МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЯ ПРОГРАМА «СИСТЕМИ КІБЕРЗАХИСТУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ»

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 № 3 від 17 березня 2026 р.
Наказ № 105 від 20 березня 2026 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з 01 вересня 2026 р.

Київ 2026

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. Начальник навчально-методичного відділу _____ Вадим ВЛАСЕНКО
4. Вчена рада Навчально-наукового інституту кібербезпеки та захисту інформації

Протокол № 8 від «26» лютого 2026 р.

Голова Вченої Ради ННІКБЗІ _____ Євгенія ІВАНЧЕНКО

5. Кафедра систем та технологій кібербезпеки

Протокол № 7/1 від «25» лютого 2026р.

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;

Марина БОЙКО – 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 стейкголдерів (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 стейкголдерів (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 – *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 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 01.09.2026 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. СКЗ. 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 си стем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах; РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами,

	проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
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	ОК01	ІК, ЗК 5	РН8
2.	Фізика	ОК02	ІК, ЗК5	РН8
3.	Англійська мова для професійної комунікації*	ОК03	ІК, ЗК4	РН2
4.	Англійська мова: комунікативний практикум*	ОК04	ІК, ЗК4	РН2
5.	Соціально-екологічна безпека життєдіяльності	ОК05	ІК, ЗК2, ЗК6, ЗК7, ЗК8	РН3, РН6
6.	Кінцеві пристрої інформаційних систем	ОК06	ІК, ЗК2, ЗК8	РН6
7.	Філософія	ОК07	ІК, ЗК3	РН1
8.	Українська мова за професійним спрямуванням	ОК8	ІК, ЗК3	РН1
9.	Теоретична підготовка базової загальновійськової підготовки	ОК9	ІК, ЗК3, ЗК6, ЗК8	РН1, РН3
10.	Бізнес аналітика в кібербезпеці	ОК10	ІК, ЗК1, ЗК2	РН4
2. Цикл дисциплін професійної та практичної підготовки				
1.	Основи кібербезпеки	ОК11	ІК, ЗК2, ЗК8	РН6
2.	Нормативно-правове забезпечення інформаційної безпеки	ОК12	ІК, СК1, ЗК6	РН9
3.	Комунікації в кібербезпеці та захисті інформації	ОК13	ІК, ЗК1, ЗК2, ЗК6, ЗК7	РН3, РН4
4.	Теорія кіл і сигналів в інформаційному та кіберпросторах	ОК14	ІК, ЗК1, ЗК2, ЗК5, СК9	РН5, РН8, РН20
5.	Прикладне програмування	ОК15	ІК, ЗК1, ЗК2, ЗК 5	РН5, РН8
6.	Стандарти кібербезпеки та захисту інформації	ОК16	ІК, ЗК 6, СК1	РН9

7.	Теорія інформації та кодування	ОК17	ІК, ЗК1, ЗК 8	РН7
8.	Захист від шкідливого програмного засобу	ОК18	ІК, СК2, СК4	РН10, РН12, РН13
9.	Аналіз та оцінка уразливостей інформаційних систем	ОК19	ІК, СК 10	РН21
10.	Прикладна криптологія	ОК20	ІК, ЗК1, ЗК8, СК8	РН7, РН18, РН19
11.	Теоретичні основи захищених інформаційно-комунікаційних технологій	ОК21	ІК, СК2, СК5	РН10, РН14, РН15
12.	SIEM системи	ОК22	ІК, СК2, СК4	РН10, РН12, РН13
13.	Політики безпеки	ОК23	ІК, СК3	РН11
14.	Теорія ризиків	ОК24	ІК, СК7	РН17
15.	Захист від несанкціонованого доступу	ОК25	ІК, СК2, СК4	РН10, РН12, РН13
16.	Система менеджменту інформаційної безпеки	ОК26	ІК, СК3, СК7	РН11, РН17
17.	Основи захисту конфіденційних даних	ОК27	ІК, СК4	РН12, РН13
18.	Основи безпеки комп'ютерних мереж	ОК28	ІК, СК2, СК4	РН10, РН12, РН13
19.	Захист кінцевих точок	ОК29	ІК, СК2, СК4	РН10, РН12, РН13
20.	Профілі безпки	ОК30	ІК, СК6, СК9	РН16, РН20
21.	Штучний інтелект в кібербезпеці	ОК31	ІК, ЗК1, ЗК2, СК2	РН5, РН10
22.	Інфраструктура відкритих ключів	ОК32	ІК, СК2, СК4	РН10, РН12, РН13
23.	Основи реагування на інциденти	ОК33	ІК, СК2, СК4, СК5	РН10, РН12, РН15
24.	Аудит систем менеджменту інформаційної безпеки	ОК34	ІК, СК 10	РН21
25.	Цифрова криміналістика	ОК35	ІК, СК2, СК5	РН10, РН14, РН15
26.	Ознайомча практика	ОК36	ІК, ЗК1, ЗК2, ЗК6, ЗК8, СК1, СК2	РН4, РН6, РН9, РН10
27.	Виробнича практика	ОК37	ІК, ЗК1, ЗК2, ЗК6, ЗК7 ЗК8, СК1, СК2, СК4	РН3, РН4, РН6, РН9, РН10, РН12, РН13
28.	Переддипломна практика	ОК38	ІК, ЗК1, ЗК2, ЗК6, ЗК7, ЗК8, СК1, СК2, СК4, СК5, СК8, СК10	РН3, РН4, РН6, РН9, РН10, РН12, РН13, РН14, РН15, РН18, РН19, РН21
29.	Кваліфікаційна робота	ОК39	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

