. Позитивні відгуки як учнів, так і вчителів свідчать про те, що інтеграція цифрової безпеки в більш широку освіту з інформатики може бути корисною.

Інституційні та кадрові виклики (необхідність підвищення кваліфікації, проблеми оплати праці вчителів, кадровий дефіцит).

Кібербезпека – це сфера, яка постійно розвивається і вимагає постійного навчання та розвитку цифрових навичок. Програми підготовки вчителів повинні заохочувати та підтримувати безперервний професійний розвиток у сфері кібербезпеки шляхом надання доступу до семінарів, онлайн-курсів,

конференцій та професійних спільнот. Це може включати встановлення партнерських відносин з організаціями з кібербезпеки та галузевими експертами, щоб запропонувати спеціалізовані можливості навчання для вчителів. Це може бути також реалізовано через додаткове навчання на семінарах, онлайн-курсах з кібербезпеки та формуванні навичок саморозвитку ще у процесі формального навчання. Відзначимо, що акцент на безперервному навчанні в галузі кібербезпеки [187] вказує на те, що програми підготовки вчителів повинні не лише забезпечувати початкові навички кібербезпеки, а й заохочувати постійний професійний розвиток у цій сфері.

Створення можливостей для вчителів інформатики ділитися своїм досвідом, найкращими практиками та ресурсами, пов’язаними з освітою в галузі цифрової безпеки, може бути дуже дієвим інструментом розвитку навичок цифрової безпеки. Це може включати створення онлайн-спільнот, організацію семінарів і конференцій, а також розробку спільних проєктів, орієнтованих на освіту в галузі цифрової безпеки. Відзначається, що співпраця та спільне використання ресурсів між учителями інформатики може значно покращити освіту з цифрової безпеки, а онлайн-платформи, такі як Google Classroom та Microsoft Teams, можуть полегшити спілкування та співпрацю між учителями. При цьому спільні репозиторії, такі як GitHub і GitLab, можуть надати платформу для обміну навчальними матеріалами, планами уроків і ресурсами з цифрової безпеки. Професійні навчальні спільноти, організовані школами, районами або професійними організаціями, можуть стати форумом для вчителів, щоб обговорювати проблеми освіти з цифрової безпеки та обмінюватися найкращими практиками.

Зокрема, у статті [90] проаналізовано особливості вибору курсів для формування інформаційної гігієни здобувачів освіти, які передбачають розвиток навичок цифрової безпеки. Крім того, важливі рекомендації та підтримку можуть надати програми наставництва, де досвідчені фахівці з цифрової безпеки наставляють вчителів інформатики. Тому заохочення

співпраці та обміну знаннями між вчителями інформатики має важливе значення для сприяння ефективній освіті з цифрової безпеки.

У дослідженні [174] виявлено суперечності між необхідністю забезпечення цифрової безпеки в педагогічній та науково-педагогічній діяльності та недостатньою розробленістю й обґрунтованістю змісту цифрової компетентності в галузі безпеки майбутніх викладачів. Науковцями наголошено на зростанні інтенсивності кібератак у національному кіберпросторі в умовах повномасштабної війни та нагальною потребою у фахівцях із високим рівнем цифрової грамотності для відновлення та технологічного розвитку країни у післявоєнний період. Дослідники обґрунтували, що відповідно до Рамки цифрової компетентності для громадян України, навички цифрової безпеки мають ураховувати захист пристроїв і безпечне підключення до мережі Інтернет, захист персональних даних і приватності, безпеку в цифровому середовищі, протидію шахрайству та зловживанням, а також захист здоров’я, добробуту та довкілля.

Інше дослідження [158] описує український досвід підготовки вчителів інформатики та наголошує, що за рівнем кваліфікації категорія вчителів інформатики залишається найнижчою. Наголошується на важливості ролі вчителів математики та інформатики у формуванні фундаментальних знань учнів, зокрема, щодо обізнаності про цифрову безпеку.

Науковці [62] виявили, що пандемія підкреслила необхідність професійного розвитку для підвищення цифрових навичок вчителів. Вони наголошують на важливості адаптації до нових методів викладання й навчання, які передбачають освіту з цифрової безпеки. Також як висновок підкреслюється нагальна потреба в постійній підтримці та навчанні вчителів для гарантії того, що вчителі можуть ефективно орієнтуватися в складнощах цифрової освіти, включаючи найкращі практики цифрової безпеки.

У дослідженні [87] встановлено професійні прогалини у вчителів, пов’язані з цифровою грамотністю та ефективним використанням цифрових технологій в освітній діяльності. Інформаційна безпека та етика в цифровому

середовищі були виділені як ключові сфери професійного розвитку. Автори дослідження підкреслили нагальну потребу інтеграції цифрової безпеки в навчальні програми підготовки вчителів. Зосередженість дослідження як на формальному, так і на неформальному професійному розвитку, включаючи самоосвіту та спонтанне навчання, дали змогу дослідниками визнати різноманітність шляхів навчання, що сьогодні доступні вчителям, та важливість підтримки як формальних, так і неформальних можливостей для навчання.

Цифрова безпека як складник цифрової компетентності (інтеграція цифрової безпеки в навчальні програми, зв'язок із загальною цифровою грамотністю).

У дослідженні [34] піднімається проблема відсутності чітких вимог до цифрової грамотності фахівця в різних професіях. Науковці обговорюють проблеми навчання програмування студентів, які не вивчають інформатику, і зазначають про відсутність чітких визначень щодо вимог до цифрової грамотності та програмування у різних професіях. Це підкреслює потребу розробки й упровадження індивідуальних програм професійного розвитку, які враховують конкретні потреби вчителів різних предметів і особливо, учителів інформатики.

Дослідження [34] щодо рамок цифрової компетентності вчителів розширює розуміння необхідних навичок і знань для ефективної освіти в галузі цифрової безпеки. Рамкова програма наголошує на цілісному сприйнятті цифрової компетентності, яка включає етичне та безпечне функціонування суб'єктів освітнього процесу в різноманітних цифрових середовищах, що є ключовим компонентом освіти з цифрової безпеки. Поширення рамкової програми для міждисциплінарної взаємодії передбачає, що вчителі різних дисциплін повинні інтегрувати цифрову безпеку у свої навчальні програми, підкреслюючи важливість спільного та інтегрованого підходу до освіти з цифрової безпеки.

Регулярний перегляд та оновлення освітніх програм підготовки вчителів інформатики для приведення їх у відповідність до міжнародних стандартів та найкращих практик дотримання кібербезпеки може гарантувати, що вчителі оснащені новітніми знаннями та навичками в цій галузі, а їхня підготовка відповідає світовим стандартам. Це передбачає регулярний перегляд та оновлення змісту освітніх компонентів для того, щоб відобразити сучасні тенденції в галузі кібербезпеки [34]. Організації, як ISO та NIST, працюють над тим, що надати різноманітні ресурси та фреймворки, які можуть автоматизовано керувати розробкою навчальних програм з кібербезпеки та гарантувати, що програми підготовки вчителів відповідатимуть світовим стандартам.

Приведення освітньо-професійних програм підготовки вчителів інформатики у відповідність до міжнародних стандартів кібербезпеки має важливе значення для забезпечення вчителів найактуальнішими знаннями та навичками в галузі цифрової безпеки. Стандарт ISO/IEC 27000 забезпечує основу для систем управління інформаційною безпекою, які можуть бути використані як основа для розробки навчальних програм з кібербезпеки. NIST Cybersecurity Framework надає набір стандартів, вказівок і найкращих практик для управління ризиками кібербезпеки, які також можуть бути включені в програми підготовки вчителів [34]. Агентство Європейського Союзу з кібербезпеки (ENISA) пропонує різноманітні ресурси та навчальні матеріали, які можуть бути використані для покращення освіти в галузі кібербезпеки.

Освітньо-політичний аспект (розробка стандартів цифрової безпеки, державні ініціативи, рекомендації щодо кадрового забезпечення).

Науковці Ayanwale et al. [5] досліджували готовність вчителів інформатики до Education 4.0, зміни парадигми в бік технологічного навчання, яке за своєю суттю охоплює аспекти цифрової безпеки. Отримані ними результати виявили позитивну налаштованість вчителів до набуття необхідних навичок використання різних IT і закцентували увагу на важливості цілеспрямованих ініціатив для професійного розвитку вчителів.

Однак у дослідженні також наголошується на необхідності індивідуальних втручань, які враховують конкретні потреби вчителів з метою дозволити їм самостійно визначати ті навички, що пов’язані з Освітою 4.0 і які, на їх особисту думку, потребують розвитку. Зазначений висновок підкреслює важливість не лише навчання, але й забезпечення того, щоб навчання було актуальним, доступним та ефективно відповідало індивідуальним потребам учителів. Зосередженість цього дослідження на формуванні у студентів навичок для Індустрії 4.0 неявно визнає важливу роль цифрової безпеки та формування відповідних навичок як в учнів, так і у вчителів.

Наукові праці свідчать, що актуалізується проблема актуальності знань в галузі технологій. Науковці Twarek et al. [111] обговорюють перелік K-12 необхідних знань та навичок для ефективного навчання інформатики, який неявно включає навички цифрової безпеки. Стандарти CSTA 2020 року для вчителів інформатики (CS – computer science) забезпечують основу, яка потенційно може охоплювати цифрову безпеку як частину вимог до знань в галузі цифрових технологій та цифрової безпеки.

Вплив пандемії COVID-19 суттєво змінив методики викладання, змістившись у бік онлайн та дистанційного навчання. Цей перехід виявив прогалини в цифрових компетентностях вчителів, включаючи навички цифрової безпеки. Ми вивчили результати досліджень, в яких послідовно вказується на критичну потребу в посиленій підготовці та професійному розвитку вчителів у галузі цифрової безпеки. Зокрема, науковці Xayakot et al. [118] при вивченні проблеми підготовленості вчителів у Лаоській НДР визначили вдосконалення навичок кібербезпеки як ключовий фактор загального розвитку цифрової грамотності вчителів. Це додатково підтверджує аргумент на користь пріоритетності опанування цифрової безпеки в програмах підготовки вчителів інформатики. Кількісний підхід дослідження, що використовує структуровану анкету та множинний регресійний аналіз, надає аргументований висновок щодо важливості навичок кібербезпеки для цифрової грамотності вчителів.

Стаття [110] підкреслює, що вчителі демонструють готовність до цифрової трансформації, але стикаються з перешкодами в адаптації до цифрових інструментів та медіа. Цим науковці додатково актуалізують проблему цифрової грамотності вчителів та важливості організації особистого інформаційного простору за допомогою цифрових технологій. Останнє підкреслює необхідність розвитку у здобувачів освіти навичок безпечного та відповідального управління своїм цифровим слідом, що узгоджується з освітою в галузі цифрової безпеки.

Університетська підготовка майбутніх учителів *(модернізація освітніх програм, підвищення кваліфікації викладачів педагогічних ЗВО).*

Стрімкий розвиток технологій та загрози кібербезпеки зумовлюють необхідність постійного оновлення освітніх програм підготовки вчителів інформатики, про що наголошується у [187]. Це вимагає проактивного/ випереджувального підходу до розробки та регулярного перегляду й модернізації програм професійної підготовки вчителів інформатики, щоб гарантувати, що зміст таких програм залишається актуальним і відповідає поточним галузевим стандартам і провідним практикам підготовки фахівців педагогічних спеціальностей.

Науковці наголошують, що «навчальні програми з кібербезпеки занадто швидко застарівають», а тому потребують частих оновлень, можливо, на щорічній основі. Враховуючи характер сфери кібербезпеки, яка швидко розвивається, важливими для вчителів інформатики є безперервне навчання та професійний розвиток в цій галузі. Програми підготовки вчителів повинні не лише забезпечувати початкові навички кібербезпеки, але й заохочувати та підтримувати постійне навчання за допомогою семінарів, онлайн-курсів, конференцій та професійних спільнот. Науковці [187] наголошують на важливості навчання впродовж життя у сфері кібербезпеки.

Нам думку [187], освітньо-професійні програми підготовки вчителів могли б мати зиск від упровадження спеціалізованих курсів, орієнтованих на розвиток навичок цифрової безпеки. Ці курси можуть охоплювати такі теми,

як мережева безпека, захист даних, криптографія, етичний хакінг та реагування на інциденти. Зміст має бути адаптований до потреб вчителів інформатики, наголошуючи на педагогічних аспектах викладання цих понять учням. Повинні бути переглянуті поточні курси з методики навчання інформатики з метою включити до професійних програм методику формування навичок цифрової безпеки, що передбачає вивчення тем, пов'язаних із концепціями кібербезпеки, стратегіями навчання та методами оцінювання. Науковці вважають, що використання проєктного навчання може бути особливо ефективним для цього.

Дослідження [6] оцінює ефективність курсу з цифрової грамотності для вчителів суспільствознавства і фіксує слабкий рівень їх навичок цифрової безпеки. Це додатково підкреслює необхідність більш ефективних навчальних програм, орієнтованих на цифрову безпеку, для всіх вчителів, у тому числі з інформатики.

При виявленні рівня розвитку цифрової грамотності вчителів у статті [97] досліджувалися готовність і бар'єри на шляху інтеграції цифрових медіа в освіту. Дослідники встановили значні розбіжності в рівнях цифрової грамотності та брак довіри серед багатьох вчителів. Дослідження закцентувало увагу на необхідності цільового професійного розвитку та інфраструктурних інвестицій для покращення цифрових компетентностей вчителів, які мають включати компетентність у галузі цифрової безпеки.

Інше дослідження [81] зосереджується на різних стратегіях викладання тем курсу «Інформаційні системи», включаючи цифрову безпеку. Науковці наголошують на необхідності адаптації навчальних програм дисциплін і освітніх програм підготовки вчителів. Щоб йти в ногу з постійно змінюваними технологіями, важливе значення для вчителів інформатики має постійний професійний розвиток, який дозволяє постійно актуалізувати знання у цій галузі та ефективно викладати цифрову безпеку.

У процесі дослідження науковці Bendechache et al. [11] зосереджуються на проєкті, який залучає підлітків до розуміння штучного інтелекту, етики та

конфіденційності даних включно з питаннями приватності та безпеки даних. Дослідники підкреслюють важливість проведення семінарів з підготовки інструкторів/ тренерів для вчителів як інструменту впливу на професійний розвиток.

У дослідженні [67] науковці зосереджуються на розвитку у вчителів інформатики для дошкільної освіти компетентностей у галузі освітньої робототехніки і роблять висновок про важливість формування у вчителів навичок роботи з новими технологіями, які передбачають наявність навичок кібербезпеки.

Дослідники Cebrin-Robles та ін. [15] піднімають питання важливості цифрової компетентності для майбутніх учителів та необхідність вирішення таких питань, як академічний кіберплагіат та безпека даних. Вони припускають, що просування цифрових навичок учнів та використання інституційних репозиторіїв може допомогти зменшити ризики, пов’язані з неетичною поведінкою в Інтернеті. Це посилює потребу в комплексному підході до розвитку навичок цифрової грамотності, яке включає обізнаність з цифрової безпеки.

Шкільна освіта (адаптація навчальних матеріалів, методики викладання цифрової безпеки у школах).

Науковці Karaman et al. [53] підкреслюють важливу роль школи для забезпечення випереджувальної освіти з цифрової грамотності, включаючи безпеку особистої інформації та безпеку в Інтернеті. Вони наголошують на відсутності сьогодні стандартизованих навчальних програм та необхідності підготовки вчителів для вирішення проблеми недостатньо розвинених навичок цифрової грамотності серед вчителів. Це посилює потребу в структурованих програмах професійного розвитку, які враховують конкретні потреби вчителів у розвитку їхніх навичок цифрової безпеки.

У дослідженнях [156; 167] вивчалося ставлення вчителів інформатики до викладання комп’ютерної безпеки молодшим школярам. Хоча вчителі в цілому позитивно ставилися до включення освіти з комп’ютерної безпеки,

було відзначено відсутність різноманітності в їхніх поглядах, що засвідчило наявність потенційної сліпої зони в їхньому розумінні комплексного характеру цифрової безпеки та необхідності індивідуальних підходів для задоволення різноманітних груп учнів і підходів до їх навчання. Дослідження також підкреслило небажання вчителів активно взаємодіяти з батьками в дискусіях про цифрову безпеку, не зважаючи на визнання важливості участі батьків [132]. Це небажання підкреслює необхідність подальших досліджень бар'єрів, які перешкоджають ефективній комунікації між учителем і батьками щодо цифрової безпеки.

Kurniawan et al. [95] визначають цифрову безпеку та дезінформацію як проблеми, з якими стикаються у цифрову епоху учні старших класів. Вони підкреслюють необхідність того, щоб вчителі були підготовлені для вирішення цих проблем і навчали учнів безпечно та відповідально орієнтуватися в цифровому світі.

Професійний розвиток учителів (масові відкриті онлайн-курси, сертифікаційні програми, тренінги з цифрової безпеки).

Про доцільність використання відкритих онлайн-курсів за IT напрямом наголошується в [182]. Семінари та конференції, запропоновані професійними організаціями, такими як ISC2 та SANS, можуть забезпечити спеціалізоване навчання з конкретних тем кібербезпеки. Онлайн-курси, пропоновані такими платформами, як edX та Udacity, можуть запропонувати гнучкі та доступні можливості навчання. Професійні сертифікати, такі як CompTIA Security+ та CISSP, можуть продемонструвати компетентність вчителів у галузі кібербезпеки та підвищити їхню професійну кваліфікацію. Участь у конференціях дає можливість ознайомлення з позитивними освітніми практиками використання цифрових інструментів [91]. Крім того, участь в онлайн-спільнотах і форумах, таких як r/cybersecurity на Reddit і сайт інформаційної безпеки Stack Exchange, може надати вчителям інформатики доступ до знань і ознайомити з досвідом фахівців з кібербезпеки. Ці

платформи можуть надати вчителям практичний досвід роботи зі сценаріями кібербезпеки, аналізу вразливостей безпеки та впровадження заходів безпеки.

На нестачі сертифікованих вчителів інформатики і необхідності їх професійного розвитку для усунення прогалин в знаннях з інформаційної безпеки наголошують Ло і Лоулер [59]. Акцент на національній стурбованості щодо інформаційної безпеки посилює нагальність забезпечення вчителів необхідними знаннями та вміннями в цій галузі.

Швидкий розвиток технологій і кіберзагроз робить актуалізацію знань постійно складним завданням [170]. Багатьом викладачам не вистачає необхідних технічних навичок та досвіду, щоб впевнено формувати навички цифрової безпеки учнів [61]. Обмеженою слід вважати доступність високоякісних освітніх ресурсів, що відповідають віку учня [191]. Вчителі часто створюють власні матеріали, але це забирає в них багато часу [133].

Слід зважати і на цифровий розрив при впровадженні освітніх програм підготовки вчителів інформатики [148]. При цьому швидкі темпи технологічного прогресу обумовлюють необхідність постійного професійного розвитку вчителів інформатики [77] для забезпечення актуальності знань про загрози безпеці та позитивні практики формування навичок цифрової безпеки. Професійний розвиток можливий за рахунок семінарів з цифровій безпеці та освітніх технологій, доступу до онлайн-курсів, вебінарів та цифрових ресурсів на проблем цифрової безпеки [124] та ін.

Іншою проблемою стає виявлення прогалин у знаннях та навичках, пов’язаних із цифровою безпекою. До них відносяться недостатнє розуміння нових загроз (фішинг, шкідливе програмне забезпечення, програми-вимагачі тощо) [119], недостатнє знання протоколів безпеки та практик протидії загрозам [120], а також обмежений досвід реагування на інциденти та незнання методів їх усунення. Більшість навчальних програм через барак часу не в змозі належним чином розглянути етичні та правові наслідки цифрової безпеки, такі як конфіденційність даних та права інтелектуальної власності [33]. Це заважає майбутнім вчителям ефективно навчати своїх учнів.

Різні дослідження, зокрема [13], підкреслюють важливість цифрової грамотності, включаючи цифрову безпеку, у 21 столітті. Відсутність спеціальної підготовки з цифрової безпеки також може призвести до зниження якості підготовки студентів [68]. Швидкий розвиток технологій також вимагає забезпечення можливості професійного розвитку викладачів, щоб забезпечити актуальність наявних знань і бути в курсі останніх тенденцій у галузі кібербезпеки. Постійна поява нових технологій також ускладнює встановлення стандартизованих методів оцінки навичок кібербезпеки.

Інше дослідження [18] доводить, що успішним може бути проєкт професійного розвитку, орієнтований на освіту з питань цифрового громадянства, цифрової безпеки та цифрового захисту. Вчителі, які брали участь у проєкті, повідомили про підвищення задоволеності та більшу схильність до впровадження цифрової безпеки на своїх уроках. Це надає емпіричні докази ефективності цілеспрямованого професійного розвитку в галузі цифрової безпеки.

Підхід, описаний у [17] наголошує на важливості аспектів конфіденційності та безпеки у використанні цифрових технологій та необхідності постійного стажування (перепідготовки) вчителів для ефективного використання передових технологій. Науковці підкреслюють потребу в програмах професійного розвитку, які не лише розвивають технічні навички, але й вирішують етичні та безпекові наслідки використання технологій в освіті.

Підготовка майбутніх вчителів інформатики до ефективного розвитку навичок цифрової безпеки учнів вимагає значних інвестицій у ресурси інституційної підтримки. Значним бар’єром є відсутність достатніх ресурсів (фінанси; комп’ютерне обладнання, програмне забезпечення тощо), що перешкоджає ефективній реалізації програм підготовки вчителів [154]. Зокрема, це включає недостатнє фінансування спеціалізованого програмного та апаратного забезпечення, а також доступ до актуальних навчальних матеріалів з кібербезпеки. Багато установ стикаються з бюджетними

обмеженнями, що ускладнює виділення достатніх коштів на комплексне навчання в галузі цифрової безпеки. Ще більше загострює цю проблему відсутність спеціалізованої інфраструктури, такої як безпечні навчальні онлайн-середовища та добре обладнані комп'ютерні класи. Значною перешкодою є відсутність спеціалізованого персоналу технічної підтримки для допомоги вчителям і викладачам, а відсутність чітких керівних принципів та політик щодо інтеграції курсів з цифрової безпеки в освітні програми підготовки вчителів також зумовлює певні ризики для майбутнього.

Ми виокремлюємо проблеми (рис. 1.6) підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.

Узагальнення наукових результатів дає певні стратегії для вирішення проблем у формуванні навичок цифрової безпеки, які охоплюють формальну освіту, просвітницькі заходи та кампанії з підвищення обізнаності громадськості у цифрових загрозах та інструментах їх запобігання.

У працях [161; 73; 99] відзначається, що інтеграція цифрової безпеки в освітні програми має важливе значення для організації освітнього середовища. Однак це часто стикається з опором через часові обмеження та відчутну відсутність інтересу молоді до проблем цифрової безпеки [25]. Ефективні освітні програми з цифрової безпеки повинні бути адаптовані до різних вікових груп і рівнів технічної експертизи. Вони повинні гарантувати, що люди отримують необхідну інформацію та навички для захисту себе та своїх даних. Школи та університети повинні інтегрувати освіту з цифрової безпеки у свої навчальні програми, навчаючи учнів безпеці в Інтернеті.

Рис.1.6. Проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів

Науковці вважають потенційно ефективними інноваційні методи навчання, серед яких гейміфікація [123] та інтерактивні електронні навчальні блоки [1]. Ці методи дозволяють моделювати реальні сценарії, чим сприяють практикувати навички цифрової безпеки в безпечному та контрольованому середовищі.

Важливим є професійний розвиток у галузі цифрової безпеки серед професіоналів [173], які зацікавлені у індивідуальних навчальних програмах, орієнтованих на конкретні посадові обов'язки й потреби галузі [142]. Організації повинні проводити регулярні навчання для своїх співробітників, охоплюючи такі теми, як управління паролями, обізнаність про фішинг та політика захисту даних. Ці програми можуть бути зосереджені на конкретних загрозах безпеці та вразливостях, що стосуються конкретних професій.

Інформаційно-просвітницькі кампанії мають важливе значення для підвищення обізнаності та популяризації відповідальної поведінки в Інтернеті [2]. Ці кампанії можуть використовувати різні медіа-канали, такі як соціальні мережі, телебачення та онлайн-реклама, для охоплення широкої аудиторії [25]. Дослідники доводять, що використання чітких, лаконічних повідомлень і привабливих візуальних матеріалів є ключем до ефективної передачі складної інформації [151]. Кампанії також повинні бути зосереджені на практичних порадах і стратегіях, які люди можуть легко реалізувати.

Незважаючи на те, що поданий аналіз дає важливу інформацію про різні аспекти підготовки вчителів інформатики до розвитку навичок цифрової безпеки учнів, ми все ж можемо відзначити кілька значних прогалин у дослідженнях науковців. Багато досліджень зосереджені на загальній цифровій грамотності або конкретних технологічних інструментах, не торкаючись безпосередньо навичок цифрової безпеки. Тому вважаємо, що є необхідними дослідження щодо конкретизації знань, умінь та ставлення вчителів до формування навичок цифрової безпеки. Існує потреба в довгострокових дослідженнях, які відстежують знання та навички вчителів з

цифрової безпеки в часі та оцінюють вплив програм професійного розвитку на їхню викладацьку практику в галузі цифрової безпеки.

Проведений нами аналіз узагальнення наукових праць дає уявлення про загальні тенденції та проблеми щодо підготовки вчителів інформатики до формування в учнів навичок цифрової безпеки. У наукових публікаціях наголошується на необхідності постійного оновлення навчальних програм в галузі ІТ, акцентується потреба формування практичних умінь з цифрової безпеки, підкреслюється важливість опанування майбутніми учителями не лише предметних знань з цифрової безпеки, але й психолого-педагогічних і методичних знань та вмінь формувати в учнів навички цифрової безпеки; опанування інноваційних цифрових стратегій викладання і навчання інформатики. Науковці відзначають як ефективний змішаний спосіб викладання курсів і доводять ефективність різноманітних методів навчання. Окремі наукові розвідки наголошують на потребі розвитку методичної компетентності вчителів інформатики.

На основі аналізу наукової літератури бачимо можливі шляхи модернізації програм підготовки вчителів для формування в учнів навичок цифрової безпеки: інтеграція цифрової безпеки в курси з методики навчання інформатики; розробка й упровадження спеціалізованих курсів з цифрової безпеки у освітньо-професійні програми підготовки вчителів; використання цифрових інструментів та технологій симуляції для формування практичних навичок цифрової безпеки; сприяння співпраці та обміну знаннями з професіоналами; приведення навчальних програм у відповідність до міжнародних стандартів.

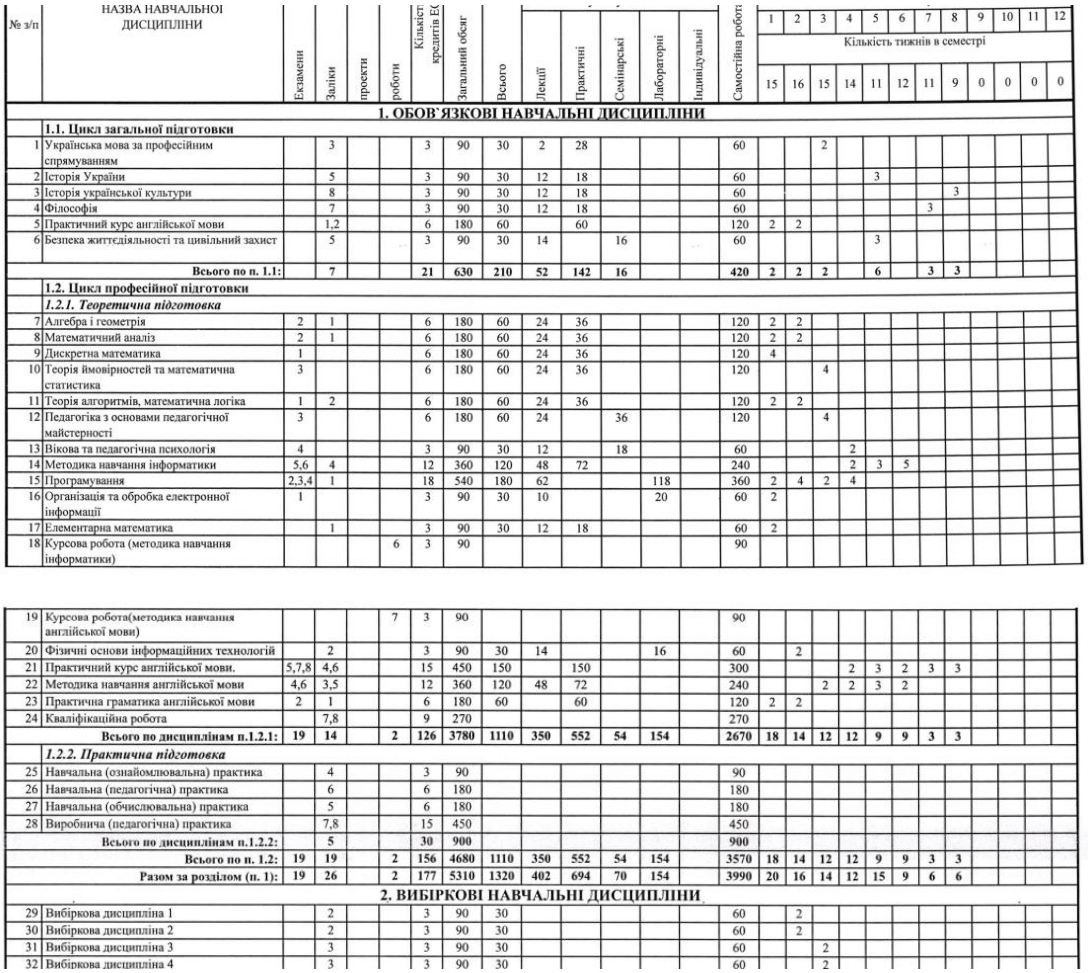
1.3. Аналіз програм підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів

Цифрова епоха кардинально змінила освіту, інтегрувавши інформаційні технології у викладання та навчання [122]. Цей зсув, хоч і корисний, створює

проблеми, особливо щодо інформаційних впливів [180] та цифрової безпеки. Тому інтеграція ІТ вимагає актуалізації, розуміння і сприйняття проблеми цифрової безпеки [143], яка має розглядатися не лише на державному рівні, а й на рівні освіти. Онлайн-платформи пропонують широке розмаїття навчальних курсів з цифрової безпеки. Водночас постійна поява нових загроз робить наявні навчальні матеріали застарілими. Це змушує освітян відповідати на виклики та шукати шляхи покращення освіти в галузі кібербезпеки, яка природно починається зі школи. Тому проблема підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів є актуальною.

Аналіз програм підготовки вчителів інформатики показує певну диспропорцію щодо навчання в галузі цифрової безпеки. Окремі освітні програми підготовки вчителів інформатики включають модулі з кібербезпеки, але деякі програми не торкаються (не передбачають) формування знань та умінь в цій галузі [154]. При цьому освітні програми часто зосереджені на теоретичних аспектах кіберзагроз і нехтують практичними навичками їх протидії у реальному житті [81]. Цей аспект з огляду на зростаючу складність кіберзагроз обумовлює важливу роль формування навичок цифрової безпеки в межах загальної підготовки для формування інтегральних практичних навичок протидії різним цифровим загрозам.

Сучасні програми підготовки вчителів інформатики різняться ([148; 47; 28] та ін.). Окремі з програм наведені на рисунку (рис.1.4, А-І).



№ з/п	НАЗВА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	Екзамени	Заліки	проекти	роботи	Кількість кредитів ЄК	Загальний обсяг	Всього	Лекції	Практичні	Семінарські	Лабораторні	Індивідуальні	Самостійна робота	1	2	3	4	5	6	7	8	9	10	11	12
															Кількість тижнів в семестрі											
															15	16	15	14	11	12	11	9	0	0	0	0
	1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																									
	1.1. Цикл загальної підготовки																									
1	Українська мова за професійним спрямуванням		3			3	90	30	2	28				60			2									
2	Історія України		5			3	90	30	12	18				60					3							
3	Історія української культури		8			3	90	30	12	18				60								3				
4	Філософія		7			3	90	30	12	18				60							3					
5	Практичний курс англійської мови		1,2			6	180	60		60				120	2	2										
6	Безпека життєдіяльності та цивільний захист		5			3	90	30	14		16			60					3							
	Всього по п. 1.1:		**7**			**21**	**630**	**210**	**52**	**142**	**16**			**420**	**2**	**2**	**2**		**6**		**3**	**3**					
	1.2. Цикл професійної підготовки																									
	1.2.1. Теоретична підготовка																									
7	Алгебра і геометрія	2	1			6	180	60	24	36				120	2	2										
8	Математичний аналіз	2	1			6	180	60	24	36				120	2	2										
9	Дискретна математика	1				6	180	60	24	36				120	4											
10	Теорія ймовірностей та математична статистика	3				6	180	60	24	36				120			4									
11	Теорія алгоритмів, математична логіка	1	2			6	180	60	24	36				120	2	2										
12	Педагогіка з основами педагогічної майстерності	3				6	180	60	24		36			120			4									
13	Вікова та педагогічна психологія	4				3	90	30	12		18			60				2								
14	Методика навчання інформатики	5,6	4			12	360	120	48	72				240				2	3	5						
15	Програмування	2,3,4	1			18	540	180	62			118		360	2	4	2	4								
16	Організація та обробка електронної інформації	1				3	90	30	10			20		60	2											
17	Елементарна математика		1			3	90	30	12	18				60	2											
18	Курсова робота (методика навчання інформатики)				6	3	90							90												
19	Курсова робота(методика навчання англійської мови)				7	3	90							90												
20	Фізичні основи інформаційних технологій		2			3	90	30	14			16		60		2										
21	Практичний курс англійської мови.	5,7,8	4,6			15	450	150		150				300				2	3	2	3	3				
22	Методика навчання англійської мови	4,6	3,5			12	360	120	48	72				240			2	2	3	2						
23	Практична граматика англійської мови	2	1			6	180	60		60				120	2	2										
24	Кваліфікаційна робота		7,8			9	270							270												
	Всього по дисциплінам п.1.2.1:	**19**	**14**		**2**	**126**	**3780**	**1110**	**350**	**552**	**54**	**154**		**2670**	**18**	**14**	**12**	**12**	**9**	**9**	**3**	**3**				
	1.2.2. Практична підготовка																									
25	Навчальна (ознайомлювальна) практика		4			3	90							90												
26	Навчальна (педагогічна) практика		6			6	180							180												
27	Навчальна (обчислювальна) практика		5			6	180							180												
28	Виробнича (педагогічна) практика		7,8			15	450							450												
	Всього по дисциплінам п.1.2.2:		**5**			**30**	**900**							**900**												
	Всього по п. 1.2:	**19**	**19**		**2**	**156**	**4680**	**1110**	**350**	**552**	**54**	**154**		**3570**	**18**	**14**	**12**	**12**	**9**	**9**	**3**	**3**				
	Разом за розділом (п. 1):	**19**	**26**		**2**	**177**	**5310**	**1320**	**402**	**694**	**70**	**154**		**3990**	**20**	**16**	**14**	**12**	**15**	**9**	**6**	**6**				
	2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																									
29	Вибіркова дисципліна 1		2			3	90	30						60		2										
30	Вибіркова дисципліна 2		2			3	90	30						60		2										
31	Вибіркова дисципліна 3		3			3	90	30						60			2									
32	Вибіркова дисципліна 4		3			3	90	30						60			2									

А) Прикарпатський національний університет імені Василя Стефаника

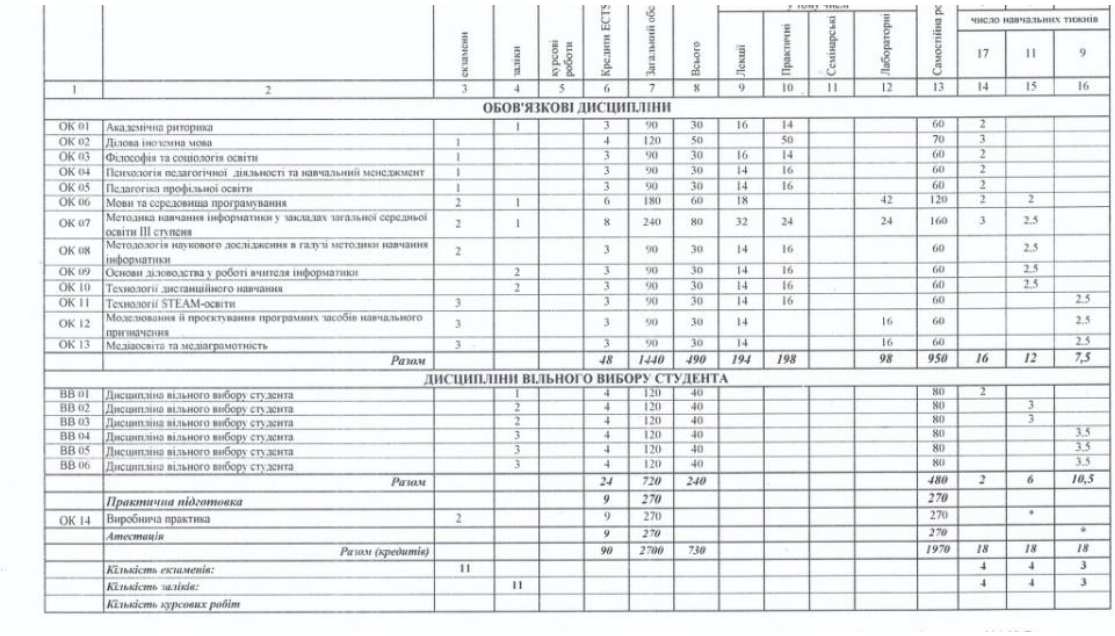
(https://nmv.pnu.edu.ua/wp-content/uploads/sites/118/2023/09/014.09-navchalnyi-plan-bak_2023.pdf)

VI. План навчального процесу

№ з/п	НАЗВА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	Розподіл за семестрами: Екзамени	Заліки	Курсові роботи	Кількість кредитів ECTS	Кількість годин: Загальний обсяг	Аудиторних годин: Всього	у тому числі: Лекції	Практич/Семін	Лабораторні	Підсумкові модульні контрольні роботи	Позааудиторних та Самостійна та індивідуальна	Розподіл аудиторних годин: I курс / II курс — Семестри 1	2	3	4 — Кількість тижнів в семестрі: 18	13	10	
	1. Цикл загальної підготовки																			
	1.1. Обов`язкові навчальні дисципліни																			
1	Методика наукових досліджень		1		4	120	40	12		28	1	80	2,2							
2	Основи професійної комунікації іноземною мовою	1			4	120	40		40		1	80	2,2							
3	Філософія науки		2		3	90	30	12	18		1	60		2,3						
	Всього по п. 1.1:	**1**	**2**		**11**	**330**	**110**	**24**	**58**	**28**	**3**	**220**	**4,4**	**2,3**						
	1.2. Дисципліни самостійного вибору університету																			
4	Психологія педагогічної діяльності		1		3	90	30	12	18		1	60	1,7							
5	Теорія та методика педагогічної діяльності	2			4	120	40	18	22		1	80		3,1						
	Всього по п. 1.2:	**1**	**1**		**7**	**210**	**70**	**30**	**40**		**2**	**140**	**1,7**	**3,1**						
	1.3. Дисципліни вільного вибору студента																			
6	ДВВС 1 з переліку запропонованого Університетом	3			4	120	44	10		34	1	76			4,4					
7	ДВВС 2 з переліку запропонованого Університетом		3		5	150	52	12		40	2	98			5,2					
	Всього по п. 1.3:	**1**	**1**		**9**	**270**	**96**	**22**		**74**	**3**	**174**			**9,6**					
	Разом за розділом (п. 1):	**3**	**4**		**27**	**810**	**276**	**76**	**98**	**102**	**8**	**534**	**6,1**	**5,4**	**9,6**					
	2. Цикл професійної підготовки																			
	2.1. Обов`язкові навчальні дисципліни																			
8	Case-технології проектування програмного забезпечення		1		4	120	42	16	6	20	1	78	2,3							
9	Курсова робота з методити навчання інформатики в профільних класах			2	1	30						30		*						
10	Методи математичної обробки даних у педагогіці та психології	1			4,5	135	48	12		36	2	87	2,7							
11	Методика навчання інформатики	2	1		5	150	64	16		48	2	86	1,9	2,3						
12	Спеціалізовані мови програмування	2			5	150	56	16		40	2	94		4,3						
13	Чисельні методи в інформатиці	2			4	120	40	14		26	1	80		3,1						
	Всього по п. 2.1:	**4**	**2**	**1**	**23,5**	**705**	**250**	**74**	**6**	**170**	**8**	**455**	**6,9**	**9,7**						
	2.2. Дисципліни самостійного вибору університету																			
14	Виконання кваліфікаційної роботи				3	90						90		*	*					
15	Комп`ютений синтез і обробка зображень	1			4,5	135	48	12		36	2	87	2,7							
16	Розробка освітніх мобільних додатків		1		4	120	40	10		30	1	80	2,2							
17	Технології розробки і супровід Інтернет сайтів		2		4	120	40	10		30	1	80		3,1						
	Всього по п. 2.2:	**1**	**2**		**15,5**	**465**	**128**	**32**		**96**	**4**	**337**	**4,9**	**3,1**						
	2.3. Дисципліни вільного вибору студента																			
18	ДВВС 3 з переліку запропонованого Університетом	3			4,5	135	48	14		34	2	87			4,8					
19	ДВВС 4 з переліку запропонованого Університетом	3			5	150	52	12		40	2	98			5,2					
20	ДВВС 5 з переліку запропонованого Університетом		3		4	120	44	14		30	1	76			4,4					
	Всього по п. 2.3:	**2**	**1**		**13,5**	**405**	**144**	**40**		**104**	**5**	**261**			**14**					
	Разом за розділом (п. 2):	**7**	**5**	**1**	**52,5**	**1575**	**522**	**146**	**6**	**370**	**17**	**1053**	**12**	**13**	**14**					
	3. Практика																			
1	Виробнича практика в закладах загальної середньої освіти		3		4,5	135						135			*					
2	Навчальна практика з розробки електронного освітнього ресурсу		2		4,5	135	54			54		81		*						
	Разом за розділом (п. 3):		**2**		**9**	**270**	**54**			**54**		**216**								
	4. Атестація																			
1	Захист кваліфікаційної роботи	3			1,5	45						45			*					
	Разом за розділом (п. 4):				**1,5**	**45**						**45**								
Загальна кількість					**90**	**2700**	**852**	**222**	**104**	**526**	**25**	**1848**	**18**	**18**	**24**					
Кількість годин на тиждень												**66**								
Кількість екзаменів												**10**	**3**	**4**	**3**					
Кількість заліків												**11**	**5**	**3**	**3**					
Кількість курсових робіт												**1**		**1**						

Б) Житомирський державний університет імені Івана Франка

(https://eportfolio.zu.edu.ua/media/Curriculum/495/juljaj.pdf)



		екзамени	заліки	курсові роботи	Кредити ЄСТС	Загальний обс	Всього	у тому числі: Лекції	Практичні	Семінарські	Лабораторні	Самостійна р	число навчальних тижнів 17	11	9
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ОБОВ'ЯЗКОВІ ДИСЦИПЛІНИ															
ОК 01	Академічна риторика		1		3	90	30	16	14			60	2		
ОК 02	Ділова іноземна мова	1			4	120	50		50			70	3		
ОК 03	Філософія та соціологія освіти	1			3	90	30	16	14			60	2		
ОК 04	Психологія педагогічної діяльності та навчальний менеджмент	1			3	90	30	14	16			60	2		
ОК 05	Педагогіка профільної освіти	1			3	90	30	14	16			60	2		
ОК 06	Мови та середовища програмування	2	1		6	180	60	18			42	120	2	2	
ОК 07	Методика навчання інформатики у закладах загальної середньої освіти III ступеня	2	1		8	240	80	32	24		24	160	3	2.5	
ОК 08	Методологія наукового дослідження в галузі методики навчання інформатики	2			3	90	30	14	16			60		2.5	
ОК 09	Основи діловодства у роботі вчителя інформатики		2		3	90	30	14	16			60		2.5	
ОК 10	Технології дистанційного навчання		2		3	90	30	14	16			60		2.5	
ОК 11	Технології STEAM-освіти	3			3	90	30	14	16			60			2.5
ОК 12	Моделювання й проєктування програмних засобів навчального призначення	3			3	90	30	14			16	60			2.5
ОК 13	Медіаосвіта та медіаграмотність	3			3	90	30	14			16	60			2.5
	Разом				*48*	*1440*	*490*	*194*	*198*		*98*	*950*	*16*	*12*	*7,5*
ДИСЦИПЛІНИ ВІЛЬНОГО ВИБОРУ СТУДЕНТА															
ВВ 01	Дисципліна вільного вибору студента		1		4	120	40					80	2		
ВВ 02	Дисципліна вільного вибору студента		2		4	120	40					80		3	
ВВ 03	Дисципліна вільного вибору студента		2		4	120	40					80		3	
ВВ 04	Дисципліна вільного вибору студента		3		4	120	40					80			3.5
ВВ 05	Дисципліна вільного вибору студента		3		4	120	40					80			3.5
ВВ 06	Дисципліна вільного вибору студента		3		4	120	40					80			3.5
	Разом				*24*	*720*	*240*					*480*	*2*	*6*	*10,5*
	Практична підготовка				*9*	*270*						*270*			
ОК 14	Виробнича практика	2			9	270						270		*	
	Атестація				*9*	*270*						*270*			*
	Разом (кредитів)				*90*	*2700*	*730*					*1970*	*18*	*18*	*18*
	Кількість екзаменів:	11											4	4	3
	Кількість заліків:		11										4	4	3
	Кількість курсових робіт														

В) Уманський державний педагогічний університет імені Павла Тичини

(https://surl.li/tuvrqp)

2 Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОПП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові освітні компоненти ОПП			
Цикл дисциплін загальної підготовки			
ООК-1	Українознавство	3	д. залік
ООК-2	Ділова українська мова та академічне письмо	3	д. залік
ООК-3	Правове регулювання суспільних відносин в Україні	3	д. залік
ООК-4	Англійська мова професійного спрямування	5	д. залік
ООК-5	Безпека життєдіяльності, охорона праці та екологічна безпека	3	д. залік
ООК-6	Загальна та вікова психологія	5	д. залік
ООК-7	Педагогіка	6	іспит
Цикл дисциплін професійної підготовки			
ООК-8	Вступ до спеціальності	6	д. залік
ООК-9	Інформаційно-комунікаційні технології в освітньому процесі	3	д. залік
ООК-10	Теорія та методика позакласної роботи	4,5	д. залік
ООК-11	Тайм менеджмент сучасного освітнього процесу	3	д. залік
ООК-12	Елементарна математика	6	іспит
ООК-13	Лінійна алгебра та аналітична геометрія	6	іспит
ООК-14	Математична логіка та дискретна математика	5,5	іспит
ООК-15	Математичний аналіз	13	іспит
ООК-16	Диференціальні рівняння	3	д. залік
ООК-17	Теорія ймовірностей, математична статистика	4,5	д. залік
ООК-18	Архітектура комп'ютерних систем та мереж	4,5	д. залік
ООК-19	Програмування	14	іспит
ООК-20	Шкільний курс інформатики	5	д. залік
ООК-21	Комп'ютерна математика	5	іспит
ООК-22	Методи обчислень та математичне моделювання	4	д. залік
ООК-23	Бази даних та інформаційні системи	5,5	іспит
ООК-24	Методика навчання інформатики	11	іспит, курсова
ООК-25	Методика навчання математики	6	іспит, курсова
ООК-26	Комп'ютерна графіка та доповнена реальність	4	іспит
ООК-27	Захист інформації в інформаційних системах	3	іспит
ООК-28	Практикум з розв'язування задач шкільного курсу математики	7	д. залік
ООК-29	Педагогічна практика (ознайомча)	3	д. залік
ООК-30	Навчальна практика з позакласної роботи з інформатики та математики	4,5	д. залік
ООК-31	Виробнича (педагогічна) практика «Інформатика»	9	д. залік
ООК-32	Виробнича (педагогічна) практика «Математика»	9	д. залік
ООК-33	Атестаційний іспит з інформатики	1,5	іспит
ООК-34	Атестаційний іспит з математики	1,5	іспит
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові освітні компоненти ОПП			
ВОК-1–ВОК-12	Дисципліни*	60	д. залік
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		**240**	

