УДК 37.396.68:004

МЕТОДИ ТА ЗАСОБИ ФОРМУВАННЯ КОМПЕТЕНТНОСТІ З КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ПРОЦЕСІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ІНЖЕНЕРІВ-ПРОГРАМІСТІВ

Кирило Комарницький

Мелітопольський державний педагогічний університет імені Богдана Хмельницького

Анотація:
У статті обґрунтовано тлумачення поняття «формування компетентності з кібернетичної безпеки» в аспекті професійної підготовки майбутніх інженерів-програмістів. Також у статті визначено та охарактеризовано ефективні методи формування компетентності з кібернетичної безпеки, які доцільно використовувати в процесі підготовки майбутніх інженерів-програмістів, а саме: методи інтерактивного навчання: моделювання атак і захисту, «Capture the Flag» (CTF), практичні лабораторії та симулятори; проєктно орієнтоване навчання: розробка захищених програмних систем, веб-безпека, інцидент-менеджмент; метод кейс-стаді (Case Study): аналіз інцидентів кібербезпеки, розгляд політик безпеки; інтеграція кібербезпеки в курс програмування: безпечне програмування, аналіз коду; навчальні платформи та інструменти: онлайн-курси і платформи для навчання кібербезпеці, віртуальні лабораторії; методи оцінювання та зворотний зв'язок: завдання на тестування безпеки, оцінка за допомогою змагань, рефлексія та обговорення; підвищення кваліфікації через сертифікаційні програми: сертифікація CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CompTIA Security. Водночас особливу увагу у статті приділено сучасним засобам формування компетентності з кібернетичної безпеки, які доцільно використовувати у професійній підготовці майбутніх інженерів-програмістів. Серед них: програмне забезпечення та інструменти для тестування безпеки: Metasploit, Wireshark, Nmap, Kali Linux; віртуальні лабораторії та тренажери: TryHackMe, Hack The Box, Cyber Range; онлайн-курси та навчальні платформи: Coursera – курси від провідних університетів та компаній з кібербезпеки, edX – платформа для навчання, яка пропонує курси з кібербезпеки від провідних університетів, Udemy – онлайн-курси з різних аспектів кібербезпеки, включаючи пентестинг, захист мереж тощо; системи управління навчанням (LMS): Moodle – платформа для створення онлайн-курсів, яка дозволяє організовувати завдання, тестування та взаємодію з студентами, Blackboard – система для управління навчанням, що включає модулі для створення інтерактивних завдань та тестів з кібербезпеки, Google Classroom – зручний інтерфейс для організації занять, дискусій та моніторингу прогресу студентів; змагання та конкурси: CTF (Capture The Flag) – популярний формат змагань з кібербезпеки, European Cyber Security Challenge (ECSC) – міжнародний конкурс, на якому студенти можуть продемонструвати свої навички у сфері кібербезпеки, National Collegiate Cyber Defense Competition (CCDC) – змагання для студентів, при якому команди змагаються в області захисту реальних мережевих систем; методичні та довідкові матеріали: книги «Кібербезпека» або «Інформаційна безпека та криптографія», наукові публікації з кібербезпеки, блоги та ресурси; симулятори кіберзагроз; менторство та наставництво.

Ключові слова:
методи, засоби; компетентності; кібернетична безпека; професійна підготовка; інженери-програмісти.

Resume:
Komarnytsky Kyrylo. Methods and Tools for Developing Cybersecurity Competence in the Professional Training of Future Software Engineering Specialists.
The article substantiates the interpretation of the concept of «cybernetic security competence formation» in the aspect of professional training of future software engineers. Also, the article defines and characterizes effective methods of forming competence in cyber security, which should be used in the process of training the future software engineers, namely: methods of interactive training: simulation of attacks and defenses, «Capture the Flag» (CTF), hands-on laboratories and simulators; project-oriented training: development of secure software systems, web security, incident management; case study method: analysis of cyber security incidents, review of security policies; integration of cyber security in the programming course: secure programming, code analysis; educational platforms and tools: online courses and platforms for cyber security training, virtual laboratories; assessment methods and feedback: security testing tasks, competitive assessment, reflection and discussion; professional development through certification programs: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CompTIA Security certification. At the same time, the article pays special attention to modern means of competence formation in cyber security, which are expedient to be used in the professional training of future software engineers. Among them there are: software and tools for security testing: Metasploit, Wireshark, Nmap, Kali Linux; virtual laboratories and simulators: TryHackMe, Hack The Box, Cyber Range; online courses and learning platforms: Coursera – courses from leading universities and companies in cyber security, edX – a learning platform that offers cyber security courses from leading universities, Udemy – online courses on various aspects of cyber security, including pentesting, network protection, etc.; learning management systems (LMS): Moodle – a platform for creating online courses that allows to organize tasks, testing and interaction with students, Blackboard – a learning management system that includes modules for creating interactive tasks and tests on cyber security, Google Classroom – a convenient interface for organizing classes, discussions and monitoring student progress; competitions and contests: CTF (Capture The Flag) – a popular format of cyber security competitions, European Cyber Security Challenge (ECSC) – an international competition where students can demonstrate their skills in the field of cyber security, National Collegiate Cyber Defense Competition (CCDC) – a competition for students, in which teams compete in the field of protection of real network systems; methodological and reference materials: books «Cyber security» or «Information security and cryptography», scientific publications on cyber security, blogs and resources; cyber threat simulators; mentoring and controlling.

