

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЯ ПРОГРАМА
«СИСТЕМИ КІБЕРЗАХИСТУ ТА РЕАГУВАННЯ НА
ІНЦИДЕНТИ»
ПРОЄКТ

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 УНІВЕРСИТЕТУ

Протокол № _____ від _____ 2026 р.

Наказ № _____ від _____ 2026 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з 01 вересня 2026 р.

**ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬОЇ ПРОГРАМИ
«СИСТЕМИ КІБЕРЗАХИСТУ ТА РЕАГУВАННЯ НА
ІНЦИДЕНТИ»
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ**

спеціальність	F5 Кібербезпека та захист інформації
галузь знань	F 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. Начальника навчально-методичного відділу _____ Вадим ВЛАСЕНКО

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

Протокол № _____ від « _____ » _____ 20 _____ р.

Голова Вченої Ради ННІКБЗІ _____ Євгенія ІВАНЧЕНКО

5. Кафедра систем та технологій кібербезпеки

Протокол № _____ від « _____ » _____ 20 _____ р.

Завідувач кафедри систем та технологій
кібербезпеки _____ Галина ГАЙДУР

Голова студентської ради ННІКБЗІ _____ Станіслав ШТЕФАН

Рецензії від зовнішніх стейкхолдерів:

1. ТОВ «ЄВРОТЕЛЕКОМ».
2. Київський національний університет ім. Т. Шевченка.

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.

Павло БУЛАВІН – директор ТОВ «ЄВРОТЕЛЕКОМ».

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.

Освітню програму розроблено відповідно до:

наказу Міністерства освіти і науки України від 13.06. 2024 р. № 842;

статті 101 Закону України «Про військовий обов'язок і військову службу» (визначено проводити базову загальновійськову підготовку громадян України у закладах вищої освіти всіх форм власності у порядку, визначеному Кабінетом Міністрів України);

підпункту 7 пункту 2 розділу II Закону України від 11 квітня 2024 року № 3633-IX «Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку» (базова загально-військова підготовка, визначена статтею 101 Закону України «Про військовий обов'язок і військову службу», розпочинається з 1 вересня 2025 року);
Постанови Кабінету Міністрів України від 21 червня 2024 р. № 734 (затверджено Порядок проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських);

пропозицій та побажань стейкхолдерів (здобувачів вищої освіти, науково-педагогічних працівників, випускників, роботодавців, громадської організації) та з урахуванням тенденцій розвитку спеціальності, ринку праці, галузевого контексту, а також досвіду аналогічних вітчизняних та іноземних освітніх програм.

2026 рік

пропозицій та побажань стейкхолдерів (здобувачів вищої освіти, науково-педагогічних працівників, випускників, роботодавців, громадської організації) та з урахуванням тенденцій розвитку спеціальності, ринку праці, галузевого контексту, а також досвіду аналогічних вітчизняних та іноземних освітніх програм.

Затверджено рішенням кафедри систем та технологій кібербезпеки

Протокол № від « » 2026 р.

Введено в дію наказом ректора № __ від _____ 20__ року.

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 – <i>бакалавр з кібербезпеки та захисту інформації</i>
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 4 роки 10 місяців заочної форми навчання. – на базі ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством, при перезарахуванні не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців.
Наявність акредитації	-
Цикл/рівень	НРК України – 6 рівень/ Бакалавр, QF-EHEA- перший цикл, EQF-LLL – 6 рівень
Передумови	Для здобуття освітнього ступеня бакалавра зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, які здобули повну загальну середню освіту. Прийом на основі здобутого ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством.
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Програма вводиться в дію з 01.09.2025 року. 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)	F Інформаційні технології F5 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітня. 100% обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю F5 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 інциденти» (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, практичних, лабораторних занять, консультації, розв'язання ситуаційних задач, тестування, презентації, ознайомча, виробнича, переддипломна практики, теоретична підготовка з базової загальної військової підготовки.
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 і розуміння професійної діяльності ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. 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 та свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК8. 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 впровадженної 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	
	RH1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків, RH2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. RH3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. RH4. 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. RH5. 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. RH6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. RH7. 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. RH8. 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. RH9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. RH10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. RH11. Планувати підготовку та забезпечувати

	неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. RH12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. RH13. 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. RH14. 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. RH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. RH16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах; RH17. 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. RH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. RH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. RH20. 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 F5 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	-

