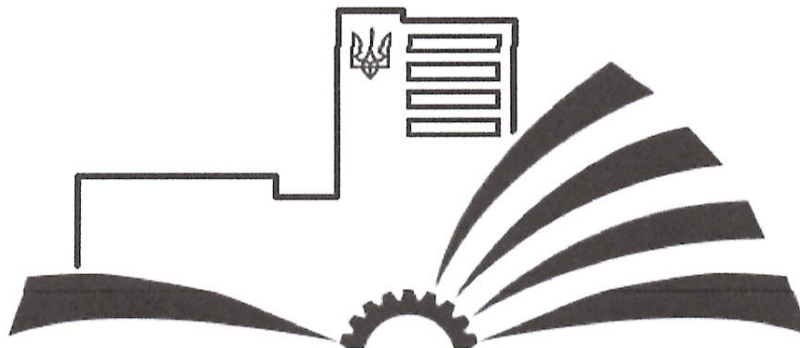


**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»**



**ОСВІТНЬО-НАУКОВА ПРОГРАМА**

**«Кібербезпека та захист інформації»**

**Третього (освітньо-наукового) рівня вищої освіти**  
**за спеціальністю F5 Кібербезпека та захист інформації**  
**галузі знань F Інформаційні технології**

**Кваліфікація: доктор філософії з кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ**

**Голова вченої ради**

**С.М. Шкарлет**

**(протокол № 13 від "23" грудня 2024 р.)**


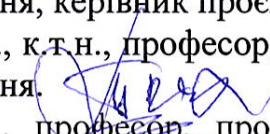

**Освітня програма вводиться в дію з 01 вересня 2025 р.**

**Ректор О.О. Новомлинцев**

**(наказ № 259/ВС від "23" грудня 2024 р.)**

## ПЕРЕДМОВА

Розроблено проектною групою у складі:

1. Шелест М.Є., д.т.н., професор, професор кафедри кібербезпеки та математичного моделювання, керівник проектної групи, гарант. 
2. Ткач Ю.М., д.пед.н., к.т.н., професор, завідувач кафедри кібербезпеки та математичного моделювання. 
3. Зайцев С.В., д.т.н., професор, професор кафедри інформаційних та комп'ютерних систем. 
4. Петренко Т.А., к.т.н., доцент кафедри кібербезпеки та математичного моделювання.

Розроблено на основі Стандарту вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» для третього (освітньо-наукового) рівня вищої освіти ступеня доктора філософії галузі знань 12 Інформаційні технології, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 29.10.2024 № 1543.

**1 Профіль освітньо-наукової програми «Кібербезпека та захист інформації» спеціальності F5 Кібербезпека та захист інформації**

| <b>1 – Загальна інформація</b>   |  |
|--|--|
| <b>Повна назва закладу вищої освіти та структурного підрозділу</b>   | Національний університет «Чернігівська політехніка».<br>Навчально-науковий інститут електронних та інформаційних технологій.<br>Кафедра кібербезпеки та математичного моделювання.   |
| <b>Ступінь вищої освіти та назва кваліфікації мовою оригіналу</b>  | Третій (освітньо-науковий) рівень вищої освіти<br>Освітня кваліфікація – доктор філософії з кібербезпеки та захисту інформації.  |
| <b>Офіційна назва освітньої програми</b>   | Освітньо-наукова програма «Кібербезпека та захист інформації»  |
| <b>Тип диплому, обсяг освітньої програми та форма здобуття вищої освіти</b>  | Диплом доктора філософії, одиничний, 60 кредитів ЄКТС (освітня складова), строк навчання - 4 роки, форма здобуття освіти – очна (денна, вечірня), заочна. Освітньо-наукова програма підготовки доктора філософії складається з освітньої та наукової складових. Наукова складова передбачає проведення власного дослідження та оформлення його результатів у вигляді дисертації. |
| <b>Наявність акредитації</b>   | Планова дата первинної акредитації -2028 рік   |
| <b>Цикл / рівень</b>   | QF-EHEA – третій цикл; EQF-LLL – 8 рівень; НРК України – 8 рівень  |
| <b>Передумови</b>  | Наявність освітнього ступеня магістра (ОКР спеціаліста)<br>Для здобуття освітнього ступеня доктор філософії зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, що здобули освітній ступінь магістр (ОКР спеціаліст).   |
| <b>Мова викладання</b>   | Українська   |
| <b>Термін дії освітньої програми</b>   | До заміни новою або до затвердження стандарту  |
| <b>Інтернет адреса постійного розміщення опису освітньої програми</b>  | <a href="https://op.stu.cn.ua/view/total_view.php">https://op.stu.cn.ua/view/total_view.php</a>  |
| <b>2 – Мета освітньо-наукової програми</b>   |  |
| Забезпечення фундаментальної та професійної підготовки висококваліфікованих, інтегрованих у світовий простір науковців, які здатні продукувати нові ідеї, розв'язувати комплексні проблеми в дослідницько-інноваційній та професійній діяльності, а також здійснювати науково-педагогічну діяльність у сфері кібербезпеки та захисту інформації. |  |
| <b>3 – Характеристика освітньо-наукової програми</b>   |  |
| <b>Предметна область (галузь знань, спеціальність)</b>   | Галузь знань: F Інформаційні технології.<br>Спеціальність: F5 «Кібербезпека та захист інформації».<br><b>Об'єкти вивчення та діяльності:</b><br>– інформаційні системи і технології на об'єктах інформаційної діяльності та критичної інфраструктури сфери кібербезпеки та захисту інформації;   |

