МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА

Першого (бакалаврського) рівня вищої освіти

за спеціальністю F5 Кібербезпека та захист інформації

галузь знань F Інформаційні технології

Кваліфікація: бакалавр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Голова Вченої ради
_____С.М. Шкарлет
(протокол № 2 від «27» січня 2025 р.)
Освітня програма вводиться в дію з 01 вересня 2025 р.

Ректор _____О.О. Новомлинець
(наказ №23/ВС від «27» січня 2025 р.)

Чернігів 2025

ПЕРЕДМОВА

Розроблено проєктною групою у складі:

1. Петренко Т.А., к.т.н., доцент кафедри кібербезпеки та математичного моделювання (керівник проектної групи).
2. Ткач Ю.М., завідувач, професор кафедри кібербезпеки та математичного моделювання, д.пед.н., професор.
3. Шелест М.Є., професор кафедри кібербезпеки та математичного моделювання, д.т.н., професор.

Розроблено відповідно до стандарту вищої освіти України за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології», затвердженого наказом МОН України від 04.10.2018 р. №1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 № 1547).

1. Профіль освітньо-професійної програми «Кібербезпека» зі спеціальності F5 Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Чернігівська політехніка» ННІ електронних та інформаційних технологій Кафедра кібербезпеки та математичного моделювання
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр. Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Кібербезпека
Тип диплому, обсяг освітньої програми та форма здобуття освіти	Тип диплому – одиничний. Диплом бакалавра, одиничний, 240 кредитів ЄКТС. Розрахунковий строк виконання освітньої програми – 4 роки. Форма здобуття освіти – очна (денна), заочна.
Наявність акредитації	Акредитаційна комісія МОН. Україна. Сертифікат Серія УД № 26017688 від 27 червня 2023 року. Термін дії сертифіката до 01.07.2026 року
Цикл/рівень	НРК України - 6 рівень, FQ-EHEA – перший цикл, EQF-LLL - 6 рівень
Передумови	Для здобуття освітнього ступеня бакалавра зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, які здобули повну загальну середню освіту. Прийом на основі здобутого ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством. При вступі на базі здобутих освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) може бути визнано та перезараховано не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців. При вступі на базі ступеня «бакалавр» за іншими спеціальностями може бути визнано та перезараховано результати навчання, отримані в межах попередньої освітньої програми обсягом не більше, ніж 90 кредитів ЄКТС.
Мова (и) викладання	Українська
Термін дії освітньої програми	до заміни новою
Інтернет адреса постійного розміщення опису освітньої програми	https://op.stu.cn.ua/view/total_view.php

2 – Мета освітньої програми	
Підготовка фахівців, здатних використовувати технології кібербезпеки, а також впроваджувати у всі сфери діяльності новітні інформаційні технології та програмне забезпечення	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань F Інформаційні технології Спеціальність F5 Кібербезпека та захист інформації **Об'єкти професійної діяльності випускників**: – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні ресурси і технології. **Цілі навчання**: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст предметної області**: Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, 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:** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Загальна освіта в галузі знань F Інформаційні технології за спеціальністю F5 Кібербезпека та захист інформації. Акцент на системному аналізі здобутків вітчизняних та зарубіжних дослідників для прийняття обґрунтованих професійних рішень за умов невизначеності та мінливості зовнішнього середовища з врахуванням резервів та можливостей інноваційного розвитку внутрішнього середовища підприємства на основі широкого використання сучасних інформаційних технологій. Ключові слова: кібербезпека, інформаційна безпека, інформаційні технології, захист інформації.
Особливості програми:	Формування компетентностей в умовах нестабільності інформаційного середовища на основі принципів інноваційного розвитку та сучасних інформаційних технологій.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	*Фахівець з кібербезпеки та захисту інформації може займати* посади у структурних підрозділах

	установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпеки та захист інформації
Подальше навчання	Випускники мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Основні підходи, методи та технології, які використовуються у даній програмі: проблемно-орієнтоване навчання, навчання в системі Moodle, самонавчання. Викладання проводиться у вигляді: лекцій, мультимедійних лекцій, семінарів, практичних занять, лабораторних робіт, самостійного навчання, індивідуальних завдань.
Оцінювання	Оцінювання рівня засвоєння освітньо-професійної програми здійснюється за допомогою поточного і підсумкового контролю (усні та письмові екзамени, диференційні заліки, залік, курсові роботи та проекти, презентації тощо), а також підсумкової атестації.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	ЗК1. Здатність застосовувати знання у практичних ситуаціях.
	ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
	ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
	ЗК4. Здатність спілкуватися іноземною мовою.
	ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
	ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.
	ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
	ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
	ЗК9. Здатність щодо ініціативності, відповідальності та навичок до безпечної діяльності відповідно до майбутнього профілю роботи, галузевих норм і правил, а також необхідного рівня індивідуального та колективного рівня безпеки у надзвичайних ситуаціях
Спеціальні (фахові, предметні) компетентності	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

	СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
	СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
	СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
	СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
	СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
	СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою
	СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
	СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.
	СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

7 – Програмні результати навчання (ПРН)

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
РНІЗ. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;
РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічною захисту інформації.
РН2l. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
РН22. Здатні до вирішення професійних задач діяльності, пов’язаних з забезпеченням життя, здоров’я і
працездатності під час роботи, оцінити середовище перебування щодо особистої безпеки, безпеки колективу, суспільства, провести моніторинг небезпечних ситуацій та обґрунтувати головні підходи та засоби збереження життя, здоров’я та захисту працівників в умовах загрози і виникнення небезпечних та надзвичайних ситуацій.
РН23 Вміти використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя з метою збереження та зміцнення власного здоров’я; дотримуватись гігієнічних вимог у процесі оздоровлення і тренувань; використовувати природні чинники з метою зміцнення здоров’я, підвищення працездатності та стійкості до захворювань
РН24 Здатність аналізувати і оцінювати явища розвитку українського суспільства в контексті світової історії, зіставляти історичні процеси з епохами, застосовувати набуті знання для аналізу сучасної ситуації й перспектив розвитку України, відстоювати національні інтереси держави.

8 – Ресурсне забезпечення реалізації програм	
Кадрове забезпечення	Кадрове забезпечення реалізації освітньої програми повністю відповідає ліцензійним умовам провадження освітньої діяльності. Підготовку фахівців спеціальності F5 «Кібербезпека та захист

	інформації» забезпечують висококваліфіковані науково-педагогічні кадри університету.
Матеріально-технічне забезпечення	Відповідно до ліцензійних вимог освітня програма має необхідне матеріально-технічне забезпечення, зокрема аудиторний та бібліотечні фонди, сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій, комп'ютерні класи, мультимедійний комплекс, гуртожитки та об'єкти соціально-побутової інфраструктури. Комп'ютерні лабораторії оснащені сучасними персональними комп'ютерами і підключені до локальної комп'ютерної мережі університету та мають вихід до Internet.
Інформаційне та навчально-методичне забезпечення	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, курсових робіт, 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.
9 – Академічна мобільність	
Національна кредитна мобільність	Реалізується в університеті відповідно до вимог чинного законодавства та регулюється Положенням про академічну мобільність учасників освітнього процесу НУ «Чернігівська політехніка». 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».
Міжнародна кредитна мобільність	Реалізується в університеті відповідно до вимог чинного законодавства та регулюється Положенням про академічну мобільність учасників освітнього процесу НУ «Чернігівська політехніка». Академічна мобільність здобувачів вищої освіти 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 програмам навчальних дисциплін. Індивідуальна академічна мобільність можлива за рахунок участі у програмі «Еразмус+» та інших програм).
Навчання іноземних здобувачів вищої освіти	Здійснюється згідно з вимогами чинного законодавства, Порядку організації набору та навчання (стажування) іноземців та осіб без громадянства у НУ «Чернігівська політехніка».