Key words:
methods; means; competences; cyber security; professional training; software engineers.

Постановка проблеми. Актуальність дослідження методів та засобів формування компетентності з кібернетичної безпеки у процесі підготовки майбутніх інженерів-програмістів зумовлена науково-технічним прогресом, зростаючими кіберзагрозами, необхідністю покращення професійної підготовки фахівців у галузі кібербезпеки та змінами в ринкових вимогах. Формування відповідної компетентності дозволить підготувати фахівців, здатних забезпечити належний рівень безпеки інформаційних систем та зменшити ймовірність кіберінцидентів, що є основною метою сучасної професійної підготовки.

Крім того, на ринку праці часто не вистачає кваліфікованих спеціалістів у галузі

кібербезпеки, а особливо інженерів-програмістів, які також володіють знаннями в галузі захисту інформації. Більшість студентів інженерних спеціальностей не отримують достатнього рівня практичної підготовки для вирішення реальних задач кібербезпеки. Це призводить до того, що багато програмістів не мають повного уявлення про те, як розробляти надійне програмне забезпечення або як виявляти і нейтралізувати кіберзагрози. В результаті багато організацій стикаються з серйозними проблемами у сфері безпеки своїх інформаційних систем, адже навіть найкращі програмні рішення можуть виявитися вразливими, якщо вони не були спроєктовані з урахуванням принципів кібербезпеки. Такий стан вимагає термінових змін у підходах до навчання майбутніх інженерів-програмістів. Потрібно інтегрувати теми кібербезпеки в усі етапи навчального процесу, забезпечити студентам доступ до сучасних інструментів та технологій для тестування безпеки, а також створити умови для розвитку практичних навичок через проєкти та лабораторні роботи. Важливо також акцентувати увагу на безпечному програмуванні, практиках захисту даних, методах запобігання атакам, а також важливості регулярних оновлень програмного забезпечення та налаштувань безпеки.

Враховуючи постійне зростання кіберзагроз і розвиток новітніх технологій, підготовка інженерів-програмістів повинна включати не лише знання традиційних методів захисту, а й уміння адаптуватися до нових викликів і загроз. Це дозволить майбутнім фахівцям ефективно працювати в умовах постійно змінюваного кіберсередовища та забезпечувати високий рівень безпеки в розроблених програмних системах і додатках.

Саме тому сучасна система освіти повинна орієнтуватися на інтеграцію теоретичних знань із практичними навичками кібербезпеки, що дозволить студентам стати не тільки висококваліфікованими програмістами, але й експертами в галузі безпеки, здатними вирішувати комплексні завдання захисту інформації в умовах сучасних кіберзагроз.

Аналіз останніх досліджень і публікацій. Такі науковці як: A. Alammari, O. Sohaib & S. Younes (2022) у своїх працях розглядали новітні методи та технології для формування компетентностей з кібербезпеки серед студентів технічних спеціальностей, зокрема інженерів-програмістів. Особливу увагу вони приділяли впровадженню інтерактивного навчання, використанню симуляцій кіберінцидентів та спеціалізованих платформ для навчання, що допомагають студентам розвивати практичні навички в реальних умовах кіберзагроз.

Варто зазначити, що A. Cartelli (2010) у своїх дослідженнях розглядав методи підготовки студентів у контексті їхніх професійних компетенцій з кібербезпеки. Особливу увагу вчений приділяв саме розробці навчальних програм, що включають теоретичні знання та практичні навички.

Крім того, V. Buriachok, V. Bogush, Y. Borsukovskii, P. Skladannyi & V. Borsukovska (2018) акцентують увагу на важливості міждисциплінарного підходу, що поєднує знання з програмування, системного адміністрування та кібербезпеки. Також науковці розробили моделі інтеграції кібербезпеки в університетські навчальні плани, зокрема для підготовки майбутніх програмістів.

Важливим аспектом є дослідження M. Lehto (2015), у яких основна увага зосереджена на необхідності впровадження навчальних програм для підготовки фахівців з кібербезпеки та необхідності розвитку м'яких навичок (soft skills), таких як критичне мислення, комунікація, етика в кіберпросторі.

Цікавими є висновки проведеного дослідження W. Yaokumah (2019), у якому вивчено взаємодію між професійною підготовкою студентів і необхідними компетенціями для роботи в сфері кібербезпеки. Науковець зазначає важливість упровадження нових методів навчання, таких як віртуалізація та онлайнові тренажери для тестування на проникнення.

Формулювання цілей статті. Основна мета статті полягає в аналізі та систематизації методів та засобів формування компетентності з кібернетичної безпеки, які доцільно використовувати в процесі підготовки майбутніх інженерів-програмістів.

Відповідно до поставленої мети необхідно виконати такі завдання:

- обґрунтувати тлумачення поняття «формування компетентності з кібернетичної безпеки» в аспекті професійної підготовки майбутніх інженерів-програмістів;
- визначити та охарактеризувати ефективні методи формування компетентності з кібернетичної безпеки в процесі підготовки майбутніх інженерів-програмістів;
- запропонувати та охарактеризувати сучасні засоби формування компетентності з кібернетичної безпеки, які доцільно використовувати у професійній підготовці майбутніх інженерів-програмістів.