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	OK01	ІК, ЗК 5	РН8
2.	Основи кібербезпеки	OK02	ІК, ЗК2, ЗК8	РН6
3.	Фізика	OK03	ІК, ЗК5	РН8
4.	Нормативно-правове забезпечення інформаційної безпеки	OK04	ІК, СК1, ЗК6	РН9
5.	Іноземна мова *	OK05	ІК, ЗК4	РН2
6.	Комунікації в кібербезпеці та захисті інформації	OK06	ІК, ЗК1, ЗК2, ЗК6, ЗК7	РН3, РН4
7.	Соціально-екологічна безпека життєдіяльності	OK07	ІК, ЗК2, ЗК6, ЗК7, ЗК8	РН3, РН6
8.	Кінцеві пристрої інформаційних систем	OK08	ІК, ЗК2, ЗК8	РН6
9.	Філософія	OK09	ІК, ЗК3	РН1
10.	Теорія інформації та кодування	OK10	ІК, ЗК1, ЗК 8	РН7
11.	Українська мова за професійним спрямуванням	OK11	ІК, ЗК3	РН1
12.	Теоретична підготовка базової загальнонавчальної підготовки	OK12	ІК, ЗК3, ЗК6, ЗК8	РН1, РН3
13.	Бізнес аналітика в кібербезпеці	OK13	ІК, ЗК1, ЗК2	РН4
2. Цикл дисциплін професійної та практичної підготовки				
1.	Теорія кіл і сигналів в інформаційному та кіберпросторах	OK14	ІК, ЗК1, ЗК2, ЗК5, СК9	РН5, РН8, РН20
2.	Прикладне програмування	OK15	ІК, ЗК1, ЗК2, ЗК 5	РН5, РН8
3.	Стандарти кібербезпеки та захисту інформації	OK16	ІК, ЗК 6, СК1	РН9
4.	Операційні системи	OK17	ІК, ЗК2, ЗК8, СК2	РН6, РН10
5.	Захист від шкідливого програмного засобу	OK18	ІК, СК2, СК4	РН10, РН12, РН13
6.	Аналіз та оцінка уразливостей інформаційних систем	OK19	ІК, СК 10	РН21

7.	Прикладна криптологія	OK20	ІК, ЗК1, ЗК8, СК8	PH7, PH18, PH19
8.	Теоретичні основи захищених інформаційно-комунікаційних технологій	OK21	ІК, СК2, СК5	PH10, PH14, PH15
9.	SIEM системи	OK22	ІК, СК2, СК4	PH10, PH12, PH13
10.	Політики безпеки	OK23	ІК, СК3	PH11
11.	Теорія ризиків	OK24	ІК, СК7	PH17
12.	Захист від несанкціонованого доступу	OK25	ІК, СК2, СК4	PH10, PH12, PH13
13.	Система менеджменту інформаційної безпеки	OK26	ІК, СК3, СК7	PH11, PH17
14.	Основи захисту конфіденційних даних	OK27	ІК, СК4	PH12, PH13
15.	Основи безпеки комп'ютерних мереж	OK28	ІК, СК2, СК4	PH10, PH12, PH13
16.	Захист кінцевих точок	OK29	ІК, СК2, СК4	PH10, PH12, PH13
17.	Комплексні системи захисту інформації	OK30	ІК, СК6, СК9	PH16, PH20
18.	Штучний інтелект в кібербезпеці	OK31	ІК, ЗК1, ЗК2, СК2	PH5, PH10
19.	Інфраструктура відкритих ключів	OK32	ІК, СК2, СК4	PH10, PH12, PH13
20.	Основи реагування на кіберінциденти	OK33	ІК, СК2, СК4, СК5	PH2, PH10, PH12, PH15
21.	Аудит систем менеджменту інформаційної безпеки	OK34	ІК, СК 10	PH21
22.	Цифрова криміналістика	OK35	ІК, СК2, СК5	PH10, PH14, PH15
23.	Ознайомча практика	OK36	ІК, ЗК1, ЗК2, ЗК6, ЗК8, СК1, СК2	PH4, PH6, PH9, PH10
24.	Виробнича практика	OK37	ІК, ЗК1, ЗК2, ЗК6, ЗК7, ЗК8, СК1, СК2, СК4	PH3, PH4, PH6, PH9, PH10, PH12, PH13
25.	Переддипломна практика	OK38	ІК, ЗК1, ЗК2, ЗК6, ЗК7, ЗК8, СК1, СК2, СК4, СК5, СК8, СК10	PH3, PH4, PH6, PH9, PH10, PH12, PH13, PH14, PH15, PH18, PH19, PH21
26.	Кваліфікаційна робота	OK39	ІК, ЗК1, ЗК2, ЗК 6, ЗК7, ЗК 8, СК2, СК4, СК5, СК8, СК10	PH3, PH4, PH6, PH9, PH10, PH12, PH13, PH14, PH15, PH18, PH19, PH21