2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонент ОП

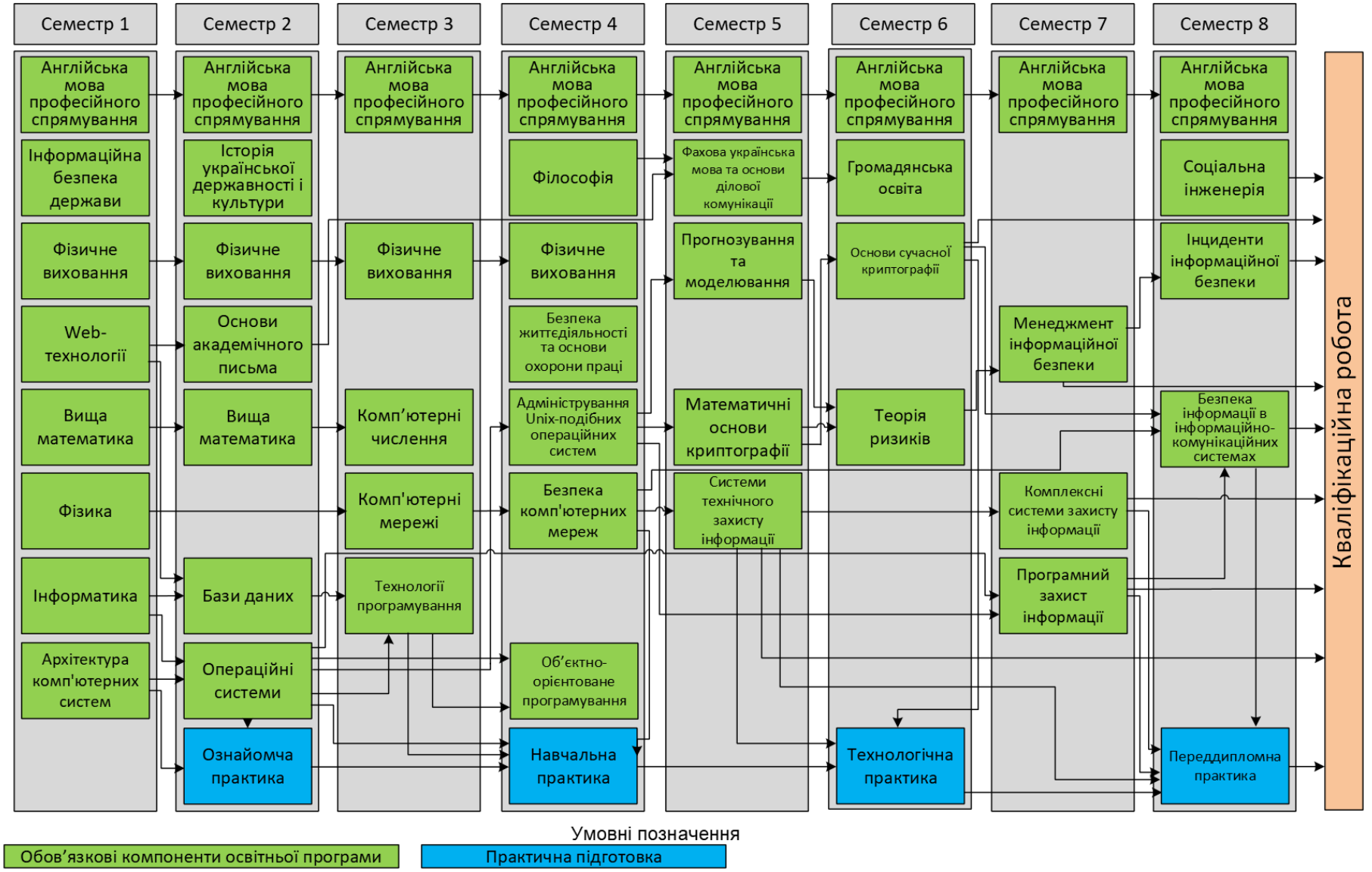
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
	2	3	4
Обов'язкові компоненти ОП (ОК)			
ОК 1	Історія української державності і культури	4	екзамен
ОК 2	Філософія	4	екзамен
ОК 3	Фахова українська мова та основи ділової комунікації	4	екзамен
ОК 4	Англійська мова професійного спрямування	16	диференційований залік, екзамен
ОК 5	Безпека життєдіяльності та основи охорони праці	3	диференційований залік
ОК 6	Основи академічного письма	3	диференційований залік
ОК 7	Громадянська освіта	3	диференційований залік
ОК 8	Фізичне виховання	12	залік
ОК 9	Вища математика	9	екзамен
ОК 10	Фізика	3	диференційований залік
ОК 11	Інформатика	5	екзамен
ОК 12	Інформаційна безпека держави	3	диференційований залік
ОК 13	Теорія ризиків	4	екзамен
ОК 14	Технології програмування	4	екзамен
ОК 15	Прогнозування та моделювання	4	диференційований залік
ОК 16	Основи сучасної криптографії	6	екзамен/ КР
ОК 17	Web-технології	5	екзамен
ОК 18	Архітектура комп'ютерних систем	4	екзамен
ОК 19	Операційні системи	5	екзамен
ОК 20	Бази даних	6	екзамен/ КР
ОК 21	Комп'ютерні мережі	6	екзамен/КП
ОК 22	Комплексні системи захисту інформації	4	екзамен
ОК 23	Менеджмент інформаційної безпеки	3	диференційований залік
ОК 24	Комп'ютерні числення	4	диференційований залік
ОК 25	Безпека комп'ютерних мереж	5	екзамен
ОК 26	Системи технічного захисту інформації	5	екзамен
ОК 27	Програмний захист інформації	4	екзамен
ОК 28	Соціальна інженерія	3	диференційований залік
ОК 29	Безпека інформації в інформаційно-комунікаційних системах	3	диференційований залік
ОК 30	Інциденти інформаційної безпеки	3	диференційований залік
ОК 31	Адміністрування Unix-подібних систем	3	диференційований залік
ОК 32	Об'єктно-орієнтоване програмування	3	диференційований залік

