МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

Кваліфікація: Бакалавр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ
Голова Вченої ради_____ Ігор РУБАН
(протокол від " 31" ____01_____2024 р. № 2)
зі змінами
протокол від " 31 " ____03_____2026 р. № 4

Освітня програма вводиться в дію з 01.09.2024 р.

Ректор _____ Ігор РУБАН
(наказ від " 02 " ___02___2024 р. № 40)
зі змінами
наказ від "31" __03_____2026 р. №166

Харків **2026** р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти

ПОГОДЖЕНО
Перший проректор

_____ Андрій ЄРОХІН

«12» 03 2026 р.

Начальник відділу ЛА та ВСЗЯО

_____ Ганна ТУГАЙ

«09» 03 2026 р.

Начальник навчального відділу

_____ Аліна МІХНОВА

«10» 03 2026 р.

Розглянуто на засіданні Вченої ради факультету КБ
Протокол від 30.03.2026 р. № 1
Декан факультету КБ

_____Аркадій СНІГУРОВ

Розглянуто на засіданні кафедри БІТ

Протокол від 10.03.2026 р. № 10
Завідувач кафедри БІТ

_____ Геннадій ХАЛІМОВ

Представники роботодавців
Виконавчий директор ПрАТ «ІІТ» _____ Володимир КРАВЧЕНКО

Представник студентського самоврядування

Голова студентського сенату факультету КБ _____ Сергій АЛФЬОРОВ

РОЗРОБЛЕНО

Проєктна група:

керівник проєктної групи:
Ляшенко Олексій Сергійович, к.т.н., доц.,
доц. каф. ЕОМ, декан факультету КІІТ, ХНУРЕ _____

члени проєктної групи:

Сєвєрінов Олександр Васильович, к.т.н., доц.,
проф. каф. БІТ, ХНУРЕ _____

Радівілова Тамара Анатоліївна, д.т.н.,
проф., професор кафедри ІКІ
імені В.В. Поповського _____

Федюшин Олександр Іванович, к.т.н., доц.,
доц. каф. БІТ, ХНУРЕ _____

Снігуров Аркадій Владиславович, к.т.н.,
доц., доц. каф. ІКІ
ім. В.В. Поповського, ХНУРЕ _____

ПЕРЕДМОВА

Розроблено проєктною групою у складі:

Керівник проєктної групи:

1. Ляшенко Олексій Сергійович - кандидат технічних наук, доцент, декан факультету КІІТ ХНУРЕ;

Члени проєктної групи:

2. Радівілова Тамара Анатоліївна - доктор технічних наук, професор, професор кафедри ІКІ імені В.В. Поповського факультету КБ ХНУРЕ;
3. Сєвєрінов Олександр Васильович - кандидат технічних наук, доцент, професор кафедри БІТ факультету КБ ХНУРЕ;
4. Федюшин Олександр Іванович - кандидат технічних наук, доцент, доцент кафедри БІТ факультету КБ ХНУРЕ;
5. Снігуров Аркадій Владиславович - кандидат технічних наук, доцент, доцент кафедри ІКІ імені В.В. Поповського факультету КБ ХНУРЕ.

Гарант освітньої програми Олександр ФЕДЮШИН

1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем» за спеціальністю 125 Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки, факультет кібербезпеки (КБ), кафедра безпеки інформаційних технологій (БІТ).
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС термін навчання 3 роки 10 місяців, (2 роки 10 місяців)
Наявність акредитації	Сертифікат про акредитацію спеціальності УД 21016832, дійсний до 31.12.2027
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта (або освітньо-кваліфікаційний рівень молодшого спеціаліста)
Мова(и) викладання	Українська, англійська для іноземних студентів
Термін дії освітньої програми:	До повного завершення періоду навчання або наступного оновлення програми.
Інтернет-адреса	https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnosti-ta-osvitni-prohramy-2018-2024-rokiv-pryjomu/spetsialnist-125-kiberbezpeka-ta-zakhyst-informatsii/bakalavr-125-kiberbezpeka-ta-zakhyst-informatsii/osvitnja-programa-bezpeka-informacijnih-i-komunikacijnih-sistem
2- Мета освітньої програми	
Забезпечити підготовку висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 Кібербезпека та захист інформації, здатних вирішувати складні спеціалізовані задачі та практичні проблеми забезпечення інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	12 Інформаційні технології 125 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітньо-професійна програма Програма зорієнтована на набуття знань, умінь, компетенцій в галузі професійної діяльності, що передбачає застосування певних теорій та методів відповідних наук і характеризується комплексністю та невизначеністю умов
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта першого (бакалаврського) рівня в галузі 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації. ***Ключові слова***: кібербезпека, інформаційна безпека, криптографічний захист інформації, технічний захист інформації, захист персональних даних, антивірусний захист, захист інформації від несанкціонованого доступу, електронний цифровий підпис, захист від технічних розвідок

