МІНІСТЕРСТВО НАУКИ І ОСВІТИ УКРАЇНИ
Національний університет водного господарства та природокористування

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
"Інформаційна безпека"
першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 "Кібербезпека та захист інформації"
галузь знань 12 "Інформаційні технології"
Кваліфікація "Бакалавр з кібербезпеки та захисту інформації"

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ НУВГП
Голова вченої ради
_____Мошинський В.С.
протокол № 7 від 05.07.2024 р.

Освітня програма вводиться в дію з 01.09.2024 р.
Ректор _____Мошинський В.С.
наказ № 517 від 09.07.2024

Рівне-2024

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

"Інформаційна безпека"

першого освітнього рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

РОЗГЛЯНУТО

На засіданні кафедри обчислювальної техніки

Протокол №15 від 26.06.2024 року

СХВАЛЕНО

Науково-методичною комісією за спеціальністю 125 "Кібербезпека та захист інформації". Протокол №8 від 27.062024 року

СХВАЛЕНО

Вченою радою ННІ кібернетики, інформаційних технологій та інженерії

Протокол №7 від 28.06.2024 року

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(керівник проектної групи)	– 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, доцент кафедри обчислювальної техніки Національного університету водного господарства та природокористування
3. Шатний Сергій В’ячеславович	– канд. техн. наук, доцент кафедри обчислювальної техніки Національного університету водного господарства та природокористування
4. Соломко Михайло Тимофійович	– канд. техн. наук, доцент кафедри обчислювальної техніки Національного університету водного господарства та природокористування
5. Тадеєв Петро Олександрович	– док. пед. наук, завідувач кафедри вищої метематики Національного університету водного господарства та природокористування

Рецензії стейкхолдерів

1. ІТ ТОВ «РЕНОМЕ-СМАРТ»
2. Рівненське районне управління поліції

1. Профіль освітньо-професійної програми зі спеціальності 125 "Кібербезпека та захист інформації"

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Національний університет водного господарства та природокористування, Навчально-науковий інститут Автоматики кібернетики та обчислювальної техніки, кафедра обчислювальної техніки.
Ступінь вищої освіти та назва кваліфікації мовою	Бакалавр, бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Освітньо-професійна програма “Інформаційна безпека” ID 58698
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 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	5 років
Інтернет-адреса постійного розміщення опису освітньої програми	**https://nuwm.edu.ua/nni-akot/kaf-ot/osvitni-proghrami**
2 – Мета освітньої програми	
Підготовка висококваліфікованих, конкурентоспроможних фахівців здатних розробляти і використовувати технології інформаційної безпеки та/або кібербезпеки; які мають теоретичні знання в точу числі стосовно математичного і комп’ютерного моделювання інформаційної безпеки систем та сформоване критичне мислення; володіють сучасними криптографічними методами захисту інформації; методами захисту мережевої інфраструктури та Web ресурсів; вміють безконфліктно та продуктивно працювати в командах щодо розв’язання проблем та прийняття рішень з питань захисту інформації, безперебійного функціонування, оперативного реагування та відновлення роботи після несанкціонованого втручання в інформаційні системи.	
3 - Характеристика освітньої програми	
Опис предметної області	12 Інформаційні технології 125 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітньо-професійна програма з кібербезпеки та захисту інформації.
Основний фокус освітньої програми	ОП фокусується на формуванні та розвитку у здобувачів професійних компетентностей, поєднання яких створює умови для вирішення складних задач щодо захисту програмного забезпечення, мережевої інфраструктури та вирішення проблем інформаційної безпеки, в тому числі методами математичного і комп’ютерного моделювання. Ключові слова: кібернетична безпека, криптографія, безпека інформаційно-комунікаційних систем, управління інформаційною