3. Дисципліни вільного вибору студента

1.	Дисципліна вільного вибору студента			
2.	Дисципліна вільного вибору студента			
3.	Дисципліна вільного вибору студента			

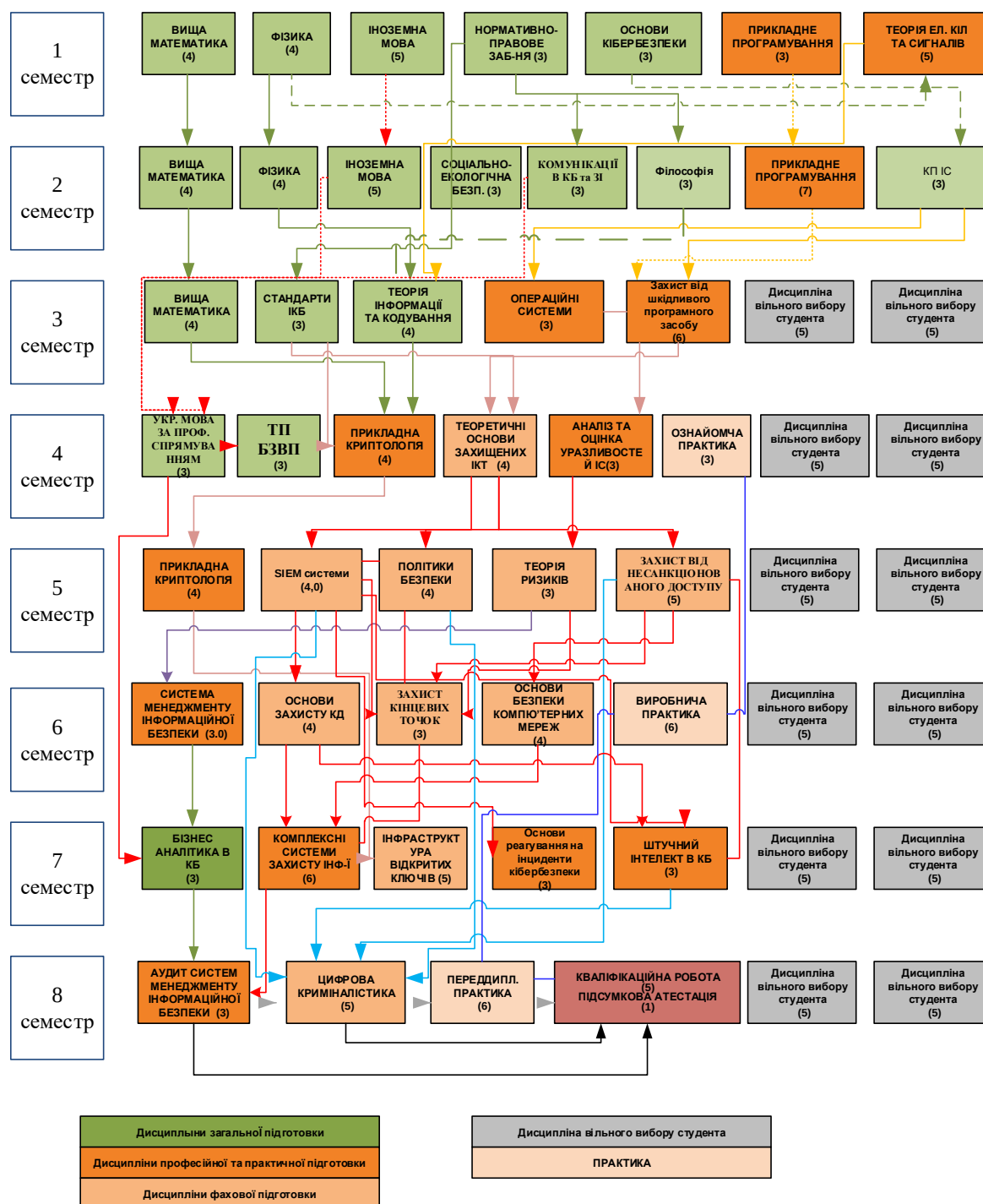
4.	Дисципліна вільного вибору студента			
5.	Дисципліна вільного вибору студента			
6.	Дисципліна вільного вибору студента			
7.	Дисципліна вільного вибору студента			
8.	Дисципліна вільного вибору студента			
9.	Дисципліна вільного вибору студента			

