ID 59794

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»
назва освітньої програми
Security of information and communication systems
назва освітньої програми англійською мовою

другого магістерського рівня вищої освіти
за спеціальністю 125 «Кібербезпека та захист інформації»
галузі знань 12 «Інформаційні технології»
Кваліфікація: Магістр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО

Вченою радою
Київського національного університету
будівництва і архітектури
зі змінами
Протокол № 20 від 29.03.2024

Освітня програма вводиться в дію з 01 вересня 2024 р.

Голова Вченої ради
_____ Петро КУЛІКОВ
«29» 03 2024 р.

Київ – 2024 р.

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми підготовки здобувачів вищої освіти
«Безпека інформаційних і комунікаційних систем»
на другому (магістерському) освітньому рівні
за спеціальністю 125 «Кібербезпека та захист інформації»

1. Погоджено на засіданні НМК зі спеціальності
(Протокол № 2 від 27.03. 2024 р.)

Гарант освітньої програми _____ Юрій ХЛАПОНІН

«___» _____ 2024 р.

2. Перевірено навчально-методичним відділом

Начальник навчально-методичного відділу _____ Ігор СКЛЯРОВ

«28» 03 2024 р.

3. Погоджено на засіданні Методичної ради Університету
(Протокол № 7 від 28.03.2024р.)

Проректор з навчально-методичної
роботи КНУБА _____ Андрій ШПАКОВ

«___» _____ 2023 р.

ПЕРЕДМОВА

РОЗРОБЛЕНО проектною групою у складі:

11. Хлапонін Юрій Іванович, д.т.н., професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури, гарант освітньої програми.

2. Сєлюков Олександр Васильович, д.т.н., професор, професор кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

3. Ізмайлова Ольга Василівна, к.т.н., доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

4. Кондакова Світлана Віталіївна, к.ф.-м.н., доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

5. Шабала Євгенія Євгенівна, к.т.н., доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

Гарант – Хлапонін Юрій Іванович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

Стейкголдери:

Академічна спільнота – Гайдур Галина Іванівна, д.т.н., професор, завідувач кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій МОН України.

Смірнов Олексій Анатолійович – д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету м. Кропивницький,

Роботодавці та/або представники професійної спільноти –
к.т.н. Ковальов Ігор Генадійович, генеральний директор ТОВ "СВІТ-ІТ»

Татьянін Вячеслав Вікторович, директор ТОВ «Автор»

Здобувачі – Кемпф Анна Борисівна – магістр вищої освіти випуску 2021 року
Власенко Мирослава Миколаївна - магістр вищої освіти випуску 2021 року

1. Профіль освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» за спеціальністю 125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Другий (магістерський) рівень Магістр, магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний. Обсяг освітньої програми на базі освітнього рівня «бакалавр» становить 90 кредитів ЄКТС;
Наявність акредитації	Міністерство Освіти і науки України, сертифікат про акредитацію спеціальності: Серія УД №11003275 від 27 грудня 2018 р.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, QF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра або освітньо-кваліфікаційного рівня спеціаліста
Мова(и) викладання	Українська мова
Термін дії освітньо-професійної програми	До наступної акредитації
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	https://www.knuba.edu.ua/
2 – Мета освітньої програми	
Надати освіту в галузі знань 12 «Інформаційні технології» та забезпечити студентам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 «Кібербезпека та захист інформації» достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій, педагогіки та методики вищої освіти.	
3 – Характеристика освітньої програми	

Предметна область (галузь знань, спеціальність)	Галузь знань: 12 «Інформаційні технології», спеціальність 125. «Кібербезпека та захист інформації»
Опис предметної області	**Об'єкти вивчення:** об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. **Цілі навчання:** підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області:** ***Знання:*** – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до ІР; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: методи, методики та технології забезпечення інформаційної та/або кібербезпеки. **Інструменти та обладнання:** системи розробки, забезпечення, моніторингу та контролю інформаційної та/або кібербезпеки; сучасне програмно-апаратне забезпечення інфокомунікаційних технологій.
Орієнтація освітньо-професійної програми	Програма освітня;