Виклад основного матеріалу дослідження. Формування компетентності з кібернетичної безпеки в процесі підготовки майбутніх інженерів-програмістів є необхідною умовою для підготовки фахівців, які зможуть ефективно працювати в умовах сучасних кіберзагроз. Це не лише технічна

необхідність, а й стратегічна вимога для забезпечення безпеки на рівні організацій, держав та глобальної спільноти. Тому навчання повинно бути спрямоване на розвиток не тільки технічних навичок, але й критичного мислення, аналітичних здібностей і здатності до оперативного реагування на нові кіберзагрози.

У наукових колах поняття «компетентність з кібернетичної безпеки» визначають як *комплекс знань, умінь, навичок і досвіду, необхідних для ефективного управління та захисту інформаційних систем, мереж і даних від загроз, атак і зловживань*. Це включає розуміння основних принципів і методів забезпечення кібербезпеки, здатність виявляти та аналізувати вразливості в системах, запобігати кіберзагрозам, розробляти і впроваджувати політики безпеки, а також реагувати на інциденти та забезпечувати відновлення систем після атак.

Крім того, компетентність у цій галузі передбачає також здатність здійснювати належний моніторинг безпеки, застосовувати актуальні інструменти для захисту даних, розуміти правові та етичні аспекти кібербезпеки та підтримувати високий рівень безпеки в умовах швидко змінюваного технологічного середовища.

В той же час, формування компетентності з кібернетичної безпеки в процесі підготовки майбутніх інженерів-програмістів доцільно визначати як *процес набуття та розвитку у студентів або фахівців знань, умінь і навичок, необхідних для ефективного виявлення, аналізу та захисту інформаційних систем, мереж і даних від різноманітних кіберзагроз (рисунок 1)*. Також сюди можна віднести як теоретичні знання з основ кібербезпеки, так і практичні вміння з використання сучасних технологій, інструментів та методів захисту, таких як криптографія, захист від кібератак, аналіз вразливостей, безпека програмного забезпечення та реагування на інциденти безпеки.

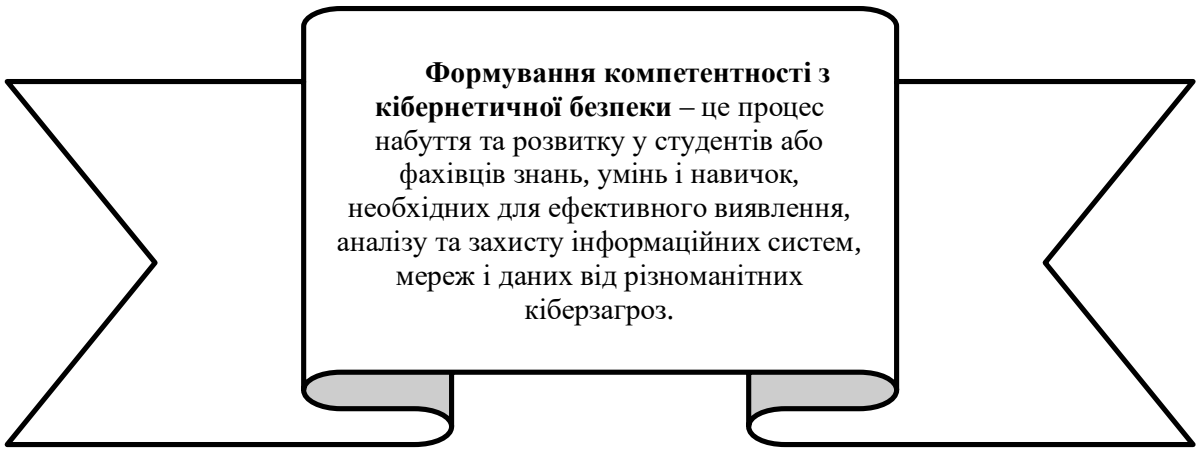

Рис. 1. Тлумачення поняття «формування компетентності з кібернетичної безпеки» в аспекті професійної підготовки майбутніх інженерів-програмістів

Формування відповідної компетентності в процесі підготовки майбутніх інженерів-програмістів сприяє підготовці фахівців, здатних забезпечити цілісність, конфіденційність і доступність інформації, а також ефективно протидіяти сучасним кіберзагрозам, що є важливим аспектом у професійній діяльності в умовах цифрової трансформації та зростаючої кіберзлочинності (Falloon, 2020).

Варто наголосити, що в аспекті формування компетентності з кібернетичної безпеки в процесі підготовки майбутніх інженерів-програмістів заслуговує на увагу те, що сам процес формування компетентностей є ключовим аспектом в освітньому процесі підготовки майбутніх інженерів-програмістів. Це обумовлено також тим, що інформаційні технології, програмне забезпечення та мережі є основою сучасної інфраструктури, і забезпечення їхньої безпеки є пріоритетом у професійній діяльності програмістів.

Слід зазначити, що у контексті формування компетентності з кібернетичної безпеки у процесі підготовки майбутніх інженерів-програмістів слід визначити ефективні сучасні методи, використання яких доцільно в процесі підготовки майбутніх інженерів-програмістів для формування у них компетентності з кібернетичної безпеки. Синтезуючи наукові напрацювання з цього питання у таблиці 1 *зазначені методи, які доцільно використовувати для формування компетентності з кібернетичної безпеки у процесі підготовки майбутніх інженерів-програмістів.*

1. *Методи інтерактивного навчання*. Інтерактивні методи є одними з найефективніших у формуванні практичних навичок з кібербезпеки, оскільки вони дозволяють студентам на практиці застосовувати теоретичні знання (Ferrari, 2012).

