

МІНІСТЕРСТВО НАУКИ І ОСВІТИ УКРАЇНИ
Національний університет водного господарства та природокористування

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
"Інформаційна безпека"
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 НУВГП



Голова вченої ради

Мошинський В.С.

протокол № 7 від 09.07.2025 р.

Освітня програма вводиться в дію з 01.09.2025 р.

Ректор

Мошинський В.С.

наказ № 496 від 14.07.2025р

Рівне-2025

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
"Інформаційна безпека"
першого освітнього рівня вищої освіти
за спеціальністю F5 Кібербезпека та захист інформації

РОЗГЛЯНУТО

На засіданні кафедри обчислювальної техніки

Протокол № 14 від 13 серпня 2025р.

СХВАЛЕНО

Науково-методичною радою з якості ННІ кібернетики, інформаційних технологій та інженерії. Протокол № 7 від 19 серпня 2025р.

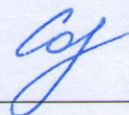
СХВАЛЕНО

Вченою радою ННІ кібернетики, інформаційних технологій та інженерії

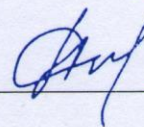
Протокол № 5 від 20 серпня 2025р.

ПОГОДЖЕНО

Проректор з науково-педагогічної
та навчальної роботи

 Сорока В.С.

Завідувач навчально-методичного
відділу

 Ковальчук Н.С.

ПЕРЕДМОВА

Розробники освітньої програми:

- | | |
|---|---|
| 1. Назарук Віталій
Дмитрович (гарант ОП) | – канд. техн. наук, старший викладач
кафедри обчислювальної техніки,
Директор інформаційно-обчислювального
центру Національного університету
водного господарства та
природокористування |
| 2. Сидор Андрій
Іванович | – канд. техн. наук, в.о. завідувача кафедри
обчислювальної техніки Національного
університету водного господарства та
природокористування |
| 3. Бабич Сергій
Васильович | – канд. техн. наук, старший викладач
кафедри обчислювальної техніки
Національного університету водного
господарства та природокористування |
| 4. Кіндрат Павло
Вадимович | – канд. юрид. наук, доцент кафедри
обчислювальної техніки Національного
університету водного господарства та
природокористування |
| 5. Герус Володимир
Андрійович | – старший викладач кафедри
обчислювальної техніки Національного
університету водного господарства та
природокористування |
| 6. Онищук Гліб
Олександрович | – студент Національного університету
водного господарства та
природокористування |

Рецензії стейкхолдерів

1. ТОВ «СМАРТ-КОРП»
2. ТОВ «Українські інформаційні технології»
3. «Рівненська обласна клінічна лікарня імені Юрія Семенюка» РОР

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

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Національний університет водного господарства та природокористування, Навчально-науковий інститут кібернетики, інформаційних технологій та інженерії, кафедра обчислювальної техніки.
Рівень вищої освіти	Перший (бакалаврський) рівень
Офіційна назва освітньої програми	Освітньо-професійна програма "Інформаційна безпека" ID 81682
Галузь знань, спеціальність, спеціалізація (за наявності)	F "Інформаційні технології", F5 "Кібербезпека та захист інформації"
Назва кваліфікації, професійна кваліфікація (за наявності)	Бакалавр з кібербезпеки та захисту інформації
Тип диплому, обсяг освітньої програми, форми здобуття освіти та розрахункові строки виконання ОП	Диплом бакалавра; одиничний; денна, заочна, дуальна; 240 кредитів ЄКТС; термін навчання: денна, заочна, дуальна форми – 3 роки 10 місяців
Наявність акредитації	Ні
Цикл/рівень	Перший (бакалаврський) рівень / НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF LLL – 6 рівень.
Передумови	Наявність повної загальної середньої освіти; ступень «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») з можливістю визнання та перерахування 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста); ступень «фаховий молодший бакалавр» з можливістю визнання та перерахування 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти.
Мова(и) викладання	Українська
Термін дії освітньої програми	Рік вступу 2025 та наступні до нової редакції освітньої програми
Інтернет-адреса постійного розміщення опису освітньої програми	
2 – Цілі освітньої програми	
Підготовка кваліфікованих фахівців здатних працювати в сфері забезпечення захисту об'єктів інформаційної інфраструктури, що передбачає: розробку, використання та впровадження технологій інформаційної та / або кібербезпеки, вирішення складних спеціалізованих задач та практичних проблем забезпечення кібербезпеки та захисту інформації. Освітньою програмою передбачається розвиток міжособистісних навичок відповідно до місії та стратегії університету, яка полягає у підготовці кваліфікованих кадрів для регіонального розвитку та міського господарства.	
3 - Характеристика освітньої програми	

