**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
Протокол № ***20*** від ***8.02.2019 р.***
Освітньо-професійна програма
вводиться в дію з ***1 липня 2019 р.***

Голова Вченої ради
_____ П.М. Куліков
«____» _____ 2019 р.

Київ – 2019

**ЛИСТ ПОГОДЖЕННЯ**

**освітньо-професійної програми**
**підготовки здобувачів вищої освіти на другому (магістерському) рівні**
**за спеціальністю 125. «Кібербезпека»**
**спеціалізації «Безпека інформаційних і комунікаційних систем»**

**1. Методична комісія спеціальності 125. «Кібербезпека»**

Протокол № ***4*** від ***29 січня 2019 р.***

Голова комісії _____ Ю.І. Хлапонін

**2. Вчена рада факультету автоматизації і інформаційних технологій**

Протокол № ***5*** від ***30 січня 2019 р.***

Голова Вченої ради _____ І.В. Русан

**3. Навчально-методичний відділ** (НМВ)

Начальник НМВ _____ І.О. Скляров

«6» 02 2019 р.

**4. Перший проректор** _____ Д.О.Чернишев

«7» 02 2019 р.

# ПЕРЕДМОВА

ОПП розроблено науково-методичною комісією зі спеціальностей 123 «Комп’ютерна інженерія» та 125 «Кібербезпека» у складі:

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. Кучанський О.Ю. к.т.н., доцент, доцент 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** | |
| **Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))** | ***Об'єкти професійної діяльності випускників:*** – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і |

| | |
|---|---|
| | технології;<br>– технології забезпечення безпеки інформації;<br>– процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.<br>***Цілі навчання*** підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки.<br>***Теоретичний зміст предметної діяльності.***<br>***Знання:***<br>– законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;<br>– принципів супроводу систем та комплексів інформаційної та/або кібербезпеки;<br>– теорії, моделей та принципів управління доступом до ІР;<br>– теорії систем управління інформаційною та/або кібербезпекою;<br>– методів та засобів виявлення, управління та ідентифікації ризиків;<br>– методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації;<br>– методів та засобів технічного та криптографічного захисту інформації;<br>– сучасних інформаційно-комунікаційних технологій;<br>– сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій;<br>– автоматизованих систем проектування.<br>***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 інфо-комунікаційних технологій. |
| **Орієнтація освітньо-професійної програми** | Освітньо-професійна програма з прикладною 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:<br>– виявляти та оцінювати ознаки стороннього кібернетичного впливу; |

| | |
|---|---|
| | – моделювати можливі ситуації стороннього кібернетичного впливу та прогнозувати їх можливі наслідки;<br>– 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;<br>– протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів;<br>– забезпечити криптозахист власного інформаційного ресурсу тощо.<br>З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає:<br>- реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів;<br>- 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<br>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:<br>1) адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.;<br>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.);<br>3) створення технічної, проектної та експлуатаційної документації інформаційно-комунікаційних систем (далі – ІКС) та систем захисту інформації (далі – СЗІ);<br>4) налагодження, експлуатації та проведення аналізу |