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
ОК 33	Математичні основи криптографії	3	диференційований залік
Загальний обсяг обов'язкових компонент:		**156**	
Вибіркові компоненти ОП (ВК)			
ВК 1.1.	Корпоративна культура	3	диференційований залік
ВК 1.2.	Тренінг-курс «Психологія ділових відносин»	3	диференційований залік
ВК 1.3.	Риторика	3	диференційований залік
ВК 1.4.	Тренінг-курс «Лідерство та «team-building»»	3	диференційований залік
ВК 1.5.	Комунікаційний менеджмент	3	диференційований залік
ВК 1.6.	Тренінг-курс «Креативне мислення та інтелектуальна власність»	3	диференційований залік
ВК 1.7.	Психологія впливу	3	диференційований залік
ВК 1.8.	Психологія успіху	3	диференційований залік
ВК 1.9.	Тренінг-курс «Сучасні медіа»	3	диференційований залік
ВК 1.10.	Generalist-курс	3	диференційований залік
ВК 1.11.	Презентації: мистецтво ефективної комунікації	3	диференційований залік
ВК 1.12.	Основи запобігання та протидії домашньому насильству	3	диференційований залік
ВК 1.13.	Антикорупція та доброчесність	3	диференційований залік
ВК 1.14.	Дисципліна на вибір з іншої ОП, яка формує соціальні навички (soft skills)	3	диференційований залік
Загальний обсяг вибіркових компонент: *(необхідно вибрати 1 дисципліну)*		**3**	
ВК 2.1	Сучасна економіка	3	диференційований залік
ВК 2.2	Управління бізнесом	3	диференційований залік
ВК 2.3	Фінансова грамотність	3	диференційований залік
ВК 2.4	Фінансово-економічна безпека	3	диференційований залік
ВК 2.5	Маркетинг	3	диференційований залік
ВК 2.6	Тренінг-курс «Start up creation»	3	диференційований залік
ВК 2.7	Економіка підприємства	3	диференційований залік
ВК 2.8	Правове регулювання підприємницької діяльності	3	диференційований залік
ВК 2.9	Дисципліна на вибір з іншої ОП, яка формує підприємницькі навички	3	диференційований залік
Загальний обсяг вибіркових компонент: *(необхідно вибрати 1 дисципліну)*		**3**	
ВК 3	Безпека в Smart технологіях	4	екзамен
ВК 4	Основи наукового дослідження	4	екзамен
ВК 5	Безпека операційних систем	4	екзамен

