

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

ПРОЄКТ

ОСВІТНЯ ПРОГРАМА

**“УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА
КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ”**

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 №
Наказ №

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію

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 навчально-виховної роботи | Артур ГУДМАНЯН |
| 3. Т.в.о. навчально-методичного відділу | Вадим ВЛАСЕНКО |
| 4. Вчена рада Навчально-наукового інституту кібербезпеки та захисту інформації | |

Протокол № від

Голова Вченої Ради ННІКБЗІ _____ Євгенія ІВАНЧЕНКО

5. Кафедра управління кібербезпекою та захистом інформації

Протокол № від

Завідувач кафедри
управління кібербезпекою
та захистом інформації _____ Світлана ЛЕГОМІНОВА

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 –

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.

Віталій ТИЩЕНКО – здобувач вищої освіти третього (освітньо-наукового) рівня спеціальності F5 “Кібербезпека та захист інформації”;

Надія Святська – здобувачка 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

Освітня програма розроблена у відповідності до:

Державного стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти (Наказ МОН України від 04.10.2018 № 1074);

Професійного стандарту на групу професій «Викладачі закладів вищої освіти» (Наказ Міністерства економіки від 23.03.2021 № 610);

Постанови Кабінету Міністрів України «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 16.12.2022 №1392;

Наказу Міністерства економіки України «Про затвердження зміни № 11 до національного класифікатора ДК 003:2010 «Класифікатор професій» від 29.12.2022 № 5573;

Наказу Міністерства освіти і науки України №1547 від 29 жовтня 2024 року “Про внесення змін до стандарту вищої освіти зі спеціальності “Кібербезпека” галузі знань 12 “Інформаційні технології” для першого (бакалаврського) рівня вищої освіти.

рекомендацій акредитаційних комісій Університету; пропозицій роботодавців;
побажань здобувачів вищої освіти.

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 1 вересня 2025 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-bezpekoju

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 розвитку 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,

	<p>семінарських та практичних, лабораторних занять з залученням фахівців-практиків з кібербезпеки.</p> <p>Об'єкти вивчення:</p> <ul style="list-style-type: none"> - 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. <p>Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації.</p> <p>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.</p> <p>Методи, методики та технології: Методи, методики та технології розв'язання теоретичних та практичних задач кібербезпеки та захисту інформації.</p> <p>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).</p>
Працевлаштування випускників	<p>На посади у структурних підрозділах установ / підприємств / організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації.</p>
Особливості програми	<p>Програма передбачає:</p> <ul style="list-style-type: none"> - 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

	<p>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.</p>
6 - Програмні компетенції	
Інтегральна компетентність	<p>Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.</p>
<p>Загальні компетентності (ЗК)</p>	<p>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 недобросовісності. 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.</p>
<p>Спеціальні (фахові, предметні) компетентності (КФ)</p>	<p>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.</p>

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. Організувати 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

	<p>функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.</p> <p>РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.</p> <p>РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.</p> <p>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.</p> <p>РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.</p> <p>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.</p> <p>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.</p>
--	--

8 – Ресурсне забезпечення реалізації програми

<p>Кадрове забезпечення</p>	<p>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 спеціальності F5 Кібербезпека та захист інформації</p>
-----------------------------	--

	<p>сформована з числа науково-педагогічних працівників Державного університету інформаційно-комунікаційних технологій. Кількісний та якісний склад групи відповідають Ліцензійним вимогам.</p>
<p>Матеріально-технічне забезпечення</p>	<p>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.</p> <p>НАВЧАЛЬНА ЛАБОРАТОРІЯ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ</p> <p>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.</p> <p>НАВЧАЛЬНА ЛАБОРАТОРІЯ МЕРЕЖЕВОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ CISCO</p> <p>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.</p> <p>НАВЧАЛЬНА ЛАБОРАТОРІЯ SECURITY OPERATION CENTER</p> <p>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</p>

