МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ

ОСВІТНЬО - ПРОФЕСІЙНА ПРОГРАМА

назва «Безпека інформаційних і комунікаційних систем»

першого (бакалаврського) рівня вищої освіти

спеціальність F5 Кібербезпека та захист інформації

галузь знань F Інформаційні технології

кваліфікація Бакалавр з кібербезпеки та захисту інформації

«ЗАТВЕРДЖЕНО»
вченою радою УДУНТ
26. 02. 2025 р. протокол № 08

«ВВЕДЕНО В ДІЮ»
наказом № 33 від 28. 02. 2025 р.

Ректор
професор _____ Костянтин СУХИЙ

Дніпро – 2025

ЛИСТ ПОГОДЖЕННЯ

освітньо - професійної програми

першого (бакалаврського) рівня вищої освіти

«Безпека інформаційних і комунікаційних систем»

(назва освітньо-професійної програми)

Перший проректор / Голова ради якості освітньої діяльності _____ Анатолій РАДКЕВИЧ

(підпис) (Ім'я ПРІЗВИЩЕ)

Протокол №06 від «18» 02 2025 р.

Проректор з науково-педагогічної роботи _____ Олександр ЗАЙЧУК

(підпис) (Ім'я ПРІЗВИЩЕ)

«25» 02 2025 р.

Директор ННІ ДІІТ _____ Михайло КАПІЦА

(підпис) (Ім'я ПРІЗВИЩЕ)

«25» 02 2025 р.

Навчально-науковий центр забезпечення якості освіти
Керівник _____ Сергій ГРИШЕЧКІН

(підпис) (Ім`я ПРІЗВИЩЕ)

«25» 02 2025 р.

Рада студентів ННІ ДІІТ
Голова _____ Анастасія БОРИСЕНКО

(підпис) (Ім'я ПРІЗВИЩЕ)

«25» 02 2025 р.

Реєстраційний номер ЕС.1.01. _____

(підпис відповідального працівника)

«26» 02 2025 р.

ПЕРЕДМОВА
освітньо - професійної програми
«Безпека інформаційних і комунікаційних систем»
першого (бакалаврського) рівня вищої освіти

ІНІЦІЙОВАНА

Кафедрою «Електронні обчислювальні машини»
«05» травня 2025 р. протокол № 13 .

В.о. завідувача кафедри Олександра ГОРБОВА

ПІДСТАВА

Програму складено на підставі стандарту вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації», що затверджений наказом МОН України від 04.10.2018р. №1074 (у редакції наказу МОН України від 29.10.2024р. №1547) та відповідно до постанови Кабінету Міністрів України від 16.12.2022р. №1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» і з метою оптимізації назви для продовження реалізації освітньої програми «Безпека інформаційних і комунікаційних систем», яка введена в дію наказом від 29.05.2024р. №67.

В освітню програму внесені зміни:

- згідно з наказом ректора №33 від 28.02.2025р. «Про затвердження освітніх програм» у зв'язку зі змінами переліку галузей знань та спеціальностей, затвердженого Постановою КМУ від 30.08.2024р. №1021 "Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти»;
- згідно з наказом ректора №360 від 30.06.2025 «Про внесення змін до освітніх програм».

Проєктна група освітньої програми:

1. Денис ОСТАПЕЦЬ, к.т.н., доцент, доцент каф. ЕОМ – гарант
   Ім'я, прізвище, науковий ступінь, звання
2. Вікторія ПАХОМОВА, к.т.н., доцент, доцент каф. ЕОМ
   Ім'я, прізвище, науковий ступінь, звання
3. Олексій ЗАЄЦЬ, старший викладач каф. ЕОМ
   Ім'я, прізвище, науковий ступінь, звання
4. Геннадій ТАРАСКІН, головний інженер ВП «Дніпровське відділення» філії «Головний ІОЦ» АТ «Укрзалізниця»
   Ім'я, прізвище, науковий ступінь, звання
5. Михайло КОННОВ, головний спеціаліст з вимірювання ефективності СУІБ АТ КБ «Приватбанк»
   Ім'я, прізвище, науковий ступінь, звання
6. Дмитро ПІРОГОВ, студент групи КБ2111

До ОПП надані такі відгуки (рецензії)

