МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЯ ПРОГРАМА

“УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ”

першого (бакалаврського) рівня вищої освіти
(оновлена)

Спеціальність	**F5 Кібербезпека та захист інформації**
Галузь знань	**F Інформаційні технології**
Кваліфікація:	**Бакалавр з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ УНІВЕРСИТЕТУ

Протокол № 7 від 08 вересня 2026 р.
Наказ № 384 від 08 вересня 2026 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з 01 жовтня 2026 р.

Київ – 2026

ЛИСТ ПОГОДЖЕННЯ

ОСВІТНЬОЇ ПРОГРАМИ
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

галузь знань	F “Інформаційні технології”
спеціальність	F5 “Кібербезпека та захист інформації”
рівень вищої освіти	перший (бакалаврський)
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 № 1 від “02“ вересня 2026 р.

Голова Вченої Ради ННІКБЗІ _____ Євгенія ІВАНЧЕНКО

5. Кафедра управління кібербезпекою та захистом інформації

Протокол № 1 від “01“ вересня 2026 р.

Завідувач кафедри
управління кібербезпекою
та захистом інформації _____ Світлана ЛЕГОМІНОВА

6. Голова студентської ради ННІКБЗІ _____ Станіслав ШТЕФАН

Рецензії від зовнішніх стейкхолдерів (компаній-партнерів):

1. Товариство з обмеженою відповідальністю “ІТ спеціаліст”;
2. ДП “ЕС ЕНД ТІ Україна”

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми (голова робочої групи) –
Тетяна МУЖАНОВА - кандидат наук з державного управління, доцент, доцент кафедри управління кібербезпекою та захистом інформації;

Члени робочої групи:
Світлана ЛЕГОМІНОВА - доктор економічних наук, професор, завідувач кафедри управління кібербезпекою та захистом інформації;
Віталій САВЧЕНКО - доктор технічних наук, професор, професор кафедри управління кібербезпекою та захистом інформації;
Дмитро РАБЧУН - кандидат технічних наук, доцент кафедри управління кібербезпекою та захистом інформації.
Діана ПРИМАЧЕНКО – здобувачка вищої освіти третього (освітньо-наукового) рівня спеціальності 125 "Кібербезпека та захист інформації";
Олександр СКРИПКА – здобувач вищої освіти другого рівня спеціальності F5 "Кібербезпека та захист інформації";
Олексій МОРОЗОВ – директор ТОВ "ІТ Спеціаліст";
Юрій ЛИСЕЦЬКИЙ – директор ДП "ЕС ЕНД ТІ Україна";

.

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Оновлено 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.
Оновлення освітньої програми 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);
зі змінами до Закону України «Про основи національного спротиву» та наказу Міністерства освіти та науки України від 30.06.2026 №1002 «Про затвердження Типової програми навчальної дисципліни «Основи національного спротиву»»;
з врахуванням 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 Управління кібербезпекою та захистом інформації

протокол № 1 від «01» вересня 2026 р.

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 – Управління інформаційною та кібернетичною безпекою
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 здобутих освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців.
Наявність акредитації	Вводиться з 1 вересня 2025 (акредитована) Сертифікат про акредитацію освітньої програми Управління інформаційною та кібернетичною безпекою спеціальності F5 Кібербезпека УД №11008702 від 18.04.2019 Термін дії сертифікату до 1.07.2029 року.
Цикл/рівень	НРК України – 6 рівень/ Бакалавр, QF-EHEA- перший цикл, EQF-LLL – 6 рівень
Передумови	Наявність атестата про повну загальну середню освіту або диплому молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста).
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Програму планується ввести в дію 01 жовтня 2026 року та може бути відкориговано відповідно до “Положення про запровадження та оновлення освітніх програм у Державному університеті інформаційно-комунікаційних

	технологій”
Інтернет - адреса постійного розміщення опису освітньої програми	https://duikt.edu.ua/ua/1826-osvitno-profesiyni-programi-kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu
2 – Мета освітньої програми	
Метою бакалаврської програми є формування та розвиток загальних і професійних компетентностей у фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації, а саме фокусуючись на управлінні кібербезпекою з правом подальшої професійної діяльності у державних та приватних підприємствах, організаціях, що сприятиме стійкому соціальному розвиткові інформаційного суспільства та нейтралізації реальних й потенційних загроз національній безпеці України у кіберпросторі.	
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, предметних) компетентностей за спеціальністю F5 Кібербезпека та захист інформації, визначеного стандартом вищої освіти. Програма носить прикладний характер, спрямована на забезпечення потреб ринку праці, зокрема в ІТ галузі.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка в галузі інформаційних технологій. – Підготовка фахівців здатних використовувати і впроваджувати: технології кібербезпеки та захисту інформації на підприємствах, організаціях; процеси управління кібербезпекою та захистом інформації об’єктів інформаційної діяльності, об’єктів критичної інфраструктури, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Ключові слова: КІБЕРБЕЗПЕКА, УПРАВЛІННЯ, ІНФОРМАЦІЯ, РИЗИКИ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ІНЦИДЕНТИ, ЗАХИСТ .
Опис предметної області	Програма передбачає викладання освітніх компонент спеціалістами з кібербезпеки та її інформаційно-аналітичного забезпечення, що суттєво поглиблює спеціальні, фахові, предметні компетентності майбутніх фахівців. Передбачено проведення лекційних курсів,