Особливості освітньої програми	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності. Підготовка висококваліфікованих фахівців на високому методичному та професійному рівні.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назва професій згідно Національного класифікатора України: Класифікатор професій (ДК 003: 2010): 2139.2 - фахівець з питань безпеки (інформаційно-комунікаційні технології); 2139.2 - фахівець з криптографічного захисту інформації; 2139.2 - фахівець з технічного захисту інформації; 2139.2 - фахівець сфери захисту інформації; 2139.2 - фахівець з підтримки інфраструктури кіберзахисту; 2139.2 - фахівець з тестування систем захисту інформації; 2139.2 - фахівець з оцінки заходів захисту інформації (кібербезпеки); 2139.2 - фахівець з реагування на інциденти кібербезпеки; 2139.2 - адміністратор безпеки мереж і систем; 2139.2 - аудитор інформаційних технологій (з кібербезпеки); 2132.2 - конструктор систем кібербезпеки; 3439 - фахівець із організації інформаційної безпеки; 3439 - фахівець із організації захисту інформації з обмеженим доступом.
Подальше навчання	Продовження навчання за програмою другого (магістерського) рівня вищої освіти
5 - Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та лабораторні заняття, самонавчання, проектно-орієнтоване навчання, консультації із науково-педагогічними співробітниками, проведення наукових досліджень, підготовка кваліфікаційної роботи
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано) та 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F)
6 – Перелік компетентностей випускника	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (КЗ)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. 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 та 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	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту Інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 - Програмні результати навчання	
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. РНІ5. 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.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов.
Матеріально-технічне забезпечення	1. Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. 2.Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях. 3. Наявність соціально-побутової інфраструктури. 4. Забезпеченість здобувачів вищої освіти гуртожитком. 5. Забезпеченість комп’ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням, необхідними для виконання навчальних планів. 6. Забезпеченість комп'ютерною технікою, контрольно-вимірювальними

	приладами, програмно-технічними засобами автоматизації та системами автоматизації проектування. Засоби обчислювальної техніки з прикладним та спеціалізованим програмним забезпеченням, спеціальні радіовимірювальні пристрої, засоби технічного захисту інформації, спеціалізовані апаратно-програмні комплекси. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітніх сферах, наявністю спеціалізованих лабораторій: основ захисту інформації, технічних і програмно-апаратних засобів захисту і обробки інформації в інформаційно-комунікаційних системах, аналізу захищених децентралізованих блокчейн систем, моніторингу та виявлення каналів витоку інформації. В 2020 році в рамках програми Tempus (Trans-European Mobility Programme for University Studies) закуплено обладнання та створено програмно-апаратний комплекс для вивчення, дослідження та супроводження об'єктів інформаційної діяльності у галузі кібербезпеки.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість вітчизняними та закордонними фаховими періодичними виданнями в галузі інформаційної безпеки та кібербезпеки, в тому числі в електронному вигляді. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. Наявність офіційного веб-сайту закладу освіти (http://nure.ua/) та кафедри (http://its.nure.ua/), на якому розміщена основна інформація про діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/ атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання, також надання доступу до правової БД "Ліга: Закон"; електронних версій підручників видавництва «Центр учбової літератури»; електронних журналів: «Захист інформації. INSIDE»; «Information Security»; online-журнали з наукової бібліотеки eLIBRARY. Специфічними характеристиками інформаційного та навчально-методичного забезпечення є: - використання методів, моделей, методик та технологій створення, обробки, передачі, приймання, знищення, відображення та кіберзахисту інформаційних ресурсів; - використання методів та моделей розробки прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та кібербезпеки; - використання сукупності нормативно-правових (національні та міжнародні стандарти) та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На основі договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн.