Таблиця 1

Методи формування компетентності з кібернетичної безпеки в процесі підготовки майбутніх інженерів-програмістів

№ п/п	Методи формування компетентності з кібернетичної безпеки	Різновиди методів формування компетентності з кібернетичної безпеки у процесі підготовки майбутніх інженерів-програмістів
1	Методи інтерактивного навчання	Моделювання атак та захисту
		«Capture the Flag» (CTF)
		Практичні лабораторії та симулятори
2	Проектно орієнтоване навчання	Розробка захищених програмних систем
		Веб-безпека
		Інцидент-менеджмент
3	Метод кейс-стаді (Case Study)	Аналіз інцидентів кібербезпеки
		Розгляд політик безпеки. Розгляд політик безпеки
4	Інтеграція кібербезпеки в курс програмування	Безпечне програмування
		Аналіз коду
5	Навчальні платформи та інструменти	Онлайн-курси і платформи для навчання кібербезпеці
		Віртуальні лабораторії
6	Методи оцінювання та зворотний зв’язок	Завдання на тестування безпеки
		Оцінка за допомогою змагань
		Рефлексія та обговорення
7	Підвищення кваліфікації через сертифікаційні програми	Сертифікація CISSP (Certified Information Systems Security Professional)
		CEH (Certified Ethical Hacker)
		CompTIA Security+

1.1. Моделювання атак і захисту: створення реалістичних сценаріїв кібератак і навчання студентів методам виявлення вразливостей та захисту від атак. Це може включати моделювання ситуацій на основі реальних кіберінцидентів.

1.2. «Capture the Flag» (CTF): змагання з кібербезпеки, де учасники повинні вирішувати серії задач, що стосуються тестування на проникнення, криптографії, експлуатації уразливостей, зломів вебсайтів та інших кіберзагроз. Участь у CTF дозволяє студентам покращити свої практичні навички.

1.3. Практичні лабораторії та симулятори: використання віртуальних лабораторій або спеціалізованих платформ для тестування та тренування на реальних інструментах, таких як Kali Linux, Metasploit, Wireshark, що дозволяє студентам практикуватися в реальних умовах без ризику для систем.

2. *Проєктно орієнтоване навчання:* проєктне навчання дозволяє студентам працювати над реальними або наближеними до реальних задачами, що допомагає їм здобувати цінний досвід у вирішенні проблем кібербезпеки (Calvani, Cartelli, Fini, & Ranieri, 2008).

2.1. Розробка захищених програмних систем: студенти можуть працювати над створенням програмного забезпечення, що включає в себе заходи кіберзахисту, такі як шифрування, автентифікація, захист від SQL-ін’єкцій, реалізація протоколів безпеки.

2.2. Веб-безпека: проєкти, які фокусуються на виявленні вразливостей у веб-додатках (наприклад, Cross-Site Scripting (XSS), SQL Injection, CSRF) і розробці методів їхнього усунення.

2.3. Інцидент-менеджмент: розробка проєктів із реагування на кіберінциденти, у яких студенти тренуються у виявленні, аналізі та реагуванні на атаки, використовуючи інструменти для моніторингу та аналізу мережевого трафіку.

3. *Метод кейс-стаді (Case Study).* Кейс-метод дозволяє студентам аналізувати реальні або вигадані ситуації, що мають відношення до кібербезпеки. Це дає змогу розв’язувати конкретні практичні проблеми та розуміти, як кіберзагрози проявляються в реальному світі.

3.1. Аналіз інцидентів кібербезпеки: студенти досліджують реальні випадки кіберзлочинності, атаки на інформаційні системи, шахрайство в мережах тощо, щоб зрозуміти механізми атак і найкращі методи захисту.

3.2. Розгляд політик безпеки: студенти можуть працювати над створенням політик безпеки для організацій або розробляти рекомендації для зміцнення захисту корпоративних інформаційних систем.

4. *Інтеграція кібербезпеки в курс програмування.* Кібербезпека повинна бути невід’ємною частиною всіх дисциплін, що стосуються програмування, адже програмісти – це ті, хто створює програмне забезпечення і має

бути готовим розуміти й застосовувати принципи безпеки на кожному етапі розробки.

4.1. Безпечне програмування: навчання студентів основам безпечного програмування, таким як використання бібліотек для захисту даних, правильне керування сесіями, уникання вразливостей, як, наприклад, buffer overflow, SQL Injection тощо.

4.2. Аналіз коду: вивчення методів статичного і динамічного аналізу коду для виявлення потенційних вразливостей і помилок програмного коду, які можуть стати об'єктами для атак.

5. *Навчальні платформи та інструменти* (Pelkonen, Savola & Salonen, 2017).

5.1. Онлайн-курси і платформи для навчання кібербезпеці: використання освітніх платформ, таких як Coursera, edX, Udemy, де є спеціалізовані курси з кібербезпеки, які включають в себе відеоуроки, лекції, практичні завдання та сертифікаційні програми.

5.2. Віртуальні лабораторії: створення або використання існуючих віртуальних лабораторій, де студенти можуть вивчати різні інструменти кібербезпеки і проводити тестування на проникнення, моніторити трафік і виконувати інші практичні завдання без шкоди для реальних систем.