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			
OK01	Вища математика	12	Залік, Іспит
OK02	Основи кібербезпеки	3	Іспит
OK03	Фізика	7	Залік, Іспит
OK04	Нормативно-правове забезпечення інформаційної безпеки	3	Іспит
OK05	Іноземна мова	10	Залік, Іспит
OK06	Комунікації в кібербезпеці та захисті інформації	4	Залік
OK07	Соціально-екологічна безпека життєдіяльності	3	Іспит
OK08	Кінцеві пристрої інформаційних систем	3	Залік
OK09	Філософія	3	Залік
OK10	Теорія інформації та кодування	4	Іспит
OK11	Українська мова за професійним спрямуванням	3	Залік
OK12	Теоретична підготовка базової загальновійськової підготовки	3	Залік
OK13	Бізнес аналітика в кібербезпеці	3	Залік
OK14	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит
OK15	Прикладне програмування	12	Залік, Іспит
OK16	Стандарти кібербезпеки та захисту інформації	3	Іспит
OK17	Операційні системи	3	Залік
OK18	Захист від шкідливого програмного засобу	6	Іспит
OK19	Аналіз та оцінка уразливостей інформаційних систем	4	Іспит
OK20	Прикладна криптологія	8	Залік, Іспит
OK21	Теоретичні основи захищених інформаційно- комунікаційних технологій	4	Залік
OK22	SIEM системи	4	Іспит
OK23	Політики безпеки	3	Іспит

OK24	Теорія ризиків	3	Залік
OK25	Захист від несанкціонованого доступу	5	Іспит
OK26	Система менеджменту інформаційної безпеки	3	Залік
OK27	Основи захисту конфіденційних даних	4	Іспит
OK28	Основи безпеки комп'ютерних мереж	4	Іспит
OK29	Безпека Web-ресурсів	3	Іспит
OK30	Комплексні системи захисту інформації	6	Іспит
OK31	Штучний інтелект в кібербезпеці	3	Залік
OK32	Інфраструктура відкритих ключів	5	Іспит
OK33	Основи реагування на кіберінциденти	3	Іспит
OK34	Аудит систем менеджменту інформаційної безпеки	3	Іспит
OK35	Цифрова криміналістика	5	Іспит
OK36	Організаційна практика	3	Залік
OK37	Виробнича практика	6	Залік
OK38	Переддипломна практика	6	Залік
OK39	Кваліфікаційна робота	6	
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 вибірових компонент:		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

2.3. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

<i>Форми атестації здобувачів вищої освіти</i>	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.
<i>Вимоги до кваліфікаційної роботи</i>	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

		OK01	OK02	OK03	OK04	OK05	OK06	OK07	OK08	OK09	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OK37	OK38	OK39		
IK		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	
3K1							•				•			•	•	•					•											•					•	•	•	•	•	
3K2			•				•	•	•					•	•	•		•														•					•	•	•	•	•	
3K3										•		•	•																													
3K4					•																																					
3K5	•		•												•	•																										
3K6				•			•	•					•				•																					•	•	•	•	
3K7							•	•																															•	•	•	•
3K8		•						•	•		•		•					•			•																•	•	•	•	•	
CK1				•													•					•	•				•		•	•						•	•	•	•	•	•	
CK2																		•	•			•	•				•			•	•			•	•	•	•	•	•	•	•	
CK3																								•			•						•	•			•	•	•	•	•	
CK4																			•				•				•		•	•				•	•			•	•	•	•	
CK5																					•						•		•	•						•			•	•	•	
CK6																																•										
CK7																									•		•															
CK8																					•						•												•	•		
CK9															•							•									•								•	•		
CK10																				•														•					•	•		

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

	OK01	OK02	OK03	OK04	OK05	OK06	OK07	OK08	OK09	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OK37	OK38	OK39
PH1																																							
PH2																																							
PH3																																							
PH4																																							
PH5																																							
PH6																																							
PH7																																							
PH8																																							
PH9																																							
PH10																																							
PH11																																							
PH12																																							
PH13																																							
PH14																																							
PH15																																							
PH16																																							
PH17																																							
PH18																																							
PH19																																							
PH20																																							
PH21																																							

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