|   |  |
|---|--|
|   | <p>– новітні системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення інформації (інформаційних потоків);</p> <p>– сучасні інформаційні ресурси різних класів (у тому числі державні інформаційні ресурси);</p> <p>– програмне та програмно-апаратне забезпечення (засоби) кіберзахисту;</p> <p>– автоматизовані системи управління інформаційною безпекою, кібербезпекою та захистом інформації;</p> <p>– методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації.</p> <p><b>Цілі навчання:</b> набуття здатності продукувати нові ідеї, розв’язувати комплексні проблеми професійної та дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, та здійснювати власні наукові дослідження, результати яких мають наукову новизну, теоретичне та практичне значення.</p> <p><b>Теоретичний зміст предметної області</b></p> <p>Принципи, концепції, теорії захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.</p> <p><b>Методи, методики та технології</b></p> <p>Сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, методи статистичного аналізу даних.</p> <p><b>Інструменти та обладнання</b></p> <p>Програмно-апаратне та програмне забезпечення, інструментальні засоби, комп’ютерна техніка, спеціальні контрольні-вимірні прилади, програмно-технічні засоби автоматизації та системи автоматизації проектування, виробництва, експлуатації, контролю, моніторингу, мережні, мобільні, хмарні технології, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків).</p> |
| <b>Орієнтація освітньої програми</b>                              | Освітньо-наукова, академічна.  |
| <b>Основний фокус (загальний, спеціальний) освітньої програми</b> | <p>Проведення досліджень в галузі F Інформаційні технології зі спеціальності F5 “Кібербезпека та захист інформації” та формування необхідних дослідницьких навиків для наукової кар’єри, викладання дисциплін у галузі кібербезпеки та захисту інформації.</p> <p><i>Базовий фокус ОП</i> – математичні методи кібербезпеки, системи, процеси кіберпростору, кіберфізичні системи, сучасні методи та засоби захисту.</p> <p><i>Ключові слова:</i> захист інформації, кібербезпека, інформаційна безпека, кіберпростір, кібератака, об’єкт інформаційної діяльності.</p>  |
| <b>Особливості програми</b>                                       | Освітньо-наукова програма спрямована на формування у здобувачів третього рівня вищої освіти дослідницьких навиків у сфері  |

