МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЯ ПРОГРАМА СИСТЕМИ КІБЕРЗАХИСТУ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

першого (бакалаврського) рівня вищої освіти

(ПРОЄКТ)

Спеціальність **125 Кібербезпека та захист інформації**

Галузь знань **12 Інформаційні технології**

Кваліфікація: **Бакалавр з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Протокол № ___ від _____ 20____ р.
Наказ
Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з 01 вересня 2025 р.

Київ 2024

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬОЇ ПРОГРАМИ

«СИСТЕМИ КІБЕРЗАХИСТУ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ»

ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

спеціальність	125 Кібербезпека та захист інформації
галузь знань	12 Інформаційні технології
рівень вищої освіти	перший (бакалавр)
Кваліфікація	бакалавр з кібербезпеки та захисту інформації

1. Перший проректор _____ Олександр КОРЧЕНКО

2. Проректор з навчальної роботи _____ Артур ГУДМАНЯН

3. В.о. Директор Навчально-методичного центру _____ Вадим ВЛАСЕНКО

4. Вчена рада Навчально-наукового інституту кібербезпеки та захисту інформації

Протокол № ____ від « » _____ 20 р.

Голова Вченої Ради ННІЗІ _____ Євгені ІВАНЧЕНКО

5. Кафедра систем та технологій кібербезпеки

Протокол № ____ від « » _____ 20 р.

Завідувач кафедри систем та технологій кібербезпеки _____ Галина ГАЙДУР

Рецензії від зовнішніх стейкхолдерів:
1.
2.

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи)

Світлана КАЗМІРЧУК – доктор технічних наук, професор, професор кафедри систем та технологій кібербезпеки.

Члени робочої групи:

Галина ГАЙДУР – доктор технічних наук, професор, завідувач кафедри систем та технологій кібербезпеки.;

Сергій ГАХОВ – кандидат військових наук, доцент, доцент кафедри систем та технологій кібербезпеки;

Віталій МАРЧЕНКО – доктор філософії, доцент кафедри систем та технологій кібербезпеки.;

Антоніна КОРЖ – здобувачка кафедри систем та технологій кібербезпеки.

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Розробляється вперше відповідно до наказу №1547 від 29 жовтня 2024 року «Про внесення змін до стандарту вищої освіти зі спеціальності «Кібербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти.

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій, Навчально-науковий інститут кібербезпеки та захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Освітня кваліфікація – *бакалавр з кібербезпеки та захисту інформації*
Офіційна назва освітньої програми	Освітня програма «Системи кіберзахисту та реагування на інциденти»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний: на базі повної загальної середньої освіти. Обсяг освітньої програми-240 кредитів ЄКТС; термін навчання 3 роки та 10 місяців денної форми навчання та 5 років заочної форми навчання). на базі ступеня молодшого бакалавра (освітньо-кваліфікаційного рівня «молодшого спеціаліста») при перезарахуванні не більше 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки.
Наявність акредитації	Сертифікат про акредитацію спеціальності 125 Кібербезпека УД № 11009229 від 18.04.19 р. Термін дії сертифікату 01.07. 2029 р.
Цикл/рівень	НРК України – 6 рівень/ Бакалавр, QF-EHEA- перший цикл, EQF-LLL – 6 рівень
Передумови	Наявність атестата про повну загальну середню освіту або диплома молодшого бакалавра (освітньо-кваліфікаційного рівня «молодший спеціаліст»)
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Програма вводиться в дію з 01.09.2025року. Програма дійсна впродовж дії державних стандартів вищої освіти та може бути відкоригована відповідно до діючих нормативних документів Університету.
Інтернет - адреса постійного розміщення опису освітньої програми	https://duikt.edu.ua/ua/1822-osvitno-profesiyni-programi-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

2 – Мета освітньої програми	
Метою бакалаврської програми є підготовка фахівців здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації, які матимуть здатність розв'язувати складні задачі у галузі кібербезпеки та захисту інформації, з правом подальшої професійної діяльності у державних та комерційних підприємствах та організаціях за спеціальністю.	
3 – Характеристика освітньої програми	
Предметна область, напрям (галузь знань, спеціальність)	12 Інформаційні технології 125 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітня. 100% обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових компетентностей за спеціальністю 125 Кібербезпека та захист інформації визначеного стандартом вищої освіти. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка в галузі кібербезпеки та захисту інформації. Підготовка фахівців здатних використовувати і впроваджувати технології інформаційної та кібернетичної безпеки. Ключові слова: КІБЕРБЕЗПЕКА. ІНФОРМАЦІЯ, КІБЕРЗАХИСТ, ІНЦИДЕНТИ, МЕТОДИ ТА ЗАСОБИ
Опис предметної області	**Об'єкти професійної діяльності випускників**: - технології кібербезпеки та захисту інформації; - процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання** підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст предметної діяльності** Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і

	потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Особливості програми	Програма передбачає: - викладання окремих дисциплін циклу професійної підготовки англійською мовою; - передбачено в межах навчального процесу отримання сертифікатів від провідних компаній в галузі інформаційних технологій; - залучення до проведення практичних занять та лабораторних робіт, фахівців-практиків з кібербезпеки та захисту інформації; - забезпечення умов підготовки здобувачів вищої освіти у реальному середовищі до майбутньої професійної діяльності для набуття відповідних компетенцій, шляхом організації проведення практик (ознайомча, виробнича та переддипломна) в організаціях-партнерів, з можливістю подальшого працевлаштування.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Бакалавр з кібербезпеки та захисту інформації за освітньою програмою «Системи кіберзахисту та реагування на кіберінциденти» (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010: **Основна:** 2139.2 Фахівець з підтримки інфраструктури кіберзахисту Фахівець з реагування на інциденти кібербезпеки
Подальше навчання	Можливість продовжити навчання за освітньою програмою другого (магістерського) освітнього рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.

5 – Викладання та оцінювання	
Викладання та навчання	Проблемно-орієнтоване навчання. Викладання проводиться державною та іноземною (викладання окремих дисциплін проводиться англійською) мовами, які формують професійні компетенції. Викладання спрямовано на засвоєння знань, умінь і навичок для подальшого застосування у практиці. Основними способами передачі змісту освітньої програми є проведення лекцій, семінарських, практичних, індивідуальних, лабораторних занять, консультації, розв'язання ситуаційних задач, тестування, презентації, ознайомча, виробнича, переддипломна практики.
Оцінювання	Оцінювання сформованих компетенцій під час контрольних заходів, які передбачені цією освітньою програмою зазначені у навчальному плані. Критерії оцінювання знань, умінь та навичок розроблені у відповідності до чинного законодавства та висвітлено у положенні про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій.
6- Програмні компетенції	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК6. 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 і Україні. ЗК7. 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 юрмаційної безпеки.
7 – Програмні результати навчання	
	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; РШ7. 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. РШ8. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. РШ9. 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	Група забезпечення спеціальності 125 Кібербезпека та захист інформації сформована із числа науково-педагогічних працівників навчально-наукового інституту кібербезпеки та захисту інформації. Кількісний та якісний склад групи відповідають ліцензійним вимогам.
Матеріально-технічне забезпечення	Теоретичні заняття проводяться в сучасних комп'ютерних класах та спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами. НАВЧАЛЬНА ЛАБОРАТОРІЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: IBM QRadar SIEM, IBM i2 Analyze Notebook Premium, Tenable Nessus Professional, Дозволяє відпрацьовувати навички роботи у Центрі забезпечення кібербезпеки (Security Operation Center) з використанням технологій моніторингу, виявлення, аналізу та реагування на кіберінциденти в корпоративних інформаційних системах. НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК Лабораторія використовується для вивчення спеціалізованих засобів криптографічного захисту. Крім того, у лабораторії проводяться тренінги з використанням криптографічних засобів захисту інформації в інформаційно-комунікаційних системах, віртуальних приватних мереж VPN, електронного цифрового підпису та інфраструктури відкритих ключів. Спеціалізований програмно-апаратний комплекс ESET Protect дозволяє відпрацьовувати навички для захисту кінцевих точок. НАВЧАЛЬНА ЛАБОРАТОРІЯ МЕРЕЖЕВОЇ БЕЗПЕКИ Лабораторія призначена для вивчення технологій мережевої безпеки CISCO та HUAWEI з можливістю проходження сертифікаційних курсів. НАВЧАЛЬНА ЛАБОРАТОРІЯ SECURITY OPERATION CENTER Лабораторія призначена для проведення занять з питань

