КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1006
УДК 004.056.5, 378.147

**Кальченко Вадим Володимирович**
старший викладач кафедри кібербезпеки
Сумський державний університет, Суми, Україна
ORCID: 0000-0001-6492-3806
*v.kalchenko@ctois.sumdu.edu.ua*

**Любчак Володимир Олександрович**
к.ф.-м.н., доцент, завідувач кафедри кібербезпеки
Сумський державний університет, Суми, Україна
ORCID: 0000-0002-7335-6716
*v.liubchak@dcs.sumdu.edu.ua*

**Ободяк Віктор Корнелійович**
к.т.н., доцент, доцент кафедри кібербезпеки
Сумський державний університет, Суми, Україна
ORCID: 0000-0002-8539-1252
*v.obodyak@cs.sumdu.edu.ua*

**Пугач Ігор Олександрович**
асистент кафедри кібербезпеки
Сумський державний університет, Суми, Україна
ORCID: 0009-0002-9644-9357
*i.puhach@dcs.sumdu.edu.ua*

# ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ МАЙБУТНІХ ФАХІВЦІВ КІБЕРБЕЗПЕКИ ЗАВДЯКИ ІНІЦІАТИВІ «СТУДЕНТСЬКІ КІБЕРБРИГАДИ»

**Анотація.** У статті досліджується актуальна проблема підготовки фахівців у галузі кібербезпеки в умовах зростання кількості кіберзагроз і дефіциту кваліфікованих кадрів. Традиційні підходи до підготовки спеціалістів з кібербезпеки, які, в основному, базуються на лекційних та лабораторних заняттях, не в повній мірі відповідають вимогам сьогодення. Нинішній час характеризується стрімким розвитком інформаційних технологій, що вимагає постійного оновлення знань і навичок по захисту від кіберзлочинців. Відповідно зростає необхідність формування практичних навичок, які можна набути лише в умовах наближених до реального професійного середовища. Визначено, що ефективне формування професійних компетентностей майбутніх спеціалістів неможливе без постійної практичної підготовки, спрямованої на набуття реального досвіду роботи з інструментами кіберзахисту, аналізу та реагування на інциденти безпеки. Як один з варіантів покращення професійної підготовки майбутніх спеціалістів з кібербезпеки запропоновано модель інтеграції практичної підготовки у вигляді ініціативи студентські кібербригади. Ця ініціатива започаткована в Сумському державному університеті. Описано структуру організації діяльності таких студентських кібербригад, основні напрямки їх роботи та результати пілотного впровадження. Показано, що реалізація такої моделі сприяє одночасному зміцненню кіберстійкості об’єктів критичної інфраструктури та формуванню кадрового резерву у сфері кібербезпеки. Результати впровадження підтвердили ефективність запропонованого підходу та його відповідність сучасним потребам держави, освіти і бізнесу. Планується розширення мережі партнерських об’єктів критичної інфраструктури на яких будуть задіяні студентські кібербригади, удосконалення програм підготовки студентів з урахуванням новітніх кіберзагроз, інтеграцію результатів роботи кібербригад у національні платформи кіберзахисту, а також поступове впровадження моделі дуальної освіти для поглибленої професійної підготовки здобувачів вищої освіти у сфері кібербезпеки.

**Ключові слова:** кіберзахист; практична підготовка; студентські кібербригади; об’єкти критичної інфраструктури; професійні компетентності.

## ВСТУП

В умовах стрімкої цифровізації та постійного зростання інтенсивності кіберзагроз, виникає гостра потреба у висококваліфікованих фахівцях з кібербезпеки. Існуючий ринок праці демонструє значний кадровий дефіцит, який, за оцінками експертів, може сягати мільйонів спеціалістів. Ця нестача зумовлена також стрімким розвитком технологій, що вимагає постійного оновлення знань і навичок.