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			

*Англійська 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			
ОК01	Вища математика	12	Залік, Залік, Іспит
ОК02	Фізика	8	Залік, Іспит
ОК03	Англійська мова для професійної комунікації	12	Залік, Іспит
ОК04	Англійська мова: комунікативний практикум	4	Залік, Іспит
ОК05	Соціально-екологічна безпека життєдіяльності	3	Залік
ОК06	Кінцеві пристрої інформаційних систем	4	Іспит
ОК07	Філософія	3	Залік
ОК8	Українська мова за професійним спрямуванням **	3	Залік
ОК9	Теоретична підготовка базової загальновійськової підготовки *	3	Залік
ОК10	Бізнес аналітика в кібербезпеці	3	Залік
ОК11	Основи кібербезпеки	3	Іспит
ОК12	Нормативно-правове забезпечення інформаційної безпеки	3	Іспит
ОК13	Комунікації в кібербезпеці та захисті інформації	4	Залік
ОК14	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит
ОК15	Прикладне програмування	12	Залік, Іспит
ОК16	Стандарти кібербезпеки та захисту інформації**	3	Іспит
ОК17	Теорія інформації та кодування***	4	Іспит

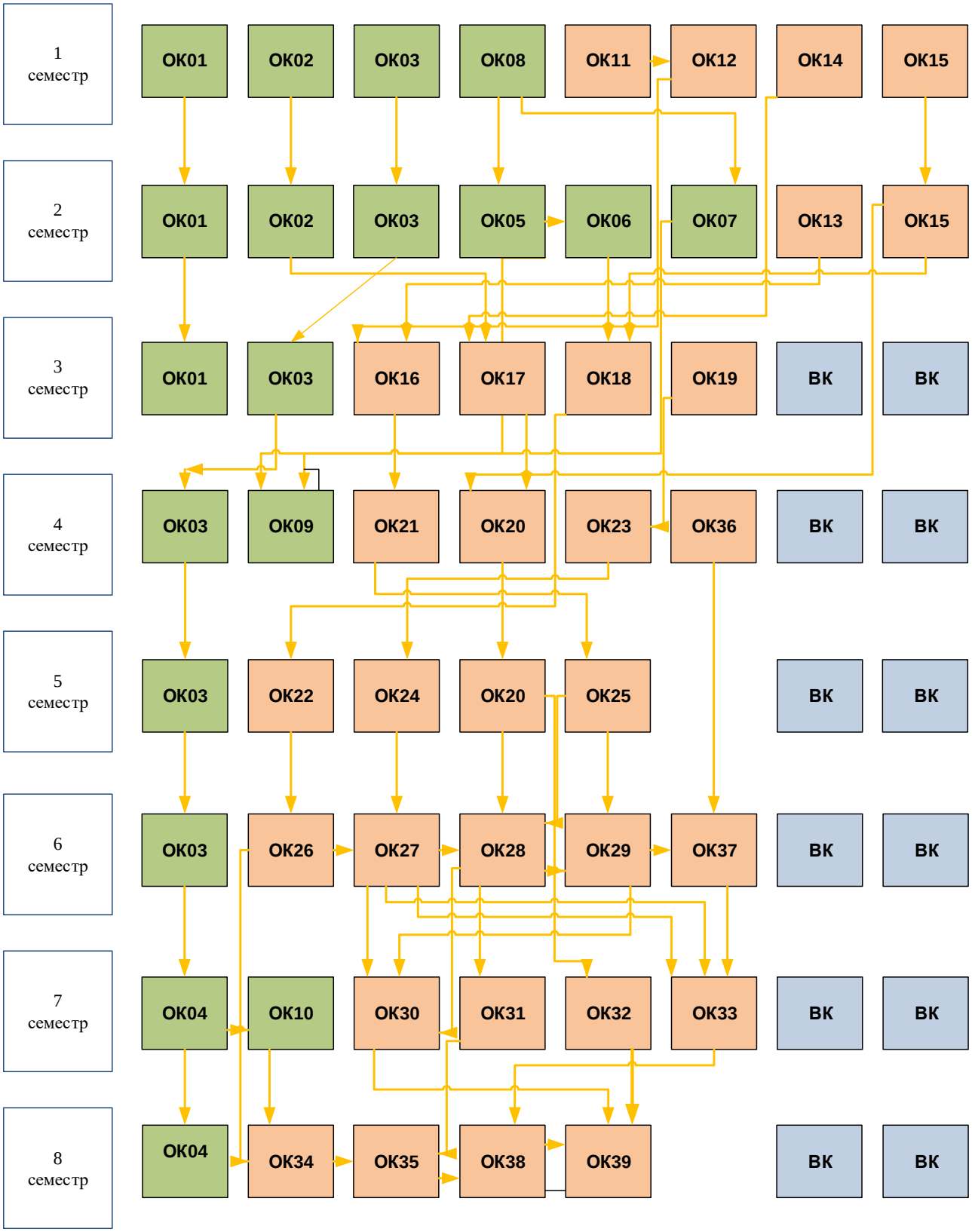
ОК18	Захист від шкідливого програмного засобу	4	Іспит
ОК19	Аналіз та оцінка уразливостей інформаційних систем	3	Залік
ОК20	Прикладна криптологія	10	Залік, Іспит
ОК21	Теоретичні основи захищених інформаційно-комунікаційних технологій	4	Залік
ОК22	SIEM системи	5	Іспит
ОК23	Політики безпеки	3	Іспит
ОК24	Теорія ризиків	3	Залік
ОК25	Захист від несанкціонованого доступу	5	Іспит
ОК26	Система менеджменту інформаційної безпеки	3	Залік
ОК27	Основи захисту конфіденційних даних	3	Іспит
ОК28	Основи безпеки компю’терних мереж	3	Іспит
ОК29	Захист кінцевих точок	3	Іспит
ОК30	Профілі безпки	5	Іспит
ОК31	Штучний інтелект в кібербезпеці	3	Залік
ОК32	Інфраструктура відкритих ключів	4	Іспит
ОК33	Основи реагування на інциденти	3	Іспти
ОК34	Аудит систем менеджменту інформаційної безпеки	3	Іспит
ОК35	Цифрова криміналістика	3	Іспит
ОК36	Організаційна практика	3	Залік
ОК37	Виробнича практика	6	Залік
ОК38	Переддипломна практика	6	Залік
ОК39	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 вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