Г) Кременчуцький національний університет імені Михайла Остроградського (http://ivm.krnu.org/opp-24-014-bakalavr)

Обов'язкові компоненти освітньо-професійної програми			
1. Цикл загальної підготовки			
ОК 1	Україна в європейському історичному та культурному контекстах	3	залік
ОК 2	Українська мова (за професійним спрямуванням)	3	екзамен
ОК 3	Іноземна мова (за професійним спрямуванням)	12	залік, екзамен, залік, екзамен
ОК 4	Правові основи громадянського суспільства	3	залік
ОК 5	Фізичне виховання	2	залік
Разом		**23**	
2. Цикл професійної підготовки			
ОК 6	Вступ до фаху	5	екзамен
ОК 7	Алгоритми та структури даних	5	екзамен
ОК 8	Дискретна математика	8	залік, екзамен
ОК 9	Вища математика	13	залік, екзамен, екзамен
ОК 10	Системне, прикладне програмне забезпечення та хмарні технології в освіті	5	залік
ОК 11	Охорона життя і здоров'я учасників освітнього процесу	3	залік
ОК 12	Теорія ймовірностей та математична статистика	5	екзамен
ОК 13	Педагогіка	6	екзамен
ОК 14	Психологія	6	залік, екзамен
ОК 15	Програмування	16	залік, екзамен, залік, екзамен
ОК 16	Архітектура обчислювальних систем	5	екзамен
ОК 17	Комп'ютерна графіка та мультимедійна продукція	4	залік
ОК 18	Бази даних	4	екзамен
ОК 19	Інклюзивна освіта	3	залік
ОК 20	Вебтехнології та дизайн	5	екзамен
ОК 21	Методика навчання інформатики	10	екзамен, екзамен
ОК 22	Комп'ютерні мережі та інтернет-технології	5	екзамен
ОК 23	STEM-технології в інформатичній освітній галузі	5	екзамен
ОК 24	Практикум зі шкільного курсу інформатики	5	екзамен
ОК 25	Чисельні методи та комп'ютерне моделювання	4	екзамен
ОК 26	Технології захисту інформації	4	залік
ОК 27	Курсова робота з програмування	3	залік
ОК 28	Курсова робота з методики навчання інформатики	3	залік
ОК 29	Навчальна практика з інформаційних технологій	3	залік
ОК 30	Психолого-педагогічна практика	3	залік
ОК 31	Практика з розробки електронних дидактичних ресурсів з інформатики	3	залік
ОК 32	Педагогічна практика 1	6	залік

Д) Волинський національний університет імені Лесі Українки

(https://surl.li/tsuzlg)

2.1. Перелік компонент освітньо-професійної програми

Код навчальної дисципліни	Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	Кредитів ECTS	Форма підсумкового контролю
2.1. Обов'язкові компоненти ОП			
2.1.1. Обов'язкові навчальні дисципліни загальної підготовки			
ЗО.01	Філософія науки	3	Екзамен
ЗО.02	Методика наукових досліджень	3	Залік
ЗО.03	Іноземна мова для академічних цілей	4	Екзамен
	Всього	**10**	
2.1.2. Обов'язкові навчальні дисципліни професійної підготовки			
ЗО.04	Психологія та педагогіка освітньої діяльності	3	Екзамен
ЗО.05	Менеджмент у освіті	3	Екзамен
ЗО.06	Проєктування та керування інформаційними системами	3	Залік
ЗО.07	Методика навчання математики	3	Екзамен
ЗО.08	Методика навчання інформатики та технології STEM-освіти	6	Залік
ЗО.09	Вибрані питання вищої математики та математичної статистики	4	Екзамен
ЗО.10	Курсова робота	3	Диф.залік
	Всього	**25**	
2.1.3. Практична підготовка			
ЗО.11	Педагогічна практика	15	Диф. залік, диф. залік
ЗО.12	Практикум із цифрових технологій в освіті та науці	3	залік
ЗО.13	Проектно-технологічна практика зі STEM-освіти	3	Залік
ЗО.14	Підготовка кваліфікаційної роботи	9	
	Всього	**30**	
2.1.4. Атестація			
А.01	Атестаційний екзамен	1	Екзамен
А.02	Кваліфікаційна робота		Публічний захист

Е) Тернопільський національний педагогічний університет імені Володимира Гнатюка (https://surl.li/tuvrqp)

Код навчальної дисципліни	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ECTS	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
1. Обов'язкові навчальні дисципліни загальної підготовки			
ЗП 1.01	Українська мова та культура мовлення	3	екзамен
ЗП 1.02	Історія та культура України	3	екзамен
ЗП 1.03	Філософія	3	екзамен
ЗП 1.04	Іноземна мова	5	залік, залік
ЗП 1.05	Іноземна мова за професійним спрямуванням	10	залік, екзамен
ЗП 1.06	Фізичне виховання	4	залік
ЗП 1.07	Правове регулювання професійної діяльності	3	залік
ЗП 1.08	Безпека життєдіяльності та охорона праці в галузі	3	залік
	Всього	**34**	
2. Обов'язкові навчальні дисципліни професійної підготовки			
ПП 2.01	Психологія	4,5	залік, екзамен
ПП 2.02	Педагогіка	9	екзамен, екзамен
ПП 2.03	Вікова фізіологія та валеологія	3	залік
	Оглядові лекції до атестації (психологія – 4 год., педагогіка – 4 год., фах – 16 год.)	1,5	
ПП 2.04	Інформатика	6	екзамен
ПП 2.05	Архітектура обчислювальних систем	3	екзамен
ПП 2.06	Сучасні операційні системи	4	екзамен
ПП 2.07	Програмування	11,5	екзамен, екзамен, екзамен
ПП 2.08	Інформаційні мережі	3,5	екзамен
ПП 2.09	Комп'ютерна графіка	3,5	залік
ПП 2.10	Захист інформації	2,5	екзамен
ПП 2.11	Бази даних та інформаційні системи	6	залік, екзамен
ПП 2.12	Віртуальні навчальні середовища	3,5	екзамен
ПП 2.13	Програмування веб-застосувань	4,5	екзамен, екзамен
ПП 2.14	Методика навчання інформатики	8	екзамен, екзамен
ПП 2.15	Практикум з розв'язування задач з інформатики	5	залік, залік
ПП 2.16	Математичний аналіз	11,5	екзамен, екзамен, екзамен
ПП 2.17	Алгебра	9	залік, екзамен, екзамен
ПП 2.18	Геометрія	6,5	екзамен, екзамен
ПП 2.19	Методика навчання математики	9,5	екзамен, екзамен, екзамен
ПП 2.20	Елементарна математика	9,5	залік, залік, залік
	Всього	**125**	
3. Практична підготовка			
ПП 2.21	Виробнича практика у школі	9	диференц. залік
ПП 2.22	Навчальна пропедевтична практика з психології	1,5	залік
ПП 2.23	Навчальна пропедевтична практика з педагогіки	1,5	залік
ПП 2.24	Навчальна комп'ютерна практика	1,5	диференц. залік
ПП 2.25	Навчальна пропедевтична практика з фаху	1,5	залік
	Всього	**15**	
4. Курсові роботи			
ПП 2.26	Курсова робота з предметної спеціальності Інформатика	1,5	диференц. залік
ПП 2.27	Курсова робота з методики навчання інформатики	1,5	диференц. залік
	Всього	**3**	
Атестація			

Є) Центральноукраїнський державний педагогічний університет імені Володимира Винниченка

(https://cusu.edu.ua/images/download-files/OP_quality-education/bakalavr/014-09_MI_B.pdf)

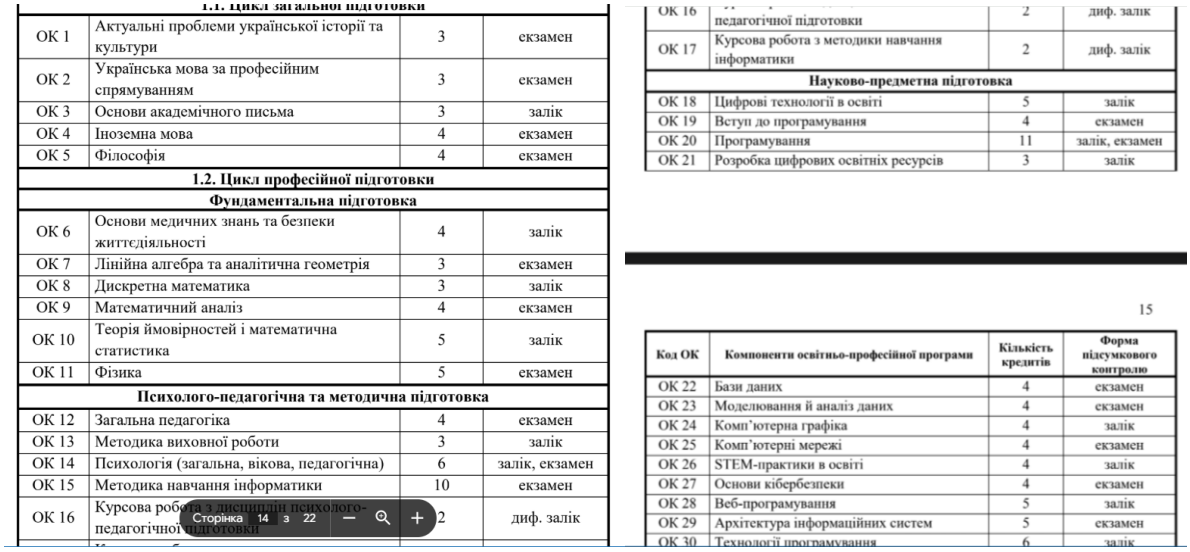
				Ку	Кіль	За	Всього ау	Л	Лабо	Пра	Сам	Кількість тижнів у семестрі							
												16	16	16	14	14	14	10	10
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1. ОБОВ'ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																			
1.1. Цикл загальної підготовки (ЗП)																			
ЗП 1	Історія та культура України		1		3	90	36	26		10	54	2							
ЗП 2	Історія та культура угорського народу		2		3	90	36	26		10	54		2						
ЗП 3	Філософія		3		3	90	36	26		10	54			2					
ЗП 4	Іноземна мова за професійним спрямуванням	8			3	90	36			36	54								4
Всього за циклом		**1**	**3**		**12**	**360**	**144**	**78**		**66**	**216**	**2**	**2**	**2**					**4**
1.2. Цикл професійної підготовки (ППП)																			
ППП 1	Сучасні інформаційні технології		1		5	150	60			60	90	4							
ППП 2	Алгебра та геометрія	1,2			8	240	96	48		48	144	3	3						
ППП 3	Інформатика та основи алгоритмізації	1,2			9	270	108	54		54	162	4	3						
ППП 4	Математичний аналіз	1,2			10	300	120	60		60	180	4	4						
ППП 5	Психологія	1			4	120	48	40		8	72	3							
ППП 6	Педагогіка	3	2		6	180	72	48		24	108		2	2					
ППП 7	Дискретна математика	2			4	120	48	24		24	72		3						
ППП 8	Методика навчання інформатики	4,5,6	3	1	18	540	216	64		152	324			4	5	4	4		
ППП 9	Системи керування базами даних		3		5	150	60	30		30	90			4					
ППП 10	Алгоритми і структури даних	3			4	120	48	24		24	72			3					
ППП 11	Математична логіка і теорія алгоритмів	3			3	90	36	18		18	54			2					
ППП 12	Програмування (Сучасні мови програмування, Веб-програмування, Технологія об'єктно-орієнтованого програмування, Логічне та функціональне програмування)	3,4,5, 6		1	16	480	192	94		98	288			2	4	5	4		
ППП 13	Теорія ймовірності та математична статистика	4			7	210	84	42		42	126				6				
ППП 14	Основи комп'ютерної графіки	5			3	90	36	18		18	54					3			
ППП 15	Сучасні технології розробки освітніх інформаційних ресурсів та систем	5			3	90	36	16		20	54					3			
ППП 16	Українська мова за професійним спрямуванням		6		3	90	36	10		26	54						3		
ППП 17	Диференціальні рівняння	6			5	150	60	30		30	90						5		
ППП 18	Комп'ютерні мережі		7		3	90	36	18		18	54							4	
ППП 19	Пакети математичних програм		7		3	90	36	18		18	54							4	
ППП 20	Методи обчислень та методи оптимізації	7,8			9	270	108	54		54	162							5	6
ППП 21	Операційні системи	7			3	90	36	18		18	54							4	
ППП 22	Загальна фізика	8			4	120	48	24		24	72								5
Всього за циклом		**26**	**7**	**2**	**135**	**4050**	**1620**	**768**		**852**	**2430**	**18**	**15**	**17**	**15**	**15**	**16**	**17**	**11**
1.3. Практична підготовка та атестація (ППА)																			
ППА 1	Педагогічна практика (Практика з виготовлення наукових текстів та засобів наочності з інформатики)		2		3	90					90		2т.						
ППА 1	Літня педагогічна практика (Практика підготовки науково-методичних текстів, Навчальна обчислювальна практика)		4		3	90					90				2т.				
ППА 2	Педагогічна практика (Виробнича)		4,5,6, 7		18	540					540				2т.	2т.	2т.	2т.	
ППА 3	Педагогічна практика (Табірна практика)		6		3	90					90						2т.		
ППА 4	Підготовка бакалаврської роботи		8		3	90					90								2т.
А	Атестація	8			3	90					90								*
Всього за циклом		**1**	**8**		**33**	**990**					**990**		**2т.**		**4т.**	**2т.**	**4т.**	**2т.**	**2т.**
Всього за обов'язковими дисциплінами		**28**	**18**	**2**	**180**	**5400**	**1764**	**846**		**918**	**3636**	**20**	**17**	**19**	**15**	**15**	**16**	**17**	**15**

Ж) Закарпатський угорський інститут імені Ференца Ракоці ІІ

(https://kmf.uz.ua/uk/strukturni-pidrozdily/kafedri/kafedra-matematiki-ta-informatiki/dokumenti-ta-materiali/)

Код н/д	*Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)*	*Кількість кредитів*	*Форма підсумкового контролю*
Обов'язкові навчальні дисципліни			
1.1 Цикл загальної підготовки			
ОК 1	Історія та культура України	4	Іспит
ОК 2	Філософія	3	Залік
ОК 3	Українська мова за професійним спрямуванням	4	Іспит
ОК 4	Англійська мова	12	Залік/Іспит/ Залік/ Іспит
ОК 5	Фізичне виховання	4	Залік
Всього за цикл:		**27**	
1.2 Дисципліни професійної підготовки			
ОК 6	Педагогіка	8	Іспит
ОК 7	Основи інклюзивного навчання	3	Залік
ОК 8	Психологія	6	Іспит
ОК 9	Вікова фізіологія та здоров'я дитини	3	Залік
ОК 10	Основи інформатики	3	Залік
ОК 11	Фізичні основи інформаційних систем	4	Іспит
ОК 12	Вища математика з комп'ютерною підтримкою	11	Залік\ Іспит
ОК 13	Веб-технології та хмарні сервіси	4	Залік
ОК 14	Комп'ютерна графіка	4	Залік
ОК 15	Інформатика в початковій школі	4	Залік
ОК 16	Цифрові технології	6	Іспит \Залік
ОК 17	Інформатика в базовій школі	3	Залік,
ОК 18	Програмування	12	Іспит/Залік/Іспит
ОК 19	Основи мікроелектроніки	5	Іспит
ОК 20	Дискретна математика	4	Іспит
ОК 21	Архітектура комп'ютера	4	Іспит
ОК 22	Цифрове середовище ЗЗСО	3	Залік
ОК 23	Основи СУБД	4	Залік
ОК 24	Інформаційний супровід діяльності вчителя	3	Залік
ОК 25	Методика навчання інформатики	8	Іспит/Іспит
ОК 26	Методи обчислень	5	Залік\ Іспит
ОК 27	Олімпіадні задачі з інформатики та інформаційних технологій	5,5	Іспит
ОК 28	Курсова робота з психолого-педагогічних дисциплін	3	Залік
ОК 29	Курсова робота з інформатики	3	Залік
ОК 30	Курсова робота з методики навчання інформатики	3	Залік
Всього за цикл:		**121,5**	

3) Сумський державний педагогічний університет імені А.С. Макаренка

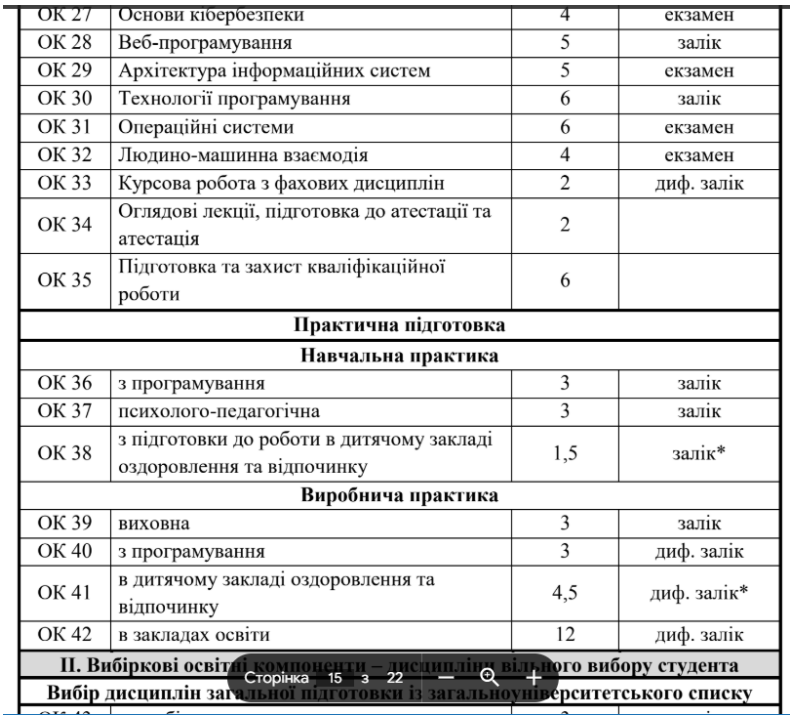


	1.1. Цикл загальної підготовки		
ОК 1	Актуальні проблеми української історії та культури	3	екзамен
ОК 2	Українська мова за професійним спрямуванням	3	екзамен
ОК 3	Основи академічного письма	3	залік
ОК 4	Іноземна мова	4	екзамен
ОК 5	Філософія	4	екзамен
	1.2. Цикл професійної підготовки		
	Фундаментальна підготовка		
ОК 6	Основи медичних знань та безпеки життєдіяльності	4	залік
ОК 7	Лінійна алгебра та аналітична геометрія	3	екзамен
ОК 8	Дискретна математика	3	залік
ОК 9	Математичний аналіз	4	екзамен
ОК 10	Теорія ймовірностей і математична статистика	5	залік
ОК 11	Фізика	5	екзамен
	Психолого-педагогічна та методична підготовка		
ОК 12	Загальна педагогіка	4	екзамен
ОК 13	Методика виховної роботи	3	залік
ОК 14	Психологія (загальна, вікова, педагогічна)	6	залік, екзамен
ОК 15	Методика навчання інформатики	10	екзамен
ОК 16	Курсова робота з дисциплін психолого-педагогічної підготовки	2	диф. залік
ОК 17	Курсова робота з методики навчання інформатики	2	диф. залік
	Науково-предметна підготовка		
ОК 18	Цифрові технології в освіті	5	залік
ОК 19	Вступ до програмування	4	екзамен
ОК 20	Програмування	11	залік, екзамен
ОК 21	Розробка цифрових освітніх ресурсів	3	залік

Сторінка 14 з 22

15

Код ОК	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
ОК 22	Бази даних	4	екзамен
ОК 23	Моделювання й аналіз даних	4	екзамен
ОК 24	Комп'ютерна графіка	4	залік
ОК 25	Комп'ютерні мережі	4	екзамен
ОК 26	STEM-практики в освіті	4	залік
ОК 27	Основи кібербезпеки	4	екзамен
ОК 28	Веб-програмування	5	залік
ОК 29	Архітектура інформаційних систем	5	екзамен
ОК 30	Технології програмування	6	залік



ОК 27	Основи кібербезпеки	4	екзамен
ОК 28	Веб-програмування	5	залік
ОК 29	Архітектура інформаційних систем	5	екзамен
ОК 30	Технології програмування	6	залік
ОК 31	Операційні системи	6	екзамен
ОК 32	Людино-машинна взаємодія	4	екзамен
ОК 33	Курсова робота з фахових дисциплін	2	диф. залік
ОК 34	Оглядові лекції, підготовка до атестації та атестація	2	
ОК 35	Підготовка та захист кваліфікаційної роботи	6	
	Практична підготовка		
	Навчальна практика		
ОК 36	з програмування	3	залік
ОК 37	психолого-педагогічна	3	залік
ОК 38	з підготовки до роботи в дитячому закладі оздоровлення та відпочинку	1,5	залік*
	Виробнича практика		
ОК 39	виховна	3	залік
ОК 40	з програмування	3	диф. залік
ОК 41	в дитячому закладі оздоровлення та відпочинку	4,5	диф. залік*
ОК 42	в закладах освіти	12	диф. залік
	II. Вибіркові освітні компоненти – дисципліни вільного вибору студента		
	Вибір дисциплін загальної підготовки із загальноуніверситетського списку		

Сторінка 15 з 22

I) Криворізький державний педагогічний університет

(https://kmf.uz.ua/uk/strukturni-pidrozdily/kafedri/kafedra-matematiki-ta-informatiki/dokumenti-ta-materiali/)

Рис. 4. Витяги з навчальних планів або освітніх програм професійної підготовки вчителів інформатики (спеціальність 014 СО (інформатика))

Деякі програми акцентують більшою мірою увагу на програмуванні, тоді як інші більшою мірою включають педагогічні підходи навчання

інформатики [197]. При цьому всі освітні програми передбачають інтеграцію ІТ у підготовку вчителів інформатики. Це є поширеним явищем, багато програм використовують онлайн-платформи та інтерактивні інструменти.

Ступінь, до якого ці програми стосуються навичок цифрової безпеки, значно варіюється [1]. Одні наголошують на цілеспрямованому навчанні з кібербезпеки, тоді як інші зосереджуються на важливості формування більш широких навичок цифрової грамотності, [102]. При цьому науковці наголошують, що проектні та активні методи навчання набувають популярності в цифровому освітньому середовищі. Вони сприяють глибшому залученню та запам’ятовуванню знань.

У науково-педагогічній літературі бракує конкретних деталей щодо назв та обсягу курсів, безпосередньо спрямованих на розвиток навичок кібербезпеки в рамках програм підготовки вчителів. Ця прогалина в літературі підкреслює необхідність додаткових досліджень та аналізу існуючих програм для виявлення того, як кібербезпека інтегрована в підготовку вчителів.

Однак кілька документів пропонують уявлення про суміжні сфери, які опосередковано сприяють розвитку навичок кібербезпеки. Наприклад, в обговоренні освіти з мережевої безпеки [4] наголошується на важливості «захисту апаратного забезпечення, інформаційних систем та електронних даних», які є важливими об’єктами кібербезпеки. Це свідчить про те, що курси з мережевої безпеки можуть бути важливими компонентами підготовки вчителів інформатики з кібербезпеки. У статті також згадується використання «існуючих рамок знань вчителів» для аналізу та вдосконалення «конструктів знань освітян» в освіті з мережевої безпеки [4], що вказує на те, що системний підхід до включення концепцій кібербезпеки в підготовку вчителів має важливе значення.

Аналіз цифрових компетентностей освітян [153] торкається важливості «цифрової безпеки та відповідального використання онлайн-середовища в освітній діяльності». Це свідчить про те, що курси, зосереджені на цифровій грамотності та безпеці в Інтернеті, можуть сприяти розвитку обізнаності та

навичок вчителів щодо кібербезпеки. Водночас, незважаючи на очевидну потребу, аналіз сучасних програм професійної підготовки вчителів інформатики вказує на значні прогалини – програми часто не містять спеціальних компонентів, спрямованих на розвиток навичок цифрової безпеки. Як наслідок, майбутні вчителі інформатики недостатньо підготовлені до розвитку подібних навичок у своїх учнів [200].

Наявна наукова література наголошує на важливості опанування методики навчання інформатики, але прямо не розглядає формування навичок цифрової безпеки в курсах з методики навчання інформатики [164]. У статті [35] обговорюється роль «методичних курсів» у формуванні педагогічних та методичних знань для майбутніх учителів інформатики, але не уточнюється, чи включають ці курси підготовку майбутніх учителів до опанування концепцій цифрової безпеки та формування відповідних методичних умінь учителів. Аналогічно, стаття [16] аналізує методи викладання інформатики, але зосереджується на загальних педагогічних підходах, а не на конкретних стратегіях навчання і викладання цифрової безпеки.

Відсутність чіткої уваги до цифрової безпеки в курсах методики навчання інформатики, які є в кожній з освітньо-професійних програм, підтверджує висновок про недостатню увагу до підготовки вчителів інформатики для розвитку навичок цифрової безпеки учнів. Наявна наукова література в першу чергу зосереджена на загально-педагогічних підходах та змісті знань з інформатики, та ігнорує конкретні педагогічні стратегії, пов’язані з формуванням навичок цифрової безпеки [147; 139; 141 та інші].

Однак у деяких роботах опосередковано зачіпаються суміжні теми. Хоча спеціальні курси з кібербезпеки є корисними, наприклад [138], ефективним підходом може бути також інтеграція концепцій кібербезпеки в існуючі ІТ-курси. Дослідники [27] стверджують, що це може передбачати включення модулів безпеки в курси з програмування, з баз даних і з комп’ютерних мереж. Це забезпечить більш цілісне розуміння принципів безпеки. Їхнє твердження

базується на реалізації модулів безпеки в курсі CS2, яка продемонструвала доцільність і ефективність такого підходу.

У науковій літературі бракує конкретних подробиць щодо назв та обсягу курсів, присвячених розвитку навичок цифрової безпеки в рамках програм підготовки вчителів. Однак ми можемо зупинитися на потенційному змісті та структурі таких курсів. Комплексний курс з кібербезпеки для вчителів інформатики може охоплювати широке коло тем (рис.1.5).

Ефективна освіта з кібербезпеки потребує збалансованого підходу, який поєднує фундаментальні знання з практичними навичками [187]. Тому зазначається, що програми підготовки вчителів повинні надавати освітянам можливість не лише вивчити теоретичні основи кібербезпеки, але й застосувати ці концепції в практичних умовах [96]. Це може включати практичні дії, такі як налаштування параметрів безпеки, аналіз вразливостей безпеки та реагування на змодельовані кібератаки. Дослідження [187] підкреслює на важливості доступу до «експериментальних баз, практичних навчальних лабораторій та штату викладачів та дослідників», щоб полегшити цей баланс між теорією та практикою.

Поряд із предметними знаннями важливу роль у підготовці вчителів інформатики відіграє психолого-педагогічна підготовка [35]. Відповідні курси (навчальні дисципліни) повинні забезпечувати освітян необхідними педагогічними знаннями та навичками для ефективного викладання понять цифрової безпеки. Це може включати опанування різних стратегій навчання, таких як проектне навчання, навчання на основі запитів і групове навчання, а також їх адаптацію до конкретного змісту – цифрової безпеки.

Friend et al. [35] наголошують на важливості «методичних курсів» як джерела знань «педагогічного та методичного змісту» для майбутніх вчителів інформатики, акцентують увагу на необхідності спеціальної педагогічної підготовки в рамках програм підготовки вчителів.

Мережева безпека

- Цей модуль може досліджувати топології мережі, мережеві протоколи, загрози та вразливості мережевої безпеки, а також методи захисту мереж, такі як брандмауери, системи виявлення вторгнень та віртуальні приватні мережі.

Захист даних

- Цей модуль може розглядати принципи безпеки даних, методи шифрування даних, стратегії резервного копіювання та відновлення даних, а також правила конфіденційності даних, такі як GDPR та CCPA.

Криптографія

- Цей модуль може впроваджувати криптографічні алгоритми, методи шифрування та дешифрування, цифрові підписи та системи керування ключами.

Етичний хакінг

- Цей модуль може досліджувати принципи етичного хакерства, методи тестування на проникнення, інструменти оцінки вразливостей та процедури реагування на інциденти.

Навчання учнів кібербезпеки

- Цей модуль може бути зосереджений на педагогічних аспектах навчання кібербезпеки, охоплюючи такі теми, як розробка змісту уроків, методи і засоби навчання та методики оцінювання знань та вмінь учнів з кібербезпеки.

Рис.1.5. Можливий зміст курсу з цифрової безпеки для вчителів інформатики

Поняття інформаційно-цифрової культури [198] та методичної компетентності, яка охоплює знання, вміння та навички, необхідні для ефективного навчання як провідної професійної діяльності вчителя, є особливо актуальним в навчанні учнів кібербезпеки з сучасній школі. Вчителі інформатики повинні не лише розуміти поняття кібербезпеки, а й володіти педагогічними знаннями, щоб ефективно доносити ці поняття до учнів. Це включає здатність розробляти цікаві освітні заходи, коректно оцінювати розуміння учнів [92], уміння адаптувати стратегії викладання для задоволення різноманітних потреб учнів. Дослідники [127] наголошують на важливості різних аспектів методичної компетентності, таких як «постановка цілей, вибір контенту, навчальні стратегії, методи оцінювання та адаптивність», які мають важливе значення для ефективної освіти в галузі цифрової безпеки.

У статті [4] згадується використання «існуючих рамок знань вчителів» для аналізу та вдосконалення «конструктів знань викладачів» в галузі мережевої безпеки. Це підкреслює важливість використання усталених рамок підготовки вчителя та їх адаптації до конкретного контексту цифрової безпеки. Обговорення в документі «знань про навчальні програми та педагогічний зміст знань, специфічних для викладання мережевої безпеки» [4] є відправною точкою для розробки більш комплексних рамок для підготовки вчителів до розвитку навичок цифрової безпеки учнів. Акцент на цифрових компетентностях для освітян свідчить про те, що може бути корисною інтеграція цифрових інструментів і технологій у розвиток навичок цифрової безпеки. Запропонована модель цифрових компетентностей [153] може бути розширена за рахунок включення конкретних знань та вмінь у сфері цифрової безпеки та використання відповідних цифрових інструментів. Наприклад, віртуальні лабораторії та симуляції можуть бути використані для надання вчителям практичного досвіду роботи зі сценаріями цифрової безпеки.

Національна освітня політика та наявні освітні ресурси також впливають на зміст та методи навчання інформатики [28], а ефективне формування навичок цифрової безпеки окрім технологічних знань вимагає знань про

можливі педагогічні стратегії та методики навчання дисциплін в галузі ІТ. Вчителі, на думку науковців [61], повинні вміти представляти складні поняття в доступній формі, зокрема, ефективними є візуальні форми. Вміння спрощувати складні поняття і процеси передбачає розуміння того, як учні вчаться, а тому важливою є здатність адаптувати методи навчання до цифрового освітнього середовища [171]. Ефективні педагогічні методики включають інтерактивне моделювання, рольові ігри, тематичні дослідження, у т.ч. реальних кібератак, та спільні проекти [1].

Ефективними є методи активного навчання, такі як вирішення проблем на основі конкретних випадків, симуляції та практичні вправи. Такі методи орієнтують на роботу з інформацією та мають важливе значення для розвитку критичного мислення. З іншого боку, наукові розвідки свідчать про потребу професійного розвитку вчителів у галузі цифрової безпеки.

У багатьох освітніх програмах підготовки вчителів інформатики відсутній акцент на практичному навчанні. Переважно теоретичний підхід обмежує здатність студентів розвивати практичні навички, і особливо, критичне мислення, необхідні для вирішення проблем цифрової безпеки. Однак у кількох роботах обговорюються суміжні педагогічні підходи та технологічні інструменти, які можуть бути адаптовані для практичної підготовки в галузі цифрової безпеки. Так, у [27], автори описують використання Model-Eliciting Activities (MEAs) як «проект з вирішення проблем» або кейс-метод, щоб допомогти студентам продемонструвати своє розуміння концепцій цифрової безпеки. Цей підхід, який переводить викладання з підходу, орієнтованого на вчителя, до підходу, орієнтованого на учня, може бути ефективно використаний у програмах підготовки вчителів, для їх залучення до активного вивчення та застосування принципів цифрової безпеки. Висновок дослідження про те, що значний відсоток рішень, прийнятих студентами, продемонстрував «креативність і придатність для реальних застосувань» [27], також свідчить про потенціал кейс-методу у сприянні розвитку практичних навичок цифрової безпеки.

Обмежена інтеграція практичних занять (реальних кейсів, симуляцій тощо) ускладнює перехід теоретичних знань майбутніх учителів у практичну площину на заняттях з інформатики або ІТ [90]. Використання віртуальних та/або хмарних середовищ у закладах освіти вимагає як оновлення цифрової інфраструктури, так і постійного розвитку навичок кібербезпеки вчителів та викладацького складу університетів.

Сьогодні, незважаючи на прогалини, з'являються позитивні тенденції для посилення освіти з цифрової безпеки. Розробляються спеціалізовані курси та модулі, орієнтовані на кібербезпеку, в рамках програм підготовки вчителів інформатики [154]. Доступність онлайн-ресурсів, (наприклад, відкриті освітні ресурси на різних цифрових платформах провідних університетів світу) надає освітянам можливості доповнювати/ поглиблювати навчальні програми.

Водночас, як відзначають науковці [там само], використання інтерактивних навчальних середовищ та гейміфікованих навчальних активностей може підвищити залученість та мотивацію студентів. Широкий спектр цифрових інструментів і технологій може бути використаний для підвищення кваліфікації вчителів інформатики у галузі цифрової безпеки. Віртуальні лабораторії, такі як ті, що пропонуються Cisco та іншими постачальниками, можуть забезпечити реалістичне моделювання мережевих середовищ і сценаріїв кібербезпеки. Інструменти тестування на проникнення, такі як Metasploit і Nmap, можуть дозволити вчителям практикувати етичні методи хакерства та виявляти вразливості безпеки. Інструменти аналізу даних, такі як Splunk і Wireshark, можуть допомогти вчителям аналізувати мережевий трафік і виявляти загрози безпеці, а онлайн-платформи, такі як Cybrary і Coursera, пропонують багато курсів і ресурсів з цифрової безпеки, для професійного розвитку.

Інтеграція рамок цифрової грамотності (фреймворк DigCompEdu [71]) у програми підготовки вчителів допомагають стандартизувати навчальні програми. Проте швидка еволюція кіберзагроз вимагає постійного оновлення навчальних програм, що вимагає значних ресурсів і досвіду [105]. Відсутність

кваліфікованих викладачів (інструкторів, практиків тощо), які мають досвід як у галузі інформатики, так і з цифрової безпеки, створює проблему наявності кадрів.

Ефективність реалізації освітніх програм підготовки вчителів інформатики залежить від рівня підготовленості викладачів відповідних освітніх компонентів. Значна їх кількість може не мати достатніх знань з питань цифрової безпеки [84], що впливає на їхню здатність ефективно навчати майбутніх учителів. Цей брак впевненості та досвіду може бути пов’язаний з обмеженим попереднім ознайомленням з концепціями кібербезпеки, недостатніми можливостями професійного розвитку та характером цифрової безпеки, яка швидко розвивається під впливом різних загроз.

Дослідники фіксують певний опір викладачів щодо впровадження нових технологій [84]. Тому освітні програми підготовки вчителів можуть надавати можливості для розвитку знань та умінь в галузі цифрової безпеки, що може бути досягнуто через упровадження більшої кількості практичних занять, фасилітації та створення сприятливого навчального середовища.

Цифровий розрив вступників на освітні програми підготовки вчителів інформатики суттєво впливає на ефективність їх навчання в галузі цифрової безпеки. Цифровий розрив (у доступі до технологій, до мережі Інтернет, у наявних ІТ-навичках) обмежує можливість якісного навчання в галузі кібербезпеки для багатьох студентів [105]. Нерівний доступ до технологій та підключення до Інтернету між студентами та викладачами створює диспропорцію у можливостях навчання. студентам може не вистачати необхідних інструментів і ресурсів для повноцінної участі в навчанні у галузі цифрової безпеки, що перешкоджає їхній здатності розвивати необхідні навички. Усунення цього бар’єру вимагає впровадження стратегій подолання цифрового розриву і забезпечення рівного доступу до технологій для всіх учасників освітнього процесу [105].

Ефективна освіта в галузі цифрової безпеки вимагає формування і розвитку міжпредметних зв’язків між різними дисциплінами професійної підготовки вчителів, включаючи інформатику, математику, освіту та інформаційну безпеку [121]. Недостатній їх розвиток може створити перешкоди для ефективного навчання. Викладачам ІТ-дисциплін може не вистачати педагогічних знань про методи навчання цифрових загроз, тоді як освітяни можуть не мати достатнього розуміння концепцій цифрової безпеки. Відсутність міжпредметних зв’язків може призвести до того, що навчальні програми будуть або занадто технічними, або занадто теоретичними, а тому не в змозі ефективно озброїти майбутніх вчителів інформатики необхідним поєднанням технічних і педагогічних навичок.

Традиційні методи оцінювання навичок цифрової безпеки можуть виявитися недостатніми для охоплення широти і глибини розуміння основних понять, концепцій, підходів, необхідних для галузі кібербезпеки [31]. Оцінювання практичних навичок, таких як виявлення загроз і реагування на них, вимагає особливого підходу, який виходить за рамки традиційних письмових іспитів [92].

Науковці відзначають, що на сьогодні залишається актуальною оцінка навичок цифрової безпеки. Існують різні методи оцінки, кожен з яких має свої сильні сторони та обмеження. Так, використовуються анкети для самооцінки [129; 38], які дозволяють людям оцінити власні знання та вміння. Однак самооцінка може бути упередженою і може неточно відображати фактичний рівень розвитку таких навичок [129].

Практичні тести та симуляції забезпечують більш об’єктивну оцінку навичок, але вони часто є більш ресурсо-місткими для опрацювання [1], хоча й включають реалістичні сценарії, що дозволяють оцінити навички в практичних умовах. Спостережні оцінки можуть бути використані для оцінки застосування навичок цифрової безпеки в реальних умовах, але вони забирають багато часу і вимагають навчених спостерігачів.

Динамічний характер проявів цифрової безпеки зумовлює потребу постійної адаптації методів оцінювання, щоб гарантувати, що вони залишаються актуальними та ефективними. Розробка надійних та валідних інструментів оцінювання, які коректно вимірюватимуть знання й уміння в галузі цифрової безпеки стає ще однією проблемою для забезпечення ефективності освітніх програм.

Ефективне викладання курсів з цифрової безпеки вимагає комплексного підходу, який виходить за рамки простих лекцій і включає активні стратегії навчання. Важливим аспектом є розуміння конкретних потреб і попередніх знань студентів [154]. І хоч сучасні студенти мають часто високий рівень цифрової грамотності [63], їхні знання принципів безпеки можуть бути обмеженими. Викладачі повинні оцінити рівень наявних знань студентів і на основі цього викладати новий матеріал [71], а тому наявною є потребу пошуку/ вибору відповідних методик навчання.

Проведений аналіз виявляє негаразди у підготовці майбутніх учителів інформатики щодо освіти в галузі цифрової безпеки. Узагальнення і систематизація проведеного аналізу дозволяють сформулювати пропозиції щодо вдосконалення освітніх програм підготовки вчителів інформатики в цій галузі.

Отже, підготовка майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів є комплексною проблемою, що вимагає системного підходу до підготовки фахівців. Вона має передбачати не тільки формування знань та навичок в галузі цифрової безпеки, але психологічну грамотність та методологічну підготовку майбутнього вчителя.

Аналіз освітньо-професійних програм підготовки вчителів інформатики в різних ЗВО України засвідчив відсутність цілеспрямованих стратегій підготовки вчителів у галузі цифрової безпеки, а тому актуальність і важливість формування готовності майбутніх вчителів інформатики до розвитку навичок цифрової безпеки учнів. Розглянуті дослідження послідовно підкреслюють зростаючу потребу в цифровій грамотності, особливо щодо безпеки, у світі, який все більше залежить від технологій.

Узагальнення сучасного стану підготовки майбутніх учителів інформатики виявляє значні прогалини в їхніх знаннях та навичках в галузі цифрової безпеки, що, у свою чергу, становить значну загрозу цифровій безпеці та благополуччю молоді, яка стає все більш вразливою до цифрових загроз та ризиків в Інтернеті. В розглянутих джерелах підкреслюється різноманітний характер освіти в галузі цифрової безпеки. Мова йде не просто про формування технічних навичок молоді. Йдеться про усвідомлення культури відповідальної поведінки молоді в Інтернеті. Тому майбутні вчителі інформатики потребують особливої підготовки, яка виходить за рамки технічних протоколів безпеки та охоплює соціальні, етичні та правові аспекти цифрової взаємодії для забезпечення їхньої готовності до розвитку навичок цифрової безпеки учнів.

Висновки до розділу 1

У першому розділі «Підготовка майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів як педагогічна проблема» охарактеризовано цифрові загрози і відповідні навички цифрової безпеки молоді та доведено важливість їх розвитку в умовах інформаційного суспільства, а також проведено оцінку теоретичного і практичного стану розробленості проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.

За результатами термінологічного аналізу понять «цифрові загрози», «цифрові небезпеки» та їх видів, зіставлення понять «кібербезпека» і «цифрова безпека» було уточнено поняття навички цифрової безпеки як сукупність знань та умінь для безпечного, відповідального та етичного використання цифрових технологій, яка забезпечує особі захист особистих даних, цифрової ідентичності, пристроїв і мереж від кібератак, а також сприяє свідомому онлайн-спілкуванню.

До основних навичок цифрової безпеки віднесено:

1) розуміння кіберзагроз та способів їх уникнення: ідентифікація основних видів загроз (фішинг, шкідливе програмне забезпечення, атаки програм-вимагачів); використання антивірусного програмного забезпечення та фаєрволів; захист пристроїв від несанкціонованого доступу;

2) управління цифровою ідентичністю та слідом: контроль над особистими даними, що залишаються в цифровому просторі; налаштування конфіденційності в соціальних мережах; використання безпечних методів аутентифікації (двофакторна автентифікація, надійні паролі);

3) здатність виявляти дезінформацію та критично оцінювати інформацію: аналіз джерел інформації на достовірність; розпізнавання маніпулятивного контенту та фейкових новин; виявлення шкідливих або шахрайських сайтів;

4) розуміння основ функціонування комп'ютерних систем та програмного забезпечення: базові знання про операційні системи, мережеві протоколи, налаштування безпеки; використання захищених каналів зв'язку (VPN, шифрування даних); виявлення підозрілої активності на пристроях та в облікових записах;

5) безпечне цифрове спілкування та культура онлайн-поведінки: дотримання правил етикету в Інтернеті (нетикету); уникнення надсилання конфіденційної інформації через незахищені канали; усвідомлення ризиків онлайн-спілкування та соціальної інженерії;

6) розуміння правових та етичних аспектів цифрової безпеки: ознайомлення з правовими нормами щодо захисту персональних даних (українське законодавство); усвідомлення відповідальності за кібербулінг, незаконний обіг інформації та порушення авторських прав; дотримання принципів інформаційної етики;

7) захист здоров'я та добробуту в цифровому середовищі: запобігання цифровій залежності та кібербулінгу; дотримання правил гігієни зору та безпечного використання гаджетів; усвідомлення психологічного впливу цифрових технологій.

Узагальнення наукових результатів дало уявлення про проблеми підготовки вчителів інформатики до розвитку навичок цифрової безпеки учнів у теорії. Так, теоретичний стан розробленості проблеми свідчить наявність наукових розвідок за такими узагальненими напрямами як сприйняття загалом цифрової безпеки вчителями, методи навчання цифрової безпеки, інституційні та кадрові виклики в галузі цифрової безпеки; цифрова безпека в контексті формування цифрової компетентності; освітньо-політичний аспект цифрової безпеки; університетська підготовка майбутніх учителів в галузі цифрової безпеки; шкільна освіта в галузі цифрової безпеки; професійний розвиток учителів у галузі цифрової безпеки.

Аналіз наукових джерел засвідчив актуальність і важливість підготовки майбутніх вчителів інформатики до розвитку в учнів навичок цифрової безпеки. Розглянуті дослідження послідовно підкреслюють зростаючу потребу в цифровій грамотності, особливо щодо безпеки, у світі, який все більше залежить від технологій. Узагальнення сучасного стану підготовки майбутніх викладачів інформатики виявляє значні прогалини в їхніх знаннях та навичках в галузі цифрової безпеки, що, у свою чергу, становить значну загрозу цифровій безпеці та благополуччю молоді, які стає все більш вразливою до кіберзагроз та ризиків в Інтернеті.

Систематизація наукових даних уможливила характеристику практичного стану розробленості проблеми підготовки вчителів інформатики до розвитку навичок цифрової безпеки учнів: диспропорція освітніх програм щодо навчання в галузі цифрової безпеки; наявність прогалин у знаннях та уміннях, пов’язаних із цифровою безпекою; відсутність спеціальної підготовки викладачів з цифрової безпеки; відсутність акценту на практичному навчанні цифрової безпеки; відсутність чітких керівних принципів та політик закладу освіти; проблема ефективного оцінювання навичок цифрової безпеки; проблема пошуку/ вибору відповідних методик навчання.

У наукових дослідженнях наголошується на необхідності постійного оновлення навчальних програм в галузі ІТ, акцентується потреба формування

практичних умінь з цифрової безпеки, підкреслюється важливість опанування майбутніми учителями не лише предметних знань з цифрової безпеки, але й психолого-педагогічних і методичних знань та вмінь формувати в учнів навички цифрової безпеки; опанування інноваційних цифрових стратегій викладання і навчання інформатики. Науковці відзначають як ефективний змішаний спосіб викладання курсів і доводять ефективність різноманітних методів навчання. Окремі наукові розвідки наголошують на потребі розвитку методичної компетентності вчителів інформатики.

На основі аналізу наукової літератури виявлено можливі шляхи модернізації програм підготовки вчителів для розвитку в учнів навичок цифрової безпеки: інтеграція цифрової безпеки в курси з методики навчання інформатики; розробка й упровадження спеціалізованих курсів з цифрової безпеки у освітньо-професійні програми підготовки вчителів; використання цифрових інструментів та технологій симуляції для формування практичних навичок цифрової безпеки; сприяння співпраці та обміну знаннями з професіоналами; приведення навчальних програм у відповідність до міжнародних стандартів.

Результати аналізу свідчать про необхідність уваги до розроблення навчальних курсів з цифрової безпеки, спеціально розроблених для майбутніх і практикуючих вчителів інформатики. Ці курси повинні не тільки озброїти вчителів технічними знаннями для розуміння та пояснення концепцій безпеки, але й надати їм педагогічні інструменти для ефективної інтеграції цих понять у власну професійну діяльність. Крім того, навчальні програми повинні приділяти особливу увагу розвитку критичного мислення та навичок вирішення проблем, пов’язаних із цифровою безпекою, що дозволяє вчителям реагувати на нові загрози та адаптуватися до них. Такий освітній компонент має включати практичні вправи та симуляції, що дозволить майбутнім учителям отримати практичний досвід роботи з інструментами та методами безпеки.

Отже, у розділі подано вирішення 1-го і 2-го завдань дослідження. Основні результати подані у публікаціях [2], [6-9] (згідно з додатком Є).

РОЗДІЛ 2.
ТЕОРЕТИЧНЕ МОДЕЛЮВАННЯ ПРОЦЕСУ ФОРМУВАННЯ ГОТОВНОСТІ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ ДО РОЗВИТКУ НАВИЧОК ЦИФРОВОЇ БЕЗПЕКИ УЧНІВ НА ЗАСАДАХ ІНФОРМАЦІЙНОГО ПІДХОДУ

2.1. Сутність і структура готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів

Питання готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів є надзвичайно актуальним у сучасному цифровому світі. Зростання кількості кіберзагроз та залежність сучасного суспільства від технологій [122] вимагають від освітньої системи підготовки компетентних фахівців, здатних забезпечити безпеку дітей в онлайн-середовищі [172; 146]. Опис сутності та структури готовності учителів інформатики до навчання цифрової безпеки учнів дозволить визначити ключові компоненти цього поняття, розробити ефективні шляхи професійної підготовки майбутніх педагогів і вдосконалити навчально-методичне забезпечення. Це сприятиме не лише успішній підготовці вчителів, але й розвитку свідомих, обізнаних користувачів цифрового середовища, які здатні захищати власні інтереси й дотримуватися етичних норм у кіберпросторі.