1. Андрій ГИРЯ – Начальник виробничого підрозділу «Дніпровське відділення» філії «Головний ІОЦ» АТ «Укрзалізниця»
2. Валерій ЄСІН – Директор ТОВ «Спеціальні захисні системи»
3. Кирило ТКАЧЕНКО – студент групи КС2421

1. Профіль освітньо-професійної програми
спеціальність F5 Кібербезпека та захист інформації
назва «Безпека інформаційних і комунікаційних систем»

1.1 - Загальна інформація	
Повна назва закладу вищої освіти	Український державний університет науки і технологій Навчально-науковий інститут «Дніпровський інститут інфраструктури і транспорту»
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Кваліфікація – Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» першого (бакалаврського) рівня вищої освіти Галузь знань F Інформаційні технології Спеціальність F5 Кібербезпека та захист інформації
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньої програми бакалавра: - на базі повної загальної середньої освіти – 240 кредитів ЄКТС - на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). На основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти. Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» здійснюється за результатами зовнішнього незалежного оцінювання в порядку, визначеному законодавством.
Форми здобуття освіти та розрахункові строки виконання освітньої програми за кожною з форм	Денна (3 роки 10 місяців)
Наявність акредитації	Міністерство освіти і науки України, ДОУ «Навчально-методичний центр з питань якості освіти», сертифікат про акредитацію спеціальності УД №04020373, дійсний до 01.07.2029.
Рівень	НРК України - 6 рівень / перший (бакалаврський) рівень вищої освіти EQF – 6 рівень, QF-EHEA – перший цикл.
Передумови	Вимоги щодо попередньої освіти: – Повна загальна середня освіта або ступінь «молодший бакалавр» (освітньо-кваліфікаційний рівень «молодший спеціаліст») – Решта вимог визначаються правилами прийому на освітньо-

	професійну програму бакалавра
Мова(и) викладання	Українська мова
Термін дії освітньої програми	До виключення з переліку освітніх програм, що реалізує університет
Інтернет-адреса постійного розміщення опису освітньої програми	https://ust.edu.ua/osvita/katalog-osvitnih-program/osvitni-programy/
1.2 - Мета освітньої програми	
Мета (цілі) освітньої програми: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, забезпечення високого рівня підготовки фахівців та формування особистості фахівця, здатного вирішувати типові та складні професійні завдання в галузі інформаційної та/або кібербезпеки. Дана ОПП корелюється зі Стратегічним планом розвитку університету щодо місії університету (зокрема, у частині підготовки висококваліфікованих фахівців, яких визнано в Україні та за її межами).	
1.3 - Характеристика освітньої програми	
Опис предметної області	**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	**Освітньо-професійна** **Види професійної діяльності**, до виконання яких готуються випускники, що освоїли програму бакалавра: проектно-технологічна; виробничо-технологічна; організаційно-управлінська; науково-дослідна; інноваційна
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі «**Інформаційні технології»** за спеціальністю **«Кібербезпека та захист інформації».** Ключові слова: – Апаратні засоби забезпечення безпеки комп'ютерних систем; – Програмні засоби забезпечення безпеки комп'ютерних систем; – Інформаційна безпека комп'ютерних систем та мереж.
Особливості програми	Підготовка висококваліфікованих фахівців для роботи в галузі 12 «Інформаційні технології», враховуючи потреби організацій, промислових підприємств, підприємств транспорту, науково-дослідних та освітніх закладів Придніпровського регіону, України та інших країн. Системний підхід до підготовки бакалаврів, інтеграції класичних методів освіти та практичного досвіду.
1.4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно з Національним класифікатором професій України (ДК 003:2010): 1. Адміністратор безпеки мереж і систем, 2139.2 2. Фахівець сфери захисту інформації, 2139.2 3. Фахівець з питань безпеки (інформаційно-комунікаційні технології), 2139.2 4. Конструктор систем кібербезпеки, 2132.2 5. Фахівець з підтримки інфраструктури кіберзахисту, 2139.2 6. Фахівець з реагування на інциденти кібербезпеки, 2139.2 7. Фахівець з криптографічного захисту інформації, 2139.2 8. Фахівець з технічного захисту інформації, 2139.2 9. Фахівець з тестування систем захисту інформації, 2139.2 10. Аудитор інформаційних технологій (з кібербезпеки), 2139.2 11. Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2
Подальше навчання	Мають право продовжити навчання на другому (магістерському) рівні за цією та іншими освітніми програмами.
1.5. Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, проблемно–орієнтоване навчання, самонавчання на основі інформаційних технологій дистанційного навчання. Основними формами організації навчального процесу є лекції, мультимедійні лекції, семінари, практичні заняття, лабораторні роботи, консультації, курсове проектування, самостійна робота (зокрема, з використанням технології дистанційного online навчання), виробнича практика, підготовка та захист кваліфікаційної бакалаврської роботи.
Оцінювання	*Види контролю*: поточний, тематичний, періодичний, підсумковий, самоконтроль.

