ПРОЄКТ

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 № __ від "__"_____ 2024 р.)

Освітня програма вводиться в дію з 01 вересня 2025 р.

Ректор _____ О.О. Новомлинець

(наказ № __ від "__"_____ 2024 р.)

Чернігів 2024

ПЕРЕДМОВА

Розроблено проєктною групою у складі:

1. Шелест М.Є., д.т.н., професор, професор кафедри кібербезпеки та математичного моделювання, керівник проєктної групи.
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.

Стандарт вищої освіти відсутній. ОНП відповідає восьмому кваліфікаційному рівню Національної рамки кваліфікацій до введення в дію офіційно затвердженого стандарту вищої освіти.

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

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Чернігівська політехніка». Навчально-науковий інститут електронних та інформаційних технологій. Кафедра кібербезпеки та математичного моделювання.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Третій (освітньо-науковий) рівень вищої освіти Освітня кваліфікація – доктор філософії з кібербезпеки та захисту інформації.
Офіційна назва освітньої програми	Освітньо-наукова програма «Кібербезпека та захист інформації»
Тип диплому, обсяг освітньої програми та форма здобуття вищої освіти	Диплом доктора філософії, одиничний, 60 кредитів ЄКТС (освітня складова), нормативний строк підготовки - 4 роки, форма здобуття освіти – очна, 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.
Наявність акредитації	Планова дата первинної акредитації -2028 рік
Цикл / рівень	QF-EHEA – третій цикл; EQF-LLL – 8 рівень; НРК України – 8 рівень
Передумови	Наявність ступеня магістр (ОКР спеціаліст) Для здобуття освітнього ступеня доктор філософії зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, що здобули освітній ступінь магістр (ОКР спеціаліст).
Мова викладання	Українська
Термін дії освітньої програми	До заміни новою або до затвердження стандарту
Інтернет адреса постійного розміщення опису освітньої програми	https://op.stu.cn.ua/view/total_view.php
2 – Мета освітньо-наукової програми	
Підготовка висококваліфікованого, конкурентоспроможного, інтегрованого в європейський та світовий науково-освітній простір фахівця ступеня доктора філософії в галузі інформаційних технологій за спеціальністю F5 «Кібербезпека та захист інформації». Розвинення в аспірантів дослідницьких навиків необхідних для цього рівня вищої освіти в предметній області, здатність використовувати і впроваджувати технології інформаційної та кібербезпеки, виконання оригінальних наукових досліджень, які направлені на отримання нових наукових знань і результатів для захисту дисертації.	
3 – Характеристика освітньо-наукової програми	
Предметна область (галузь знань, спеціальність,)	Галузь знань: F Інформаційні технології. Спеціальність:F5 «Кібербезпека та захист інформації». **Об'єкти вивчення та діяльності:**

	– інформаційні системи і технології на об'єктах інформаційної діяльності та критичної інфраструктури сфери кібербезпеки та захисту інформації; – новітні системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення інформації (інформаційних потоків); – сучасні інформаційні ресурси різних класів (у тому числі державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – автоматизовані системи управління інформаційною безпекою, кібербезпекою та захистом інформації; – методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації. **Цілі навчання:** 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. **Теоретичний зміст предметної області** 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. **Методи, методики та технології** 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. **Інструменти та обладнання** Програмно-апаратне та програмне забезпечення, інструментальні засоби, комп'ютерна техніка, спеціальні контрольно-вимірювальні 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).
Орієнтація освітньої програми	Освітньо-наукова програма, яка спрямована на актуальні аспекти спеціальності, в рамках якої можлива подальша наукова та викладацька діяльність.
Основний фокус (загальний, спеціальний) освітньої програми	Загальна освіта в галузі F Інформаційні технології зі спеціальності F5 «Кібербезпека та захист інформації». *Базовий фокус ОП* – математичні методи кібербезпеки, системи, процеси кіберпростору, кіберфізичні системи, сучасні методи та засоби захисту. *Ключові слова*: захист інформації, кібербезпека, інформаційна безпека, кіберпростір, кібератака, об'єкт інформаційної діяльності
Особливості програми	Освітньо-наукова програма спрямована на формування у здобувачів третього рівня вищої освіти міждисциплінарних дослідницьких