Для визначення сутності і структури поняття «готовність учителів інформатики до розвитку навичок цифрової безпеки учнів» розглянемо послідовно поняття "готовність", "готовність до професійної діяльності" та "готовність вчителя до професійної діяльності", спираючись на наявні наукові публікації.

У психології готовність розглядається як особливий стан налаштованості особистості до виконання певної діяльності. Цей стан включає мотиваційні, емоційні та вольові компоненти, які забезпечують успішне виконання завдань. Згідно з дослідженнями, готовність може бути

ситуативною (короткочасною) або стійкою (довготривалою), залежно від умов та характеру діяльності [128].

Готовність до професійної діяльності є інтегративною характеристикою особистості, яка включає сукупність знань, умінь, навичок, мотиваційних та особистісних якостей, необхідних для ефективного виконання професійних обов'язків. Це складне структурне явище, яке формується в процесі професійної підготовки та практичної діяльності [194].

Готовність вчителя до професійної діяльності охоплює не лише загальні компоненти професійної готовності, але й специфічні педагогічні аспекти. Це, зокрема, педагогічні здібності, методичні компетенції, комунікативні навички, емоційна стійкість та здатність до рефлексії. Ця готовність формується під час фахової підготовки та вдосконалюється в процесі педагогічної практики [192].

Аналіз наявних досліджень виявляє неоднозначну картину щодо тлумачення поняття готовності вчителів інформатики до формування в учнів навичок цифрової безпеки. Робота [30] над рамками цифрової компетентності вчителів надає важливі уявлення про ширший контекст для розуміння необхідних знань і вмінь у галузі цифрової безпеки. Рамкова програма наголошує на цілісному розумінні цифрової компетентності, яка включає етичне та безпечне функціонування в різноманітних цифрових середовищах, що є ключовим компонентом освіти з цифрової безпеки. Поширення і популяризація рамкової програми для міждисциплінарної взаємодії наслідує ідею того, що вчителі різних дисциплін повинні інтегрувати цифрову безпеку у свої навчальні програми, підкреслюючи важливість спільного та інтегрованого підходу до освіти з цифрової безпеки.

Дослідження [78] піднімає важливі етичні міркування щодо формування і розвитку потенційно шкідливих навичок, таких як хакерські методи, які є важливими для освіти з кібербезпеки. У статті обґрунтовується важливість впровадження цих навичок у сильні професійні спільноти, які встановлюють етичні принципи та заохочують відповідальне використання таких методів. У дослідженні [81] обговорюються різні стратегії викладання тем

інформаційних систем, включаючи цифрову безпеку. Вони наголошують на необхідності адаптації навчальних програм, щоб йти в ногу з постійно змінюваними технологіями та очікуваннями в IT-галузі. Інші науковці [111] обговорюють необхідні знання та навички для ефективного навчання інформатики в рамках K-12, що неявно включає навички цифрової безпеки. Дослідники демонструють успішний проєкт професійного розвитку, орієнтований на освіту з питань цифрового громадянства, який включає цифрову безпеку та захист [18], а також використання гейміфікації у викладанні кібербезпеки [107].

Ми впевнені, що готовність учителів інформатики до розвитку навичок цифрової безпеки учнів охоплює готовність ефективно навчати учнів різним аспектам цифрової безпеки. Це включає володіння необхідними знаннями, навичками та ставленням для розробки та проведення цікавих та ефективних уроків, оцінки розуміння учнями, адаптації до мінливих загроз та сприяння культурі відповідального цифрового громадянства. [20; 177]. Ця готовність стосується не лише технічної підготовки, а й педагогічної підготовки, розуміння відповідних педагогічних підходів та здатності створювати безпечне та сприятливе навчальне середовище [5]. Крім того, це передбачає розуміння психологічних факторів, які впливають на поведінку учнів в Інтернеті, та здатність вирішувати медіапроблеми [89].

Сутність готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів має враховувати комплекс знань та умінь, необхідних для ефективного навчання дітей основам безпечної поведінки в цифровому середовищі [145]. Це передбачає не тільки технічні аспекти цифрової безпеки, але й педагогічні знання й уміння, які дозволяють адаптувати навчальний матеріал до вікових особливостей учнів та ефективно доносити інформацію [185]. Важливою складовою є також розуміння психологічних аспектів поведінки дітей в інтернеті та вміння формувати у них відповідальне ставлення до цифрових технологій [149].

Крім того, тлумачення готовності має враховувати потребу постійного оновлення знань та їх адаптацію до нових тенденцій цифрової безпеки [162]. Швидкий розвиток технологій та поява нових загроз вимагають від учителів постійного навчання та самовдосконалення, щоб забезпечити актуальність освітнього процесу [134; 175], чим додатково підкреслюється важливість безперервного професійного розвитку в галузі цифрової безпеки для педагогів [193].

З урахуванням наведених визначень і міркувань про те, що має увиразнювати готовність учителів інформатики до розвитку навичок цифрової безпеки учнів, та раніше сформульованого поняття "навички цифрової безпеки", надамо відповідне тлумачення провідному поняттю нашого дослідження.

Готовність учителів інформатики до розвитку навичок цифрової безпеки учнів - це інтегративна особистісна здатність майбутнього вчителя інформатики розвивати навички цифрової безпеки учнів, яка поєднує: (1) усвідомлені прагнення такого розвитку; (2) специфічні знання й уміння; (3) навички рефлексії щодо успішності такого розвитку.

Отже, готовність учителів інформатики до розвитку навичок цифрової безпеки учнів є складним особистісним надбанням з певною множиною взаємопов’язаних компонентів. Ми можемо ідентифікувати ці компоненти за трьома ключовими напрямками:

Мотиваційний компонент (прагнення розвитку навичок цифрової безпеки учнів).

В умовах стрімкого розвитку цифрових технологій учні активно взаємодіють з інтернетом, що підвищує ризики цифрових загроз [26]. Тому вчителі повинні бути мотивованими не лише підвищувати власні знання у сфері цифрової безпеки, але й активно передавати ці знання учням. Мотивоване прагнення вчителів розвивати навички цифрової безпеки учнів залежить від їхньої професійної підготовки, підтримки з боку освітнього середовища та усвідомлення важливості даної проблематики.

Учні активно взаємодіють з ресурсами мережі Інтернет, і водночас зростає кількість кіберзагроз, таких як фішингові атаки, кібербулінг, витік персональних даних. Усвідомлення цих загроз спонукає вчителів поглиблювати знання учнів у галузі цифрової безпеки та розвивати відповідні уміння. Вчителі, які розуміють ризики цифрового середовища, сприймають себе як ключових агентів у захисті учнів. Це підвищує їхню відповідальність і мотивацію розвивати відповідні навички в учнів.

Дослідження також показують, що вчителі з вищим рівнем цифрової грамотності частіше інтегрують теми цифрової безпеки в навчальний процес. Ті ж, хто має недостатню підготовку, можуть уникати цієї тематики через невпевненість у власних знаннях. Звіт OECD [75] зазначає, що у країнах, де впроваджено системні освітні програми з цифрової безпеки, вчителі демонструють значно вищий рівень зацікавленості у формуванні відповідних навичок в учнів. Також дослідження [69] вказує, що недостатнє розуміння цифрових ризиків серед вчителів призводить до того, що теми безпеки розглядаються поверхово або взагалі ігноруються. Тому усвідомлення вчителями важливості цифрової безпеки є ключовим мотивуючим чинником для розвитку навичок цифрової безпеки учнів.

Мотивація вчителів розвивати навички цифрової безпеки в учнів тісно пов’язана з їхнім усвідомленням необхідності формування таких власних навичок. Це усвідомлення є ключовим фактором, що спонукає педагогів інтегрувати принципи цифрової безпеки в освітній процес [131; 163]. Вчителі, які розуміють важливість цифрової безпеки, відчувають професійний обов’язок забезпечити учнів необхідними знаннями та навичками для безпечної роботи в інтернеті. Усвідомлення значущості цифрової безпеки стимулює вчителів до підвищення власної цифрової компетентності, що дозволяє їм ефективніше передавати знання учням та слугувати прикладом безпечної поведінки в цифровому середовищі.

Вчителі, які розуміють ризики цифрового світу, прагнуть створити безпечне освітнє середовище. Це включає не лише технічні аспекти, але й

формування культури відповідального використання цифрових ресурсів серед учнів. Усвідомлення важливості цифрової безпеки спонукає вчителів до співпраці з батьками та місцевою спільнотою. Це забезпечує комплексний підхід до виховання навичок цифрової безпеки, що підсилює мотивацію педагогів у цій сфері.

Отже, усвідомлення вчителями потреби розвитку навичок цифрової безпеки у учнів є фундаментом їхньої мотивації діяти в цьому напрямку. Це усвідомлення впливає на їхню професійну діяльність, сприяє особистісному розвитку та забезпечує безпечне освітнє середовище.

Предметно-методичний компонент (специфічні знання й уміння)

Предметно-методичний компонент поєднує в собі предметні знання про цифрову безпеку і методичні знання щодо стратегій розвитку навичок цифрової безпеки учнів. Цей компонент включає характеризується розумінням вчителями концепцій, принципів та сучасних загроз цифрової безпеки. [55], а тому включає знання про цифрові загрози, вразливості та стратегії пом’якшення, а також етичні та юридичні аспекти, пов’язані з цифровою безпекою і розуміння основних загроз та ризиків, пов’язаних з використанням інтернету, знання методів захисту інформації та способів запобігання кіберзлочинам.

Вчителі повинні розуміти різні типи шкідливого програмного забезпечення, методи фішингу та соціальної інженерії, а також принципи криптографії та захисту даних [150]. Крім знань про зміст, вчителі повинні знати, як складні концепції цифрової безпеки перевести у відповідний віку цікавий навчальний досвід [117].

Також важливим є те, що вчителі повинні усвідомлювати етичні та правові наслідки освіти з цифрової безпеки. Це передбачає розуміння питань, пов’язаних із конфіденційністю, захистом даних, інтелектуальною власністю та безпекою в Інтернеті. Вчителі повинні мати можливість враховувати ці етичні та правові міркування на своїх уроках, допомагаючи учням зрозуміти важливість відповідального цифрового громадянства та наслідки неетичної

або незаконної поведінки в Інтернеті. Також вони повинні бути обізнані зі шкільною політикою та законодавчими рамками щодо використання технологій та конфіденційності даних учнів [55].

Крім теоретичних знань, майбутні вчителі повинні володіти практичними навичками роботи з цифровими технологіями та засобами захисту інформації [159]. Ефективна освіта з цифрової безпеки вимагає від учителів вміння користуватися різними технологіями. Це включає вміння користуватися відповідним програмним забезпеченням та інструментами для викладання та оцінювання, а також здатність усувати технічні проблеми, які можуть виникнути під час уроків. Крім того, вчителі повинні бути винахідливими у пошуку та адаптації відповідних цифрових ресурсів, включаючи онлайн-інструменти, симуляції та ігри, для покращення навчання учнів [107]. Це включає в себе вміння використовувати антивірусні програми, налаштовувати брандмауери, створювати надійні паролі та використовувати інші методи захисту даних [157]. Вони повинні вміти використовувати різні інструменти для моніторингу безпеки та аналізу загроз [195].

Важливою складовою готовності є методичні уміння, які дозволяють ефективно передавати і розвивати знання та навички з цифрової безпеки учням [152]. Це включає в себе вміння розробляти та проводити цікаві та ефективні уроки, використовувати інтерактивні методи навчання, а також враховувати індивідуальні особливості учнів [184]. Важливо також вміти оцінювати рівень знань учнів та адаптувати навчальний процес відповідно до їх потреб [188].

Вчителі повинні вміти мотивувати учнів до навчання, формувати у них відповідальне ставлення до цифрових технологій та розвивати їхню критичне мислення [149]. Вони повинні знати, як спілкуватися з дітьми на тему цифрової безпеки, враховуючи їхній вік та рівень розвитку [160]. Важливим для вчителя інформатики є володіння різними підходами до навчання цифрової безпеки [178]. Це включає в себе використання інтерактивних ігор, симуляцій та інших інноваційних методів навчання, які допомагають учням краще засвоїти матеріал [183]. Вчителі повинні вміти використовувати різні

ресурси та інструменти для навчання, включаючи онлайн-платформи та навчальні матеріали. Оцінка розуміння учнями цифрової безпеки має важливе значення для оцінки ефективності викладання та виявлення сфер, де учні потребують додаткової підтримки [92]. Вчителі повинні вміти розробляти, використовувати та впроваджувати різні методи оцінювання, включаючи формувальне та підсумкове оцінювання, для вимірювання знань, навичок та ставлення учнів, пов’язаних із цифровою безпекою. Це також включає здатність надавати конструктивний зворотний зв’язок учням, допомагаючи їм зрозуміти свої сильні та слабкі сторони та спрямовуючи їх до власного розвитку [39].

Отже, предметно-методичний компонент характеризується сукупністю предметних знань, знань методичних підходів для розвитку навичок цифрової безпеки та психолого-педагогічних знань та умінь дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки учнів.

Особистісний компонент (навички рефлексії щодо успішності розвитку навичок цифрової безпеки учнів)

Рефлексивна діяльність допомагає вчителю адаптувати підходи до навчання, оцінювати власні знання та вдосконалювати освітній процес. Рефлексія дає змогу вчителю оцінити свої знання у сфері цифрової безпеки та виявити прогалини, які необхідно заповнити через професійний розвиток. Дослідження показують, що вчителі, які регулярно аналізують свої навички, частіше беруть участь у курсах підвищення кваліфікації [45]. Вчителі, які володіють навичками рефлексії, можуть оцінити ефективність своїх підходів до викладання цифрової безпеки та вносити корективи на основі відгуків учнів. Використання рефлексії сприяє розвитку адаптивних методик навчання, що дозволяє вчителям інтегрувати цифрову безпеку в різні предмети та освітні платформи [115]. Вчителі, які рефлексують над власною діяльністю, більш ефективно розвивають навички критичного мислення учням, що є важливим для розвитку навичок цифрової безпеки (наприклад, аналіз фейкових новин, виявлення шахрайських схем), що підтверджує [88]. Через рефлексію вчителі

можуть аналізувати етичні та правові аспекти цифрової безпеки, що дозволяє їм коригувати свої підходи відповідно до сучасних законодавчих норм і стандартів [58].

Сфера цифрової безпеки постійно розвивається, регулярно з'являються нові загрози та вразливості [93]. Тому вчителям інформатики необхідно займатися безперервним професійним розвитком, щоб бути в курсі останніх тенденцій, технологій та передового досвіду. Це передбачає активний пошук можливостей для професійного навчання, включаючи семінари, конференції, онлайн-курси та можливості спільного навчання. Також важливим є вміння критично оцінювати інформацію та адаптуватися до нових подій.

Ефективна освіта з цифрової безпеки часто передбачає співпрацю з іншими зацікавленими сторонами, включаючи батьків, шкільних адміністраторів та громадські організації. Вчителі повинні вміти ефективно спілкуватися з цими зацікавленими сторонами, обмінюватися інформацією про загрози цифровій безпеці та найкращі практики, а також будувати партнерства для підтримки навчання учнів. Це також передбачає співпрацю з колегами для обміну ресурсами, кращими практиками та підтримки один одного в їхніх зусиллях щодо ефективного викладання цифрової безпеки [20]. Міждисциплінарна співпраця також важлива, оскільки виклики кібербезпеки часто вимагають експертизи з різних галузей.

Отже, особистісний компонент є важливою складовою готовності вчителя інформатики до розвитку навичок цифрової безпеки учнів. Рефлексивна діяльність дозволяє аналізувати власний рівень цифрової компетентності, вдосконалювати методики навчання, формувати критичне мислення у школярів та усвідомлювати етичні аспекти цифрової взаємодії.

Узагальнюючи наші міркування щодо сутності й структури готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів, вважаємо що вона може бути представлена структурою, що включає в себе декілька взаємопов'язаних компонентів (рис.2.1).

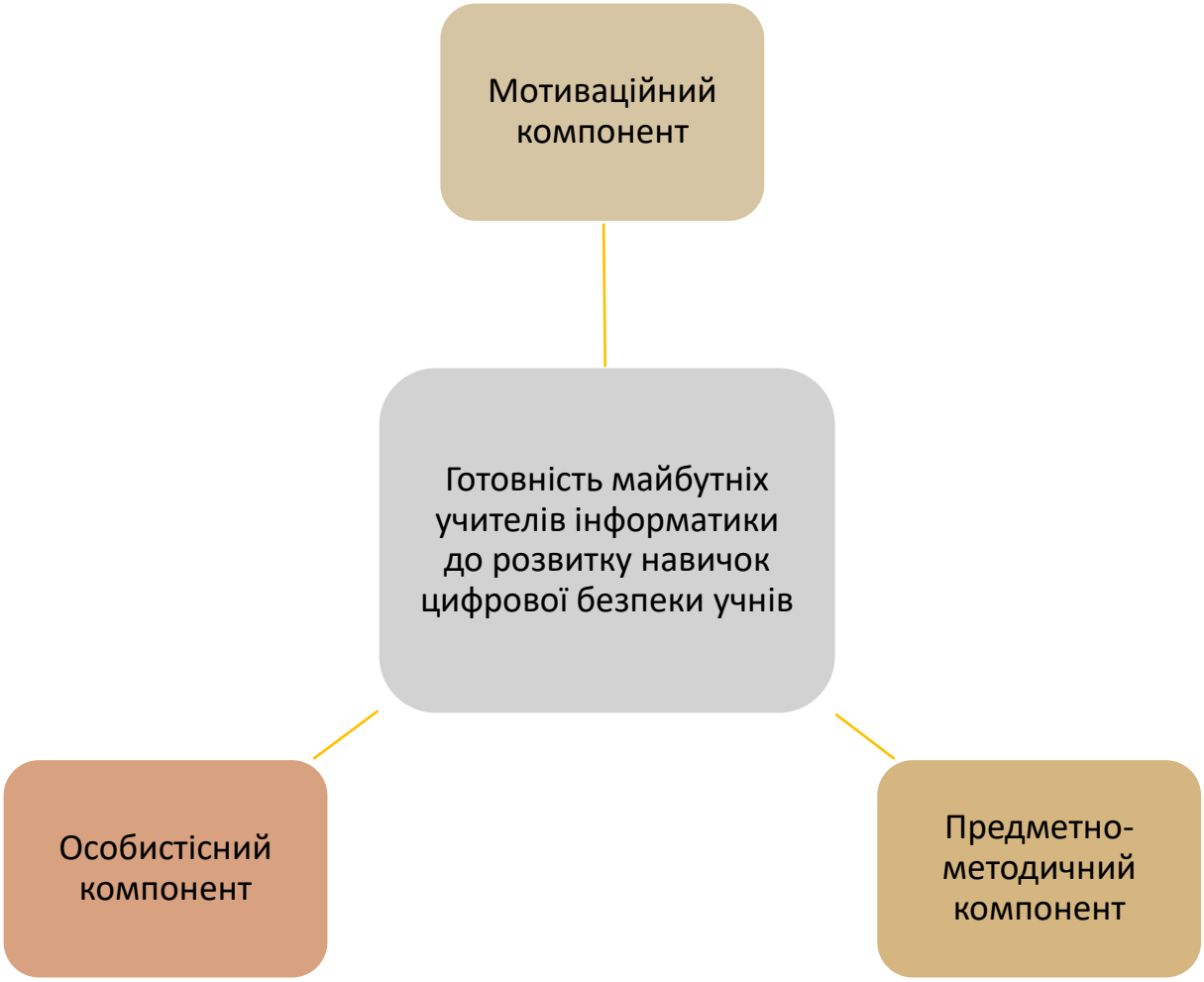


Рис. 2.1. Структура готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів

Ці компоненти включають: розуміння різноманітних загроз (шкідливе програмне забезпечення, фішинг, соціальна інженерія та інші), здатність до аналізу загроз та їх впливу, усвідомлення правових та етичних наслідків кібербезпеки (закони про конфіденційність даних, права інтелектуальної власності, відповідальна поведінка в Інтернеті), а також наявність практичних навичок безпечної онлайн-практики, управління паролями та захисту даних тощо. Формування цих та інших навичок потребує розроблення і упровадження ефективних стратегій навчання через перехід від традиційних методів навчання до більш ефективних і цікавих для молоді.

Серед стратегій формування готовності вчителів до розвитку навичок цифрової безпеки учнів науковці пропонують інвестування у високоякісні, комплексні програми професійного розвитку, спеціально орієнтовані на освіту з цифрової безпеки [5]. Ці програми мають бути зосереджені не лише на знаннях зі змісту, а й на педагогічних підходах, стратегіях оцінювання та використанні ІТ для розвитку навичок цифрової безпеці. Програми також повинні бути постійними та адаптованими до мінливого характеру цифрових загроз.

Також науковці наголошують на тому, що школи повинні забезпечити, щоб вчителі інформатики мали доступ до необхідних ресурсів і технологій для ефективного викладання цифрової безпеки [24]. Це включає надання оновленого програмного забезпечення, надійного доступу до Інтернету, захоплюючих цифрових навчальних матеріалів та можливостей професійного розвитку, орієнтованих на ефективне використання технологій в освіті.

Ще один шлях, який виокремлюють науковці, - це інтеграція цифрової безпеки в існуючі навчальні програми з інформатики. Це потрібно для забезпечення того, щоб учні отримували всебічне і вчасне уявлення про цифрові небезпеки. Результати досліджень [24; 39; 93] свідчать про необхідність уваги до розроблення комплексних навчальних курсів з цифрової безпеки, спеціально розроблених для майбутніх і практикуючих вчителів інформатики. Ці курси повинні не тільки озброїти вчителів технічними знаннями для розуміння та пояснення концепцій безпеки, але й надати їм педагогічні інструменти для ефективної інтеграції цих понять у власну професійну діяльність. Крім того, навчальні програми повинні приділяти особливу увагу розвитку критичного мислення та навичок вирішення проблем, пов’язаних із цифровою безпекою, що дозволяє вчителям реагувати на нові загрози та адаптуватися до них. Такий освітній компонент має включати практичні вправи та симуляції, що дозволить майбутнім учителям отримати практичний досвід роботи з інструментами та методами безпеки. Цей комплексний підхід вимагає зміни педагогічних стратегій – заохочення

активного навчання, розвиток навичок критичного мислення, формування культури цифрової відповідальності з самого початку освітнього шляху учня. Важливим є посилення впевненості та постійний розвиток цифрової компетентності вчителів для протидії виникаючим цифровим загрозам, тим самим надаючи їм можливість створювати безпечне та надійне освітнє середовище для своїх учнів.

Однією з ефективних стратегій навчання цифрової безпеки є впровадження інформаційного підходу, який базується на уміннях шукати, опрацьовувати і поширювати різноманітні дані у цифровому просторі. Його використання у підготовці вчителів інформатики бачиться ефективним, а тому актуалізується контекст підготовки вчителів інформатики – формування готовності вчителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

2.2. Інформаційний підхід як провідний підхід в організації сучасного освітнього процесу

Перелічені нами (розділ 1) аспекти (зміст освітніх програм підготовки вчителів інформатики; інтеграція ІТ у професійну підготовку вчителів інформатики; освітня політика та наявні цифрові освітні ресурси; потреба у вміннях перетворювати інформацію; доцільність інтерактивного моделювання; потреба професійного розвитку вчителів за рахунок різноманітних цифрових ресурсів) пов’язані з інформаційними технологіями ІТ та інформаційними ресурсами, що вказує на потенціал інформаційного підходу як провідного у підготовці вчителів інформатики для формування в учнів навичок цифрової безпеки. Тому надалі наведемо аргументи на користь інформаційного підходу у підготовці вчителів інформатики для формування в учнів навичок цифрової безпеки. Аргументацію проведемо поетапно з використанням різних методів наукового пізнання (термінологічний аналіз, контент-аналіз, порівняльний аналіз).

Інформаційний підхід в освіті: визначення та характеристика

«Інформаційний підхід» в освіті, хоча і не має жорсткого визначення, охоплює педагогічні стратегії з використанням ІТ для поліпшення викладання і навчання [48]. Його основу складають постулати [176]: «інформація є універсальною та фундаментальною категорією; в основі будь-якого процесу чи явища можна виокремити інформаційну складову; інформація відображає сутність процесів, що відбуваються в природі та суспільстві; усі існуючі взаємозв'язки мають інформаційну природу; Всесвіт розглядається як глобальний інформаційний простір, у межах якого функціонують і взаємодіють багаторівневі інформаційні системи.

Значущість інформаційного підходу обумовлена такими факторами: інформація має універсальний характер і проникає в усі сфери людської діяльності, що робить її однією з ключових категорій соціального розвитку; постійне зростання обсягів інформації, її доступність та можливість ефективного й творчого використання; активні процеси інформатизації суспільства; розвиток сучасних інформаційних технологій та технічних засобів; інформація та знання є визначальними результатами формування інформаційного суспільства [176].

Підхід виходить за рамки простої заміни традиційних методів навчання. Він наголошує на трансформації процесу навчання, сприянні розвитку критичного мислення, вирішенню проблем в освіті. ІТ уможливлюють створення інтерактивного освітнього середовища, що задовольняє різноманітні моделі навчання [104]. Так, у дослідження [1] показано практичне застосування інформаційного підходу, за якого інтерактивні моделі електронного навчання значно покращують навички кібербезпеки учнів.

Інформаційний підхід ґрунтується на ідеї, що навчання в основі своїй є діяльністю з обробки інформації [197]. Він розглядає знання не як статичні факти, а як їх динамічну систему, яку люди конструюють і використовують. На відміну від традиційних підходів, орієнтованих на передачу знань, інформаційний підхід надає пріоритет активному навчанню, коли студенти

займаються вибором, організацією, інтерпретацією та застосуванням даних. Така активна участь сприяє розвитку критичного мислення, дозволяючи студентам оцінювати джерела інформації, виявляти упередження та синтезувати інформацію з різних точок зору [148].

Успішна реалізація інформаційного підходу вимагає детального аналізу педагогічних стратегій та розвитку відповідних навичок цифрової грамотності [102]. Ефективне використання ІТ передбачає попереднє проектування освітнього процесу для формування навчального досвіду з використанням ІТ [85]. Реальні сценарії допомагають студентам зрозуміти цифрові небезпеки та важливість превентивних заходів [44], імітація фішингової атаки може надати важливий досвід негативного впливу [77], а спільна навчальна діяльність (групові проекти або взаємне навчання) підвищує зацікавленість студентів та сприяє розвитку навичок командної роботи.

Інформаційний підхід визнає важливість індивідуальних підходів навчання, що надають можливості реалізації персоналізованих освітніх траєкторій [148]. Також інформаційний підхід вимагає розвитку інформаційної грамотності – здатності знаходити, оцінювати та ефективно використовувати інформацію як важливої навички 21-го століття [197]. Він часто передбачає включення різноманітних освітніх ресурсів, різноманітних цифрових інструментів та технологій для підвищення мотивації та пізнавальної активності.

Цифрова безпека розглядається як сукупність процесів усвідомлення, аналізу, збереження, захисту, передачі та відповідального використання інформації в цифровому середовищі. Вона базується на критичному мисленні, інформаційній грамотності та знаннях про можливі кіберзагрози. Готовність учителів до формування навичок цифрової безпеки в учнів у межах інформаційного підходу передбачає активну взаємодію педагогів із різними типами цифрової інформації, її оцінку, розпізнавання потенційних ризиків та розробку стратегії їхнього уникнення.

Застосування інформаційного підходу сприяє ефективному розвитку цифрових компетентностей учителів, оскільки забезпечує системний аналіз інформаційних потоків, механізмів їх захисту та методів безпечної взаємодії в цифровому просторі. Використання різних цифрових платформ, соціальних мереж, електронних освітніх ресурсів і хмарних сервісів дозволяє інтегрувати принципи цифрової безпеки в освітній процес, формуючи відповідальне ставлення учнів до персональних даних, онлайн-спілкування та інформаційної гігієни.

Дослідження [155] показало, що сьогодні «лише інформаційний підхід враховує специфіку інформаційного суспільства». Автори рекомендують «доповнити базову сукупність педагогічних підходів …кіберонтологічним підходом….- узагальнити та систематизувати знання у галузі застосування сучасних інформаційно-комунікаційних, комп'ютерних, цифрових, електронних та інтернет-технологій у системі освіти, які стали актуальними для сучасного «цифрового» суспільства».

Інформаційний підхід покращує результати навчання за рахунок зміщення акценту з пасивного сприйняття інформації студентом на активне його залучення у процес навчання [197]. Поширені методи, такі як лекції, часто призводять до пасивного навчання. На противагу цьому, інформаційний підхід заохочує активні методи навчання, серед яких проблемно-орієнтовані, проєктні, ігрові та навчання на основі запитів. Такі методи навчання вимагають від студентів активного пошуку, аналізу та синтезу інформації для вирішення проблем, виконання проектів або пошуку відповідей на дослідницькі питання, чим розвивають власне критичне мислення. Таке активне навчання покращує запам'ятовування знань та розвиває навички аналізу, оцінки, вирішення проблем та співпраці.

Інформаційний підхід сприяє активним дискусіям, використанню симуляцій та дослідженню різних (навіть великої кількості) конкретних випадків різних навчальних завдань. Дослідження свідчать про позитивний вплив активного навчання на залученість студентів та їхню академічну

успішність. На думку [148], інформаційний підхід сприяє індивідуалізованому навчанню, розпізнаванню різних темпів і стилів навчання.

Інформаційний підхід уможливлює інтеграцію цифрових інструментів і ресурсів в освітній процес. Інформація в Інтернеті та інтерактивні цифрові технології сприяють у набутті потрібного досвіду. Цифрові інструменти полегшують доступ до різноманітних джерел інформації, і це дозволяє проводити дослідження різних проблемних питань [148], і використання цифрових середовищ (інтерактивні симуляції, віртуальні лабораторії та онлайн-платформи для спільної роботи) підвищує залученість студентів до процесу навчання та забезпечує практико-орієнтоване навчання.

Залучення цифрових інструментів як засобів інформаційного підходу сприяє персоналізованому навчанню, яке базується на адаптивному навчанні на цифрових освітніх платформах. Прикладами таких платформ можуть служити Moodle, Google Cloud Services і BigBlueButton [148]. Інтерактивні блоки електронного навчання значно покращують цифрові навички студентів [1]. Однак, як зазначено у [61], інтерактивне навчання вимагає врахування рівня цифрової грамотності суб’єктів учіння, а також забезпечення доступу та безпеки в Інтернет, що також вимагає навичок цифрової безпеки. Майбутні учителі інформатики потребують навчання використанню цих інструментів, тому освітні ініціативи і заходи в форматі е-навчання мають забезпечувати безпечне навчальне середовище [4].

Інформаційний підхід та навички цифрової безпеки

Інформаційний підхід відіграє важливу роль у формуванні в учнів навичок цифрової безпеки. Приділяючи особливу увагу критичному мисленню та оцінці інформації, він дає здобувачам освіти змогу виявляти та пом’якшувати загрози із мережі Інтернеті [61], що включає розпізнавання спроб фішингу, розуміння надійних паролів і практику безпечного перегляду веб-сторінок в Інтернеті [77]. Інтеграція цифрових інструментів забезпечує практичний аспект розвитку навичок цифрової безпеки при вивченні ІТ-дисциплін. Тому студенти, майбутні учителі інформатики, а також учні на

уроках інформатики можуть брати участь у симульованих кібератаках, аналізувати вразливості безпеки та експериментувати із заходами безпеки. Проектне навчання є ефективним, дозволяючи студентам застосовувати свої знання в реальних ситуаціях [43]. При цьому саме інформаційний підхід допомагає учням зрозуміти етичні аспекти цифрової безпеки, пропагуючи відповідальне використання технологій та повагу до приватності.

Ми виявили кілька закордонних досліджень, які висвітлюють успішні стратегії інтеграції інформаційного підходу в програми підготовки вчителів. Один із підходів передбачає створення інтерактивних одиниць електронного навчання, адаптованих до конкретних детермінант цифрового громадянства [1]. Дослідження, яке проведено в Університеті Умм аль-Кура, використовувало квазі-експериментальний дизайн з когнітивними тестами та картками спостережень для вимірювання ефективності когнітивних та виконавських проявів навичок кібербезпеки. Результати продемонстрували статистично значуще покращення знань та навичок в галузі кібербезпеки.

Ще одна успішна стратегія передбачала використання проектного навчання [43]. Науковці довели, що такий підхід не тільки дає базові знання з цифрової безпеки, а й вчить студентів застосовувати набуті знання у технологічному середовищі. Дослідження продемонструвало, що проєктний підхід дозволяє майбутнім вчителям охопити весь процес вирішення проблем.

Аналізуючи освітні практики, відзначаємо важливість добре структурованої програми навчальної дисципліни, використання активних та інтерактивних методів навчання, необхідність постійного оцінювання студентів, а також важливість адаптації методів навчання для задоволення потреб цифрового покоління. Дослідження [24], засвідчило, що створення сприятливого інформаційно-освітнього середовища (включає Moodle, хмарні сервіси Google та інструменти для відеоконференцій) має важливе значення для ефективної підготовки вчителів, де важливі різноманітний навчальний зміст, різні методи і форми освітньої діяльності для задоволення індивідуальних потреб студентів.

Упровадження інформаційного підходу пов’язане з труднощами. Підготовка та професійний розвиток вчителів інформатики мають важливе значення для розвитку знань та вмінь учнів у галузі цифрової безпеки. Тому вчителям інформатики потрібні відповідні методичні навички та ІТ-знання для реалізації стратегій активного навчання та інтеграції цифрових інструментів в процес навчання інформатики.

Майбутні учителі інформатики також мають усвідомлювати, що забезпечення рівного доступу до технологій та ресурсів для всіх учнів є важливим [102], як і вирішення питань цифрової грамотності, безпеки в Інтернеті та управління власною діяльністю в мережі Інтернет [61], усвідомленням ризиків та знанням методів їх уникнення через розвиток навичок інформаційної гігієни [90]. При цьому використання інформаційного підходу до підготовки майбутніх учителів інформатики дає різні можливості. Зростаюча доступність цифрових ресурсів та поширення інноваційних підходів до навчання, організація різноманітних електронних навчальних середовищ можуть загалом сприяти розвитку критичного мислення, навичок вирішення проблем та інших важливих навичок 21-го століття. Обмежений доступ до технологій та підключення до Інтернету може бути бар’єром у використанні інформаційного підходу.

Отже, ефективне формування навичок цифрової безпеки в учнів неможливе без випереджувальної підготовки вчителя інформатики, яка повинна не лише забезпечувати знання про сучасні цифрові загрози, а й озброювати педагога дієвими підходами до навчання цифрової безпеки. Інформаційний підхід у цьому контексті відіграє ключову роль, оскільки дозволяє майбутнім учителям опанувати принципи безпечної взаємодії в цифровому середовищі, критичного аналізу інформації, захисту персональних даних та етичного використання цифрових ресурсів.

Застосування цього підходу в підготовці вчителів інформатики сприяє їхній здатності передбачати потенційні ризики цифрового середовища, аналізувати інформаційні загрози та адаптувати освітній процес відповідно до

змін у сфері кібербезпеки. Активна взаємодія з цифровими платформами, інструментами управління інформацією та засобами захисту даних дозволяє майбутнім педагогам не тільки опанувати цифрову безпеку особисто, а й ефективно передавати ці знання учням. Інформаційний підхід забезпечує системне розуміння того, як інформація циркулює в цифровому середовищі, які механізми впливають на її безпеку та як навчити учнів захищати себе від можливих загроз.

2.3. Модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу

Попередньо нами обґрунтовано, що в сучасних умовах цифрової трансформації освіти формування навичок цифрової безпеки учнів стає однією з ключових задач педагогічної діяльності. Майбутні вчителі інформатики повинні володіти не лише глибокими знаннями з предмету, але й навичками, які розвивають в учнів навички безпечної поведінки в цифровому середовищі. Для цього необхідно розробити модель формування таких навичок в межах їх професійної підготовки.

Сьогодні поняття «модель» інтерпретують як: «спрощене представлення реального об’єкта, процесу або системи, що відображає їх ключові характеристики та взаємозв’язки» [64]; «абстрактне представлення реальних об’єктів, процесів або явищ, яке відображає їхні суттєві характеристики та зв’язки між ними [82] та інші. Але всі означення свідчать, що це представлення чогось з обов’язковим відображенням певних характеристик чи властивостей. Тому моделювання - це процес створення та використання моделей для вивчення, аналізу та прогнозування поведінки об’єктів або систем .

У педагогіці модель використовується для опису, аналізу та прогнозування освітніх процесів. Згідно з дослідженнями, модель є інструментом, який дозволяє структурувати професійну підготовку та

визначати шляхи досягнення поставлених цілей [82]. Відповідно, «моделювання» у педагогіці — це метод дослідження, який передбачає створення теоретичної конструкції, що відображає етапи, компоненти та механізми формування професійної якості майбутніх фахівців. Наприклад, модель підготовки вчителя інформатики — це систематизований опис компонентів, які забезпечують формування професійної готовності педагога до навчання учнів інформатики.

Українська освітня система активно розвивається, зокрема, відбувається удосконалення підготовки вчителів інформатики, що обумовлено потребами цифрової трансформації та зростанням значущості цифрової грамотності молоді. Ми провели аналіз сучасних моделей підготовки вчителів інформатики і виділили такі. Загалом для підготовки вчителів інформатики сьогодні використовуються різні моделі, серед яких відзначимо [19]: модель професійного розвитку через курси підвищення кваліфікації; модель самостійного навчання через відео-тренінги; інтерактивна модель навчання через вебінари; модель очного навчання, яка включає практичні семінари та тренінги для вчителів інформатики та інші. Однак, ці моделі не завжди повністю враховують методичний аспект підготовки вчителя та охоплюють загалом аспект формування готовності вчителів інформатики до розвитку навичок цифрової безпеки учнів. Наприклад, деякі курси, як-от "Вступ до кібербезпеки для педагогів" [14], пропонують базові знання з кібербезпеки, але не фокусуються на методиці формування або розвитку цих навичок.

Модель підготовки вчителів інформатики на засадах компетентнісного підходу базується на формуванні ключових компетентностей, необхідних для ефективної роботи вчителя інформатики в умовах цифрової освіти. Вона включає формування низки компетентностей: професійних (основ програмування, алгоритмізації, роботи з даними, а також сучасних ІТ); цифрових (вміння використовувати цифрові інструменти для навчання, організації дистанційного навчання тощо), методичних (навички розробки

навчальних матеріалів, використання інтерактивних методів навчання та інтеграції цифрових технологій у навчальний процес).

Модель інтеграції STEM-освіти в підготовку вчителів [199] є важливим кроком для розвитку інноваційних підходів у навчанні. Ця модель передбачає: міждисциплінарний підхід як поєднання знань з інформатики, математики, фізики та інженерії для розв'язання практичних задач; проектну діяльність для розробки та реалізації навчальних проектів, які сприяють розвитку креативного мислення учнів; використання сучасних технологій: застосування робототехніки, 3D-моделювання, штучного інтелекту та інших інноваційних інструментів.

Модель формування цифрової грамотності вчителів у системі післядипломної освіти є особливо актуальною у контексті зростання кіберзагроз [190]. У цій моделі передбачено «програми та курси, спрямовані на формування цифрової грамотності вчителів».

Сьогодні визначено умови формування цифрової компетентності вчителів, які реалізуються у системі післядипломної педагогічної освіти. Однією з провідних «визначено мотивацію вчителя до неперервного професійного розвитку та самооцінювання ним цифрової компетентності» [135].

Проаналізовані нами моделі підготовки вчителів інформатики в Україні демонструють різні підходи до формування професійної готовності педагогів у контексті цифрової трансформації. Кожна з моделей має свої переваги та орієнтована на різні аспекти підготовки: від формування компетентностей до інтеграції інноваційних методів навчання та цифрових засобів їх підтримки. Використання цих моделей дозволяє підвищити якість підготовки майбутніх вчителів інформатики та забезпечити їхню готовність до роботи в умовах сучасних викликів цифрової ери.

Водночас стверджуємо, що для ефективного формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу необхідно розробити комплексну модель,

яка б включала: теоретичну підготовку з питань цифрової безпеки; формування практичних навичок застосування заходів цифрової безпеки; опанування методики викладання і навчання цифрової безпеки для різних вікових груп; розвиток критичного мислення та навичок аналізу ризиків; вивчення сучасних тенденцій та загроз у цифровому просторі; шляхи інтеграції питань цифрової безпеки в загальний курс інформатики. Така модель повинна базуватися на інформаційному підході, який передбачає систематичне використання та аналіз актуальної інформації про цифрові загрози та методи захисту. Це дозволить майбутнім учителям інформатики бути завжди в курсі останніх тенденцій у сфері цифрової безпеки та ефективно передавати ці знання учням.

Узагальнення наукових результатів показало, що сучасні моделі формування цифрової компетентності майбутніх педагогів містять елементи, що опосередковано стосуються цифрової безпеки, але не мають цілісного підходу до розвитку відповідних навичок у учнів.

Аналіз джерел свідчить про увиразнення у моделях етапів професійного розвитку (зокрема, мотиваційний етап із залученням цифрових ресурсів, практичне опанування ІТ, використання проектних методів навчання). Хоча ці моделі формують загальну цифрову грамотність, питання цифрової безпеки розглядаються фрагментарно – лише як частина загальних компетенцій цифрового громадянина [126]. Аналіз структурних компонентів існуючих моделей [136; 189 та ін.] показує включення кількох аспектів цифрової безпеки до ключових компонентів цифрової компетентності (табл. 2.1).

Таблиця 2.1

Включеність цифрової безпеки до складу цифрової компетентності

Компонент цифрової компетентності	**Характеристика**	**Включеність аспектів безпеки**
Технічний	Робота з цифровими інструментами	Часткове (на рівні базових навичок)
Методичний	Педагогічне застосування	Відсутнє

Компонент цифрової компетентності	Характеристика	Включеність аспектів безпеки
	технологій	
Етико-правовий	Академічна доброчесність, авторське право	Неявне
Безпека	Захист від кіберзагроз	Як окремий підрозділ

Також аналіз свідчить, що європейські підходи до підготовки вчителів інформатики акцентують на формуванні критичного мислення для аналізу інформаційних ризиків; розвитку навичок захисту персональних даних; використанні цифрових технологій з дотриманням етичних норм [140]. Проте жодна з розглянутих моделей не містить: спеціалізованих модулів з методики навчання цифрової безпеки; системи формування вмінь моделювати загрози цифрового середовища та відповідати на них; механізмів оцінювання рівня сформованості навичок безпеки в учнів; імплементації інформаційного підходу (системного аналізу загроз, прогнозування ризиків тощо).

Отже, наявні моделі лише частково враховують аспекти цифрової безпеки, а тому потребують доповнення. Такими доповненнями можуть стати цільові тренінги з кіберзахисних стратегій; практикуми з моделювання небезпечних ситуацій; методики адаптування контенту з безпеки або системою моніторингу актуальних кіберзагроз для освіти [126; 136] або інші. При цьому, як наголошують науковці [189, 140], для реалізації інформаційного підходу варто використовувати алгоритми оцінки інформаційних ризиків, технології аналізу цифрового сліду, методи проектування безпечних освітніх середовищ, механізми оперативного оновлення знань про кіберзагрози .

Нами розроблено модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу (рис.2.2).

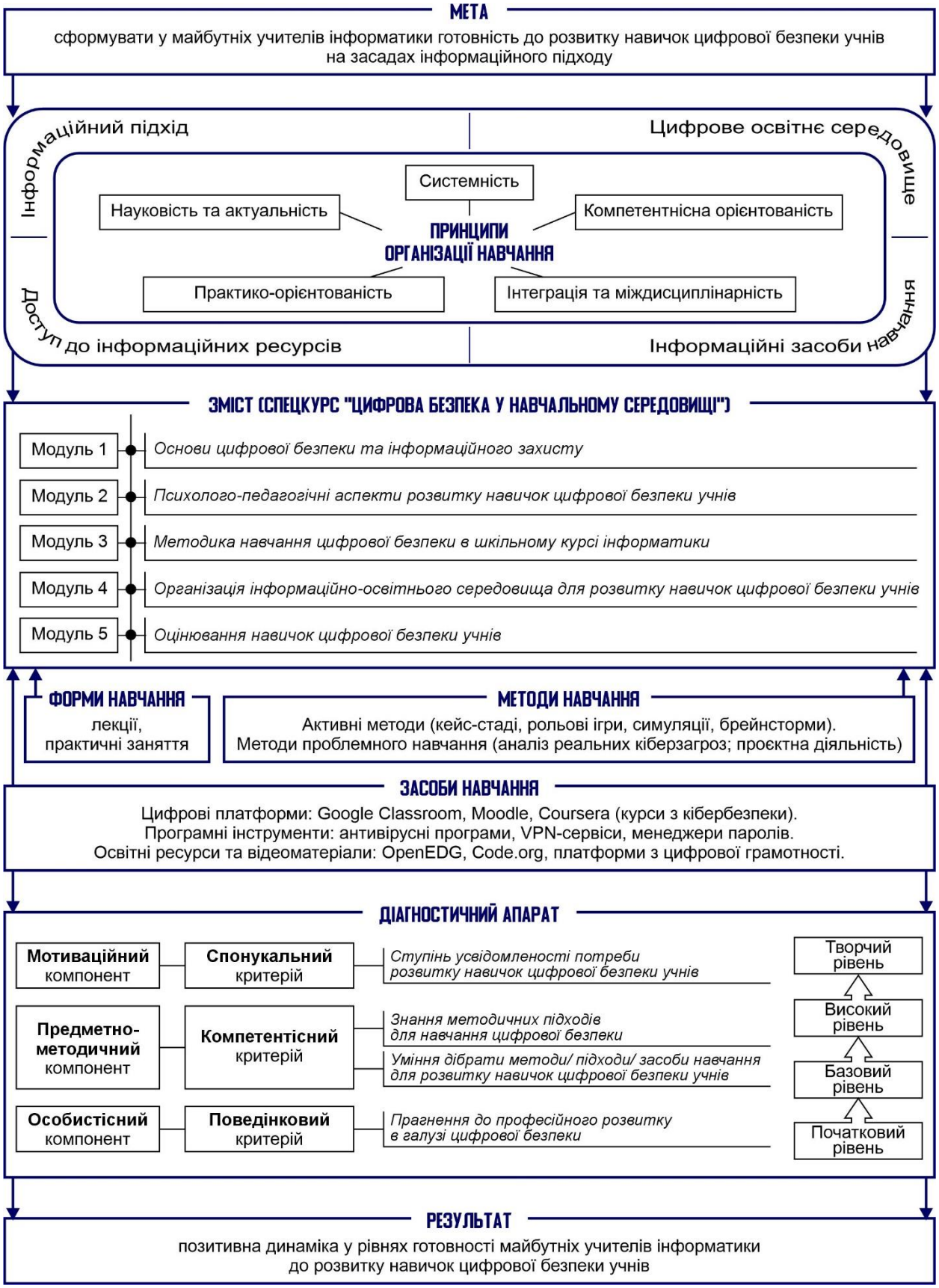


Рис.2.2. Модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу

Модель орієнтована на досягнення результату: сформувати у майбутніх учителів інформатики готовність до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу. Успіх досягнення результату буде визначатися позитивною динамікою рівнів такої готовності після впровадження авторської стратегії.

Авторська стратегія формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу передбачає наслідування таких принципів підготовки вчителів інформатики до розвитку навичок цифрової безпеки учнів (рис.2.3).

Рис. 2.3. Принципи підготовки вчителів інформатики до розвитку навичок цифрової безпеки учнів

Обґрунтуємо важливість дотримання наведених принципів.

Науковість та актуальність. Цифрова безпека є динамічною сферою, в якій постійно з'являються нові загрози (фішинг, соціальна інженерія, кібератаки). Тому професійна підготовка вчителів інформатики має ґрунтуватися на актуальних наукових дослідженнях, міжнародних стандартах безпеки (GDPR, ISO/IEC 27001), а також рекомендаціях профільних організацій (наприклад, Європейського агентства з кібербезпеки – ENISA). Це гарантує, що майбутні вчителі отримають актуальні й релевантні знання, які зможуть ефективно передавати учням.