	Форми контролю: усне та письмове опитування, тестові завдання, захист лабораторних та практичних робіт, захисти курсових проектів та робіт, захист кваліфікаційної роботи, єдиний державний кваліфікаційний іспит.
1.6. Програмні компетентності	
Інтегральна компетентність	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 (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК 4. Здатність спілкуватися іноземною мовою. ЗК 5. Здатність вчитися і оволодівати сучасними знаннями. ЗК 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. ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК 8. 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.
Спеціальні (фахові, предметні) компетентності (СК)	СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та

	технічних засобів і методів, процедур, практичних прийомів тощо) СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
1.7. Програмні результати навчання (РН)	
	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

	РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому. РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси

	захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
1.8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає ліцензійним умовам згідно з Постановою КМУ від 10.12.15 №1187 (в редакції постанови КМУ від 24.03.21 №365). Кадровий склад науково-педагогічних, педагогічних працівників, що забезпечує навчальний процес на здобуття студентами першого (бакалаврського) рівня вищої освіти за освітньою програмою: доктори наук, професори – 28%, кандидати наук, доценти – 72%.
Матеріально-технічне забезпечення	Лекційні аудиторії, що мають мультимедійне обладнання; Лабораторії, що мають обладнання, яке відповідає предметній галузі (вимірювальні пристрої, комп'ютери, мережеве обладнання, стенди, тощо). Перелік обладнання та приміщень, де воно розташовано, вказано на сайті університету: http://diit.edu.ua/faculty/tk/kafedra/evm/material_base Відповідно договорам про філії кафедри ЕОМ (виробничій підрозділ «Дніпровського відділення» філії «Головний інформаційно-обчислювальний центр», філії «Проектно-конструкторське технологічне бюро інформаційних технологій» АТ «Українська залізниця», лабораторії спецзв'язку та захисту інформації першого відділку «Дніпровського відділення» АТ «Українська залізниця») можливо використання лабораторій цих підприємств в начальному процесі кафедри. У цілому матеріально-технічне забезпечення освітнього процесу відповідає ліцензійним умовам згідно з Постановою КМУ від 10.12.15 №1187 (в редакції постанови КМУ від 24.03.21 №365).
Інформаційне та навчально-методичне забезпечення	**Інформаційно-технологічне забезпечення освітнього процесу** Бібліотека: – використання бібліотечного фонду університету, онлайн-ресурсів та баз даних; – інформаційне забезпечення студентів, які працюють над проектами та дипломами Навчальні ресурси: – довгострокові і короткострокові позики книг, доступ до онлайн- ресурсів, міжбібліотечні позики, відеотека; – продовження терміну позики та бронювання книг онлайн; – доступ до електронних журналів; – доступ до електронних бібліотечних ресурсів світу; – доступ до електронного навчального середовища Moodle; – технологічне і матеріально-технічне забезпечення освітнього процесу Академічна підтримка: – консультації з вибору програми, окремих вибіркових дисциплін, – проектування індивідуальних навчальних траєкторій – персональне консультування
1.9. Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність регламентується «Положенням про порядок реалізації права на академічну

	мобільність учасників освітнього процесу», затвердженого наказом ректора.
Міжнародна кредитна мобільність	Міжнародна кредитна мобільність здійснюється на основі договорів між іноземними університетами та УДУНТ і регламентується «Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу», затвердженого наказом ректора.
Навчання іноземних здобувачів вищої освіти	Підготовка іноземців здійснюється згідно із Законами 15 здобувачів вищої освіти України «Про вищу освіту», «Про правовий статус іноземців та осіб без громадянства», постановою Кабінету Міністрів України від 11 вересня 2013 року № 684 «Деякі питання набору для навчання іноземців та осіб без громадянства», наказом Міністерства освіти і науки України від 01 листопада 2013 року № 1541 «Деякі питання організації набору та навчання (стажування) іноземців та осіб без громадянства», зареєстрованим у Міністерстві юстиції України 25 листопада 2013 року № 2004/24536. Наявність в університеті відділу міжнародних зав'язків, відділу роботи з іноземними студентами, гуртожитку та інформаційного пакету для іноземних студентів.