	Програма з прикладною спрямованістю за спеціалізацією безпека інформаційних і комунікаційних систем.
Основний фокус освітньо- професійної програми	Загальна програма. Дослідження в області практики та науки захисту інформації, організації та забезпечення інформаційної та/або кібербезпеки об'єктів, що підлягають захисту.
Особливості освітньо-професійної програми	З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації магістр з кібербепеки, програма забезпечує підготовку професіоналів, здатних: – виявляти та оцінювати ознаки стороннього кібернетичного впливу; – моделювати можливі ситуації стороннього кібернетичного впливу та прогнозувати їх можливі наслідки; – організовувати і підтримувати комплекс заходів щодо забезпечення інформаційної та/або кібербезпеки; – проводити дослідження у напрямах забезпечення інформаційної та/або кібербезпеки національних інтересів України й обґрунтовувати шляхи підвищення їх ефективності; – протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів; – забезпечити криптозахист власного інформаційного ресурсу тощо. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає: - реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; - залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі інформаційних технологій та телекомунікацій, а також представників бізнесу

	Кафедра здійснює реалізацію Міжнародного Erasmus+KA2 проекту «GameHub: Співпраця університетів-підприємств в ігровій індустрії в Україні»
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати в державному та приватному секторах Києва, України та Європейського Союзу у таких сферах діяльності: 1) адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.; 2)застосування засобів антивірусного захисту (ESET, McAfee, Zilly , etc.), програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, etc.); 3) створення технічної, проектної та експлуатаційної документації інформаційно-комунікаційних систем (далі – ІКС) та систем захисту інформації (далі – СЗІ); 4) налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; 5) проведення моніторингу несанкціонованої активності в обчислювальних системах; 6) створення, впровадження та експлуатації комплексних систем захисту інформації (далі – КСЗІ), а також СЗІ в складі інформаційно телекомунікаційних (далі – ІТС) та обчислювальних систем; 7) формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; 8) проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки; 9) підтримка наукових досліджень, педагогічна діяльність тощо. Згідно з Національним класифікатором професій ДК 003:2010 фахівці, які здобули освіту за освітньою програмою «Безпека інформаційних і комунікаційних систем» можуть обіймати такі первинні посади, як: - програміст/тестувальник програмного забезпечення систем інформаційної та кібербезпеки; - адміністратор комп'ютерних систем і мереж; - адміністратор інформаційної та кібербезпеки; - аудитор/пентестер безпеки інформаційно-комунікаційних систем; - розробник засобів захисту інформації;

	- провідний спеціаліст/керівник служби технічного захисту інформації тощо.
Подальше навчання	Можливість продовження навчання за програмою третього рівня вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу; реалізують-ся через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямовано-сті у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи з використанням елементів дистанційного навчання, розв'язування прикладних задач, виконання прое-ктів, навчальних та виробничих практик, курсових робіт, кваліфікаційної магістерської роботи.
Оцінювання	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЕКТС (ECTS), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системами. Види контролю: поточний, тематичний, періодич-ний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестові завдання в тому числі комп'ютерне тестування, лабораторні звіти, презентації, захист курсових робіт та проектів, звітів з практик, захист кваліфікаційної роботи магістра.
6 – Програмні компетентності	
Інтегральна компетентність (ІК)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	**КЗ-1.** Здатність застосовувати знання у практичних ситуаціях. **КЗ-2.** Здатність проводити дослідження на відповідному рівні. **КЗ-3.** Здатність до абстрактного мислення, аналізу та синтезу. **КЗ-4.** Здатність оцінювати та забезпечувати якість виконуваних робіт. **КЗ-5.** Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

Фахові компетентності (КФ)	**КФ1.** Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. **КФ2.** Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. **КФ3.** Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. **КФ4.** Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. **КФ5.** Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ6.** Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ7.** Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати

	рекомендації щодо попередження та аналізу кіберінцидентів в цілому. **КФ8.** Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ9.** Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. **КФ10.** Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
7 – Програмні результати навчання	
Програмні результати навчання (РН)	**РН1.** Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **РН2.** Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. **РН3.** Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. **РН4.** Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

	РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. **РН6.** Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. **РН7.** Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **РН8.** Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. **РН9.** Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. **РН10**. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. **РН11**. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **РН12**. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. **РН13**. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного

	та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. **РН14**. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. **РН15**. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. **РН16**. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. **РН17**. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. **РН18**. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. **РН19**. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. **РН20**. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. **РН21**. Використовувати методи натурного, фізичного і комп'ютерного моделювання для

	дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. **РН22**. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. **РН23**. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітню програму відповідають профілю та напряму дисциплін, що викладаються. 90% науково-педагогічних працівників задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності мають наукові ступені та вчені звання, з досвідом практичної роботи за фахом.
Матеріально-технічне забезпечення	Навчальні приміщення дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою, оскільки мають достатню кількість комп'ютеризованих та спеціалізованих робочих місць та обладнанні необхідними комп'ютерними засобами та програмним забезпеченням.
Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт https://www.knuba.edu.ua/ містить інформацію про освітні програми, навчальну та наукову діяльність, структурні підрозділи, правила прийому, контакти. Ресурси науково-технічної бібліотеки доступні через сайт: http://library.knuba.edu.ua/ Для забезпечення навчального процесу використовується навчальне середовище на базі системи дистанційного навчання Moodle, де розміщені матеріали навчально-методичного забезпечення ОП.

	Використання дистанційного, навчального середовища університету та авторських розробок науково-педагогічних працівників; підручників та навчальних посібників з грифом Вченої ради КНУБА.
9 – Академічна мобільність	
Національна кредитна мобільність	Положенням університету передбачена можливість національної кредитної мобільності.
Міжнародна кредитна мобільність	Положенням університету передбачена можливість міжнародної кредитної мобільності
Навчання іноземних здобувачів ВО	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою

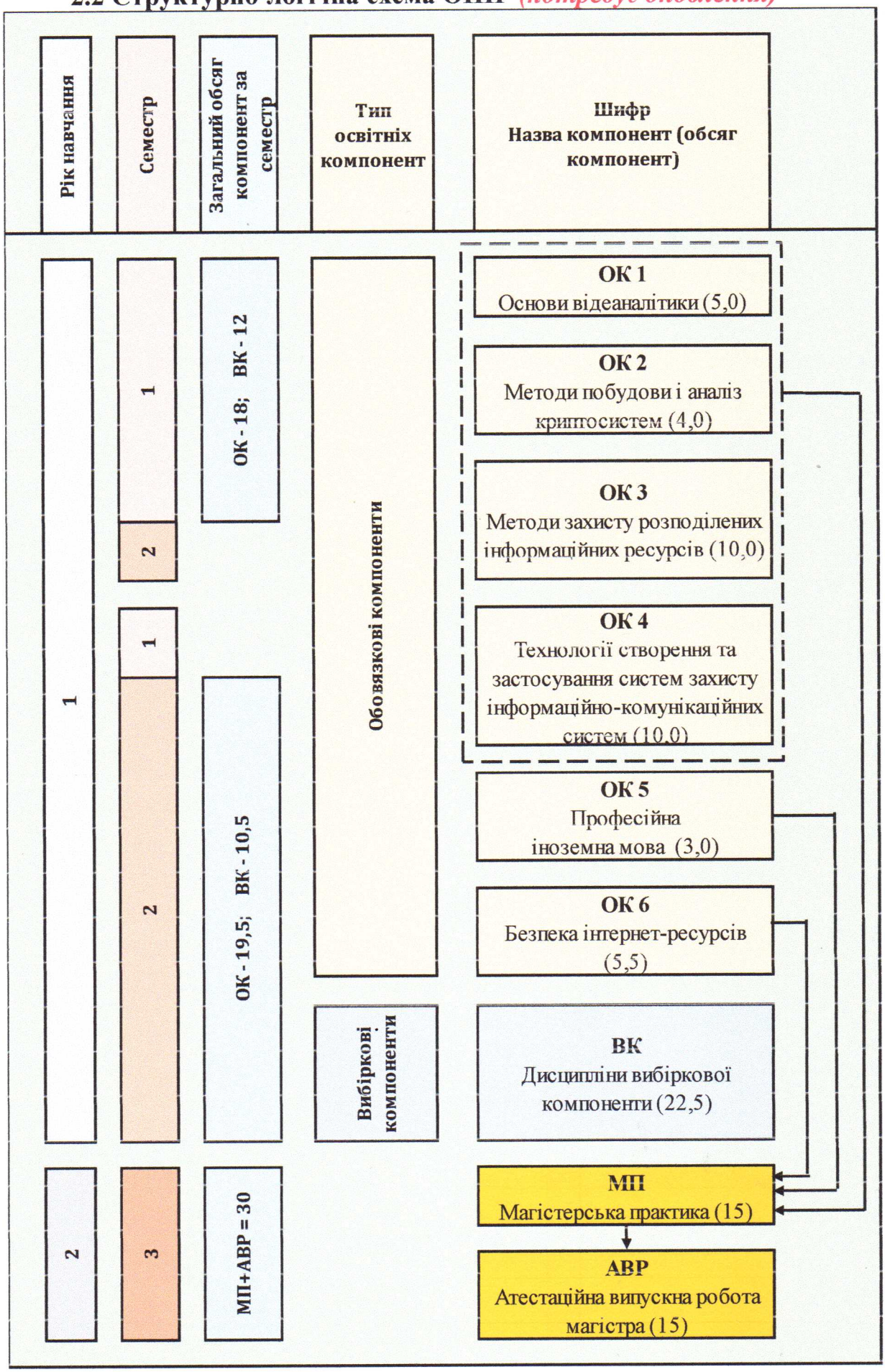
2. Перелік компонент освітньо-професійної програми та її логічна послідовність