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
ВК 6	Комп'ютерна схемотехніка	4	екзамен
ВК 7	Психологія управління	4	екзамен
ВК 8	Комп'ютерна графіка	4	екзамен
ВК 9	Системне програмування	4	екзамен
ВК 10	Основи національної безпеки	4	екзамен
ВК 11	Системи банківської безпеки	4	екзамен
ВК 12	Адміністрування серверних систем Windows	4	екзамен
ВК 13	ECM – системи	4	екзамен
ВК 14	Фізичні основи технічних засобів розвідки	4	екзамен
ВК 15	Цифрова обробка сигналів	4	екзамен
ВК 16	Імітаційне моделювання	4	екзамен
ВК 17	Емпіричні дослідження	4	екзамен
ВК 18	Основи тестування програмного забезпечення	4	екзамен
ВК 19	Організаційне забезпечення захисту інформації	4	екзамен
ВК 20	Основи стеганографії	4	екзамен
ВК 21	Системи штучного інтелекту	4	екзамен
ВК 22	Експертні системи	4	екзамен
ВК 23	Програмування мобільних пристроїв	4	екзамен
ВК 24	Управління проектами	4	екзамен
ВК 25	Системи охорони державної таємниці	4	екзамен
ВК 26	Технології прикладного програмування	4	екзамен
ВК 27	Інтелектуальні системи кібербезпеки	4	екзамен
ВК 28	Організація та архітектура інфраструктури відкритих ключів	4	екзамен
ВК 29	Захист інформації	4	екзамен
ВК 30	Організація спеціального діловодства	4	екзамен
ВК 31	Датчики та виконавчі механізми систем безпеки	4	екзамен
ВК 32	Інтернет розвідка	4	екзамен
ВК 33	Blockchain: основи та приклади застосування	4	екзамен
ВК 34	Мережі мобільного зв'язку	4	екзамен
Загальний обсяг вибіркових компонент: *(необхідно вибрати 15 дисциплін)*		**60**	
ОК 34	Ознайомча практика	3	диференційований залік
ОК 35	Навчальна практика	3	диференційований залік
ОК 36	Технологічна практика	3	диференційований залік
ОК 37	Переддипломна практика	3	диференційований залік
ОК 38	Підготовка кваліфікаційної роботи	6	захист
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.2. Структурно-логічна схема ОП

Структурно-логічна схема дисциплін ОПП «Кібербезпека»
спеціальності F5 Кібербезпека та захист інформації
освітньо-кваліфікаційного рівня Бакалавр



3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту (ЄДКІ) та кваліфікаційної роботи.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених відповідним стандартом та цією освітньою програмою.

Кваліфікаційна робота має передбачати розв’язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації.

У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації.

Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) у репозитарії Університету.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

Обов'язкові компоненти (ОК)

	ОК 1.	ОК 2.	ОК 3.	ОК 4.	ОК 5.	ОК 6.	ОК 7.	ОК 8.	ОК 9.	ОК 10.	ОК 11.	ОК 12.	ОК 13.	ОК 14.	ОК 15.	ОК 16.	ОК 17.	ОК 18.	ОК 19.	ОК 20.	ОК 21.	ОК 22.	ОК 23.	ОК 24.	ОК 25.	ОК 26.	ОК 27.	ОК 28.	ОК 29.	ОК 30.	ОК 31.	ОК 32.	ОК 33.	ОК 34.	ОК 35.	ОК 36.	ОК 37.	ОК 38.
ЗК1.											+	+		+		+	+	+	+	+	+	+		+	+	+	+			+	+	+	+	+	+	+	+	+
ЗК2.										+	+	+		+		+	+		+	+	+	+		+	+	+	+		+	+	+	+		+	+	+	+	+
ЗК3.			+			+																																+
ЗК4.				+																																		
ЗК5.									+		+					+	+							+									+					
ЗК6.							+					+																										
ЗК7.						+	+																															
ЗК8.	+	+						+																														
ЗК9.					+																																
СК1.												+										+								+				+	+	+		+
СК2.															+		+				+	+			+				+	+	+			+	+	+	+	+
СК3.																							+															
СК4.																	+	+	+	+	+	+			+	+			+	+	+							+
СК5.														+				+	+		+	+			+		+		+	+	+	+						
СК6.																						+				+											+	
СК7.													+									+	+															
СК8.																+																			+			
СК9.																						+				+										+		
СК10.																			+			+	+			+	+	+	+	+	+							+

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми.