2. Перелік компонентів освітньо-професійної програми та її логічна послідовність

2.1 Перелік компонентів ОП

Код освітньої компоненти	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові компоненти (ОК) ***1.1. Обов'язкові компоненти загальної підготовки***			
ОК1.1	Історія та культура України	3	Залік
ОК1.2	Українська мова за професійним спрямуванням	3	Залік
ОК1.3	Іноземна мова за професійним спрямуванням	8	Залік, Екзамен
ОК1.4	Філософія	4	Екзамен
ОК1.5	Основи охорони праці та безпека життєдіяльності	4	Залік
ОК1.6	Правознавство	3	Залік
ОК1.7	Вища математика	12	Екзамен
ОК1.8	Фізика	6	Екзамен
ОК1.9	Алгоритми та методи обчислень	4	Екзамен
ОК1.10	Комп'ютерна дискретна математика	5	Екзамен
ОК1.11	Математичні основи інформаційної безпеки	5	Екзамен
ОК1.12	Теорія електричних та магнітних кіл	6	Екзамен
ОК1.13	Фізична культура	4	Залік
ОК1.14	Інформаційні технології в діяльності бакалавра	4	Залік
1.2. Обов'язкові компоненти професійної підготовки			
ОК2.1	Вступ до спеціальності	3	Залік
ОК2.2	Основи програмування	10	Екзамен
ОК2.3	Комп'ютерна схемотехніка	5	Екзамен
ОК2.4	Комп'ютерна логіка (+ курсовий проект)	6	Екзамен, Залік
ОК2.5	Комп'ютерні мережі	5	Екзамен
ОК2.6	Локальні мережі	5	Екзамен
ОК2.7	Управління інформаційною безпекою	4	Екзамен
ОК2.8	Архітектура комп'ютерних систем	7	Залік, Екзамен
ОК2.9	Операційні системи	5	Екзамен

ОК2.10	Методи та засоби захисту інформації	6	Екзамен
ОК2.11	Бази даних	5	Екзамен
ОК2.12	Захист інформації в комп'ютерних мережах	5	Екзамен
ОК2.13	Прикладна криптологія (+ курсова робота)	8	Екзамен
ОК2.14	Нормативно-правове та організаційне забезпечення систем захисту інформації	4	Залік
ОК2.15	Комплексні системи захисту інформації (+ курсовий проект)	6	Екзамен
ОК2.16	Системи технічного захисту інформації	4	Екзамен
ОК2.17	Виробнича практика	6	Залік
ОК2.18	Кваліфікаційна робота	15	Захист роботи
ОК2.19	Єдиний державний кваліфікаційний іспит*)		Екзамен
2. Вибіркові компоненти (ВК)			
2.1. Вибіркові компоненти загальної підготовки			
ВК1.1	Вибіркова 1.1	4	Залік
ВК1.2	Вибіркова 1.2**	3	Залік
2.2. Вибіркові компоненти професійної підготовки			
ВК2.1	Вибіркова 2.1	5	Залік
ВК2.2	Вибіркова 2.2	4	Залік
ВК2.3	Вибіркова 2.3	6	Залік
ВК2.4	Вибіркова 2.4	5	Залік
ВК2.5	Вибіркова 2.5	4	Залік
ВК2.6	Вибіркова 2.6	6	Залік
ВК2.7	Вибіркова 2.7	5	Залік
ВК2.8	Вибіркова 2.8	4	Залік
ВК2.9	Вибіркова 2.9	5	Залік
ВК2.10	Вибіркова 2.10	3	Залік
ВК2.11	Вибіркова 2.11	6	Залік

*) Компонента ОК2.19 є позакредитною.

**)* Включає «Теоретична підготовка БЗВП», яка є обов'язковою для здобувачів вищої освіти, для яких це передбачено законодавством, та інші дисципліни для вибору іншими здобувачами

Вибіркові компоненти ВК1.1 та ВК1.2 обираються з загального університетського каталогу.