	аналізу, обробки та аудиту інформаційної безпеки. Крім того, дозволяє вивчати методи управління ризиками на основі методологій CRAMM, OCTAVE та RiskWatch у відповідності до вимог міжнародних стандартів з кібербезпеки та захисту інформації.
Інформаційне та навчально-методичне забезпечення	Інформація про освітню програму, її освітні компоненти та вимоги до осіб, які можуть здобувати вищу освіту за цією програмою розміщена на офіційному сайті Державного університету інформаційно-комунікаційних технологій. Усі освітні компоненти освітньої програми забезпечені навчально-методичними матеріалами, є у вільному доступі у якості ресурсів бібліотеки, системи дистанційного навчання (GWE) університету.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між Державним університетом інформаційно-комунікаційних технологій та закладами вищої освіти України забезпечує національну кредитну мобільність.
Міжнародна кредитна мобільність	Зміст навчання відповідає світовим освітнім стандартам, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	Дозволяє можливість навчання іноземним громадянам.

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

2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

№ п.п.	Дисципліна	Шифр	Компетентність	Результат навчання
1. Цикл дисциплін загальної підготовки				
1.	Вища математика	ЗК11.1.01	ІК, ЗК 5	РН8
2.	Основи кібербезпекки	ЗК11.1.02	ІК, ЗК2, ЗК8	РН6
3.	Фізика	ЗК11.1.03	ІК, ЗК5	РН8
4.	Нормативно-правове забезпечення інформаційної безпеки	ЗК11.1.04	ІК, СК1, ЗК6	РН9
5.	Іноземна мова *	ЗК11.1.05	ІК, ЗК4	РН2
6.	Групова динаміка і комунікації	ЗК11.1.06	ІК, ЗК1, ЗК2, ЗК6, ЗК7	РН3, РН4
7.	Соціально-екологічна безпека життєдіяльності	ЗК11.1.07	ІК, ЗК2, ЗК6, ЗК7, ЗК8	РН3, РН6
8.	Основи інформаційних технологій	ЗК11.1.08	ІК, ЗК2, ЗК8	РН6
9.	Основи телекомунікацій	ЗК11.1.09	ІК, ЗК2, ЗК8	РН6
10.	Теорія інформації та кодування	ЗК11.1.10	ІК, ЗК1, ЗК 8	РН7
11.	Українська мова за професійним спрямуванням	ЗК11.1.11	ІК, ЗК3	РН1
12.	Філософія	ЗК11.1.12	ІК, ЗК3	РН1
13.	Засади відкриття власного бізнесу	ЗК11.1.13	ІК, ЗК1, ЗК2	РН4
2. Цикл дисциплін професійної та практичної підготовки				
1.	Теорія кіл і сигналів в інформаційному та кіберпросторах	ПП11.2.01	ІК, ЗК1, ЗК2, ЗК5, СК9	РН5, РН8, РН20
2.	Прикладне програмування	ПП11.2.02	ІК, ЗК1, ЗК2, ЗК 5	РН5, РН8
3.	Стандарти інформаційної та кібербезпеки	ЗК11.1.03	ІК, ЗК 6, СК1	РН9
4.	Операційні системи	ПП11.2.04	ІК, ЗК2, ЗК8, СК2	РН6, РН10
5.	Захист від шкідливого програмного засобу	ПП11.2.05	ІК, СК2, СК4	РН10, РН12, РН13
6.	Аналіз та оцінка уразливостей інформаційних систем	ПП11.2.06	ІК, СК 10	РН21