|   |  |
|---|--|
|   | інформаційних технологій та кібербезпеки, викладацьких навиків у сфері інформаційної та кібербезпеки.  |
| <b>4 – Придатність випускників до працевлаштування та подальшого навчання</b> |  |
| <b>Придатність до працевлаштування</b>  | Працевлаштування на посадах наукових і науково-педагогічних працівників в наукових установах і закладах вищої освіти, посадах працівників найвищої кваліфікації у дослідницьких, проектних, конструкторських й т.п. установах і підрозділах підприємств.<br>Назва професій (робіт) згідно з Національним класифікатором України «Класифікатор професій» (ДК 003:2010):<br>1226.2 Начальник відділення установи, організації (сфера захисту інформації);<br>1229.7 (99) Керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної);<br>2149.2 Професіонал із організації інформаційної безпеки;<br>2149.2 Професіонал із організації захисту інформації з обмеженим доступом;<br>2149.1 Наукові співробітники (інформаційна та кібербезпека);<br>2149.2 Фахівець (сфера захисту інформації);<br>2310 Викладачі університетів та вищих навчальних закладів;<br>2310.1 Докторант;<br>2310.1 Доцент.  |
| <b>Подальше навчання</b>  | Доктор філософії має право на здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих.  |
| <b>5 – Викладання та оцінювання</b>   |  |
| <b>Викладання та навчання</b>   | Для освітньої складової: лекції, практичні заняття, консультації, самостійна робота, науково-педагогічна практика.<br>Для наукової складової: проведення наукового дослідження, консультування з науковим керівником, оприлюднення результатів досліджень, комунікації з представниками наукової спільноти, підготовка та захист дисертації.   |
| <b>Оцінювання</b>   | Оцінювання поділяється на оцінювання освітньої та наукової складової.<br>Оцінювання освітньої складової здійснюється під час екзаменів, заліків та захисту практики. Оцінюванню в балах з дисципліни підлягає рівень знань, умінь і навичок аспірантів, що визначається при проведенні контрольних заходів у ході освітнього процесу згідно з відповідними критеріями. Контрольні заходи містять поточний та підсумковий контроль. Поточний контроль включає оцінювання рівня знань, умінь і навичок аспірантів, що здійснюється в ході освітнього процесу шляхом проведення усного опитування, модульних контрольних робіт, тестування, семінарів тощо. Підсумковий контроль проводиться з метою оцінювання результатів навчання по завершенню певного освітнього компоненту. Підсумковий контроль містить модульний та семестровий контроль (диференційований залік чи екзамен). Оцінювання результатів проводиться відповідно до Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка». Оцінювання наукової складової здійснюється наприкінці кожного семестру у відповідності до індивідуального плану підготовки аспіранта на засіданні випускової кафедри за результатами заслуховування звіту аспіранта, який містить інформацію як про узагальнені результати наукової роботи, так і про їх апробацію у |

|   |   |
|---|---|
|   | вигляді опублікованих наукових статей, доповідей на конференціях, тощо.   |
| <b>6 – Програмні компетентності</b>                       |   |
| <b>Інтегральна компетентність</b>                         | Здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.  |
| <b>Загальні компетентності (ЗК)</b>                       | ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.<br>ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.<br>ЗК3. Здатність працювати в міжнародному контексті.<br>ЗК4. Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.   |
| <b>Спеціальні (фахові, предметні) компетентності (СК)</b> | СК1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації.<br>СК2. Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проекти в сфері кібербезпеки та захисту інформації.<br>СК3. Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики.<br>СК4. Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації.<br>СК5. Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень.<br>СК6. Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому українською та англійською мовами.<br>СК7. Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти. |
| <b>7 – Програмні результати навчання</b>                  |   |
|   | РН1. Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій.<br>РН2. Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики.   |

|  |  |
|--|--|
|  | <p>PH3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.</p> <p>PH4. Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці.</p> <p>PH5. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.</p> <p>PH6. Вільно презентувати та обговорювати з фахівцями і нефхівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних вітчизняних та міжнародних наукових виданнях.</p> <p>PH7. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації.</p> <p>PH8. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеці та захисту інформації та дотичних міждисциплінарних напрямках.</p> <p>PH9. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.</p> <p>PH10. Організувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.</p> |
| <b>8 – Ресурсне забезпечення реалізації програми</b> |  |
| <b>Кадрове забезпечення</b>                          | <p>Всі науково-педагогічні працівники, які забезпечують підготовку за освітньо-науковою програмою, мають відповідну кваліфікацію та відповідають профілю і напрямку дисциплін, що викладаються, мають необхідний стаж науково-педагогічної роботи та досвід практичної діяльності. Система підбору і розподілу кадрів в університеті вирішує завдання забезпечення освітнього процесу висококваліфікованими викладачами, здатними передавати здобувачам вищої освіти не лише традиційні знання, але й сучасні відомості з дисциплін, які забезпечують підготовку фахівця рівня доктора філософії. Наукові керівники мають значний досвід наукової роботи, відповідні наукові публікації, що внесені до наукометричних баз Scopus та Web of Sciences Core Collection, керували та брали участь у виконанні українських та міжнародних освітніх та наукових проектів.</p>  |
| <b>Матеріально-технічне забезпечення</b>             | <p>Освітній процес за ОНП забезпечений ресурсами (обладнанням, матеріалами тощо) та інфраструктурою (навчальними приміщеннями з мультимедійними проекторами, робочими місцями з відповідною комп'ютерною технікою), необхідною для забезпечення досягнення визначених в освітньо-науковій програмі результатів навчання.</p> <p>Для проведення наукових досліджень здобувачами освітньо-наукової програми в закладі створено спеціалізовані науково-дослідні</p>   |