Системність. Цифрова безпека включає не тільки технічні аспекти (антивіруси, шифрування), а й соціальні та правові компоненти (етика в Інтернеті, захист персональних даних). Для ефективної підготовки вчителів необхідно забезпечити широке охоплення теми цифрової безпеки та формування в учнів навичок цифрової безпеки, що передбачає інтеграцію знань з інформатики, психології, права та педагогіки. Лише така комплексна підготовка дозволить майбутнім учителям інформатики розвивати в учнів навички безпечної поведінки в цифровому середовищі.

Компетентнісна орієнтація. Знання самі по собі не гарантують цифрової безпеки, якщо вони не трансформуються у реальні вміння. Тому підготовка вчителів має бути спрямована на формування знань та вмінь щодо аналізу загроз та ризиків у цифровому середовищі; практичного застосування цифрових інструментів для захисту даних; технологій розвитку учнів безпечній поведінці онлайн тощо. Такий підхід відповідає сучасним освітнім стандартам, орієнтованим на формування здатності діяти, а не просто знати.

Практико-орієнтованість. Оскільки цифрова безпека має реалізуватися на практиці, навчання має включати реальні кейси та практичні завдання. Наприклад, майбутні вчителі інформатики повинні навчитися налаштовувати безпечне цифрове середовище, вміти безпечно використовувати цифрові пристрої, розпізнавати фішингові атаки, пояснювати учням ризики використання соціальних мереж. Практико-орієнтоване навчання забезпечить

ефективне засвоєння матеріалу та його подальше застосування в освітньому процесі.

Інтеграція та міждисциплінарність. Цифрова безпека стосується не лише ІТ-галузі. Наприклад, ефективне навчання інформатики учнів вимагатиме від майбутніх учителів знання вікової психології (наприклад, як діти реагують на кібербулінг), правових аспектів (що таке захист персональних даних) та педагогічних підходів (як мотивувати школярів дотримуватися безпечної поведінки онлайн). Тому модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів має передбачати реалізацію міждисциплінарних зв'язків (міждисциплінарність).

Дотримання зазначених принципів забезпечить ефективну підготовку вчителів, які зможуть не лише володіти знаннями про цифрову безпеку, а й навчати учнів правильній поведінці в онлайн-просторі, використовуючи сучасні методи та інструменти.

Наукові джерела містять обмежені конкретні вказівки щодо форм, методів і засобів навчання, які безпосередньо сприяють розвитку навичок цифрової безпеки вчителів. Однак у кількох роботах обговорюються суміжні педагогічні підходи та технологічні інструменти, які можуть бути адаптовані для підготовки в галузі цифрової безпеки і про які ми зазначили раніше (у п.1.3). З урахуванням здобутків інших науковців, вважаємо доцільним вибір традиційних для вищої школи форм навчання - лекції, практичні заняття. Водночас серед методів виділяємо:

– *активні методи* – кейс-стаді, рольові ігри, симуляції, брейнсторми;

– *методи проблемного навчання* – аналіз реальних кіберзагроз, проєктна діяльність.

Серед засобів навчання обираємо:

– *цифрові платформи*: Google Classroom, Moodle, Coursera (курси з кібербезпеки);

– *програмні інструменти*: антивірусні програми, VPN-сервіси, менеджери паролів;

– *освітні ресурси та відеоматеріали*: OpenEDG, Code.org, платформи з цифрової грамотності.

Цифрові інструменти та технології, такі як віртуальні лабораторії, симуляції та онлайн-платформи, також можуть відігравати значну роль у формуванні готовності вчителів до розвитку навичок цифрової безпеки учнів. Ці інструменти можуть забезпечити досвід навчання, який потім можна буде упроваджувати у майбутню професійну діяльність [130]. Наприклад, віртуальні лабораторії можуть моделювати реальні кібератаки і надавати вчителям практичний досвід аналізу вразливостей цифрових систем та впровадження заходів безпеки. Використання ігрових технологій та інтерактивних симуляцій може підвищити мотивацію до навчання.

Описані методи і засоби навчання використовуються в межах розробленого нами спецкурсу «Цифрова безпека у навчальному середовищі», який опишемо більш детально.

Спецкурс спрямований на формування у майбутніх учителів інформатики навичок цифрової безпеки учнів. Курс розрахований на 4 кредити (120 годин) і містить 5 модулів.

Модуль 1. Основи цифрової безпеки та інформаційного захисту

Мета: ознайомити майбутніх учителів ынформатики із ключовими поняттями цифрової безпеки, сучасними загрозами та методами їхнього запобігання.

Основні теми. Основні поняття цифрової безпеки: персональні дані, цифровий слід, кіберзагрози. Види кіберзагроз: фішинг, шкідливе програмне забезпечення, соціальна інженерія, витік даних. Правові аспекти цифрової безпеки: міжнародні та національні нормативно-правові акти (Закон України "Про захист персональних даних"). Інструменти захисту інформації: антивіруси, брандмауери, VPN, двофакторна аутентифікація. Цифрова безпека

дітей та підлітків: безпечна поведінка в соцмережах, протидія кібербулінгу, приватність даних.

Типові практичні завдання Модуля 1. Аналіз реальних випадків кібератак, використання онлайн-сервісів для перевірки паролів, налаштування параметрів конфіденційності в соцмережах.

Модуль 2. Психолого-педагогічні аспекти формування цифрової безпеки учнів

Мета: надати майбутнім учителям інформатики знання щодо вікових особливостей сприйняття інформації про цифрову безпеку та методів її формування.

Основні теми. Вплив цифрового середовища на психіку дитини: кіберстрес, інформаційне перевантаження, цифрова залежність. Вікові особливості сприйняття загроз у цифровому середовищі: як діти різного віку реагують на небезпеку. Методи розвитку критичного мислення та цифрової грамотності: рольові ігри, моделювання ситуацій, дискусії. Етика та відповідальність в Інтернеті: поняття цифрового етикету, правові наслідки онлайн-документування (фото, відео). Роль вчителя у формуванні культури безпеки в Інтернеті: як стати наставником у сфері цифрової безпеки для учнів і батьків.

Типові практичні завдання Модуля 2. Розробка навчальних кейсів для учнів різних вікових груп, аналіз реальних випадків небезпечної поведінки в Інтернеті, підготовка тренінгового заняття для батьків про цифрову безпеку.

Модуль 3. Методика викладання цифрової безпеки в шкільному курсі інформатики

Мета: навчити майбутніх учителів ефективних методів і технологій розвитку навичок цифрової безпеки учнів у школі.

Основні теми. Місце цифрової безпеки у шкільному курсі інформатики: інтеграція тем у навчальну програму. Методи викладання цифрової безпеки: проблемне навчання, проєктний підхід, гейміфікація. Розробка навчальних матеріалів з цифрової безпеки: створення інструкцій, відеоуроків,

інтерактивних презентацій. Використання EdTech-інструментів у навчанні цифрової безпеки: платформи Google Classroom, Kahoot, PhishMe, CyberSmart. Оцінювання рівня сформованості навичок цифрової безпеки учнів: тести, практичні кейси, аналіз поведінки в Інтернеті.

Типові практичні завдання Модуля 3. Розробка навчального заняття з цифрової безпеки з використанням інтерактивних методів, проведення міні-уроку, оцінювання рівня знань учнів за допомогою тестів та кейсів.

Модуль 4. Організація інформаційно-освітнього середовища для розвитку навичок цифрової безпеки.

Мета: надати майбутнім учителям інформатики практичні інструменти для створення безпечного та ефективного освітнього середовища та сформувати вміння їх використовувати.

Основні теми. Розробка політики цифрової безпеки в закладі освіти: правила використання гаджетів, паролі та доступи. Організація безпечного освітнього простору в Інтернеті: налаштування корпоративних акаунтів, Google Workspace для навчання. Створення навчальних матеріалів із цифрової безпеки: інтерактивні веб-квести, відеоуроки, чек-листи. Співпраця з батьками у питаннях цифрової безпеки дітей: проведення просвітницьких заходів. Інтерактивні форми роботи з учнями та батьками: тренінги, ігри, симуляційні вправи.

Типові практичні завдання Модуля 4. Створення навчального відео про правила безпечного користування Інтернетом, моделювання ситуацій із кібербезпеки, розробка політики цифрової безпеки для школи.

Модуль 5. Оцінювання навичок цифрової безпеки учнів

Мета: сформувати вміння оцінювати навички цифрової безпеки.

Основні теми. Тренінгові методи навчання: як ефективно навчати учнів через практичні вправи та оцінювати їх вплив. Моделювання уроків із цифрової безпеки: планування та проведення уроків у тестовому форматі, організація перевірки знань та вмінь. Коучинг та менторство у сфері цифрової безпеки: як допомагати колегам і батькам розбиратися в питаннях

кібербезпеки. Застосування отриманих знань у реальних шкільних умовах: адаптація навчальних матеріалів під конкретні освітні програми. Рефлексія та самооцінка викладання цифрової безпеки: аналіз проведених занять, визначення точок росту.

Типові практичні завдання Модуля 5. Розроблення тестових завдань, практичних задач, кейсів для перевірки сформованості навичок цифрової безпеки, проведення демонстраційних уроків, розробка авторських тренінгів, участь у дискусіях щодо проблем оцінювання навичок цифрової безпеки.

Кожен модуль передбачає одне лекційне заняття та три практичних заняття на поглиблення теоретичних знань та набуття досвіду їх застосування на практиці. Надалі опишемо практичні завдання для кожного модуля.

Модуль 1. Основи цифрової безпеки та інформаційного захисту

Практичні завдання та коментарі-обґрунтування до них

1. Аналіз кіберзагроз та їх наслідків.

Завдання: Ознайомитися з реальними випадками кібератак (наприклад, витік даних у великих компаніях) та підготувати короткий аналіз ситуації, її причин та наслідків.

Коментар: Важливо, щоб майбутні вчителі інформатики навчилися розбирати реальні кейси та пояснювали учням потенційні загрози через конкретні приклади.

2. Перевірка власної цифрової безпеки

Завдання: Використати сервіси типу Have I Been Pwned для перевірки, чи не потрапили їхні облікові дані у витоки. Проаналізувати налаштування конфіденційності власних акаунтів у соцмережах.

Коментар: Майбутній вчитель інформатики має не лише знати правила безпеки, а й показувати власний приклад безпечної поведінки в Інтернеті.

3. Налаштування безпечного робочого середовища

Завдання: Налаштувати двофакторну аутентифікацію на своїх акаунтах, створити складний пароль за правилами безпеки та використати менеджер паролів.

Коментар: Майбутній учитель інформатики повинен не лише сам знати ці правила, а й навчати цьому учнів.

4. Інтерактивний тест із цифрової безпеки

Завдання: Пройти один із відкритих онлайн-тестів на знання правил цифрової безпеки (наприклад, Google Safety Center) та проаналізувати власні результати.

Коментар: Завдання допоможе майбутнім учителям краще розуміти власний рівень знань і визначити, які питання слід допрацювати.

5. Розробка інструкції з цифрової безпеки для учнів

Завдання: Створити короткий гайд (рекомендації) для школярів із основними правилами безпечної поведінки в Інтернеті.

Коментар: Рекомендації мають бути зрозумілими, доступними та оформленими у привабливій для дітей формі (інфографіка, відео тощо).

Аналогічні завдання і контрольні запитання до курсу зосереджені у Додатку А, а залікові тести – у додатку Б.

Ми вважаємо доцільною реалізацію цього спецкурсу на третьому році навчання, коли майбутні учителі інформатики вже опанували майже всі професійно орієнтовані дисципліни, але перед педагогічною практикою з метою вчасної підготовки студентів до роботи з учнями.

За результатами спецкурсу мають бути сформовані всі компоненти готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів: усвідомлені прагнення такого розвитку; специфічні знання й уміння; навички рефлексії щодо успішності такого розвитку.

Курс побудовано за принципами: науковості та актуальності, оскільки його зміст орієнтується на сучасні наукові дослідження і досягнення у сфері цифрової безпеки; системності, оскільки підготовка здобувачів освіти охоплює різні аспекти цифрової безпеки (технічний, правовий, етичний, психолого-педагогічний); інтеграції та міждисциплінарності, оскільки у спецкурсі передбачено поєднання знань з інформатики, права, психології, педагогіки.

Викладання курсу має підпорядковуватися принципам організації навчання: компетентнісної орієнтованості, коли формування конкретних навичок цифрової безпеки відбувається разом із передаванням теоретичних знань, та практико-орієнтованості, коли для формування знань і вмінь в галузі цифрової безпеки використовуються реальні кейси, симуляції цифрових загроз, інтерактивні методи навчання.

Процес формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів за розробленою моделлю відбувається на засадах інформаційного підходу, оскільки створюється освітнє середовище підготовки майбутніх учителів інформатики, яке передбачає не лише доступ до дидактичних матеріалів курсу (лекції, презентації, популярні відео, практичні заняття, інформаційні джерела тощо), а й обов’язкове використання інших інформаційних джерел та засобів, включаючи цифрові освітні платформи та спеціалізовані програмні засоби/ сервіси.

Бачимо доречним аналізувати реальні кейси, які пов’язані з соцмережами, смс та е-поштою, а також художні фільми, які торкаються проблем соціальної інженерії, кібербулінгу тощо.

Ми рекомендували студентам ознайомитися з різними художніми фільмами про кібербулінг або соціальну інженерію тощо, а потім пропонували розбити їх на групи за віковими характеристиками. Студенти склали такий перелік.

1. Для учнів 10–13 років (молодший підлітковий вік)

Фільм "Cyberbully" (2011, США, Канада): Дівчина стає жертвою онлайн-знущань після реєстрації в соціальній мережі. Фільм показує, як кібербулінг впливає на психіку підлітків та як з цим боротися.

Фільм "Trust" (2010, США). 14-річна дівчина знайомиться в інтернеті з хлопцем, який виявляється зовсім не тим, ким здавався. Фільм розкриває проблему довіри в мережі та маніпуляцій.

Фільм "Disconnect" (2012, США). Кілька сюжетних ліній про різні аспекти інтернет-небезпеки: кібербулінг, крадіжку особистих даних та маніпуляції в мережі.

2. Для учнів 14–16 років (старший підлітковий вік)

Фільм "The Duff" (2015, США). Дівчина дізнається, що в школі її вважають "непривабливою подругою" (DUFF). Соцмережі відіграють ключову роль у приниженні та самооцінці.

Фільм "Unfriended" (2014, США). Група підлітків стає жертвою кіберпомсти після того, як їхня подруга вчинила самогубство через онлайн-знущання.

Фільм "The Social Dilemma" (2020, США, документальний-драматичний). Фільм досліджує, як соціальні мережі маніпулюють нашою увагою, сприяють булінгу та соціальному тиску.

3. Для учнів 17+ років (старшокласники, студенти)

Фільм "Nerve" (2016, США). Студентка потрапляє в небезпечну гру в інтернеті, де виклики стають дедалі ризикованішими. Порушує питання впливу анонімного інтернет-середовища на поведінку.

Фільм "Searching" (2018, США). Батько розшукує зниклу доньку через її сліди в соцмережах, стикаючись із небезпечними аспектами онлайн-життя.

Фільм "Hated in the Nation" (2016, Великобританія, серіал 'Black Mirror', S03E06). У майбутньому онлайн-ненависть має фатальні наслідки. Фільм аналізує вплив соціальних мереж на людську моральність.

Перелічені та інші фільми є основою для дискусій в аудиторії на заняття. Ми вважаємо, що вони можуть сприяти усвідомленню ризиків цифрового світу.

Для перевірки ефективності розробленої моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу розроблено діагностичний апарат, який включає критерії і показники готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.

Отже, нами розроблено модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу, яка передбачає дотримання принципів (науковість та актуальність, системність, компетентісна орієнтованість, практико-орієнтованість, інтеграція та міждисциплінарність) при організації навчання спецкурсу «Цифрова безпека у навчальному середовищі» у традиційній формі (лекції, практичні заняття) з використанням активних і проблемних методів навчання та різних цифрових засобів навчання (цифрові навчальні середовища, цифрові освітні ресурси та програми спеціалізованого спрямування). Запропонована модель дозволить сформувати в майбутніх учителів інформатики не лише знання про цифрову безпеку, а й методичні уміння для ефективного розвитку в учнів навичок цифрової безпеки.

Висновки до розділу 2

У другому розділі «Теоретичне моделювання процесу формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу» уточнено сутність і структуру готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів, а також розроблено й теоретично обґрунтовано модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

За результатами понятєвого аналізу ключових понять дослідження («готовність», «готовність до професійної діяльності», «готовність учителя») було уточнено сутність ключової категорії дослідження: готовність учителів інформатики до розвитку навичок цифрової безпеки учнів - це інтегративна особистісна здатність майбутнього вчителя інформатики розвивати навички цифрової безпеки учнів, яка поєднує: усвідомлені прагнення такого розвитку; специфічні знання й уміння; навички рефлексії щодо успішності такого розвитку. Виявлена сутність обумовила розгляд поняття «готовність учителів

інформатики до розвитку навичок цифрової безпеки учнів» як складного особистісного утворення, яке поєднує в собі три компоненти:

- мотиваційний компонент (прагнення розвитку навичок цифрової безпеки учнів) характеризує усвідомлення студентами потреби розвитку навичок цифрової безпеки учнів і є фундаментом їхньої мотивації діяти в цьому напрямку. Це усвідомлення впливає на їхню професійну діяльність, сприяє особистісному розвитку та забезпечує безпечне освітнє середовище;
- предметно-методичний компонент (специфічні знання й уміння) поєднує в собі предметні знання про цифрову безпеку і методичні знання щодо стратегій розвитку навичок цифрової безпеки учнів. Він характеризується сукупністю предметних знань, знань методичних підходів для розвитку навичок цифрової безпеки та психолого-педагогічних знань та умінь дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки учнів;
- особистісний компонент (навички рефлексії щодо успішності розвитку навичок цифрової безпеки учнів) є важливою складовою готовності і охоплює рефлексивну діяльність, яка дозволяє аналізувати власний рівень цифрової безпеки, вдосконалювати методики навчання, формувати критичне мислення у школярів та усвідомлювати етичні аспекти цифрової взаємодії.

На основі узагальнення наукових результатів було обґрунтовано необхідність використання інформаційного підходу як провідного у формуванні готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів, оскільки саме інформаційний підхід дозволяє майбутнім учителям опанувати принципи безпечної взаємодії в цифровому середовищі, розвинути навички критичного аналізу інформації, захисту персональних даних та етичного використання цифрових ресурсів. Застосування цього підходу в підготовці вчителів інформатики уможливлює формування в них здатності передбачати потенційні ризики цифрового середовища, аналізувати інформаційні загрози та адаптувати освітній процес відповідно до змін у сфері кібербезпеки. Активна взаємодія з цифровими

платформами, інструментами управління інформацією та засобами захисту даних дозволяє майбутнім педагогам не тільки опанувати цифрову безпеку особисто, а й ефективно передавати ці знання учням. Інформаційний підхід забезпечує системне розуміння того, як інформація циркулює в цифровому середовищі, які механізми впливають на її безпеку та як навчити учнів захищати себе від можливих загроз.

З використанням методу моделювання нами було представлено модель процесу формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу. Авторська модель базується на дотриманні принципів (науковість та актуальність, системність, компетентісна орієнтованість, практико-орієнтованість, інтеграція та міждисциплінарність) при організації навчання спецкурсу «Цифрова безпека у навчальному середовищі» у традиційній формі (лекції, практичні заняття) з використанням активних і проблемних методів навчання та різних цифрових засобів навчання (цифрові навчальні середовища, цифрові освітні ресурси та програми спеціалізованого спрямування).

Отже, в другому розділі подано вирішення 3-го і 4-го завдань дослідження. Основні результати представлені у публікаціях [3], [4] (згідно з додатком Є).

РОЗДІЛ 3.
ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ЕФЕКТИВНОСТІ МОДЕЛІ ФОРМУВАННЯ ГОТОВНОСТІ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ ДО РОЗВИТКУ НАВИЧОК ЦИФРОВОЇ БЕЗПЕКИ УЧНІВ НА ЗАСАДАХ ІНФОРМАЦІЙНОГО ПІДХОДУ

3.1. Опис діагностичного інструментарію дослідження

Діагностичний апарат у наукових освітніх дослідженнях передбачає використання критеріїв та показників для об’єктивної оцінки явищ. У контексті освітньої діагностики критерій – це чітко визначений стандарт або правило, щодо якого оцінюється рівень досягнення освітніх цілей. Наприклад, у тестуванні критерій визначає предметну область знань, а не лише прохідний бал [106]. Як зазначає Education Glossary, критерій-орієнтовані тести "вимірюють успішність студентів щодо фіксованого набору визначених стандартів" [там само].

Показник – це конкретна статистична величина або індикатор, який відображає стан певного аспекту освітньої системи. На відміну від критерію, показник слугує "вимірювальним приладом" для аналізу ефективності освітнього процесу. Наприклад, показником може бути "відсоток учнів, які завершили курс математики" [46]. Як підкреслюється у дослідженні [135], освітні показники мають бути частиною системи, що охоплює "входи, процеси та результати навчання" [112].

За аналізом джерел [21; 109] можна прослідкувати зв’язок між критерієм і показником в освітніх дослідженнях (табл.3.1).

Таблиця 3.1

Приклад зв'язку критерію та показника

Критерій	Показник	Джерело
Засвоєння базових навичок математики	Відсоток учнів з результатом тесту ≥80%	[21]
Ефективність цифрових навчальних середовищ	Кількість активних користувачів платформи	[109]

У нашому дослідженні ми маємо оцінити (діагностувати) готовність майбутніх учителів інформатики до розвитку в учнів навичок цифрової безпеки. Саме поняття готовність розглядається нами як інтегративна єдність трьох компонентів – мотиваційного, предметно-методичного та особистісного. Тому вважаємо коректним розробити три критерії – по одному на кожен компонент готовності. Такими критеріями будуть: спонукальний, компетентісний та поведінковий (рис. 3.1).

Рис.3.1. Критерії сформованості компонентів готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів

Ці критерії забезпечують комплексну оцінку готовності майбутнього вчителя інформатики розвивати навички цифрової безпеки учнів.

Надалі обґрунтуємо свій вибір.

Спонукальний критерій (мотиваційний компонент)

Спонукальний критерій акцентує увагу на внутрішньому бажанні майбутнього вчителя інформатики займатися діяльністю, пов'язаною з розвитком навичок цифрової безпеки в учнів. Це включає їхнє розуміння важливості цифрової безпеки, ентузіазм щодо навчання цим навичкам і зобов'язання бути в курсі останніх загроз і найкращих практик. Учитель з високим рівнем мотивації з більшою ймовірністю інвестуватиме час і зусилля у створення цікавого та ефективного навчального досвіду для учнів.

Учитель повинен визнати критичну потребу в тому, щоб учні добре розбиралися в питаннях цифрової безпеки. Це усвідомлення випливає з розуміння потенційних ризиків, з якими учні стикаються в Інтернеті, таких як кібер-залякування, фішингові атаки, шкідливе програмне забезпечення та порушення конфіденційності. Вчителі також повинні розуміти ширші соціальні наслідки цифрової безпеки, включаючи захист персональних даних, інтелектуальної власності та національну безпеку.

Мотивований учитель демонструє справжній ентузіазм щодо викладання навичок цифрової безпеки. Цей ентузіазм перетворюється на більш цікаві уроки, що може значно покращити результати навчання учнів. Пристрасть вчителя може надихнути учнів серйозно ставитися до цифрової безпеки та застосовувати безпечну поведінку в Інтернеті.

Цифровий ландшафт постійно розвивається, регулярно з'являються нові загрози та вразливості. Мотивований учитель демонструє прихильність до постійного навчання, залишаючись в курсі останніх тенденцій, інструментів і методів цифрової безпеки. Це включає участь у заходах з професійного розвитку, читання галузевих публікацій та взаємодію з онлайн-спільнотами експертів з цифрової безпеки.

Методами оцінювання спонукального критерію можуть бути такі емпіричні методи:

- Анкети для самооцінки - вчителі можуть заповнювати анкети, які оцінюють їхнє ставлення, переконання та цінності, пов’язані з цифровою безпекою. Ці анкети можуть включати запитання про їхню сприйняття важливості цифрової безпеки, їхню впевненість у навчанні цим навичкам і готовність інвестувати час у професійний розвиток;
- Інтерв’ю - структуровані інтерв’ю можуть дати більш глибоке розуміння мотиваційних факторів роботи вчителя. За допомогою запитань на співбесіді можна дослідити досвід формування навичок цифрової безпеки, якщо такий був, боротьби з інцидентами цифрової безпеки, дізнатися їхні погляди на роль школи і уроків інформатики у сприянні цифровій безпеці, а також їхні особисті стратегії для розвитку навичок цифрової безпеки учнів;
- Спостереження – може надати більш детальну інформацію про залученість та ентузіазм вчителя щодо розвитку навичок цифрової безпеки учнів у класі через фіксацію пов’язаних із темою запитань, обмін думками та демонстрацію щирого інтересу до теми.

Виходячи з викладеного, показниками спонукального критерію можуть бути: (а) усвідомленість потреби формування навичок цифрової безпеки (коли оцінка сформованості мотиваційного компонента готовності відбувається через анкети, опитування або інтерв’ю, які виявляють рівень розуміння вчителем важливості навичок цифрової безпеки для учнів); (б) інтерес до теми цифрової безпеки (коли оцінка відбувається на основі самозвітів, аналізу вибору тем для учнівських досліджень або участі в тренінгах/конференціях на тему цифрової безпеки); (в) ініціативність у впровадженні нових практик цифрової безпеки (коли оцінка відбувається через спостереження за участю вчителя у впровадженні нових стратегій розвитку навичок цифрової безпеки учнів). Водночас з огляду на побудову і реалізацію власного дослідження, обираємо показником лише *П1-ступінь усвідомлення потреби розвитку*

навичок цифрової безпеки учнів, оскільки саме цей показник ми можемо реально виміряти на практиці.

Компетентісний критерій (предметно-методичний компонент готовності)

Компетентісний критерій охоплює сформованість знань та навичок майбутнього вчителя в галузі цифрової безпеки, а також його здатність переводити ці знання в їх практичне застосування на заняттях. Це включає як розуміння ключових концепцій цифрової безпеки, так і вміння використовувати відповідні інструменти та технології, а також здатність розробляти та проводити ефективні уроки, які сприяють розвитку в учнів навичок цифрової безпеки.

Компетентісний критерій має увиразнювати сформованість у майбутнього вчителя:

- знань концепцій цифрової безпеки, а саме: розуміння різних типів цифрових загроз, таких як зловмисне програмне забезпечення, фішинг, програми-вимагачі та соціальна інженерія: знання принципів захисту даних, правил конфіденційності та найкращих практик захисту особистої інформації; розуміння мережевих протоколів, брандмауерів, систем виявлення вторгнень та інших заходів безпеки; знання різних методів аутентифікації, механізмів контролю доступу та методів управління ідентифікацією; розуміння алгоритмів шифрування, цифрових підписів та інших криптографічних інструментів;
- навичок використання інструментів та технологій цифрової безпеки, а саме: встановлення, налаштування та використання антивірусного програмного забезпечення для виявлення та видалення шкідливого програмного забезпечення; налаштування брандмауерів для захисту мереж і систем від несанкціонованого доступу; використання менеджерів паролів для створення та зберігання надійних паролів; використання інструментів шифрування для захисту конфіденційних даних; використання інструментів аудиту безпеки для виявлення вразливостей у системах та мережах;

- методичних умінь розробляти та проводити ефективні уроки, які сприяють розвитку в учнів навичок цифрової безпеки, а саме: розробка відповідних віку актуальних дидактичних матеріалів, які охоплюють ключові теми цифрової безпеки; використання різноманітних доцільних форм, методів і засобів навчання учнів; використання різноманітних методів оцінювання, таких як вікторини, тести, проекти та презентації; диференційована адаптація навчального матеріалу для задоволення різноманітних освітніх потреб учнів.

Методами оцінювання сформованості предметно-методичного компоненту готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів можуть бути:

- тести на перевірку знань - студенти можуть пройти тести, які оцінюють їхнє розуміння концепцій цифрової безпеки і які можуть включати запитання з різною формою відповіді;
- демонстрація навичок - студенти можуть продемонструвати свої навички використання цифрових інструментів та технологій цифрової безпеки при виконання практичних завдань (наприклад, налаштувати брандмауер, встановити антивірусне програмне забезпечення або зашифрувати файл);
- оцінювання планів уроків – студенти можуть розробити плани уроків, які будуть оцінені на основі їх відповідності стандартам цифрової безпеки, використання ефективних навчальних методик та включення відповідних методів оцінювання;
- спостереження – метод, який дозволяє спостерігати і оцінити роботу вчителя в контексті їхньої здатності проводити ефективні уроки для розвитку навичок цифрової безпеки учнів.

З урахуванням наведених аргументів можливими показниками для вимірювання сформованості предметно-методичного компонента готовності за компетентісним критерієм можуть бути: (а) знання методів та стратегій формування навичок цифрової безпеки, яка оцінюється через письмові тести або практичні завдання, що перевіряють знання методів розвитку навичок цифрової безпеки; (б) здатність вибирати відповідні методи навчання, коли

відбувається оцінка планів учителя, спостереження за його професійною діяльністю і вибором форм, методів і засобів навчання учнів; (с) ступінь застосування інтерактивних і практичних методів, яке можна оцінити через спостереження за уроками, де вчитель використовує інтерактивні методи або ситуаційні вправи для формування навичок цифрової безпеки учнів; вміння адаптувати методи навчання для різних вікових груп учнів, коли оцінка здійснюється через аналіз уроків та зворотний зв'язок від учнів щодо того, наскільки ефективно застосовані методи для розвитку навичок цифрової безпеки. Водночас з огляду на побудову і реалізацію власного дослідження, обираємо показниками *П2-знання методичних підходів для розвитку навичок цифрової безпеки* та *П3- уміння добирати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки учнів,* оскільки саме ці показники ми можемо реально виміряти на практиці.

Поведінковий критерій (особистісний компонент)

Поведінковий критерій зосереджується на реальних практиках та поведінці вчителя, пов'язаних із цифровою безпекою в класі та за його межами. Це включає не лише впровадження ними заходів безпеки, моделювання безпечної поведінки в Інтернеті та забезпечення дотримання політик цифрової безпеки. Учитель із сильними поведінковими практиками має потребу створити безпечне та надійне освітнє середовище для учнів та пропагує культуру цифрової відповідальності, тому наслідує практики постійного саморозвитку.

Поведінковий критерій ураховує прихильність майбутнього вчителя інформатики до безперервного навчання. Оскільки технології постійно розвиваються, регулярно з'являються нові загрози та вразливості. Особистісно умотивований вчитель буде демонструвати прихильність до безперервного навчання, залишаючись в курсі останніх тенденцій, інструментів та методів цифрової безпеки. Це включає бажання вчитися та участь у заходах з професійного розвитку, читання галузевих публікацій та взаємодію з онлайн-спільнотами експертів з цифрової безпеки.

Поведінковий критерій увиразнює не лише уміння майбутнього вчителя інформатики активно впроваджувати заходи безпеки для захисту учнів та шкільних ресурсів від цифрових загроз, що включає: забезпечення дотримання політики надійних паролів та навчання студентів важливості безпеки паролів; забезпечення того, щоб усе програмне забезпечення та операційні системи були оновлені з останніми виправленнями безпеки; впровадження заходів мережевої безпеки, таких як брандмауери та системи виявлення вторгнень, для захисту шкільної мережі від несанкціонованого доступу; впровадження процедур резервного копіювання та відновлення даних для захисту від втрати даних; моделювання безпечної поведінки в Інтернеті, що включає демонстрацію того, як захистити особисту інформацію та уникнути обміну конфіденційними даними з ненадійними джерелами; розпізнавання та уникнення фішингових атак та інших шахрайств із соціальною інженерією; відповідальне використання платформ соціальних мереж та уникнення публікації неприйнятного контенту; повага до законів про авторське право та уникнення незаконного завантаження або обміну матеріалами, захищеними авторським правом.

Поведінковий критерій охоплює застосування політик цифрової безпеки, коли вчитель підтримує безпечне та надійне навчальне середовище. Це включає: впровадження політик щодо запобігання кібербулінгу та реагування на випадки переслідування в Інтернеті; забезпечення дотримання політик прийнятного використання, які визначають належну поведінку учнів в Інтернеті; ефективне реагування на інциденти цифрової безпеки, такі як зараження шкідливим програмним забезпеченням або витік даних.

До методів оцінювання готовності за поведінковим критерієм відносимо такі емпіричні методи:

- Спостереження - за вчителями в класі та шкільному середовищі може надати характерну інформацію про їхні поведінкові практики з упровадження заходів безпеки, моделювання безпечної поведінки в Інтернеті та застосування політики цифрової безпеки;

- інтерв’ю - з вчителями, учнями та шкільною адміністрацією може дати уявлення про поведінкові практики вчителя інформатики, якщо ставити запитання про їхній досвід з цифрової безпеки, стратегій сприяння безпечній поведінці в Інтернеті та дотримання політик цифрової безпеки;
- аналіз документів - перегляд шкільної політики, звітів про інциденти та інших відповідних документів може надати докази поведінкових практик учителя.

З урахуванням вищенаведеного, вважаємо, що показниками готовності до розвитку навичок цифрової безпеки учнів за поведінковим критерієм можуть бути: (а) особиста зацікавленість у постійному вдосконаленні в галузі цифрової безпеки, коли відбувається оцінка через самозвіт, участь у тренінгах і сертифікаційних курсах з цифрової безпеки; (б) ступінь самооцінки вчителя в контексті власних знань і навичок у галузі цифрової безпеки, коли оцінка відбувається через анкети або інтерв’ю, де вчитель оцінює свій рівень знань і досвіду в сфері цифрової безпеки; ініціативність у підвищенні власної кваліфікації, коли ведуться спостереження за участю вчителя в профільних заходах (семінари, конференції, онлайн-курси); (в) прагнення до професійного розвитку в галузі кібербезпеки, яке проявляється у прихильності майбутнього вчителя інформатики до безперервного навчання, бажання бути ознайомленим з актуальними методами цифрової безпеки та трендами можливих цифрових небезпек; (г) спроможність до змін та адаптації до нових технологій, які оцінюються через спостереження за здатністю вчителя інтегрувати нові технології та інструменти для цифрової безпеки в освітній процес. Водночас з огляду на побудову і реалізацію власного дослідження, обираємо показником *П4- прагнення до професійного розвитку в галузі кібербезпеки*, оскільки саме цей показник ми можемо реально виміряти на практиці.

Оскільки готовність майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів розглядається нами як єдність трьох компонентів, то щоб діагностувати її сформованість, важливо відслідковувати результати за цими трьома критеріями: мотиваційним, компетентісним та

поведінковим. Тому перевірка ефективності розробленої моделі формування готовності учителів інформатики до розвитку навичок цифрової безпеки учнів буде відбуватися за всіма показниками П1-П4 одночасно.

Надалі обґрунтовані нами критерії та показники готовності учителів інформатики до розвитку навичок цифрової безпеки учнів дають можливість охарактеризувати чотири рівні такої готовності: початковий, базовий, високий і творчий.

Початковий рівень готовності учителів інформатики до розвитку навичок цифрової безпеки учнів характеризується низьким рівнем усвідомлення важливості цієї теми, обмеженими методичними знаннями та недостатнім прагненням до професійного розвитку.

Студент має загальне уявлення про цифрову безпеку, але не усвідомлює глибини її важливості для учнів. Він може визнавати загрозу цифрової безпеки, але не пов’язують її з необхідністю навчати учнів захищати свої особисті дані чи розуміти основи цифрової етики. Студент може сказати, що "цифрова безпека важлива, але я не знаю, як вчити дітей безпечному використанню технологій". Це свідчить про побіжне сприйняття значущості питання для учнів. Усвідомлення потреби в цифровій безпеці є, але немає глибокого розуміння необхідності розвитку навичок цифрової безпеки учнів у цифровому середовищі.

Студент знайомий з основними термінами і поняттями цифрової безпеки, але не має чіткого уявлення про методичні стратегії або технології, які можна застосувати в навчанні учнів. Він може вказати на важливі теми, але не розуміє, як їх правильно інтегрувати в процес навчання. Студент, наприклад, може говорити, що потрібно "використовувати інтернет безпечно", але не здатен розробити план уроку чи застосувати відповідні педагогічні методи для формування знань та умінь в учнів, щоб останні використовували інтернет безпечно. Студент може згадати теоретичні основи цифрової безпеки, але не володіє конкретними знаннями про підходи до розвитку учнів у цій сфері, не може дібрати методи/ підходи/ засоби навчання для розвитку навичок

цифрової безпеки у учнів. Студент не здатний обґрунтовано вибирати та застосовувати методи або засоби навчання для розвитку навичок цифрової безпеки у учнів. Він використовує загальні методи, але не спроможний адаптувати їх до конкретних навчальних ситуацій. Наприклад, студент може використовувати традиційні методи навчання (наприклад, виклад нового матеріалу), але не враховує важливість інтерактивних чи цифрових інструментів для залучення учнів до опанування знань та вмінь у галузі цифрової безпеки.

Прагнення до професійного розвитку в галузі цифрової безпеки обмежені. Студент не проявляє ініціативи у поглибленому вивченні проблем цифрової безпеки . Він може бути не зацікавленим у додаткових курсах або тренінгах і не бачить необхідності постійно вдосконалювати свої знання. Прагнення до професійного розвитку в галузі цифрової безпеки у нього практично відсутнє.

Отже, на початковому рівні готовності майбутні вчителі інформатики хоч і мають загальне уявлення про цифрову безпеку, але не володіють достатніми знаннями і навичками для того, щоб ефективно розвивати ці навички у учнів. Їхня мотивація до професійного розвитку є мінімальною, а методичні та педагогічні підходи до навчання цієї теми залишаються на початковому етапі опанування.

Базовий рівень готовності майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів характеризується наявністю базових знань та усвідомлення важливості цифрової безпеки, а також готовністю до використання деяких методичних підходів та інструментів для її викладання. Однак, на цьому рівні вчитель ще не володіє достатньо глибокими та різноманітними методичними стратегіями, і його професійна мотивація до розвитку в цій галузі потребує вдосконалення.

Студент починає усвідомлювати важливість розвитку навичок цифрової безпеки учнів та розуміє її значення в контексті сучасних цифрових загроз, однак ще не має достатньої переконаності в необхідності інтегрувати ці знання

в освітній процес. Студент, зокрема, визнає важливість цифрової безпеки для учнів і може говорити про загрози кібербулінгу, але ще не може точно сформулювати, як ці навички варто розвивати на уроках інформатики. Усвідомлення важливості теми є, але обмежене розумінням загальних аспектів безпеки в цифровому світі. Це може проявлятись у плануванні уроків, де цифрова безпека не є основним фокусом, а лише згадується як один із результатів навчання інформатики.

Студент володіє базовими знаннями про методичні підходи до викладання цифрової безпеки. Він розуміє значення основних підходів, таких як лекції, групові роботи, або проєктні методи, але їх використання обмежене базовими стратегіями. Студент, зокрема, може розпізнати такі методичні підходи, як "обговорення", "демонстрація", або "пояснення" основних понять, але не знає, як адаптувати ці методи для ефективного розвитку навичок безпеки в учнів. Знання методів є, але вони ще не обґрунтовані з точки зору інтеграції в освітній процес, а також студент немає чіткого розуміння, як конкретні методи сприяють розвитку навичок цифрової безпеки учнів.

Студент вже здатен використовувати базові методи навчання цифрової безпеки, зокрема інтерактивні вправи або заняття на прикладах. Однак, цей підхід обмежений лише стандартними методами, і студент ще не спроможний адаптувати їх до різних ситуацій чи учнів. Наприклад, він може застосовувати лекції та завдання на комп’ютері, щоб продемонструвати основи цифрової безпеки, але не використовує додаткові інструменти, такі як відео, онлайн-курси чи симуляції для поглибленого засвоєння матеріалу. Уміння вибирати методи навчання є, однак їх різноманітність та адаптація до конкретних учнів потребує розвитку. Студент не завжди може виявити відповідні підходи для диференціації учнів.

Студент демонструє базову мотивацію до самовдосконалення в галузі цифрової безпеки, проте це прагнення не завжди проявляються в конкретних діях. Вони можуть звертати увагу на курси, тренінги чи додаткові ресурси, але часто зволікають або відтерміновують участь у професійному розвитку.

Студент може стверджувати, що хоче вивчати галузь цифрової безпеки, але ще не зареєструвався на жоден онлайн-курс або тренінг з цієї теми, посилаючись на відсутність часу чи інших пріоритетів. Прагнення до розвитку є, але виявляється не настільки активним і не має постійного характеру. Студент готовий інколи брати участь у тренінгах, але потребує додаткового стимулу та організації для більш ефективних самоосвітніх дій.

Отже, на базовому рівні готовності майбутні вчителі інформатики вже мають загальне уявлення про цифрову безпеку і базові методичні знання. Вони здатні застосовувати стандартні методи та інструменти для викладання теми, але їм ще не вистачає глибини та адаптивності в підходах. Вони також мають початкову мотивацію до розвитку своїх професійних навичок у галузі цифрової безпеки, але це прагнення ще не є стійким і систематичним.

Високий рівень готовності майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів характеризується глибокими знаннями, умінням застосовувати різноманітні методичні підходи та інструменти для навчання цифрової безпеки, а також високою мотивацією до професійного розвитку в цій галузі. Студент на цьому рівні активно інтегрує цифрову безпеку в освітній процес і продовжує працювати над власним розвитком у цій сфері.

Студент має чітке усвідомлення важливості формування навичок цифрової безпеки серед учнів і вважає це пріоритетним завданням у своїй педагогічній діяльності. Він активно включає теми цифрової безпеки в свої плани уроків і вважає їх важливими для формування здорової цифрової поведінки у учнів. Студент, зокрема, розробляє спеціалізовані курси або додаткові заняття з цифрової безпеки для учнів, враховуючи сучасні загрози та технологічні зміни, може ініціювати й реалізовувати навчальні проекти, що включають інтернет-безпеку, кібербулінг, захист персональних даних тощо. Усвідомлення важливості формування навичок цифрової безпеки є основним пріоритетом у навчальній діяльності студента, і ця тема активно інтегрується у навчальні програми та плани.

Студент володіє ґрунтовними знаннями методичних підходів, що дозволяють ефективно розвивати в учнів навички цифрової безпеки. Студент використовує не тільки традиційні форми (лекції, дискусії), але й активно впроваджують інноваційні підходи, такі як проєктно-орієнтоване навчання, ситуаційні вправи, інтерактивні онлайн-курси, тренінги з використанням реальних кіберзагроз. Зокрема, студент активно використовує симуляції реальних ситуацій кіберзагроз, тренування з використання захищених онлайн-сервісів або розробку інтерктивних завдань для учнів, що відображають реальні сценарії кібербезпеки. Знання методичних підходів є вичерпними, і студент здатен застосовувати різноманітні стратегії для інтеграції цифрової безпеки в навчальний процес, враховуючи актуальні тренди та технології.

Студент здатний не тільки вибирати відповідні методи і засоби для розвитку навичок цифрової безпеки, але й адаптувати їх до різних учнівських груп і навчальних ситуацій. Вони можуть використовувати як традиційні (лекції, тестування), так і новітні технології (ігрові методи, віртуальні лабораторії, симуляції), забезпечуючи тим самим високий рівень залучення учнів. Студент, зокрема, розробляє індивідуальні завдання для учнів відповідно до їх рівня знань та умінь, застосовує різні форми цифрового навчання (вебінари, онлайн-семінари, тренінги), а також використовує цифрові технології для моніторингу прогресу учнів. Студент вміє адаптувати методи і засоби для різних учнівських груп, здатен впроваджувати інноваційні технології для більш ефективного навчання.

Студент демонструє високий рівень професійної мотивації та самостійно шукає можливості для розвитку своїх знань і вмінь у сфері цифрової безпеки. Він активно бере участь у спеціалізованих тренінгах, семінарах, курсах, а також здійснює постійне самостійне вивчення нових технологій, методів і практик. Студент активно і систематично розвиває свої професійні навички в галузі кібербезпеки, має високий рівень прагнення до самовдосконалення.

Отже, на високому рівні готовності майбутній вчитель інформатики має чітке розуміння важливості цифрової безпеки для учнів і активно використовує різноманітні методичні стратегії та інструменти для її викладання. Студент демонструє високий рівень самостійності в адаптації методів до різних учнівських груп і активно займається саморозвитком у галузі кібербезпеки, прагнучи постійно вдосконалювати свої професійні навички.

Творчий рівень готовності майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів характеризується високим рівнем інноваційного підходу, креативності, активного експериментування та впровадження нових методик і технологій у навчальний процес. Студент на цьому рівні здатен не лише адаптувати існуючі методи навчання, а й розробляти і втілювати власні, які значно покращують процес навчання цифрової безпеки та інтегрують новітні технології в освітній процес.

Студент на творчому рівні готовності має глибоке та цілісне розуміння потреби у формуванні навичок цифрової безпеки в учнів. Він не лише визнає важливість цієї теми, але і активно інтегрує її в загальну програму з інформатики. Такий студент здатен формулювати нові ідеї та концепції щодо того, як забезпечити безпеку в цифровому середовищі для учнів. Студент, зокрема, розробляє новаторські програми або курси з цифрової безпеки, орієнтуючись на актуальні виклики сучасного цифрового світу (наприклад, цифрові загрози, новітні технології в освіті, штучний інтелект), і пропонує інтеграцію таких курсів в шкільну освітню систему. Студент виявляє високий рівень інноваційного мислення, пропонує нові моделі навчання, адаптовані до сучасних умов, та активно інтегрує цифрову безпеку в освітній процес з урахуванням сучасних проблем і загроз.

Студент володіє глибокими знаннями з методики навчання цифрової безпеки, здатний адаптувати наявні методи навчання під конкретні ситуації та потреби учнів. Студент може самостійно розробляти і впроваджувати інноваційні методи та підходи для розвитку навичок цифрової безпеки учнів.

Творчий підхід дозволяє студену розробляти унікальні форми навчання, що максимально підвищують ефективність засвоєння матеріалу. Студент створює інтерактивні ігри або симуляції, що моделюють реальні ситуації кіберзагроз, де учні в реальному часі повинні приймати рішення. Студент може також застосовувати віртуальну або доповнену реальності для проведення уроків цифрової безпеки.

Студент здатний не тільки вибирати, але й створювати нові засоби для розвитку навичок цифрової безпеки. Це може включати розробку персоналізованих освітніх траєкторій, інноваційних технологічних інструментів, інтерфейсів або застосунків, що спеціально розроблені для навчання цифрової безпеки. Студент, наприклад, самостійно розробляє веб-платформи, мобільні додатки або програмне забезпечення для навчання учнів основам цифрової безпеки. Вони можуть організовувати практичні заняття із застосуванням реальних сценаріїв безпеки в Інтернеті, що дозволяють учням тренувати навички безпечного використання цифрових технологій. Студент здатен створювати оригінальні методи та підходи, що максимально відповідають вимогам сучасного цифрового середовища, та активно їх використовує для навчання учнів.

Студент демонструє надзвичайно високий рівень професійної мотивації, активно шукаючи нові можливості для розвитку своїх знань і вмінь у сфері цифрової безпеки. Вони не тільки прагнуть вдосконалювати свої навички, але й активно працюють над удосконаленням методики навчання в цій галузі, мають бажання бути лідерами в галузі цифрової безпеки. Студент активно бере участь у конференціях, розробляє власні навчальні програми або сертифікаційні курси з цифрової безпеки для учнів. Студент активно сприяє розвитку галузі, постійно шукає нові способи саморозвитку і вважає професійний розвиток у сфері цифрової безпеки однією з головних складових своєї кар’єри.

Отже, на творчому рівні готовності майбутній вчитель інформатики не лише володіє знаннями і навичками для викладання цифрової безпеки, але й

активно займається розробкою нових підходів, інструментів та методик для навчання цієї теми. Вони здатні створювати інноваційні та нестандартні рішення для інтеграції цифрової безпеки в навчальний процес, активно працюють над вдосконаленням своїх навичок і є лідерами в цій галузі.

Таким чином, ми розробили і обґрунтували діагностичний апарат дослідження. Для визначення сформованості готовності майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів будемо використовувати спонукальний, компетентісний і поведінковий критерії, які увиразнюються чотирма показниками: ступінь усвідомленості потреби розвитку навичок цифрової безпеки учнів; знання методичних підходів для розвитку навичок цифрової безпеки; уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки учнів; прагнення до професійного розвитку в галузі цифрової безпеки. Готовність майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів як особистісна якість розглядається на чотирьох рівнях свого розвитку: початковий, базовий, високий, творчий.