7.	Прикладна криптологія	ПП11.2.07	ІК, ЗК1, ЗК8, СК8	РН7, РН18, РН19
8.	Теоретичні основи захищених інформаційно-комунікаційних технологій	ПП11.2.08	ІК, СК2, СК5	РН10, РН14, РН15
9.	SIEM системи	ПП11.2.09	ІК, СК2, СК4	РН10, РН12, РН13
10.	Політики безпеки	ПП11.2.10	ІК, СК3	РН11
11.	Теорія ризиків	ПП11.2.11	ІК, СК7	РН17
12.	Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу	ПП11.2.12	ІК, СК2, СК4	РН10, РН12, РН13
13.	Система менеджменту інформаційної безпеки	ПП11.2.13	ІК, СК3, СК7	РН11, РН17
14.	Основи захисту конфіденційних даних	КФ11.2.14	ІК, СК4	РН12, РН13
15.	Основи безпеки комп'ютерних мереж	ПП11.2.15	ІК, СК2, СК4	РН10, РН12, РН13
16.	Безпека Web-ресурсів	ПП11.2.16	ІК, СК2, СК4	РН10, РН12, РН13
17.	Комплексні системи захисту інформації	ПП11.2.17	ІК, СК6, СК9	РН16, РН20
18.	Штучний інтелект	ПП11.2.18	ІК, ЗК1, ЗК2, СК2	РН5, РН10
19.	Інфраструктура відкритих ключів	ПП11.2.19	ІК, СК2, СК4	РН10, РН12, РН13
20.	Основи реагування на інциденти	ПП11.2.20	ІК, СК2, СК4, СК5	РН10, РН12, РН15
21.	Аудит систем менеджменту інформаційної безпеки	ПП11.2.21	ІК, СК 10	РН21
22.	Цифрова криміналістика	ПП11.2.22	ІК, СК2, СК5	РН10, РН14, РН15