	семінарських та практичних, лабораторних занять з залученням фахівців-практиків з кібербезпеки. **Об'єкти вивчення**: - 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. **Теоретичний зміст предметної області:** Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання Кіберпростору, за якого забезпечуються стійкий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** Методи, методики та технології розв'язання теоретичних та практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** Засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проєктування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Працевлаштування випускників	На посади у структурних підрозділах установ / підприємств / організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації.
Особливості програми	Програма передбачає: - викладання компонент циклу професійної підготовки англійською мовою; - отримання в межах навчального процесу сертифікатів від провідних компаній у галузі інформаційних технологій; - залучення до проведення семінарських, практичних та лабораторних занять фахівців-практиків з інформаційної та кібербезпеки; - забезпечення умов підготовки здобувачів вищої освіти у реальному середовищі майбутньої професійної

	діяльності для набуття відповідних компетентностей шляхом організації проведення практик (ознайомча, виробнича та переддипломна) у організаціях і компаніях 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 Управління кібербезпекою та захистом інформації, здатний виконувати професійні роботи за Національним класифікатором професій ДК 003: 2010: **Основна:** 2139.2 – Фахівець сфери захисту інформації; 2139.2 – Фахівець з питань безпеки (інформаційно-комунікаційні технології); 2139.2 – Аудитор інформаційних технологій (з кібербезпеки). **Додаткова**: 2139.2 – Фахівець з оцінки заходів захисту інформації (кібербезпеки).
Академічні права випускників	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання і викладання. Викладання проводиться державною мовою. Іноземною мовою (англійською) проводяться викладання окремих дисциплін, які формують професійні компетентності. Викладання спрямовано на засвоєння знань, умінь і навичок для подальшого застосування у практиці. Основними способами передачі змісту освітньої програми є проведення лекцій, практичних, лабораторних, семінарських та індивідуальних занять, консультацій, розв'язання ситуаційних задач, тестування, презентації, ознайомча, виробнича, переддипломна практика.
Оцінювання	Види контролю: поточний, рубіжний (модульний, тематичний) та підсумковий контроль. Оцінювання сформованих компетентностей проводиться під час контрольних заходів, які передбачені цією освітньою програмою та зазначені у навчальному плані. Критерії

	оцінювання знань, умінь та навичок здобувачів вищої освіти розроблені у відповідності до чинного законодавства та затверджені у «Положенні про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій». Також, з метою отримання додаткових балів в межах дисциплін зараховуються здобуті студентами сертифікати відомих компаній за тематикою дисциплін.
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 и діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК 8.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальні (фахові, предметні) компетентності (КФ)	**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 із встановленою політикою інформаційної 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. **РН 8.** Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. **РН9.** Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. **РН10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. **РН11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. **РН12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. **РН13.** Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому. **РН14.** Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати

	функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. **РН15.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. **РН16.** Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. **РН17.** Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. **РН18.** Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **РН19.** Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. **РН20.** Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. **РН21.** Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Усі науково-педагогічні працівники, залучені до реалізації освітньої складової освітньо-професійної програми є штатними співробітниками Державного університету інформаційно-комунікаційних технологій, мають підтверджений рівень наукової і професійної активності. Група забезпечення освітньо-професійної програми сформована з числа науково-