* Для денної форми навчання

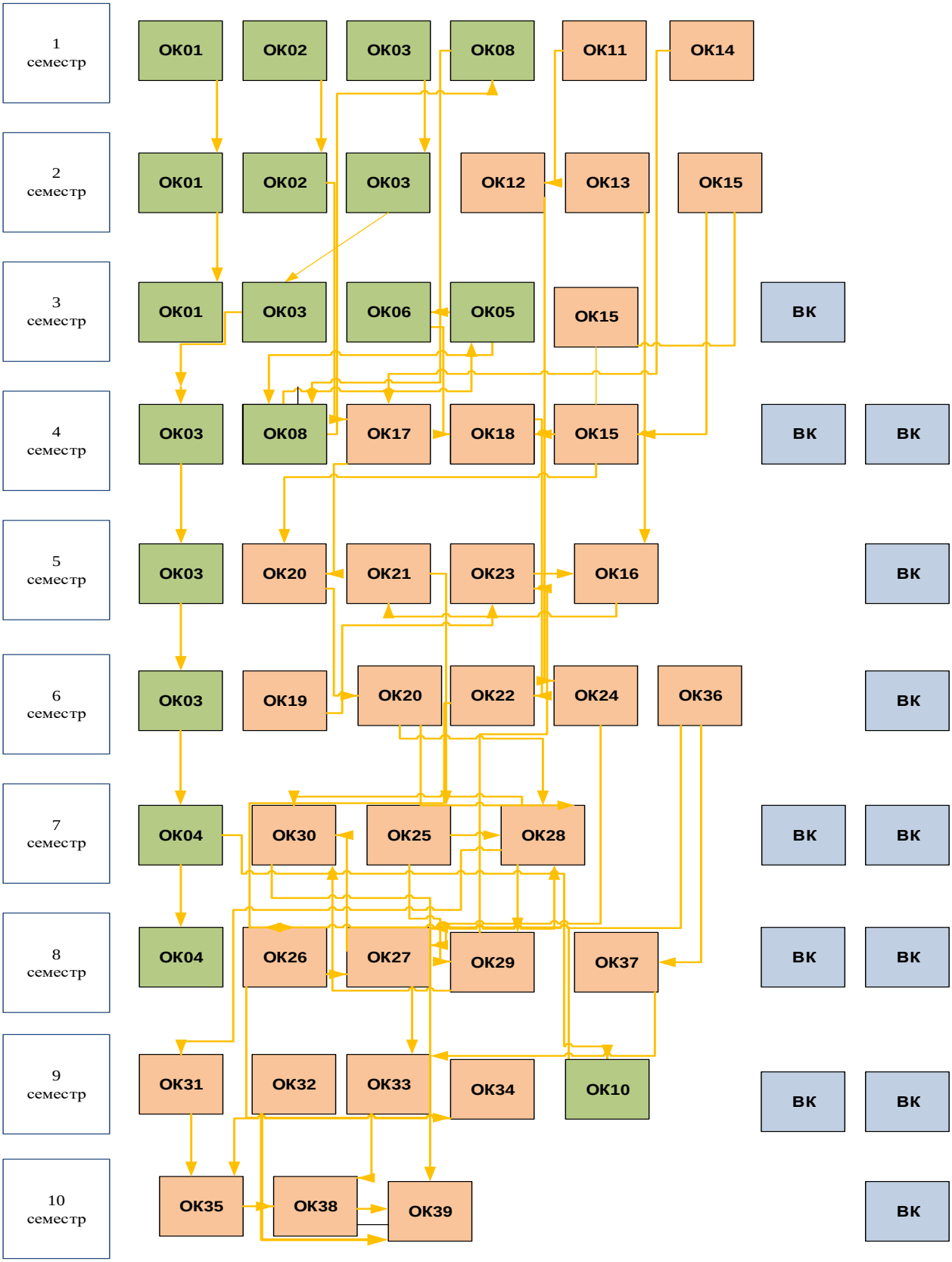
**Для заочної форми навчання обсяг кредитів – 4 ECTS

*** Для заочної форми навчання обсяг кредитів – 5 ECTS

2.3. Структурно-логічна схема ОП



Заочна


1 семестр
ОК01
ОК02
ОК03
ОК08
ОК11
ОК14
2 семестр
ОК01
ОК02
ОК03
ОК12
ОК13
ОК15
3 семестр
ОК01
ОК03
ОК06
ОК05
ОК15
ВК
4 семестр
ОК03
ОК08
ОК17
ОК18
ОК15
ВК
ВК
5 семестр
ОК03
ОК20
ОК21
ОК23
ОК16
ВК
6 семестр
ОК03
ОК19
ОК20
ОК22
ОК24
ОК36
ВК
7 семестр
ОК04
ОК30
ОК25
ОК28
ВК
ВК
8 семестр
ОК04
ОК26
ОК27
ОК29
ОК37
ВК
ВК
9 семестр
ОК31
ОК32
ОК33
ОК34
ОК10
ВК
ВК
10 семестр
ОК35
ОК38
ОК39
ВК

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

	ОК01	ОК02	ОК03	ОК04	ОК05	ОК06	ОК07	ОК08	ОК09	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
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

	ОК01	ОК02	ОК03	ОК04	ОК05	ОК06	ОК07	ОК08	ОК09	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
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**

РЕЦЕНЗІЯ
на освітню програму
«СИСТЕМИ КІБЕРЗАХИСТУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 Кібербезпека та захист інформації

Освітньо-професійна програма «Системи кіберзахисту та реагування на інциденти» спрямована на підготовку фахівців, здатних здійснювати моніторинг подій безпеки, аналіз кіберінцидентів та забезпечувати функціонування систем кіберзахисту інформаційно-комунікаційних систем.

Мета, інтегральні, загальні та фахові компетентності програми є узгодженими та забезпечують досягнення визначених програмних результатів навчання. Простежується відповідність між освітніми компонентами, компетентностями та результатами навчання, що свідчить про системний підхід до проєктування освітнього процесу.

Структура освітньої програми поєднує фундаментальну підготовку з професійно орієнтованими дисциплінами, зокрема у сферах мережевих технологій, аналізу кіберзагроз, цифрової криміналістики, моніторингу подій безпеки та реагування на інциденти. Значна увага приділяється формуванню практичних навичок роботи з журналами подій, мережевим трафіком, системами виявлення атак та управління інцидентами інформаційної безпеки.

