



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

ОСВІТНЯ ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

першого бакалаврського рівня вищої освіти

за спеціальністю 125. «Кібербезпека»

галузі знань 12 «Інформаційні технології»

Кваліфікація: Фахівець із організації інформаційної безпеки

«ЗАТВЕРДЖЕНО»

Вченою радою Київського національного
університету будівництва і архітектури
зі змінами від *01.03.2021, № 38*

Освітня програма
вводиться в дію з *1 липня 2021 р.*

Голова Вченої ради

_____ П.М. Куліков

« ____ » _____ 2021 р.

ЛИСТ ПОГОДЖЕННЯ
освітньої програми
підготовки здобувачів вищої освіти на першому (бакалаврському) рівні
за спеціальністю 125. «Кібербезпека»

1. Методична комісія спеціальності 125. «Кібербезпека»

Протокол № 6 від 23.02.2021 р.

Голова комісії _____ О.О. Терентьев

2. Проректор з НМР _____ Г.М. Тонкачев

« 01 » березня 2021 р.

3. Навчально-методичний відділ (НМВ)

Начальник НМВ _____ І.О. Склярів

« 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 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 і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр, фахівець із організації інформаційної безпеки
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. - Обсяг освітньої програми: - на базі повної загальної середньої освіти з терміном навчання 11 років становить 240 кредитів ЄКТС; термін навчання 3 роки 10 місяців; - на базі освітньо-кваліфікаційного рівня «молодший спеціаліст» становить 180-240 кредитів ЄКТС; термін навчання 2 роки 10 місяців.
Наявність акредитації	Наказ МОН України № 1565 від 19.12.2016р.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – перший цикл, QF-LLL – 6 рівень
Передумови	Атестат про повну середню освіту або диплом молодшого спеціаліста (молодшого бакалавра) за спеціальністю. Умови вступу визначаються «Правилами прийому до Київського національного університету будівництва і архітектури», затвердженими Вченою радою.
Мова викладання	українська
Термін дії освітньої програми	5 років (з дня акредитації до наступного оновлення ОП)
Інтернет-адреса постійного розміщення опису освітньої програми	http://org2.knuba.edu.ua/
2 - Мета освітньої програми	
Надати освіту в галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», забезпечити теоретичну та практичну підготовку висококваліфікованих кадрів, які б набули базових фахових знань для виконання професійних завдань та обов'язків прикладного характеру в галузі. Забезпечити	

умови формування і розвитку програмних компетентностей, що дозволять оволодіти основними знаннями, вміннями, навичками, необхідними для подальшого навчання та подальшої професійної та професійно-наукової діяльності.

3 - Характеристика освітньої 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 фахівців, здатних використовувати і впроваджувати технології 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 інформаційних ресурсів;

– 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, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки.

Інструменти та обладнання:

– системи розробки, забезпечення, моніторингу та

	контролю процесів інформаційної та/ або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітня; основна орієнтованість програми - прикладна; Програма базується на загальновідомих наукових результатах із врахуванням сучасного стану галузі інформаційна безпека, орієнтує на актуальні питання спеціальності 125 «Кібербезпека», в рамках яких можлива подальша професійна та наукова кар'єра.
Особливості програми	Інтеграція виявлення програмно-апаратних засобів, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, наявністю спеціалізованих лабораторій. Фахівці, залучені до професійної підготовки, пройшли стажування у провідних європейських та українських університетах, мають міжнародний досвід освітньої і наукової діяльності. Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти.
4 - Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець підготовлений до роботи в галузі - Інформаційна безпека за ДК 009-2005: Код 72 Діяльність у сфері інформатизації; Код 72.1 Консультування з питань інформатизації; Код 72.2 Розроблення програмного забезпечення та консультування в цій сфері; Код 72.3 Оброблення даних; Код 72.4 Діяльність пов'язана з банками даних; Код 72.6 Інша діяльність у сфері інформатизації; Код 74.6 Проведення розслідувань та забезпечення безпеки. Фахівець здатний виконувати зазначену професійну роботу і може займати первинні посади, що передбачені штатним розписом за професійним спрямуванням, такі як: інспектор та спеціаліст державної служби.

	<p>ОП орієнтована на наступні види діяльності випускників:</p> <ul style="list-style-type: none"> - дослідницька і проектно-конструкторська; - виробничо-технологічна та виробничо-управлінська; - експериментально-дослідницька.
Подальше навчання	Навчання на другому (магістерському) рівні вищої освіти
5 - Викладання та оцінювання	
Викладання та навчання	<p>Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, кредитно-модульна система організації навчання, електронне навчання в системі Moodle, самонавчання, навчання на основі досліджень.</p> <p>Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка кваліфікаційної роботи бакалавра (проекту).</p>
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 безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p>

	<p>КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p>
<p>Фахові компетентності (КФ)</p>	<p>КФ 1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.</p> <p>КФ 2. Здатність до використання інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>КФ 3. Здатність до використання програмних та програмноапаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>К 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p>

	<p>КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційнотелекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.</p>
7 - Програмні результати навчання	
<p>Програмні результати навчання (ПРН)</p>	<p>ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;</p> <p>ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;</p> <p>ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;</p> <p>ПРН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;</p> <p>ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий</p>

результат;

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

ПРН 9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

ПРН12. Розробляти моделі загроз та порушника;

ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;

ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

ПРН15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

ПРН17. Забезпечувати процеси захисту та функціонування інформаційнотелекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей

захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

ПРН19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

ПРН21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах;

ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;

ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;

ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;

ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та\або кібербезпеки відповідно до цілей і завдань організації;

ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної

і\або кібербезпеки;

ПРН36. Виявляти небезпечні сигнали технічних засобів;

ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витіку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;

ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і\або кібербезпеки;

ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та\ або кібербезпеки для розслідування інцидентів;

ПРН44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

ПРН45. Застосовувати рині класи політик інформаційної безпеки та\ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

	<p>ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;</p> <p>ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;</p> <p>ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> <p>ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p> <p>ПРН50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);</p> <p>ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;</p> <p>ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;</p> <p>ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз;</p> <p>ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</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. Допускається перезарахування кредитів, отриманих у інших закладах освіти України
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 освітньої програми та їх логічна послідовність

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП на базі повної загальної середньої освіти			
OK01	Фізичне виховання	6,0	залік
OK02	Ділова іноземна мова	3,0	залік
OK03	Фізика	8,0	залік, іспит
OK04	Математичний аналіз	8,0	іспит, залік
OK05	Алгоритмізація та програмування	8,5	іспит, залік
OK06	Вступ до фаху	4,0	іспит
OK07	Чисельні методи в інформатиці	4,0	іспит
OK08	Комп'ютерна графіка та моделювання	3,5	іспит
OK09	Історія української державності та культури	3,0	залік
OK10	Об'єктно - орієнтоване програмування	8,0	залік, іспит
OK11	Дискретна математика	4,0	іспит
OK12	Організація баз даних	4,0	іспит
OK13	Основи інформаційної безпеки держави	4,0	іспит
OK14	Фізичні основи захисту інформації	4,0	залік
OK15	Історія філософії та філософської думки	3,0	іспит
OK16	Спеціалізовані архітектури комп'ютерів	6,0	залік
OK17	Теорія інформації та кодування	6,0	іспит
OK18	Основи академічного письма	3,0	залік
OK19	Політологія	3,0	іспит
OK20	Дослідження операцій	5,0	іспит
OK21	Системний аналіз	5,0	іспит
OK22	Програмно-апаратні засоби захисту	5,0	залік
OK23	Тестування програмного забезпечення систем	6,0	іспит
OK24	Системи штучного інтелекту	6,0	іспит
OK25	Прикладна криптологія	4,0	іспит
OK26	Проектування інформаційних систем	5,0	іспит
OK27	Технології віртуалізації	6,0	іспит
OK28	Комплексні системи захисту інформації	6,0	іспит
OK29	Сучасні та перспективні системи технічного захисту інформації	4,0	іспит
OK30	Захист даних в інформаційно-комунікаційних	11,0	залік, іспит

	системах		
OK31	Фахова іноземна мова	3,0	залік
Загальний обсяг обов'язкових компонент на базі повної загальної середньої освіти		159,0	
Обов'язкові компоненти ОП на базі освітнього рівня «молодший спеціаліст»			
OK01	Фізичне виховання	3,0	залік
OK10	Об'єктно - орієнтоване програмування	8,0	залік, іспит
OK11	Дискретна математика	4,0	іспит
OK12	Організація баз даних	4,0	іспит
OK13	Основи інформаційної безпеки держави	4,0	іспит
OK14	Фізичні основи захисту інформації	4,0	залік
OK15	Історія філософії та філософської думки	3,0	іспит
OK16	Спеціалізовані архітектури комп'ютерів	6,0	залік
OK17	Теорія інформації та кодування	6,0	іспит
OK18	Основи академічного письма	3,0	залік
OK19	Політологія	3,0	іспит
OK20	Дослідження операцій	5,0	іспит
OK21	Системний аналіз	5,0	іспит
OK22	Програмно-апаратні засоби захисту	5,0	залік
OK23	Тестування програмного забезпечення систем	6,0	іспит
OK24	Системи штучного інтелекту	6,0	іспит
OK25	Прикладна криптологія	4,0	іспит
OK26	Проектування інформаційних систем	5,0	іспит
OK27	Технології віртуалізації	6,0	іспит
OK28	Комплексні системи захисту інформації	6,0	іспит
OK29	Сучасні та перспективні системи технічного захисту інформації	4,0	іспит
OK30	Захист даних в інформаційно-комунікаційних системах	11,0	залік, іспит
OK31	Фахова іноземна мова	3,0	залік
Загальний обсяг обов'язкових компонент на базі освітнього рівня «молодший спеціаліст»		114,0	
Вибіркові компоненти ОП на базі повної загальної середньої освіти <i>(здобувач обирає дисципліни сумарним обсягом 60,0 кредитів)</i>			
ВК	Дисципліни вибіркової компоненти	60	Залік
Загальний обсяг вибірових компонент на базі повної загальної середньої освіти		60	

Вибіркові компоненти ОП на базі освітнього рівня «молодший спеціаліст» <i>(здобувач обирає дисципліни сумарним обсягом 45,0 кредитів)</i>			
ВК	Дисципліни вибіркової компоненти	45	Залік
Загальний обсяг вибіркового компонента на базі освітнього рівня «молодший спеціаліст»		45	
Практика			
ВП	Виробнича практика	6,0	Залік
ПП	Переддипломна практика	6,0	Залік
Загальний обсяг практик		12,0	
Атестаційна випускна робота на здобуття ОС «бакалавр»			
АВР	Атестаційна випускна робота бакалавра	9,0	
Загальний обсяг АВР бакалавра		9,0	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ НА БАЗІ ПОВНОЇ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ		240	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ НА БАЗІ ОСВІТНЬОГО РІВНЯ «МОЛОДШИЙ СПЕЦІАЛІСТ»		180	

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

2.2. Структурно-логічна схема освітньої програми

Обов'язкові компоненти освітньої програми на базі повної загальної середньої освіти (ОП 160,5) Обов'язкові компоненти освітньої програми на базі освітнього рівня «молодший спеціаліст» (ОП 115,5)				
ОК 1 Фізичне виховання (6,0)	ОК 2 Ділова іноземна мова (3,0)	ОК 3 Фізика (8,0)	ОК 4 Математичний аналіз (8,0)	ОК 5 Алгоритмізація та програмування (8,5)
ОК 6 Вступ до фаху (4,0)	ОК 7 Чисельні методи в інформатиці (4,0)	ОК 8 Комп'ютерна графіка та моделювання (3,5)	ОК 9 Історія української державності та культури (3,0)	ОК 10 Об'єктно- орієнтоване програмування (8,0)
ОК 11 Дискретна математика (4,0)	ОК 12 Організація баз даних (4,0)	ОК 13 Основи інформаційної безпеки держави (4,0)	ОК 14 Фізичні основи захисту інформації (4,0)	ОК 15 Історія філософії та філософської думки (3,0)
ОК 16 Спеціалізовані архітектури комп'ютерів (6,0)	ОК 17 Теорія інформації та кодування (6,0)	ОК 18 Основи академічного письма (3,0)	ОК 19 Політологія (3,0)	ОК 20 Дослідження операцій (5,0)
ОК 21 Системний аналіз (5,0)	ОК 22 Програмно- апаратні засоби захисту (5,0)	ОК 23 Тестування програмного забезпечення систем (6,0)	ОК 24 Системи штучного інтелекту (6,0)	ОК 25 Прикладна криптологія (4,0)
ОК 26 Проектування інформаційних систем (5,0)	ОК 27 Технології віртуалізації (6,0)	ОК 28 Комплексні системи захисту інформації (6,0)	ОК 29 Сучасні та перспективні системи технічного захисту інформації (4,0)	ОК 30 Захист даних в інформаційно- комунікаційних системах (11,0)
ОК 31 Фахова іноземна мова (3,0)				

Вибіркова компонента на базі повної загальної середньої освіти (ВК-60) Вибіркова компонента на базі освітнього рівня «молодший спеціаліст» (ВК-45)	
Виробнича та переддипломна практика (ВП-6,0, ПП-6,0) (ОК17-ОК26, ОК28-ОК31, ОК33)	Атестаційна випускна робота на здобуття ОС «бакалавр» (АВР-9,0) (ОК10, ОК15, ОК17-ОК26, ОК28-ОК31, ОК33)

* - в дужках вказана кількість кредитів

3. Форма атестації здобувачів вищої освіти освітньої програми

Атестація випускників спеціальності 125 «Кібербезпека» проводиться у формі захисту атестаційної випускної роботи і завершується видачею документів встановленого зразка про присудження йому рівня бакалавра з присвоєння кваліфікації: Фахівець із організації інформаційної безпеки.

Атестація здійснюється відкрито і публічно.

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Кваліфікаційний проект/робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки.

Кваліфікаційний проект/ робота має бути перевірений на плагіат.

Оприлюднення на сайті.

4. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У закладі вищої освіти повинна функціонувати система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

- 1) визначення принципів та процедур забезпечення якості вищої освіти;
- 2) здійснення моніторингу та періодичного перегляду освітніх програм;
- 3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників закладу вищої освіти та регулярне оприлюднення результатів таких оцінювань на його офіційному веб-сайті, на інформаційних стендах та в будь-який інший спосіб;
- 4) забезпечення підвищення кваліфікації педагогічних, наукових і науковопедагогічних працівників;
- 5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;
- 6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
- 7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;
- 8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників закладів вищої освіти і здобувачів вищої освіти;
- 9) інших процедур і заходів.

Система забезпечення закладом вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням закладу вищої освіти оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним агентством із забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

5. Перелік нормативних документів, на яких базується Стандарт вищої освіти

1. Закон України від 01.07.2014 р. № 1556-VII «Про вищу освіту» [Режим доступу: <http://zakon5.rada.gov.ua/laws/show/2145-19>];
2. Закон України від 05.09.2017 р. «Про освіту» - [Режим доступу: <http://zakon5.rada.gov.ua/laws/show/2145-19>];
3. Постанова Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р. №266 [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/266-2015-п>];
4. Постанова Кабінету Міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р. № 1187 [Режим доступу; <http://zakon4.rada.gov.Ua/laws/show/1187-2015-n/page>]
5. Постанова Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій» від 23.11.2011 р. №1341 [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1341-2011-п>];
6. Національний класифікатор України: «Класифікація видів економічної діяльності» ДК 009: 2010 [Режим доступу; <http://www.ukrstat.gov.ua/>];
7. Національний класифікатор України: «Класифікатор професій» ДК 003: 2010 [Режим доступу: <http://www.dk003.com>];

Інші рекомендовані джерела

1. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG) [Режим доступу: http://ihed.org.ua/images/doc/04_2016_ESG_2015.pdf];
2. International Standard Classification of Education (ISCED 2011): UNESCO Institute for Statistics [Режим доступу: <http://www.uis.unesco.org/education/documents/isced-2011-en.pdf>];
3. ISCED Fields of Education and Training 2013 (ISCED-F 2013): UNESCO Institute for Statistics [Режим доступу: <http://www.uis.unesco.org/Education/Documents/isced-fields-of-educationtraining-2013.pdf>].
4. Методичні рекомендації щодо розроблення стандартів вищої освіти, затверджені Наказом Міністерства освіти і науки України від 01 червня 2016 р. № 600 (зі змінами) [Електронний ресурс]. – режим доступу:

<https://mon.gov.ua/ua/news/usi-novivni-povidomlennya-2016-06-01-metodichnirekomendacziyi-shhodo-rozroblennya-stand>

5. Розроблення освітніх програм. Методичні рекомендації [Режим доступу:

http://ihed.org.ua/images/doc/04_2016_rozroblennya_osv_program_2014_tempus-office.pdf];

6. Національний освітній глосарій: вища освіта [Режим доступу: http://ihed.org.ua/images/doc/04_2016_glossariy_Visha_osvita_2014_tempusoffice.pdf];

7. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд [Режим доступу: http://ihed.org.ua/images/doc/04_2016_Rozvitok_sisitemi_zabesp_yakosti_VO_UA_2015.pdf];

8. Європейська кредитна трансферна накопичувальна система: Довідник користувача [Режим доступу: http://ihed.org.ua/images/doc/04_2016_ECTS_Users_Guide-2015_Ukrainian.pdf].

9. EQF-LLL - European Qualifications Framework for Lifelong Learning [Режим доступу: https://ec.europa.eu/ploteus/sites/eac-eqf/files/brochexp_en.pdf];

10. QF-EHEA - Qualification Framework of the European Higher Education Area [Режим доступу: <http://www.ehea.info/article-details.aspx?ArticleId=67>];

11. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти. - Львів: Видавництво Львівської політехніки, 2014 - 168 с. URL:

<http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3materialy-natsionalnoi-komandy-ekspertiv-shhodo-zaprovadzhenniainstrumentiv-bolonskoho-protseu.html?download=82:bolonskyi-protseu-novaparadyhma-vyshchoi-osvity-yu-rashkevych&start=80>

12. TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів [Режим доступу: <http://www.unideusto.org/tuningeu/>].