3.2. Перебіг експериментального впровадження моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу

Дисертаційне дослідження проводилося у кілька етапів.

На *першому* етапі (2022-2023) було здійснено теоретичний і практичний аналіз та обґрунтування проблеми дослідження, виявлено наявні суперечності для уточнення предмету дослідження, а також розроблено науковий апарат дослідження та відповідний тезаурус. Зокрема, показано, що сьогодні множаться цифрові загрози, і молодь стикається з численними проблемами в галузі цифрової безпеки. Тому актуальною стає потреба формування і розвитку відповідних навичок в учнів, що вимагає випереджувальної підготовки вчителів інформатики.

Для з’ясування практичного стану проблеми дослідження ми провели опитування працюючих учителів інформатики (додаток Е). В опитуванні взяли участь 23 учителі інформатики (вчителі різного віку, з різним досвідом і рівнем ІТ-підготовки).

Аналіз відповідей засвідчив таке.

На запитання «1. Як ви оцінюєте важливість формування навичок цифрової гігієни в учнів?» більшість (18, 78%) вчителів оцінили це як "дуже важливо" або "швидше важливо". Старші вчителі (50+ років) недооцінювали значення цифрової безпеки через слабшу ІТ-підготовку та менший досвід цифрових загроз. Молоді вчителі (до 35 років), знайомі з сучасними загрозами кіберпростору, тому їх відповіді підтверджували критичну потребу формування цифрової гігієни. Отже, хоча більшість вчителів усвідомлюють важливість цифрової безпеки, виявляється необхідним підвищувати обізнаність у сфері цифрової безпеки.

На запитання «2. Чи вважаєте ви, що цифрова безпека має бути частиною шкільного курсу інформатики?» 13 (57%) учителів підтримали ідею, що цифрова безпека має бути обов’язковою частиною курсу інформатики. При цьому старші вчителі вважали, що такі навички мають формуватися на інших предметах або у процесі проведення виховних годин. Молоді вчителі та ті, хто часто працює з учнями в цифрових середовищах, підтримують розвиток навичок цифрової безпеки на уроках інформатики.

На запитання «3. Які аспекти цифрової безпеки є найбільш важливими для учнів?» ми отримали такі відповіді: захист персональних даних та інформаційна безпека 15 (65%) вчителів, причому критичне мислення та оцінка інформації відзначені як більш важливі для молодих вчителів, знайомих із проблемами дезінформації; етика цифрового спілкування отримала більше підтримки від учителів із педагогічним стажем (пояснюємо це тим, що вони частіше стикаються з кібербулінгом серед учнів).

На запитання «4. Чи відчуваєте ви себе достатньо підготовленими для розвитку навичок цифрової безпеки?» 10 (43%) вчителів вказали, що

потребують додаткову підготовку. Причому ми відзначили, що старші вчителі та ті, хто не має ІТ-освіти, частіше визнають недостатню підготовленість. Молодші вчителі з ІТ-досвідом почувалися впевненіше, але також вказали на потребу в методичних матеріалах та формуванні в них спеціально орієнтованих умінь.

На запитання 5. Чи використовуєте ви на уроках практичні завдання для розвитку навичок цифрової безпеки? 7(30%) вчителів зазначили, що використовують такі завдання час від часу. При цьому старші вчителі майже не використовують практичних завдань через нестачу методичних рекомендацій. Молоді вчителі зазначили, що використовують більше інтерактивних вправ.

У відповідь на запитання «6. Які труднощі у викладанні цифрової безпеки?» серед головних труднощів були відзначені брак методичних матеріалів (16, 70%), недостатня методична підготовка вчителів (13, 57%). Молоді вчителі вказували на низький рівень зацікавленості учнів. Старші вчителі частіше зазначали про брак на брак чітких вимог у навчальній програмі.

Щодо запитання «7. Чи потрібні вам додаткові курси або тренінги з розвитку навичок цифрової безпеки?» більшість вчителів (19, 82%) визнали, що такі курси потрібні.

Також ми цікавилися відношенням вчителів до роботи з батьками в галузі цифрової безпеки дітей. На запитання «8. Чи повинні батьки також долучатися до розвитку навичок цифрової безпеки дітей? Відповіді поділилися: 13(57%) вчителів зазначили, що це спільна відповідальність, 5 (22%) учителів зазначили, що це першочергове завдання батьків; 4(17%) зазначили, що школа має взяти на себе основну відповідальність через недостатню обізнаність батьків; 1(4%) не мав чіткої позиції щодо цього питання. При цьому ми відзначили, що молодші вчителі частіше визнавали роль батьків, оскільки вважали сильним вплив соціальних мереж на учнів поза

школою. Досвідчені вчителі більше спиралися на шкільну систему як основний інструмент впливу на дітей.

На запитання «9. Чи помічаєте ви серед учнів проблеми, пов'язані з відсутністю навичок цифрової безпеки?» знову думки розділилися: 14 (61%) вчителів відповіли, що спостерігають такі проблеми періодично; 5(22%) вказали, що зіштовхуються з такими проблемами постійно; 3(13%) не помічали серйозних проблем (ймовірно, це були вчителі молодших класів).

Серед типових проблеми вчителі відзначали безпечну поведінку в соцмережах (розголошення особистої інформації, контакти з незнайомцями); слабкі паролі (учні часто не розуміють цифрові небезпеки); кібербулінг і токсичне онлайн-спілкування; а також залежність від гаджетів, проблеми з тайм-менеджментом онлайн-навчання. При цьому вчителі старших класів частіше зауважують кібербулінг, маніпуляції в соцмережах та порушення приватності. Також учителі зазначали про встановлення учнями програм з мережі Інтернет зі шкідливим ПЗ.

На запитання «10. На вашу думку, що може покращити навчання учнів у галузі цифрової безпеки в школах? Відповіді розділилися: 16(70%) учителів підтримує включення цифрової безпеки до навчальної програми з інформатики; 14(61%) вказали на потребу в спеціальних тренінгах для вчителів; 8(35%) визнають необхідність вебінарів та відкритих уроків для учнів і батьків. При цьому досвідчені вчителі частіше підтримують традиційний підхід (включення теми в навчальну програму, тренінги для педагогів), а молоді вчителі визнають ефективність інтерактивних методів навчання (онлайн-симулятори, ігри, тестування). Вчителі, які обізнані на проблемах цифрової безпеки, підтримують комплексний підхід

На запитання «Які аспекти цифрової безпеки ви вважаєте найважливішими?» молоді вчителі звернули увагу на кібербезпеку, фішинг, критичне мислення. Досвідчені вчителі – на культуру цифрового спілкування та поведінку учнів у соцмережах. На запитання «Які методи розвитку навичок цифрової безпеки ви вважаєте ефективними?» молоді вчителі вказували

інтерактивні платформи, ігри, кейси, а старші вчителі зазначали про діалогічні методи (обговорення, дискусія) та використання відеоматеріалів. Нам запитання «Що могло б мотивувати вас розвивати навички цифрової безпеки учнів?» ми отримали такі відповіді: офіційне включення теми в навчальні програми; наявність готових матеріалів та методичних рекомендацій; підвищення рівня власної кваліфікації

Отже, опитування засвідчило, що більшість вчителів визнають важливість цифрової безпеки, але їм бракує методичних матеріалів та спеціальної підготовки. Є значна різниця у підходах між молодими та досвідченими вчителями. Розроблення спецкурсу, орієнтованого на підготовку вчителів до розвитку навичок цифрової безпеки учнів, є необхідним, оскільки: більшість учителів усвідомлює важливість цифрової безпеки, але потребує спеціальної підготовки. Наявні проблеми серед учнів (небезпека в соцмережах, фішинг, кібербулінг) підтверджують потребу в створенні відповідних дидактичних матеріалів. Вчителі визнають, що розвивати навички цифрової безпеки потрібно через їх інтеграцію в освітній процес , але є багато таких, які не знають, як це робити ефективно.

Аналіз освітньо-професійних програм підготовки вчителів показав, що навчальні плани не передбачають окремих курсів спеціалізованої підготовки, а серед результатів навчання навички цифрової безпеки не відображені окремо, а включені до загальних цифрових навичок вчителя. Такий результат охарактеризовано нами через категорію «готовність майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів».

Узагальнення теоретико-практичних розвідок дало підстави стверджувати, що для забезпечення готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів освітньо-професійна програма повинна охоплювати: фундаментальні концепції безпеки (основні принципи кібербезпеки, включаючи конфіденційність, цілісність та доступність); поширені кіберзагрози (фішинг, шкідливе програмне забезпечення та соціальна інженерія), а також стратегії пом’якшення

наслідків; опанування безпечних Інтернет-практик (безпечні звички перегляду, управління паролями та відповідальне використання соціальних мереж); конфіденційність та захист даних (правила конфіденційності даних та практики захисту інформації); правові та етичні наслідки питань цифрової безпеки.

Нами доведено, що слід акцентувати увагу на практичних навичках майбутніх учителів інформатики, зокрема на опануванні методик, стратегій, методів і засобів ефективного навчання викладання понять цифрової безпеки на рівні, доступному для молоді. Отже, на першому етапі ми з'ясували потребу розроблення особливого змісту підготовки майбутніх учителів інформатики, на якому буде формуватися їх готовність до розвитку навичок цифрової безпеки учнів і який має бути опановано в межах наявних освітньо-професійних програм. Це спонукало нас до розроблення моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу

На *другому* етапі (2023 рік) ми розробили і обґрунтували модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу. Авторська модель вимагала дотримання певних принципів (науковість та актуальність, системність, компетентісна орієнтованість, практико-орієнтованість, інтеграція та міждисциплінарність) у організацію спецкурсу «Цифрова безпека у навчальному середовищі». Було обґрунтовано вибір форм (лекції, практичні заняття), методів (активних і проблемних) і цифрових засобів навчання (цифрові навчальні середовища, цифрові освітні ресурси та програми спеціалізованого спрямування).

Перевірка ефективності моделі вимагала наявності діагностичного апарату, тому було розроблено критерії (спонукальний, компетентісний і поведінковий), показники (ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів; знання методичних підходів для розвитку навичок цифрової безпеки; уміння дібрати методи/ підходи/ засоби навчання для

розвитку навичок цифрової безпеки в учнів; прагнення до професійного розвитку в галузі цифрової безпеки) та схарактеризовано рівні готовності (початковий, базовий, високий, творчий).

Третій етап, експериментальне впровадження моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу, відбувся протягом 2024-2025 років. Особливістю моделі був спецкурс.

Спецкурс «Цифрова безпека у навчальному середовищі» (далі – спецкурс) пропонувався як вибірковий для здобувачів першого і другого рівнів вищої освіти за спеціальністю «Середня освіта (інформатика)». Спецкурс вимагав проведення лекцій, до який було розроблено супровідні мультимедійні матеріали (презентації, практичні кейси, навчальні відео; рис. 3.2).

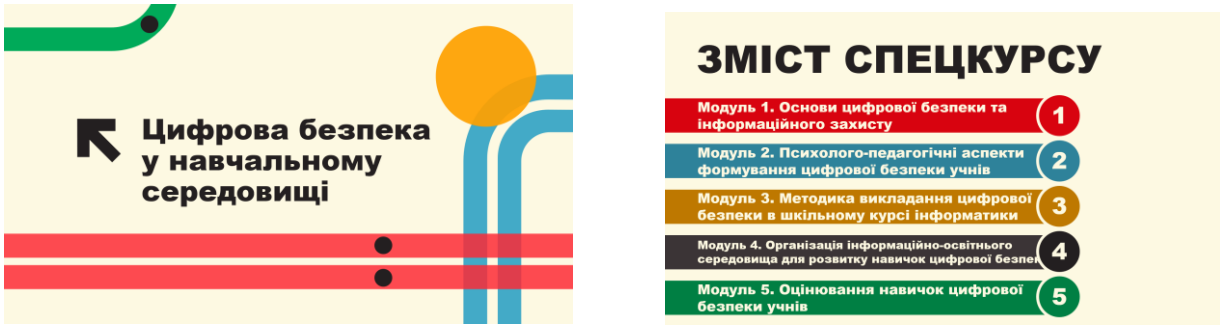


Рис.3.2. Перші слайди презентації

Серед дидактичних матеріалів ми пропонували відеоматеріали (практичні кейси, навчальні відео) з відеохостингу YouTube:

1. Загальні поняття цифрової безпеки. Відео «Інформаційна безпека: Загрози при роботі в Інтернеті і їх уникнення» розглядає основні загрози в Інтернеті та способи їх уникнення. [https://www.youtube.com/watch?v=vTosEd5LoLA&ab_channel=%D0%A8%D0%BF%D0%B0%D1%80%D0%B3%D0%B0%D0%BB%D0%BA%D0%B0%D1

%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0].

2. Кібербезпека в освітньому середовищі Відеоурок «Всеукраїнський онлайн-урок із кібербезпеки “Я. Безпека. Інтернет”» присвячений основам безпечної поведінки в Інтернеті для учнів та вчителів або Відео «Безпечне та доступне навчання: як захистити дитину та себе в Інтернеті» надає рекомендації щодо захисту дітей та дорослих від інтернет-загроз.

3. Захист персональних даних. Відео-рекомендації «Як захистити свої персональні дані в Інтернеті» щодо збереження конфіденційності та захисту особистої інформації онлайн [https://www.youtube.com/watch?v=example1]

4. Соціальна інженерія та фішинг. Відео «Соціальна інженерія: як не стати жертвою маніпуляцій» пояснює методи соціальної інженерії та як протидіяти їм. [https://www.youtube.com/watch?v=example2] або Відеоогляд «Фішинг: як розпізнати та уникнути» дає поради щодо їх розпізнавання. [https://www.youtube.com/watch?v=example3].

5. Налаштування безпеки пристроїв та мереж. Відео-інструкції «Безпечні налаштування Wi-Fi мережі» описують захист домашньої або шкільної Wi-Fi мережі від несанкціонованого доступу. [https://www.youtube.com/watch?v=example4] або відео-поради «Захист смартфона: поради та рекомендації» дають практичні поради щодо забезпечення безпеки мобільних пристроїв. [https://www.youtube.com/watch?v=example5].

Ми пропонували декілька короткометражних фільмів, які демонструють випадки кібербулінгу: «Історія одного булінгу» про проблему булінгу, де показано, як булери усвідомлюють безглуздість своїх дій. (https://www.youtube.com/watch?v=5uzmkul5Tb0&ab_channel=%D0%9D%D0%92%D0%9A%D0%A2%D1%80%D1%83%D1%81%D0%BA%D0%B0%D0%B2%D0%B5%D1%86%D1%8C); "Без маски (булінг)" про проблеми булінгу та його наслідків для жертв (https://www.youtube.com/watch?v=fmNyc51ZVYI&ab_channel=%D0%92%D0

%BE%D0%BB%D0%BE%D0%B4%D0%B8%D0%BC%D0%B8%D1%80%D0%9A%D0%BE%D1%80%D0%BE%D0%BF); "Відеоурок про кібербулінг" про що таке кібербулінг, як його розпізнати та як з ним боротися (https://www.youtube.com/watch?v=lCfNGCDYXpg&ab_channel=%D0%91%D0%BE%D0%B1%D1%80%D0%BE%D0%B2%D0%B8%D1%86%D1%8C%D0%BA%D0%B8%D0%B9%D0%97%D0%97%D0%A1%D0%9E%D0%86-%D0%86%D0%86%D0%86%D1%81%D1%82%D1%83%D0%BF%D0%B5%D0%BD%D1%96%D0%B2%E2%84%961); «Про кібербулінг для підлітків. Серія 1 — Що таке кібербулінг?" - відео пояснює підліткам, що таке кібербулінг, як він проявляється та як його уникнути (https://www.youtube.com/watch?v=5eELHySnFho&ab_channel=UNICEFUkraine).

Практичні заняття передбачали використання активних і проблемних методів навчання.

В реалізації спецкурсу ми стикнулися з певними проблемами. Студенти мали різний рівень попередніх знань у сфері інформаційних технологій та цифрової безпеки. Це ускладнювало засвоєння понять у галузі цифрової безпеки (Модуль 1). Тому ми починали курс із визначення рівня знань студентів і на основі цього адаптувати теми. Проводити додаткові заняття чи семінари для тих, хто потребував покращення знань. Також ми стикнулися з проблемою невідповідності тематики курсу до реальних очікувань студентів. Окремі студенти відчували, що курс не відповідає їхнім практичним потребам або не має прямого зв’язку з їхньою щоденною діяльністю в класі. Тому нам було важливо на початку курсу чітко пояснити, як ці знання і навички можуть бути використані у їхній педагогічній практиці. Ми залучали реальні кейси для того, щоб зробити авторський курс максимально практичним.

Інша проблема - недостатнє технологічне забезпечення, яке було обмеженим через війну. Відсутність доступу до необхідного програмного забезпечення або інтернет-зв’язку серйозно ускладнювало процес навчання. Тому ми підготували резервні варіанти для занять, зокрема, офлайн-матеріали

або спрощені варіанти завдань, а також пропонувати онлайн-курси чи ресурси для самостійного вивчення матеріалу поза аудиторними заняттями.

Відзначаємо також низьку мотивацію студентів. Студенти часто не усвідомлювали важливість теми цифрової безпеки і не бачили її значущості для свого професійного становлення, а тому не проявляли достатньої активності у процесі навчання. Ми використовували мотивуючі приклади та роз'яснення, чому ці знання є важливими для їхньої роботи в школі. Ми залучали студентів до обговорення актуальних загроз та ситуацій у реальному житті, де вони можуть використовувати ці навички.

На практичних заняттях ми побачили, що питання цифрової безпеки для майбутніх учителів інформатики можуть бути складними, і це іноді знижувало інтерес студентів, а заняття перетворювалося на пасивне слухання. Тому ми включали більше інтерактивних елементів, таких як симуляції, рольові ігри, ситуаційні задачі, де студенти мали змогу застосовувати на практиці свої знання. Ми також пропонували групові проєкти і тренінги, щоб стимулювати групову співпрацю. Ми добирали цікаві завдання, але експериментальне навчання виявило, що вони могли бути занадто складними або занадто простими для студентів, тому ми дозволити студентам самостійно вибирати завдання або працювати в групах, де кожен може запропонувати своє рішення в залежності від рівня підготовки.

Готовність майбутніх учителів до розвитку навичок цифрової безпеки учнів вимагала формування методичних знань та вмінь. Для цього ми використовували не лише метод кейс-стаді, а й рольові ігри та проєктну діяльність. Наприклад, студентам пропонувалися реальні завдання.

Завдання 1. Аналіз випадку з порушенням цифрової безпеки. Студент отримує опис ситуації, де учень випадково розповсюдив особисті дані в Інтернеті. Він повинен:

- Оцінити ризики та наслідки для учня і школи.
- Запропонувати стратегії для запобігання подібним випадкам у майбутньому.

– Розробити урок, який навчить учнів уникати таких ситуацій.

Критерії оцінювання:

– Аналіз ситуації: Чи розпізнав учитель ключові фактори порушення безпеки? (0–2 балів)

– Рекомендації: Наскільки запропоновані стратегії є практичними та ефективними? (0–2 балів)

– План уроку: Чи правильно сформульовані цілі уроку, що сприяють розвитку навичок цифрової безпеки? (0–2 балів)

– Загальна оцінка: Відповіді на питання та план уроку не мають суттєвих пропусків. (0-2 балів)

Завдання 2. Проектування інтерактивних занять з цифрової безпеки. Студент розробляє низку інтерактивних занять для учнів середньої школи, який охоплює поняття «конфіденційність», «паролі», «кібербулінг». Учитель повинен:

– Визначити цільову аудиторію (вік учнів).

– Скласти план уроків і розподілити матеріали для кожного заняття.

– Включити цифрові інструменти для оцінки ефективності курсу.

Критерії оцінювання:

– Зміст курсу: Чи охоплює курс всі важливі теми цифрової безпеки? (0-2 балів)

– Інтерактивні елементи: Чи є елементи, що сприяють активному залученню учнів? (0-2 балів)

– Методи оцінювання: Чи запропоновано коректні методи оцінки результатів учнів? (0-2 балів)

– Загальна оцінка: Наявність чіткої структури, детальних пояснень і плану для кожного етапу курсу (0-2 балів)

Також ми ставили практико-орієнтовані запитання:

1. Які методи соціальної інженерії використовують кіберзлочинці?

Можлива відповідь:

Кіберзлочинці використовують такі методи соціальної інженерії, як фішинг (обманне отримання конфіденційної інформації через електронні листи або сайти), вішинг (шахрайство через телефонні дзвінки), смішинг (шахрайство через SMS), а також метод «довіри» – коли злочинець видає себе за авторитетну особу (наприклад, адміністратора або керівника). Основна мета – маніпуляція жертвою для отримання особистих даних або доступу до облікових записів.

2. Як правильно налаштувати конфіденційність у соціальних мережах?

Можлива відповідь:

Для забезпечення конфіденційності в соціальних мережах слід:

- *Встановити обмеження на перегляд профілю, публікацій та списку друзів (наприклад, лише для друзів або певних груп людей).*
- *Вимкнути геолокацію, якщо вона не є необхідною.*
- *Уникати публікації особистої інформації, такої як адреса, номер телефону чи фінансові дані.*
- *Використовувати двофакторну аутентифікацію для додаткового захисту облікового запису.*
- *Регулярно переглядати та оновлювати налаштування конфіденційності відповідно до оновлень платформи.*

3. Які вправи допомагають учням навчитися розпізнавати кіберзагрози?

Можлива відповідь:

Серед ефективних вправ для навчання розпізнавання кіберзагроз:

- *Аналіз електронних листів – учні отримують зразки листів і визначають, які з них є фішинговими.*
- *Гра «Кібердетектив» – учні шукають ознаки шахрайства на фейкових вебсайтах.*
- *Сценарії кібербулінгу – розбір ситуацій і обговорення способів захисту та реагування.*

- *Квест «Захисти свій акаунт» – учні складають надійний пароль і налаштовують безпеку свого акаунту.*
- *Розбір новин – аналіз інформації в інтернеті та визначення фейкових новин.*

4. Які інструменти самооцінювання можуть використовувати учні?

Можлива відповідь:

Учні можуть використовувати такі інструменти самооцінювання:

- *Онлайн-тести з цифрової безпеки (наприклад, Google Safety Center або «Digital Skills» від Microsoft).*
- *Чек-листи безпечної поведінки в інтернеті (наприклад, чи використовують вони складні паролі, двофакторну аутентифікацію).*
- *Щоденники цифрової безпеки, де вони записують випадки кіберзагроз і те, як їх вирішували.*
- *Інтерактивні опитування (наприклад, у Google Forms або Kahoot) для визначення рівня цифрової грамотності.*
- *Симуляційні завдання, у яких вони оцінюють власні дії в змодельованих загрозливих ситуаціях.*

5. Як цифрова гігієна допомагає запобігати кіберзагрозам?

Можлива відповідь:

Цифрова гігієна включає правила безпечного використання цифрових пристроїв та інтернету, такі як регулярне оновлення програмного забезпечення, використання складних паролів, уникнення підозрілих посилань і файлів, а також обмеження обміну персональними даними. Дотримання цих правил допомагає мінімізувати ризики вірусних атак, фішингу, витоку даних і кібербулінгу.

При розв’язуванні такого типу завдань ми відзначали типові помилки студентів:

– Студенти можуть неправильно інтерпретувати завдання, що призведе до вибору невірного підходу або застосування невдалих методів. Наприклад, вони можуть неправильно оцінити потреби учнів у цифровій безпеці. Тому ми зосереджували увагу на чіткому визначенні умови завдання, щоб конкретизувати, що саме потрібно зробити, і просили студентів уточнити питання, якщо щось незрозуміло;

– Студенти можуть неправильно вибрати методи чи підходи для розвитку навичок цифрової безпеки учнів (не врахувати вік учнів або специфіку теми). Тоді ми пояснювали різницю між методами навчання для різних вікових груп і рівнів знань, надавали приклади, як ці методи можуть бути ефективно використані для досягнення результатів.

– Іноді студенти можуть не враховувати етичні та правові питання цифрової безпеки, наприклад, у контексті збору та обробки даних учнів, або допустити порушення конфіденційності в процесі навчання. Тому ми проводили додатковий тренінг-консультацію з етики і правових аспектів цифрової безпеки;

– Студенти можуть бути схильні до спрощених рішень або застосування загальних підходів, не враховуючи специфіку ситуацій або загроз. Тому ми заохочувати студентів до деталізованого аналізу завдання та адаптації можливих рішень під конкретні умови (наприклад, вік учнів, тип школи, особливості цифрових загроз);

– Студенти можуть неправильно використовувати інструменти та ресурси для розвитку навичок цифрової безпеки, наприклад, застосовувати недоцільні програми або сервіси для навчання учнів. Тому ми додатково пояснювали студентам, як правильно вибирати інструменти, що підходять до задачі, зокрема, звертаючи увагу на надійність, безпеку та доступність цих інструментів для учнів.

– Студенти можуть не враховувати важливість зворотного зв’язку для учнів у процесі розвитку в них навичок цифрової безпеки, що знижує

ефективність навчання. Тоді ми додатково пояснювали важливість зворотного зв’язку та ефективної взаємодії з учнями;

– Студенти можуть не достатньо критично підходити до оцінки потенційних загроз і не враховувати всі можливі аспекти ризиків для навчального середовища. Тому ми додатково вимагали від студентів аналізувати ситуації з різних точок зору і виявляти приховані ризики.

Реалізація курсу вимагала використання різних цифрових інструментів. Тут найбільше проявився інформаційний підхід, на засадах якого ми формували готовність учителів до розвитку навичок цифрової безпеки учнів. Ми передбачили застосування ресурсів мережі Інтернет як основи для отримання актуальної інформації про кіберзагрози, методи захисту даних та цифрову безпеку. Ми популяризували використання: освітніх платформ (Coursera, Udemy, Google for Education), де розміщено курси з цифрової безпеки; наукових та аналітичних ресурсів (Cybersecurity & Infrastructure Security Agency (CISA), Europol Cybercrime Centre), що містять рекомендації щодо протидії кіберзагрозам; форумів та онлайн-спільнот (Reddit r/cybersecurity, CyberAware Community), які дозволяють ділитися досвідом та отримувати поради від експертів.

Також на практичних заняттях ми використовували різні онлайн-симулятори як інтерактивних інструменти, що дають можливість моделювати різні сценарії кіберзагроз і відпрацьовувати стратегії їх подолання: PhishSim та KnowBe4 для розпізнавання фішингових атак, CyberCIEGE (навчальна гра для освоєння основ інформаційної безпеки) та Hack The Box (HTB) та TryHackMe (платформи для практичного навчання етичному хакінгу та захисту цифрових систем).

Також ми знайомили студентів із ресурсами для створення захищених онлайн-просторів, які забезпечують безпечну комунікацію та захист конфіденційних даних у межах освітнього процесу (навчального середовища): менеджери паролів (Bitwarden, 1Password) для навчання безпечному зберіганню паролів; зашифровані месенджери (Signal, Telegram з секретними

чатами), які ілюструють механізми шифрування повідомлень; VPN-сервіси (ProtonVPN, NordVPN), що демонструють принципи анонімності та захисту підключення в Інтернеті; хмарні сервіси з розширеними функціями безпеки (Google Workspace for Education, Microsoft 365 Education), що забезпечують збереження та спільну роботу з документами в безпечному середовищі.

Відзначимо, що ми намагалися використовувати вільно поширювані цифрові інструменти, тому обирали повністю безкоштовні для навчання цифрової безпеки (Google for Education, CyberCIEGE, Signal, Telegram, Bitwarden, Hack The Box (обмежений доступ), TryHackMe (обмежений доступ), Google Workspace for Education, Microsoft 365 Education) або інструменти з безкоштовними демо-версіями або пробним періодом (KnowBe4, PhishSim, ProtonVPN, 1Password, NordVPN, Coursera, Udemy).

Отже, інтеграція цих цифрових технологій дозволила не лише надавати теоретичні знання з цифрової безпеки, а й сформувати практичні вміння майбутніх учителів інформатики через моделювання реальних загроз та розв’язання відповідних проблем.

Навчання за спецкурсом відбувалося у форматах офлайн та онлайн. Тому можемо відзначити кілька ключових відмінностей. Офлайн навчання дозволяє студентам отримувати миттєвий зворотний зв’язок, ставити питання безпосередньо і мати більш інтерактивну взаємодію. При цьому студенти могли обмінюватися думками, працювати в групах, що сприяло розвитку командних навичок і кращому засвоєнню матеріалу через обговорення. Ми відзначили фізичну присутність в аудиторії як фактор більш серйозного ставлення до навчання і підвищення уваги. Водночас офлайн навчання може бути обмеженим для деяких студентів, потребувати узгодження навчального і робочого графіків для студентів з обмеженим часом, а також ускладненим для викладача, який має організувати індивідуальну підтримку для кожного студента.

Онлайн навчання є більш гнучким, оскільки студенти можуть вчитися у зручний час і з будь-якого місця, доступним через онлайн, що дає студентам

можливість переглядати їх у будь-який час, персоналізованим та більш інтерактивним, оскільки онлайн-платформ дозволяє використовувати різні інструменти для інтерактивного навчання, такі як відео, форми зворотного зв'язку, форуми, чати тощо. Разом з цим ми відзначили проблеми з мотивацією:, часті технічні проблеми (погане з'єднання з Інтернетом або проблеми з доступом до Moodle); брак соціальної взаємодії. Тому найбільш ефективним вважаємо комбінований підхід (blended learning), що поєднує переваги офлайн та онлайн навчання. При такому навчанні студенти можуть користуватися гнучкістю онлайн занять, а також отримувати важливий зворотний зв'язок і соціальні взаємодії в офлайн-сесіях.

Завершення вивчення спецкурсу означало закінчення педагогічного експерименту. На початку і наприкінці вивчення спецкурсу ми використовували інструменти для кількісного визначення показників. Отримані емпіричні дані дали нам можливість перейти до заключного, *четвертого етапу (2025 рік*) дослідження, на якому проведено статистичний аналіз даних та зроблено якісні висновки.

3.3. Статистичний аналіз результатів педагогічного експерименту

Педагогічний експеримент передбачав статистичний аналіз емпіричних даних щодо результатів формування у майбутніх учителів інформатики готовності до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу. Для цього нами було розроблено діагностичний апарат для визначення рівнів (початковий, базовий, високий, творчий) сформованості зазначеної категорії за різними показниками та дібрано відповідні методики їхнього розрахунку (табл. 3.2).

Експериментальною базою дослідження стали три ЗВО: Сумський державний педагогічний університет імені А.С. Макаренка, Харківський національний педагогічний університет імені Григорія Сковороди, Уманський державний педагогічний університет імені Павла Тичини.

Таблиця 3.2

Діагностичний апарат дослідження

Компоненти	*Критерії*	*Показник*	*Обрана методика*
Мотиваційний компонент	Спонукальний критерій	Ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів	Анкетування
Предметно-методичний компонент	Компетентісний критерій	Знання методичних підходів для розвитку навичок цифрової безпеки	Тестування
		Уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки у учнів	Компетентісна задача
Особистісний компонент	Поведінковий критерій	Прагнення до професійного розвитку в галузі цифрової безпеки	Анкетування

Загальна кількість учасників педагогічного експерименту складала 81 особа: 42 студенти контрольної групи (КГ) і 39 осіб експериментальної групи (ЕГ).

Для статистичного аналізу результатів використано параметри описової статистики та критерій Стьюдента оцінки середніх.

Деталізуємо методики визначення рівнів сформованості у майбутніх учителів інформатики готовності до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу за кожним із показників та представимо статистичний аналіз відповідних емпіричних даних.

Показник «П1: Ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів»

Для визначення рівня сформованості у майбутніх учителів інформатики готовності до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу за показником «Ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів» було розроблено анкету (Додаток В). Приклади запитань наведені на рисунку (рис. 3.2).

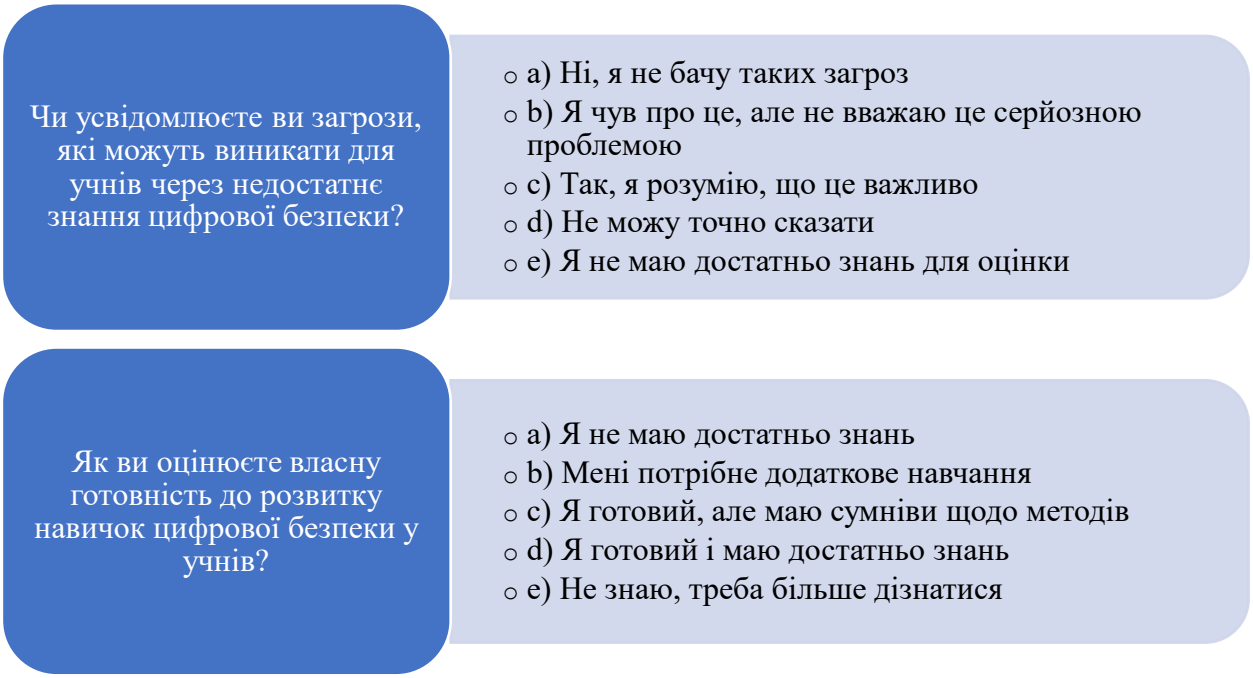


Рис. 3.2. Приклади запитань анкети для показника П1

Максимальна оцінка - 50 балів, які розподілені на чотири рівні (рис.3.3).

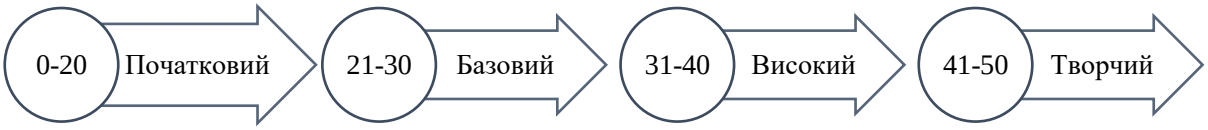


Рис. 3.3. Розподіл балів за рівнями для показника П1

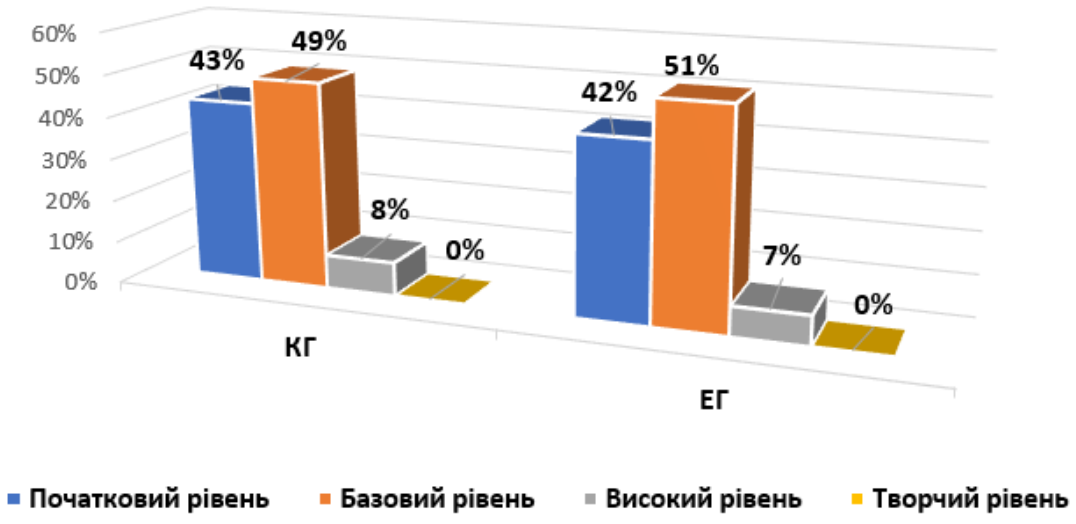
Таке анкетування проводилося на початку і наприкінці експерименту для того, щоб оцінити ефективність впливу авторської моделі формування готовності до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу на сформованість мотиваційного компонента означеної готовності.

Загальні результати, одержані на початку та в кінці педагогічного експерименту, подані у табл. 3.3 та на рис. 3.4.

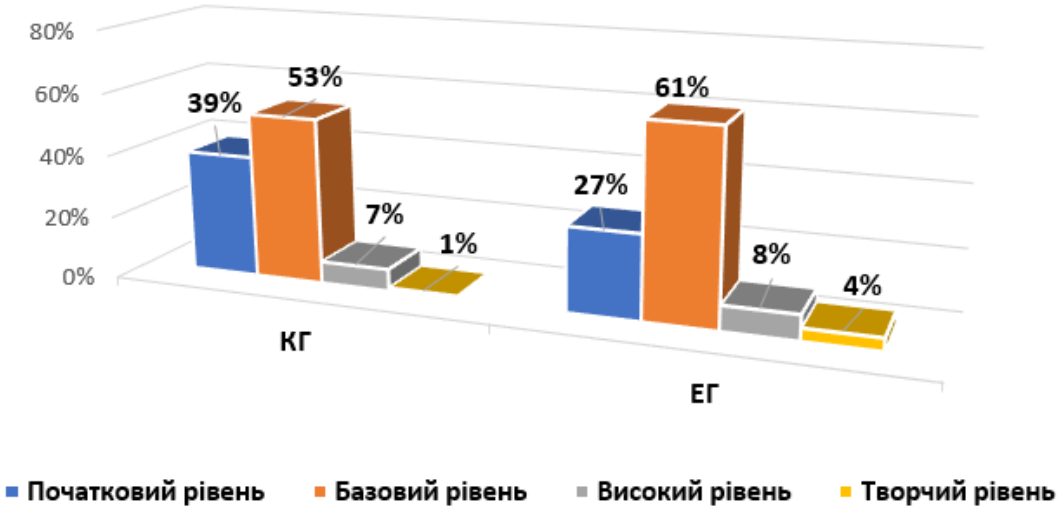
Таблиця 3.3

Розподіл рівнів за показником П1
на початку та в кінці експерименту (%)

Рівні		Початковий рівень	Базовий рівень	Високий рівень	Творчий рівень
КГ	*до*	43%	49%	8%	0%
	після	39%	53%	7%	1%
ЕГ	*до*	42%	51%	7%	0%
	після	27%	61%	8%	4%



А) на початку експерименту



Б) в кінці експерименту

Рис.3.4. Розподіл рівнів за показником П1

Аналіз даних описової статистики, який відбувався з використанням табличного процесора MS Excel, показав асиметрію і ексцес для вибірок в межах [-0.5; 0.5] і [-1; 1] відповідно, що дозволяє говорити про нормальність розподілу та можливість використання критерію Стьюдента оцінки середніх [103; 116].

Застосування критерію Стьюдента тут і надалі проводимо з використанням Пакет аналізу в MS Excel. Тут і далі обираємо рівень значущості 0,05 з гіпотезами: «H_0: $\mu_{ЕГ} = \mu_{КГ}$ (середні в ЕГ і КГ однакові)» і «H_a: $\mu_{ЕГ} \neq \mu_{КГ}$ (середні в ЕГ і КГ різні)».

У таблиці зосереджені узагальнені розрахунки на основі отриманих емпіричних дані (табл.3.4).

Виходячи з таблиці, де $T_{крит.} = 1{,}97$ більше за $T_{експ.} = 0{,}39$, стверджуємо, що вибірки, які входять у педагогічний експеримент, є статистично однаковими. Аналогічно, для випадку кінця експерименту, де $T_{крит.} = 1{,}97$ менше за модуль $T_{експ.} = -2{,}18$, стверджуємо, що ЕГ і КГ в кінці експерименту є статистично різними.

Таблиця 3.4.

Оцінка середніх за критерієм Стьюдента
для показника П1 на початку та в кінці експерименту

Двовибірковий t-тест з різними дисперсіями	**КГ**	**ЕГ**		**КГ**	**ЕГ**
Середнє	21,56	20,85		23,59	26,85
Різниця середніх для гіпотези H_0	0			0	
t-статистика (експериментальне)	0,39			-2,18	
t критичне двостороннє	1,97			1,97	

Отже, статистичні розрахунки розподілу результатів у групах ЕГ і КГ на рівні значущості 0,05 для показника «Ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів» підтвердили позитивні зрушення у формуванні мотиваційного компонента готовності майбутніх учителів інформатики до розвитку навичок цифрової гігієни учнів на засадах інформаційного підходу. Ми вважаємо, що цьому сприяли проблемно-орієнтоване навчання, коли студентам пропонувалися реальні або змодельовані ситуації, що ілюстрували цифрові загрози (наприклад, витік персональних даних, кібербулінг, фішингові атаки). Цим ми впливали на підвищення усвідомлення того, що цифрова безпека є не лише технічною, а й педагогічною проблемою. Також дієвим вважаємо використання інтерактивних симуляцій та рольових ігор, впливали на формування емоційного зв’язку з проблемою та підвищення рефлексії. Аналіз реальних кейсів та розбір практик сприяв усвідомленню того, що їхня майбутня роль як учителя – активне формування навичок цифрової безпеки в учнів.

Показник «П2: Знання методичних підходів
для розвитку навичок цифрової безпеки»

Для визначення рівня сформованості предметно-методологічного компоненту готовності майбутніх учителів інформатики до розвитку навичок

цифрової безпеки учнів на засадах інформаційного підходу ми використовували показник «Знання методичних підходів для розвитку навичок цифрової безпеки».

Методикою кількісної оцінки показника було тестування (Додаток Д). Студенти мали пройти тестування до і після вивчення спецкурсу. Приклади запитань наведені на рисунку (рис.3.5).

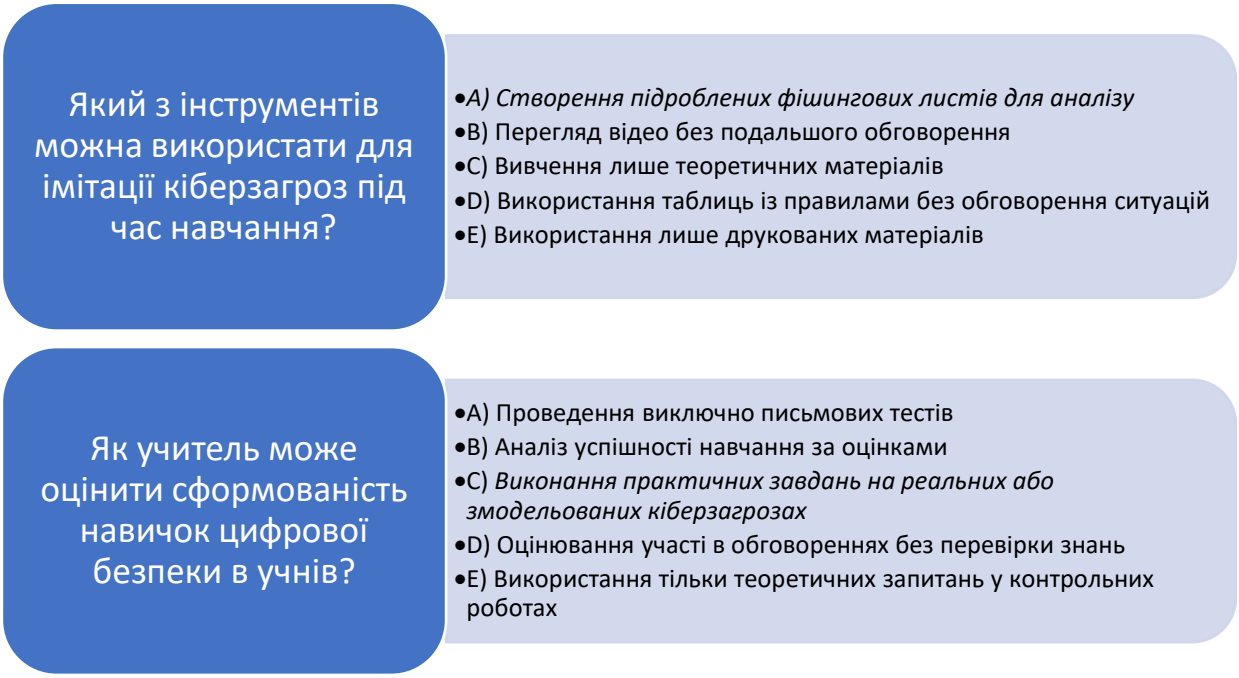


Рис. 3.5. Приклади запитань тесту для вимірювання показника П2

За результатами тесту студент мав можливість обрати максимальну оцінку - 30 балів (рис.3.6).

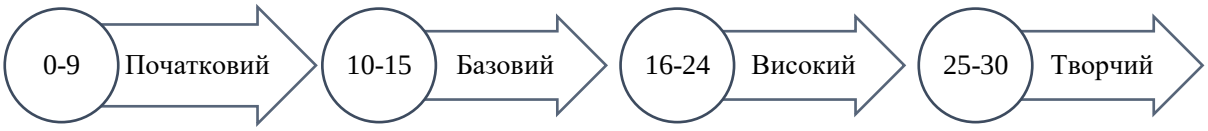


Рис. 3.6. Розподіл балів за рівнями для показника П2

Загальні результати, одержані на початку та в кінці педагогічного експерименту для показника П2, подані у табл. 3.5 та на рис. 3.7-3.8.