Опис предметної області	Об'єкти вивчення: - технології кібербезпеки та захисту інформації; - процеси управління кібербезпекою та захистом інформації; - об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, 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 забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в 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 програма з кібербезпеки та захисту інформації.
Основний фокус освітньої програми	Фокус освітньої програми зосереджено на формуванні знань і професійних навичок, що необхідні у розв'язанні складних спеціалізованих задач та практичних проблем у сфері інформаційної та/або кібербезпеки. Акцентуючи на забезпечення захисту об'єктів критичної інфраструктури, зокрема критичної інфраструктури об'єктів водного господарства.
Особливості програми	Особливістю освітньої програми є формування компетенції фахівців, що передбачає: організацію політики інформаційної безпеки та її дотриманням, організацію політики управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення, організацію комплексних систем захисту інформації або систем інформаційної безпеки з підтвердженою відповідністю на всіх етапах їх життєвого циклу, імплементація заходів з кіберзахисту в бізнес/операційні процеси на всіх стадіях життєвого циклу об'єктів критичної інфраструктури.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може працювати в підрозділах великих підприємств та установ у сфері забезпечення кіберзахисту, зокрема на підприємствах критичної інфраструктури: сфери водопостачання, електроенергетики та інших об'єктах критичної інфраструктури. Фахівець може займати первинні посади (згідно з ДК 003:2010): Адміністратор безпеки мереж і систем, 2139.2; Фахівець сфери захисту інформації, 2139.2; Фахівець з питань безпеки (інформаційно-комунікаційні технології), 2139.2;

	Конструктор систем кібербезпеки, 2132.2; Фахівець з підтримки інфраструктури кіберзахисту, 2139.2; Фахівець з реагування на інциденти кібербезпеки, 2139.2; Фахівець з криптографічного захисту інформації, 2139.2; Фахівець з технічного захисту інформації, 2139.2; Фахівець з тестування систем захисту інформації, 2139.2; Аудитор інформаційних технологій (з кібербезпеки), 2139.2; Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2; Кібероператор, 4113.
Подальше навчання	Бакалавр може продовжувати навчання на другому (магістерському) рівні вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Студенто-центроване навчання, самонавчання, проблемно-орієнтоване навчання, кредитно-трансферна система організації навчання, навчання з використанням системи навчання Moodle, Google Meet, лекції, практичні та лабораторні заняття, консультації з науково-педагогічними працівниками, роботодавцями.
Оцінювання	Модульний контроль, заліки, екзамени, курсові роботи, тести, поточне опитування, комплексні практичні індивідуальні завдання, тренінги. Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації
Загальні компетентності (КЗ)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК 3. Здатність спілкуватися державною мовою як усно так і письмово. ЗК 4. Здатність спілкуватися іноземною мовою. ЗК 5. Здатність вчитися і оволодівати сучасними знаннями. ЗК 6. 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. ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК 8. 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. ЗК 9. Здатність володіти навичками публічних виступів, ведення переговорів, професійної та наукової дискусії, підготовки та демонстрації результатів дослідження. ЗК 10. Здатність мобілізувати ресурси та створювати цінність, планувати, організовувати та управляти власною діяльністю.
Фахові компетентності спеціальності	СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

	СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки та захисту інформації. СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів, тощо). СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. СК 11. Здатність управляти організаційно-методологічними, технічними та технологічними умовами кіберзахисту інформаційної інфраструктури об'єкту критичної інфраструктури, згідно нормативно-правових вимог.
--	--

7 – Програмні результати навчання

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН 3. Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН 4. 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. РН 5. 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. РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН 7. Застосовувати й адаптувати теорії інформації та кодування математичної статистики, чисел, криптографії та стенографії, оброблення і передачі сигналів, тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН 8. 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. РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

- РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
- РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
- РН 13. 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.
- РН 14. 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.
- РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
- РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
- РН 17. 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.
- РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
- РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
- РН 20. 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 технічного захисту інформації.
- РН 21. 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.
- РН 22. Набуття практичних навичок із планування, організації, фінансового забезпечення та управління власною діяльністю.
- РН 23. Знати та володіти інструментами для формування та валідації підприємницької ідеї
- РН 24. Організовувати методику управління ризиками кібербезпеки об'єктів критичної інфраструктури.