Поряд із дефіцитом професійних захисників, критичною проблемою залишається недостатній рівень кіберграмотності серед пересічних працівників державних установ та приватних підприємств. Статистика кіберінцидентів послідовно підтверджує, що саме людський фактор є найслабшою ланкою в системі інформаційної безпеки. Працівники, які не мають належних знань про основи цифрової гігієни, легко стають жертвами соціальної інженерії, зокрема фішингу та інших маніпулятивних технік. Такий низький рівень обізнаності створює внутрішній вектор загрози, оскільки необережна дія одного співробітника може скомпрометувати всю корпоративну мережу, незалежно від рівня захисту

Професійна підготовка фахівців у галузі кібербезпеки вимагає не лише ґрунтовного теоретичного знання, а й високого рівня практичних навичок. Практична складова навчального процесу виступає ключовим елементом у формуванні компетентностей, необхідних для ефективного реагування на сучасні кіберзагрози та забезпечення захисту інформаційних систем.

Зокрема, практика дозволяє студентам набути досвіду роботи з реальними інструментами та технологіями кіберзахисту, засвоїти методики виявлення, аналізу та нейтралізації кіберінцидентів, а також розвивати аналітичне мислення, необхідне для проведення розслідувань та аудиту безпеки. Окрім того, практична підготовка сприяє формуванню стійких навичок командної роботи в умовах динамічного та стресового середовища, що є характерним для сфери кібербезпеки.

Інтеграція практичних занять, лабораторних робіт, симуляцій кіберінцидентів, стажування в ІТ-компаніях або державних структурах у навчальний процес підвищує рівень професійної готовності випускників до виконання функціональних обов’язків у реальному середовищі.

**Постановка проблеми.** Кіберзагрози швидко еволюціонують, використовують новітні технології та вимагають від фахівців оперативного реагування, глибокого аналітичного мислення, вміння працювати з інструментами кіберзахисту, проводити тестування на вразливості та аналіз інцидентів безпеки. У зв’язку з цим зростає потреба у формуванні практичних навичок, які можна набути лише в умовах наближених до реального професійного середовища.

Першою проблемою є недостатній рівень кадрового потенціалу та функціональної спроможності об’єктів критичної інфраструктури (ОКІ). Значна частина персоналу цих об'єктів демонструє низьку обізнаність у питаннях кібербезпеки, що створює широке поле для успішного застосування методів соціальної інженерії та компрометації систем через людський фактор. Це обумовлює нагальну необхідність регулярного та якісного навчання, а також консультаційної підтримки персоналу ОКІ, спрямованої на впровадження базових принципів кібергігієни як первинного бар'єра захисту.

Другою проблемою є існуюча система підготовки фахівців у сфері кібербезпеки в закладах вищої освіти часто страждає від відірваності теоретичної підготовки від динамічної практичної складової. Випускники, попри ґрунтовну теоретичну базу, часто не мають необхідного досвіду роботи з реальними інструментами, архітектурами захисту

та унікальними інцидентами, що ускладнює їхню ефективну інтеграцію в професійне середовище. Необхідно забезпечити виконання вимог стандарту вищої освіти, зокрема в частині формування фахових компетентностей.

Для підготовки фахівців з кібербезпеки викликом є питання тривалості та змістовного наповнення практик, передбачених навчальним планом.

Навчальні практики мають обмежені терміни і часто зводяться до формального ознайомлення студентів зі структурою підприємства чи установи, не забезпечуючи глибинного занурення у реальні процеси забезпечення інформаційної безпеки. Для якісного формування компетентностей, необхідних сучасному фахівцю, потрібен триваліший період занурення у практичні ситуації. Це має бути не епізодичне спостереження, а безпосередня, пролонгована участь у проєктах кіберзахисту, що дозволяє відпрацювати навички командної взаємодії, ухвалення рішень та застосування складного інструментарію в умовах динамічної зміни кіберзагроз.

**Аналіз останніх досліджень і публікацій.** Питання підготовки фахівців з кібербезпеки розглядались багатьма авторами. Так наприклад в роботі Ю. Даника розглядається питання створення кіберполігонів, які надають можливість проведення досліджень та підготовки фахівців [2], іншою роботою обґрунтовується актуальність впровадження лабораторій для моделювання процесів в кібербезпеці [3].

Ящик О. Б., Ящик А. О. в роботі наголошують на необхідності комплексного підходу до формування професійних компетентностей здобувачів [4]. Проблеми підготовки фахівців та підходи до їх вирішення в роботі розглядали Ю. Є. Яремчук та В. С. Катаєв [5], в іншій роботі проведено аналіз системи компетентностей фахівців з кібербезпеки [6] та особливості освітнього процесу в університеті [7].