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

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни			
ОК 1	Українське фахове мовлення	4	залік
ОК 2	Іноземна мова	8	залік, екзамен
ОК 3*	Українська мова як іноземна	12	залік, екзамен
ОК 4	Філософія	4	екзамен
ОК 5	Основи права	2	залік
ОК 6	Фізичне виховання (за рахунок вільного часу студентів)		залік
ОК 7*	Українська мова як іноземна (за рахунок вільного часу студентів)		залік
Загальний обсяг обов'язкових компонентів за циклом		**18**	
Природничо-наукові (фундаментальні) дисципліни			
ОК 8	Вища математика	12	екзамен
ОК 9	Фізика	6	залік, екзамен
Загальний обсяг обов'язкових компонентів за циклом		**18**	
Дисципліни базової (професійної) підготовки за спеціальністю			
ОК 10	Безпека життєдіяльності	3	залік
ОК 11	Економіка та бізнес	3	залік
ОК 12	Вступ до спеціальності	4	залік
ОК 13	Вища математика (спец. розділи)	4	залік
ОК 14.1	Програмування	9	залік, екзамен
ОК 14.2	Курсова робота з дисципліни Програмування	1	захист курсової роботи
ОК 15	Об'єктно-орієнтоване програмування	4	екзамен
ОК 16	Крос-платформне програмування	4	екзамен
ОК 17	Основи операційних систем	4	екзамен
ОК 18	Схемотехніка	4	залік
ОК 19	Електрорадіовимірювання	4	залік
ОК 20.1	Теорія інформації і кодування	4	екзамен
ОК 20.2	Курсова робота з дисципліни Теорія інформації і кодування	1	захист курсової роботи
ОК 21	Інформаційні технології	4	залік
ОК 22	Архітектура комп'ютерних систем	4	залік
ОК 23	Управління інформаційною безпекою	4	екзамен
ОК 24	Інформаційно-комунікаційні системи	9	залік, екзамен

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОК 25	Нормативно-правове забезпечення інформаційної безпеки	4	залік
ОК 26	Операційні системи	4	залік
Загальний обсяг обов'язкових компонентів за циклом		**78**	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою «Безпека інформаційних і комунікаційних систем»			
ОК 27	Теорія ймовірностей	4	залік
ОК 28	Теорія еліптичних кривих	3	залік
ОК 29	Бази даних	3	залік
ОК 30.1	Прикладна криптологія	7,5	екзамен
ОК 30.2	Курсова робота з дисципліни Прикладна криптологія	1	захист курсової роботи
ОК 31	Тестування програмного забезпечення	3,5	екзамен
ОК 32.1	WEB-програмування та захист веб-додатків	4	залік
ОК 32.2	Курсова робота з дисципліни WEB-програмування та захист веб-додатків	1	захист курсової роботи
ОК 33	Криптосистеми і протоколи	3	екзамен
ОК 34	Комплекси технічного захисту інформації	4	екзамен
ОК 35.1	Проєктування комплексів технічного захисту інформації	3,5	екзамен
ОК 35.2	Курсовий проєкт з дисципліни Проєктування комплексів технічного захисту інформації	1	захист курсового проєкту
ОК 36	Проєктування систем безпеки інформації	3,5	екзамен
ОК 37	Захист інформації в інформаційно-комунікаційних системах	6	екзамен
ОК 38	Виробнича практика	4,5	залік
ОК 39	Передатестаційна практика	4,5	залік
ОК 40	Кваліфікаційна робота	9	екзамен
Загальний обсяг обов'язкових компонентів за циклом		**66**	
ВИБІРКОВІ КОМПОНЕНТИ ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни **			
Дисципліни з загального каталогу вибіркових навчальних дисциплін		**6**	залік
Загальний обсяг вибіркових компонентів за циклом		**6**	
Дисципліна обов'язкова для здобувачів вищої освіти чоловічої статі (жіночої статі – добровільно)			
	Базова загальновійськова підготовка (теоретична підготовка)	**3**	диф. залік
	Базова загальновійськова підготовка (практична підготовка)	**7**	

