

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ



КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Безпека інформаційних і комунікаційних систем»
другого магістерського рівня вищої освіти
за спеціальністю 125. «Кібербезпека»
галузі знань 12 «Інформаційні технології»
Кваліфікація: Професіонал із організації інформаційної безпеки

«ЗАТВЕРДЖЕНО»

Вченою радою Київського національного
університету будівництва і архітектури
зі змінами від **01.03.2021, № 38**
Освітньо-професійна програма
вводиться в дію з **1 липня 2021 р.**

Голова Вченої ради

_____ П.М. Куліков

« ____ » _____ 2021 р.

Київ – 2021

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
підготовки здобувачів вищої освіти на другому (магістерському) рівні
за спеціальністю 125. «Кібербезпека»

1. Методична комісія спеціальності 125. «Кібербезпека»

Протокол № 6 від 23.02.2021 р.

Голова комісії _____ О.О. Терентьєв

2. Проректор з НМР _____ Г.М. Тонкачєєв

« 01 » березня 2021 р.

3. Навчально-методичний відділ (НМВ)

Начальник НМВ _____ І.О. Склєров

« 01 » березня 2021 р.

4. Перший проректор _____ Д.О. Чернишев

« 01 » березня 2021 р.

РОЗРОБНИКИ

1. Хлапонін Ю. І., д.т.н., професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури, гарант освітньої програми.

2. Шабала Є.Є., к.т.н., доцент, доцент 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. Рудницька Олена Володимирівна, д. філ. кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

**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, професіонал із організації інформаційної безпеки
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	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 – 8 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра або освітньо-кваліфікаційного рівня спеціаліста
Мова викладання	українська
Термін дії освітньо-професійної програми	5 років (з дня акредитації до наступного оновлення ОП)
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 інформаційних технологій, педагогіки та методики вищої освіти.	

3 - Характеристика освітньо-професійної програми

<p>Предметна область (галузь знань, спеціальність)</p>	<p>Об'єкти професійної діяльності випускників:</p> <ul style="list-style-type: none">– 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. <p>Цілі навчання підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки.</p> <p>Теоретичний зміст предметної діяльності.</p> <p>Знання:</p> <ul style="list-style-type: none">– 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 IP;– 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. <p>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 інформаційно-комунікаційних технологій.</p>
<p>Орієнтація освітньо-професійної програми</p>	<p>Освітньо-професійна програма з прикладною спрямованістю за спеціалізацією безпека інформаційних і комунікаційних систем.</p>

<p>Основний фокус освітньо-професійної програми та спеціалізації</p>	<p>Дослідження в області практики та науки захисту інформації, організації та забезпечення інформаційної та/або кібербезпеки об'єктів, що підлягають захисту.</p>
<p>Особливості програми</p>	<p>З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації магістр з кібербезпеки, програма забезпечує підготовку професіоналів, здатних:</p> <ul style="list-style-type: none"> – 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 напрямках 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. <p>З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає:</p> <ul style="list-style-type: none"> - 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 <p>Кафедра здійснює реалізацію Міжнародного Erasmus+KA2 проекту «GameHub: Співпраця університетів-підприємств в ігровій індустрії в Україні»</p>

**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;

	<ul style="list-style-type: none"> - 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	<p>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.</p> <p>Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль.</p> <p>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.</p>
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)	<p>ЗК 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК 2. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово</p> <p>ЗК 4. Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок</p>

	та їх застосування в практичних ситуаціях ЗК 5. Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням
Фахові компетентності спеціальності (ФК)	<p>ФК 1. Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації</p> <p>ФК 2. Здатність до виявлення вразливостей та забезпечення безпеки проводових і бездротових мереж, розслідування інцидентів інформаційної та/або кібербезпеки та протидії злочинному програмному забезпеченню.</p> <p>ФК 3. Здатність до забезпечення безпеки Web ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження.</p> <p>ФК 4. Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.</p> <p>ФК 5. Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації.</p>
7 - Програмні результати навчання	
Програмні результати навчання (ПРН)	<p>ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.</p> <p>ПРН2. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.</p> <p>ПРН3. Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки.</p> <p>ПРН4. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації.</p> <p>ПРН5. Знати методи організації захищеної передачі даних у незахищеному середовищі.</p> <p>ПРН6. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж.</p> <p>ПРН7. Знати методи і способи розробки та тесту-</p>

	<p>вання програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів).</p> <p>ПРН8. Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки</p> <p>ПРН9. Вміти проектувати перспективні крипто-системи та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.</p>
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 освіти	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 <i>(здобувач обирає дисципліни сумарним обсягом 22,5 кредитів)</i>			
ВК	Дисципліни вибіркової компоненти	22,5	Залік
Загальний обсяг вибірових компонент:		22,5	
Практика			
ВП	Виробнича практика	6,0	Залік
Загальний обсяг виробничої практики		6,0	
Атестаційна випускна робота на здобуття ОР «магістр»			
АВР	Атестаційна випускна робота магістра	24,0	
Загальний обсяг АВР магістра		24,0	
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

ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (ОПП 37,5)		
ОК 1 Основи відеаналі- тики (5,0)	ОК 2 Методи побудови і аналіз криптосистем (4,0)	ОК 3 Методи захисту розподілених інформаційних ресурсів (10,0)
ОК 4 Технології створення та засто- сування систем захисту інфор- маційно-комунікаційних систем (10,0)	ОК 5 Професійна іноземна мова (3,0)	ОК 6 Безпека інтернет- ресурсів (5,5)
Вибіркова компонента (ВК 22,5)		
Виробнича практика (ВП 6,0) (ОК1-ОК6)	Атестаційна випускна робота (АВР 24,0), (ОК1-ОК6)	

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: Професіонал із організації інформаційної безпеки.

Атестація здійснюється відкрито і публічно.

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	+	+	+			
ФК 1		+	+	+		
ФК 2	+	+	+	+	+	+
ФК 3	+	+	+	+	+	+
ФК 4			+			+
ФК 5	+	+		+	+	+

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6
ПРН1	+			+		+
ПРН2	+	+	+	+	+	+
ПРН3		+	+			
ПРН4	+	+	+	+	+	+
ПРН5		+	+			
ПРН6				+	+	+
ПРН7		+				
ПРН8					+	
ПРН9				+	+	+

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».