Питання європейської інтеграції та підготовки здобувачів розглядали Ю.В. Синявіна, І.В. Чалий, Т.А. Бутенко [8]. В дослідженні Б. В. Брайко розглянуто особливості підготовки магістрів з кібербезпеки в університетах Великої Британії [9], а в роботі Бистрової Б. В. вивчено досвід США [10]

**Мета статті.** Метою статті є обґрунтування значущості практичної підготовки у формуванні професійних компетентностей студентів спеціальності «Кібербезпека та захист інформації», пропозиція створення студентських кібербригад для покращення практичної складової підготовки та для можливої допомоги об’єктам проходження практики/стажування.

Діяльність студентських кібербригад виступає як інструмент реалізації Стандарту [1], пропонуючи студентам середовище для набуття інтегральних та спеціальних компетентностей в реальних умовах підприємства/організації. Ця діяльність набуває подвійного значення: одночасно підвищує якість підготовки фахівців, вирівнюючи їхні навички відповідно до вимог ринку, і слугує ефективним механізмом для підтвердження здобутих результатів навчання.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Практична підготовка у галузі кібербезпеки — це процес набуття студентами прикладних знань, умінь і навичок, які необхідні для виявлення, аналізу, попередження та нейтралізації кіберзагроз. Така підготовка охоплює різноманітні форми діяльності: лабораторні заняття, курсові проєкти, моделювання кіберінцидентів, участь у CTF-змаганнях, стажування тощо.

Практика сприяє розвитку компетентностей, серед яких ключовими є:

- вміння використовувати інструменти моніторингу та аналізу безпеки;

- здатність проводити тестування на на проникнення (penetration testing);
- навички оперативного реагування на інциденти;
- аналітичне мислення та здатність до системного підходу в ухваленні рішень;
- командна робота над попередженням кібератак та усуненням наслідків в разі їх реалізації.

Без постійної практики студенти не здатні сформувати стійкі навички, необхідні для роботи з сучасними технологіями та сценаріями атак.

Однією з можливостей є проходження стажувань на базі реальних підприємств, установ, організацій та інфраструктурних об'єктів, де функціонують сучасні інформаційно-комунікаційні системи системи. Такий формат навчання дозволяє студентам безпосередньо ознайомитися з особливостями забезпечення кіберзахисту в умовах реального ІТ-середовища.

Зокрема, студенти працюють з реальною мережевою інфраструктурою, політиками безпеки, системами моніторингу та аудиту, беруть участь у виявленні інцидентів безпеки й аналізі вразливостей. Вони взаємодіють з фахівцями-практиками, вивчаючи корпоративні стандарти інформаційної безпеки, та адаптуються до робочого середовища й організаційної культури, що є ключовим для професійної соціалізації. Крім того, стажування дає змогу ознайомитися з актуальними технологіями та програмними засобами, недоступними в закладах освіти, розширюючи технічні навички та формуючи конкурентоспроможність на ринку праці. Важливо, що стажування часто стає підґрунтям для подальшого працевлаштування, забезпечуючи плавний перехід від навчання до професійної діяльності.

З метою впровадження цього принципу в Сумському державному університеті (СумДУ) було започатковано ініціативу студентські кібербригади.

Поштовхом для створення цього проєкту було ознайомлення з досвідом кіберклінік в університетах США [11]. Ця освітня модель, що функціонує на базі університетів та коледжів і схожа за принципом дії на юридичні або медичні клініки. Вони мають подвійне призначення: забезпечити студентам практичний досвід у сфері кібербезпеки та одночасно підвищити кіберстійкість місцевих спільнот.

Ці клініки активно підтримуються та слугують критично важливим ресурсом для підвищення кіберстійкості громад, забезпечуючи безкоштовну допомогу організаціям із обмеженими ресурсами, як-от невеликі підприємства, некомерційні структури, лікарні та місцеві органи влади. Модель клінік створює кваліфіковану робочу силу, надаючи студентам із різним освітнім досвідом реальний практичний досвід у зміцненні цифрового захисту.