6. *Методи оцінювання та зворотний зв'язок.* Для ефективного формування компетентності з кібернетичної безпеки важливо застосовувати різноманітні методи оцінки знань та навичок студентів.

6.1. Завдання на тестування безпеки: студенти можуть виконувати завдання, що включають виявлення вразливостей, аналіз атак, розробку протоколів безпеки.

6.2. Оцінка за допомогою змагань: використання змагань або імітаційних ігор, таких як Capture the Flag (CTF) або тестування на проникнення, де студентам надається сценарій реальної кіберзагрози, і вони повинні вирішити проблему.

6.3. Рефлексія та обговорення: після виконання завдань та проєктів важливо проводити обговорення і аналіз, щоб студенти мали можливість оцінити свою роботу і зрозуміти, що вони зробили правильно, а де могли б покращити результати.

7. *Підвищення кваліфікації через сертифікаційні програми.* Один із ефективних способів підвищити рівень компетентності – це сертифікаційні курси та програми, що підтверджують знання та навички в галузі кібербезпеки.

7.1. Сертифікація CISSP (Certified Information Systems Security Professional).

7.2. CEH (Certified Ethical Hacker): сертифікація для спеціалістів з етичного хакінгу.

7.3. CompTIA Security+: основна сертифікація для фахівців з інформаційної безпеки.

Таким чином, резюмуючи зазначені вище методи формування компетентності з кібернетичної безпеки у процесі професійної підготовки майбутніх інженерів-програмістів слід зазначити, що дані методи повинні бути комплексними, інтерактивними та практично орієнтованими. Вони мають поєднувати теоретичні знання з практичними навичками, використання реальних інструментів та технік для виявлення і захисту від кібератак. У результаті майбутні інженери-програмісти повинні бути готовими до вирішення реальних проблем безпеки, які вони можуть зустріти у своїй професійній діяльності.

Водночас заслуговує на увагу питання визначення сучасних засобів формування компетентності з кібернетичної безпеки під час навчання інженерів-програмістів. Так, засоби формування компетентності з кібернетичної безпеки – це різноманітні інструменти, методи та ресурси, які використовуються для розвитку знань, навичок і ставлення студентів до аспектів кібербезпеки. Вони сприяють інтеграції теоретичних знань з практичними навичками, а також дозволяють сформувати необхідні компетенції для ефективного реагування на сучасні кіберзагрози.

Аналізуючи наукову зарубіжну та вітчизняну літературу слід зазначити наявність значної кількості засобів формування компетентності з кібернетичної безпеки, які можна використати під час навчання інженерів-програмістів, однак враховуючи особливості підготовки вказаних фахівців доцільно *запропонувати наступні засоби (рисунок 2):*

1. *Програмне забезпечення та інструменти для тестування безпеки.* Для розвитку практичних навичок у галузі кібербезпеки студенти повинні працювати з реальними інструментами для тестування та захисту інформаційних систем (Sadovyi, & Tryfonova, 2024):

- Metasploit – популярний інструмент для вивчення вразливостей та тестування систем на проникнення.

- Wireshark – аналізатор мережевого трафіку, який дозволяє студентам вивчати мережеві протоколи та виявляти аномалії або зловмисний трафік.

- Nmap – інструмент для сканування мереж і пошуку відкритих портів або вразливих служб.

- Kali Linux – дистрибутив Linux, що містить набір інструментів для пентестингу та оцінки безпеки.

Використання цих інструментів дає можливість студентам на практиці ознайомитися

з техніками зламування, виявлення вразливостей, а також проведення тестування на проникнення.

2. *Віртуальні лабораторії та тренажери*. Віртуальні лабораторії та тренажери дозволяють інженерам-програмістам безпечно навчатися та набувати практичних навичок, не ризикуючи реальними системами. Такі лабораторії зазвичай створюються на основі віртуальних машин або контейнерів, де студенти можуть:

- практикуватися в аналізі інцидентів безпеки;
- відпрацьовувати методи захисту від атак (наприклад, firewall, IDS/IPS);
- моделювати реальні кіберінциденти та реагувати на них.

Прикладами таких ресурсів є (Szczepaniuk, & Szczepaniuk, 2022):

- TryHackMe – інтерактивні завдання для навчання кібербезпеці.
- Hack The Box – платформа для тестування навичок хакерів, яка пропонує різні рівні складності.
- Cyber Range – спеціалізовані тренувальні платформи для професіоналів з кібербезпеки.

3. *Онлайн-курси та навчальні платформи*. Вивчення кібербезпеки через онлайн-курси є дуже популярним засобом, який дозволяє отримати теоретичні знання та навички на основі сучасних практик і підходів. Деякі платформи пропонують інтерактивні курси, де студентам дають реальні завдання для розв'язання:

- Coursera – курси від провідних університетів та компаній з кібербезпеки.
- edX – платформа для навчання, яка пропонує курси з кібербезпеки від провідних університетів.
- Udemy – онлайн-курси з різних аспектів кібербезпеки, включаючи пентестинг, захист мереж тощо.

Зазначені курси часто мають інтерактивні завдання, тести та сертифікацію, що допомагає студентам перевірити свої знання.

4. *Системи управління навчанням (LMS).* Для організації навчального процесу в університетах чи на курсах часто використовують системи управління навчанням (LMS), які включають не лише матеріали для вивчення, а й інструменти для тестування, зворотного зв'язку та співпраці:

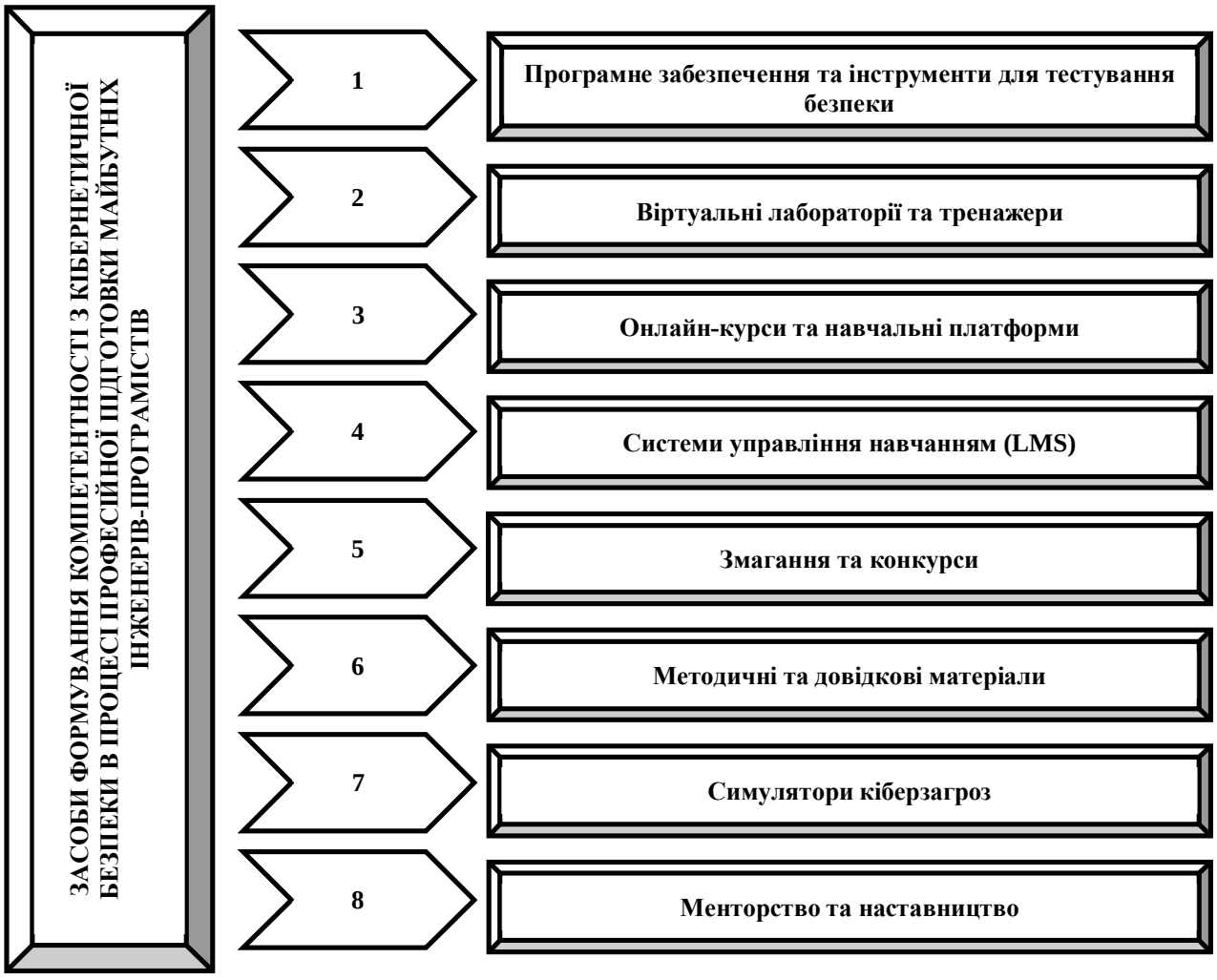

Рис. 2. Запропоновані засоби, використання яких доцільно для формування компетентності з кібернетичної безпеки в процесі професійної підготовки майбутніх інженерів-програмістів

- Moodle – платформа для створення онлайн-курсів, яка дозволяє організовувати завдання, тестування та взаємодію з студентами.

- Blackboard – система для управління навчанням, що включає модулі для створення інтерактивних завдань та тестів з кібербезпеки.

- Google Classroom – зручний інтерфейс для організації занять, дискусій та моніторингу прогресу студентів.

5. *Змагання та конкурси*. Змагання з кібербезпеки є чудовим способом стимулювати студентів до розвитку навичок. Участь у таких змаганнях дозволяє застосовувати теоретичні знання в реальних умовах:

- CTF (Capture The Flag) – популярний формат змагань з кібербезпеки, де учасники виконують завдання на виявлення вразливостей, злом систем та аналіз інцидентів.

- European Cyber Security Challenge (ECSC) – міжнародний конкурс, на якому студенти можуть продемонструвати свої навички у сфері кібербезпеки.

- National Collegiate Cyber Defense Competition (CCDC) – змагання для студентів, при якому команди змагаються в області захисту реальних мережевих систем.

6. Методичні та довідкові матеріали. Важливим засобом для навчання є доступ до сучасних підручників, статей, досліджень та довідкових матеріалів, які дозволяють студентам освоювати теоретичні основи кібербезпеки:

- Книги: «Кібербезпека» або «Інформаційна безпека та криптографія».