	навиків у сфері інформаційних технологій та кібербезпеки, викладацьких навиків у сфері інформаційної та кібербезпеки. Наукова складова освітньо-наукової програми передбачає проведення власного наукового дослідження та оформлення його результатів у вигляді дисертації
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	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. Назва професій (робіт) згідно з Національним класифікатором України «Класифікатор професій» (ДК 003:2010): 1226.2 Начальник відділення установи, організації (сфера захисту інформації); 1229.7 (99) Керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної); 2149.2 Професіонал із організації інформаційної безпеки; 2149.2 Професіонал із організації захисту інформації з обмеженим доступом; 2149.1 Наукові співробітники (інформаційна та кібербезпека); 2149.2 Фахівець (сфера захисту інформації); 2310 Викладачі університетів та вищих навчальних закладів; 2310.1 Докторант; 2310.1 Доцент.
Подальше навчання	Доктор філософії має право на здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Для освітньої складової: лекції, практичні заняття, консультації, самостійна робота, науково-педагогічна практика. Для наукової складової: проведення наукового дослідження, консультування з науковим керівником, оприлюднення результатів досліджень, спілкування з представниками наукової спільноти, підготовка та захист дисертації.
Оцінювання	Оцінювання поділяється на оцінювання освітньої та наукової складової. 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.
6 – Програмні компетентності	
Інтегральна компетентність	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.
Загальні компетентності (ЗК)	ЗК1. Здатність до абстрактного мислення, аналізу і синтезу. ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК3. Здатність працювати в міжнародному контексті. 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.
Спеціальні (фахові, предметні) компетентності (СК)	СК1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації. СК2. Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації. СК3. Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики. 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. 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. 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. СК7. Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти.
7 – Програмні результати навчання	
	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. 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. РН3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. РН4. 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. РН5. 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. РН6. Вільно презентувати та обговорювати з фахівцями і нефахівцями 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. РН7. 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. РН8. 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 кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах. РН9. 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. РН10. Організовувати 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.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, які забезпечують підготовку за освітньо-науковою програмою, мають відповідну кваліфікацію та відповідають профілю і напряму 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 науковометричних баз Scopus та Web of Sciences Core Collection, керували та брали участь у виконанні українських та міжнародних освітніх та наукових проєктів.
Матеріально-технічне забезпечення	100% аспірантів забезпечені 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.

	Для проведення наукових досліджень здобувачами освітньо-наукової програми в закладі створено спеціалізовані науково-дослідні лабораторії з необхідним лабораторним обладнанням та сучасною вимірювальною технікою, забезпечено безкоштовний безлімітний швидкісний доступ до мережі Інтернет (включаючи до публікацій з спеціалізованих науковометричних баз), надано комп'ютеризовані робочі місця з встановленим спеціалізованим програмним забезпеченням.
Інформаційне та навчально-методичне забезпечення	Всю необхідну інформацію аспіранти можуть знайти на сайті Національного університету «Чернігівська політехніка», що містить інформацію щодо освітньо-наукової програми, навчальної і наукової діяльності, структурних підрозділів, правил прийому, контактів тощо. Всі аспіранти мають доступ до фондів науково-технічної бібліотеки університету, де представлена література з питань комп'ютерних наук та інформаційних технологій, а також суміжних галузей науки - математики, фізики, радіотехніки, електротехніки, обчислювальної техніки. Навчально-методичні матеріали з всіх освітніх компонент програми розміщено в системі дистанційного навчання Moodle Національного університету «Чернігівська політехніка», через яку також здійснюється зв'язок з викладачами. При необхідності викладання курсів здійснюється в on-line режимі через систему Microsoft Teams. Публікації наукових статей аспірантів можуть здійснюватися безкоштовно у Науковому журналі «Технічні науки та технології» - фаховому виданні НУ «Чернігівська політехніка», що відноситься до категорії В. Міжнародні публікації та апробація результатів забезпечуються участю в Міжнародній науково-практичній конференції «Математичне та імітаційне моделювання систем. МОДС», яка проводиться щорічно в НУ «Чернігівська політехніка». Матеріали конференції видаються видавництвом Springer та індексуються науковометричною базою Scopus.
9 – Академічна мобільність	
Національна кредитна мобільність	Реалізується відповідно до Положення про академічну мобільність учасників освітнього процесу Національного університету «Чернігівська політехніка». Право здобувачів на академічну мобільність може бути реалізоване на підставі міжнародних договорів про співробітництво в галузі освіти та науки, міжнародних програм та проєктів, договорів про співробітництво між НУ «Чернігівська політехніка» та вітчизняними закладами вищої освіти (науковими установами) або їх основними структурними підрозділами, між НУ «Чернігівська політехніка» та іноземними закладами вищої освіти (науковими установами) та їх основними структурними підрозділами, а також може бути реалізоване здобувачем з власної ініціативи, підтриманої адміністрацією НУ «Чернігівська політехніка» на основі індивідуальних запрошень та інших механізмів. 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.
Міжнародна кредитна мобільність	Національний університет «Чернігівська політехніка» співпрацює з науково-дослідними і навчальними установами країн Європейського Союзу у рамках програми Еразмус+ (К1) та на основі двосторонніх договорів про співпрацю.