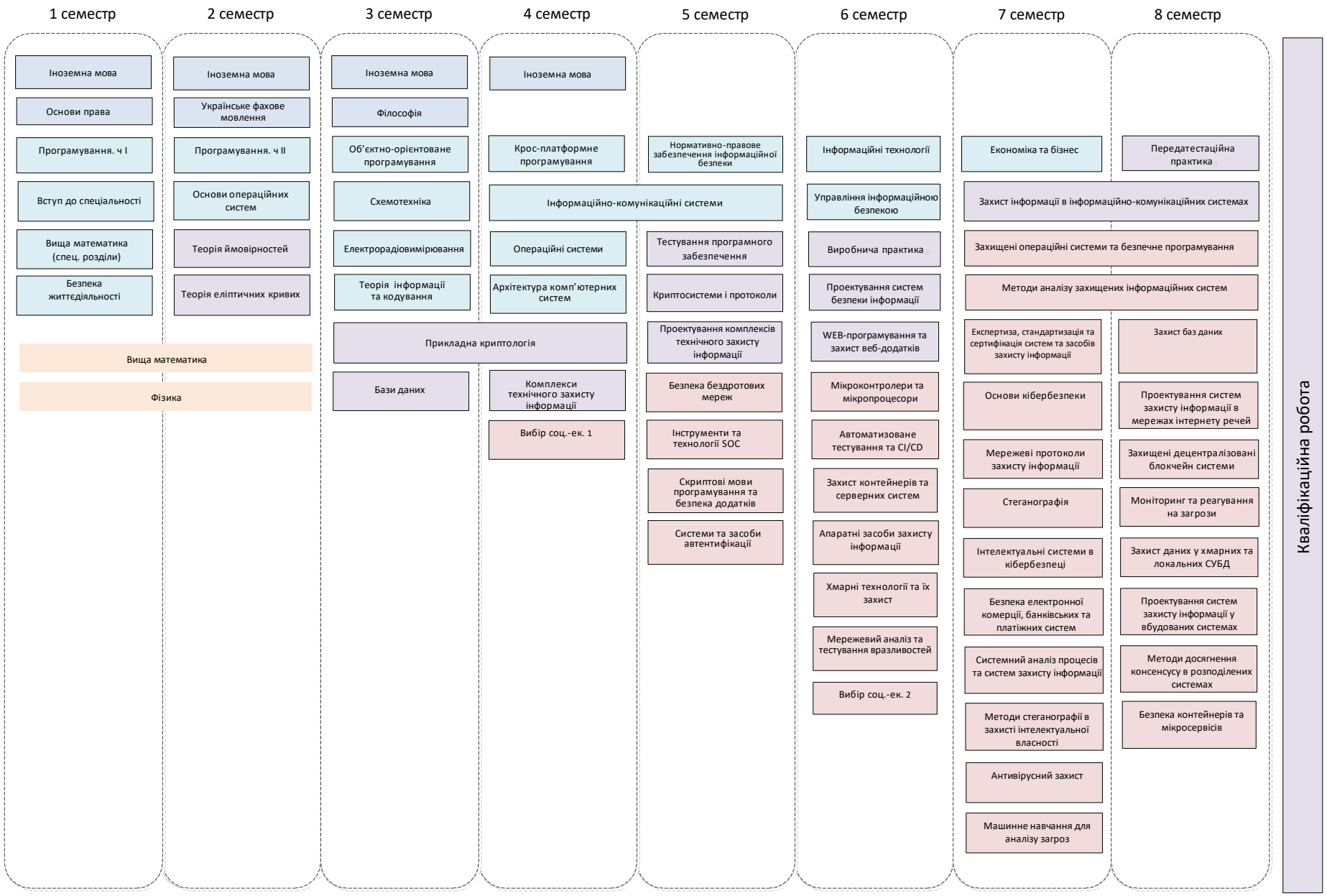
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою «Безпека інформаційних і комунікаційних систем»			
ВК 1	Безпека бездротових мереж	4,5	залік
ВК 2	Системи та засоби автентифікації	4,5	залік
ВК 3	Інструменти та технології SOC	4	залік
ВК 4	Скриптові мови програмування та безпека додатків	4	залік
ВК 5	Мікроконтролери та мікропроцесори	4	залік
ВК 6	Автоматизоване тестування та CI/CD	4	залік
ВК 7	Апаратні засоби захисту інформації	4	залік
ВК 8	Хмарні технології та їх захист	4	залік
ВК 9	Захист контейнерів та серверних систем	4	залік
ВК 10	Мережевий аналіз та тестування вразливостей	4	залік
ВК 11	Експертиза, стандартизація та сертифікація систем та засобів захисту інформації	4	екзамен
ВК 12	Безпека електронної комерції, банківських та платіжних систем	4	екзамен
ВК 13	Основи кібербезпеки	4	залік
ВК 14	Системний аналіз процесів та систем захисту інформації	4	залік
ВК 15	Мережеві протоколи захисту інформації	4	екзамен
ВК 16	Антивірусний захист	4	екзамен
ВК 17	Стеганографія	4	екзамен
ВК 18	Інтелектуальні системи в кібербезпеці	4	залік
ВК 19	Методи стеганографії в захисті інтелектуальної власності	4	екзамен
ВК 20	Машинне навчання для аналізу загроз	4	залік
ВК 21.1	Методи аналізу захищених інформаційних систем	6,5	залік, екзамен
ВК 21.2	Курсова робота з дисципліни Методи аналізу захищених інформаційних систем	1	захист курсової роботи
ВК 22.1	Захищені операційні системи та безпечне програмування	6,5	залік, екзамен
ВК 22.2	Курсова робота з дисципліни Захищені операційні системи та безпечне програмування	1	захист курсової роботи
ВК 23	Захист баз даних	4	залік
ВК 24	Проєктування систем захисту інформації в мережах інтернету речей	3	залік
ВК 25	Захищені децентралізовані блокчейн системи	3	залік
ВК 26	Моніторинг та реагування на загрози	3	залік
ВК 27	Захист даних у хмарних та локальних СУБД	4	залік
ВК 28	Проєктування систем захисту інформації у вбудованих системах	3	залік
ВК 29	Методи досягнення консенсусу в розподілених системах	3	залік