Актуальність цієї діяльності підтверджується тим, що для масштабування Google, інвестує до 1 мільйона доларів у кожну обрану установу [12]. Ця підтримка включає фінансування, доступ до сертифікації Google з кібербезпеки та менторську допомогу від співробітників Google.

Федеральне агентство США з питань кібербезпеки та безпеки інфраструктури (CISA) активно підтримує цю ініціативу, визнаючи клініки важливим фундаментом для своєї місії із захисту вразливих організацій. CISA публікує спеціальні рекомендації та ресурси для клінік та їх клієнтів, підвищує обізнаність про їх цінність, посилює взаємодію на місцевому рівні через своїх регіональних радників і розглядає клініки як ключовий канал рекрутингу майбутніх кіберфахівців [13].

Основними завданнями ініціативи студентських кібербригад є:

1) Підготовка висококваліфікованих молодих фахівців у галузі шляхом залучення здобувачів до реальних кейсів, обладнання, програмного забезпечення та інформаційних систем на об’єктах критичної інфраструктури.

2) Зміцнення кібербезпеки об'єктів критичної інфраструктури шляхом надання можливих консультацій, розробки та впровадження заходів безпеки, проведення навчань персоналу з кібергігієни.

Під час проходження стажування або виконання практичних завдань на об’єктах критичної інфраструктури студенти залучаються до виконання комплексу робіт, спрямованих на підвищення рівня кіберзахисту. До можливих видів діяльності, за узгодженням та завданнями керівництва ОКІ, належать:

1) Проведення навчання з основ кібергігієни для персоналу ОКІ. Студенти беруть участь в організації та проведенні освітніх заходів, спрямованих на підвищення обізнаності співробітників щодо базових принципів безпеки, типових кіберзагроз, правил безпечної поведінки в цифровому середовищі та реагування на інциденти.

2) Інвентаризація інформаційних активів. За згодою ОКІ здійснюється повна або вибіркова інвентаризація технічних засобів (комп’ютерної техніки, мережевого обладнання), а також ліцензійного та інстальованого програмного забезпечення. Метою є створення актуального реєстру активів, для проведення подальшої роботи з посилення рівня захищеності інформаційних ресурсів.

3) Аналіз вразливостей ІТ-інфраструктури. За погодженням та під керівництвом відповідальних спеціалістів студенти здійснюють сканування та аналіз комп’ютерних мереж з метою виявлення потенційних вразливостей. За результатами складаються звіти з рекомендаціями щодо усунення знайдених проблем. За погодженням керівництва ОКІ можливе практичне усунення виявлених недоліків.

4) Аудит облікових записів. Проводиться пошук облікових записів із паролями за замовчуванням в операційних системах, мережевому обладнанні та прикладному програмному забезпеченні. За необхідності виконується заміна паролів на більш складні, відповідно до внутрішніх політик безпеки або рекомендацій міжнародних стандартів.

5) Управління обліковими записами користувачів та контролем доступу. Студенти виконують завдання зі створення та налаштування облікових записів працівників, реалізують принцип мінімального необхідного доступу (Least Privilege), проводять базове налаштування групових політик та розмежування прав доступу до ресурсів.

6) Налаштування систем аудиту подій. Впроваджуються або оптимізуються механізми реєстрації подій у системах та мережах. Це охоплює налаштування журналів подій, логування критичних дій користувачів та спроб доступу, що є важливою складовою виявлення інцидентів безпеки.

7) Організація резервного копіювання критичних даних. Проводиться аудит поточної системи резервного копіювання або її впровадження з нуля, з урахуванням особливостей функціонування ОКІ. Визначаються типи даних, що підлягають збереженню, періодичність та методи резервного копіювання.

8) Безпечне налаштування програмного забезпечення та операційних систем. Студенти здійснюють налаштування компонентів ІТ-інфраструктури відповідно до актуальних рекомендацій національного (CERT-UA) та міжнародного рівня (Center for Internet Security – CIS Benchmarks). Це забезпечує відповідність систем найкращим практикам з захисту інформації. Надання студентам доступу до обладнання та інформаційно-комунікаційних мереж об’єктів критичної інфраструктури

здійснюватиметься виключно відповідно до чинної політики інформаційної безпеки конкретного об'єкта. У випадках, коли відповідний нормативний документ відсутній, порядок і умови доступу визначатимуться на основі погодження з керівництвом ОКІ та уповноваженими особами, відповідальними за функціонування й безпеку комп'ютерної мережі (зокрема, системним адміністратором, адміністратором безпеки тощо).