Обов'язкові компоненти (ОК)

	ОК 1.	ОК 2.	ОК 3.	ОК 4.	ОК 5.	ОК 6.	ОК 7.	ОК 8.	ОК 9.	ОК 10.	ОК 11.	ОК 12.	ОК 13.	ОК 14.	ОК 15.	ОК 16.	ОК 17.	ОК 18.	ОК 19.	ОК 20.	ОК 21.	ОК 22.	ОК 23.	ОК 24.	ОК 25.	ОК 26.	ОК 27.	ОК 28.	ОК 29.	ОК 30.	ОК 31.	ОК 32.	ОК 33.	ОК 34.	ОК 35.	ОК 36.	ОК 37.	ОК 38.
РН1.			+			+																															+
РН2.				+																																	
РН3.						+	+																														
РН4.											+	+		+			+							+								+					+
РН5.											+																		+						+	+	+
РН6.		+															+	+						+											+	+	+
РН7.																+	+							+								+					+
РН8.									+	+														+								+					
РН9.												+										+								+			+	+			+
РН10.															+		+				+	+			+				+	+	+				+	+	+	+
РН11.																							+															
РН12.																	+	+	+	+	+	+			+	+			+	+	+							+
РН13.																	+	+	+	+	+	+			+	+			+	+	+			+	+	+	+	+
РН14.														+				+	+		+	+			+		+		+	+	+	+						
РН15.														+				+	+		+	+			+		+		+	+	+	+						
РН16.																						+				+												
РН17.													+									+	+															
РН18.																+																						
РН19.																+																						
РН20.																						+				+										+	+	
РН21.																			+			+	+		+	+	+	+	+	+	+							+
РН22.					+																																	
РН23.								+																														
РН24.	+																																					

6. Перелік нормативних документів, на яких базується освітня програма

1. Про вищу освіту. - Закон України від 01.07.2014р. № 1556-VII // ВВРУ від 19.09.2014р., № 37-38, стор. 2716, стаття 2004. URL: https://zakon.rada.gov.ua/laws/show/1556-18
2. Про освіту. - Закон України від 5 вересня 2017р. № 2145-VIII // ВВРУ від 29.09.2017р., №38-39, стор. 5, стаття 380. URL: https://zakon.rada.gov.ua/laws/show/2145-19
3. Національний класифікатор України: «Класифікатор професій» ДК 003:2010 (Редакція від 25.10.2021). URL: http://zakon.rada.gov.ua/rada/show/va327609-10
4. Національна рамка кваліфікацій. - Постанова КМУ від 23 листопада 2011 р. № 1341 // ОВУ від 06.01.2012р., № 101, стор. 15, ст. 3700, код акта 59774/2011. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-п
5. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. - Постанова КМУ від 29 квітня 2015р. № 266 // ОВУ від 22.05.2015р., №38, стор. 194, ст. 1147, код акта 76797/2015. URL: https://zakon.rada.gov.ua/laws/show/266-2015-п
6. Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015р. № 1187 // ОВУ від 02.02.2016р., № 7, стор. 23, ст. 345, код акта 80480/2016. URL: https://zakon.rada.gov.ua/laws/show/1187-2015-п
7. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. URL: https://naqa.gov.ua/wp-content/uploads/2019/07/Додаток-1.-Стандарти-і-рекомендації-щодо-забезпечення-якості-в-Європейському-просторі-вищої-освіти.pdf
8. Стандарт вищої освіти України першого (бакалаврського) рівня, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека. Наказ Міністерства освіти і науки України 04.10.2018 р. № 1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 №11547). https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-bakalavr-1547-vid-29-10-2024.pdf