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проекти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ВК 30	Безпека контейнерів та мікросервісів	3	залік
Загальний обсяг вибіркових компонентів за циклом		**54**	
Загальний обсяг вибіркових компонентів		**60**	
Загальний обсяг обов'язкових компонентів		**180**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

* – для іноземних здобувачів вищої освіти;
** – перелік вибіркових компонентів може бути доповнено у робочому навчальному плані з загального каталогу вибіркових дисциплін Університету – у разі вибору здобувачами вищої освіти;

2.2 Структурно логічна схема наведена на рисунку 1.

Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньою програмою «Безпека інформаційних і комунікаційних систем» спеціальності 125 Кібербезпека та захист інформації здійснюється у формі єдиного державного кваліфікаційного іспиту. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою.

Додатковим видом атестації здобувачів вищої освіти передбачено захист кваліфікаційної роботи з видачою документу встановленого зразка про присудження здобувачеві ступеня бакалавра із присвоєнням освітньої кваліфікації: «Бакалавр з кібербезпеки та захисту інформації».

Захист кваліфікаційної роботи здійснюється у формі публічного захисту кваліфікаційної роботи. Кваліфікаційна робота має продемонструвати здатність випускника розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки і\або кібербезпеки та захисту інформації, що характеризується комплексністю та неповною визначеністю умов і вимог.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його підрозділу, або у репозиторії закладу вищої освіти

4. Матриця відповідності компетентностей компонентам освітньої програми

Складається з двох частин у таблицях:

4.1. Матриця відповідності компетентностей обов'язковим компонентам освітньої програми. Може корегуватися за рішенням Вченої ради факультету КБ.

4.2. Матриця відповідності компетентностей варіативним компонентам освітньої програми. Може корегуватися за рішенням кафедри БІТ.

5. Матриця забезпечення результатів навчання компонентам освітньої програми

Складається з двох частин у таблицях:

5.1. Матриця забезпечення результатів навчання обов'язковими компонентами освітньої програми. Може корегуватися за рішенням Вченої ради факультету КБ.