23.	Ознайомча практика	ПП11.2.23	ІК, ЗК1, ЗК2, ЗК6, ЗК8, СК1, СК2	РН4, РН6, РН9, РН10
24.	Виробнича практика	ПП11.2.24	ІК, ЗК1, ЗК2, ЗК6, ЗК7 ЗК8, СК1, СК2, СК4	РН3, РН4, РН6, РН9, РН10, РН12, РН13
25.	Переддипломна практика	ПП11.2.25	ІК, ЗК1, ЗК2, ЗК6, ЗК7, ЗК8, СК1, СК2, СК4, СК5, СК8, СК10	РН3, РН4, РН6, РН9, РН10, РН12, РН13, РН14, РН15, РН18, РН19, РН21
26.	Кваліфікаційна робота	ПП11.2.26	ІК, ЗК1, ЗК2, ЗК 6, ЗК7, ЗК 8, СК2, СК4, СК5, СК8? СК10	РН3, РН4, РН6, РН9,РН10, РН12, РН13, , РН14, РН15, РН18, РН19, РН21
27.	Підсумкова атестація			
3. Дисципліни вільного вибору студента				
1.	Дисципліна вільного вибору студента			
2.	Дисципліна вільного вибору студента			

3.	Дисципліна вільного вибору студента			
4.	Дисципліна вільного вибору студента			
5.	Дисципліна вільного вибору студента			
6.	Дисципліна вільного вибору студента			
7.	Дисципліна вільного вибору студента			
8.	Дисципліна вільного вибору студента			
9.	Дисципліна вільного вибору студента			

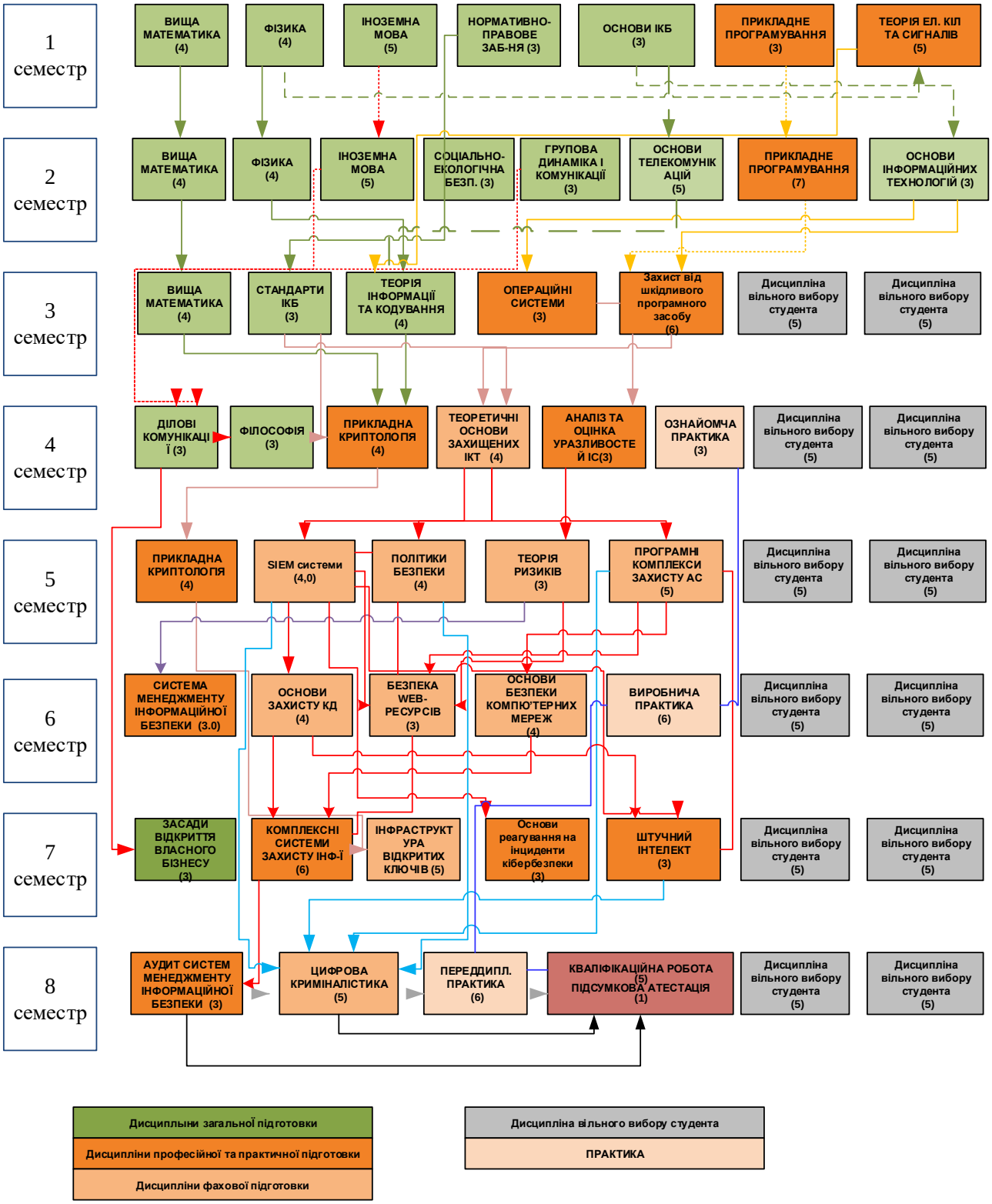
*Іноземна мова у навчальних планах для іноземців та осіб без громадянства замінюється на українську мову (за професійним спрямуванням)