Таблиця 3.5

Розподіл рівнів за показником П2 на початку та в кінці експерименту

Рівні		Початковий рівень	Базовий рівень	Високий рівень	Творчий рівень
КГ	*до*	47%	51%	2%	0%
	після	41%	53%	5%	1%
ЕГ	*до*	48%	50%	2%	0%
	після	31%	59%	7%	3%

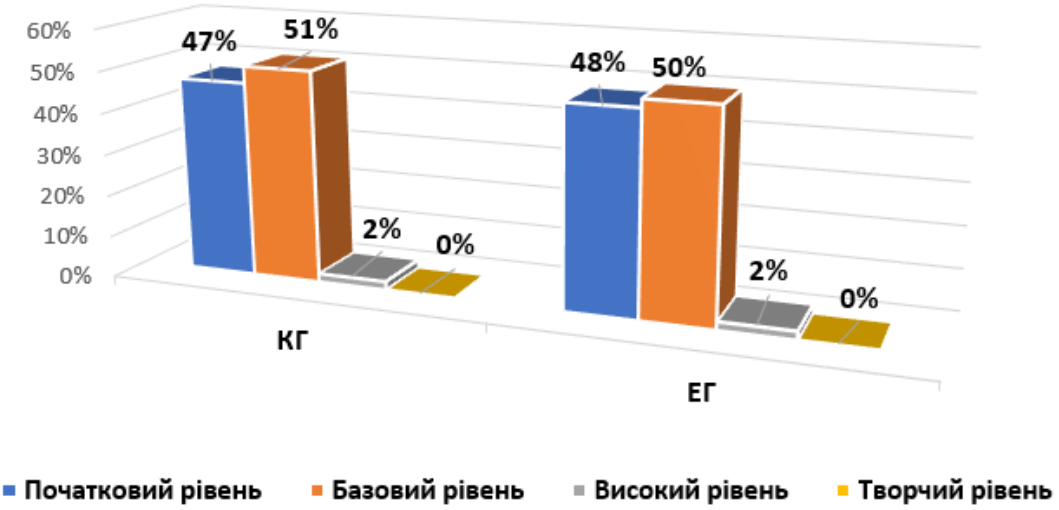


Рис.3.7. Розподіл рівнів за показником П2 на початку експерименту

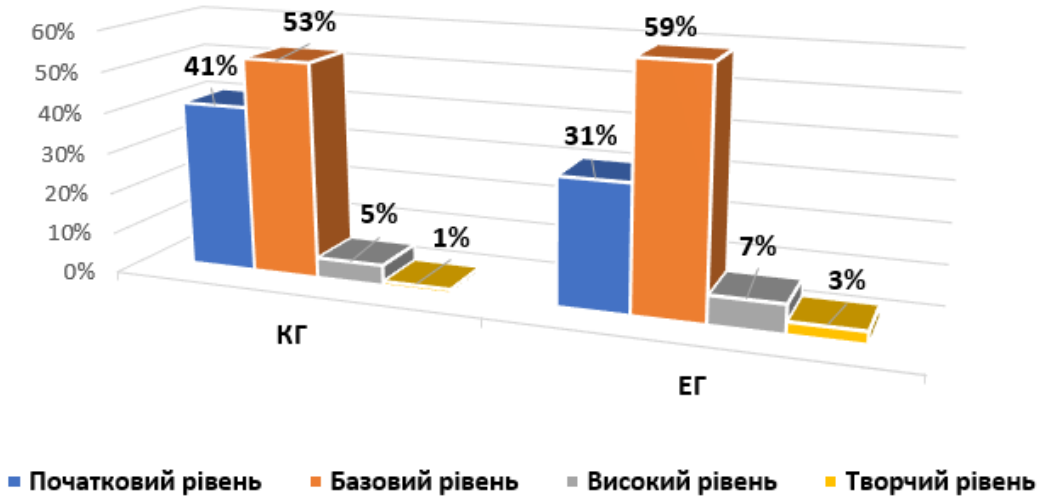


Рис.3.8. Розподіл рівнів за показником П2 в кінці експерименту

Функціонал описової статистики підтвердив, що для вибірок ЕГ і КГ асиметрія в межах -1 і 1, а ексцес у межах -1 і 1, тобто розподіл близький до

нормального, тому можна застосовувати критерій Стьюдента. Ми побудували ідентичні гіпотези, перевірка яких знову здійснена з використанням статистичних функцій MS Excel. Результати подані у таблиці (табл.3.6).

Таблиця 3.6.

Оцінка середніх для показника П2 на початку та в кінці експерименту

Двовибірковий t-тест з різними дисперсіями	**КГ**	**ЕГ**		**КГ**	**ЕГ**
Середнє	8,03	9,07		9,66	12,22
Різниця середніх для гіпотези H_0	0			0	
t-статистика (експериментальне)	-1,05			-2,08	
t критичне двостороннє	1,97			1,97	

Ми статистично підтвердили подібність (статистичну ідентичність) вибірок ЕГ та КГ до експерименту (на рівні значущості 0,05 значення $T_{крит.}$ = 1,97 більше за модуль $T_{експ.}$ = -1,05) та статистичну відмінність ЕГ і КГ після експерименту ($T_{крит.}$ = 1,97 воно менше за модуль $T_{експ.}$ = -2,08). Іншими словами, статистичний аналіз показав успішність розробленої моделі за показником П2 «Знання методичних підходів для розвитку навичок цифрової безпеки». Вважаємо, що позитивна динаміка обумовлена особливостями вибору змісту авторського спецкурсу та використанням інформаційного підходу як інструменту доступу до множини знань. Зокрема, вважаємо виправданим вивчення Модуля 3. «Методика викладання цифрової безпеки в шкільному курсі інформатики» та модуля 4. «Організація інформаційно-освітнього середовища для розвитку навичок цифрової безпеки».

При вивченні цих модулів передбачено комплексний огляд методичних підходів до навчання цифрової безпеки і формування відповідних навичок учнів: на початку ми пропонуємо студентам структуровану класифікацію методичних підходів (традиційний (лекції, семінари, підручники); практико-орієнтований підхід (тренінги, кейс-стаді, практичні завдання); ігрові методи

(квестові навчальні модулі); проєктне навчання (розробка методичних рекомендацій, створення навчальних матеріалів); Проблемно-орієнтоване навчання (аналіз реальних інцидентів із цифрової безпеки). Після цього обов'язковим є використання дискусії як інтерактивного методу навчання (наприклад, провести дискусію "Які методи найефективніші для навчання цифрової безпеки в школі?") та ознайомити студентів з нормативними документами (DigCompEdu, DigComp 2.2, концепція цифрової грамотності МОН України).Це забезпечує розуміння різних методичних підходів та їхньої ефективності. Також важливим є використання інтерактивних методів навчання: кейс-методу (розбір ситуацій того, як вчитель може захистити персональні дані учнів або що робити, якщо учень став жертвою кібербулінгу); симуляції та рольові ігри (наприклад, моделювання фішингових атак, розробка безпечного пароля). Вважаємо, що саме це забезпечує знання методичних підходів до розвитку навичок цифрової безпеки учнів.

Показник «П3: Уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки у учнів»

Для визначення сформованості предметно-методичного компонента готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу ми використали показник «Уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки у учнів».

Методикою оцінки цього показника було розв'язування практико-орієнтованої задачі «Розроблення уроку з аналізу кіберзагроз та безпечного поведінки в Інтернеті» (рис. 3.9).

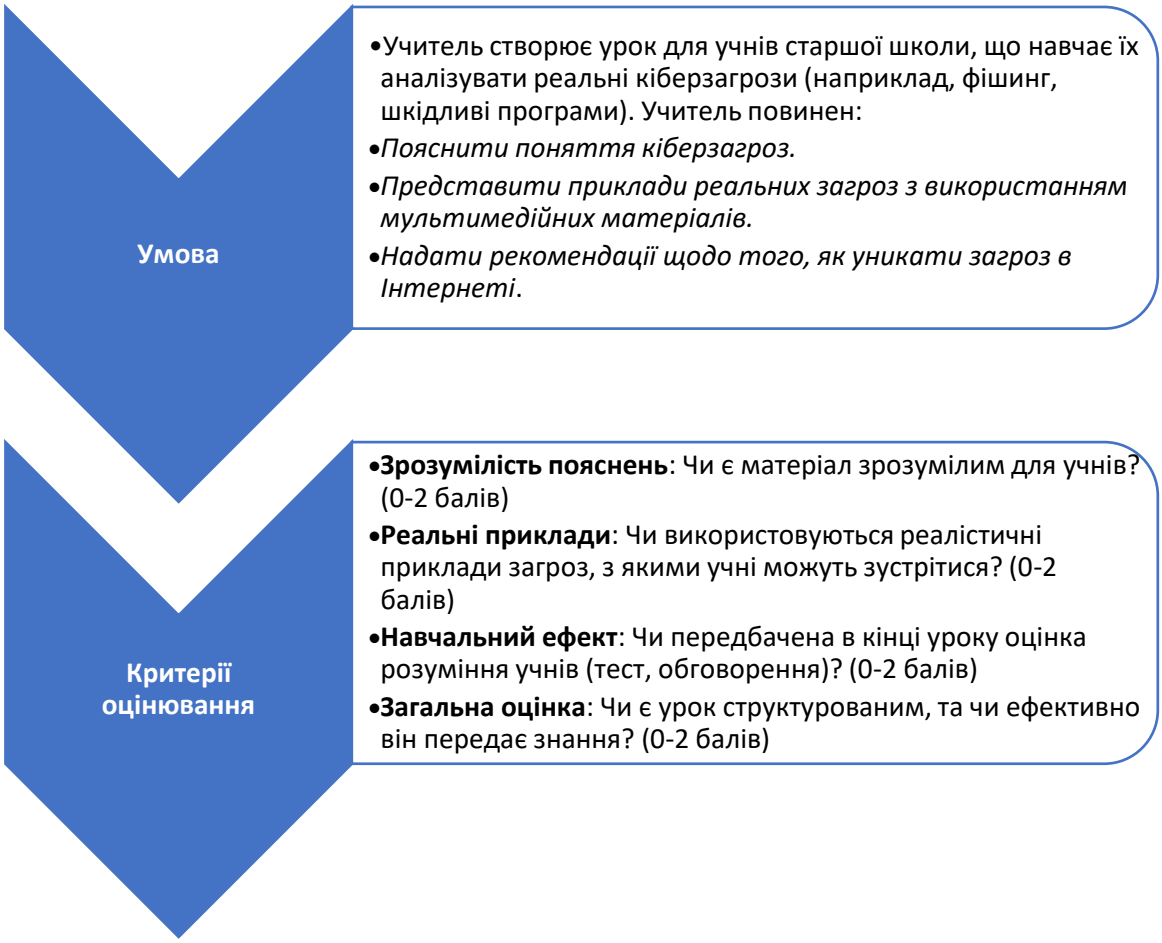


Рис. 3.9. Практико-орієнтована задача «Розроблення уроку з аналізу цифрових загроз та безпечного поведінки в Інтернеті» та критерії її оцінювання

Максимальна оцінка, яку міг отримати студент за розв'язання задачі, - 8 балів. На її розв'язання відводилося одне заняття (рис.3.10).

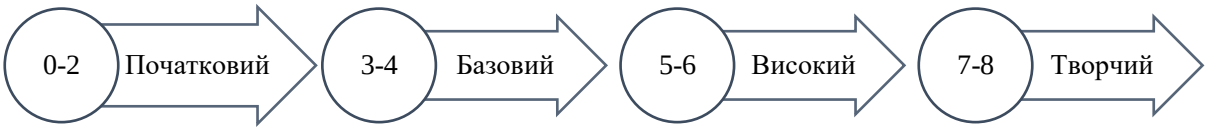


Рис. 3.10. Розподіл балів за тестування

Загальні результати, одержані студентами на початку та в кінці педагогічного експерименту, подані у табл. 3.7 та на рис. 3.11-3.12.

Таблиця 3.7

Розподіл рівнів за показником ПЗ на початку та в кінці експерименту

Рівні		Початковий рівень	Базовий рівень	Високий рівень	Творчий рівень
КГ	*до*	47%	50%	3%	0%
	після	42%	54%	4%	0%
ЕГ	*до*	47%	52%	1%	0%
	після	28%	59%	10%	3%

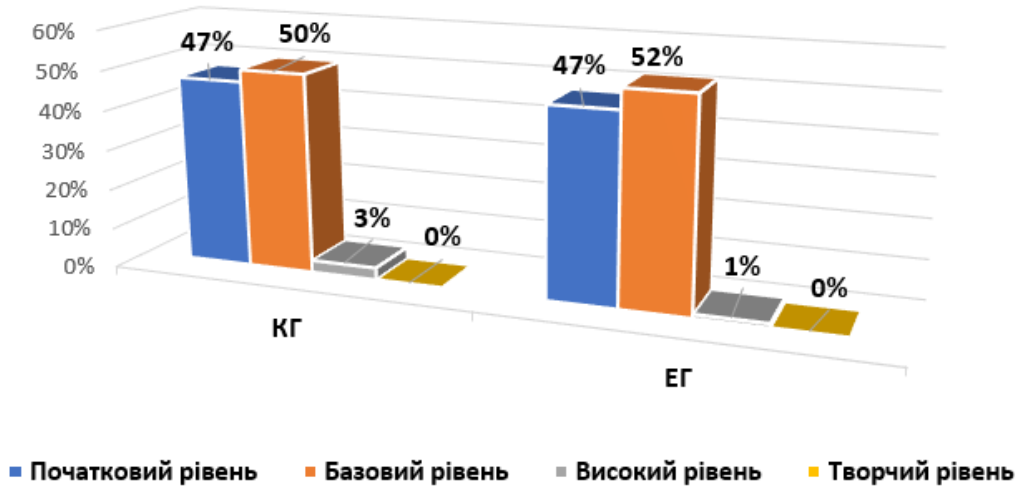


Рис.3.11. Розподіл рівнів за показником ПЗ на початку експерименту

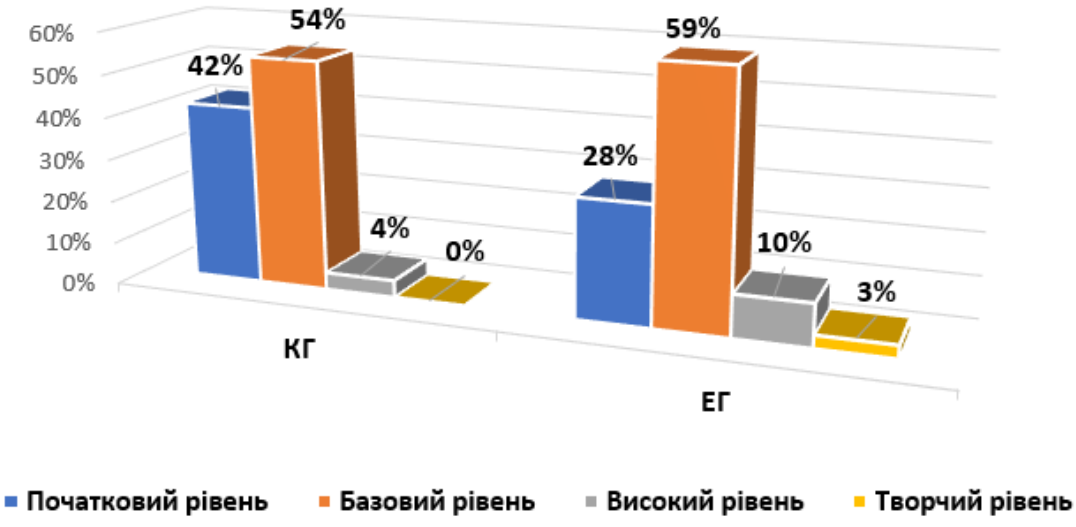


Рис.3.12. Розподіл рівнів за показником ПЗ в кінці експерименту

Аналіз даних описової статистики підтвердив нормальність розподілів у обох вибірках. Перевірка статистичної подібності середніх для вибірок за критерієм Стьюдента з використанням статистичних функцій MS Excel представлена у таблиці (табл.3.8).

Таблиця 3.8.

Оцінка середніх для показника П3
на початку та в кінці експерименту (%)

Двовибірковий t-тест з різними дисперсіями	**КГ**	**ЕГ**		**КГ**	**ЕГ**
Середнє	2,63	2,52		2,69	3,59
Різниця середніх для гіпотези H_0	0			0	
t-статистика (експериментальне)	0,31			-2,34	
t критичне двостороннє	1,97			1,97	

Розрахунки свідчать, що на початку експерименту вибірки були статистично однаковими до експерименту ($T_{крит.}$ = 1,97 більше за $T_{експ.}$ = 0,31), а в кінці експерименту вони показали статистичну розбіжність($T_{крит.}$ = 1,97 менше за модуль $T_{експ.}$ = -2,34). Іншими словами, в у групах ЕГ і КГ на рівні значущості 0,05 для показника «Уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки у учнів» маємо вищі середні, а, отже, вищі показники сформованості предметно-методичного компонента готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу, що пояснюємо обраними змістом і методами навчання спецкурсу. Зокрема, для формування умінь студентів добирати методи і засоби навчання для розвитку навичок цифрової безпеки у учнів вважаємо ефективним впровадження проєктної діяльності, коли студенти виконують методичні проєкти з розроблення методичних рекомендацій з навчання учнів цифрової безпеки, розробляють міждисциплінарні сценарії заходів з популяризації цифрових небезпек та методів їх уникнення.

Вважаємо, що на результат за показником П3 позитивно вплинула рефлексія та аналіз ефективності вивчення модулів. Доцільним виявилося проводити самооцінювання та обговорення після кожного модуля курсу (що спрацювало найкраще? як можна покращити методику навчання цифрової безпеки?) та аналізувати педагогічний досвід інших учителів, які вже мають позитивні навчальні практики. Це розвивало у студентів уміння критично оцінювати та адаптувати методики навчання цифрової безпеки.

Показник «П4: Прагнення до професійного розвитку в галузі цифрової безпеки»

Для визначення рівня сформованості у майбутніх учителів інформатики готовності до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу за показником «Прагнення до професійного розвитку в галузі цифрової безпеки» було проведено анкетування. Приклади запитань наведені на рисунку (рис.3.13).

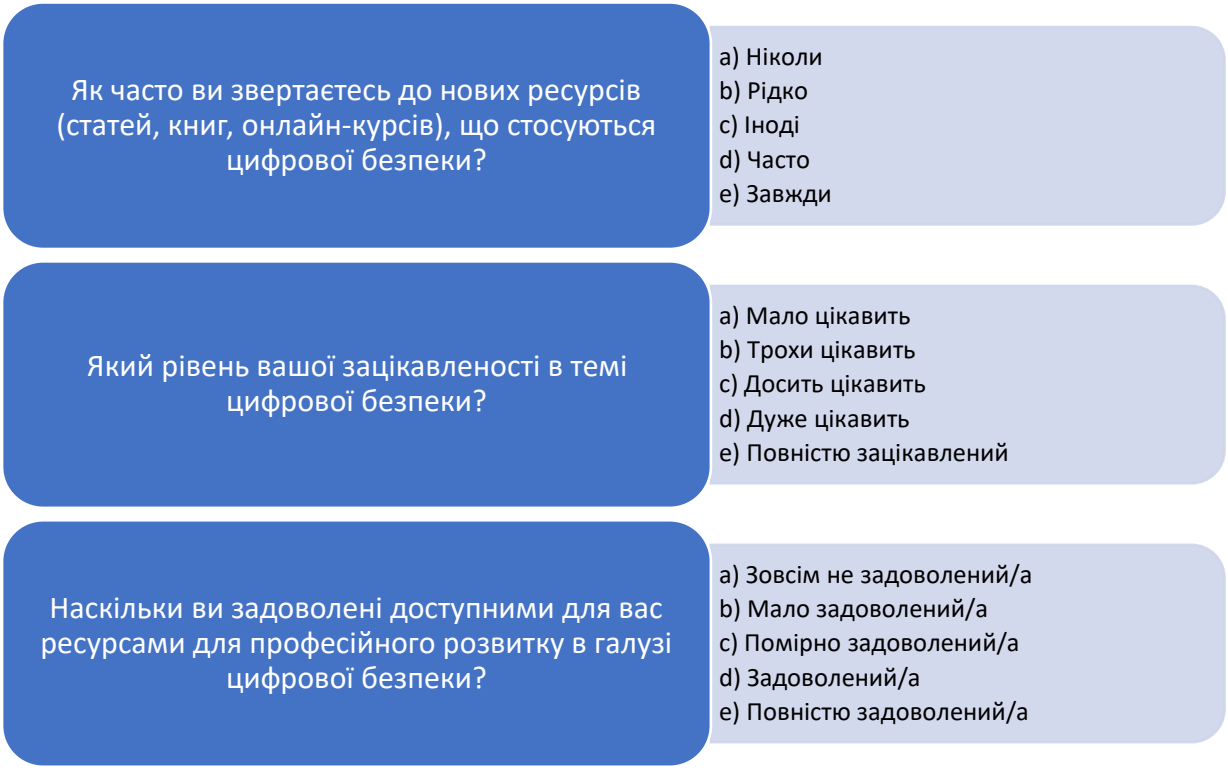


Рис. 3.13. Приклади запитань анкети (показник П4)

Анкета повністю представлена у додатку Е. Відповіді оцінювалися за школою Лайкерта від 1 (абсолютно ні) до 5 (абсолютно, так). Максимальна кількість балів - 35 балів, які були розподілені за рівнями (рис.3.14).

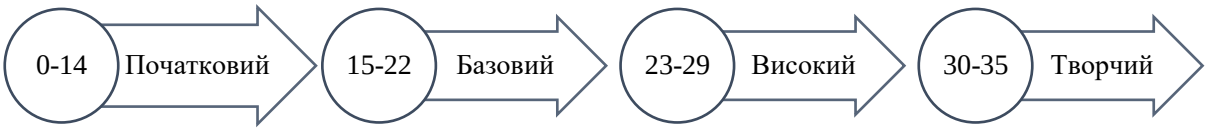


Рис. 3.14. Розподіл балів за рівнями для показника П4

Анкетування проводилося на початку та в кінці експерименту. Для емпіричних даних рахувалися показники описової статистики. Ексцес і асиметрія були за модулем менше одиниці, що підтверджувало нормальність розподілу і дозволяло використати критерій Стьюдента оцінки середніх. Загальні результати, одержані на початку та в кінці педагогічного експерименту, подані у табл. 3.9 та на рис. 3.15-3.16.

Таблиця 3.9

Розподіл рівнів за показником П4
на початку та в кінці експерименту (%)

Рівні		**Початковий рівень**	**Базовий рівень**	**Високий рівень**	**Творчий рівень**
КГ	*до*	37%	51%	12%	0%
	після	31%	54%	14%	1%
ЕГ	*до*	38%	50%	11%	1%
	після	29%	52%	14%	5%

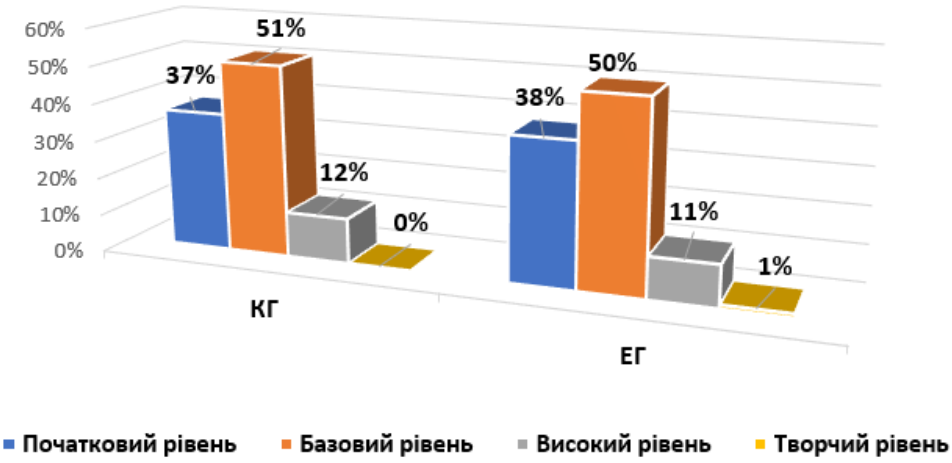


Рис.3.15. Розподіл рівнів за показником П4 на початку експерименту

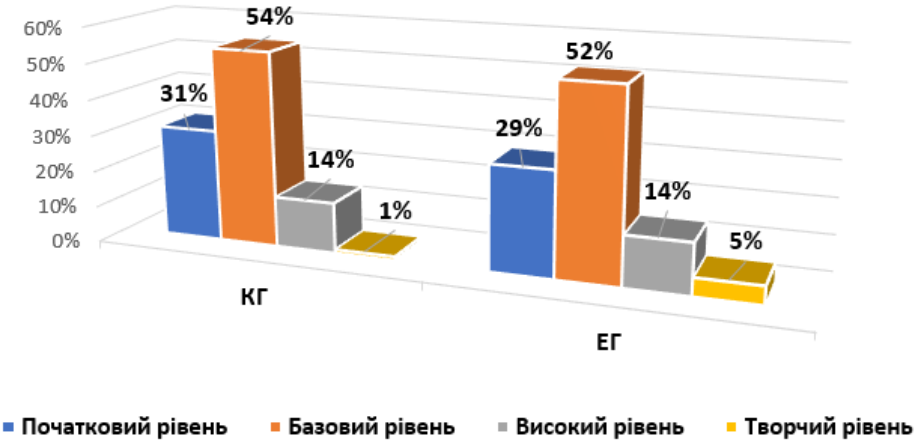


Рис.3.16. Розподіл рівнів за показником П4 в кінці експерименту

Розрахунки за критерієм Стьюдента з використанням статистичних функцій MS Excel подані у таблиці (табл.3.10).

Таблиця 3.10.

Оцінка середніх для показника П4 на початку та в кінці експерименту

Двовибірковий t-тест з різними дисперсіями	**КГ**	**ЕГ**		**КГ**	**ЕГ**
Середнє	16,63	15,85		17,34	20,37
Різниця середніх для гіпотези H_0	0			0	
t-статистика (експериментальне)	0,56			-2,11	
t критичне двостороннє	1,97			1,97	

Зіставлення розрахованих статистик підтвердила однаковість вибірок КГ і ЕК на початку експерименту (на рівні значущості 0,05 значення $T_{крит.}$ = 1,97 більше за $T_{експ.}$ = 0,56) і їхню статистичну різницю наприкінці експерименту ($T_{крит.}$ = 1,97 менше за модуль $T_{експ.}$ = -2,11). Тому маємо підстави зробити висновок, що для показника «Прагнення до професійного розвитку в галузі цифрової безпеки» розроблена модель дала позитивні зрушення щодо сформованості особистісного компоненту готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

Вважаємо, що цьому сприяли обрані засоби та підходи до вивчення спецкурсу, які були орієнтовані на усвідомлення цінності знань та вмінь в галузі цифрової безпеки, де можливе й важливе професійне зростання, на ознайомлення студентів із міжнародними сертифікаційними програмами з кібербезпеки (*CompTIA Security+*, *Certified Ethical Hacker (CEH)*, *Google Cybersecurity Certificate*). Також вважаємо дієвими рефлексії та побудову індивідуальних траєкторій розвитку в галузі цифрової безпеки, які ми реалізовували наприкінці практичних занять через самооцінювання (що я вже знаю про цифрову безпеку? В яких напрямах я хочу розвиватися? Який індивідуальний освітній маршрут я собі обираю (наприклад, викладання цифрової безпеки, розробка навчальних курсів, практична кібербезпека). Вважаємо, що персоналізоване навчання також стимулювало бажання професійного розвитку.

Загальна динаміка

Загальну динаміку рівнів сформованості у майбутніх учителів інформатики готовності до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу за кожним із показників наведено в табл. 3.11.

Таблиця 3.11.

Динаміка рівнів готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу у ЕГ і КГ (%)

Критерій та показник	*Рівні сформованості*	*КГ*	*ЕГ*
Спонукальний критерій			
Показник «Ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів»	початковий	-4%	-15%
	базовий	4%	10%
	високий	-1%	1%
	творчий	1%	4%
Компетентісний критерій			
Показник «Знання методичних підходів до розвитку цифрової безпеки учнів»	початковий	-6%	-17%
	базовий	2%	9%
	високий	3%	5%
	творчий	1%	3%
Показник «Уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки у учнів»	початковий	-5%	-19%
	базовий	4%	7%
	високий	1%	9%
	творчий	0%	3%
Поведінковий критерій			
Показник «Прагнення до професійного розвитку в галузі цифрової безпеки»	початковий	-6%	-9%
	базовий	3%	2%
	високий	2%	3%
	творчий	1%	4%

Отже, проведений педагогічний експеримент підтвердив позитивні зрушення середніх для ЕГ по відношенню до КГ, причому за кожним із показників. Для ЕГ найбільшої динаміки набув предметно-методичний

компонент готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів – обидва показники (П2 і П3) продемонстрували значне зростання: початковий рівень показника «Уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки у учнів» (він склав «-19%», який переріс у «+7%» базового, «+9%» високого й «+3%» творчого рівнів) та початковий рівень для показника «Знання методичних підходів до розвитку цифрової безпеки учнів» (він склав «-17%», який переріс у «+9%» базового, «+5%» високого й «+3%» творчого рівнів). Найнижчу, але позитивну, динаміку зафіксовано для показника «Прагнення до професійного розвитку в галузі кібербезпеки» (зсув на +9%).

Виявлені в ході дослідження проблеми (розділ 1) і результати (розділ 3) дали можливість сформулювати рекомендації щодо вдосконалення відповідних освітніх програм.

Освітнім (освітньо-професійним та освітньо-науковим) програмам часто бракує глибини та широти, необхідної для ефективного навчання майбутніми вчителями інформатики учнів цифрової безпеки. Тому вдосконалення освітніх програм підготовки вчителів має передбачати не лише формування теоретичних знань, але й практичних умінь, що можливе на основі упровадження окремого, бажано нормативного, освітнього компоненту освітньої програми підготовки вчителів інформатики.

По-перше, такий освітній компонент не має бути зосереджений виключно на навчанні цифрової безпеки як технічної дисципліни. Як окремий курс, він повинен заглиблюватися в ефективні методики навчання часто складних і абстрактних ідей та понять цифрової безпеки. Курс має надати майбутнім учителям знання для розробки цікавих уроків, що відповідають віку, сформувати уміння оцінювати розуміння учнів цифрових загроз і цифрової безпеки, їхню спроможність уникати цифрових загроз. Такий освітній компонент дозволить більш глибоко вивчати проблеми цифрової безпеки та особливості формування відповідних навичок в учнів.

По-друге, лінія формування навичок цифрової безпеки може бути інтегрована в наявні курси професійної підготовки (різні освітні компоненти) для забезпечення успішного формування відповідних знань та навичок у галузі цифрової безпеки. Ця інтеграція освітніх компонентів не повинна обмежуватися технічними аспектами цифрової безпеки. Вона має включати етичні міркування, правові рамки та соціальні наслідки. Такий підхід гарантуватиме, що цифрова безпека сприйматиметься майбутніми учителями не як ізольована дисципліна, а як невід'ємна частина навчання інформатики.

По-третє, такий освітній компонент має передбачати різноманітні методи та інформаційні ресурси для їх подальшого перенесення у професійну практику майбутнього вчителя інформатики. Це може включати конспекти практичних занять, симуляції, розроблені кейси та проєктні дослідження різних проблем , щоб зробити освітній процес більш цікавим і актуальним.

Відзначаємо важливість постійного професійного розвитку вчителів у сфері цифрової безпеки. Характер цифрової безпеки, яка швидко розвивається в умовах надшвидкого розвитку ІТ, вимагає постійного професійного розвитку як безперервного процесу навчання, постійного вдосконалення методики навчання, особливо в контексті еволюції ІТ галузі. Тому бачиться доцільним проведення регулярних семінарів / тренінгів для інформування майбутніх вчителів про останні виявлені загрози, вразливості та ефективні методи уникнення цифрових загроз. Такі заняття мають бути зосереджені на розумінні/ опануванні нових загроз та інформаційної підтримки її викладання для різних вікових груп учнів, проведенні практикумів із виявлення і попередження нових цифрових загроз у своїй практиці викладання. Заняття, які передбачають можливості для вчителів поділитися своїм досвідом з колегами сприяють створенню продуктивного навчального середовища.

По-друге, майбутнім учителям має бути забезпечений доступ до онлайн-ресурсів. Це дозволило б їм бути в курсі останніх подій та отримати консультаційну підтримку від експертів. Створення і підтримка онлайн-форумів, можливо, з використанням існуючих платформ, таких як Moodle,

могли б сприяти навчанню за принципом «рівний-рівному» та обміну ефективними практиками.

По-третє, бачимо доцільними програми наставництва для об’єднання досвідчених викладачів або фахівців ІТ-галузі з тими, хто тільки знайомиться з проблемами цифрової безпеки. Такі програми нададуть можливість навчатися у професіоналів та отримувати персоналізовані рекомендації. Наставники можуть надати підтримку, зворотний зв’язок та рекомендації щодо інтеграції концепцій цифрової безпеки у викладацьку практику.

Забезпечення актуальних знань в галузі цифрової безпеки потребує співпраці між освітніми установами та професіоналами з ІТ-сфери. Надшвидкий розвиток цифрових загроз вимагає партнерства для подолання розриву між академічними знаннями та реальною практикою. По-перше, створення консультативних рад, може сприяти поширенню інформацію про поточні виклики цифрової безпеки та позитивні практики її забезпечення. Члени ради можуть допомогти розробити освітню програму або ж її компонент із дотриманням відповідності галузевим потребам і стандартам. Залучення професіоналів ІТ-галузі до розробки освітніх програм може гарантувати, що навички, які формуються освітньою програмою, безпосередньо застосовні до реальних ситуацій життя.

По-друге, слід передбачити регулярні стажування та можливості інтегрованого навчання, щоб надати студентам практичний досвід у сфері цифрової безпеки. Це дозволить студентам не лише поглиблювати й осучаснювати свої знання в галузі цифрової безпеки, але й отримати досвід під наставництвом професіоналів ІТ-галузі, що значно покращить розуміння викликів і складнощів, пов’язаних із цифровою безпекою.

По-третє, спільні дослідницькі проєкти між освітніми установами та промисловістю можуть призвести до розробки інноваційних навчальних матеріалів та ресурсів. Об’єднаний (спільний) підхід гарантує, що освітня програма залишатиметься актуальною та затребуваною, забезпечуючи майбутніх учителів знаннями та навичками, необхідними для підготовки своїх

учнів до викликів цифрової епохи. Такі партнерства можуть призвести до розробки важливих ресурсів, таких як навчальні онлайн-модулі або інтерактивні симуляції, які можуть бути широко поширені в освітній галузі.

Висновки до розділу 3

У третьому розділі «Експериментальна перевірка ефективності моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу» розроблено діагностичний інструментарій дослідження та експериментально перевірено ефективність моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

На основі структурно-логічного аналізу з урахуванням означення категорії «готовність майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів» та характеристики її компонентів було розроблено критерії та показники сформованості мотиваційного, предметно-методичного та особистісного компонентів готовності. У дослідженні використано спонукальний, компетентісний і поведінковий критерії, які увиразнюються чотирма показниками: «П1: ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів»; «П2: знання методичних підходів для розвитку навичок цифрової безпеки»; «п3: уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки в учнів»; «П3: прагнення до професійного розвитку в галузі цифрової безпеки».

У дослідженні з використанням порівняльного аналізу схарактеризовано чотири рівні готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів.

Початковий рівень. Студенти демонструють обмежене розуміння основ цифрової безпеки та методів її формування у учнів. Вони мають поверхневе уявлення про важливість цієї теми, але не в змозі застосувати основні стратегії

на практиці. Методичні знання та вміння потребують значного удосконалення, а також розширення розуміння технологій, що використовуються для навчання. Студенти не мають достатньої мотивації до розвитку в цій сфері.

Базовий рівень. Студенти здатний застосовувати базові знання та методи для формування навичок цифрової безпеки у учнів, однак часто потребують методичної підтримки. Вони можуть обґрунтувати важливість цієї теми для учнів, застосовувати деякі методичні стратегії на практиці, але їх знання та вміння ще обмежені. Мотивація до професійного розвитку існує, але проявляється на мінімальному рівні. Студенти демонструють зацікавленість в удосконаленні своїх навичок, хоча й не завжди активно шукають нові можливості для професійного зростання.

Високий рівень. Студенти мають добре сформовані знання та навички для формування навичок цифрової безпеки у учнів. Вони активно застосовують методи навчання та здатні адаптувати стратегії до різних ситуацій. Мотивація до розвитку у сфері цифрової безпеки є стійкою та усвідомленою, що відображається в участі в додаткових навчальних заходах та самостійному удосконаленні своїх професійних навичок. Вони можуть запропонувати ефективні підходи для інтеграції цифрової безпеки в навчальний процес.

Творчий рівень. Студенти демонструють високу здатність до інновацій у розвитку навичок цифрової безпеки у учнів. Вони не лише застосовують наявні методи, але й розробляють нові підходи, активно експериментують із різними цифровими інструментами для навчання. Мотивація до професійного розвитку є внутрішньою та постійно зростає. Студенти ініціативно шукають нові ресурси, беруть участь у наукових чи практичних заходах і готові до впровадження інновацій у освітньому процесі.

Представлено коротко поетапний перебіг процесу дослідження: на першому етапі було здійснено теоретичний і практичний аналіз та обґрунтування проблеми дослідження, виявлено наявні суперечності для уточнення предмету дослідження, а також розроблено науковий апарат

дослідження та відповідний тезаурус; на другому етапі розроблено і обґрунтовано модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу; третій етап визначався експериментальним упровадженням моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу; на заключному, четвертому етапі, проведено статистичний аналіз даних та зроблено якісні висновки.

Педагогічний експеримент як провідний метод науково-педагогічного дослідження використаний для підтвердження теоретичних висновків через статистичні методи. Зібрані в ході педагогічний експерименту емпіричні дані за всіма показниками підтвердили позитивні зрушення середніх для ЕГ по відношенню до КГ: найбільшу динаміку в ЕГ набув предметно-методичний компонент готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів – обидва показники («П2: Знання методичних підходів до розвитку цифрової безпеки учнів» і «П3: Уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки у учнів») продемонстрували суттєве зростання середніх (9,07 і 2,52 проти 12,22 і 3,59 відповідно). Статистичний аналіз підтвердив основне припущення нашого дослідження про ефективність розробленої моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

Виявлені в ході дослідження проблеми й отримані результати дали підстави для формулювання рекомендацій розробникам та викладачам, які реалізують освітні програми підготовки вчителів інформатики. Зокрема, відсутність послідовної та ефективної політики в галузі цифрової безпеки в освітніх програмах підготовки учителів інформатики може мати відтерміновані негативні наслідки. Інтеграція курсів з цифрової безпеки в освітні програми підготовки вчителів інформатики має вийти за рамки ізольованих вибіркових або факультативних курсів і стати нормативним

компонентом освітньої програми, а освітні установи повинні розвивати культуру безперервного навчання для професійного розвитку в галузі цифрової безпеки

Отже, в розділі подано вирішення останнього, п’ятого, завдання дослідження. Основні наукові результати представлені у публікаціях [1], [5], [10] (згідно з додатком Є).

ВИСНОВКИ

У дисертації запропоновано розв’язання наукової проблеми формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу, яке дало можливість отримати нові наукові результати та сформулювати такі висновки.

1. Охарактеризовано цифрові загрози і відповідні навички цифрової безпеки молоді та доведено важливість їх розвитку в умовах інформаційного суспільства. Під цифровими загрозами сьогодні розуміють широкий спектр загроз, пов’язаних з використанням цифрових технологій. Класифікація цифрових відбувається сьогодні за різними критеріями, включаючи їхню природу, ціль та метод атаки. Розмаїття джерел цифрових загроз є досить широким і включає різні фактори (кіберзлочинці; malware; вразливості в програмному забезпеченні; людський фактор). Цифрові загрози поділяють на навмисні (зловмисні) і ненавмисні небезпеки за такою класифікацією: витік та крадіжка даних, зловмисне програмне забезпечення та програми-вимагачі, фішинг та соціальна інженерія, DDoS-атаки; системні збої та помилки.

Під навичками цифрової безпеки розуміють сукупність знань та умінь для безпечного, відповідального та етичного використання цифрових технологій, яка забезпечує особі захист особистих даних, цифрової ідентичності, пристроїв і мереж від кібератак, а також сприяє свідомому онлайн-спілкуванню. Серед дієвих шляхів розвитку навичок цифрової безпеки молоді сьогодні науковці відзначають підтримку цифрової грамотності, популяризацію знань про цифрові загрози, формування навичок цифрової безпеки ще зі школи. Тому необхідною є відповідна і завчасна підготовка вчителів інформатики.

2. Проведено оцінку стан розробленості проблеми підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів. Теоретичний стан розробленості проблеми засвідчив наявність наукових розвідок щодо зростаючої потреби в розвитку цифрової грамотності, особливо щодо цифрової безпеки. Практичний стан розробленості проблеми підготовки

вчителів інформатики до розвитку навичок цифрової безпеки учнів виявив: диспропорцію освітніх програм щодо навчання в галузі цифрової безпеки; наявність прогалин у знаннях та уміннях здобувачів освіти, пов'язаних із цифровою безпекою; відсутність спеціальної підготовки викладачів з цифрової безпеки при реалізації освітньо-професійних програм; відсутність акценту на практичному навчанні цифрової безпеки; відсутність чітких керівних принципів та політик закладу освіти; проблема ефективного оцінювання навичок цифрової безпеки; проблема пошуку ефективних методик навчання.

Серед можливих шляхів модернізації програм підготовки вчителів для розвитку в учнів навичок цифрової безпеки відзначаються: інтеграція цифрової безпеки в курси з методики навчання інформатики; розробка й упровадження спеціалізованих курсів з цифрової безпеки у освітньо-професійні програми підготовки вчителів; використання цифрових інструментів та технологій симуляції для формування практичних навичок цифрової безпеки; сприяння співпраці та обміну знаннями з професіоналами; приведення навчальних програм у відповідність до міжнародних стандартів.

3. Уточнено сутність і структуру готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів. Так, сутність поняття «готовність учителів інформатики до розвитку навичок цифрової безпеки учнів» визначено як інтегративну особистісну здатність майбутнього вчителя інформатики розвивати навички цифрової безпеки учнів, яка поєднує: усвідомлені прагнення такого розвитку; специфічні знання й уміння; навички рефлексії щодо успішності такого розвитку. Означене поняття розглядається у єдності трьох компонентів: мотиваційного (прагнення розвитку навичок цифрової безпеки учнів), предметно-методичного (специфічні знання й уміння в галузі цифрової безпеки та підходів, форм, методів, засобів для ефективного розвитку навичок цифрової безпеки учнів), особистісного (навички рефлексії щодо успішності розвитку навичок цифрової безпеки учнів).

4. Розроблено й теоретично обгрунтовано процес формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу. Авторська модель базується на інформаційному підході, оскільки він дозволяє майбутнім учителям опанувати принципи безпечної взаємодії в цифровому середовищі, критичного аналізу інформації, захисту персональних даних та етичного використання цифрових ресурсів. Реалізація моделі передбачає дотримання принципів (науковість та актуальність, системність, компетентісна орієнтованість, практико-орієнтованість, інтеграція та міждисциплінарність) при організації навчання. Основним змістом, на якому побудовано модель, виступає авторський спецкурс «Цифрова безпека у навчальному середовищі», який передбачає реалізацію у традиційній формі (лекції, практичні заняття) з використанням активних і проблемних методів навчання та різних цифрових засобів навчання (цифрові навчальні середовища, цифрові освітні ресурси та програми спеціалізованого спрямування).

5. Розроблено діагностичний інструментарій дослідження та експериментально перевірено ефективність моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу. Діагностичний апарат дослідження включає критерії (спонукальний, компетентісний і поведінковий), які увиразнюються чотирма показниками: ступінь усвідомленості потреби розвитку навичок цифрової безпеки учнів; знання методичних підходів для розвитку навичок цифрової безпеки; уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки учнів; прагнення до професійного розвитку в галузі цифрової безпеки. Готовність майбутнього вчителя інформатики до розвитку навичок цифрової безпеки учнів як особистісна якість розглядається на чотирьох рівнях свого розвитку: початковий, базовий, високий, творчий.

Проведений педагогічний експеримент підтвердив позитивні зрушення середніх для ЕГ по відношенню до КГ, причому за кожним із показників. Для

ЕГ найбільшої динаміки набув предметно-методичний компонент готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів – обидва показники (П2 і П3) продемонстрували значне зростання: початковий рівень показника «Уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки у учнів» (він склав «-19%», який переріс у «+7%» базового, «+9%» високого й «+3%» творчого рівнів) та початковий рівень для показника «Знання методичних підходів до розвитку цифрової безпеки учнів» (він склав «-17%», який переріс у «+9%» базового, «+5%» високого й «+3%» творчого рівнів). Найнижчу, але позитивну, динаміку зафіксовано для показника «Прагнення до професійного розвитку в галузі цифрової безпеки» (зсув на +9%).

Проведене дослідження не вичерпує усіх проблем, виявлених у ході його реалізації. Актуальними напрямами подальших досліджень вбачаємо: дослідження моделей розвитку інформаційної/ цифрової грамотності/ цифрової компетентності / цифрової культури вчителя, які включають навички цифрової безпеки в різних умовах його підготовки (неформальна освіта, мобільне навчання, післядипломна освіта); напрацювання технологій створення безпечного цифрового середовища, орієнтованого на розвиток навичок цифрової безпеки майбутніх учителів інформатики; дослідження ефективності різних методичних підходів до навчання цифрової безпеки учнів (для розвитку в учнів навичок безпечної поведінки в інтернеті, включаючи використання цифрових інструментів та технологій симуляції).

Бачимо доцільним проводити крос-культурні порівняння, щоб зрозуміти, як варіюється готовність вчителів до розвитку навичок цифрової безпеки учнів у різних освітніх системах (освітніх системах різних рівнів освіти; освітніх системах різних країн). Такі дослідження мають виявити ефективність різних педагогічних підходів для формування навичок цифрової безпеки. Цікавим уявляється дослідження участі батьків та залучення громади для підтримки освіти в галузі цифрової безпеки та її популяризації.

Також корисним вважаємо детальний аналіз конкретних проблем, з якими стикаються вчителі з урахуванням різних умов їх професійної діяльності (наприклад, сільські та міські школи, різні рівні освіти).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Almehmadi, G.(2023). The Interactive of E-Learning Unit to employ The Students Skills in Cyber Security According to Determinates of Digital Citizenship, *Journal of Umm Al-Qura University for Educational and Psychological Sciences, 15*(1), pp. 142-165. https://doi.org/10.54940/ep89401679.

2. Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability*, *15*(15), 11512. https://doi.org/10.3390/su151511512.

3. Amin, M. (2024). The Importance of Cybersecurity and Protecting of Digital Assets and Understanding the Role of Cybersecurity Laws in Safeguarding Digital Assets. *Indian Journal of Public Administration*, *70*(3), 493-501. https://doi.org/10.1177/00195561241271520.

4. Ata, R., & Yıldırım, K. (2019). Turkish pre-service teachers' perceptions of digital citizenship in education programs. *Journal of Information Technology Education: Research*, *18*, 419-438. https://doi.org/10.28945/4392.

5. Ayanwale, M. A., Adelana, O. P., Ishola, A. M., & Adeeko, O. (2024). Education 4.0: Exploring computer science teachers' readiness. *Eurasia Journal of Mathematics, Science and Technology Education*, *20*(8), em2492. https://doi.org/10.29333/ejmste/14918

6. Aydın, M., & Çelik, T. (2021). Impact of the Digital Literacy Courses Taken by the Prospective Social Studies Teachers by Distance Learning on Digital Citizenship Skills. *Research on Education and Media*, *12*(1), 42–57. https://doi.org/10.2478/rem-2020-0006

7. Baghdasarin, D. (2019). MRO Cybersecurity SWOT. *International Journal of Aviation, Aeronautics, and Aerospace, 6*(1). https://doi.org/10.15394/ijaaa.2019.1318.

8. Bakov, K. (June 2024). The New Realities in Synchronizing Physical Security and Cybersecurity in Digital Societies. *Security and Defense*(1), 75-93. https://doi.org/10.70265/GRGI5006.

9. Bandapelli, A., Prasad, D. S. ., & Kethar, J. (2024). The Importance of Cybersecurity Measures in Business Operations to Combat Phishing Attacks. *Journal of Student Research*, *13*(2). https://doi.org/10.47611/jsrhs.v13i2.6783.

10. Bellatti, I., Sabido Codina, J., Sosa, L., & Hurtado Torres, D. (2023). La enseñanza de las ciencias sociales para una ciudadanía digital. Estudio interdisciplinar sobre alfabetización mediática en los currículos de Educación Secundaria. *Áreas. Revista Internacional de Ciencias Sociales*, (45), 75–88. https://doi.org/10.6018/areas.528641.

11. Bendechache, M., Tal, I., Wall, P., Grehan, L., Clarke, E., Odriscoll, A., Der Haegen, L. V., Leong, B., Kearns, A., & Brennan, R. (2021). AI in My Life: AI, Ethics & Privacy Workshops for 15-16-Year-Olds. *Companion Publication of the 13th ACM Web Science Conference 2021*, 34–39. https://doi.org/10.1145/3462741.3466664

12. Bhagat C.K.., (2023). Study of Current Cyber Security Threats to Information & Operational Technology (IOT) and Their Effect on E-Governance in Nepal., JUEM 1(1), 41-50. https://doi.org/10.5281/zenodo.8116802.

13. Boer, K. M., Juwita, R., & Nurliah. (2023). Penggunaan Metode Blanded Learning Untuk Meningkatkan Pengetahuan Literasi Digital Mahasiswa Ilmu Komunikasi Fisip Universitas Mulawarman. *IQTIDA : Journal of Da'wah and Communication*, *3*(1), Article 1. https://doi.org/10.28918/iqtida.v3i1.340

14. Canada, C. S. E. (2024, February 15). *Course 623: Introduction to Cyber Security for Educators*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/education-community/learning-hub/courses/623-introduction-cyber-security-educators

15. Cebrián-Robles, V., Ruíz-Rey, F. J., Raposo-Rivas, M., & Cebrián-de-la-Serna, M. (2023). Impact of Digital Contexts in the Training of University Education Students. *Education Sciences*, *13*(9), 923. https://doi.org/10.3390/educsci13090923.