	педагогічних працівників Державного університету інформаційно-комунікаційних технологій. Кількісний та якісний склад групи відповідають Ліцензійним вимогам.
Матеріально-технічне забезпечення	Для проведення практичних та лабораторних занять з метою формування спеціальних компетентностей зі спеціальності F5 Кібербезпека та захист інформації освітньої програми Управління інформаційною та кібернетичною безпекою використовуються спеціалізовані лабораторії Державного університету інформаційно-комунікаційних технологій, які оснащені сучасними комп'ютерами та програмно-апаратними комплексами. НАВЧАЛЬНА ЛАБОРАТОРІЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: USM/SIEM від компанії-вендора AlienVault, IBM QRadar SIEM, IBM i2 Analyze Notebook Premium, Tenable Nessus Professional. Лабораторія 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 МЕРЕЖЕВОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ CISCO Лабораторія призначена для вивчення технологій мережевої безпеки CISCO, проведення тренінгів із впровадження технології HoneyPot щодо протидії кібератакам на корпоративні інформаційні системи та сертифікаційних курсів від партнера кафедри інформаційної та кібернетичної безпеки – компанії CISCO: Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations. Лабораторія створена за сприяння компанії CISCO. НАВЧАЛЬНА ЛАБОРАТОРІЯ SECURITY OPERATION CENTER Лабораторія призначена для проведення практичних занять з питань аналізу, обробки та аудиту інформаційної безпеки та/або кібербезпеки за допомогою SIEM систем і програмних сканерів типу Nessus та Kali Linux. Крім того, на базі лабораторії вивчаються методи управління ризиками на основі

	методологій CRAMM, OCTAVE та RiskWatch відповідно до вимог міжнародних стандартів з інформаційної безпеки та/або кібербезпеки.
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 в якості ресурсів бібліотеки, електронної бібліотеки Державного університету інформаційно-комунікаційних технологій й системи управління навчанням Google Classroom.
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між ДУІКТ та закладами вищої освіти України забезпечує національну кредитну мобільність.
Міжнародна кредитна мобільність	Зміст навчання відповідає світовим освітнім стандартам, що дозволяє здобувачам брати участь у програмах подвійних дипломів і бути конкурентоспроможними на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	Надається можливість навчання іноземним громадянам.

2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

№ п.п.	Компонента	Шифр	Компетентність	Результат навчання
1. Цикл компонент загальної підготовки				
1.	Вища математика	ОК1	ІК, ЗК5	РН8
2.	Основи управління інформаційною та кібербезпекою	ОК2	ІК, ЗК6, СК1, СК2, СК3	РН9, РН10, РН11
3.	Бізнес аналітика в кібербезпеці	ОК3	ІК, ЗК1, ЗК2	РН4
4.	Філософія	ОК4	ІК, ЗК3	РН1
5.	Українська мова за професійним спрямуванням	ОК5	ІК, ЗК3	РН1
6.	Соціально-екологічна безпека життєдіяльності	ОК6	ІК, ЗК2, ЗК6, ЗК7, ЗК8	РН3, РН6
7.	Фізика	ОК7	ІК, ЗК8	РН8
8.	Кінцеві пристрої інформаційних систем	ОК8	ІК, ЗК 2, ЗК8	РН2, РН6
9.	Основи національного спротиву	ОК9	ІК, ЗК6, ЗК8	РН3, РН6, РН9
10.	Англійська мова для професійної комунікації	ОК10	ІК, ЗК4	РН2
11.	Англійська мова: комунікативний практикум	ОК11	ІК, ЗК4	РН2
2. Цикл компонент професійної та практичної підготовки				
1.	Теорія інформації та кодування	ОК12	ІК, ЗК1, ЗК8	РН7
2.	Комунікації в кібербезпеці та захисті інформації	ОК13	ІК, ЗК1, ЗК2, ЗК6, ЗК7	РН3, РН4
3.	Нормативно-правове забезпечення інформаційної безпеки	ОК14	ІК, ЗК6, СК1	РН 9
4.	Теорія кіл і сигналів в інформаційному та кіберпросторах	ОК15	ІК, ЗК1, ЗК2, ЗК5, СК9	РН5, РН8, РН20
5.	Прикладне програмування	ОК16	ІК, ЗК1, ЗК2, ЗК5	РН5, РН8