|   |  |
|---|--|
|   | <p>лабораторії з необхідним лабораторним обладнанням та сучасною вимірювальною технікою, забезпечено безкоштовний безлімітний швидкісний доступ до мережі Інтернет (включаючи до публікацій зі спеціалізованих наукометричних баз), надано комп'ютеризовані робочі місця з встановленим спеціалізованим програмним забезпеченням.</p>  |
| <b>Інформаційне та навчально-методичне забезпечення</b> | <p>«Навчально-методичне забезпечення навчальних дисциплін (робочі програми навчальних дисциплін, силабуси, конспекти лекцій, методичні матеріали для проведення практичних (лабораторних) занять, самостійної та індивідуальної роботи здобувачів вищої освіти, завдання для поточного та підсумкового оцінювання знань, перелік рекомендованої літератури тощо) представлено в системі дистанційного навчання MOODLE НУ «Чернігівська політехніка». Здобувачі вищої освіти та викладачі можуть використовувати бібліотечно-інформаційну систему, наукову бібліотеку Університету. Інформаційні ресурси бібліотеки за освітньою програмою формуються відповідно до предметної області та сучасних тенденцій наукових досліджень у галузі. Ресурси Наукової бібліотеки НУ «Чернігівська політехніка» доступні через внутрішню та зовнішню мережі.</p> |
| <b>9 – Академічна мобільність</b>                       |  |
| <b>Національна кредитна мобільність</b>                 | <p>Реалізується в Університеті відповідно до вимог чинного законодавства та регулюється Положенням про академічну мобільність учасників освітнього процесу НУ «Чернігівська політехніка». Здійснюється на основі двосторонніх договорів між НУ «Чернігівська політехніка» та закладами вищої освіти України. Кредити, отримані в інших університетах України, перезараховуються відповідно до Порядку визначення академічної різниці та визнання результатів попереднього навчання в Національному університеті «Чернігівська політехніка».</p> <p>Національний університет «Чернігівська політехніка» в Україні співпрацює з науково-дослідними установами НАН України та промисловими підприємствами, підтримує тісні зв'язки із навчальними закладами України і установами спорідненого профілю на основі двосторонніх договорів.</p>             |
| <b>Міжнародна кредитна мобільність</b>                  | <p>Реалізується в університеті відповідно до вимог чинного законодавства та регулюється Положенням про академічну мобільність учасників освітнього процесу НУ «Чернігівська політехніка». Академічна мобільність ЗВО здійснюється на підставі угод про співробітництво між НУ «Чернігівська політехніка» та закладами вищої освіти зарубіжних країн-партнерів, затверджених в установленому порядку індивідуальних навчальних планів та робочих програм навчальних дисциплін. Індивідуальна академічна мобільність можлива за рахунок участі у програмі «Еразмус+» та інших програм.</p>   |
| <b>Навчання іноземних здобувачів вищої освіти</b>       | <p>Здійснюється відповідно до вимог чинного законодавства, Порядку організації набору та навчання (стажування) іноземців та осіб без громадянства у НУ «Чернігівська політехніка».</p>   |