16. Chauvot, J., Gurkan, D., & Horn, C. (2023). Exploring Network Security Educator Knowledge. *Journal of Cybersecurity Education, Research and Practice, 2023*(2). https://doi.org/10.32727/8.2023.20

17. Chesney, B., & Citron, D. (Eds.). (2019). *Deep Fakes: A Looming Challenge for Privacy*. https://doi.org/10.15779/Z38RV0D15J

18. Chong, E. K., & Pao, S. S. (2021). Promoting digital citizenship education in junior secondary schools in Hong Kong: Supporting schools in professional development and action research. *Asian Education and Development Studies*, *11*(4), 677–690. https://doi.org/10.1108/AEDS-09-2020-0219

19. *Computer Science Teacher Training*. (n.d.). Ellipsis Education. Retrieved 14 March 2025, from https://ellipsiseducation.com/computer-science-teacher-training/

20. Conte, M. M., Roman, F., Sacchet, M., Spinello, E., Voicu, D., Rykala, M., & Nikolov, L. (2024). Development of Digital Competencies in Education Through Staff Training Events and International Schools. *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*, 103–108. https://doi.org/10.1109/COMPSAC61105.2024.00024

21. Criterion-Referenced Test Definition. (2014, April 30). *The Glossary of Education Reform*. https://www.edglossary.org.

22. *Cyber Security Unveiled: Trends and Protections in the Digital World – IJSREM*. (n.d.). Retrieved 13 March 2025, from https://ijsrem.com/download/cyber-security-unveiled-trends-and-protections-in-the-digital-world/

23. Damilos, S., Saliakas, S., Karasavvas, D., & Koumoulos, E. P. (2024). An Overview of Tools and Challenges for Safety Evaluation and Exposure Assessment in Industry 4.0. *Applied Sciences*, *14*(10), 4207. https://doi.org/10.3390/app14104207.

24. Diachuk, O. (2024). Development of digital competence of teachers in vocational education institutions. *Scientia et Societus*, *1*(3), Article 3(1). https://doi.org/10.69587/ss/1.2024.77

25. Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society, 21*(5), 712–728. https://doi.org/10.1080/1369118X.2018.1428652.

26. Dubinsky, V. (2024). Training of computer science teachers for the formation of cybersecurity skills in students: actualization of problems and their possible solutions. *Education. Innovation. Practice*, *12*(10), 6–11. https://doi.org/10.31110/2616-650X-vol12i10-001.

27. Earwood, B., Yang, J., & Kim, Y. R. (2021). Effective Learning of Cybersecurity Concepts with Model-Eliciting Activities. *2021 IEEE International Conference on Engineering, Technology & Education (TALE)*, 01–07. https://doi.org/10.1109/TALE52509.2021.9678713

28. Elías, M., Pérez, J., Cassot, M. del R., Carrasco, E. A., Tomljenovic, M., & Zúñiga, E. A. (2022). Development of digital and science, technology, engineering, and mathematics skills in chemistry teacher training. *Frontiers in Education*, *7*. https://doi.org/10.3389/feduc.2022.932609

29. Falloon, G. (2020). From digital literacy to digital competence: The teacher digital competency (TDC) framework. *Educational Technology Research and Development*, *68*(5), 2449–2472. https://doi.org/10.1007/s11423-020-09767-4

30. Falloon, G. (2020). From digital literacy to digital competence: the teacher digital competency (TDC) framework. *Education Tech Research Dev*, 68, 2449–2472. https://doi.org/10.1007/s11423-020-09767-4.

31. Fang, F. (2024). University Data Security Practice Under the Background of Digital Transformation. *2024 3rd International Conference on Artificial Intelligence and Computer Information Technology (AICIT)*, 1–4. https://doi.org/10.1109/AICIT62434.2024.10730168

32. Faris, W. F. ., & Mirajkar, R. R. . (2023). Securing the Digital Perimeter Intrusion Detection for Robust Data Protection in Cybersecurity. *Research Journal of Computer Systems and Engineering*, *4*(1), 84–92. https://doi.org/10.52710/rjcse.66.

33. Feng, L., Li, T., Yu, L., & Dong, Z. (2022). Application of OpenIPMP and Network Teaching Resources in Graduate Student Training. *2022 3rd International Conference on Education, Knowledge and Information Management (ICEKIM)*, 50–53. https://doi.org/10.1109/ICEKIM55072.2022.00019

34. Fojcik, M. K., & Fojcik, M. (2021). Teachers experience with introducing programming in different courses for non-computer science students. *Education and New Developments 2021*, 491–495. https://doi.org/10.36315/2021end104

35. Friend, M., Leftwich, A., Schafer, J. B., Simon, B., & Morrison, B. B. (2021). Teaching the Methods of Teaching CS. *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 459–460. https://doi.org/10.1145/3408877.3432573

36. Gallego-Arrufat, M., Torres-Hernández, N., & Pessoa, T. (2019). Competence of future teachers in the digital security area. *Comunicar*, 61, 57-67. https://doi.org/10.3916/C61-2019-05.

37. Galupa, N. (2006). Variable SYNC Signal Definition for Automata Performance Improvment. *2006 Canadian Conference on Electrical and Computer Engineering*, 779–782. https://doi.org/10.1109/CCECE.2006.277375

38. García-Vandewalle García, J.M., García-Carmona, M., & Trujillo Torres, J.M. (2023). Analysis of digital competence of educators (DigCompEdu) in teacher trainees: the context of Melilla, Spain. *Tech Know Learn*, 28, 585–612. https://doi.org/10.1007/s10758-021-09546-x.

39. Grover, S., & Twarek, B. (2023). A Formative Assessment Literacy Module for K-12 Computer Science Teachers: Need, Design, and Teacher Feedback. *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 2*, 1281. https://doi.org/10.1145/3545947.3576227

40. Guru Rao, C. V., Mohammad Ali Chisty, N., Mishra, S. K., Sathe, M., Rizvi, S., & Soni, M. (2024). Innovations, Difficulties, and Approaches for Next-Generation Cybersecurity: Protecting the Digital Future. *2024 International*

Conference on Trends in Quantum Computing and Emerging Business Technologies, 1–6. https://doi.org/10.1109/TQCEBT59414.2024.10545178

41. Hanim, W. (2024). The Relationship Between Teacher Readiness in Terms of Knowledge, Literacy and Attitudes Towards Digital Transformation. *Online Journal for TVET Practitioners*, *9*(1), Article 1.

42. Haseski, H. İ. (2020). Cyber Security Skills of Pre-Service Teachers as a Factor in Computer-Assisted Education. *International Journal of Research in Education and Science*, 484–500. https://doi.org/10.46328/ijres.v6i3.1006.

43. Hedzyk, A., Shuliak, A., & Hedzyk, A. (2020). Using the Project Method during the Graphic Training of Future Computer Science Teachers. *Universal Journal of Educational Research*, *8*(12A), 7733–7740. https://doi.org/10.13189/ujer.2020.082560

44. Herath, A., Herath, S., Samarasinghe, P., Herath, J., & Herath, S. (2005). Computer forensics, information security and law: A case study. *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, 135–141. https://doi.org/10.1109/SADFE.2005.7

45. Howard, S. K., Tondeur, J., Ma, J., & Yang, J. (2021). What makes a 'good' digital teacher? A qualitative study exploring instructional behaviors and student perceptions in online learning environments. *Computers & Education*, 168, 104237. https://doi.org/10.1016/j.compedu.2021.104237.

46. Huitt, W. (n.d.). *What Are Educational Indicators and Indicator Systems*? http://www.edpsycinteractive.org.

47. Ihnatenko, O., Tolmachov, V., & Ryabko, A. (2024). Training of future primary school and computer science teachers in the structure of information systems. *Scientific Bulletin of Mukachevo State University. Series "Pedagogy and Psychology", 10*(2), 98-109. https://doi.org/10.52534/msu-pp2.2024.98.

48. Ihnatenko, O., Tolmachov, V., & Ryabko, A. (2024). Training of future primary school and computer science teachers in the structure of information systems. *Scientific Bulletin of Mukachevo State University. Series "Pedagogy and Psychology"*, *2*(10), Article 10(2). https://doi.org/10.52534/msu-pp2.2024.98

49. Israa Akram Alzuabidi. (2024). Building a Resilient Architecture with an Intelligent System Based on Support Vector Machines Algorithm for Cybersecurity. *Journal of Electronics, Computer Networking and Applied Mathematics* , *4*(5), 16–26. https://doi.org/10.55529/jecnam.45.16.26.

50. Jacobs, R., van Laar, J., & Schutte, C. (2022). Strategy to identify and mitigate hazards in deep-level mine ventilation systems using a calibrated digital twin. *The South African Journal of Industrial Engineering*, *33*(3), 204–217. https://doi.org/10.7166/33-3-2795.

51. Jeamaon, A., & Khemapatapan, C. (2022). Cybersecurity Risk Assessment for Insurance in Thailand using Bayesian Network Model. *2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON)*, 257–260. https://doi.org/10.1109/ECTIDAMTNCON53731.2022.9720387.

52. Kamuangu, P. (2024). A Review on Cybersecurity in Fintech: Threats, Solutions, and Future Trends. *Journal of Economics, Finance and Accounting Studies* , *6*(1), 47-53. https://doi.org/10.32996/jefas.2024.6.1.5.

53. Karaman, J., Widaningrum, I., Setyawan, M. B., & Sugianti, S. (2021). Penerapan Model Literasi Digital Berbasis Sekolah Untuk Membangun Konten Positif Pada Internet. *Aksiologiya: Jurnal Pengabdian Kepada Masyarakat*, *5*(1), Article 1. https://doi.org/10.30651/aks.v5i1.3701

54. Karen Issamar, F. H. M., & Roberto, R. L. (2019). New and Emerging Occupational Risks (NER) in Industry 4.0: Literature Review. *2019 7th International Engineering, Sciences and Technology Conference (IESTEC)*, 394–399. https://doi.org/10.1109/IESTEC46403.2019.00078

55. Li, Huifang (2023). An Exploration of Information Technology Security Education and Training Strategies for Higher Education Teaching Services. *Contemporary Education and Teaching Research*, *4*(09), 434-439. https://doi.org/10.61360/BoniCETR232014840904.

56. Li, Y., Liu, C., Sun, J., Zhang, J., Li, X., & Zhang, Z. (2024). The Digital Divide and Cognitive Disparities Among Older Adults: Community-Based Cohort Study in China. *Journal of Medical Internet Research*, *26*(1), e59684. https://doi.org/10.2196/59684

57. Liesaputra, V., Ramirez-Prado, G., Barmada, B., & Song, L. (2020). Future-Proofing Kiwi Kids Through the Use of Digital Technology. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 507–513. https://doi.org/10.1145/3328778.3366902

58. Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age. *An evidence review*. London School of Economics and Political Science. https://doi.org/10.2139/ssrn.3469937.

59. Lo, D. C.-T., & Lawler, B. (2022). Enhance Capacity to Foster Secondary Computer Science Teachers in Multiple Pathways. *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2*, 1157. https://doi.org/10.1145/3478432.3499077

60. Luthfia, A., Handayani, F., Gasa, F. M., Ramadanty, S., & Ridzuan, A. R. (2023). Navigating the Cyber Frontier: Youth Capabilities to Confront Dis/Misinformation with Digital Literacy and Digital Security. *2023 17th International Conference on Telecommunications (ConTEL)*, 1–8. https://doi.org/10.1109/ConTEL58387.2023.10198919

61. Maqsood, S., & Chiasson, S. (2021). "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–17. https://doi.org/10.1145/3411764.3445224

62. Marchisio, M., Roman, F., Sacchet, M., Spinello, E., Nikolov, L., Grzelak, M., & Moldoveanu, M. R. and C.-E. (2022). *Teachers' digital competences before and during the COVID-19 pandemic for the improvement of security and defence higher education*. 68–75. https://www.iadisportal.org/digital-

library/teachers-digital-competences-before-and-during-the-covid-19-pandemic-for-the-improvement-of-security-and-defence-higher-education

63. Martin, F., Ceviker, E., & Gezer, T. (2024). From digital divide to digital equity: Systematic review of two decades of research on educational digital divide factors, dimensions, and interventions. *Journal of Research on Technology in Education*. https://doi.org/10.1080/15391523.2024.2425442

64. *Modelling Learning*. (n.d.). Retrieved 14 March 2025, from https://www.structural-learning.com/post/modelling-learning

65. Mohammed, D., Omar, M., Nguyen, V., Mohammed, D., Omar, M., & Nguyen, V. (2017). *Enhancing Cyber Security for Financial Industry through Compliance and Regulatory Standards* (enhancing-cyber-security-for-financial-industry-through-compliance-and-regulatory-standards) [Chapter]. https://doi.org/10.4018/978-1-5225-0741-3.ch005

66. Mohammed, M., Prasanth, K. K., & Sai Subhash, S. V. (2022). Phishing Detection Using Machine Learning Algorithms. *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 921–924. https://doi.org/10.1109/ICSSIT53264.2022.9716269.

67. Morze, N. V., & Strutynska, O. V. (2023). Advancing educational robotics: competence development for pre-service computer science teachers. *CTE Workshop Proceedings*, *10*, 107-123. https://doi.org/10.55056/cte.549.

68. Mostaghimi, A., Olszewski, A. E., Bell, S. K., Roberts, D. H., & Crotty, B. H. (2017). Erosion of Digital Professionalism During Medical Students' Core Clinical Clerkships. *JMIR Medical Education*, *3*(1), e6879. https://doi.org/10.2196/mededu.6879

69. Naumova, V., & Bulvinska, O. (2024). Управління безпекою учнів в інтернеті: Відкриті освітні ресурси на допомогу освітянам. *Освітологія*, 13(13), 78–90. https://doi.org/10.28925/2412-124X.2024.13.8.

70. *Navigating the Cybersecurity Landscape: Trends, Threats, and Strategies – IJSREM*. (n.d.). Retrieved 13 March 2025, from

https://ijsrem.com/download/navigating-the-cybersecurity-landscape-trends-threats-and-strategies/

71. Ng, D.T.K., Leung, J.K.L., Su, J. et al. (2023). Teachers' AI digital competencies and twenty-first century skills in the post-pandemic world. *Education Tech Research Dev*, 71, 137–161. https://doi.org/10.1007/s11423-023-10203-6.

72. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119.

73. Niyazova, A. Y., Chistyakov, A. A., Volosova, N. Y., Krokhina, J. A., Sokolova, N. L., & Chirkina, S. E. (2023). Evaluation of pre-service teachers' digital skills and ICT competencies in context of the demands of the 21st century. *Online Journal of Communication and Media Technologies, 13*(3), e202337. https://doi.org/10.30935/ojcmt/13355.

74. Nugent, G., Chen, K., Soh, L.-K., Choi, D., Trainin, G., & Smith, W. (2022). Developing K-8 Computer Science Teachers' Content Knowledge, Self-efficacy, and Attitudes through Evidence-based Professional Development. *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*, 540–546. https://doi.org/10.1145/3502718.3524771

75. OECD. (2023). *Digital Security in Education: Ensuring Safe Online Learning Environments.* OECD Publishing. https://doi.org/10.1787/7cb15030-en.

76. Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, *21*(1), 2286–2295. https://doi.org/10.30574/wjarr.2024.21.1.0315.

77. Oliinyk, B. M., & Oleksiuk, V. P. (2024). Social engineering as a component of professional competence in information security of future computer science teachers. *Educational Dimension, 11,* 129-145. https://doi.org/10.55056/ed.778.

78. Olivier, M. S. (2016). On the Morality of Teaching Students IT Crime Skills: Extended Abstract. *Proceedings of the Computer Science Education Research Conference 2016*, 2–3. https://doi.org/10.1145/2998551.2998553

79. Pande, P., Mathur, H., & Gupta, L. K. (2024). Machine Learning-based Intrusion Detection System using Wireless Sensor Networks. *2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, 1–10. https://doi.org/10.1109/ICAECT60202.2024.10469465.

80. Pavan Navandar (2023) Evolving Trends in Cybersecurity: Exploring the Latest Technologies and Strategies. Journal of Mathematical & Computer Applications. SRC/JMCA-207. https://doi.org/10.47363/JMCA/2023(2)172.

81. Port, D., & Kessler, G. C. (2014). Introduction to IS Education and Training Minitrack. *2014 47th Hawaii International Conference on System Sciences*, 4921–4921. https://doi.org/10.1109/HICSS.2014.603

82. Prasetya, D. Y., Suparmin, S., & Johan, A. B. (2019). Application of project based learning learning models to improve student learning results techniques of manufacturing images of vocational school students. *Jurnal Taman Vokasi*, *7*(1), 82–84. https://doi.org/10.30738/jtv.v7i1.4783.

83. Rahim, M. J., Ibn Rahim, M. I., Afroz, A., & Akinola, O. (2024). Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *6*(1), 438–462. https://doi.org/10.60087/jaigs.v6i1.268.

84. Rahmatullah, A. S., Mulyasa, E., Syahrani, S., Pongpalilu, F., & Putri, R. E. (2022). Digital era 4.0: The contribution to education and student psychology. *Linguistics and Culture Review*, *6*(S3), 89-107. https://doi.org/10.21744/lingcure.v6nS3.2064.

85. Ratheeswari, K. (2018). Information Communication Technology in Education. *Journal of Applied and Advanced Research*, S45–S47. https://doi.org/10.21839/jaar.2018.v3iS1.169

86. Raufi, B. R. A. M., & Usmani, M. H. (2024). Physical Security to Cybersecurity (Challenges and Implications in the Modern Digital Landscape). *Journal of Electrical Systems*, *20*(4s), Article 4s. https://doi.org/10.52783/jes.2090

87. Reddy, P., Chaudhary, K., & Hussein, S. (2023). A digital literacy model to narrow the digital literacy skills gap. *Heliyon*, *9*(4). https://doi.org/10.1016/j.heliyon.2023.e14878.

88. Redmond, P. (2019). Student engagement and digital technologies: What the research says. *British Journal of Educational Technology*, *50*(6), 2978-2993. https://doi.org/10.1111/bjet.12832.

89. Rudenko, Y., Ahadzhanova, S., Ahadzhanov-Honsales, K., Bieliaieva, O., Korovai, A., & Semenikhina, O. (2023). Effective Educational Ukrainian Practices of the Formation of Media Literacy. *46th MIPRO ICT and Electronics Convention (MIPRO)*, Opatija, Croatia, 654-659. https://doi.org/10.23919/MIPRO57284.2023.10159822.

90. Rudenko, Y., Ahadzhanov-Honsales, K., Ahadzhanova, S., Batalova, A., Bieliaieva, O., Yurchenko, A., & Semenikhina, O. (2024). Modeling the choice of an online course for information hygiene skills using the Saaty Method. *Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska*, *14*(2), 127–132. https://doi.org/10.35784/iapgos.5691.

91. Rudenko, Y., Ahadzhanov-Honsales, K., Ahadzhanova, S., Batalova, A., Diemientiev, Y., & Semenikhina, O. (2024). Interactive Boards as Digital Tools in the Modern Educational Process. *2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, 329–333. https://doi.org/10.1109/MIPRO60963.2024.10569393

92. Rudenko, Yu., Proshkin, V., Naboka, O., Yurchenko, A., & Semenikhina, O. (2023). Using Bloom's taxonomy to assess information hygiene skills. E-*learning & Artificial Intelligence (AI) Scientific Editor Eugenia Smyrnova-Trybulska "E-learning*", 15, Katowice–Cieszyn, 137–148 https://doi.org/10.34916/el.2023.15.12.

93. Salman, H. A., & Alsajri, A. (2023). The Evolution of Cybersecurity Threats and Strategies for Effective Protection. A review. *SHIFRA, 2023*, 73-85. https://doi.org/10.70470/SHIFRA/2023/009.

94. Salutina, T. Y., Platunina, G. P., & Frank, I. A. (2024). Cybersecurity, Risk Management and Monitoring of Digital and Infocommunication Development of the Company. *2024 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, 1–5. https://doi.org/10.1109/EMCTECH63049.2024.10741653

95. Sena Kurniawan, & Yuni Siti Sarah. (2023). Meningkatkan Literasi Digital di Sekolah Menengah Atas: Tantangan, Strategi dan Dampaknya pada Keterampilan Siswa. *INSOLOGI: Jurnal Sains Dan Teknologi*, *2*(4), 712–718. https://doi.org/10.55123/insologi.v2i4.2321.

96. Shyshenko, I., & Semenikhina, O. (2024). Specific principles of introducing innovations in the professional training of future specialists. *IT and Educational Analytics*, *1*(1), 36-41. https://doi.org/10.31110/ITandEA-v.2024.v1.05

97. Siregar, L., & Siregar, S. (2024). Assessing Teacher Competency and Preparedness for Integrating Digital Media in 21st-Century Education: An Exploratory Review. *AL-ISHLAH: Jurnal Pendidikan, 16*(4), 5794-5804. doi:https://doi.org/10.35445/alishlah.v16i4.5619.

98. Soumya, K. (2024). A literature review on the digital marketing unveiled comprehensive review of core concepts. *EPRA International Journal of Economics, Business and Management Studies (EBMS)*, *11*(7), Article 7. https://doi.org/10.36713/epra17725.

99. Spanou, Despina (2024). The EU Cybersecurity Skills Academy : A silver bullet to address the cyber security skills gap in the European Union?. In the *Cyber Security: A Peer-Reviewed Journal*, Volume 7, Issue 3. https://doi.org/10.69554/KONO7296.

100. Speiser, K., & Teizer, J. (2024). Automatic creation of personalised virtual construction safety training in digital twins. *Proceedings of the Institution of*

Civil Engineers - Management, Procurement and Law, *177*(4), 173–183. https://doi.org/10.1680/jmapl.23.00104.

101. Sushil Mahato, Ranjit Sah, & Sushil Sapkota. (2024). Cybersecurity Challenges and Threats: The Risks in Digital World. *International Journal of Advanced Research in Science, Communication and Technology*, 651–655. https://doi.org/10.48175/IJARSCT-22497

102. Syarova, S., & Toleva-Stoimenova, S. (2023). Cybersecurity Issues in the Secondary and Higher Education Systems' Curricula. *InSITE 2023: Informing Science + IT Education Conferences*, 003.

103. Tabachnick, B. G., & Fidell, L. S. (2019). *Using multivariate statistics* (7th ed.). Pearson.

104. Tan, X., & Wang, H. (2011). Information technology in teacher's professional skill training application. *2011 6th International Conference on Computer Science & Education (ICCSE)*, 365–369. https://doi.org/10.1109/ICCSE.2011.6028656

105. Tang, Y., & Fan, J. (2024). Challenges, Opportunities and Countermeasures of Education and Teaching Management in the Digital Age. *Research and Commentary on Humanities and Arts*, *2*(6), Article 6. https://doi.org/10.18686/rcha.v2i6.4722

106. *The Glossary of Education Reform*. (n.d.). The Glossary of Education Reform. Retrieved 14 March 2025, from https://www.edglossary.org/

107. Thombre, S., & Velankar, M. (2022). Gamification by Students: An effective approach to cyber security concept learning. *Journal of Engineering Education Transformations*, *36*(S1), 73–81. https://doi.org/10.16920/jeet/2022/v36is1/22178

108. Thushari, P. D. (2022). Current security and privacy issues, and concerns of Internet of Things (IoT) and Cloud Computing: A review. *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 13–17. https://doi.org/10.1109/ICCCIS56430.2022.10037730

109. Tobin, M., & Sprague, D. (2008). Towards an Understanding of Educational Indicators. *Policy Futures in Education, 6*(4). https://journals.sagepub.com.

110. Turrohmah, H., & Suryanto, S. (2023). Teacher Readiness for Digital Transformation. *Jurnal EDUCATIO: Jurnal Pendidikan Indonesia, 9*(2), 942-951. http://dx.doi.org/10.29210/1202323284.

111. Twarek, B., Seehorn, D., Friend, M., Mak, J., O'Grady-Cunniff, D., Ray, M., & Sedgwick, V. (2021). Developing Effective and Equitable K-12 Computer Science Teachers. *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 1360. https://doi.org/10.1145/3408877.3439512

112. University of California, Los Angeles. (2021). *Indicators to Measure More and Better Learning Time*. https://docs.rwu.edu.

113. Untawale, Tejaswini (2021). Importance of Cyber Security in Digital Era. *International Journal for Research in Applied Science and Engineering Technology*, *9*(8), 963–966. https://doi.org/10.22214/ijraset.2021.37519

114. Uşaklıoğlu, A. Y. (2020). *The Need Before the Law: Main Issues of Cybersecurity & Law* (SSRN Scholarly Paper 3637365). Social Science Research Network. https://doi.org/10.2139/ssrn.3637365

115. Voogt, J., Knezek, G., Cox, M., Knezek, D., & ten Brummelhuis, A. (2013). Under which conditions does ICT have a positive effect on teaching and learning? A systematic review of meta-analyses. *Computers & Education*, 70, 210-222. https://doi.org/10.1016/j.compedu.2013.07.001.

116. West, J. F., Finch, J. F., & Curran, P. J. (1995). *Structural equation models with nonnormal variables: Problems and remedies.* In R. H. Hoyle (Ed.), *Structural equation modeling: Concepts, issues, and applications* (pp. 56-75).

117. Wu, T., Tien, K.-Y., Hsu, W.-C., & Wen, F.-H. (2021). Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge. *Applied Sciences*, *11*(19), 9266. https://doi.org/10.3390/app11199266.

118. Xayakot, H., Bhumpenpein, N., & Nuchitprasitchai, S. (2024). Improving Digital Literacy Skills of Teachers in Lao PDR: Analyzing Key

Contributing Factors. *2024 8th International Conference on Information Technology (InCIT)*, 536–541. https://doi.org/10.1109/InCIT63192.2024.10810532

119. Yousif Yaseen, K. A. (2022). Importance of Cybersecurity in The Higher Education Sector 2022. *Asian Journal of Computer Science and Technology*, *11*(2), 20–24. https://doi.org/10.51983/ajcst-2022.11.2.3448.

120. Yu, L., Harrison, L., Lu, A., Li, Z., & Wang, W. (2011). 3D Digital Legos for Teaching Security Protocols. *IEEE Transactions on Learning Technologies*, *4*(2), 125–137. IEEE Transactions on Learning Technologies. https://doi.org/10.1109/TLT.2010.19

121. Yuan, X., & Malki, H., & Song, G., & Waight, C. (2009). *Introducing Advanced Wireless Sensor Networks Into Undergraduate Research* Paper presented at 2009 Annual Conference & Exposition, Austin, Texas. https://doi.org/10.18260/1-2--5023.

122. Yurchenko, A., Rozumenko, A., Rozumenko, A., Momot, R., & Semenikhina, O. (2023). Cloud technologies in education: the bibliographic review. *Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska*, *13*(4), 79–84. https://doi.org/10.35784/iapgos.4421.

123. Zenkina, S. V., Ivshin, M. S., Kobeleva, G. A., Mikhlyakova, E. A., & Omelin, V. N. (2020). Capabilities of digital gamification resources to form the basis of information security. *Journal of Physics: Conference Series*, *1691*(1), 012064. https://doi.org/10.1088/1742-6596/1691/1/012064

124. Zenko, S. (2022). Methodological Training of Future Teachers of Computer Science to Carry Out Their Activities in a Remote Form on the Basis of New Models. *2022 2nd International Conference on Technology Enhanced Learning in Higher Education (TELE)*, 294–299. https://doi.org/10.1109/TELE55498.2022.9801006

125. Zhuang, J., Wang, C., & Lambert, J. H. (2022). Machine learning and other information analyses for risk in social networks. *Risk Analysis*, *42*(8), 1603–1605. https://doi.org/10.1111/risa.13945

126. Бахмат, Н. В., Сторчова, Т. В., Моцик, Р. В., Мєлєкєсцева, Н. В., & Братиця, Г. Г. (2023). Сучасні тенденції розвитку цифрової компетентності майбутніх учителів: європейський досвід. *Академічні Візії, 15*. https://doi.org/10.5281/zenodo.7575753.

127. Бирка, М. Ф. (2024). Авторські концепти професійної підготовки майбутніх вчителів інформатики. *Сучасні цифрові технології та інноваційні методики навчання: досвід, тенденції, перспективи»,* 13, 22-25.

128. Білик, Н. І. (2018). Характеристика готовності до професійної діяльності як педагогічної категорії. *Вісник Житомирського державного університету імені Івана Франка, 4*(95), 24-29. https://www.researchgate.net/publication/329872875.

129. Буйницька, О. (2018). Тест з самодіагностики як один із інструментів визначення рівня цифрової компетентності магістра. *Електронне наукове фахове видання "Відкрите освітнє е-середовище сучасного університету"*, (5), 29–40. https://doi.org/10.28925/2414-0325.2018.5.2940.

130. Буц, К. (2021). Методичні рекомендації до викладання курсу за вибором «Основи кібербезпеки». *Наукові записки молодих учених,* 8. Отримано з https://phm.cuspu.edu.ua/ojs/index.php/SNYS/article/view/1895.

131. Василенко, Р. М. (2022). Цифрова компетентність вчителя: Виклики та шляхи розвитку. Збірник матеріалів всеукраїнського науково-практичного семінару «*Безпечне середовище для учнів та вчителів: виклики та практичні рішення*», 99–104. Інститут цифровізації освіти НАПН України. https://lib.iitta.gov.ua/id/eprint/731117.

132. Василенко, Р.М. (2022) *Робота вчителя з інтернет-безпеки дітей* In: Цифрова компетентність сучасного вчителя нової української школи: 2022 (Безпечне середовище для учнів та вчителів: виклики та практичні рішення) : зб.матеріалів всеукр.наук.-практ.семінару (Київ, 3 березня 2022 р.) . Інститут цифровізації освіти НАПН України, м. Київ, Україна, стор. 99-104.

133. Вембер, В.П. (2016). Створення інтерактивного дидактичного матеріалу в процесі підготовки майбутніх вчителів інформатики. *Електронне наукове фахове видання "Відкрите освітнє е-середовище сучасного університету"*, (2), 137–144. https://doi.org/10.28925/2414-0325.2016.2.vb137144.

134. Вербівський, Д. С. (2024). Застосування інноваційних технологій в підготовці майбутніх вчителів інформатики. *Педагогічна Академія: наукові записки*, (7). https://doi.org/10.57125/pedacademy.2024.06.29.11.

135. Воротникова, І. П. (2019) Умови формування цифрової компетентності вчителя у післядипломній освіті. *Відкрите освітнє е-середовище сучасного університету*, (6), 101-118.

136. Германсон, Г. (2022). Розвиток цифрової компетентності вчителів закладів загальної середньої освіти методами НУШ. *Adaptive Management Theory and Practice Pedagogics*, *14*(27). https://doi.org/10.33296/2707-0255-14(27)-07

137. Годована, М., & Мичуда, Л. (2024). Атаки на таблиці мас-адрес, методи боротьби з цими атаками. *Grail of Science*, (41), 265–271. https://doi.org/10.36074/grail-of-science.05.07.2024.041.

138. Головко, Д.Ю. (2024). Бепек в цифровому просторі : електронний навчальний курс. Біла Церква : БІНПО ДЗВО «УМО» НАПН України. https://lib.iitta.gov.ua/id/eprint/739432/1/ЕНК%20Безпека%20в%20ЦП.pdf.

139. Грицюк, О. С. (2021). Робоча програма навчальної дисципліни «Методика навчання інформатики» для здобувачів вищої освіти зі спеціальності 014 «Середня освіта (Інформатика)», освітньо-професійної програми «Середня освіта (Інформатика)». Кременчуцький національний університет імені Михайла Остроградського. http://ivm.krnu.org/assets/files/ook-22/OOK-20-22.pdf.

140. Дебич, М. (2023). Інтернаціоналізація вищої освіти в контексті відновлення україни: цілі та виклики. *Неперервна професійна освіта: теорія і практика*, *2*(75), 7–15. https://doi.org/10.28925/1609-8595.2023.2.1.

141. Дегтярьова, Н.В. (2019). Робоча програма навчальної дисципліни «Методика навчання інформатики» для здобувачів вищої освіти зі спеціальності 014 «Середня освіта (Інформатика)». СумДПУ імені А.С.Макаренка. https://fizmat.sspu.edu.ua/images/kaf_informatiki/october2021/rob_programs_osnovni/2019/_ok25-014-bak-rp-2019-metodika_navchannya_informatiki_ab9b2.pdf

142. Деркаченко, Я. А., & Дзюба, Т. М. (2021). Забезпечення кіберстійкості України за сучасних умов: Цифрові навички та компетентності. *Зв'язок, 3*, 12–16.

143. Друшляк, М. Г., Семеног, О. М., Грона, Н. В., Пономаренко, Н. П., Семеніхіна, О. В. (2022). Типологія інтернет-ресурсів для розвитку інфомедійної грамотності молоді. *Інформаційні технології і засоби навчання*, 88(2), 1-22. https://doi.org/10.33407/itlt.v88i2.4786.

144. Дубасенюк, О., & Марченко, Г. (2024). Методологічні засади реалізації інформаційного підходу у процесі підготовки майбутніх педагогів у сфері медіаосвіти. http://eprints.zu.edu.ua/42138/1/1.pdf.

145. Дуляба, Н., & Обрамич, О. (2023). Теоретичні засади дослідження сутності цифрової безпеки. *Економіка та суспільство*, (55). https://doi.org/10.32782/2524-0072/2023-55-66.

146. Єсімов, С. С. (2024). Контроль і нагляд поліції у сфері забезпечення публічної безпеки та порядку в умовах цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична), 3,* Article 3. https://doi.org/10.32782/2311-8040/2024-3-5

147. Жмуд, О.В., & Колмакова, В.О. (2019). Робоча програма навчальної дисципліни «Методика навчання інформатики у профільній школі» для студентів спеціальності 014.06 Середня освіта (Хімія). https://pgf.udpu.edu.ua/wp-content/uploads/2019/12/%D0%A0%D0%9F-%D0%9C%D0%9D%D0%86-%D0%A8%D0%9F.pdf

148. Захар, О., & Тихонова, Т. (2017). Інформаційно-освітнє середовищє підвищення кваліфікації як засіб забезпечення якісної

післядипломної педагогічної освіти вчителів інформатики. *Електронне наукове фахове видання "Відкрите освітнє е-середовище сучасного університету"*, (3), 220–229. https://doi.org/10.28925/2414-0325.2017.3.220.29.

149. Карабін, О. (2024). Структура професійної підготовки майбутніх учителів інформатики у системі неперервної освіти. *Освіта. Інноватика. Практика*, *12*(7), 43–48. https://doi.org/10.31110/2616-650X-vol12i7-006.

150. Карабін, О. (2023). Сучасний стан професійної підготовки майбутніх учителів інформатики у системі неперервної освітисучасний стан професійної підготовки майбутніх учителів інформатики у системі неперервної освіти. *Професіоналізм педагога: теоретичні й методичні аспекти*, (18), 106–114. https://doi.org/10.31865/2414-9292.18.2022.272665.

151. Кива, В. Ю., Застело, О. В., & Наконечний, О. М. (2022). Формування навичок з кібербезпеки з використанням методів злому, обходу та захисту процедури надання доступу в операційній системі Microsoft Windows. *Інформаційні технології і засоби навчання*, *89*(3), 233-248. https://doi.org/10.33407/itlt.v89i3.4949.

152. Кириленко, С. В. (2024). Система економічної безпеки в умовах цифрової економіки. *Журнал стратегічних економічних досліджень*, (1), 40–47. https://doi.org/10.30857/2786-5398.2024.1.4.

153. Когут, У. П., Сікора, О. В., & Вдовичин, Т. Я. (2022). Формування індивудуальної освітньої траєкторії вчителя з розвитку цифрової компетентності. *Інформаційні технології і засоби навчання*, *91*(5), 186-204. https://doi.org/10.33407/itlt.v91i5.5006.

154. Кожухова, Х., & Прошкін, В. (2021). Зміст вибіркової дисципліни «цифрові технології в освіті» як засіб формування цифрової компетенції в майбутніх учителів гуманітарних спеціальностей. *Збірник наукових праць Уманського державного педагогічного університету*, (3), 81–91. https://doi.org/10.31499/2307-4906.3.2021.241576.

155. Козубцов, І.М., Козубцова, Л.М., Палагута, А.М., Сновида, В.Є., & Сухомлинова, О.В (2023) Систематизація підходів до навчання здобувачів

вищої освіти в «цифровому освітньо-науковому середовищі». *Наукові інновації та передові технології (Серія «Державне управління», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»),* 1 (15), 374-384.

156. Комар, О. А. (2024). Цифрова компетентність майбутнього вчителя початкової школи: підготовка до уроку математики. *Наукові записки. Серія: Педагогічні науки*, (215), 51-55. https://doi.org/10.36550/2415-7988-2024-1-215-51-55.

157. Крамаренко, Т. (2013). До питання підвищення інформаційної культури вчителя математики. *Новітні комп'ютерні технології*, *4*(1), 35-36. https://doi.org/10.55056/nocote.v4i1.18.

158. Кремень, В., Гриневич, Л. М., Луговий, В., Таланова, Ж. (2021). *Формування цифрової компетентності у школі: кадрові виклики і відповіді для України* Український педагогічний журнал, (4), 6-28. https://doi.org/10.1145/3328778.3366902.

159. Куриленко, Н., Сліпухіна, І., & Мєняйлов, С. (2023). Розвиток поняття інформаційно-цифрової компетентності в практиці вітчизняної природничої освіти. *Фізико-математична освіта*, *38*(2), 27–36. https://doi.org/10.31110/2413-1571-2023-038-2-005.

160. Кухарчук, Р., & Нагай, Д. (2024). Інноваційні цифрові освітні технології у професійній підготовці й діяльності вчителів інформатики. *Вісник Глухівського національного педагогічного університету імені Олександра Довженка*, *3*(56), 56-62. https://doi.org/10.31376/2410-0897-2024-3-56-56-62.

161. Латорре-Медіна, М. Х., & Тнібар-Харрус, Х. (2023). Цифрова безпека в освітніх програмах: дослідження на основі сприйняття майбутніх учителів. *Інформаційні технології і засоби навчання*, *95*(3), 102-111. https://doi.org/10.33407/itlt.v95i3.5204.

162. Мальський, В. (2024). Особливості забезпечення економічної безпеки в умовах гібридних загроз та збройної агресії. *Науковий часопис УДУ імені Михайла Драгоманова. Серія 22. Політичні науки та методики*

викладання соціально-політичних дисциплін, *22*(35), 123–133. https://doi.org/10.31392/UDU-nc.series22.2024.35.14.

163. Міністерство освіти і науки України. (2022). Методичні рекомендації з розвитку цифрової компетентності вчителів. *Український інститут розвитку освіти.* https://uied.org.ua/wp-content/uploads/2022/07/metodychni-rekomendacziyi-z-rozvytku-czyfrovoyi-kompetentnosti.pdf.

164. Млавець, Ю.Ю. (2021). Методика навчання інформатики (конспект лекцій для студентів факультету суспільних наук). Ужгород: ДВНЗ "УжНУ".

165. Наумова, В., & Бульвінська, О. (2024). Управління безпекою учнів в інтернеті: відкриті освітні ресурси на допомогу освітянам. *Освітологія*, *13*(13), 78–90. https://doi.org/10.28925/2412-124X.2024.13.8.

166. Овчаренко, Л. В. (2021). Дистанційна робота як фактор впливу на економічну безпеку підприємства. *Ефективна економіка*. 7. https://doi.org/10.32702/2307-2105-2021.7.93.

167. Овчарук, О.В., Сороко, Н.В., Шимон, О.М. (2024) *Самооцінювання цифрової компетентності вчителів: результати всеукраїнського опитування в умовах воєнного часу. Аналітичні матеріали : препринт* . ІЦО НАПН України, м. Київ, Україна.

168. Опанович, М. (2024). Аналіз свособів обходу інструментів для запобіганням загроз та дослідження методів протидії цьому. *Наукоємні технології, 62*(2), Article 2. https://doi.org/10.18372/2310-5461.62.18705

169. Осипчук, Т.О. (2024). *Роль цифрових освітніх ресурсів у розвитку цифрової компетенції вчителів у контексті кібербезпеки.* Сучасні технології візуалізації колекцій цифрових освітніх ресурсів : зб. матеріалів круглого столу (до Всеукраїнського фестивалю науки), 14 трав. 2024 р., Київ . Ніланд-ЛТД, м. Вінниця, Україна, 66-69.

170. Павленко, Л., Павленко, М., & Павленко, Є. (2023). Дослідження необхідності впровадження технологій DevOps у навчання майбутніх вчителів

інформатики. *Освітологічний дискурс*, (2(41), 219–246. https://doi.org/10.28925/2312-5829.2023.214.

171. Павлова, Н. С. (2023). Практико-орієнтована підготовка майбутніх учителів інформатики, *Науковий вісник Південноукраїнського національного педагогічного університету імені К. Д. Ушинського, 4* (145), 53-60. https://doi.org/10.24195/2617-6688-2023-4-8.

172. Павлова, Н., & Музичук, К. (2020). Компетентнісно орієнтована професійна підготовка майбутніх учителів інформатики. *Humanities science current issues*, *4*(30), 168–176. https://doi.org/10.24919/2308-4863.4/30.212575

173. Патряк, О. (2023). Цифрові навички в сучасних бізнес-моделях. *Цифрова платформа: інформаційні технології в соціокультурній сфері*, 6(2), 419–430. https://doi.org/10.31866/2617-796X.6.2.2023.293616.

174. Петренко, Л. (2023). Цифрова безпека в стуктурі цифрової компетентності майбутнього викладача педагогічного закладу вищої освіти: змістовий компонент. *Освіта дорослих: теорія, досвід, перспективи*, *23*(1), 98-109. https://doi.org/10.35387/od.1(23).2023.98-109.

175. Пузікова, А. В., & Лупан, І. В. (2024). Застосування навчальних проєктів у навчанні програмування. *Наукові записки. Серія: Проблеми природничо-математичної, технологічної та професійної освіти*, *1*, Article 1. https://doi.org/10.32782/cusu-pmtp-2024-1-9

176. Рашкевич, Н. В., & Отрош, Ю. А. (2022). Методологія та організація наукових досліджень: навчальний посібник. Харків.

177. Роганов, М. (2023). Formation of information and technological competence of future computer science teachers in the process of professional training. *Духовність Особистості: Методологія, Теорія і Практика*, *1*(3 (107)), Article 3 (107). https://doi.org/10.33216/2220-6310/2023-107-3-92-102

178. Романюк, П. (2023). Основні проблеми електронної комерції в умовах цифрової трансформації бізнесу. *Цифрова економіка та економічна безпека*, (4 (04), 32-37. https://doi.org/10.32782/dees.4-6.

179. Руденко Ю. О., Друшляк М. Г., Шамоня В. Г., Острога М. М., Семеніхіна О. В. (2023). Розвиток здатності студентської молоді протистояти інформаційним впливам. *Інформаційні технології і засоби навчання, 94*(2), 54–71. https://doi.org/10.33407/itlt.v94i2.5162.

180. Руденко, Ю. О., Друшляк, М. Г., Шамоня, В. Г., Острога, М. М., & Семеніхіна, О. В. (2023). Розвиток здатності студентської молоді протистояти інформаційним впливам. Інформаційні технології і засоби навчання. 94(2), 54–71. https://doi.org/10.33407/itlt.v94i2.5162.

181. Савіцький, Л., Безносенко, С., & Горбач, Р. (2024). Концептуальні погляди на побудову системи захисту від кібератак із застосуванням методів штучного інтелекту в інформаційно-комунікаційних системах. Сучасні інформаційні технології у сфері безпеки та оборони, 49(1), 77–85. https://doi.org/10.33099/2311-7249/2024-49-1-77-85.

182. Семеніхіна, О. В., Юрченко, А. О., Сбруєва, А. А., Кузьмінський, А. І., Кучай, О. В., & Біда, О. А. (2020). Відкриті цифрові освітні ресурси у галузі ІТ: кількісний аналіз. *Інформаційні технології і засоби навчання*, *75*(1), 331-348. https://doi.org/10.33407/itlt.v75i1.3114.

183. Сікора, О. В., & Пазюк, Р. І. (2024). Формування позитивної мотивації до навчання засобами ігрових прийомів. *Таврійський науковий вісник. Серія: Технічні науки*, (3), 62-69. https://doi.org/10.32782/tnv-tech.2024.3.7.

184. Сікора, Я. Б., & Іванова, С. М. (2024). Критерії та показники розвитку цифрової компетентності наукових і науково-педагогічних працівників. *Науковий часопис Українського державного університету імені Михайла Драгоманова. Серія 2. Комп'ютерно-орієнтовані системи навчання*, (23 (30), 74–83. https://doi.org/10.31392/UDU-nc.series2.2024.23(30).07.

185. Славко, Г. В., Григорова, Т. А., Максимова, Л. П., Бриль, Т. С., & Черненко, В. П. (2023). Формування в майбутніх вчителів інформатики компетентностей у сфері інформаційної безпеки. *Педагогічні науки: теорія та практика*, (2), 37-43. https://doi.org/10.26661/2786-5622-2023-2-06.

186. Слюсаренко, І. Ю. (2024). Сутність та класифікація загроз міжнародній безпеці на глобальному рівні: (на основі резолюцій Першого комітету Генеральної Асамблеї ООН 2014–2021 рр.). *Міжнародні відносини: теоретико-практичні аспекти,* (13), 57–70. https://doi.org/10.31866/2616-745X.13.2024.306861/

187. Соколов, В., & Складанний, П. (2023). Порівняльний аналіз стратегій побудови другого та третього рівня освітніх програм зі спеціальності 125 «Кібербезпека». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4*(20), 183–204. https://doi.org/10.28925/2663-4023.2023.20.183204.

188. Сорока, М., & Шамоня, В. (2024). Вплив учителів фізики та інформатики на розвиток інформаційно-цифрової компетентності учнів: світові практики. *Освіта. Інноватика. Практика, 12*(10), 49–55. https://doi.org/10.31110/2616-650X-vol12i10-007.

189. Спірін, О., Олексюк, В., Василенко, Я., & Сіренко, О. (2024). Модель розвитку цифрової компетентності наукових та науково-педагогічних працівників. *Інформаційні технології і засоби навчання, 104*(6), 156-179. https://doi.org/10.33407/itlt.v104i6.5889.

190. Стойка, О. (2023). Формування цифрової грамотності вчителя в системі післядипломної освіти України. *Неперервна професійна освіта: теорія і практика, 2*(75), 61–76. https://doi.org/10.28925/1609-8595.2023.2.7.

191. Ткаченко, А., Гриценко, В., & Кулик, Л. (2023). Розвиток методичної компетентності майбутніх вчителів фізики та інформатики в умовах реалізації мультидисциплінарності в освітньому процесі. *Збірник наукових праць кам'янець-подільського національного університету імені Івана Огієнка. Серія педагогічна, 29*. https://doi.org/10.32626/2307-4507.2023-29.80-84

192. Ткаченко, О. П. (2020). Готовність майбутнього вчителя до професійної діяльності в умовах реформування освіти. *Науковий вісник*

Миколаївського національного університету імені В. О. Сухомлинського, 2(9), 112-118. https://journals.indexcopernicus.com/api/file/viewByFileId/721118.pdf.

193. Фесьоха, Н. О. (2024). Стан та тенденції розвитку кібербезпеки в епоху цифрової трансформації – аналіз сучасних за гроз та заходів захисту. *Вісник Херсонського національного технічного університету*, *2(89)*, Article 2(89). https://doi.org/10.35546/kntu2078-4481.2024.2.33

194. Шарко, В. Д., & Козлова, О. В. (2021). Формування готовності студентів до професійної діяльності в умовах цифровізації освіти. *Педагогічні науки: теорія, історія, інноваційні технології, 3*(117), 125-137. https://er.knutd.edu.ua/bitstream/123456789/25909/1/41.pdf.

195. Шостак, Л., & Помазун, О. (2024). Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. *Цифрова економіка та економічна безпека*, (5 (14), 160-165. https://doi.org/10.32782/dees.14-25.

196. Шульжик, Ю. О., Грицко, Р. Ю., & Пеканець, С. Р. (2022). Управління змінами в умовах цифровізації. *Публічне урядування*, (2 (30), 127-134. https://doi.org/10.32689/2617-2224-2022-2(30)-16.