6.	Стандарти кібербезпеки та захисту інформації	ОК17	ІК, ЗК6, СК1	РН9
7.	Операційні системи	ОК18	ІК, ЗК 3, ЗК8, СК2	РН6, РН10
8.	Аналіз та оцінка уразливостей інформаційних систем	ОК19	ІК, СК10	РН21
9.	Захист від шкідливого програмного засобу	ОК20	ІК, СК2, СК4	РН10, РН12, РН13
10.	Прикладна криптологія	ОК21	ІК, ЗК1, ЗК8, СК8	РН7, РН18, РН19
11.	Хмарні технології	ОК22	ІК, СК2	РН10
12.	Профілі безпеки	ОК23	ІК, СК6, СК9	РН16, РН20
13.	Штучний інтелект в кібербезпеці	ОК24	ІК, ЗК1, ЗК2, СК2	РН5, РН10
14.	Основи національної безпеки	ОК25	ІК, ЗК2, ЗК6, ЗК7, СК1	РН3, РН4, РН5, РН9
15.	Інформаційна безпека держави	ОК26	ІК, ЗК2, ЗК6, ЗК7, СК1	РН3, РН4, РН5, РН9
16.	Система менеджменту інформаційної безпеки	ОК27	ІК, СК3, СК 7	РН2, РН11, РН17
17.	Теорія ризиків	ОК28	ІК, СК7	РН17
18.	Цифрова криміналістика	ОК29	ІК, СК2, СК5	РН10, РН14, РН15
19.	Економічна безпека діяльності підприємств	ОК30	ІК, СК3	РН11
20.	SIEM системи	ОК31	ІК, СК2, СК5	РН10, РН12, РН13
21.	Організаційне забезпечення захисту інформації	ОК32	ІК, СК3, СК4	РН11, РН12, РН13
22.	Організація конфіденційного діловодства	ОК33	ІК, ЗК1, ЗК4, ЗК6, ЗК7	РН1, РН2, РН3
23.	Аудит систем менеджменту інформаційної безпеки	ОК34	ІК, СК10	РН21
24.	Стратегічні комунікації	ОК35	ІК, ЗК1, ЗК2, ЗК4, СК1	РН2, РН4, РН9

25.	Політики інформаційної безпеки	ОК36	ІК, СК1, СК3, СК7	РН9, РН11, РН17
26.	Ознайомча практика	ОК37	ІК, ЗК1, ЗК2, ЗК6, ЗК8, СК1, СК2	РН4, РН6, РН9, РН10
27.	Виробнича практика	ОК38	ІК, ЗК1, ЗК2, ЗК5,ЗК6, ЗК7, ЗК8, СК1, СК2, СК3	РН3, РН4, РН6, РН7, РН8, РН9, РН10, РН11
28.	Переддипломна практика	ОК39	ІК, ЗК1, ЗК2, ЗК5,ЗК6, ЗК7, ЗК8, СК1, СК2, СК3,СК4,СК5	РН3, РН4, РН6, РН7, РН8, РН9, РН10, РН11, РН12, РН13, РН14, РН15
29.	Кваліфікаційна робота	ОК40	ІК, ЗК1, ЗК2, ЗК5,ЗК6, ЗК7, ЗК8, СК1, СК2, СК3,СК4, СК5, СК7, СК10	РН3, РН4, РН6, РН7, РН8, РН9, РН10, РН11, РН12, РН 13, РН14, РН15, РН17, РН21
3.Дисципліни вільного вибору студента				
1.	Компонента вільного вибору студента			
2.	Компонента вільного вибору студента			
3.	Компонента вільного вибору студента			
4.	Компонента вільного вибору студента			
5.	Компонента вільного вибору студента			
6.	Компонента вільного вибору студента			
7.	Компонента вільного вибору студента			
8.	Компонента вільного вибору студента			
9.	Компонента вільного вибору студента			
10.	Компонента вільного вибору студента			
11.	Компонента вільного вибору студента			
12.	Компонента вільного вибору студента			