- Наукові журнали: публікації з кібербезпеки, як-от Journal of Cyber Security, IEEE Transactions on Information Forensics and Security.

- Блоги та ресурси: ресурси на зразок Dark Reading, KrebsOnSecurity, або блогів таких компаній, як Trend Micro або Symantec.

7. Симулятори кіберзагроз. Використання симуляторів кіберзагроз є корисним інструментом для підготовки до реальних атак. Такі симулятори дозволяють моделювати реальні сценарії кіберінцидентів, що допомагає студентам на практиці відпрацьовувати техніки виявлення, аналізу та реагування на загрози. Це можуть бути спеціалізовані програми або тренажери, які імітують атакуючі дії (злом, DDoS, фішинг тощо).

8. Менторство та наставництво. Ментори і наставники з досвідом у сфері кібербезпеки можуть бути незамінним засобом для формування компетентності. Вони надають студентам цінні поради, допомагають у вирішенні складних завдань і проєктів, а також сприяють професійному розвитку.

Отже, засоби формування компетентності з кібербезпеки мають бути інтегрованими та різноманітними, щоб ефективно поєднувати теорію та практику. Використання сучасних інструментів, тренажерів, навчальних платформ та змагань дозволяє студентам не лише засвоювати важливі концепції, а й набути необхідних навичок для роботи в умовах реальних кіберзагроз.

Висновки. Таким чином, формування компетентності з кібернетичної безпеки є важливою складовою сучасної освіти, оскільки кіберзагрози постійно зростають, і фахівці з цієї галузі користуються великим попитом. Водночас, формування компетентності з кібернетичної безпеки доцільно розглядати як процес набуття та розвитку у студентів або фахівців знань умінь і навичок, необхідних для ефективного виявлення, аналізу та захисту інформаційних систем, мереж і даних від різноманітних кіберзагроз.

Для досягнення формування компетентності з кібернетичної безпеки необхідно використовувати різні методи, які дозволяють розвивати не лише теоретичні знання, але й практичні навички. Серед яких: методи інтерактивного навчання, проектно орієнтоване навчання, метод кейс-стаді (Case Study), інтеграція кібербезпеки в курс програмування, навчальні платформи та інструменти, методи оцінювання та зворотний зв'язок, підвищення кваліфікації через сертифікаційні програми.

Крім того, у статті визначені сучасні засоби формування компетентності з кібернетичної безпеки, які доцільно використовувати у професійній підготовці майбутніх інженерів-програмістів. Це такі як: програмне забезпечення та інструменти для тестування безпеки: Metasploit, Wireshark, Nmap, Kali Linux; віртуальні лабораторії та тренажери: TryHackMe, Hack The Box, Cyber Range; онлайн-курси та навчальні платформи: Coursera, edX, Udemy; системи управління навчанням (LMS): Moodle, Blackboard, Google Classroom; змагання та конкурси: CTF (Capture The Flag), European Cyber Security Challenge (ECSC), National Collegiate Cyber Defense Competition (CCDC); методичні та довідкові матеріали: книги «Кібербезпека» або «Інформаційна безпека та криптографія», наукові публікації з кібербезпеки, блоги та ресурси; симулятори кіберзагроз; менторство та наставництво.

Підсумовуючи вищезазначене, можна дійти висновку, що формування компетентності з кібернетичної безпеки у процесі професійної підготовки майбутніх інженерів-програмістів є важливим завданням, оскільки забезпечення безпеки інформаційних систем і програмного забезпечення стає критичним аспектом сучасної IT-індустрії. Засоби формування компетентності з кібернетичної безпеки у процесі підготовки

майбутніх інженерів-програмістів включають як теоретичні, так і практичні методи, що дозволяють отримати всебічні знання та навички в цій критично важливій галузі. Сучасні методи навчання, інструменти для тестування безпеки, а також реальні проекти і взаємодія з професіоналами забезпечують високий рівень підготовки студентів, готових вирішувати завдання кібербезпеки в умовах швидко змінюваного технологічного середовища.

Перспективою подальших досліджень є детальний аналіз прикладного застосування запропонованих методів та засобів формування компетентності з кібернетичної безпеки у процесі підготовки майбутніх інженерів-програмістів.

Список використаних джерел

Alammari, A., Sohaib, O. & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Comput Sci*. URL: https://peerj.com/articles/cs-827/.

Buriachok, V., Bogush, V., Borsukovskii, Y., Skladannyi, P. & Borsukovska, V. (2018). Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. *Information Technologies and Learning Tools.* URL: https://journal.iitta.gov.ua /index.php/itlt/article/view/2347.

Calvani, A., Cartelli, A., Fini, A. & Ranieri, M. (2008). Models and instruments for assessing digital competence at school. *Journal of E-Learning and Knowledge Society*, 4, 183-193. https://doi.org/10.20368/1971-8829/288.

Cartelli, A. (2010). Frameworks for digital competence assessment: proposals, instruments and evaluation. *Proceedings of Informing Science & IT Education Conference*, 10, 561-574. URL: https://www.informingscience.org/ Publications/1274.

Falloon, G. (2020) From digital literacy to digital competence: the teacher digital competency (TDC) framework. *Education Technology Research Development*, 68, 2449–2472. https://doi.org/10.1007/s11423-020-09767-4.