Навчання іноземних здобувачів вищої освіти	Здійснюється відповідно до вимог чинного законодавства, Порядку організації набору та навчання (стажування) іноземців та осіб без громадянства у НУ «Чернігівська політехніка». Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою задля їх адаптації в Україні. Дисципліни освітньо-наукової програми можуть викладатися українською або англійською мовою за бажанням іноземного здобувача вищої освіти.

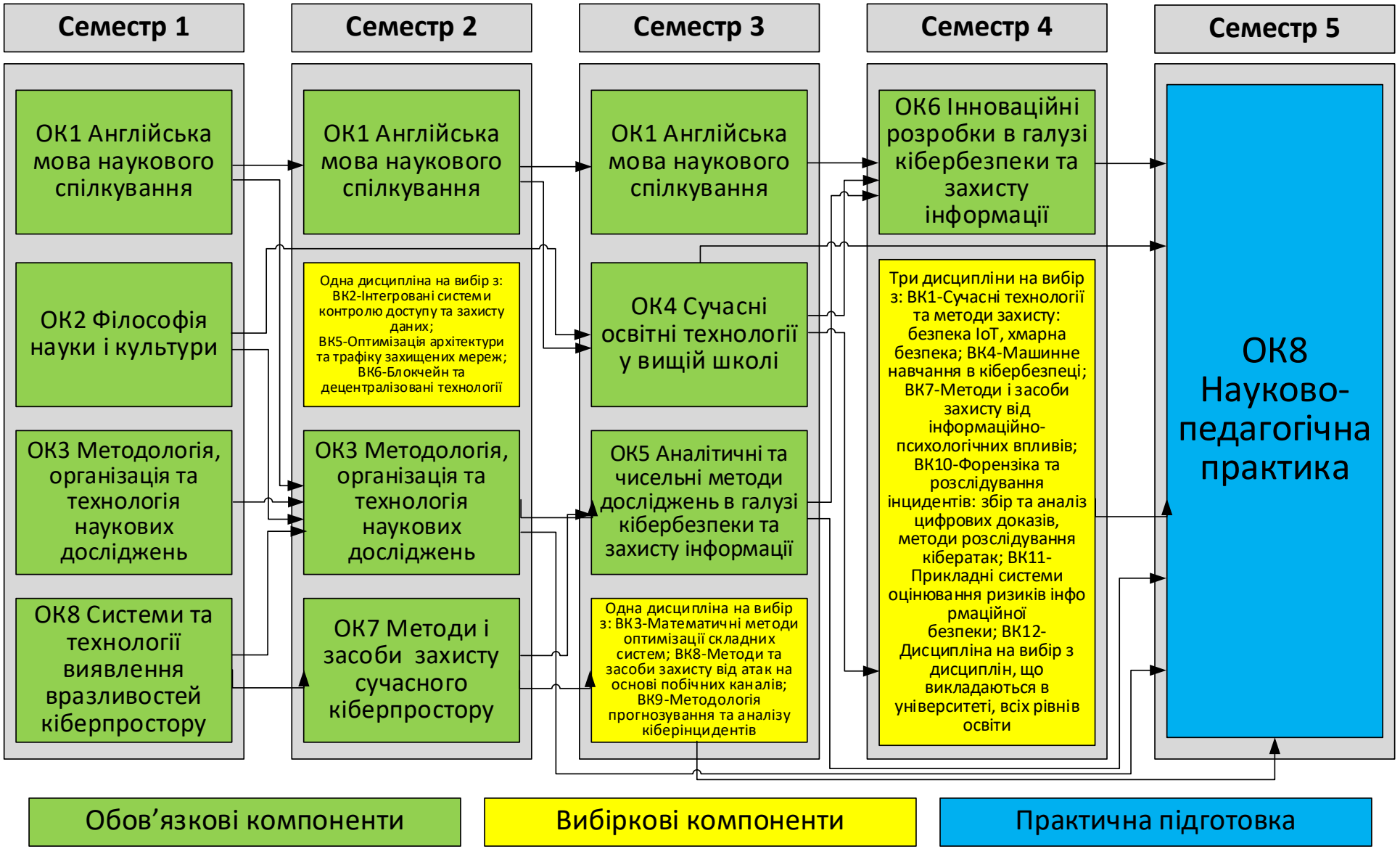
2 Перелік компонент освітньої програми та їх логічна послідовність

