МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»
назва освітньої програми

другого магістерського рівня вищої освіти

за спеціальністю 125 «Кібербезпека»»

галузі знань 12 «Інформаційні технології»

Кваліфікація: Магістр з кібербезпеки

ЗАТВЕРДЖЕНО

Вченою радою
Київського національного університету
будівництва і архітектури
зі змінами
Протокол № 46 від 20.12.2021

Освітня програма вводиться в дію з 01 вересня 2022 р.

Голова Вченої ради

_____ П.М. Куліков

«20» грудня 2021 р.

Київ – 2021 р.

ЛИСТ ПОГОДЖЕННЯ

освітньої програми підготовки здобувачів вищої освіти
на другому (магістерському) освітньому рівні
за спеціальністю 125 «Кібербезпека»

1. Погоджено на засіданні НМК зі спеціальності
(Протокол № 3 від 15.12. 2021 р.)

Гарант освітньої програми

_____ Юрій ХЛАПОНІН

«15» 12 2021 р.

2. Перевірено навчально-методичним відділом

Начальник навчально-методичного відділу _____ Ігор СКЛЯРОВ

«16» 12 2021 р.

3. Погоджено на засіданні Методичної ради Університету
(Протокол № 3 від 17.12.2021 р.)

Проректор з навчально-методичної
роботи КНУБА _____ Андрій ШПАКОВ

«17» грудня 2021 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.т.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.

Стейкґолдери:

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 освітньої-професійної програми
«Безпека інформаційних і комунікаційних систем»
зі спеціальності 125 «Кібербезпека»

1 - Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Київський національний університет будівництва і архітектури, факультет автоматизації та інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр, Магістр з кібербезпеки
Офіційна назва освітньо-професійної програми	Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» другого рівня вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології»
Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1,4 роки
Наявність акредитації	Первинна акредитація як правильно для магістрів ? Міністерство Освіти і науки України, сертифікат про акредитацію спеціальності: Серія УД №11003275 від 27 грудня 2018 р., термін дії сертифіката до 1 липня 2024р.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – перший цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра або освітньо-кваліфікаційного рівня спеціаліста
Мова викладання	українська
Термін дії освітньо-професійної програми	До наступної акредитації
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://org2.knuba.edu.ua/
2 - Мета освітньо-професійної 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» достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та ін-	

формаційних технологій, педагогіки та методики вищої освіти.	
3 - Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність)	***Об'єкти професійної діяльності випускників:*** – 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 діяльності.*** ***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-	Освітньо-професійна програма з прикладною

професійної програми	спрямованістю за спеціалізацією безпека інформаційних і комунікаційних систем.
Основний фокус освітньо-професійної програми та спеціалізації	Дослідження в області практики та науки захисту інформації, організації та забезпечення інформаційної та/або кібербезпеки об’єктів, що підлягають захисту.
Особливості 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 Укра-

	їні»
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; реалізуються через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи з використанням елементів дистанційного навчання, розв'язування прикладних задач, виконання проектів, 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, періодичний, 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 бакалавра.
6 – Програмні компетентності	
Інтегральна Компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
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 спеціальності (ФК)	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 (ПРН)	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 кі-

	бербезпеки. 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	Кількісні та якісні показники рівня наукової та професійної активності науково-педагогічних працівників, які забезпечують навчальний процес за освітньою програмою повністю відповідають Ліцензійним умовам впровадження освітньої діяльності закладів освіти
Матеріально-технічне забезпечення	Кількісні показники матеріально-технічного забезпечення повністю відповідають Ліцензійним умовам впровадження освітньої діяльності закладів освіти
Інформаційне та навчально-методичне забезпечення	Обсяг, склад та якість інформаційного та навчально- методичного забезпечення повністю відповідають Ліцензійним умовам впровадження освітньої діяльності закладів освіти
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 вищої освіт	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 відеаналітики	5,0	Іспит
ОК 2	Методи побудови і аналіз криптосистем	4,0	Іспит
ОК 3	Методи захисту розподілених інформаційних ресурсів	10,0	Залік,Іспит
ОК 4	Технології створення та застосування систем захисту інформаційно-комунікаційних систем	10,0	Залік,Іспит
ОК 5	Професійна іноземна мова	3,0	Залік
ОК 6	Безпека інтернет-ресурсів	5,5	Іспит
Загальний обсяг обов`язкових компонент		**37,5**	
Вибіркові компоненти ОПП *(здобувач обирає дисципліни сумарним обсягом 22,5 кредитів)*			
ВК	Дисципліни вибіркової компоненти	22,5	Залік
Загальний обсяг вибіркових компонент:		**22,5**	
Практика			
ВП	Переддипломна практика і виправити навч план)	15,0	Залік
Загальний обсяг виробничої практики		**15,0**	
Атестаційна випускна робота на здобуття ОР «магістр»			
АВР	Атестаційна випускна робота магістра	15,0	
Загальний обсяг АВР магістра		**15,0**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		**90**	