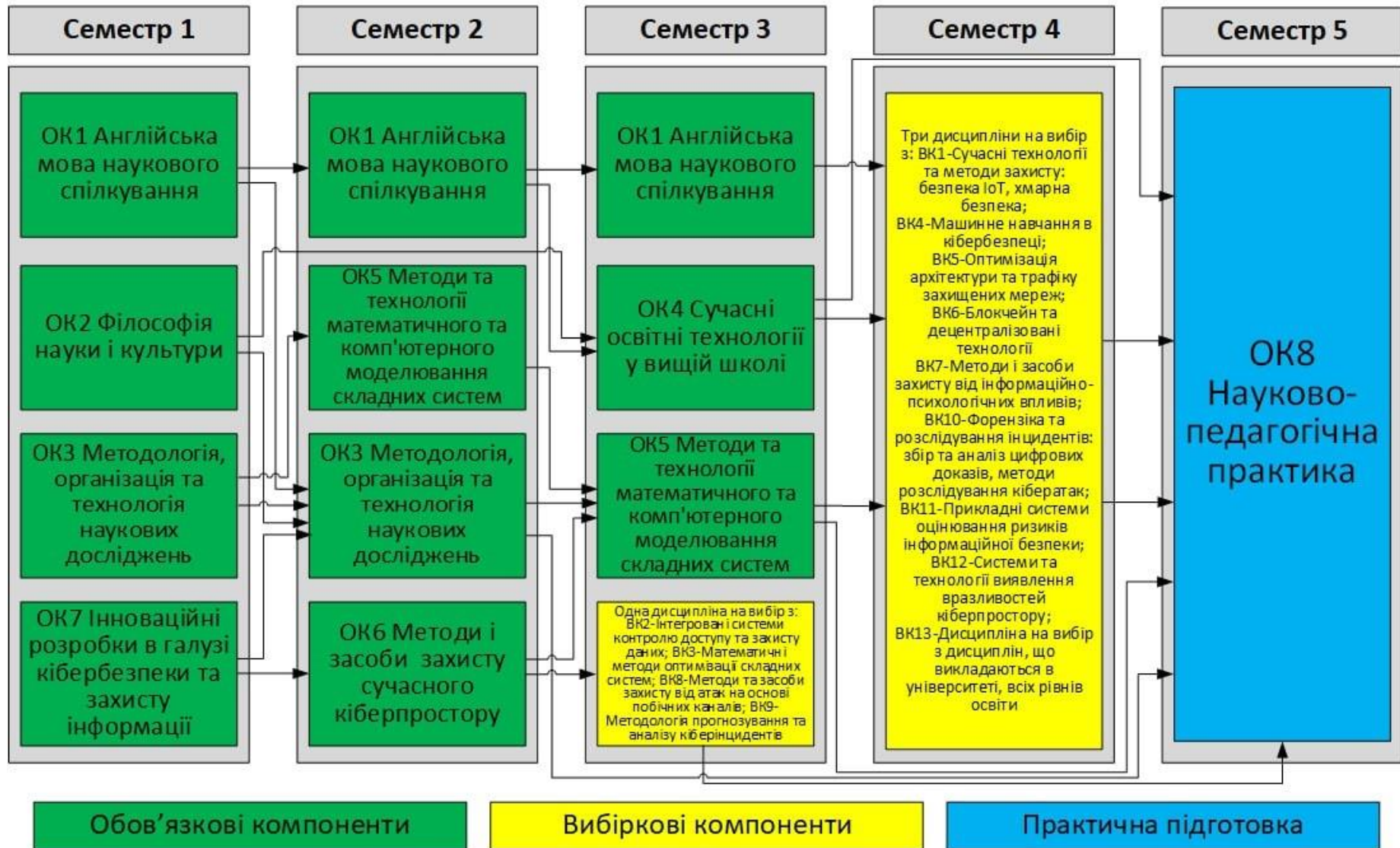
## 2 Перелік компонент освітньої програми та їх логічна послідовність