Перелік вибіркових компонент ВК2.1 – ВК2.11 наведено в додатку А.

2.2. Розподіл змісту освітньо-професійної програми за групами компонентів та циклами підготовки

Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
	обов'язкові компоненти	вибіркові компоненти	всього за весь термін навчання
Цикл загальної підготовки	71/29,6	7/2,9	78/32,5
Цикл професійної підготовки	109/45,4	53/22,1	162/67,5
Всього за весь термін навчання	180/75	60/25	240/100

2.3. Структурно-логічна схема освітньої програми

Код навчальної дисципліни	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Код навчальної дисциплін, яка забезпечується зазначеною в стовпчику 1
1	2	
1. Обов'язкові компоненти (ОК)		
ОК1.1	Історія та культура України	ОК1.2
ОК1.2	Українська мова за професійним спрямуванням	ОК2.18
ОК1.3	Іноземна мова за професійним спрямуванням	ОК2.18
ОК1.4	Філософія	ОК2.18
ОК1.5	Основи охорони праці та безпека життєдіяльності	ОК2.18
ОК1.6	Правознавство	ОК2.18
ОК1.7	Вища математика	ОК1.8, ОК1.10, ОК1.11, ОК1.12
ОК1.8	Фізика	ОК1.12
ОК1.9	Алгоритми та методи обчислень	ОК1.11, ОК2.4
ОК1.10	Комп'ютерна дискретна математика	ОК2.4
ОК1.11	Математичні основи інформаційної безпеки	ОК2.7, ОК2.13, ОК2.17
ОК1.12	Теорія електричних та магнітних кіл	ОК2.16
ОК1.13	Фізична культура	ОК2.18
ОК1.14	Інформаційні технології в діяльності бакалавра	ОК1.9, ОК2.18
ОК2.1	Вступ до спеціальності	ОК2.2, ОК2.4, ОК2.7, ОК2.14
ОК2.2	Основи програмування	ОК2.17, ОК2.6, ОК2.9, ОК2.11,

		ОК2.5
ОК2.3	Комп'ютерна схемотехніка	ОК2.8, ОК2.16, ОК2.17
ОК2.4	Комп'ютерна логіка (+ курсовий проект)	ОК2.3, ОК2.8
ОК2.5	Комп'ютерні мережі (+ курсовий проект)	ОК2.12, ОК2.17
ОК2.6	Локальні мережі	ОК2.5
ОК2.7	Управління інформаційною безпекою	ОК2.15, ОК2.18, ОК2.19
ОК2.8	Архітектура комп'ютерних систем	ОК2.9, ОК2.13, ОК2.18, ОК2.19
ОК2.9	Операційні системи	ОК2.10, ОК2.12, ОК2.19
ОК2.10	Методи та засоби захисту інформації	ОК2.12, ОК2.15, ОК2.18, ОК2.19
ОК2.11	Бази даних	ОК2.9, ОК2.10
ОК2.12	Захист інформації в комп'ютерних мережах	ОК2.18, ОК2.19
ОК2.13	Прикладна криптологія (+ курсова робота)	ОК2.9, ОК2.10, ОК2.12, ОК2.15, ОК2.18, ОК2.19
ОК2.14	Нормативно-правове та організаційне забезпечення систем захисту інформації	ОК2.7, ОК2.15, ОК2.18, ОК2.19
ОК2.15	Комплексні системи захисту інформації (+ курсовий проект)	ОК2.18, ОК2.19
ОК2.16	Системи технічного захисту інформації	ОК2.15, ОК2.18, ОК2.19
ОК2.17	Виробнича практика	ОК2.18
ОК2.18	Кваліфікаційна робота	
ОК2.19	Єдиний державний кваліфікаційний іспит	

3. Форма атестації здобувачів вищої освіти

Атестація випускників за освітньою програмою «Безпека інформаційних і комунікаційних систем» спеціальності F5 «Кібербезпека та захист інформації» проводиться у формі єдиного державного кваліфікаційного іспиту та (або) захисту кваліфікаційної роботи і завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації бакалавра з кібербезпеки та захисту інформації.