За потреби, а також відповідно до внутрішніх вимог та домовленостей із керівництвом об'єкта, передбачається оформлення студентами письмового зобов'язання про нерозголошення відомостей, які можуть стати їм відомими у процесі виконання робіт. Такий підхід забезпечує баланс між необхідністю практичної підготовки фахівців та дотриманням вимог інформаційної безпеки об'єкта.

Передбачувані результати цієї співпраці мають двовекторний характер. З одного боку, підвищується рівень захищеності інформаційно-комунікаційних систем об'єктів критичної інфраструктури шляхом виявлення та усунення потенційних вразливостей та прогалин в безпеці. З іншого боку, студенти отримують можливість закріпити теоретичні знання на практиці, розвинути професійні компетентності та сформувати передумови для подальшого працевлаштування за фахом, у тому числі безпосередньо на базі відповідного ОКІ.

Для пілотного впровадження ініціативи студентські кібербригади кафедрою кібербезпеки СумДУ завдяки постійним партнерам-роботодавцям та залученням нових зацікавлених сторін, було досягнуто домовленостей щодо організації діяльності студентських кібербригад на кількох об'єктах критичної інфраструктури. Окрім того, визначено низку інших підприємств та установ Сумської області, що виявили зацікавленість у співпраці.

Під час пілотного впровадження було сформовано три окремі кібербригади. Для забезпечення їх ефективної роботи проведено серію навчально-тренувальних заходів для студентів, що входять до складу зазначених команд. Програма підготовки передбачала: проведення очних навчальних занять; виконання індивідуальних завдань у форматі самостійної роботи; тестування здобутих знань і практичних навичок.

Для методичної та консультативної підтримки за кожною кібербригадою закріплено викладача-наставника. Навчальні завдання, що опрацьовувались студентами, були розроблені з урахуванням актуальних вимог Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) та погоджені після консультацій.

Для забезпечення оперативної комунікації між учасниками кібербригад і викладачами створено окремий канал у месенджері, що забезпечило швидкий обмін інформацією, координацію дій та вирішення поточних питань у режимі онлайн.

Спільно з керівництвом кожного ОКІ було узгоджено:

1) завдання для студентів у межах їхньої компетентності;
2) режим роботи та умови доступу;
3) призначено відповідальних кураторів від підприємств.

Протягом 2025 року кібербригади проходили стажування безпосередньо на визначених об'єктах. У межах цієї діяльності студентами виконувались такі завдання:

1) частковий огляд активів інформаційної системи та пошук вразливостей (у межах наданих прав доступу);
2) проведення консультацій з кібергігієни для співробітників;
3) аудит та налаштування безпечної роботи користувацьких робочих станцій;
4) створення та адміністрування облікових записів користувачів, розмежування доступу до інформаційних ресурсів;

5) моніторинг інформаційних ресурсів для виявлення кіберзагроз, зокрема дипфейків;

6) виявлення фішингових повідомлень та впровадження відповідних заходів протидії;

7) аналіз безпеки вебресурсів;

8) надання допомоги у розробленні внутрішніх нормативних документів з питань кіберзахисту та інформаційної безпеки.

За результатами роботи студентами були підготовлено узагальнені звіти (у варіантах, дозволених для відкритого доступу), які містили аналіз проведених заходів та рекомендації щодо підвищення рівня кіберзахисту відповідних ОКІ.

Паралельно було врегульовано питання зарахування участі у складі кібербригад як проходження навчальних практик студентами. Зокрема, діяльність кібербригад оформлюється як проходження стажування на підприємствах та організаціях-партнерах, результати якого зараховувались як виробнича та переддипломна практика. Такий підхід створює умови для інтеграції освітнього процесу з реальними потребами сфери кібербезпеки та підвищує рівень готовності випускників до роботи за фахом у сучасних умовах.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Пілотне впровадження ініціативи студентських кібербригад довело її практичну ефективність та доцільність інтеграції такого формату співпраці в освітній процес підготовки фахівців з кібербезпеки.