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

2.2. Перелік компонент ОП

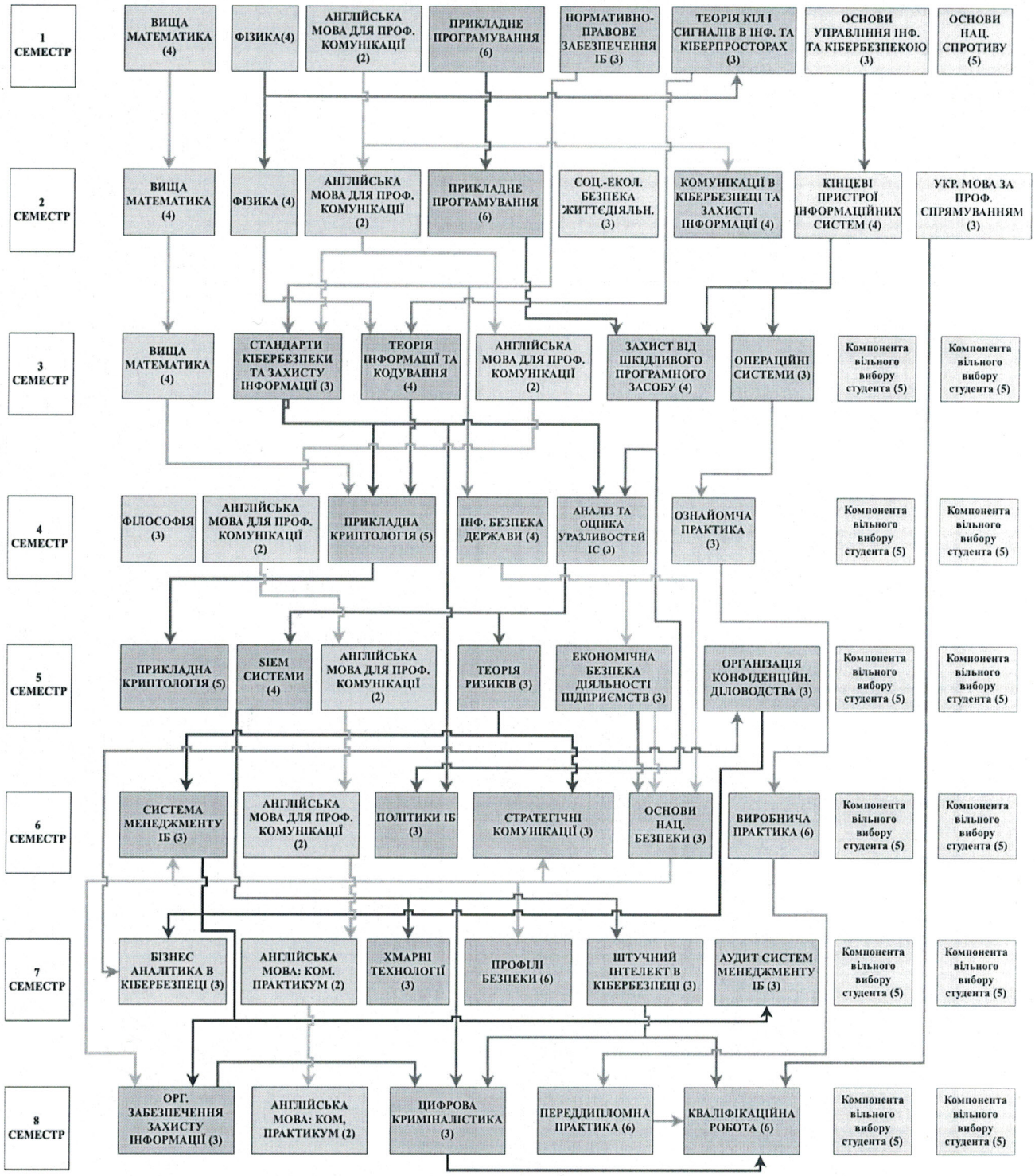
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК1	Вища математика	12	Залік, залік, Іспит
ОК2	Основи управління інформаційною та кібербезпекою**	3	Залік
ОК3	Бізнес аналітика в кібербезпеці	3	Залік
ОК4	Філософія	3	Залік
ОК5	Українська мова за професійним спрямуванням	3	Залік
ОК6	Соціально-екологічна безпека життєдіяльності	3	Іспит
ОК7	Фізика	8	Залік, Іспит
ОК8	Кінцеві пристрої інформаційних систем	4	Залік
ОК9	Основи національного спротиву*	5	Залік
ОК10	Англійська мова для професійної комунікації	12	Залік, Іспит, Залік, Іспит, Залік, Іспит
ОК11	Англійська мова: комунікативний практикум	4	Залік, Іспит
ОК12	Теорія інформації та кодування	4	Іспит
ОК13	Комунікації в кібербезпеці та захисті інформації	4	Залік
ОК14	Нормативно-правове забезпечення інформаційної безпеки**	3	Іспит
ОК15	Теорія кіл і сигналів в інформаційному та кіберпросторах**	3	Іспит
ОК16	Прикладне програмування	12	Залік, залік, Іспит
ОК17	Стандарти кібербезпеки та захисту інформації	3	Іспит
ОК18	Операційні системи	3	Залік
ОК19	Аналіз та оцінка уразливостей інформаційних систем**	3	Іспит Курсова робота
ОК20	Захист від шкідливого програмного засобу	4	Залік
ОК21	Прикладна криптологія	10	Залік, Іспит Курсова робота
ОК22	Хмарні технології	3	Залік
ОК23	Профілі безпеки	6	Іспит, Курсова робота
ОК24	Штучний інтелект в кібербезпеці	3	Залік
ОК25	Основи національної безпеки	3	Іспит