Ferrari, A. (2012). Digital competence in practice: an analysis of frameworks. *European Union.* URL: https://op.europa.eu/ en/publication-detail/-/publication/2547ebf4-bd21-46e8-88e9-f53c1b3b927f/language-en.

Lehto, M. (2015). Cyber security competencies: cyber security education and research in Finnish universities. *ECCWS-Proceedings of the 14th European conference on cyber warfare & security*, 179-188. URL: https://jyx.jyu.fi/ bitstream/handle/123456789/46540/lehtoeccws2015.pdf ;sequence=1.

Pelkonen, A., Savola, R. & Salonen. J. (2017). Cybersecurity Competences – Research, Development and Innovation Perspective. *Engineering & Technology Reference*. URL: https://digital-library.theiet.org/doi/10.1049/etr. 2016.0184.

Sadovyi, M. & Tryfonova, O. (2024). Methods of forming cyber security competence of students of natural, mathematical and digital fields. *Innovate Pedagogy*, 2, 44-48. URL: https://www.researchgate.net/publication/ 379255709_METHODS_OF_FORMING_CYBER_ SECURITY_COMPETENCE_OF_STUDENTS_OF _NATURAL_MATHEMATICAL_AND _DIGITAL_FIELDS.

Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy*, 46 (3), 102282. URL: https://www.sciencedirect.com/ science/ article/pii/S0308596121001865?via%3Dihub.

Yaokumah, W. (2019). Cyber security competency model based on learning theories and learning continuum hierarchy. *Global cyber security labor shortage and international business risk*, 94-110. URL: https://www.igi-global.com/gateway/chapter/213448.

References

Alammari, A., Sohaib, O. & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Comput Sci*. https://peerj.com/articles/cs-827/ [in English].

Buriachok, V., Bogush, V., Borsukovsky, Y., Skladanny, P. & Borsukovska, V. (2018). Model of training specialists in the field of information and cybernetic security in higher education institutions of Ukraine. *Information Technologies and Learning Tools.* https://journal.iitta.gov.ua/index.php/itlt/article/ view/2347 [in Ukrainian].

Calvani, A., Cartelli, A., Fini, A. & Ranieri, M. (2008). Models and instruments for assessing digital competence at school. *Journal of E-Learning and Knowledge Society*, 4, 183-193. https://doi.org/10.20368/1971-8829/288 [in English].

Cartelli, A. (2010). Frameworks for digital competence assessment: proposals, instruments and evaluation. *Proceedings of Informing Science & IT Education Conference*, 10, 561-574. https://www.informingscience.org/Publications/1274 [in English].

Falloon, G. (2020) From digital literacy to digital competence: the teacher digital competency (TDC) framework. *Education Technology Research Development*, 68, 2449–2472. https://doi.org/10.1007/s11423-020-09767-4 [in English].

Ferrari, A. (2012). Digital competence in practice: an analysis of frameworks. *European Union.* https://op.europa.eu/en/ publication-detail/-/publication/2547ebf4-bd21-46e8-88e9-f53c1b3b927f/language-en [in English].

Lehto, M. (2015). Cyber security competencies: cyber security education and research in Finnish universities. *ECCWS-Proceedings of the 14th European conference on cyber warfare & security*, 179-188. https://jyx.jyu.fi/bitstream/ handle/123456789/46540/lehtoeccws2015.pdf; sequence=1 [in English].

Pelkonen, A., Savola, R. & Salonen, J. (2017). Cybersecurity Competences – Research, Development and Innovation Perspective. Engineering & Technology Reference. https://digital-library.theiet.org/doi/10.1049/etr.2016 .0184 [in English].

Sadovy, M. & Tryfonova, O. (2024). Methods of forming cyber security competence of students of natural, mathematical and digital fields. *Innovate Pedagogy*, 2, 44-48. https://www.researchgate.net/publication/ 379255709_METHODS_OF_FORMING_CYBER _SECURITY_COMPETENCE_OF_STUDENTS_OF _NATURAL_MATHEMATICAL_AND_DIGITAL _FIELDS [in Ukrainian].

Szczepaniuk, E.K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy*, 46 (3), 102282. https://www.sciencedirect.com/science/ article/pii/S0308596121001865?via%3Dihub [in English].

Yaokumah, W. (2019). Cyber security competency model based on learning theories and learning continuum hierarchy. *Global cyber security labor shortage and*

international business risk, 94-110. https://www.igi-global.com/gateway/chapter/213448 [in English].

Відомості про автора:
Комарницький Кирило Сергійович
kyrylo_komarnytskyi@mdpu.org.ua
Мелітопольський державний педагогічний університет імені Богдана Хмельницького
Наукове Містечко, вулиця, 59, Запоріжжя
Запорізька обл., 69000, Україна

doi: 10.33842/22195203-2025-34-135-191-199

Матеріал надійшов до редакції 05. 06. 2025 р.
Прийнято до друку 13. 06. 2025 р.

Information about the author:
Komarnytsky Kyrylo Serhiiovych
kyrylo_komarnytskyi@mdpu.org.ua
Bogdan Khmelnitsky Melitopol State Pedagogical University
Scientific Town, Street 59, Zaporizhzhia,
Zaporizhzhia region, 69000, Ukraine

doi: 10.33842/22195203-2025-34-135-191-199

Received at the editorial office 05. 06. 2025.
Accepted for publishing 13. 06. 2025.