Запропонована модель забезпечує подвійний ефект: з одного боку, підвищується рівень захищеності інформаційно-комунікаційних систем підприємств та організацій, що належать до категорії ОКІ; з іншого боку, здобувачі вищої освіти отримують можливість опанувати сучасні методи виявлення та нейтралізації кіберзагроз у реальних умовах.

Впровадження механізму зарахування участі в кібербригадах як форми проходження практики відповідно до чинних нормативних документів Сумського державного університету (у тому числі за накопичувальною системою та з урахуванням результатів неформальної освіти) створює нормативно-правові підстави для стабільного розвитку цієї ініціативи та її масштабування.

Організаційна модель взаємодії (узгодження завдань, визначення рівнів доступу, призначення кураторів, створення каналів онлайн-комунікації) продемонструвала свою результативність, забезпечивши одночасно дотримання вимог інформаційної безпеки та комфортні умови для роботи студентів.

Ініціатива студентські кібербригади отримали підтримку від проекту USAID «Кібербезпека критично важливої інфраструктури України»

Отримані результати свідчать про потенціал даної ініціативи як складової формування кадрового резерву у сфері кібербезпеки, що відповідає актуальним потребам держави та бізнесу у кваліфікованих фахівцях, здатних працювати з об’єктами критичної інфраструктури.

Подальший розвиток ініціативи передбачає розширення мережі партнерських об’єктів критичної інфраструктури, удосконалення програм підготовки студентів з урахуванням новітніх кіберзагроз, інтеграцію результатів роботи кібербригад у національні платформи кіберзахисту, а також поступове впровадження моделі дуальної

освіти для поглибленої професійної підготовки здобувачів вищої освіти у сфері кібербезпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти, Наказ № 1074 (2018) (Україна). https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/12/21/125-Kiberbezpeka-bakalavr.20.01.22.pdf
2. Даник, Ю. (2019). Особливості створення кіберполігонів для дослідження комплексних кібердій та підготовки фахівців з кібербезпеки. *Сучасні інформаційні технології у сфері безпеки та оборони, 34*(1), 95–102. https://doi.org/10.33099/2311-7249/2019-34-1-95-102
3. Бурячок, В. Л., Шевченко, С. М., Складаний, П. М. (2018). Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(2), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104
4. Ящик, О. Б., Ящик, А. О. (2025). Професійна спрямованість навчання кібербезпеки студентів інженерних спеціальностей: особливості формування знань та вмінь. У Цифрова трансформація в освіті: виклики та перспективи (с. 198–201). Вид-во УДУ імені Михайла Драгоманова. https://enpuirb.udu.edu.ua/server/api/core/bitstreams/ce307511-660a-482c-8929-ad9271535916/content
5. Катаєв, В. С., Яремчук, Ю. Є. (2020). Проблеми підготовки фахівців у сфері кібербезпеки. Проблеми вищої математичної освіти: виклики сучасності. ВНТУ. https://conferences.vntu.edu.ua/index.php/pmovc/pmovc20/paper/view/10326
6. Горлинський, В. В., Горлинський, Б. В. (2021). Аналіз ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки. Information Technology and Security, 9(2), 219–231. https://doi.org/10.20535/2411-1031.2021.9.2.249976
7. Меркулова, К. В. (2018). Особливості підготовки фахівців з кібербезпеки у маріупольському державному університеті. У Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку (с. 59–61). Маріупольський державний університет.
8. Синявіна, Ю. В., Чалий, І. В., Бутенко, Т. А. (2024). Європейська інтеграція та практична підготовка фахівців з кібербезпеки: виклики і можливості. У Модернізація вищої освіти та забезпечення якості освітньої діяльності в умовах європейської інтеграції (с. 245–247). ДБТУ. https://repo.btu.kharkiv.ua/items/40e96ef8-bfd9-4281-8c05-57730ed6fbdb
9. Брайко, Б. В. (2020). Професійна підготовка магістрів з кібербезпеки в університетах Великої Британії [Автореф. дис. канд. пед. наук, Хмельницький національний університет]. https://elar.khmnu.edu.ua/items/85b986c1-c90d-4908-82a4-b954996d787e
10. Бистрова, Б. В. (2018). Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США [Дис. канд. пед. наук, Інститут педагогічної освіти і освіти дорослих]. https://ipood.com.ua/data/avtoreferaty_i_dysertatsii/2018/diser_BYSTROVA_pas.pdf
11. Fore, P., Suarez, J. (2023, 25 october). Google is providing $20 million to university-based cybersecurity clinics—empowering students to gain hands-on experience within their own communities | Fortune Education. Fortune Education. https://fortune.com/education/articles/consortium-of-cybersecurity-clinics-google-investment-cyber-learning-certificates/
12. Google Cybersecurity Clinics Fund. (б. д.). Google Cybersecurity Clinics Fund. https://cyberclinics.withgoogle.com/
13. CISA Publishes Guide to Support University Cybersecurity Clinics | CISA. (2024, 28 лютого). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/cisa-publishes-guide-support-university-cybersecurity-clinics