ОК26	Інформаційна безпека держави	4	Іспит
ОК27	Система менеджменту інформаційної безпеки	3	Іспит Курсова робота
ОК28	Теорія ризиків	3	Залік
ОК29	Цифрова криміналістика	3	Іспит
ОК30	Економічна безпека діяльності підприємств**	3	Залік
ОК31	SIEM системи	4	Іспит
ОК32	Організаційне забезпечення захисту інформації	3	Іспит
ОК33	Організація конфіденційного діловодства	3	Залік
ОК34	Аудит систем менеджменту інформаційної безпеки	3	Іспит
ОК35	Стратегічні комунікації	3	Залік
ОК36	Політики інформаційної безпеки	3	Залік
ОК37	Ознайомча практика	3	Залік
ОК38	Виробнича практика	6	Залік
ОК39	Переддипломна практика	6	Залік
ОК40	Кваліфікаційна робота	6	Залік
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП			
ВК1	Компонента вільного вибору студента	5	Залік
ВК2	Компонента вільного вибору студента	5	Залік
ВК3	Компонента вільного вибору студента	5	Залік
ВК4	Компонента вільного вибору студента	5	Залік
ВК5	Компонента вільного вибору студента	5	Залік
ВК6	Компонента вільного вибору студента	5	Залік
ВК7	Компонента вільного вибору студента	5	Залік
ВК8	Компонента вільного вибору студента	5	Залік
ВК9	Компонента вільного вибору студента	5	Залік
ВК10	Компонента вільного вибору студента	5	Залік
ВК11	Компонента вільного вибору студента	5	Залік
ВК12	Компонента вільного вибору студента	5	Залік
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