Заклад вищої освіти забезпечує перевірку кваліфікаційної роботи на плагіат. Реферат кваліфікаційної роботи оприлюднюється у репозитарії університету. Захист кваліфікаційної роботи здійснюється відкрито та публічно.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом спеціальності 125 «Кібербезпека та захист інформації» та цією освітньою програмою.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК1.1	ОК1.2	ОК1.3	ОК1.4	ОК1.5	ОК1.6	ОК1.7	ОК1.8	ОК1.9	ОК1.10	ОК1.11	ОК1.12	ОК1.13	ОК1.14	ОК2.1	ОК2.2	ОК2.3	ОК2.4	ОК2.5	ОК2.6	ОК2.7	ОК2.8	ОК2.9	ОК2.10	ОК2.11	ОК2.12	ОК2.13	ОК2.14	ОК2.15	ОК2.16	ОК2.17	ОК2.18	ОК2.19
ЗК 1			+	+	+	+	+	+	+	+	+				+	+			+	+	+			+			+	+	+	+	+	+
ЗК 2													+										+		+	+		+	+	+	+	
ЗК 3		+	+																												+	+	
ЗК 4															+					+									+		+	+	+
ЗК 5	+	+	+	+	+	+	+	+	+	+	+		+	+		+	+	+	+		+	+	+	+		+	+	+			+	+	+
ЗК 6	+			+								+																+					
ЗК 7	+	+	+	+	+	+						+																			+	+	+
ЗК 8																				+								+	+				
СК1														+		+	+	+			+	+		+	+		+						
СК2																+	+						+		+				+		+	+	
СК3																				+								+			+	+	
СК4																						+	+	+	+	+			+	+			
СК5																						+										+	+	
СК6																	+	+		+								+	+				+
СК7																				+												+	
СК8																				+								+				+	
СК9																							+		+	+			+	+		+	
СК10																						+	+		+							+	

5. Матриця відповідності програмних результатів навчання компонентам освітньої програми

	ОК1.1	ОК1.2	ОК1.3	ОК1.4	ОК1.5	ОК1.6	ОК1.7	ОК1.8	ОК1.9	ОК1.10	ОК1.11	ОК1.12	ОК1.13	ОК1.14	ОК2.1	ОК2.2	ОК2.3	ОК2.4	ОК2.5	ОК2.6	ОК2.7	ОК2.8	ОК2.9	ОК2.10	ОК2.11	ОК2.12	ОК2.13	ОК2.14	ОК2.15	ОК2.16	ОК2.17	ОК2.18	ОК2.19
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
РН1	+	+	+	+																													
РН2																								+							+	+	+
РН3					+	+	+	+	+	+	+		+	+	+	+		+	+		+							+			+		+
РН4					+		+	+	+	+	+			+		+								+		+			+		+		+
РН5																	+	+			+					+					+	+	
РН6					+	+	+	+		+	+				+					+				+	+			+					
РН7																				+								+	+				
РН8																				+								+	+				
РН9																				+								+					+
РН10															+	+	+	+			+	+	+		+				+	+			+
РН11															+									+							+		
РН12															+	+									+			+	+			+	+
РН13															+		+	+	+						+							+	
РН14															+	+						+	+		+				+	+		+	+
РН15														+											+				+	+			
РН16																									+				+			+	
РН17													+		+			+		+	+		+					+					
РН18																							+		+						+	+	+
РН19															+					+		+			+	+	+	+	+	+			
РН20																	+						+		+								
РН21																				+			+	+				+	+				

ДОДАТОК А
Перелік вибіркових компонент професійної підготовки

Код компоненти	Назва компоненти
ВК2.1	Програмні засоби загального користування
	Основи програмування мовою Pyton
ВК2.2	Проектний практикум
	Візуальне програмування
ВК2.3	Мобільні пристрої та додатки
	Технології бездротових мереж
ВК2.4	Системне програмування
	Мова асемблера
ВК2.5	Проектування мікропроцесорних систем захисту
	Комп’ютерні системи збору інформації
ВК2.6	Побудова мікроконтролерних систем захисту
	Програмування апаратних засобів захисту
ВК2.7	ІНТЕРНЕТ технології
	Web-програмування мовою JavaScript
ВК2.8	Теорія інформації та кодування
	Основи цифрової обробки даних та сигналів
ВК2.9	Фізичні основи бездротових мереж
	Теорія радіокіл
ВК2.10	Комп'ютерна електроніка
	Основи дискретної електроніки
ВК2.11	Логічні основи штучного інтелекту
	Інтелектуальні системи аналізу даних