| | |
|---|---|
| | системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій;<br>5) проведення моніторингу несанкціонованої активності в обчислювальних системах;<br>6) створення, впровадження та експлуатації комплексних систем захисту інформації (далі – КСЗІ), а також СЗІ в складі інформаційно телекомунікаційних (далі – ІТС) та обчислювальних систем;<br>7) формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки;<br>8) проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки;<br>9) підтримка наукових досліджень, педагогічна діяльність тощо.<br>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:<br>- програміст/тестувальник програмного забезпечення систем інформаційної та кібербезпеки;<br>- адміністратор комп'ютерних систем і мереж;<br>- адміністратор інформаційної та кібербезпеки;<br>- аудитор/пентестер безпеки інформаційно-комунікаційних систем;<br>- розробник засобів захисту інформації;<br>- 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.<br>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 (КЗ)** | **ЗК 1**. Здатність застосовувати знання у практичних ситуаціях.<br>**ЗК 2.** Знання та розуміння предметної області та розуміння професії.<br>**ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово<br>**ЗК 4.** Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях<br>**ЗК 5.** Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням |
| **Фахові компетентності спеціальності (КС) (загально-професійні)** | **ФК 1.** Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації<br>**ФК 2.** Здатність до виявлення вразливостей та забезпечення безпеки проводових і бездротових мереж, розслідування інцидентів інформаційної та/або кібербезпеки та протидії злоякісному програмному забезпеченню.<br>**ФК 3.** Здатність до забезпечення безпеки Web ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження.<br>**ФК 4.** Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.<br>**ФК 5.** Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації. |
| **7 - Програмні результати навчання** | |
| **За загальними та загально-професійними компетентностями** | **ПРН1.** Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.<br>**ПРН2**. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. |

| | |
|---|---|
| | **ПРН3.** Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки.<br>**ПРН4**. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації.<br>**ПРН5.** Знати методи організації захищеної передачі даних у незахищеному середовищі.<br>**ПРН6.** Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж.<br>**ПРН7.** Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів).<br>**ПРН8.** Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки<br>**ПРН9.** Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки. |
| **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 «Безпека інформаційних і комунікаційних систем» та її логічна послідовність

2.1. Перелік компонент ОПП

| Код н/д | Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумкового контролю |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **Обов'язкові компоненти ОПП** | | | |
| ОК 1 | Наукова іноземна мова | 3,0 | залік |
| ОК 2 | Інтелектуальна власність | 2,0 | залік |
| ОК 3 | Охорона праці в галузі | 2,0 | залік |
| ОК 4 | Методика наукових досліджень, ліцензування і патентування наукової продукції | 2,0 | залік |
| ОК 5 | Методологія наукових досліджень в галузі ІТ | 3,5 | залік |
| ОК 6 | Основи відеаналітики | 5,0 | екзамен |
| ОК 7 | Інтелектуальні системи та технології обробки даних | 5,0 | екзамен |
| ОК 8 | Безпека інтернет-ресурсів | 6,0 | екзамен |
| ОК 9 | Методи захисту розподілених інформаційних ресурсів | 8,0 | залік |
| ОК 10 | Моніторинг та аудит інформаційно-комунікаційних систем | 4,5 | залік |
| ОК 11 | Біометричні системи аутентифікації | 4,0 | залік |
| ОК 12 | Переддипломна практика | 4,5 | |
| ОК 13 | Атестаційна випускова робота магістра | 25,5 | |
| **Загальний обсяг обов'язкових компонент:** | | **75,0** | |
| **Вибіркові компоненти ОПП** | | | |
| ВК 1 | Методи побудови і аналізу криптосистем | 3,0 | екзамен |
| ВК 3 | Цифрові системи зв'язку | 2,0 | екзамен |
| ВК 2 | Технології створення та застосування систем захисту інформаційно-комунікаційних систем | 10,0 | залік |
| ВК 4 | Моделювання пристроїв та лінійні компоненти комп'ютерних систем | | залік |
| **Загальний обсяг вибіркових компонент:** | | **15,0** | |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ** | | **90,0** | |

2.2 Структурно-логічна схема освітньо-професійної програми «Безпека інформаційних і комунікаційних систем»

У структурно-логічній схемі освітньо-професійної програми спеціальності 125 «Кібербезпека» використані наступні позначення, цифрами вказано:

- в чисельнику – кількість навчальних кредитів;
- в знаменнику – порядковий номер семестру;
- в дужках – пререквізити (номера попередніх забезпечуючих дисциплін).