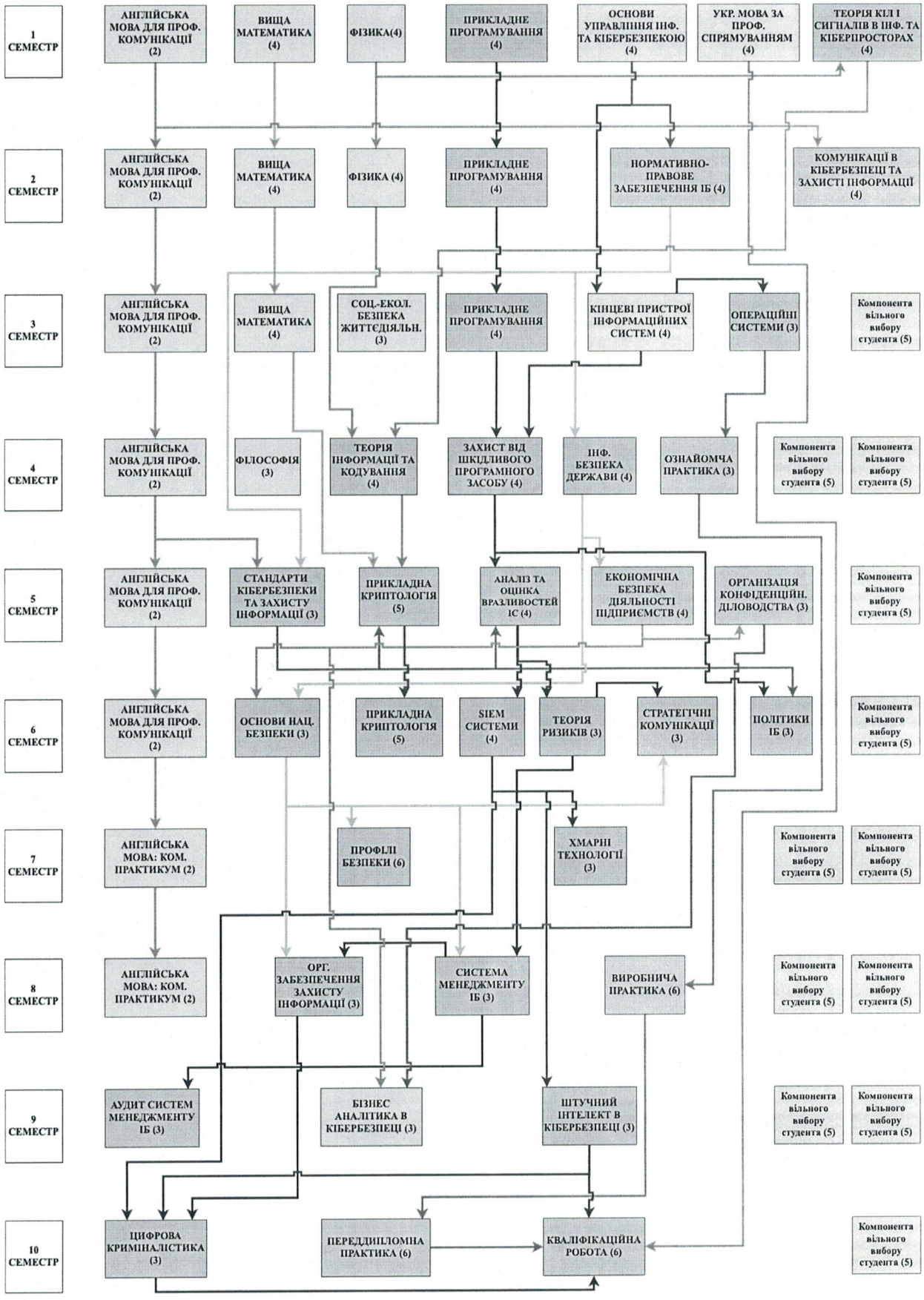
* Для денної форми навчання

**Для заочної форми навчання обсяг кредитів – 4 ECTS

2.3. Структурно-логічна схема ОП



заочна


1 СЕМЕСТР
АНГЛІЙСЬКА МОВА ДЛЯ ПРОФ. КОМУНІКАЦІЙ (2)
ВИЩА МАТЕМАТИКА (4)
ФІЗИКА(4)
ПРИКЛАДНЕ ПРОГРАМУВАННЯ (4)
ОСНОВИ УПРАВЛІННЯ ІНФ. ТА КІБЕРБЕЗПЕКОЮ (4)
УКР. МОВА ЗА ПРОФ. СПРЯМУВАННЯМ (4)
ТЕОРІЯ КІЛ І СИГНАЛІВ В ІНФ. ТА КІБЕРПРОСТОРАХ (4)
2 СЕМЕСТР
АНГЛІЙСЬКА МОВА ДЛЯ ПРОФ. КОМУНІКАЦІЙ (2)
ВИЩА МАТЕМАТИКА (4)
ФІЗИКА (4)
ПРИКЛАДНЕ ПРОГРАМУВАННЯ (4)
НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІБ (4)
КОМУНІКАЦІЇ В КІБЕРБЕЗПЕЦІ ТА ЗАХИСТІ ІНФОРМАЦІЇ (4)
3 СЕМЕСТР
АНГЛІЙСЬКА МОВА ДЛЯ ПРОФ. КОМУНІКАЦІЙ (2)
ВИЩА МАТЕМАТИКА (4)
СОЦ.-ЕКОЛ. БЕЗПЕКА ЖИТТЄДІЯЛЬН. (3)
ПРИКЛАДНЕ ПРОГРАМУВАННЯ (4)
КІНЦЕВІ ПРИСТРОЇ ІНФОРМАЦІЙНИХ СИСТЕМ (4)
ОПЕРАЦІЙНІ СИСТЕМИ (3)
Компонента вільного вибору студента (5)
4 СЕМЕСТР
АНГЛІЙСЬКА МОВА ДЛЯ ПРОФ. КОМУНІКАЦІЙ (2)
ФІЛОСОФІЯ (3)
ТЕОРІЯ ІНФОРМАЦІЇ ТА КОДУВАННЯ (4)
ЗАХИСТ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАСОБУ (4)
ІНФ. БЕЗПЕКА ДЕРЖАВИ (4)
ОЗНАЙОМЧА ПРАКТИКА (3)
Компонента вільного вибору студента (5)
Компонента вільного вибору студента (5)
5 СЕМЕСТР
АНГЛІЙСЬКА МОВА ДЛЯ ПРОФ. КОМУНІКАЦІЙ (2)
СТАНДАРТИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ (3)
ПРИКЛАДНА КРИПТОЛОГІЯ (5)
АНАЛІЗ ТА ОЦІНКА ВРАЗЛИВОСТЕЙ ІС (4)
ЕКОНОМІЧНА БЕЗПЕКА ДІЯЛЬНОСТІ ПІДПРИЄМСТВ (4)
ОРГАНІЗАЦІЯ КОНФІДЕНЦІЙН. ДІЛОВОДСТВА (3)
Компонента вільного вибору студента (5)
6 СЕМЕСТР
АНГЛІЙСЬКА МОВА ДЛЯ ПРОФ. КОМУНІКАЦІЙ (2)
ОСНОВИ НАЦ. БЕЗПЕКИ (3)
ПРИКЛАДНА КРИПТОЛОГІЯ (5)
SIEM СИСТЕМИ (4)
ТЕОРІЯ РИЗИКІВ (3)
СТРАТЕГІЧНІ КОМУНІКАЦІЇ (3)
ПОЛІТИКИ ІБ (3)
Компонента вільного вибору студента (5)
7 СЕМЕСТР
АНГЛІЙСЬКА МОВА: КОМ. ПРАКТИКУМ (2)
ПРОФІЛІ БЕЗПЕКИ (6)
ХМАРНІ ТЕХНОЛОГІЇ (3)
Компонента вільного вибору студента (5)
Компонента вільного вибору студента (5)
8 СЕМЕСТР
АНГЛІЙСЬКА МОВА: КОМ. ПРАКТИКУМ (2)
ОРГ. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ (3)
СИСТЕМА МЕНЕДЖМЕНТУ ІБ (3)
ВИРОБНИЧА ПРАКТИКА (6)
Компонента вільного вибору студента (5)
Компонента вільного вибору студента (5)
9 СЕМЕСТР
АУДИТ СИСТЕМ МЕНЕДЖМЕНТУ ІБ (3)
БІЗНЕС АНАЛІТИКА В КІБЕРБЕЗПЕЦІ (3)
ШТУЧНИЙ ІНТЕЛЕКТ В КІБЕРБЕЗПЕЦІ (3)
Компонента вільного вибору студента (5)
Компонента вільного вибору студента (5)
10 СЕМЕСТР
ЦИФРОВА КРИМІНАЛІСТИКА (3)
ПЕРЕДДИПЛОМНА ПРАКТИКА (6)
КВАЛІФІКАЦІЙНА РОБОТА (6)
Компонента вільного вибору студента (5)
Компоненти циклу загальної підготовки
Компоненти вільного вибору студента
Компоненти циклу професійної підготовки
ПРАКТИКА