		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 мобільність	кредитна	Наявність двосторонніх договорів між ДУІКТ та закладами вищої освіти України забезпечує національну кредитну мобільність.
Міжнародна мобільність	кредитна	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	OK01	ІК, ЗК5	PH8
2.	Основи управління інформаційною та кібербезпекою	OK02	ІК, ЗК6, СК1, СК2, СК3	PH9, PH10, PH11
3.	Бізнес аналітика в кібербезпеці	OK03	ІК, ЗК1, ЗК2	PH4
4.	Філософія	OK04	ІК, ЗК3	PH1
5.	Іноземна мова*	OK05	ІК, ЗК4	PH2
6.	Українська мова за професійним спрямуванням	OK06	ІК, ЗК3	PH1
7.	Комунікації в кібербезпеці та захисті інформації	OK07	ІК, ЗК1, ЗК2, ЗК6, ЗК7	PH3, PH4
8.	Соціально-екологічна безпека життєдіяльності	OK08	ІК, ЗК2, ЗК6, ЗК7, ЗК8	PH3, PH6
9.	Нормативно-правове забезпечення інформаційної безпеки	OK09	ІК, ЗК6, СК1	PH 9
10.	Фізика	OK10	ІК, ЗК8	PH8
11.	Теорія інформації та кодування	OK11	ІК, ЗК1, ЗК8	PH7
12.	Кінцеві пристрої інформаційних систем	OK12	ІК, ЗК 2, ЗК8	PH2, PH6
13.	Базова загальна військова підготовка	OK13		
2. Цикл компонент професійної та практичної підготовки				
1.	Теорія кіл і сигналів в інформаційному та кіберпросторах	OK14	ІК, ЗК1, ЗК2, ЗК5, СК9	PH5, PH8, PH20
2.	Прикладне програмування	OK15	ІК, ЗК1, ЗК2, ЗК5	PH5, PH8
3.	Стандарти інформаційної та кібербезпеки	OK16	ІК, ЗК6, СК1	PH9
4.	Операційні системи	OK17	ІК, ЗК 3, ЗК8, СК2	PH6, PH10

5.	Аналіз та оцінка уразливостей інформаційних систем	OK18	ІК, СК10	PH21
6.	Захист від шкідливого програмного засобу	OK19	ІК, СК2, СК4	PH10, PH12, PH13
7.	Прикладна криптологія	OK20	ІК, ЗК1, ЗК8, СК8	PH7, PH18, PH19
8.	Хмарні технології	OK21	ІК, СК2	PH10
9.	Комплексні системи захисту інформації	OK22	ІК, СК6, СК9	PH16, PH20
10.	Штучний інтелект	OK23	ІК, ЗК1, ЗК2, СК2	PH5, PH10
11.	Основи національної безпеки	OK24	ІК, ЗК2, ЗК6, ЗК7, СК1	PH3, PH4, PH5, PH9
12.	Інформаційна безпека держави	OK25	ІК, ЗК2, ЗК6, ЗК7, СК1	PH3, PH4, PH5, PH9
13.	Система менеджменту інформаційної безпеки	OK26	ІК, СК3, СК 7	PH2, PH11, PH17
14.	Теорія ризиків	OK27	ІК, СК7	PH17
15.	Системний аналіз інформаційної безпеки	OK28	ІК, СК7	PH17
16.	Цифрова криміналістика	OK29	ІК, СК2, СК5	PH10, PH14, PH15
17.	Економічна безпека діяльності підприємств	OK30	ІК, СК3	PH11
18.	SIEM системи	OK31	ІК, СК2, СК5	PH10, PH12, PH13
19.	Організаційне забезпечення захисту інформації	OK32	ІК, СК3, СК4	PH11, PH12, PH13
20.	Організація конфіденційного діловодства	OK33	ІК, ЗК1, ЗК4, ЗК6, ЗК7	PH1, PH2, PH3
21.	Аудит систем менеджменту інформаційної безпеки	OK34	ІК, СК10	PH21
22.	Стратегічні комунікації	OK35	ІК, ЗК1, ЗК2, ЗК4, СК1	PH2, PH4, PH9
23.	Політики інформаційної безпеки	OK36	ІК, СК1, СК3, СК7	PH9, PH11, PH17