2.1. Перелік компонент ОПП

Код н/д	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП			
ОК 1	Основи відеоаналітики	5,0	Іспит
ОК 2	Методи побудови і аналіз криптосистем	4,0	Іспит
ОК 3	Програмування динамічних систем	10,0	Залік, Іспит
ОК 4	Розробка стартапів і Agile-проектів	5,0	Залік
ОК 5	Аудит кібербезпеки в IoT-компонентах будівельних екосистем	5,0	Залік
ОК 6	Професійна іноземна мова	3,0	Залік
ОК 7	Безпека інтернет-ресурсів	5,5	Іспит
ПП	Переддипломна практика	15,0	Залік
АВР	Атестаційна випускна робота магістра	15,0	
Загальний обсяг обов`язкових компонент		**67,5**	
Вибіркові компоненти ОПП *(здобувач обирає дисципліни сумарним обсягом 22,5 кредитів)*			
ВК	Дисципліни вибіркової компоненти	22,5	Залік
Загальний обсяг вибіркових компонент:		**22,5**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		**90**	

Здобувач вищої освіти з другого освітньо-професійного рівня самостійно обирає дисципліни вибіркової компоненти, представлені:
на офіційному сайті КНУБА: https://www.knuba.edu.ua

2.2 Структурно-логічна схема ОПП *(потребує оновлення)*



3. Форма атестації здобувачів вищої освіти освітньо-професійної програми

Завершальним етапом навчання студентів зі спеціальності 125 «Кібербезпека та захист інформації» є підсумкова атестація.

Підсумкова атестація здобувачів вищої освіти – це встановлення відповідності рівня та обсягу знань, умінь та компетентностей здобувача вищої освіти, яка навчається за освітньою програмою, вимогам стандартів вищої освіти.

Атестація здійснюється у формі публічного захисту кваліфікаційної роботи і завершується видачею документів встановленого зразка про присудження йому рівня магістр з присвоєнням кваліфікації: Магістр з кібербезпеки та захисту інформації.

Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	МП	АВР
ІК	+	+	+	+	+	+	+	+
КЗ-1	+		+	+		+	+	+
КЗ-2		+	+	+		+	+	+
КЗ-3							+	+
КЗ-4	+		+	+		+	+	+
КЗ-5		+			+	+	+	+
КФ 1	+	+	+	+		+	+	+
КФ 2		+	+	+			+	+
КФ 3	+	+	+	+		+	+	+
КФ 4			+	+		+	+	+
КФ 5		+	+	+		+	+	+
КФ 6	+	+	+	+		+	+	+
КФ 7			+	+		+	+	+
КФ 8	+	+				+	+	+
КФ 9			+	+		+	+	+
КФ 10			+	+		+	+	+

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідним компонентам освітньо-професійної програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	МП	АВР
РН1					+		+	+
РН2	+	+	+	+		+	+	+
РН3		+				+	+	+
РН4		+	+	+		+	+	+
РН5	+	+	+	+		+	+	+
РН6	+		+	+		+	+	+
РН7		+	+	+		+	+	+
РН8	+	+				+	+	+
РН9			+	+		+	+	+
РН10			+	+		+	+	+
РН11			+	+		+	+	+
РН12			+	+		+	+	+
РН13		+				+	+	+
РН14			+	+		+	+	+
РН15		+				+	+	+
РН16			+	+		+	+	+
РН17		+				+	+	+
РН18			+	+		+	+	+
РН19		+					+	+
РН20		+				+	+	+
РН21		+	+	+		+	+	+
РН22		+				+	+	+
РН23	+					+	+	+

6. Перелік нормативних документів, на яких базується освітньо-наукова програма

1. Стандарт вищої освіти магістерського рівня «125 – Кібербезпека». Затверджено наказом Міністерства освіти і науки України №332 від 18.03.2021 // https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx

2. Стандарти та рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG) // URL: https://ihed.org.ua/wpcontent/uploads/2018/10/04_2016_ESG_2015.pdf.

3. EQF 2017 (Європейська рамка кваліфікацій) // URL: https://ec.europa.eu/ploteus/sites/eac-eqf/files/en.pdf;

4. https://ec.europa.eu/ploteus/content/descriptors-page.

5. QF EHEA 2018 (Рамка кваліфікацій ЄПВО) // URL: http://www.ehea.info/Upload/document/ministerial_declarations/EHEAParis2018_C ommunique_AppendixIII_952778.pdf

6. ISCED (Міжнародна стандартна класифікація освіти, МСКО) 2011 // URL: http://uis.unesco.org/sites/default/files/documents/international-standardclassification-of-education-isced-2011-en.pdf.

7. ISCED-F (Міжнародна стандартна класифікація освіти – Галузі, МСКО-Г) 2013 // URL: http://uis.unesco.org/sites/default/files/documents/internationalstandard-classification-of-education-fields-of-education-and-training-2013-detailedfield-descriptions-2015-en.pdf.

8. TUNING (для ознайомлення зі спеціальними (фаховими) та загальними компетентностями та прикладами стандартів – http://www.unideusto/ org/tuningeu/.

9. Національний освітній глосарій: вища освіта / 2-е вид., перероб. і доп. / авт.-уклад. : В. М. Захарченко, С. А. Калашнікова, В. І. Луговий, А. В. Ставицький, Ю. М. Рашкевич, Ж. В. Таланова / За ред. В. Г. Кременя.– К. : ТОВ "Видавничий дім . "Плеяди", 2014.– 100 с. – http://erasmusplus.org.ua/korysnainformatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandyekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskohoprotsesu.html?download=83:hlosarii-terminiv-vyshchoi-osvity-2014-r-onovlenevydannia-z-urakhuvanniam-polozhen-novoho-zakonu-ukrainy-pro-vyshchuosvitu&start=80.

10. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3 materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentivbolonskoho-protsesu.html?download=82:bolonskyi-protses-nova-paradyhmavyshchoi-osvity-yu-rashkevych&start=80.

11. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertiv-shchodozaprovadzhennia-instrumentiv-bolonskoho-protsesu.html?download=88: rozvytoksystemy-zabezpechennia-iakosti-vyshchoi-osvity-ukrainy&start=80.

12. Розроблення освітніх програм: методичні рекомендації / Авт.: В.М. Захарченко, В.І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. – К. ДП "НВЦ "Пріоритети", 2014. – 120 с. – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoikomandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskohoprotsesu.html?download=84: rozroblennia-osvitnikh-prohram-metodychnirekomendatsii&start=80.