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 єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом.
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

Освітні компоненти	Компетентності																			
	Загальні компетентності									Спеціальні (фахові) компетентності										
	ІК	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК 1	СК 2	СК 3	СК 4	СК 5	СК 6	СК 7	СК 8	СК 9	СК 10
ОК1	+					+													
ОК2	+						+			+	+	+							
ОК3	+	+	+																
ОК4	+			+															
ОК5	+			+															
ОК6	+		+				+	+	+										
ОК7	+								+										
ОК8	+		+						+										
ОК9	+						+		+										
ОК10	+				+														
ОК11	+				+														
ОК12	+	+							+										
ОК13	+	+	+				+	+											
ОК14	+						+			+									
ОК15	+	+	+			+												+	
ОК16	+	+	+			+													
ОК17	+						+			+									
ОК18	+			+					+		+								
ОК19	+																		+
ОК20	+										+		+						
ОК21	+	+							+								+		
ОК22	+										+								
ОК23	+														+			+	
ОК24	+	+	+								+								
ОК25	+		+				+	+		+									
ОК26	+		+				+	+		+									
ОК27	+											+				+			
ОК28	+															+			
ОК29	+										+			+					
ОК30	+											+							
ОК31	+										+			+					
ОК32	+											+	+						
ОК33	+	+			+		+	+											
ОК34	+																		+
ОК35	+	+	+		+					+									
ОК36	+									+		+				+			
ОК37	+	+	+				+		+	+	+								
ОК38	+	+	+			+	+	+	+	+	+	+							
ОК39	+	+	+			+	+	+	+	+	+	+	+	+					
ОК40	+	+	+			+	+	+	+	+	+	+	+	+		+			+

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

Освітні компоненти	Результати навчання																				
	РН 1	РН2	РН3	РН4	РН5	РН6	РН7	РН8	РН 9	РН 10	РН 11	РН 12	РН 13	РН 14	РН 15	РН 16	РН 17	РН 18	РН 19	РН 20	РН 21
ОК1								+													
ОК2									+	+	+										
ОК3				+																	
ОК4	+																				
ОК5	+																				
ОК6			+			+															
ОК7								+													
ОК8		+				+															
ОК9			+			+			+												
ОК10		+																			
ОК11		+																			
ОК12							+														
ОК13			+	+																	
ОК14									+												
ОК15					+			+												+	
ОК16					+			+													
ОК17									+												
ОК18						+				+											
ОК19																					+
ОК20										+		+	+								
ОК21							+											+	+		
ОК22										+											
ОК23																+				+	
ОК24					+					+											
ОК25			+	+	+				+												
ОК26			+	+	+				+												
ОК27		+									+						+				
ОК28																	+				
ОК29										+				+	+						
ОК30											+										
ОК31										+		+	+								
ОК32											+	+	+								
ОК33	+	+	+																		
ОК34																					+
ОК35		+		+					+												
ОК36									+		+						+				
ОК37				+		+			+	+											
ОК38			+	+		+	+	+	+	+	+										
ОК39			+	+		+	+	+	+	+	+	+	+	+	+						
ОК40			+	+		+	+	+	+	+	+	+	+	+	+		+				+

Гарант освітньої програми
Доцент кафедри управління кібербезпекою та захистом інформації
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету
інформаційно-комунікаційних технологій
Кандидат наук з держ. управл., доцент Тетяна МУЖАНОВА