## Структурно-логічна схема ОПП «Безпека інформаційних і комунікаційних систем»

<table>
<tr><td colspan="4">Обов’язкові компоненти освітньо–професійної програми</td></tr>
<tr><td>ОК 1. Наукова іноземна мова<br>3,0/ 2</td><td>ОК 2. Інтелектуальна власність<br>2,0/2</td><td>ОК 3. Охорона праці в галузі<br>2,0/1</td><td>ОК 4 Методика наукових досліджень<br>2,0/ 2</td></tr>
<tr><td>ОК 5. Методологія наукових досліджень<br>2,5/ 2 (ОК 4; ОК 7)</td><td>ОК 6. Основи відеаналітики<br>5,0/ 1</td><td>ОК 7. Інтелектуальні системи<br>5.0/ 1 (ОК 2)</td><td>ОК 8. Безпека інтернет-ресурсів<br>6,0/2 (ОК5, ОК7)</td></tr>
<tr><td>ОК 9. Методи захисту<br>3,5/ 1,2 (ОК 5, ОК8)</td><td>ОК 10. Моніторинг та аудит<br>4,5/2 (ОК4)</td><td>ОК 11. Біометричні системи аутентифікації<br>4,0/1</td><td>ОК 12. Переддипломна практика<br>4,5/1</td></tr>
<tr><td colspan="4">Вибіркові компоненти освітньо-професійної програми</td></tr>
<tr><td>ВК1 Методи побудови і аналізу криптосистем<br>6,0/1</td><td>ВК2 Технології створення та застосування систем<br>9,0/ 1,2</td><td>ВК 3 Цифрові системи зв’язку<br>6,0/1</td><td>ВК 4 Моделювання пристроїв<br>10,0/ 1,2</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">ОК 13 Атестаційна випускова робота магістра 25,5/2</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: Професіонал із організації інформаційної безпеки.

Атестація здійснюється відкрито і публічно.

## 4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

4.1. Обов’язкові компоненти освітньої програми

| | ОК 1 | ОК 2 | ОК 3 | ОК 4 | ОК 5 | ОК 6 | ОК 7 | ОК 8 | ОК 9 | ОК 10 | ОК 11 | ОК 12 | ОК 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ЗК 1** | | | | | | | | + | + | + | | | |
| **ЗК 2** | | | | | | | | | + | + | | + | |
| **ЗК 3** | | | | | | | | + | | | | | |
| **ЗК 4** | | | | | | | | | | | | | |
| **ЗК 5** | | + | + | | | | | | | | | | + |
| **ФК 1** | | + | + | + | | | + | | | | | | + |
| **ФК 2** | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **ФК 3** | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **ФК 4** | | | + | | | + | + | | + | | + | | |
| **ФК 5** | + | + | | + | + | + | + | | | | | | |

4.2. Вибіркові компоненти освітньої програми

| | ВК 1 | ВК 2 | ВК 3 | ВК 4 |
|---|---|---|---|---|
| **ЗК 1** | + | + | + | + |
| **ЗК 2** | + | + | + | + |
| **ЗК 3** | + | + | + | + |
| **ЗК 4** | | | + | |
| **ЗК 5** | + | + | | + |
| **ФК 1** | | + | + | + |
| **ФК 2** | + | + | + | + |
| **ФК 3** | + | + | + | + |
| **ФК 4** | | | + | |
| **ФК 5** | + | + | | + |

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

| | ОК 1 | ОК 2 | ОК 3 | ОК 4 | ОК 5 | ОК 6 | ОК 7 | ОК 8 | ОК 9 | ОК 10 | ОК 11 | ОК 12 | ОК 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПРН1** | + | | | + | | + | + | + | + | + | + | + | |
| **ПРН2** | + | + | + | + | + | + | + | | | | | | |
| **ПРН3** | | + | + | | | | | | | | | | |
| **ПРН4** | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **ПРН5** | | + | + | | | | | | | | | | |
| **ПРН6** | + | | | + | | + | + | + | + | + | + | + | |
| **ПРН7** | | + | | | | | | + | | | | | + |
| **ПРН8** | | | | | | | | | + | | + | | |
| **ПРН9** | + | | | + | | + | + | + | + | + | + | + | |