2.2. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ЗК11.1.01	Вища математика	12	Залік, Іспит
ЗК11.1.02	Основи інформаційної та кібернетичної безпеки	3	Залік
ЗК11.1.03	Фізика	7	Залік, Іспит
ЗК11.104	Нормативно-правове забезпечення інформаційної безпеки	3	Іспит
ЗК11.1.05	Іноземна мова	10	Залік, Іспит
ЗК11.1.06	Групова динаміка і комунікації	4	Залік
ЗК11.1.07	Соціально-екологічна безпека життєдіяльності	3	Іспит
ЗК11.1.08	Основи інформаційних технологій	3	Залік
ЗК11.1.09	Основи телекомунікацій	3	Залік
ЗК11.1.10	Теорія інформації та кодування	4	Іспит
ЗК11.1.11	Українська мова за професійним спрямуванням	3	Залік
ЗК11.1.12	Філософія	3	Іспит
ЗК11.1.13	Засади відкриття власного бізнесу	3	Залік
ПП11.2.01	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит
ПП11.2.02	Прикладне програмування	12	Залік, Іспит
ПП11.2.03	Стандарти інформаційної та кібербезпеки	3	Іспит
ПП11.2.04	Операційні системи	3	Залік

ПП11.2.05	Захист від шкідливого програмного засобу	6	Іспит
ПП11.2.06	Аналіз та оцінка уразливостей інформаційних систем	4	Іспит
ПП11.2.07	Прикладна криптологія	8	Залік, Іспит
ПП11.2.08	Теоретичні основи захищених інформаційно-комунікаційних технологій	4	Залік
ПП11.2.09	SIEM системи	4	Іспит
ПП11.2.10	Політики безпеки	3	Іспит
ПП11.2.11	Теорія ризиків	3	Залік
ПП11.2.12	Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу	5	Іспит
ПП11.2.13	Система менеджменту інформаційної безпеки	3	Залік
ПП11.2.14	Основи захисту конфіденційних даних	4	Іспит
ПП11.2.15	Основи безпеки компю’терних мереж	4	Іспит
ПП11.2.16	Безпека Web-ресурсів	3	Іспит
ПП11.2.17	Комплексні системи захисту інформації	6	Іспит
ПП11.2.18	Штучний інтелект	3	Залік
ПП11.2.19	Інфраструктура відкритих ключів	5	Іспит
ПП11.2.20	Основи реагування на інциденти	3	Іспти
ПП11.2.21	Аудит систем менеджменту інформаційної безпеки	3	Іспит
ПП11.2.22	Цифрова криміналістика	5	Іспит
ПП11.2.23	Організаційна практика	3	Залік
ПП11.2.24	Виробнича практика	6	Залік
ПП11.2.25	Переддипломна практика	6	Залік
ПП11.2.26	Кваліфікаційна робота	6	
	Підсумкова атестація		
Загальний обсяг обов’язкових компонент:		**180**	
Вибіркові компоненти ОП			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Дисципліна вільного вибору студента			
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.3. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачити розв'язання спеціалізованої задачі в галузі кібербезпеки та захисту інформації. Має бути перевірено на плагіат відповідно «Положення про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій. Кваліфікаційна робота має бути оприлюднена у репозитарії Державного університету інформаційно-комунікаційних технологій.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ЗК1.1.1.01	ЗК1.1.1.02	ЗК1.1.1.03	ЗК1.1.1.04	ЗК1.1.1.05	ЗК1.1.1.06	ЗК1.1.1.07	ЗК1.1.1.08	ЗК1.1.1.09	ЗК1.1.1.10	ЗК1.1.1.11	ЗК1.1.1.12	ЗК1.1.1.13	ППП1.2.01	ППП1.2.02	ППП1.2.03	ППП1.2.04	ППП1.2.05	ППП1.2.06	ППП1.2.07	ППП1.2.08	ППП1.2.09	ППП1.2.10	ППП1.2.11	ППП1.2.12	ППП1.2.13	ППП1.2.14	ППП1.2.15	ППП1.2.16	ППП1.2.17	ППП1.2.18	ППП1.2.19	ППП1.2.20	ППП1.2.21	ППП1.2.22	ППП1.2.23	ППП1.2.24	ППП1.2.25	ППП1.2.26
ІК	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК1						•				•			•	•	•					•										•					•	•	•	•
ЗК2		•				•	•	•	•				•	•	•		•													•					•	•	•	•
ЗК3											•	•																										
ЗК4					•																																	
ЗК5	•		•											•	•																							
ЗК6				•		•	•									•																				•	•	•	•
ЗК7						•	•																														•	•	•
ЗК8		•					•	•	•	•							•			•																•	•	•	•
СК1				•												•																				•	•	•	
СК2																	•	•			•	•			•			•	•		•	•	•		•	•	•	•	•
СК3																							•			•													
СК4																		•				•			•		•	•	•			•	•			•	•	•	•
СК5																					•												•		•			•	•
СК6																														•									
СК7																								•		•													
СК8																				•																		•	•
СК9														•																•									
СК10																			•															•				•	•

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ЗК1 1.1.01	ЗК1 1.1.02	ЗК1 1.1.03	ЗК1 1.1.04	ЗК1 1.1.05	ЗК1 1.1.06	ЗК1 1.1.07	ЗК1 1.1.08	ЗК1 1.1.09	ЗК1 1.1.10	ЗК1 1.1.11	ЗК1 1.1.12	ЗК1 1.1.13	ППІ 1.2.01	ППІ 1.2.02	ППІ 1.2.03	ППІ 1.2.04	ППІ 1.2.05	ППІ 1.2.06	ППІ 1.2.07	ППІ 1.2.08	ППІ 1.2.09	ППІ 1.2.10	ППІ 1.2.11	ППІ 1.2.12	ППІ 1.2.13	ППІ 1.2.14	ППІ 1.2.15	ППІ 1.2.16	ППІ 1.2.17	ППІ 1.2.18	ППІ 1.2.19	ППІ 1.2.20	ППІ 1.2.21	ППІ 1.2.22	ППІ 1.2.23	ППІ 1.2.24	ППІ 1.2.25	ППІ 1.2.26
РН1											•	•																										
РН2					•																																		
РН3						•	•																													•	•	•
РН4						•							•																							•	•	•	•
РН5														•	•																•								
РН6		•					•	•	•								•																		•	•	•	•
РН7										•										•																			
РН8	•		•											•	•																								
РН9				•												•																				•	•	•	
РН10																	•	•			•	•			•			•	•		•	•	•		•	•	•	•	•
РН11																							•			•													
РН12																		•				•			•		•	•	•			•	•			•	•	•
РН13																		•				•			•		•	•	•			•				•	•	•
РН14																					•													•			•	•
РН15																					•												•	•			•	•
РН16																														•								
РН17																							•		•													
РН18																				•																	•	•
РН19																				•																	•	•
РН20														•																•								
РН21																			•															•			•	•

Гарант освітньої програми
Професор кафедри Систем та технологій кібербезпеки
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій

Доктор технічних наук, професор **Світлана Казмірчук**