	безпекою, інформаційна безпека держави, поширення інформації, інформаційна боротьба.
Особливості програми	ОП передбачає використання математичних та комп'ютерних моделей і методів в інформаційній безпеці
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 2132.2- Розробник систем захисту інформації; 2139.2- Адміністратор мереж і систем; Аналітик з безпеки інформаційно-телекомунікаційних систем; Аналітик загроз безпеки; Аналітик систем захисту інформації та оцінки вразливостей; Аудитор інформаційних технологій Фахівець з криптографічного захисту інформації; Фахівець з питань безпеки (інформаційно-комунікаційні технології); Фахівець з тестування систем захисту інформації; Фахівець з технічного захисту інформації.
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 та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 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 і свобод людини і громадянина в Україні. КЗ 7. 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. КЗ 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів не доброчесності.
Фахові компетентності	КФ 1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні та міжнародні вимоги, практики і стандарти з

спеціальності (КФ)	метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно- апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. КФ 13. Здатність використовувати комп’ютерні технології для вирішення спеціалізованих задач інформаційної безпеки засобами математичного та комп’ютерного моделювання.

7 – Програмні результати навчання

ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН7. Діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
ПРН10. Виконувати аналіз та декомпозицію інформаційно телекомунікаційних систем.
ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
ПРН12. Розробляти моделі загроз та порушника.
ПРН13. Аналізувати проекти інформаційно телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно телекомунікаційних системах програмно апаратними засобами та давати оцінку результативності якості прийнятих рішень.
ПРН15. Використовувати сучасне програмно апаратне забезпечення інформаційно комунікаційних технологій.
ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно правових документів.
ПРН17. Забезпечувати процеси захисту та функціонування інформаційно телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН18. Використовувати програмні та програмно апаратні комплекси захисту інформаційних ресурсів.
ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах;
ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно телекомунікаційних системах.
ПРН21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.
ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.
ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно

телекомунікаційних (автоматизованих) системах.
ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно телекомунікаційних систем.
ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно телекомунікаційних систем.
ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН36. Виявляти небезпечні сигнали технічних засобів.
ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
ПРН44. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
ПРН45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик орієнтованому контролі доступу до інформаційних активів.
ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно телекомунікаційних системах.
ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та

використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно телекомунікаційних системах.
ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно телекомунікаційних системах.
ПРН50. Забезпечувати функціонування програмних та програмно апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично сигнатурних).
ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах.
ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно телекомунікаційних системах.
ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ПРН55 Володіти елементами математичного та комп'ютерного моделювання, в тому числі стосовно практичних задач інформаційної безпеки. Знати основи та принципи числових методів дискретизації відповідних математичних моделей. Здійснювати програмну реалізацію дискретних схем, ефективно використовувати можливості комп'ютерної техніки та сучасного програмного забезпечення для розв'язування прикладних задач в інформаційній безпеці.

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 тавключає 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 (https://lib.nuwm.edu.ua/) Навчально-методичне забезпечення розміщується в рипозиторії НУВГП (https://ep3.nuwm.edu.ua/) та на платформі Moodle (https://exam.nuwm.edu.ua/) Офіційний веб-сайт (https://nuwm.edu.ua/) 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 розробо професорсько-викладацького складу.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним університетом водного господарстів 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	6.0	Е
ОК 8	Вища математика	10.0	Е
ОК 9	Основи кібербезпеки	4.0	Е
ОК 10	Теорія інформації та кодування	6.0	Е
ОК 11	Дискретна математика	4.0	Е
ОК 12	Алгоритми та методи обчислень	4.5	З
ОК 13	Програмування	5.5	Е
ОК 14	Практична підготовка з програмування	6.0	З
ОК 15	Теорія електричних і магнітних кіл	4.0	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	4.5	З
ОК18	Практична підготовка з комп'ютерної схемотехніки	6.0	З
ОК 19	Нормативно-правове забезпечення інформаційної безпеки	4.0	З
ОК 20	Архітектура комп'ютерів	3.5	Е