5.2. Матриця забезпечення результатів навчання вибірковими компонентами освітньої програми. Може корегуватися за рішенням кафедри БІТ.

4.1 Матриця відповідності компетентностей обов’язковим компонентам освітньої програми

	ОК1	ОК2	ОК*3	ОК4	ОК5	ОК6	ОК*7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38	ОК39	ОК40
ЗК-1										+		+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК-2								+	+	+		+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+
ЗК-3	+																																							
ЗК-4		+	+																																					
ЗК-5	+	+		+	+			+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК-6				+	+	+				+	+														+															
ЗК-7				+	+						+														+															
ЗК-8				+		+				+																														
СК-1					+																				+												+			+
СК-2														+	+	+	+				+	+	+	+		+			+	+	+	+	+			+	+			+
СК-3																							+													+	+			+
СК-4																							+	+						+			+	+	+	+	+			+
СК-5																							+														+	+	+	+
СК-6																							+							+			+	+	+	+	+			+
СК-7											+												+													+				+
СК-8																				+								+		+			+							+
СК-9																			+															+	+					+
СК-10																							+	+							+	+					+			+

4.2 Матриця відповідності компетентностей варіативним компонентам 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	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29	ВК 30
ЗК-1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК-2	+	+	+				+	+	+	+	+		+	+	+	+	+	+			+	+	+	+	+	+	+			
ЗК-3																														
ЗК-4																														
ЗК-5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК-6											+	+																		
ЗК-7											+																			
ЗК-8																														
СК-1											+	+																		
СК-2	+	+	+	+	+	+		+	+	+			+	+	+	+		+		+	+	+	+				+			
СК-3			+			+			+																					
СК-4	+	+						+	+	+		+			+	+					+	+	+				+			
СК-5			+						+																	+				
СК-6			+			+		+	+		+										+	+		+				+		
СК-7			+								+			+																
СК-8		+										+			+		+		+						+				+	
СК-9					+		+																	+				+		
СК-10	+		+							+			+			+		+		+						+				

5.1 Матриця забезпечення результатів навчання обов’язковими компонентами освітньої програми

	ОК1	ОК2	ОК*3	ОК4	ОК5	ОК6	ОК*7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38	ОК39	ОК40
РН 1	+																																							+
РН 2		+	+																																					+
РН 3				+	+						+																													+
РН 4											+	+		+									+															+	+	+
РН 5				+						+	+	+											+													+	+	+	+	+
РН 6												+		+		+					+																	+	+	+
РН 7													+							+							+	+		+			+							
РН 8								+	+				+																											
РН 9					+																				+												+			+
РН 10														+	+	+	+				+	+	+	+		+			+	+	+	+	+			+	+			+
РН 11																							+													+	+			
РН 12																								+						+			+	+	+	+	+			+
РН 13																							+							+			+	+	+	+	+	+		
РН 14																							+														+	+	+	
РН 15																							+														+	+	+	+
РН 16																							+							+				+	+	+	+	+		
РН 17											+												+													+	+			
РН 18																				+								+		+			+							
РН 19																														+			+							
РН 20																			+															+	+					
РН 21																							+	+							+	+					+			+

5.2 Матриця забезпечення результатів навчання вибірковими компонентами 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	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29	ВК 30
РН 1																														
РН 2																														
РН 3											+																			
РН 4			+			+					+										+	+								
РН 5										+	+										+	+								+
РН 6			+	+		+		+					+							+										
РН 7															+		+		+						+				+	
РН 8																														
РН 9											+	+																		
РН 10	+	+	+	+		+		+	+	+			+	+	+	+		+		+	+	+	+				+			+
РН 11			+			+			+																					+
РН 12	+	+						+	+	+		+			+	+					+	+	+				+			+
РН 13	+	+	+			+		+	+							+					+	+	+				+			+
РН 14			+						+																	+				
РН 15			+							+								+		+						+				
РН 16			+			+		+	+		+										+	+		+				+		
РН 17			+								+			+																
РН 18		+										+			+		+		+						+				+	
РН 19		+													+		+		+											
РН 20					+		+																	+				+		
РН 21	+		+							+			+			+		+		+						+				