197. Юрків, Я. І. (2022). Інформаційно-цифрова компетентність викладача в умовах освітнього процесу online. *Вісник Луганського національного університету імені Тараса Шевченка. Педагогічні науки* , (3 (351), 385–394. https://doi.org/10.12958/2227-2844-2022-3(351)-385-394.

198. Юрченко А., Момот Р., Семеніхіна О. Про розвиток інформаційно-цифрової культури вчителів з використанням комп'ютерної візуалізації. *Освіта. Інноватика. Практика*, 2024. Том 12, № 6. С. 93-99. https://doi.org/10.31110/2616-650X-vol12i6-014.

199. Юрченко, К. (2024). Готовність учителів природничо-математичних дисциплін до застосування технологій STEM у професійній діяльності за показниками когнітивного критерію. *Освіта. Інноватика. Практика*, *12*(7), 102–108. https://doi.org/10.31110/2616-650X-vol12i7-015.

200. Ящик, О. Б. (2019). Зміцнення глобальної культури кібербезпеки в мережі Інтернет. *Науковий часопис Українського державного університету імені Михайла Драгоманова. Серія 2. Комп'ютерно-орієнтовані системи навчання*, (19 (26), 136–140. вилучено із https://sj.udu.edu.ua/index.php/kosn/article/view/24.

ДОДАТКИ

Додаток А

Спецкурс "Цифрова безпека у навчальному середовищі"

Очікувані результати спецкурсу. Вчителі інформатики матимуть глибоке розуміння основних понять цифрової безпеки та її важливості, здобудуть навички викладання цифрової безпеки учням різного віку, зможуть розробляти навчальні матеріали та проводити тренінги, будуть готові до впровадження заходів цифрової безпеки в школі та співпраці з батьками.

Модуль 1. Основи цифрової безпеки та інформаційного захисту

Мета: ознайомити майбутніх учителів із ключовими поняттями цифрової безпеки, сучасними загрозами та методами їхнього запобігання.

Основні теми. Основні поняття цифрової безпеки: персональні дані, цифровий слід, цифрові загрози. Види загроз: фішинг, шкідливе програмне забезпечення, соціальна інженерія, витік даних. Правові аспекти цифрової безпеки: міжнародні та національні нормативно-правові акти (Закон України "Про захист персональних даних"). Інструменти захисту інформації: антивіруси, брандмауери, VPN, двофакторна аутентифікація. Цифрова безпека дітей та підлітків: безпечна поведінка в соцмережах, протидія кібербулінгу, приватність даних.

Типові практичні завдання Модуля 1. Аналіз реальних випадків кібератак, використання онлайн-сервісів для перевірки паролів, налаштування параметрів конфіденційності в соцмережах.

Модуль 2. Психолого-педагогічні аспекти формування цифрової безпеки учнів

Мета: надати майбутнім учителям знання щодо вікових особливостей сприйняття інформації про цифрову безпеку та методів її формування.

Основні теми. Вплив цифрового середовища на психіку дитини: кіберстрес, інформаційне перевантаження, цифрова залежність. Вікові особливості сприйняття загроз у цифровому середовищі: як діти різного віку реагують на небезпеку. Методи розвитку критичного мислення та цифрової грамотності: рольові ігри, моделювання ситуацій, дискусії. Етика та відповідальність в Інтернеті: поняття цифрового етикету, правові наслідки онлайн-документування (фото, відео). Роль вчителя у формуванні культури безпеки в Інтернеті: як стати наставником у сфері цифрової безпеки для учнів і батьків.

Типові практичні завдання Модуля 2. Розробка навчальних кейсів для учнів різних вікових груп, аналіз реальних випадків небезпечної поведінки в Інтернеті, підготовка тренінгового заняття для батьків про цифрову безпеку.

Модуль 3. Методика викладання цифрової безпеки в шкільному курсі інформатики

Мета: навчити майбутніх учителів ефективних методів і технологій розвитку навичок цифрової безпеки учнів у школі.

Основні теми. Місце цифрової безпеки у шкільному курсі інформатики: інтеграція тем у навчальну програму. Методи викладання цифрової безпеки: проблемне навчання, проєктний підхід, гейміфікація. Розробка навчальних матеріалів з цифрової безпеки: створення інструкцій, відеоуроків, інтерактивних презентацій. Використання EdTech-інструментів у навчанні цифрової безпеки: платформи Google Classroom, Kahoot, PhishMe, CyberSmart. Оцінювання рівня сформованості навичок цифрової безпеки учнів: тести, практичні кейси, аналіз поведінки в Інтернеті.

Типові практичні завдання Модуля 3. Розробка навчального заняття з цифрової безпеки з використанням інтерактивних методів, проведення міні-уроку, оцінювання рівня знань учнів за допомогою тестів та кейсів.

Модуль 4. Організація інформаційно-освітнього середовища для розвитку навичок цифрової безпеки.

Мета: надати вчителям практичні інструменти для створення безпечного та ефективного освітнього середовища та сформувати вміння їх використовувати.

Основні теми. Розробка політики цифрової безпеки в закладі освіти: правила використання гаджетів, паролі та доступи. Організація безпечного освітнього простору в Інтернеті: налаштування корпоративних акаунтів, Google Workspace для навчання. Створення навчальних матеріалів із цифрової безпеки: інтерактивні веб-квести, відеоуроки, чек-листи. Співпраця з батьками у питаннях цифрової безпеки дітей: проведення просвітницьких заходів. Інтерактивні форми роботи з учнями та батьками: тренінги, ігри, симуляційні вправи.

Типові практичні завдання Модуля 4. Створення навчального відео про правила безпечного користування Інтернетом, моделювання ситуацій із цифрової безпеки, розробка політики цифрової безпеки для школи.

Модуль 5. Оцінювання навичок цифрової безпеки учнів

Мета: сформувати вміння оцінювати навички цифрової безпеки.

Основні теми. Тренінгові методи навчання: як ефективно навчати учнів через практичні вправи та оцінювати їх. Моделювання уроків із цифрової безпеки: планування та проведення уроків у тестовому форматі. Коучинг та менторство у сфері цифрової безпеки: як допомагати колегам і батькам розбиратися в питаннях цифрової безпеки. Застосування отриманих знань у реальних шкільних умовах: адаптація навчальних матеріалів під конкретні освітні програми. Рефлексія та самооцінка викладання цифрової безпеки: аналіз проведених занять, визначення точок росту.

Типові практичні завдання Модуля 5. Розроблення тестових завдань, практичних задач, кейсів для перевірки сформованості навичок цифрової безпеки, проведення демонстраційних уроків, розробка авторських тренінгів, участь у дискусіях щодо проблем оцінювання навичок цифрової безпеки. Проведення демонстраційних уроків, розробка авторських тренінгових занять, участь у дискусіях щодо проблем цифрової безпеки в освіті.

Приклади практичних завдань для кожного модуля

Модуль 1. Основи цифрової безпеки та інформаційного захисту

Практичні завдання та коментарі-обґрунтування до них

1. Аналіз кіберзагроз та їх наслідків.

Завдання: Ознайомитися з реальними випадками кібератак (наприклад, витік даних у великих компаніях) та підготувати короткий аналіз ситуації, її причин та наслідків.

Коментар: Важливо, щоб майбутні вчителі навчилися розбирати реальні кейси та пояснювали учням потенційні загрози через конкретні приклади.

2. Перевірка власної цифрової безпеки

Завдання: Використати сервіси типу Have I Been Pwned для перевірки, чи не потрапили їхні облікові дані у витоки. Проаналізувати налаштування конфіденційності власних акаунтів у соцмережах.

Коментар: Майбутній вчитель інформатики має не лише знати правила безпеки, а й показувати власний приклад безпечної поведінки в Інтернеті.

3. Налаштування безпечного робочого середовища

Завдання: Налаштувати двофакторну аутентифікацію на своїх акаунтах, створити складний пароль за правилами безпеки та використати менеджер паролів.

Коментар: Майбутній учитель інформатики повинен не лише сам знати ці правила, а й навчати цьому учнів.

4. Інтерактивний тест із цифрової безпеки

Завдання: Пройти один із відкритих онлайн-тестів на знання цифрової безпеки (наприклад, Google Safety Center) та проаналізувати результати.

Коментар: Завдання допоможе майбутнім учителям краще розуміти власний рівень знань і визначити, які питання слід допрацювати.

5. Розробка інструкції з цифрової безпеки для учнів

Завдання: Створити короткий гайд для школярів із основними правилами безпечної поведінки в Інтернеті.

Коментар: Гайд має бути зрозумілим, доступним та оформленим у привабливій для дітей формі (інфографіка, відео тощо).

Модуль 2. Психолого-педагогічні аспекти формування цифрової безпеки учнів

1. **Аналіз психологічних особливостей вікових груп**

Завдання: Вивчити характеристики сприйняття інформації про цифрову безпеку учнями різного віку та підготувати короткий аналіз.

Коментар: Розуміння вікових особливостей допоможе вчителю адаптувати методи подачі матеріалу.

2 **Виявлення інформаційного перевантаження**

Завдання: Провести опитування серед учнів щодо часу, проведеного в Інтернеті, та проаналізувати можливий рівень інформаційного перевантаження.

Коментар: Дослідження дасть змогу адаптувати навчальний процес під реальні потреби дітей.

3 **Розробка сценарію рольової гри про небезпеки в Інтернеті**

Завдання: Створити сценарій навчальної гри, де учні потрапляють у різні онлайн-загрози та шукають шляхи їх вирішення.

К*оментар:* Гейміфікація є ефективним інструментом навчання для дітей різного віку.

4 **Дискусія про цифровий етикет**

Завдання: Провести дискусію серед колег або учнів про правила поведінки в Інтернеті, використовуючи реальні кейси.

Коментар: Навчання через обговорення допомагає формувати відповідальність за власні дії в Інтернеті.

5 **Створення навчального відео**

Завдання: Записати коротке відео для учнів про основні правила цифрової безпеки.

К*оментар:* Відеоконтент є більш привабливим і доступним для учнів, ніж текстові матеріали.

Модуль 3. Методика навчання цифрової безпеки в шкільному курсі інформатики

1 **Розробка інтегрованого уроку**

Завдання: Створити план уроку з цифрової безпеки, інтегрувавши його у стандартний курс інформатики.

Коментар: Інтеграція таких тем у базові уроки підвищує ефективність навчання.

2 **Гейміфікація навчання**

Завдання: Розробити інтерактивну гру для навчання основ цифрової безпеки (наприклад, вікторину в Kahoot).

Коментар: Гейміфіковані методи покращують засвоєння інформації.

3 **Практична симуляція фішингової атаки**

Завдання: Створити фіктивний фішинговий лист і провести з учнями експеримент, визначаючи, хто розпізнає загрозу.

К*оментар:* Практичні симуляції допомагають зрозуміти реальні загрози.

4 **Оцінка рівня цифрової безпеки учнів**

Завдання: Розробити тест або чек-лист для визначення рівня цифрової безпеки учнів.

Коментар: Це допоможе оцінити прогрес та виявити проблемні зони.

5 **Захист персональних даних**

Завдання: Провести практикум із налаштування приватності в популярних соцмережах.

Коментар: Учні повинні вміти самостійно керувати своїми даними.

Модуль 4. Організація інформаційно-освітнього середовища для навчання цифрової безпеки

1 **Розробка політики цифрової безпеки для школи**

Завдання: Написати правила користування гаджетами в школі.

Коментар: Це допоможе зменшити ризики в освітньому середовищі.

2 **Навчання батьків**

Завдання: Підготувати інформаційний буклет для батьків про безпеку дітей в Інтернеті.

К*оментар:* Батьки мають брати активну участь у вихованні цифрової грамотності.

3 **Створення EdTech-інструменту**

Завдання: Розробити навчальний сайт або блог із цифрової безпеки.

К*оментар:* Власні онлайн-ресурси полегшують доступ до матеріалів.

4 **Проведення тренінгу для колег**

Завдання: Організувати міні-семінар про цифрову безпеку для вчителів школи.

К*коментар:* Взаємонавчання є ефективним у підготовці педагогів.

5 **Моделювання уроку для дітей**

Завдання: Провести пробний урок у вигляді відкритого заняття.

К*оментар:* Практичний досвід є найкращим способом навчання.

Модуль 5. Оцінювання навичок цифрової безпеки в учнів

1 **Розробка критеріальної системи оцінювання навичок цифрової безпеки**

Завдання: Створити набір критеріїв для оцінювання рівня цифрової безпеки учнів, включаючи знання загроз, уміння захищати персональні дані та здатність розпізнавати кіберзагрози.

Коментар: Важливо, щоб критерії були адаптовані до вікових особливостей учнів і враховували їхню реальну поведінку в цифровому середовищі.

2 **Розробка діагностичного тесту для оцінювання рівня знань учнів**

Завдання: Створити тест із 15–20 питань (з відкритими та закритими відповідями) для перевірки знань учнів про цифрову безпеку.

К*оментар:* Такий тест можна використовувати як до, так і після навчального курсу, щоб оцінити прогрес учнів.

3 **Аналіз цифрової поведінки учнів через самооцінювання**

Завдання: Розробити анкету, в якій учні самостійно оцінюють свої знання та звички щодо цифрової безпеки (наприклад, як часто вони змінюють паролі, чи використовують двофакторну аутентифікацію).

Коментар: Самооцінювання дозволяє учням усвідомити власні слабкі місця та підвищує їхню мотивацію до навчання.

4 **Ситуаційні завдання для практичної перевірки навичок цифрової безпеки**

Завдання: Підготувати набір ситуацій, у яких учні мають визначити, як правильно діяти. Наприклад, що робити, якщо отримав підозрілий лист із вкладенням.

К*оментар:* Важливо перевіряти не лише теоретичні знання, а й здатність учнів приймати правильні рішення в реальних умовах.

5 **Оцінювання впливу навчання на поведінку учнів у цифровому середовищі**

Завдання: Організувати спостереження за поведінкою учнів у соціальних мережах та під час роботи з гаджетами, щоб оцінити, чи вплинули знання з курсу на їхні звички.

Коментар: Оцінювання має включати аналіз змін у поведінці учнів після проходження курсу та порівняння з їхнім початковим рівнем. Цей модуль дозволяє не тільки визначити ефективність навчального процесу, а й зробити висновки щодо подальшого вдосконалення курсу підготовки вчителів.

Контрольні запитання

1. Що таке цифрова безпека, і чому вона важлива для учнів?
2. Які основні види цифрових загроз ви можете назвати?
3. Які є основні цифрові загрози для дітей у цифровому середовищі?
4. Які міжнародні та українські нормативно-правові акти регулюють цифрову безпеку в освіті?
5. Які основні принципи захисту персональних даних учнів?
6. Як цифрова гігієна допомагає запобігати цифровим загрозам?
7. Які правові наслідки має порушення цифрової безпеки для вчителів та учнів?
8. Що таке кібербулінг, і які заходи боротьби з ним існують у школах?
9. Чим фішинг відрізняється від інших видів шахрайства в інтернеті?
10. Як розпізнати підозрілу електронну пошту або повідомлення в соцмережах?
11. Які методи соціальної інженерії використовують кіберзлочинці?
12. Що таке шкідливе програмне забезпечення та як воно поширюється?
13. Які ризики пов’язані з використанням загальнодоступних Wi-Fi мереж?
14. Як розпізнати фейкові акаунти та дезінформацію в соціальних мережах?
15. Що таке багатофакторна аутентифікація, і чому її варто використовувати?
16. Як створити надійний пароль, і як часто його слід змінювати?
17. Які основні антивірусні програми рекомендується використовувати у школі?
18. Що таке VPN, і як він допомагає підвищити рівень цифрової безпеки?
19. Як правильно налаштувати конфіденційність у соціальних мережах?
20. Чим хмарні технології корисні для збереження даних, і які ризики вони несуть?
21. Які програми та інструменти можна використовувати для захисту дітей в інтернеті?
22. Які підходи до навчання цифрової безпеки є найбільш ефективними?
23. Як інтегрувати тематику цифрової безпеки у викладання інформатики?
24. Які інтерактивні методи навчання можна застосовувати для формування навичок цифрової безпеки?
25. Як використовувати гейміфікацію для навчання цифрової безпеки?
26. Які вправи допомагають учням навчитися розпізнавати кіберзагрози?
27. Як залучати батьків до формування цифрової безпеки учнів?
28. Які освітні платформи та курси можна використовувати для підготовки вчителів із цифрової безпеки?
29. Які основні критерії оцінювання цифрової безпеки учнів?
30. Чому важливо оцінювати не лише знання, а й навички цифрової безпеки?
31. Які методи оцінювання цифрової грамотності можна використовувати?
32. Як скласти ефективний тест для перевірки знань із цифрової безпеки?
33. Як аналізувати цифрову поведінку учнів для оцінювання рівня їхньої безпеки?
34. Які інструменти самооцінювання можуть використовувати учні?
35. Як результати оцінювання можуть вплинути на коригування навчального процесу?

Додаток Б

ТЕСТ
на перевірку знань про цифрові загрози та методи їх протидії

1. Який із принципів цифрової безпеки є основним?
- A) Конфіденційність ✅
- B) Доступність
- C) Відкритість
- D) Гнучкість
- E) Анонімність

2. Що таке фішинг?
- A) Вид шкідливого програмного забезпечення
- B) Шахрайський метод отримання персональних даних ✅
- C) Атака на веб-сервер
- D) Використання шифрування для захисту даних
- E) Контроль доступу до інформації

3. Який із методів соціальної інженерії використовує телефонні дзвінки?
- A) Фішинг
- B) Смішинг
- C) Вішинг ✅
- D) Спуфінг
- E) Скімінг

4. Що означає двофакторна аутентифікація?
- A) Використання пароля та біометричних даних ✅
- B) Перевірка особи за допомогою IP-адреси
- C) Застосування VPN для захисту даних
- D) Використання кількох акаунтів для входу
- E) Використання одного пароля для всіх сайтів

5. Який файл найчастіше використовують для розповсюдження вірусів?
- A) .txt
- B) .docx
- C) .exe ✅
- D) .png
- E) .csv

6. Як перевірити надійність пароля?
- A) Переконатися, що він містить лише цифри
- B) Використовувати дату народження
- C) Створити пароль довжиною від 12 символів із цифрами, літерами та символами ✅
- D) Використовувати один і той самий пароль для всіх акаунтів
- E) Вибрати слово з особистого життя

7. Що означає поняття "цифровий слід"?
- A) Діяльність користувача в інтернеті, яка залишає дані про нього ✅
- B) Шлях поширення комп’ютерного вірусу
- C) Список заблокованих сайтів
- D) Відеоспостереження через веб-камеру
- E) Витік персональних даних

8. Яке правило є основним при створенні електронної пошти?
- A) Використання реального імені
- B) Відмова від паролів

- C) Встановлення складного пароля та двофакторної аутентифікації ✅
- D) Надання доступу до пошти всім знайомим
- E) Використання однакової пошти для всіх сервісів

9. Що таке VPN?

- A) Проксі-сервер
- B) Мережа захисту від вірусів
- C) Технологія шифрування трафіку для захисту даних ✅
- D) Система моніторингу активності в мережі
- E) Захист від фішингових атак

10. Який із видів атак спрямований на перехоплення даних у бездротових мережах?

- A) Brute force
- B) DDoS
- C) Man-in-the-Middle ✅
- D) SQL-ін’єкція
- E) Фішинг

11. Що означає термін "бекдор" у кібербезпеці?

- A) Вразливість у програмному забезпеченні, яка дозволяє несанкціонований доступ ✅
- B) Метод шифрування даних
- C) Система захисту від вірусів
- D) Використання складних паролів
- E) Використання антивірусних програм

12. Як захистити свої персональні дані в соціальних мережах?

- A) Відкрито публікувати всі особисті дані
- B) Використовувати тільки один пароль
- C) Налаштувати конфіденційність акаунту ✅
- D) Додавати всіх підряд у друзі
- E) Використовувати лише громадські Wi-Fi мережі

13. Що таке шифрування даних?

- A) Метод збереження паролів
- B) Процес перетворення даних у захищений формат ✅
- C) Вид хакерської атаки
- D) Метод відновлення загублених файлів
- E) Використання слабких паролів

14. Який алгоритм найчастіше використовується для хешування паролів?

- A) RSA
- B) AES
- C) SHA-256 ✅
- D) DES
- E) ZIP

15. Які дії слід вжити при підозрі на злам акаунту?

- A) Змінити пароль та активувати двофакторну аутентифікацію ✅
- B) Повідомити друзям у соцмережах
- C) Відкрити підозрілий лист
- D) Видалити акаунт
- E) Використовувати той самий пароль надалі

16. Які програми можна використовувати для керування паролями?

- A) Notepad
- B) Excel
- C) Менеджери паролів (1Password, LastPass) ✅

- D) Антивірусні програми
- E) Блокнот на телефоні

17. Що таке соціальна інженерія в кібербезпеці?

- A) Використання психологічних методів для отримання конфіденційних даних ✅
- B) Аналіз поведінки в соціальних мережах
- C) Метод шифрування даних
- D) Техніка захисту від вірусів
- E) Використання VPN

18. Як захиститися від вірусів і шкідливих програм?

- A) Використовувати антивірусне програмне забезпечення ✅
- B) Відключити антивірус
- C) Відвідувати незахищені сайти
- D) Відкривати всі отримані файли
- E) Ігнорувати оновлення

19. Яка основна загроза при використанні громадського Wi-Fi?

- A) Високий рівень енергоспоживання
- B) Можливість перехоплення даних ✅
- C) Обмежена швидкість
- D) Відсутність підтримки VPN
- E) Погана якість з’єднання

20. Який інструмент використовується для перевірки сайтів на фішинг?

- A) Google Safe Browsing ✅
- B) Microsoft Word
- C) Блокнот
- D) VLC Player
- E) YouTube

21. Який основний підхід слід використовувати для формування навичок цифрової безпеки в учнів?

- A) Лекційний виклад теоретичних матеріалів
- B) Демонстрація реальних кіберзагроз без пояснення способів їх уникнення
- C) Використання ігрових, проблемних і практико-орієнтованих методів ✅
- D) Навчання лише через перегляд відеоуроків
- E) Повна заборона використання гаджетів у навчальному процесі

22. Яка методика є найефективнішою для пояснення принципів безпечної поведінки в інтернеті?

- A) Проведення відкритої лекції
- B) Організація практичних ситуацій і аналіз кіберзагроз ✅
- C) Оголошення списку правил без пояснення
- D) Використання підручника без інтерактивних методів
- E) Оцінювання лише теоретичних знань

23. Як найкраще пояснити учням важливість складних паролів?

- A) Дати список правил і змусити їх запам’ятати
- B) Провести експеримент із підбором паролів та продемонструвати ризики ✅
- C) Заборонити використовувати паролі взагалі
- D) Використовувати лише паролі, які містять дати народження
- E) Навчити учнів записувати паролі в блокноті

24. Який підхід найефективніше розвиває в учнів критичне мислення щодо кіберзагроз?

- A) Читання теоретичних матеріалів
- B) Механічне запам’ятовування правил

- C) Аналіз реальних випадків шахрайства та обговорення їх наслідків ✅
- D) Регулярне тестування без практичної роботи
- E) Використання одних і тих самих завдань для всіх вікових категорій

25. Який з інструментів можна використати для імітації кіберзагроз під час навчання?

- A) Створення підроблених фішингових листів для аналізу ✅
- B) Перегляд відео без подальшого обговорення
- C) Вивчення лише теоретичних матеріалів
- D) Використання таблиць із правилами без обговорення ситуацій
- E) Використання лише друкованих матеріалів

26. Як учитель може оцінити сформованість навичок цифрової безпеки в учнів?

- A) Проведення виключно письмових тестів
- B) Аналіз успішності навчання за оцінками
- C) Виконання практичних завдань на реальних або змодельованих кіберзагрозах ✅
- D) Оцінювання участі в обговореннях без перевірки знань
- E) Використання тільки теоретичних запитань у контрольних роботах

27. Який метод роботи з батьками допоможе підвищити цифрову грамотність учнів?

- A) Залучення батьків до участі в навчальних тренінгах з цифрової безпеки ✅
- B) Надсилання батькам списку правил без пояснень
- C) Розміщення інформації на сайті школи без додаткових заходів
- D) Перекладання всієї відповідальності на дітей
- E) Виключення батьків із процесу навчання

28. Як учителю організувати інтерактивне навчання цифрової безпеки?

- A) Використовувати тільки презентації
- B) Створювати симуляції кібератак та розбирати варіанти їх запобігання ✅
- C) Використовувати лише підручник
- D) Дати учням завдання вивчити правила самостійно
- E) Використовувати традиційні лекції без обговорень

29. Які методи допомагають розвивати навички самозахисту в цифровому середовищі?

- A) Аналіз практичних кейсів та реальних ситуацій ✅
- B) Читання статей без практичних завдань
- C) Використання лише тестів
- D) Перегляд документальних фільмів без аналізу
- E) Оцінювання знань лише за правильністю відповідей у тестах

30. Яким чином учитель може підтримувати інтерес учнів до теми цифрової безпеки?

- A) Регулярне оновлення навчального матеріалу відповідно до сучасних кіберзагроз ✅
- B) Використання лише одного підручника протягом багатьох років
- C) Повне уникнення теми кіберзагроз
- D) Запам’ятовування правил без пояснення їхньої важливості
- E) Використання одних і тих самих матеріалів для всіх вікових груп

Додаток В

Анкета
для вимірювання показника П1 (ступінь усвідомленості потреби в формуванні навичок цифрової безпеки учнів

Шановні студенти! Анкета передбачає запитання, на які потрібно дати одну відповідь, яка оцінюється за шкалою Лайкерта від 1 балу (зовсім ні) до 5 балів (завжди так)

1. Як ви вважаєте, наскільки важливо вчити учнів основам цифрової безпеки?
    - a) Не важливо
    - b) Тільки для старших класів
    - c) Важливо для кожного учня незалежно від віку
    - d) Це більше стосується лише окремих учнів
    - e) Не знаю
2. Яку роль ви відводите цифровій безпеці у навчанні учнів?
    - a) Вона не має великого значення
    - b) Це важлива, але другорядна складова
    - c) Це одна з основних навичок для сучасних учнів
    - d) Це важливо тільки для учнів старших класів
    - e) Не можу оцінити
3. Чи вважаєте ви, що учні повинні розвивати навички цифрової безпеки з початкових класів?
    - a) Ні
    - b) Так, але лише в старших класах
    - c) Так, я думаю це має бути важливо з раннього віку
    - d) Не знаю, потрібно досліджувати
    - e) Це залежить від ситуації
4. Чи усвідомлюєте ви загрози, які можуть виникати для учнів через недостатнє знання цифрової безпеки?
    - a) Ні, я не бачу таких загроз
    - b) Я чув про це, але не вважаю це серйозною проблемою
    - c) Так, я розумію, що це важливо
    - d) Не можу точно сказати
    - e) Я не маю достатньо знань для оцінки
5. Як ви оцінюєте власну готовність до розвитку навичок цифрової безпеки у учнів?
    - a) Я не маю достатньо знань
    - b) Мені потрібне додаткове навчання
    - c) Я готовий, але маю сумніви щодо методів
    - d) Я готовий і маю достатньо знань
    - e) Не знаю, треба більше дізнатися
6. Яким чином ви оцінюєте важливість навчання учнів безпечному використанню інтернет-ресурсів?
    - a) Це не є важливим
    - b) Це важливо лише для старших класів
    - c) Це повинно бути важливо для всіх учнів
    - d) Це стосується лише певних груп учнів
    - e) Не маю думки
7. Чи є важливою для освітньої установи програма або заходи щодо розвитку навичок цифрової безпеки учнів?

   - a) Ні, такого немає
   - b) Є окремі заходи, але вони недостатні
   - c) Так, є певні програми
   - d) Я не знаю про це
   - e) Так, і ці програми ефективні
8. Чи готові ви використовувати нові технології для розвитку цифрової безпеки учнів?
   - a) Ні, я не бачу в цьому потреби
   - b) Я не знаю, що саме можна використовувати
   - c) Це залежить від конкретної ситуації
   - d) Так, але я не впевнений, як це зробити
   - e) Так, я готовий вивчати нові технології
9. Як часто ви вважаєте за необхідне проводити заняття з цифрової безпеки для учнів?
   - a) Один раз на рік
   - b) Пару разів на рік
   - c) Щомісяця
   - d) Постійно, в рамках навчального процесу
   - e) Не знаю
10. Наскільки важливим для вас є удосконалення своїх знань у галузі цифрової безпеки?

- a) Це не є важливим
- b) Це важливо, але не є пріоритетом
- c) Це дуже важливо для моєї професії
- d) Я не думаю про це
- e) Не знаю

Додаток Д

Методика
оцінки показника П2 «Знання методичних підходів розвитку цифрової безпеки учнів»

Шановні студенти! Просимо обрати один, правильний на вашу думку, варіант відповіді.

1. Який основний підхід слід використовувати для формування навичок цифрової безпеки в учнів?
- A) Лекційний виклад теоретичних матеріалів
- B) Демонстрація реальних кіберзагроз без пояснення способів їх уникнення
- C) Використання ігрових, проблемних і практико-орієнтованих методів ✅
- D) Навчання лише через перегляд відеоуроків
- E) Повна заборона використання гаджетів у навчальному процесі

2. Яка методика є найефективнішою для пояснення принципів безпечної поведінки в інтернеті?
- A) Проведення відкритої лекції
- B) Організація практичних ситуацій і аналіз кіберзагроз ✅
- C) Оголошення списку правил без пояснення
- D) Використання підручника без інтерактивних методів
- E) Оцінювання лише теоретичних знань

3. Як найкраще пояснити учням важливість складних паролів?
- A) Дати список правил і змусити їх запам’ятати
- B) Провести експеримент із підбором паролів та продемонструвати ризики ✅
- C) Заборонити використовувати паролі взагалі
- D) Використовувати лише паролі, які містять дати народження
- E) Навчити учнів записувати паролі в блокноті

4. Який підхід найефективніше розвиває в учнів критичне мислення щодо кіберзагроз?
- A) Читання теоретичних матеріалів
- B) Механічне запам’ятовування правил
- C) Аналіз реальних випадків шахрайства та обговорення їх наслідків ✅
- D) Регулярне тестування без практичної роботи
- E) Використання одних і тих самих завдань для всіх вікових категорій

5. Який з інструментів можна використати для імітації кіберзагроз під час навчання?
- A) Створення підроблених фішингових листів для аналізу ✅
- B) Перегляд відео без подальшого обговорення
- C) Вивчення лише теоретичних матеріалів
- D) Використання таблиць із правилами без обговорення ситуацій
- E) Використання лише друкованих матеріалів

6. Як учитель може оцінити сформованість навичок цифрової безпеки в учнів?
- A) Проведення виключно письмових тестів
- B) Аналіз успішності навчання за оцінками
- C) Виконання практичних завдань на реальних або змодельованих кіберзагрозах ✅
- D) Оцінювання участі в обговореннях без перевірки знань
- E) Використання тільки теоретичних запитань у контрольних роботах

7. Який метод роботи з батьками допоможе підвищити цифрову грамотність учнів?
- A) Залучення батьків до участі в навчальних тренінгах з цифрової безпеки ✅

- B) Надсилання батькам списку правил без пояснень
- C) Розміщення інформації на сайті школи без додаткових заходів
- D) Перекладання всієї відповідальності на дітей
- E) Виключення батьків із процесу навчання

8. Як учителю організувати інтерактивне навчання цифрової безпеки?

- A) Використовувати тільки презентації
- B) Створювати симуляції кібератак та розбирати варіанти їх запобігання ✅
- C) Використовувати лише підручник
- D) Дати учням завдання вивчити правила самостійно
- E) Використовувати традиційні лекції без обговорень

9. Які методи допомагають розвивати навички самозахисту в цифровому середовищі?

- A) Аналіз практичних кейсів та реальних ситуацій ✅
- B) Читання статей без практичних завдань
- C) Використання лише тестів
- D) Перегляд документальних фільмів без аналізу
- E) Оцінювання знань лише за правильністю відповідей у тестах

10. Яким чином учитель може підтримувати інтерес учнів до теми цифрової безпеки?

- A) Регулярне оновлення навчального матеріалу відповідно до сучасних кіберзагроз ✅
- B) Використання лише одного підручника протягом багатьох років
- C) Повне уникнення теми кіберзагроз
- D) Запам’ятовування правил без пояснення їхньої важливості
- E) Використання одних і тих самих матеріалів для всіх вікових груп

Кожна правильна відповідь оцінюється у 3 бали

Додаток Е

Опитування вчителів інформатики

Шановні колеги!
Це опитування має на меті з'ясувати вашу думку щодо важливості формування навичок цифрової безпеки в учнів та вашу готовність до цього. Опитування є анонімним, а отримані результати будуть використані виключно в науково-методичних цілях.

Будь ласка, оберіть відповідь, яка найбільш точно відображає вашу позицію.

1. Як ви оцінюєте важливість формування навичок цифрової безпеки в учнів?
☐ Дуже важливо
☐ Швидше важливо
☐ Швидше неважливо
☐ Зовсім неважливо
☐ Важко відповісти
2. Чи вважаєте ви, що цифрова гігієна має бути частиною шкільного курсу інформатики?
☐ Так, це обов'язково
☐ Так, але лише в рамках окремих уроків
☐ Може викладатися іншими вчителями
☐ Не вважаю це необхідним
☐ Важко відповісти
3. Які аспекти цифрової безпеки, на вашу думку, є найбільш важливими для учнів? ***(можна обрати кілька варіантів)***
☐ Захист персональних даних
☐ Інформаційна безпека (паролі, фішинг)
☐ Критичне мислення та оцінка інформації в Інтернеті
☐ Етика цифрового спілкування
☐ Обмеження часу перед екраном
☐ Захист від кібербулінгу
4. Чи відчуваєте ви себе достатньо підготовленими для викладання цифрової безпеки?
☐ Так, повністю
☐ Так, частково
☐ Ні, потребую додаткової підготовки
☐ Ні, вважаю, що це не є завданням вчителя інформатики
5. Чи використовуєте ви на уроках практичні завдання з цифрової безпеки?
☐ Так, регулярно
☐ Іноді, залежно від теми
☐ Ні, але планую впровадити
☐ Ніколи
6. Які труднощі ви бачите у викладанні цифрової безпеки? ***(можна обрати кілька варіантів)***
☐ Брак методичних матеріалів
☐ Недостатня підготовка вчителів
☐ Низький рівень зацікавленості учнів
☐ Відсутність чітких вимог у навчальній програмі

🔲 Відсутність часу на уроках
🔲 Інше (вкажіть): _____

7. Чи потрібні вам додаткові навчальні курси або тренінги для викладання цифрової безпеки?
🔲 Так, дуже потрібні
🔲 Так, але лише в окремих аспектах
🔲 Ні, мені достатньо наявних знань
🔲 Важко відповісти

8. Чи повинні батьки також долучатися до навчання дітей цифрової безпеки?
🔲 Так, це їхня відповідальність у першу чергу
🔲 Так, але лише разом із вчителями
🔲 Ні, це завдання школи
🔲 Важко відповісти

9. Чи помічаєте ви серед учнів проблеми, пов'язані з відсутністю цифрової безпеки?
🔲 Так, постійно
🔲 Іноді
🔲 Рідко
🔲 Ніколи не помічав(ла)

10. На вашу думку, що може покращити навчання цифрової безпеки в школах? ***(можна обрати кілька варіантів)***
🔲 Включення теми цифрової безпеки до навчальної програми
🔲 Організація тренінгів для вчителів
🔲 Проведення відкритих уроків або вебінарів для учнів і батьків
🔲 Використання інтерактивних навчальних платформ
🔲 Інше (вкажіть): _____

11. Які ще аспекти цифрової безпеки ви вважаєте важливими для учнів, але вони недостатньо висвітлюються у школі?
_____

12. Які методи або підходи, на вашу думку, є найефективнішими для навчання цифрової безпеки?
_____

13. Що могло б мотивувати вас більше впроваджувати цифрову гігієну у ваші уроки?
_____

Дякуємо за вашу участь! Ваша думка дуже важлива для дослідження.

Додаток Ж

Методика визначення показника П4

Анкета
для оцінки прагнення до професійного розвитку в області кібербезпеки

Шановні студенти! Просимо відповісти на запитання, обравши один, найбільш притаманний вам, варіант

1. **Як часто ви бере участь у професійних тренінгах або курсах з кібербезпеки?**
    - a) Ніколи
    - b) Рідко
    - c) Іноді
    - d) Часто
    - e) Завжди
2. **Чи намагаєтесь ви самостійно покращувати свої знання в галузі цифрової безпеки?**
    - a) Зовсім не намагаюсь
    - b) Рідко
    - c) Іноді
    - d) Часто
    - e) Завжди
3. **Як часто ви звертаєтесь до нових ресурсів (статей, книг, онлайн-курсів), що стосуються цифрової безпеки?**
    - a) Ніколи
    - b) Рідко
    - c) Іноді
    - d) Часто
    - e) Завжди
4. **Який рівень вашої зацікавленості в темі цифрової безпеки?**
    - a) Мало цікавить
    - b) Трохи цікавить
    - c) Досить цікавить
    - d) Дуже цікавить
    - e) Повністю зацікавлений
5. **Наскільки ви задоволені доступними для вас ресурсами для професійного розвитку в галузі цифрової безпеки?**
    - a) Зовсім не задоволений/а
    - b) Мало задоволений/а
    - c) Помірно задоволений/а
    - d) Задоволений/а
    - e) Повністю задоволений/а
6. **Як би ви оцінили свою готовність впроваджувати нові знання з кібербезпеки в навчальну практику?**
    - a) Зовсім не готовий
    - b) Мало готовий
    - c) Частково готовий
    - d) Дуже готовий
    - e) Повністю готовий
7. **Наскільки ви згодні з твердженням, що ви регулярно займаєтесь самостійним навчанням у сфері цифрової безпеки?**

- a) Зовсім не згоден(-а)

- b) Швидше не згоден(-а)
- c) Не впевнений(-а)
- d) Швидше згоден(-а)
- e) Повністю згоден(-а)

Додаток И

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України

1. **Dubinsky V.** Information approach in education and its use in the training of computer science teachers to form students' digital safety skills. *Академічні візії, 2024. 38*. https://doi.org/10.5281/zenodo.14594487. Отримано з https://www.academy-vision.org/index.php/av/article/view/1587.
2. **Dubinsky V.** Training of computer science teachers for the formation of cybersecurity skills in students: actualization of problems and their possible solutions. *Освіта. Інноватика. Практика*, 2024. Том 12, № 10. С. 6-11. https://doi.org/10.31110/2616-650X-vol12i10-001.
3. **Dubinsky V. O.** The readiness of computer science teachers to develop students' digital security skills. *Наукові інновації та передові технології» (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»),* 2025. № 2(42). С. 1075-1087. https://doi.org/10.52058/2786-5274-2025-2(42)-1075-1087.

Публікації у закордонних виданнях

4. **Dubinsky V.** Preparing future computer science teachers for the formation of digital security skills in students: generalization of the results of scientific papers. Academia Polonica, 2024. Vol. 66(6). Pp. 12-24

Публікації у виданнях, що індексуються у наукометричних базах Scopus та/ або Web of science

5. M. Yachmenyk et al., "Development of Information and Media Literacy in the System "Students-Parents-Teachers": Ukrainian Practice," 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, pp. 430-435, doi: 10.1109/MIPRO60963.2024.10569314 (Scopus)

Наукові праці, які засвідчують апробацію матеріалів дисертації

6. **Dubinsky V. O.**, Shamonia V. G. On the development of information and digital competence of future teachers of vocational education. *Вектори розвитку науки, освіти, технологій і суспільства в умовах глобалізації*: збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 19 жовтня 2023 р.): у 2 ч. Полтава: ЦФЕНД, 2023. Ч. 1. С.17-18.

7. **Дубинський В.**, Шамоня В. Про інформаційно-цифрову компетентність як сучасну педагогічну категорію. *Наукова діяльність як шлях формування професійних компетентностей майбутнього фахівця* (НПК-2023) : матеріали Міжнародної науково-практичної конференції, 7-8 грудня 2023 р., м. Суми. Суми : ФОП Цьома С.П., 2023. С. 26-27.

8. **Дубинський В.** Академічна доброчесність – невід'ємний складник інформаційно-цифрової компетентності майбутніх викладачів ЗП(ПТ)О. *Академічна культура дослідника в освітньому просторі: європейський та національний досвід*: збірник матеріалів VII Міжнародної науково-практичної конференції (м. Суми, 17-18 травня 2024 року) / за ред. О. М. Семеног. Суми : Видавництво СумДПУ імені А. Макаренка, 2024. С. 172-174.

9. **Дубинський В. О.**, Шамоня В. Г. До питання про розвиток інформаційно-цифрової компетентності в умовах неформальної освіти. *Інформаційні технології в соціокультурній сфері, освіті та економіці* : матеріали IIIV Міжнародної науково-практичної конференції студентів і молодих учених. / М-во освіти і науки України; Київ. нац. ун-т культури і мистецтв. Київ : Видавничий центр КНУКіМ, 2024. С.93-95.

10. **Dubinsky V.**, Shamonia V. On the development of students' digital security skills based on the information approach. *Наукова діяльність як шлях формування професійних компетентностей майбутнього фахівця (НПК-2024)* : матеріали Міжнародної науково-практичної конференції (5-6 грудня 2024 р., м. Суми). Суми : СумДПУ ім. А. С. Макаренка, 2024. С. 12-13.

Основні положення та результати дисертаційної роботи доповідалися та отримали позитивну оцінку на наукових, науково-методичних і науково-практичних конференціях та семінарах різних рівнів:

міжнародних: «Вектори розвитку науки, освіти, технологій і суспільства в умовах глобалізації» (Полтава, 19 жовтня 2023 р.); «Наукова діяльність як шлях формування професійних компетентностей майбутнього фахівця» (Суми, 7-8 грудня 2023 р., 5-6 грудня 2024 р.); «Академічна культура дослідника в освітньому просторі: європейський та національний досвід» (м. Суми, 17-18 травня 2024 р.); «Інформаційні технології в соціокультурній сфері, освіті та економіці» (Київ, 2024).

Матеріали дисертаційного дослідження доповідалися й обговорювалися на засіданнях кафедри інформатики, науково-методичних семінарах наукових лабораторій – Лабораторії використання інформаційних технологій в освіті та Лабораторії «Академічна культура дослідника» Сумського державного педагогічного університету імені А. С. Макаренка (2023-2025 рр.).

Додаток К

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УМАНСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТІМЕНІ ПАВЛА ТИЧИНИ
20300, Черкаська обл., м. Умань, вул. Садова, 2, тел. (04744) 3-45-82, факс (04744)
3-45-82, E-mail: post@udpu.edu.ua УДПУ імені Павла Тичини р/р UA14 820172 0343 12100 22 0000 4420,
банк одержувача Державна казначейська служба України, м. Київ МФО 820172, код 02125639

14.03.2025 № 470/01

На №_____від_____

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Дубинського Віталія Олеговича
на тему: «Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу»
на здобуття ступеня доктора філософії
зі спеціальності 015 Професійна освіта. Цифрові технології

Результати дисертаційного дослідження Дубинського Віталія Олеговича на тему: «Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу» впроваджувалися в освітній процес факультету фізики, математики та інформатики Уманського державного педагогічного університету імені Павла Тичини протягом 2023–2024 рр.

Наукові напрацювання Дубинського В. О., у тому числі розроблена модель формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу, яка передбачає дотримання принципів науковості та актуальності, системності, компетентнісної орієнтованості, практико-орієнтованості, інтеграції та міждисциплінарності, використовувалися викладачами кафедри інформатики і інформаційно-комунікаційних технологій, зокрема в процесі викладання навчальних дисциплін: «Захист інформаційних ресурсів», «Інформаційна безпека», «Основи кібербезпеки», «Безпека комп'ютерних систем та мереж», «Безпека хмарних обчислень».

Отримані результати заслуговують на увагу в теоретичному та методичному аспектах, засвідчують доцільність їх використання в освітньому процесі вищої школи. Розроблені автором науково-методичні матеріали, сприяли підвищенню рівня підготовки майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу.

Основні положення та результати впровадження дисертаційної роботи Дубинського Віталія Олеговича на тему: «Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу» обговорено та схвалено на засіданні кафедри інформатики і інформаційно-комунікаційних технологій (протокол № 12 від 26 лютого 2025 року).

1120 Перший проректор Андрій ГЕДЗИК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені А. С. МАКАРЕНКА
вул. Роменська, 87, м. Суми, 40002, факс (0542) 22-15-17, тел. (0542) 68-59-02
e-mail: rector@sspu.edu.ua, www.sspu.edu.ua
Код ЄДРПОУ 02125510

21.02.2025 № 542/1 На № _____ від _____

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Віталія Дубинського
«ФОРМУВАННЯ ГОТОВНОСТІ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ ДО РОЗВИТКУ НАВИЧОК ЦИФРОВОЇ БЕЗПЕКИ УЧНІВ НА ЗАСАДАХ ІНФОРМАЦІЙНОГО ПІДХОДУ»
на здобуття наукового ступеня доктора філософії
за спеціальністю 015 Професійна освіта (цифрові технології)

Протягом 2023-2025 рр. на базі кафедри інформатики Сумського державного педагогічного університету імені А.С. Макаренка проходили апробацію і впровадження результати наукового дослідження В. Дубинського на тему «Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу».

Перевірялася ефективність розробленої автором моделі формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу через удосконалення змісту професійної підготовки вчителів інформатики, зокрема, розроблення й упровадження вибіркового курсу «Цифрова безпека у навчальному середовищі» для студентів бакалаврату і магістратури спеціальності 014 СО (Інформатика), результатом якого було передбачено формування мотиваційного, предметно-методичного і особистісного компонентів такої готовності.

За результатами педагогічного експерименту (38 здобувачів освіти) зафіксовано позитивну динаміку за показниками «ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів», «знання методичних підходів для розвитку навичок цифрової безпеки учнів», «уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки в учнів», «прагнення до професійного розвитку в галузі цифрової безпеки».

Результати обговорені і затверджені на засіданні кафедри інформатики (протокол №6/1 від 11.02.2025).

Ректор Юрій ЛЯННОЙ

Завідувач кафедри інформатики Неля ДЕГТЯРЬОВА

УКРАЇНА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ імені Г.С. СКОВОРОДИ
вул. Алчевських, 29, м. Харків, 61002, тел. (057) 700-35-23, факс (057) 700-69-09
e-mail: rector@hnpu.edu.ua, код ЄДРПОУ 02125585

Від 13.03.2025 р. № 01/10-244

На № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Віталія Дубинського
«Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу»
на здобуття наукового ступеня доктора філософії
(015 Професійна освіта. Цифрові технології)

Протягом 2023-2025років на базі кафедри інформатики Харківського національного педагогічного університету імені Г.С. Сковороди проходили апробацію та впровадження матеріали дисертаційного дослідження Віталія Дубинського «Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу». Зокрема, проводилася оцінка діагностичного інструментарію для визначення позитивних зрушень у рівнях готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів. За висновками провідних викладачів кафедри інформатики, розроблений В.О. Дубинським діагностичний апарат у складі трьох критеріїв (спонукальний, компетентісний і поведінковий) і чотирьох показників (ступінь усвідомленості потреби розвитку навичок цифрової безпеки у учнів; знання методичних підходів для розвитку навичок цифрової безпеки; уміння дібрати методи/ підходи/ засоби навчання для розвитку навичок цифрової безпеки в учнів; прагнення до професійного розвитку в галузі цифрової безпеки)дає можливість відслідковувати зміни у знаннях та вміннях майбутніх учителів інформатики на чотирьох рівнях (початковий, базовий, високий, творчий).

Додатково вивчалася думка стейхолдерів спеціальності «Середня освіта (інформатика)» (викладачі – 6 осіб, студенти-бакалаври – 45 осіб, студенти-магістранти – 30 осіб) про професійний рівень підготовки вчителів щодо розвитку навичок цифрової гігієни учнів та доцільність удосконалення змісту професійної підготовки майбутніх учителів інформатики. Опитування проводилося двічі.

Результати опитування піддані аналізу і обговорені на засіданні кафедри інформатики (протокол № 15 від 04.03.2025 р.). За результатами обговорення рекомендовано модернізацію змісту окремих обов'язкових компонентів освітніх програм.

Проректор з наукової, інноваційної і міжнародної діяльності Світлана БЕРЕЖНА