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

**Vadym V. Kalchenko**
Senior Lecturer at the Department of Cybersecurity
Sumy State University, Sumy, Ukraine
ORCID: 0000-0001-6492-3806
*v.kalchenko@ctois.sumdu.edu.ua*

**Volodymyr O. Liubchak**
Candidate of Physical and MathematicalSciences, Associate Professor,
Head of the Department of Cybersecurity Sumy
State University, Sumy, Ukraine
ORCID: 0000-0002-7335-6716
*v.liubchak@dcs.sumdu.edu.ua*

**Viktor K. Obodiak**
Candidate of Technical Science, Associate Professor,
Associate Professor of the Department of Cybersecurity
Sumy State University, Sumy, Ukraine
ORCID: 0000-0002-8539-1252
*v.obodyak@cs.sumdu.edu.ua*

**Ihor O. Puhach**
Assistant Lecturer Department of Cybersecurity
Sumy State University, Sumy, Ukraine
ORCID: 0009-0002-9644-9357
*i.puhach@dcs.sumdu.edu.ua*

# FORMATION OF COMPETENCES OF FUTURE CYBERSECURITY SPECIALISTS BY THE "STUDENT CYBERBRIGADES" INITIATIVE

**Abstract.** The article examines the current problem of training specialists in the field of cybersecurity in the context of the growing number of cyber threats and the shortage of qualified personnel. Traditional approaches to training cybersecurity specialists, which are mainly based on lectures and laboratory classes, do not fully meet the requirements of today. The present time is characterized by the rapid development of information technologies, which requires constant updating of knowledge and skills in protecting against cybercriminals. Accordingly, the need for the formation of practical skills that can be acquired only in conditions close to the real professional environment is increasing. It is determined that the effective formation of professional competencies of future specialists is impossible without constant practical training aimed at gaining real experience in working with cyber protection tools, analyzing and responding to security incidents. As one of the options for improving the professional training of future cybersecurity specialists, a model of integrating practical training in the form of the student cyber brigades initiative is proposed. This initiative was launched at Sumy State University. The organizational structure of such student cyber teams, the main areas of their work and the results of the pilot implementation are described. It is shown that the implementation of such a model contributes to the simultaneous strengthening of the cyber resilience of critical infrastructure facilities and the formation of a personnel reserve in the field of cybersecurity. The implementation results confirmed the effectiveness of the proposed approach and its compliance with the modern needs of the state, education and business. It is planned to expand the network of partner critical infrastructure facilities where student cyber teams will be involved, improve student training programs taking into account the latest cyber threats, integrate the results of the work of cyber teams into national cyber defense platforms, as well as gradually implement a dual education model for advanced professional training of higher education applicants in the field of cybersecurity.

**Keywords:** cyber defense; practical training; student cyber teams; critical infrastructure facilities; professional competencies.