24.	Ознайомча практика	OK37	ІК, ЗК1, ЗК2, ЗК6, ЗК8, СК1, СК2	PH4, PH6, PH9, PH10
25.	Виробнича практика	OK38	ІК, ЗК1, ЗК2, ЗК5, ЗК6, ЗК7, ЗК8, СК1, СК2, СК3	PH3, PH4, PH6, PH7, PH8, PH9, PH10, PH11
26.	Переддипломна практика	OK39	ІК, ЗК1, ЗК2, ЗК5, ЗК6, ЗК7, ЗК8, СК1, СК2, СК3, СК4, СК5	PH3, PH4, PH6, PH7, PH8, PH9, PH10, PH11, PH12, PH13, PH14, PH15
27.	Кваліфікаційна робота	OK40	ІК, ЗК1, ЗК2, ЗК5, ЗК6, ЗК7, ЗК8, СК1, СК2, СК3, СК4, СК5, СК7, СК10	PH3, PH4, PH6, PH7, PH8, PH9, PH10, PH11, PH12, PH 13, PH14, PH15, PH17, PH21
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			

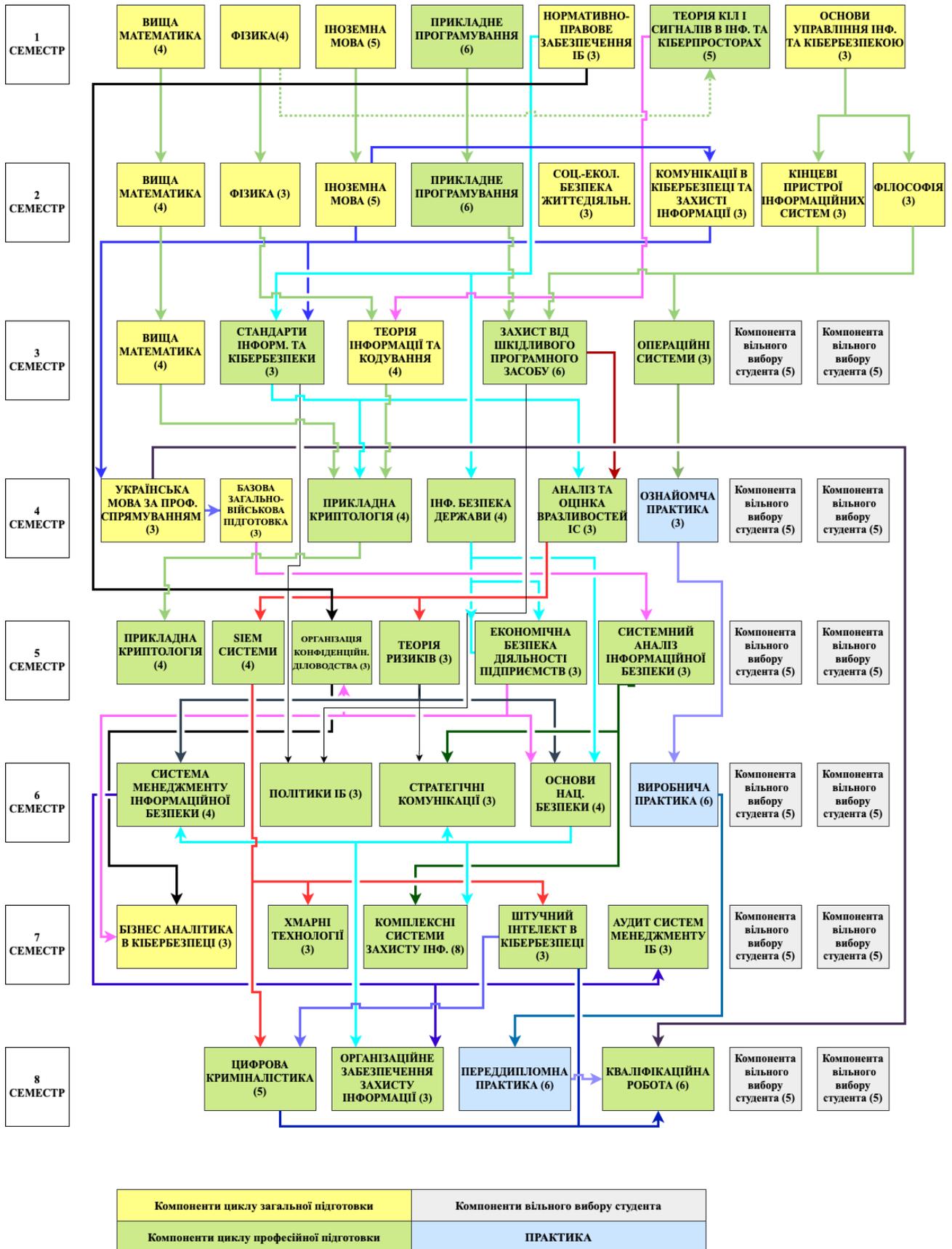
* Іноземна мова у навчальних планах для іноземців та осіб без громадянства замінюються на українську мову (за професійним спрямуванням).