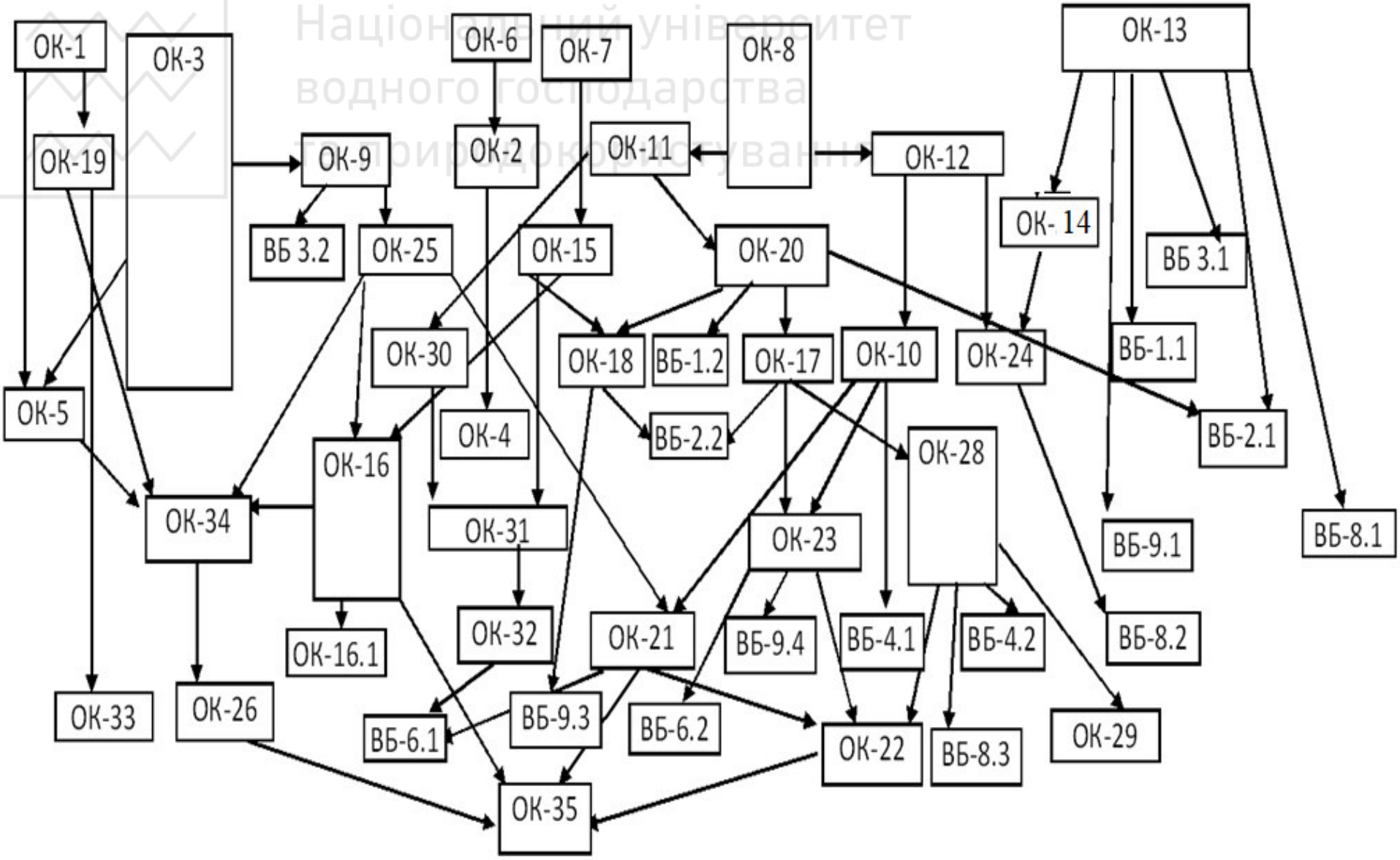
ОК 21	Оцінювання та управління ризиками інформаційної безпеки	4.5	Е
ОК 22	Безпека в інформаційно-комунікаційних системах	6.0	Е
ОК 23	Технічні засоби захисту інформації	6.0	Е
ОК 24	Організація баз даних	4.0	Е
ОК 25	Управління інформаційною безпекою	7.0	Е
ОК 26	Практична підготовка з управління інформаційною безпекою	6.0	З
ОК 27	Основи криптографії та криптоаналізу	7.5	Е
ОК 28	Комп’ютерні системи і мережі	9.0	Е
ОК 29	Безпека бездротових технологій передачі даних	3.5	Е
ОК 30	Диференціальні рівняння та комп’ютерна математика	4.0	З
ОК 31	Алгоритми та обчислювальні методи математичної фізики	3.0	З
ОК 32	Математичне та комп'ютерне моделювання в інформаційній безпеці	4.0	Е
ОК 33	Інформаційна безпека держави	5.0	Е
ОК 34	Виробнича практика	3	З
ОК 35	Єдиний державний кваліфікаційний іспит	1.5	Е
	Разом обов'язкових компонентів ОП	**180**	
	Вибіркові компоненти ОП		
ВБ 1.1.	Об'єктно-орієнтоване програмування	4.0	З
ВБ 1.2.	Технічне обслуговування комп'ютерних систем		
ВБ 2.1.	Системне програмування	3.5	З
ВБ 2.2.	Інформаційні системи реального часу		
ВБ 3.1.	Інженерія програмного забезпечення	5.0	З
ВБ 3.2.	Безпека банківських систем		
ВБ 4.1.	Захист програмного забезпечення	4.0	З
ВБ 4.2.	Системна інтеграція інтелектуальних ІТ		
ВБ 5.1.	Хмарні інформаційні технології	3.0	З
ВБ 5.2.	Основи Web-безпеки		
ВБ 6.1.	Економіка захисту інформаційних систем	5.5	З
ВБ 6.2.	Smart забезпечення бізнес процесів		
	Разом	**25**	
Вибірковий блок 1			
ВБ 7	Спецкурс за вибором	18	З
ВБ 8.1.	Крос-платформене програмування	5	З
ВБ 8.2.	Програмування мобільних пристроїв	4	З
ВБ 8.3.	Кіберфізичні та гібридні комп'ютерні системи	4	З
ВБ 8.4.	Web-програмування	4	З
	Разом за блоком 1 вільного вибору	**35**	
Вибірковий блок 2			
ВБ 7	Спецкурс за вибором	18	З
ВБ 9.1.	Штучні нейроні мережі	5	З