2.1 Перелік компонент освітньо-наукової програми (освітня складова)

Код н/д	Компонент освітньо-наукової програми (навчальні дисципліни, курсові проекти/роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОНП			
Цикл загальної підготовки			
ОК1	Англійська мова наукового спілкування	8	диф. залік екзамен
ОК2	Філософія науки і культури	6	екзамен
ОК3	Методологія, організація та технологія наукових досліджень	7	диф. залік екзамен
ОК4	Сучасні освітні технології у вищій школі	3	диф. залік
Цикл професійної підготовки			
ОК5	Аналітичні та чисельні методи досліджень в галузі кібербезпеки та захисту інформації	4	екзамен
ОК6	Інноваційні розробки в галузі кібербезпеки та захисту інформації	3	диф. залік екзамен
ОК7	Методи і засоби захисту сучасного кіберпростору	5	диф. залік екзамен
ОК 8	Системи та технології виявлення вразливостей кіберпростору	4	диф. залік екзамен
Загальний обсяг обов'язкових компонент		**40**	
Вибіркові компоненти ОНП			
ВК1	Сучасні технології та методи захисту: безпека IoT, хмарна безпека	4	екзамен
ВК2	Інтегровані системи контролю доступу та захисту даних	4	екзамен
ВК3	Математичні методи оптимізації складних систем	4	диф. залік
ВК4	Машинне навчання в кібербезпеці	4	диф. залік
ВК5	Оптимізація архітектури та трафіку захищених мереж	4	диф. залік
ВК6	Блокчейн та децентралізовані технології	4	диф. залік
ВК7	Методи і засоби захисту від інформаційно-психологічних впливів	4	екзамен
ВК8	Методи та засоби захисту від атак на основі побічних каналів	4	екзамен
ВК9	Методологія прогнозування та аналізу кіберінцидентів	4	диф. залік
ВК10	Форензіка та розслідування інцидентів: збір та аналіз цифрових доказів, методи розслідування кібератак	4	диф. залік
ВК 11	Прикладні системи оцінювання ризиків інформаційної безпеки	4	диф. залік
ВК 12	Дисципліна на вибір з дисциплін, що викладаються в університеті, всіх рівнів освіти	4	диф. залік
Загальний обсяг вибіркових компонент		**16**	
Практична підготовка			
ОК9	Науково-педагогічна практика	4	диф. залік
Загальний обсяг освітньо-наукової програми		**60**	

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. Формулювання постановки задачі. Огляд стану проблеми, вибір та обґрунтування методології проведення власного наукового дослідження. 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. 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. 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. Атестація аспіранта.
3	Проведення власного наукового дослідження згідно з індивідуальним планом роботи аспіранта. 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. Атестація аспіранта.
4	Аналіз та узагальнення отриманих результатів власного наукового дослідження, визначення рамок застосування моделей. Підготовка та публікація статті за темою дослідження у фахових наукових виданнях. Оформлення дисертації. Визначення повноти висвітлення результатів дисертації у наукових статтях. Доповідь за результатами дисертаційної роботи на науковому семінарі. Підготовка документів до захисту.	Звітування про хід виконання індивідуального плану аспіранта двічі на рік. Підсумкова атестація. Надання висновку про наукову новизну, теоретичне та практичне значення результатів дисертації. 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 має бути розміщена на сайті 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.

Дисертаційна робота перевіряється на плагіат згідно з Порядком проведення перевірки кваліфікаційних робіт та індивідуальних завдань здобувачів вищої освіти на плагіат в Національному університеті "Чернігівська політехніка" (https://stu.cn.ua/normatyvna-baza/normatyvne-zabezpechennya-osvitnogo-proczesu/) та після захисту розміщується в репозиторії Наукової бібліотеки для вільного доступу.

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 https://mon.gov.ua/ua/osvita/visha-osvita/naukovo-metodichna-radaministerstva-osviti-i-nauki-ukrayini/metodichni-rekomendaciyi-vo
8. Наказ Міністерства освіти і науки України «Про затвердження Вимог до міждисциплінарних освітніх (наукових) програм» від 01.02.2021 р. № 128 URL: https://zakon.rada.gov.ua/laws/show/z0454-21#Text
9. Стандарт вищої освіти за спеціальністю 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf .
10. Стандарт вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти. URL: https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx .