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

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

Київ – 2019

ЛИСТ ПОГОДЖЕННЯ

освітньої програми
підготовки здобувачів вищої освіти на першому (бакалаврському) 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

ОП 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 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. Об'єкт діяльності – методи, системи та комплекси забезпечення безпеки інформаційних і комунікаційних систем.	
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність,	***Об'єкти*** *професійної діяльності випускників*: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні,

спеціалізація (за наявності))	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.
Основний фокус освітньої програми та спеціалізації	Здобуття вищої освіти в галузі інформаційна безпека, спеціальності 125 «Кібербезпека». Основний фокус на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку

	технологій захисту інформації. Освітньо-професійна програма передбачає такі цикли підготовки: – цикл гуманітарної та соціально-економічної підготовки, – цикл математичної та природничо-наукової підготовки, забезпечують певний освітній рівень; – цикл професійної (професійно-орієнтованої) та практичної підготовки, що разом із попередніми циклами забезпечує певний освітньо-кваліфікаційний рівень.
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. 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	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. ОПП орієнтована на наступні види діяльності випускників: - 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	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. 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).
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 безпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	**ЗК 1**. Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації.
Фахові компетентності спеціальності (КС) (загально-професійні)	**ФК 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. **ФК 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. **ФК 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

	ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. **ФК 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. **ФК 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. **ФК 7.** Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) **ФК 8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку **ФК 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. **ФК 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. **ФК 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. **ФК 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам.
Спеціальні (фахові) компетентності (КСП) (спеціалізовано-професійні)	**КСП101**. Здатність до проектування будівель та споруд промислового та цивільного призначення з використанням збірних і монолітних залізобетонних, металевих, кам’яних та дерев'яних конструкцій, в тому числі застосовуючи сучасні програмні комплекси. **КСП102**. Знання та розуміння будівельної механіки та її застосування при розрахунку й проектуванні будівельних конструкцій із використанням систем автоматизованого проектування. **КСП103**. Здатність до розрахунку та конструювання несучих конструкцій і вузлів з’єднання залізобетонних, кам'яних, металевих і дерев’яних конструкцій, в тому числі з використанням сучасних інформаційних технологій. **КСП104**. Здатність аналізувати властивості ґрунтів основи, обирати та проектувати економічні фундаменти різних типів (неглибокого закладання, пальові) з урахуванням взаємодії будівельних конструкцій між собою та із неоднорідним природним або штучним ґрунтовим середовищем при різних за характером навантаженнях. **КСП105**. Здатність забезпечити організацію будівництва будівель та інженерних споруд різної архітектурної та

	технічної складності із використанням сучасних конструкційних матеріалів та енергоефективних технологій. **КСП106**. Здатність до проектування організаційно-технологічних рішень зведення будівель та споруд, володіння базою сучасних технологій будівельного виробництва і вміння впроваджувати їх у практичну діяльність з урахуванням техніко-економічних показників. **КСП107**. Здатність до участі в управлінні комплексними будівельними проектами з усвідомленням відповідальності за прийняті рішення та забезпеченням якості робіт. **КСП 108**. Здатність прогнозувати та вміти оцінювати економічну доцільність зведення будівель та інженерних споруд на етапі проектування.
7 - Програмні результати навчання	
За загальними та загально-професійними компетентностями	**ПРН1.** Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **ПРН2**. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність. **ПРН3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **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. **ПРН5.** Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. **ПРН6.** Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. **ПРН7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки. **ПРН8.** Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН9. 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 ІТС. **ПРН11**. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. **ПРН12.** Розробляти моделі загроз та порушника. **ПРН13.** Аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі

	даних. **ПРН14**. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень. **ПРН15.** Реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів. **ПРН16.** Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (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. **ПРН17.** Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. **ПРН18.** Застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС. **ПРН19.** Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. **ПРН20.** Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **ПРН21.** Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки. **ПРН22.** Здійснювати протидію отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **ПРН23.** Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). **ПРН24**. 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. **ПРН25**. Забезпечувати процеси захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. **ПРН26**. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних

	(автоматизованих) системах. **ПРН27.** Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; **ПРН28.** Виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС та ефективності використання КЗЗ в умовах реалізації загроз різних класів. **ПРН29**. Здійснювати оцінювання можливості несанкціонованого доступу до елементів ІТС. **ПРН30**. Застосовувати теорії та методи захисту для забезпечення безпеки елементів ІТС. **ПРН31**. Вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки. **ПРН32**. Вирішувати задачі забезпечення неперервності бізнес процесів організації. **ПРН33.** Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. **ПРН34.** Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. **ПРН35.** Виявляти небезпечні сигнали технічних засобів. **ПРН36**. Вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації. **ПРН37.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. **ПРН38.** Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. **ПРН39.** Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. **ПРН40**. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. **ПРН41**. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або

	кібербезпеки для розсліду- вання інцидентів. **ПРН42**. вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів. **ПРН43.** Застосовувати політики, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. **ПРН44.** Здійснювати аналіз ризиків обробки інформації в ІТС. **ПРН45.** Вирішувати задачі захисту інформації, що обробляється в ІТС з використанням сучасних методів та засобів криптографічного захисту інформації. **ПРН46**. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІТС. **ПРН47.** Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС. **ПРН48.** Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). **ПРН49.** Забезпечувати конфігурування та робото-спроможність систем виявлення вторгнень в ІТС. **ПРН50**. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. **ПРН51.** Вирішувати задачі аналізу програмного коду на наявність можливих вразливостей.
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 освіт	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою

2. Перелік компонент освітньої програми «Безпека інформаційних і комунікаційних систем» та її логічна послідовність

2.1. Перелік компонент ОП

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 ОП			
ОК 1	Фізичне виховання	4,0	залік
ОК 2	Історія української державності та культури	3,0	залік
ОК 3	Ділова іноземна мова	3,0	залік
ОК 4	Фізика	7,0	залік, екзамен
ОК 5	Математичний аналіз	9,0	екзамен, екзамен
ОК 6	Вступ до фаху	1,5	залік
ОК 7	Чисельні методи в інформатиці	4,0	залік
ОК 8	Комп'ютерна графіка та моделювання	4,0	екзамен
ОК 9	Комп'ютерні технології статистичної обробки інформації	3,5	залік
ОК 10	Інформаційна культура	3,0	залік
ОК 11	Основи теорії кіл, сигнали та процеси в електроніці	5,0	залік
ОК 12	Ділова українська мова	2,0	залік
ОК 13	Філософія	3,0	екзамен
ОК 14	Електротехніка та електроніка	3,5	екзамен
ОК 15	Теорія ймовірностей, ймовірнісні процеси та математична статистика	4,0	екзамен
ОК 16	Дискретна математика	3,5	екзамен
ОК 17	Організація баз даних	3,5	залік
ОК 18	Комп'ютерні мережі	3,0	залік
ОК 19	Системне програмування	4,0	залік
ОК 20	Архітектура комп'ютерних систем	6,0	екзамен
ОК 21	Фізичні основи захисту інформації	4,5	екзамен
ОК 22	Електроживлення захищених інформаційно-комунікаційних систем	3,0	залік
ОК 23	Основи інформаційної безпеки держави	4,0	залік
ОК 24	Економіка і бізнес	1,0	залік
ОК 25	Економіка і бізнес (Економічна теорія)	1,0	залік
ОК 26	Політологія	3,0	залік
ОК 27	Дослідження операцій	4,0	екзамен
ОК 28	Системи штучного інтелекту	6,0	екзамен
ОК 29	Системний аналіз	6,0	екзамен
ОК 30	Веб-програмування	4,5	залік
ОК 31	Технології проектування комп'ютерних ігор: Game design & development	6,0	екзамен
ОК 32	Нормативно-правове забезпечення інформаційної безпеки	3,5	залік
ОК 33	Теоретичні основи захищених інформаційних технологій	5,5	екзамен
ОК 34	Виробнича практика	4,5	залік
ОК 35	Фахова іноземна мова	2,0	залік

ОК 36	Основи охорони праці та безпека життєдіяльності	2,5	залік
ОК 37	Правознавство	2,5	залік
ОК 38	Сучасні техн. створення інтерактивних веб-вузлів	6,0	екзамен
ОК 39	Надійність комп`ютерних систем	4,5	залік
ОК 40	Комплексні системи захисту інформації: проектування, впровадження, супровід	5,5	залік, екзамен
ОК 41	Основи фінансової криптографії	6,0	екзамен
ОК 42	Переддипломна практика	4,5	залік
ОК 43	Атестаційна випускова робота бакалавра	10,5	
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП			
ВК 1	Комп'ютерна схемотехніка та архітектура комп'ютерів	6,0	екзамен
ВК 2	Комп`ютерні мультимедійні системи		екзамен, залік
ВК 3	Алгоритмізація та програмування	9,0	екзамен, залік
ВК 4	Інструментальні засоби програмування		екзамен, залік
ВК 5	Об`єктно - орієнтоване програмування	8,0	залік, екзамен
ВК 6	Інженерія програмного забезпечення		залік, екзамен
ВК 7	Теорія інформації та кодування	6,0	екзамен
ВК 8	Цифрова обробка сигналів		екзамен
ВК 9	Теорія і практика інфраструктури відкритих ключів	3,0	залік
ВК 10	Паралельні та розподілені обчислення		залік
ВК 11	Прикладна криптологія	6,0	екзамен
ВК 12	Технології цифрової обробки інформації		екзамен
ВК 13	Програмно-апаратні засоби захисту	6,0	залік
ВК 14	Лінійні та інтегральні схеми		залік
ВК 15	Теорія прийняття рішень	6,0	екзамен
ВК 16	Проектування інформаційних систем		екзамен
ВК 17	Захист інформації в інформаційно-комунікаційних системах	8,0	залік, екзамен
ВК 18	Адміністрування комп`ютерних мереж		залік, екзамен
ВК 19	Сучасні та перспективні системи технічного захисту інформації	2,0	залік
ВК 20	Цифрова обробка зображень		залік
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

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

У структурно-логічній схемі освітньої 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 ОП
«Безпека інформаційних і комунікаційних систем»

Обов'язкові компоненти освітньої програми

ОК 1. Фізичне виховання 4,0/1-4	**ОК 2. Історія української державності та культури** 3,0/2	**ОК 3. Ділова іноземна мова** 3,0/1	**ОК 4 Фізика** 7,0/1.2
ОК 5. Математичний аналіз 9,0/1,2 (ОК 4; ОК 7)	**ОК 6. Вступ до фаху** 1,5/1	**ОК 7. Чисельні методи в інформатиці** 4.0/2 (ОК 5; ОК 4)	**ОК 8. Комп'ютерна графіка та моделювання** 4,0/2 (ОК5, ОК7)
ОК 9. Комп'ютерні технології статистичної обробки інформації 3,5/ 2 (ОК 5, ОК8)	**ОК 10. Інформаційна культура** 3,0/1 (ОК2;ОК8)	**ОК 11. Основи теорії кіл, сигнали та процеси** 5,0/2	**ОК 12. Ділова українська мова** 2,0/4
ОК 13. Філософія 3,0/4	**ОК 14. Електротехніка та електроніка** 3,5/3 (ОК5)	**ОК 15. Теорія ймовірностей** 4,0/3	**ОК 16. Дискретна математика** 3,5/3 (ОК 5; ОК 4)
ОК 17. Організація баз даних 3,5/3	**ОК 18. Комп'ютерні мережі** 3,0/ 3 (ОК8, ОК9)	**ОК 19. Системне програмування** 4,0/4 (ОК8;ОК5;ОК16)	**ОК 20. Архітектура комп'ютерних систем** 6,0/4 (ОК19)
ОК 21. Фізичні основи захисту інформації 4,5/ 3 (ОК17; ОК18)	**ОК 22. Електроживлення** 3,0/3 (ОК4)	**ОК 23.Основи інформаційної безпеки держави** 4,0/4 (ОК21)	**ОК 24. Економіка** 1,0/6 (ОК5)
ОК 26. Політологія 3,0/5 (ОК24)	**ОК 27. Дослідження операцій** 4,0/5 (ОК5)	**ОК 28. Системи штучного інтелекту** 6,0/6 (ОК9;ОК17)	**ОК 29. Системний аналіз** 6,0/5 (ОК5)
ОК 30. Веб-програмування 4,5/5 (ОК5;ОК27)	**ОК 31. Технології проектування** 6,0/6 (ОК8,ОК5)	**ОК 32. Нормативно-правове забезпечення** 3,5/6	**ОК 33. Теоретичні основи** 5,5/5 (ОК10;ОК29)
ОК 34. Виробнича практика 4,5/6	**ОК 35. Фахова іноземна мова** 2,0/8 (ОК3)	**ОК 36. Основи охорони праці** 2,5/8 (ОК6)	**ОК 37. Правознавство** 2,5/8

ОК 38. Сучасні технології 6,0/7	**ОК 39. Надійність комп'ютерних систем** 4,5/8	**ОК 42. Преддипломна практика** 4,5,/7

Вибіркові компоненти освітньої програми

ВК1 Комп'ютерна схемотехніка 6,0/1	**ВК2 Алгоритмізація** 9,0/1,2	**ВК 3 Комп'ютерні мультимедійні** 6,0/1	**ВК 4 Інструментальні засоби** 9,0/1,2
ВК 5 Об'єктивно-орієнтоване програмування 8,0/3,4	**ВК 6 Теорія інформації** 6,0/4	**ВК 7 Інженерія програмного забезпечення** 8,0/3,4	**ВК 8 Цифрова обробка сигналів** 6,0/4
ВК 9 Теорія і практика інфраструктури 3,0/6	**ВК 10 Прикладна криптологія** 6,0/6	**ВК 11 Програмно-апаратні засоби** 6,0/5	**ВК 12 Паралельні та розподілені обчислення** 3,0/6
ВК 13 Технології цифрової обробки 6,0/6	**ВК 14 Лінійні та інтегральні схеми** 6,0/6	**ВК 15 Теорія прийняття рішень** 6,0/7	**ВК 16 Захист інформації в інформаційно-комун.** 8,0/7,8
ВК 17 Сучасні та перспективні системи 2,0/8	**ВК 18 Проектування інформаційних систем** 6,0/7	**ВК 19 Адміністрування комп'ютерних мереж** 8,0/7,8	**ВК 20 Цифрова обробка зображень** 2,0/8

ОК 43 Атестаційна випускна робота бакалавра 10,5/8

3. Форма атестації здобувачів вищої освіти освітньої 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 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.

4. Матриця відповідності програмних компетентностей компонентам освітньої 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	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК3 5	ОК 36	ОК 37	ОК 38	ОК 39	ОК 40	ОК 41	ОК 42	ОК 43
ЗК 1								+	+	+							+	+					+			+					+	+					+	+	+	+	+	+
ЗК 2									+	+		+					+		+	+							+								+	+	+	+	+			
ЗК 3								+												+													+		+	+	+	+	+			
ЗК 4																+				+				+	+		+	+								+	+	+				
ЗК 5		+	+										+							+																+	+		+			
ФК 1		+	+	+			+						+							+																+	+					
ФК 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ФК 3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ФК 4			+			+	+		+		+				+																			+	+	+	+				
ФК 5	+	+		+	+	+	+							+		+																			+	+	+		+			
ФК 6												+									+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ФК 7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ФК 8	+			+		+						+			+												+		+	+				+				+			
ФК 9	+	+	+	+	+	+	+							+																				+					+			
ФК 10	+			+	+	+	+	+		+				+			+	+					+			+						+	+						+	+	+	
ФК 11									+		+	+						+			+	+	+																+			
ФК 12								+	+												+																+	+	+		+		