ВБ 9.2.	Системи відеонагляду	4	З
ВБ 9.3.	Signal Processing	4	З
ВБ 9.4.	Системи контролю і управління доступом	4	З
	Разом за блоком 1 вільного вибору	**35**	
	Вибірковий блок 3		
ВБ 7	Спецкурси за вибором	6	З
ВБ 10	Військова підготовка	29	Е
	Разом за блоком 3 вільного вибору	**35**	
	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.
Вимоги до кваліфікаційної роботи/проекту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

2.2. Структурно - логічна схема ОП



4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10	ФК11	ФК12	ФК13
ОК1	+		+				+														
ОК2						+	+														
ОК3			+																		
ОК4				+	+	+															
ОК5					+							+									
ОК6							+														
ОК7	+																				
ОК8	+				+																
ОК9		+			+			+	+	+		+				+					
ОК10		+								+	+			+							
ОК11				+	+																
ОК12	+				+																
ОК13		+									+		+								
ОК14		+									+		+								
ОК15																		+			
ОК16	+	+		+					+		+		+		+						
ОК17	+	+		+						+	+										
ОК18																			+		
ОК19		+						+	+												
ОК20									+			+				+					
ОК21	+			+				+	+					+						+	
ОК22	+									+		+	+	+		+			+	+	
ОК23											+			+				+			
ОК24											+								+		
ОК25	+	+		+					+	+		+	+	+	+	+	+		+		
ОК26	+	+		+					+	+		+	+	+	+	+	+		+		
ОК27		+											+					+			
ОК28		+								+			+	+							
ОК29										+			+								
ОК30																					+
ОК31																					+
ОК32																					+
ОК33					+			+										+		+	
ОК34	+	+		+					+			+		+		+	+				+
ОК35		+	+							+								+	+	+	

Матриця відповідності програмних компетентностей компонентам освітньої програми (Вибіркові компоненти)