## REFERENCES


1. Pro zatverdzhennia standartu vyshchoi osvity za spetsialnistiu 125 «Kiberbezpeka» dlia pershoho (bakalavrskoho) rivnia vyshchoi osvity, Nakaz No. 1074 (2018) (Ukraine). https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/12/21/125-Kiberbezpeka-bakalavr.20.01.22.pdf
2. Danyk, Y. (2019). Osoblyvosti stvorennia kiberpolihoniv dlia doslidzhennia kompleksnykh kiberdii ta pidhotovky fakhivtsiv z kiberbezpeky. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, *34*(1), 95–102. https://doi.org/10.33099/2311-7249/2019-34-1-95-102
3. Buriachok, V. L., Shevchenko, S. M., & Skladannyi, P. M. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of StudentS. *Cybersecurity: Education, Science, Technique*, (2), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104
4. Yashchyk, O. B., & Yashchyk, A. O. (2025). Profesiina spriamovanist navchannia kiberbezpeky studentiv inzhenernykh spetsialnostei: osoblyvosti formuvannia znan ta vmin. In *Tsyfrova transformatsiia v osviti: vyklyky ta perspektyvy* (pp. 198–201). Vyd-vo UDU imeni Mykhaila Drahomanova. https://enpuirb.udu.edu.ua/server/api/core/bitstreams/ce307511-660a-482c-8929-ad9271535916/content
5. Kataiev, V. S., & Yaremchuk, Yu. Ye. (2020). Problemy pidhotovky fakhivtsiv u sferi kiberbezpeky. In *Problemy vyshchoi matematychnoi osvity: vyklyky suchasnosti*. VNTU. https://conferences.vntu.edu.ua/index.php/pmovc/pmovc20/paper/view/10326
6. Horlynskyi, V. V., & Horlynskyi, B. V. (2021). Analiz kliuchovykh chynnykiv formuvannia systemy kompetentnostei fakhivtsiv u haluzi kiberbezpeky. *Information Technology and Security*, *9*(2), 219–231. https://doi.org/10.20535/2411-1031.2021.9.2.249976
7. Merkulova, K. V. (2018). Osoblyvosti pidhotovky fakhivtsiv z kiberbezpeky u mariupolskomu derzhavnomu universyteti. In *Kiberbezpeka u systemi natsionalnoi bezpeky Ukrainy: priorytetni napriamy rozvytku* (pp. 59–61). Mariupolskyi derzhavnyi universytet.
8. Syniavina, Yu. V., Chalyi, I. V., & Butenko, T. A. (2024). Yevropeiska intehratsiia ta praktychna pidhotovka fakhivtsiv z kiberbezpeky: vyklyky i mozhlyvosti. In *Modernizatsiia vyshchoi osvity ta zabezpechennia yakosti osvitnoi diialnosti v umovakh yevropeiskoi intehratsii* (pp. 245–247). DBTU. https://repo.btu.kharkiv.ua/items/40e96ef8-bfd9-4281-8c05-57730ed6fbdb
9. Braiko, B. V. (2020). *Profesiina pidhotovka mahistriv z kiberbezpeky v universytetakh Velykoi Brytanii* [Extended abstract of dissertation of Candidate of Pedagogical Sciences, Khmelnytskyi Natsionalnyi Universytet]. https://elar.khmnu.edu.ua/items/85b986c1-c90d-4908-82a4-b954996d787e
10. Bystrova, B. V. (2018). *Profesiina pidhotovka bakalavriv z kiberbezpeky u vyshchykh navchalnykh zakladakh SShA* [Dissertation of Candidate of Pedagogical Sciences, Instytut pedahohichnoi osvity i osvity doroslykh]. https://ipood.com.ua/data/avtoreferaty_i_dysertatsii/2018/diser_BYSTROVA_pas.pdf
11. Fore, P., & Suarez, J. (2023, October 25). *Google is providing $20 million to university-based cybersecurity clinics—empowering students to gain hands-on experience within their own communities | Fortune Education*. Fortune Education. https://fortune.com/education/articles/consortium-of-cybersecurity-clinics-google-investment-cyber-learning-certificates/
12. *Google Cybersecurity Clinics Fund*. (n.d.). Google Cybersecurity Clinics Fund. https://cyberclinics.withgoogle.com/
13. *CISA Publishes Guide to Support University Cybersecurity Clinics | CISA*. (2024, February 28). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/cisa-publishes-guide-support-university-cybersecurity-clinics