8 – Ресурсне забезпечення реалізації програми

Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають достатній досвід навчально-методичної, науково-дослідної і практичної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення підготовки здобувачів вищої освіти відповідає сучасним вимогам та включає кабінети і лабораторії з дисциплін гуманітарного, фундаментального і професійно орієнтованого напрямків. Навчальні аудиторії та лабораторії обладнані сучасними технічними засобами навчання, комп'ютерною технікою. У кожному з комп'ютерних класів встановлено необхідне програмне забезпечення, що дозволяє проводити навчальний процес

	відповідно до сучасних вимог. Університет має локальну комп'ютерну мережу, є доступ до всесвітньої мережі Інтернет. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць в гуртожитках відповідає вимогам. Приміщення відповідають нормам санітарії та охорони праці. Обладнання в робочому стані і відповідає нормам охорони праці.
Інформаційне та навчально-методичне забезпечення	Інформаційне та навчально методичне забезпечення знаходиться в науковій бібліотеці НУВГП. Навчально-методичне забезпечення розміщується в рипозиторії НУВГП та на платформі Moodle. Офіційний веб-сайт містить інформацію про навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньо-професійної програми викладені на ресурсах локальної мережі. Посилання на навчально-методичне забезпечення кожної компоненти ОП також розміщується на сайті кафедри. Інформаційне та навчально-методичне забезпечення дисциплін передбачає використання авторських розробок професорсько-викладацького складу.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним університетом водного господарства та природокористування та закладами вищої освіти України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між НУВГП та навчальними закладами країн-партнерів.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою.

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

2.1. Перелік компонент ОП

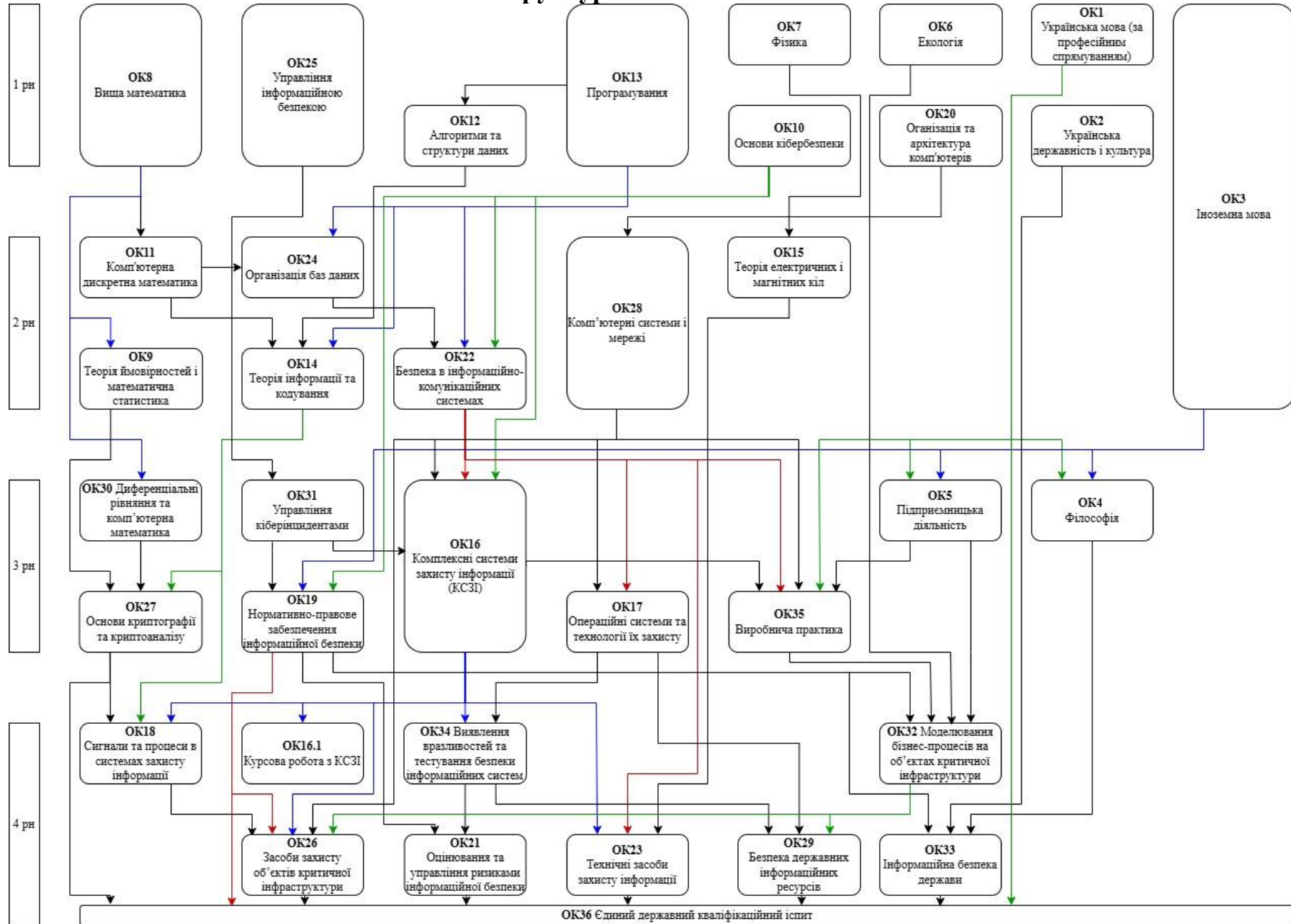
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контр.
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1	Українська мова (за професійним спрямуванням)	3.0	Е
ОК 2	Українська державність і культура	4.0	З
ОК 3	Іноземна мова	12.0	Е
ОК 4	Філософія	3.0	Е
ОК 5	Підприємницька діяльність	3.0	З
ОК 6	Екологія	3.0	З
ОК 7	Фізика	4.0	Е
ОК 8	Вища математика	10.0	Е
ОК 9	Теорія ймовірностей і математична статистика	4.0	З
ОК 10	Основи кібербезпеки	4.0	З
ОК 11	Комп'ютерна дискретна математика	3.0	Е
ОК 12	Алгоритми та структури даних	4.0	З