4.2. Вибіркові компоненти освітньої програми

	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20
ЗК 1								+	+	+							+	+		
ЗК 2									+	+		+					+		+	+
ЗК 3								+												+
ЗК 4																+				+
ЗК 5		+	+										+							+
ФК 1		+	+	+			+						+							+
ФК 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ФК 3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ФК 4			+			+	+		+		+				+					
ФК 5	+	+		+	+	+	+								+					
ФК 6												+								
ФК 7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ФК 8	+			+		+						+								
ФК 9	+	+	+	+	+	+	+							+						
ФК 10	+			+	+	+	+	+		+				+			+	+		
ФК 11									+		+	+						+		
ФК 12								+	+											

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідним компонентам 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	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК3 5	ОК 36	ОК 37	ОК 38	ОК 39	ОК 40	ОК 41	ОК 42	ОК 43	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9	ВБ 10
ПРН1	+			+		+	+	+	+	+	+	+																																							
ПРН2	+	+	+	+	+	+	+							+																																					
ПРН3		+	+																	+																																+	
ПРН4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН5		+	+																																			+		+											+	
ПРН6																				+	+														+	+	+																
ПРН7		+						+					+							+							+	+	+	+	+	+	+		+	+	+	+	+	+	+	+					+	+			+	
ПРН8									+		+							+				+	+	+									+		+	+	+		+					+				+			
ПРН9													+						+	+								+											+									+				+	+
ПРН10									+		+	+										+	+			+							+		+										+						
ПРН11								+	+	+	+		+				+			+			+			+						+	+							+		+	+	+						+	
ПРН12								+	+	+							+							+	+	+						+	+									+	+					+			
ПРН13								+	+		+							+				+	+					+	+	+									+		+									
ПРН14						+						+																					+	+		+	+			+					+	+			+		
ПРН15								+					+	+	+									+									+							+	+		+					+	+			+	+
ПРН16								+	+	+	+	+	+			+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+			+	+	+	
ПРН17								+	+	+	+	+	+			+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+	+	+			+		+
ПРН18																																																				
ПРН19								+	+	+					+		+	+	+	+								+				+	+					+	+				+			+				+	
ПРН20								+	+	+							+	+		+			+			+		+				+	+						+				+	+	+					+	
ПРН21								+	+	+							+			+			+			+						+	+						+	+				+			+				+	
ПРН22								+	+	+	+			+							+	+	+													+	+	+			+	+									
ПРН23		+				+		+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН24			+			+		+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН25		+				+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+
ПРН26	+		+		+	+		+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+
ПРН27	+			+		+	+	+	+	+	+	+																																								
ПРН28	+	+	+	+	+	+	+							+																																							
ПРН29		+	+																	+																																+	
ПРН30	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН31		+	+																																			+		+											+	
ПРН32																				+	+														+	+	+																
ПРН33		+						+					+							+							+	+	+	+	+	+	+		+	+	+	+	+	+	+	+					+	+			+	
ПРН34									+		+							+				+	+	+									+											+							+	
ПРН35													+						+	+								+											+									+				+	+
ПРН36									+		+	+										+	+			+							+		+										+						
ПРН37								+	+	+	+		+				+			+			+			+						+	+							+		+	+	+						+	
ПРН38								+	+	+							+							+	+	+						+	+									+	+					+			
ПРН39								+	+		+							+				+	+					+	+	+									+		+									
ПРН40						+						+																					+	+		+	+			+					+	+			+		
ПРН41								+					+	+	+									+									+							+	+		+					+	+			+	+

ПРН42								+	+	+	+	+	+			+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+			+	+	+	
ПРН43								+	+	+	+	+	+			+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+	+	+		+			+
ПРН44																																																					
ПРН45								+	+	+					+		+	+	+	+								+				+	+						+	+				+	+	+				+		+	
ПРН46								+	+	+							+	+		+			+			+		+				+	+											+	+	+						+	
ПРН47								+	+	+							+						+			+						+	+						+	+	+				+					+		+	
ПРН48								+	+	+	+			+							+	+	+													+	+	+			+	+					+						
ПРН49		+				+		+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+
ПРН50			+			+		+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+
ПРН51		+				+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+