### 2.1 Перелік компонент освітньо-наукової програми (освітня складова)

| Код н/д   | Компонент освітньо-наукової програми<br>(навчальні дисципліни, курсові проекти/роботи, практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумкового контролю |
|---|---|--------------------|-----------------------------|
| 1   | 2   | 3                  | 4                           |
| <b>Обов'язкові компоненти ОНП</b>                 |   |                    |                             |
| <b>Цикл загальної підготовки</b>                  |   |                    |                             |
| OK1   | Англійська мова наукового спілкування   | 8                  | диф. залік<br>екзамен       |
| OK2   | Філософія науки і культури  | 6                  | екзамен                     |
| OK3   | Методологія, організація та технологія наукових досліджень  | 7                  | диф. залік<br>екзамен       |
| OK4   | Сучасні освітні технології у вищій школі  | 3                  | диф. залік                  |
| <b>Цикл професійної підготовки</b>                |   |                    |                             |
| OK5   | Методи та технології математичного та комп'ютерного моделювання складних систем   | 7                  | диф. залік<br>екзамен       |
| OK6   | Методи і засоби захисту сучасного кіберпростору   | 5                  | екзамен                     |
| OK7   | Інноваційні розробки в галузі кібербезпеки та захисту інформації  | 4                  | екзамен                     |
| <b>Загальний обсяг обов'язкових компонент</b>     |   | <b>40</b>          |                             |
| <b>Вибіркові компоненти ОНП</b>                   |   |                    |                             |
| BK1   | Сучасні технології та методи захисту: безпека IoT, хмарна безпека   | 4                  | екзамен                     |
| BK2   | Інтегровані системи контролю доступу та захисту даних   | 4                  | диф. залік                  |
| BK3   | Математичні методи оптимізації складних систем  | 4                  | диф. залік                  |
| BK4   | Машинне навчання в кібербезпеці   | 4                  | екзамен                     |
| BK5   | Оптимізація архітектури та трафіку захищених мереж  | 4                  | екзамен                     |
| BK6   | Блокчейн та децентралізовані технології   | 4                  | екзамен                     |
| BK7   | Методи і засоби захисту від інформаційно-психологічних впливів  | 4                  | екзамен                     |
| BK8   | Методи та засоби захисту від атак на основі побічних каналів  | 4                  | диф. залік                  |
| BK9   | Методологія прогнозування та аналізу кіберінцидентів  | 4                  | диф. залік                  |
| BK10  | Форензика та розслідування інцидентів: збір та аналіз цифрових доказів, методи розслідування кібератак                  | 4                  | екзамен                     |
| BK 11   | Прикладні системи оцінювання ризиків інформаційної безпеки  | 4                  | екзамен                     |
| BK 12   | Системи та технології виявлення вразливостей кіберпростору  | 4                  | екзамен                     |
| BK 13   | Дисципліна на вибір з дисциплін, що викладаються в університеті, всіх рівнів освіти                                     | 4                  | екзамен                     |
| <b>Загальний обсяг вибірових компонент</b>        |   | <b>16</b>          |                             |
| <b>Практична підготовка</b>                       |   |                    |                             |
| OK8   | Науково-педагогічна практика  | 4                  | диф. залік                  |
| <b>Загальний обсяг освітньо-наукової програми</b> |   | <b>60</b>          |                             |

## 2.2 Структурно-логічна схема освітньо-наукової програми

### Структурно-логічна схема дисциплін освітньо-наукової програми «Кібербезпека та захист інформації» третього (освітньо-наукового) рівня вищої освіти



## 2.3 Наукова складова освітньо-наукової програми

Наукова робота здобувача ступеня доктора філософії регламентується індивідуальним планом наукової роботи аспіранта.

| Курс | Зміст наукової складової  | Форми контролю  |
|------|---|---|
| 1    | Вибір та обґрунтування теми дисертації, розробка календарного плану його виконання.<br>Формулювання постановки задачі.<br>Огляд стану проблеми, вибір та обґрунтування методології проведення власного наукового дослідження.<br>Підготовка та публікація статті (у наукових фахових виданнях (вітчизняних або закордонних) за темою дослідження; участь у науково-практичних конференціях (семінарах) з публікацією тез доповідей. | Затвердження індивідуального плану роботи аспіранта.<br>Звітування про хід виконання індивідуального плану аспіранта двічі на рік. Надання науковим керівником та кафедрою висновків щодо виконання плану. Атестація аспіранта. |
| 2    | Проведення власного наукового дослідження згідно з індивідуальним планом роботи аспіранта.<br>Підготовка та публікація статті за темою дослідження у фахових наукових виданнях. Участь у наукових конференціях (семінарах).   | Звітування про хід виконання індивідуального плану аспіранта двічі на рік. Надання науковим керівником та кафедрою висновків щодо виконання плану.<br>Атестація аспіранта.  |
| 3    | Проведення власного наукового дослідження згідно з індивідуальним планом роботи аспіранта.<br>Підготовка та публікація статті за темою дослідження у фахових наукових виданнях.<br>Участь у наукових конференціях (семінарах).  | Звітування про хід виконання індивідуального плану аспіранта двічі на рік. Надання науковим керівником та кафедрою висновків щодо виконання плану. Атестація аспіранта.   |
| 4    | Аналіз та узагальнення отриманих результатів власного наукового дослідження, визначення рамок застосування моделей.<br>Підготовка та публікація статті за темою дослідження у фахових наукових виданнях.<br>Оформлення дисертації. Визначення повноти висвітлення результатів дисертації у наукових статтях.<br>Доповідь за результатами дисертаційної роботи на науковому семінарі. Підготовка документів до захисту.              | Звітування про хід виконання індивідуального плану аспіранта.<br>Підсумкова атестація.<br>Надання висновку про наукову новизну, теоретичне та практичне значення результатів дисертації.<br>Публічний захист дисертації.        |

### **3 Форма атестації здобувачів вищої освіти**

Атестація здобувачів освітнього рівня доктора філософії здійснюється у формі публічного захисту дисертації.

Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання комплексної проблеми в сфері кібербезпеки та захисту інформації, результати якого мають наукову новизну, теоретичне та практичне значення.

Дисертація не повинна містити академічного плагіату, фальсифікації, фабрикації.

Дисертація розміщується у репозиторії Університету (окрім робіт, які містять інформацію з обмеженим доступом).

Порядок розгляду та захисту дисертацій доктора філософії регламентується Положенням «Про організацію атестації здобувачів вищої освіти ступеня доктора філософії в Національному університеті «Чернігівська політехніка».

Дисертаційна робота повинна мати обсяг основного тексту 110 – 160 сторінок, що відповідає 4,5 – 7 авторським аркушам, (авторський аркуш дорівнює 40 000 символів). Дисертаційна робота має відповідати вимогам, встановленим законодавством.

У випадку успішного захисту дисертації здобувачу видається документ встановленого зразка про присудження йому ступеня доктора філософії із присвоєнням кваліфікації: доктор філософії з кібербезпеки та захисту інформації.

#### 4 Матриця відповідності програмних компетентностей компонентам освітньо-наукової програми

| Програмні компетентності | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 |
|--------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| ЗК01                     |     |     |     |     | +   |     |     | +   |     |
| ЗК02                     |     |     | +   |     |     | +   | +   | +   |     |
| ЗК03                     | +   |     |     |     |     |     |     |     |     |
| ЗК04                     |     | +   |     |     | +   |     |     |     |     |
| СК01                     |     |     |     |     |     |     | +   |     |     |
| СК02                     |     |     | +   |     |     | +   |     |     |     |
| СК03                     |     |     |     |     |     |     | +   | +   |     |
| СК04                     |     |     |     |     | +   |     |     | +   |     |
| СК05                     |     |     | +   |     |     | +   | +   |     |     |
| СК06                     | +   |     |     |     |     | +   |     | +   |     |
| СК07                     |     |     |     | +   |     |     |     |     | +   |

#### 5 Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-наукової програми

| Програмні результати навчання | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 |
|-------------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| РН01                          |     |     |     |     |     | +   | +   | +   |     |
| РН02                          |     | +   |     |     |     |     | +   |     |     |
| РН03                          |     | +   |     |     | +   |     |     |     |     |
| РН04                          |     |     |     |     |     |     | +   |     |     |
| РН05                          |     |     |     |     | +   |     |     |     |     |
| РН06                          | +   |     |     |     |     | +   |     |     |     |
| РН07                          |     |     |     |     | +   |     |     |     |     |
| РН08                          |     |     | +   |     | +   |     |     |     |     |
| РН09                          |     |     | +   |     |     |     |     | +   |     |
| РН10                          |     |     |     | +   |     |     |     |     | +   |

## **6 Перелік нормативних документів, на яких базується освітня програма**

1. Закон «Про вищу освіту» – <http://zakon4.rada.gov.ua/laws/show/1556-18>.
2. Закон «Про освіту» – <http://zakon5.rada.gov.ua/laws/show/2145-19>.
3. Національна рамка кваліфікацій – <http://zakon4.rada.gov.ua/laws/show/13412011-п>.
4. Перелік галузей знань і спеціальностей, 2015 – <http://zakon4.rada.gov.ua/laws/show/266-2015-п>.
5. Постанова Кабінету Міністрів України «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)» від 23 березня 2016 р. № 261 <https://zakon.rada.gov.ua/laws/show/261-2016-%D0%BF#Text>.
6. Постанова Кабінету Міністрів України від 12.01.2022 № 44 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (зі змінами). URL : <https://zakon.rada.gov.ua/laws/show/44-2022-%D0%BF#Text>
7. Методичні рекомендації щодо розроблення стандартів вищої освіти, затверджені наказом Міністерства освіти і науки України від 01.06.2017 р. № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584), схвалені сектором вищої освіти Науково-методичної Ради Міністерства освіти і науки України
8. Стандарт вищої освіти за спеціальністю 125 Кібербезпека для третього (освітньо-наукового) рівня вищої освіти. URL: <https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-doktor-filosofiyi-1543-vid-29-10-2024.pdf>