ОК 13	Програмування	10.0	Е
ОК 14	Теорія інформації та кодування	6.0	З
ОК 15	Теорія електричних і магнітних кіл	3.5	Е
ОК 16	Комплексні системи захисту інформації (КСЗІ)	7.0	Е
ОК 16.1	Курсова робота з КСЗІ	3.0	З
ОК 17	Операційні системи та технології їх захисту	4.0	З
ОК 18	Сигнали та процеси в системах захисту інформації	4.5	З
ОК 19	Нормативно-правове забезпечення інформаційної безпеки	3.0	З
ОК 20	Організація та архітектура комп'ютерів	4.0	З
ОК 21	Оцінювання та управління ризиками інформаційної безпеки	4.5	Е
ОК 22	Безпека в інформаційно-комунікаційних системах	5.0	Е
ОК 23	Технічні засоби захисту інформації	6.0	Е
ОК 24	Організація баз даних	4.5	Е
ОК 25	Управління інформаційною безпекою	8.0	Е
ОК 26	Засоби захисту об'єктів критичної інфраструктури	6.0	З
ОК 27	Основи криптографії та криптоаналізу	6.5	Е
ОК 28	Комп'ютерні системи і мережі	10.0	Е
ОК 29	Безпека державних інформаційних ресурсів	3.5	З
ОК 30	Диференціальні рівняння та комп'ютерна математика	3.5	З
ОК 31	Управління кіберінцидентами	3.0	Е
ОК 32	Моделювання бізнес-процесів на об'єктах критичної інфраструктури	4.0	Е
ОК 33	Інформаційна безпека держави	5.0	Е
ОК 34	Виявлення вразливостей та тестування безпеки інформаційних систем	4.0	Е
ОК 35	Виробнича практика	3	З
ОК 36	Єдиний державний кваліфікаційний іспит	1.5	Е
	Разом обов'язкових компонентів ОП	180	
МД	Мейджор	36	З
БЗВП	Базова загальновійськова підготовка (теоретична частина)	3	З
ВК 1	Спецкурс за вибором		
ВК 2	Спецкурс за вибором	3	З
МН	Майнор	18	З
	Всього освітніх компонент вільного вибору	60	
	Загальний обсяг освітніх компонент:	240	

Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
--	--

2.2. Структурно-логічна схема ОП



4. Матриця відповідності програмних компетентностей компонентам освітньої програми

[illegible]

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

OK	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
PH1	+	+																																	+	+	
PH2			+																																		
PH3		+		+	+	+													+						+								+				
PH4	+		+							+			+			+	+	+	+		+	+	+	+	+	+	+	+	+		+	+		+	+	+	
PH5	+		+							+			+			+	+	+	+		+	+	+	+	+	+	+	+	+		+	+		+	+	+	
PH6	+	+		+		+				+						+	+	+	+		+	+	+		+	+	+	+	+		+	+	+		+	+	
PH7	+	+	+	+		+				+			+			+	+	+	+		+	+	+	+	+			+			+		+	+	+		
PH8				+			+	+	+		+	+	+	+	+					+			+							+				+	+		
PH9		+		+		+				+						+			+		+				+				+				+		+		
PH10										+			+	+			+				+	+	+		+									+	+		
PH11					+											+					+	+		+	+	+					+				+		
PH12													+			+						+			+		+	+	+								
PH13													+			+						+			+		+	+	+								
PH14																	+			+				+	+			+			+				+		
PH15																	+			+				+	+			+			+				+		
PH16																+									+												
PH17																									+										+		
PH18										+			+	+				+										+							+		
PH19										+			+	+				+										+								+	
PH20															+			+				+	+			+		+									
PH21										+											+				+							+		+	+		
PH22					+															+	+	+			+									+	+		
PH23					+																															+	
PH24																+			+							+							+				