Позитивною особливістю програми є орієнтація на практичну підготовку, що реалізується через лабораторні роботи, практичні заняття та навчальні кейси, наближені до реальних умов функціонування центрів моніторингу безпеки (SOC). Це сприяє формуванню здатності здобувачів приймати обґрунтовані рішення під час аналізу та локалізації кіберінцидентів.

Освітня програма відповідає стандарту вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації», узгоджується з сучасними тенденціями розвитку галузі та може бути співвіднесена з аналогічними освітніми програмами європейського простору вищої освіти.

Передбачені форми контролю та атестації забезпечують об'єктивне оцінювання досягнення результатів навчання, а зміст програми створює передумови для подальшого навчання на другому рівні вищої освіти.

Освітньо-професійна програма «Системи кіберзахисту та реагування на інциденти» є актуальною, методично обґрунтованою та відповідає вимогам підготовки бакалаврів у сфері кібербезпеки. Програма рекомендується до впровадження в освітній процес.

РЕЦЕНЗЕНТ
Професор кафедри кібербезпеки та захисту інформації
факультету інформаційних технологій Київського національного
університету імені Тараса Шевченка
доктор технічних наук, професор Сергій ТОЛЮПА

Підпис професора Сергія ТОЛЮПИ засвідчую.
Заступник декана з навчально-виховної роботи
кандидат фізико - математичних наук, доцент Наталія ТМЄНОВА

eurotelecom

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ЄВРОТЕЛЕКОМ» 34837389

+38 099 915-915 9
office@etele.com.ua

03151, Україна, м.Київ, вул.Волинська, буд.10

Рецензія
на освітню програму
«Системи кіберзахисту та реагування на інциденти»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 Кібербезпека та захист інформації

Стрімкий розвиток сучасних інформаційних технологій у цифровому середовищі обумовлює постійне зростання ролі кібербезпеки та захисту інформації в діяльності організацій усіх форм власності. У зв'язку з цим підготовка фахівців, здатних протидіяти кіберзагрозам, є актуальним і стратегічно важливим завданням системи вищої освіти.

Освітня програма «Інформаційна та кібернетична безпека» охоплює комплекс ключових питань у сфері кіберзахисту, зокрема: виявлення та реагування на шкідливе програмне забезпечення, протидію кібератакам, криптографічний захист інформації, безпеку комп'ютерних мереж та інші сучасні напрями захисту інформаційних систем. Це підтверджує її актуальність для підготовки фахівців, здатних запобігати, виявляти та нейтралізувати сучасні кіберзагрози.

У програмі чітко визначено предметну область, мету навчання та теоретичний зміст професійної діяльності, що полягає у застосуванні технологій кібербезпеки для захисту кіберпростору та інформаційних ресурсів. Структура освітньої програми є логічною та збалансованою, містить обов'язкові та вибіркові освітні компоненти, взаємозв'язок яких відображено у структурно-логічній схемі.

Освітня програма відповідає стандарту вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації» та враховує сучасні потреби ринку праці, що забезпечується формуванням загальних і фахових компетентностей у межах дисциплін професійної та практичної підготовки.

Вагомою перевагою програми є наявність сучасного матеріально-технічного забезпечення, зокрема навчальних лабораторій:

- мережевої безпеки,
- реагування на інциденти,
- захисту кінцевих точок.

Зазначена лабораторна база дозволяє сформувати практичні навички та досягти визначених результатів навчання відповідно до вимог професійної діяльності у сфері кібербезпеки.

Здобуті компетентності надають можливість випускникам виконувати професійну діяльність відповідно до Державного класифікатора професій, зокрема на посадах:

- «Фахівець з підтримки інфраструктури кіберзахисту»,
- «Фахівець з реагування на інциденти кібербезпеки»,
- «Молодший адміністратор мереж і систем».

Таким чином, освітня програма забезпечує підготовку фахівців, здатних впроваджувати та ефективно використовувати технології кібербезпеки для захисту інформаційних систем сучасних організацій.

Оновлена освітньо-професійна програма «Інформаційна та кібернетична безпека» спеціальності F5 «Системи кіберзахисту та реагування на інциденти» галузі знань F «Інформаційні технології» є актуальною, якісною та відповідає сучасним вимогам підготовки фахівців. Програма рекомендується до використання в освітньому процесі для підготовки здобувачів вищої освіти першого (бакалаврського) рівня.

Директор ТОВ «ЄВРОТЕЛЕКОМ» **Павло БУЛАВІН**