Здобувач вищої освіти самостійно обирає дисципліни вибіркової компоненти на освітньому сайті КНУБА org2.knuba.edu.ua

2.2 Структурно-логічна схема ОПП

<table>
<tr><td colspan="3">ОБОВ’ЯЗКОВІ КОМПОНЕНТИ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (ОПП 37,5)</td></tr>
<tr><td>ОК 1
Основи відеаналітики
(5,0)</td><td>ОК 2
Методи побудови і аналізу криптосистем
(4,0)</td><td>ОК 3
Методи захисту розподілених інформаційних ресурсів
(10,0)</td></tr>
<tr><td>ОК 4
Технології створення та застосування систем захисту інформаційно-комунікаційних систем
(10,0)</td><td>ОК 5
Професійна іноземна мова
(3,0)</td><td>ОК 6
Безпека інтернет-ресурсів
(5,5)</td></tr>
<tr><td colspan="3">Вибіркова компонента (ВК 22,5)</td></tr>
<tr><td colspan="2">Переддипломна практика (ПП 15,0) (ОК1-ОК6)</td><td>Атестаційна випускна робота (АВР 15,0), (ОК1-ОК6)</td></tr>
</table>

3. Форма атестації здобувачів вищої освіти освітньо-професійної програми

Завершальним етапом навчання студентів зі спеціальності 125 «Кібербезпека» 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 випускників спеціальності 125 «Кібербезпека» проводиться у формі захисту магістерської випускної роботи і завершується видачею документів встановленого зразка про присудження йому рівня магістр з присвоєння кваліфікації: Магістр з кібербезпеки.

Атестація здійснюється відкрито і публічно.

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. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Система внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти (далі СВЗЯ) в Університеті відповідає вимогам Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG), статті 16 Закону України «Про вищу освіту» (2014) та статті 41 Закону України «Про освіту» (2017).

Система внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти містить:

1) стратегію (політику) та процедури забезпечення якості освіти;
2) систему та механізми забезпечення академічної доброчесності;
3) здійснення моніторингу та періодичного перегляду освітніх програм;
4) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;
5) оприлюднені критерії, правила і процедури оцінювання здобувачів освіти;
6) оприлюднені критерії, правила і процедури оцінювання педагогічної (науково-педагогічної) діяльності педагогічних та науково-педагогічних працівників;
7) забезпечення наявності необхідних ресурсів для організації освітнього процесу, в тому числі для самостійної роботи здобувачів освіти;
8) забезпечення підвищення кваліфікації педагогічних, наукових і науковопедагогічних працівників;
9) забезпечення наявності інформаційних систем для ефективного управління закладом освіти;

10) створення у закладі освіти інклюзивного освітнього середовища, універсального дизайну та розумного пристосування;

11) інші процедури та заходи, що визначаються спеціальними законами або документами.

5. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6
ЗК 1	+	+	+	+	+	+
ЗК 2	+	+	+	+		+
ЗК 3		+	+	+		
ЗК 4		+	+	+		+
ЗК 5		+	+	+	+	+
КФ 1	+	+	+	+		+
КФ 2		+	+	+		
КФ 3		+	+	+		+
КФ 4		+	+	+		+
КФ 5		+	+	+		+
КФ 6		+	+	+		+
КФ 7		+	+	+		+
КФ 8	+	+	+	+		+
КФ 9	+	+	+	+		+
КФ 10	+	+	+	+	+	+
ПП	+	+	+	+	+	+
АВР	+	+	+	+	+	+

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

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

7. Використані джерела

1. Закон України «Про освіту» [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2145-19.
2. Закон “Про вищу освіту” [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18.
3. Рівні Національної рамки кваліфікацій [Електронний ресурс]. – Режим доступу: https://mon.gov.ua/ua/osvita/nacionalna-ramka-kvalifikacij/rivni-nacionalnoyi-ramki-kvalifikacij.
4. Ліцензійні умови провадження освітньої діяльності.
5. Методичні рекомендації щодо розроблення стандартів вищої освіти. Наказ МОНУ від 01.06.2017 № 600 (у редакції наказів МОНУ від 21.12.2017 № 1648).
6. Лист МОНУ від 05.06.2018 № 1/9-377 «Щодо надання роз’яснень стосовно освітніх програм».
7. Лист МОНУ від 28.04.2017 № 1/9-239 «Зразок освітньо-професійної програми для першого та другого рівнів вищої освіти».