	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10	ФК11	ФК12	ФК13
ВБ 1.1.											+										
ВБ 1.2.																		+	+		
ВБ 2.1.																			+		
ВБ 2.2.																			+		
ВБ 3.1.	+																				
ВБ 3.2.																+	+			+	
ВБ 4.1.													+				+			+	
ВБ 4.2.																			+		
ВБ 5.1.					+																
ВБ 5.2.					+																
ВБ 6.1.									+	+											
ВБ 6.2.										+		+									
ВБ 8.1.	+			+																	
ВБ 8.2.											+										
ВБ 8.3.	+																				
ВБ 8.4.	+												+								
ВБ 9.1.	+																				
ВБ 9.2.		+			+																
ВБ 9.3.																		+			
ВБ 9.4.													+					+	+		

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

ОК	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
РН1	+		+																																+
РН2					+		+	+			+										+				+	+								+	+
РН3								+	+				+	+																					+
РН4												+				+					+				+	+									+
РН5									+								+																	+	
РН6							+	+			+																+								
РН7				+					+				+	+		+			+	+					+	+								+	
РН8									+							+			+	+					+	+									
РН9																+				+					+	+							+		
РН10										+		+				+	+											+							
РН11																	+					+		+				+						+	
РН12																+									+	+									+
РН13										+							+			+		+						+	+						
РН14													+	+								+	+				+							+	
РН15													+	+			+						+						+						+
РН16																+																		+	+
РН17										+							+					+			+	+		+						+	
РН18										+			+	+		+						+												+	
РН19									+													+													
РН20																+						+			+	+	+								
РН21																									+	+								+	
РН22																+	+					+			+	+								+	
РН23																						+	+		+	+									
РН24																						+			+	+	+								
РН25																						+			+	+									
РН26																+						+			+	+		+							
РН27																						+			+	+									
РН28								+													+	+			+	+								+	
РН29									+							+					+	+			+	+									
РН30																						+													

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

ОК	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
РН31									+													+											+		
РН32																									+	+		+							
РН33																					+				+	+									
РН34																+						+	+		+	+								+	+
РН35																+									+	+		+							+
РН36															+								+											+	
РН37																							+												
РН38																							+												
РН39																							+												
РН40															+								+												+
РН41																						+			+	+		+						+	
РН42																+									+	+									+
РН43									+																+	+							+		
РН44					+																+				+	+							+		
РН45																					+	+			+	+		+							
РН46																					+				+	+									
РН47																								+			+							+	
РН48																						+	+				+	+							
РН49																+		+				+													
РН50										+			+	+						+							+							+	+
РН51																+							+											+	+
РН52																+		+							+	+		+							
РН53										+			+	+			+			+														+	+
РН54	+	+		+		+																											+		+
РН55																														+	+	+		+	

ВБ	1.1	1.2	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2	6.1	6.2	8.1	8.2	8.3	8.4	9.1	9.2	9.3	9.4
РН1																				
РН2																				
РН3													+							
РН4																	+			
РН5				+									+							
РН6																				
РН7											+									
РН8											+									
РН9																				
РН10					+								+		+		+			
РН11				+											+					
РН12																				
РН13				+																
РН14									+											
РН15	+											+		+						
РН16																				
РН17																				
РН18																				
РН19			+																	
РН20																				
РН21																				
РН22										+						+				
РН23										+						+				
РН24										+						+				+
РН25				+						+										
РН26			+																	+
РН27									+						+					
РН28							+				+									
РН29							+													
РН30																				

ВБ	1.1	1.2	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2	6.1	6.2	8.1	8.2	8.3	8.4	9.1	9.2	9.3	9.4
РН31																				
РН32																		+		
РН33						+						+								
РН34								+	+											
РН35					+		+											+		
РН36		+																	+	
РН37		+																	+	
РН38																				
РН39																				+
РН40																			+	
РН41								+										+		
РН42																				
РН43																				
РН44						+						+								
РН45																				
РН46							+													
РН47																				
РН48																				
РН49		+																		
РН50														+						
РН51																				
РН52								+												
РН53	+		+											+						
РН54																				
РН55	+																+			