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			
OK1	Вища математика	12	Залік, залік, Іспит
OK2	Основи управління інформаційною та кібербезпекою	3	Залік
OK3	Бізнес аналітика в кібербезпеці	3	Залік
OK4	Філософія	3	Іспит
OK5	Іноземна мова	10	Залік, Іспит
OK6	Українська мова за професійним спрямуванням	3	Залік
OK7	Комунікації в кібербезпеці та захисті інформації	3	Залік
OK8	Соціально-екологічна безпека життєдіяльності	3	Іспит
OK9	Нормативно-правове забезпечення інформаційної безпеки	3	Іспит
OK10	Фізика	7	Залік, Іспит
OK11	Теорія інформації та кодування	4	Іспит
OK12	Кінцеві пристрої інформаційних систем	3	Залік
OK13	Базова загальна військова підготовка	3	Залік
OK14	Теорія кіл і сигналів в інформаційному та кіберпросторах	5	Іспит
OK15	Прикладне програмування	12	Залік, Іспит
OK16	Стандарти інформаційної та кібербезпеки	3	Іспит
OK17	Операційні системи	3	Іспит
OK18	Аналіз та оцінка уразливостей інформаційних систем	3	Іспит Курсова робота
OK19	Захист від шкідливого програмного засобу	6	Залік
OK20	Прикладна криптологія	8	Залік, Іспит Курсова робота
OK21	Хмарні технології	3	Залік
OK22	Комплексні системи захисту інформації	8	Іспит, Курсова робота
OK23	Штучний інтелект в кібербезпеці	3	Іспит
OK24	Основи національної безпеки	4	Іспит
OK25	Інформаційна безпека держави	4	Іспит
OK26	Система менеджменту інформаційної безпеки	4	Іспит Курсова робота
OK27	Теорія ризиків	3	Залік
OK28	Системний аналіз інформаційної безпеки	3	Залік
OK29	Цифрова криміналістика	5	Іспит
OK30	Економічна безпека діяльності підприємств	3	Залік

OK31	SIEM системи	4	Іспит
OK32	Організаційне забезпечення захисту інформації	3	Іспит
OK33	Організація конфіденційного діловодства	3	Залік
OK34	Аудит систем менеджменту інформаційних систем	3	Залік
OK35	Стратегічні комунікації	3	Залік
OK36	Політики інформаційної безпеки	3	Залік
OK37	Ознайомча практика	3	Залік
OK38	Виробнича практика	6	Залік
OK39	Переддипломна практика	6	Залік
OK40	Кваліфікаційна робота	6	Залік
Загальний обсяг обов'язкових компонент:		180	
Вибіркові компоненти ОП			
OK41	Компонента вільного вибору студента	5	Залік
OK42	Компонента вільного вибору студента	5	Залік
OK43	Компонента вільного вибору студента	5	Залік
OK44	Компонента вільного вибору студента	5	Залік
OK45	Компонента вільного вибору студента	5	Залік
OK46	Компонента вільного вибору студента	5	Залік
OK47	Компонента вільного вибору студента	5	Залік
OK48	Компонента вільного вибору студента	5	Залік
OK49	Компонента вільного вибору студента	5	Залік
OK50	Компонента вільного вибору студента	5	Залік
OK51	Компонента вільного вибору студента	5	Залік
OK52	Компонента вільного вибору студента	5	Залік
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 здобувачів вищої освіти здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної бакалаврської роботи.
<i>Вимоги до кваліфікаційної роботи</i>	Кваліфікаційна бакалаврська робота передбачає розв'язання спеціалізованої задачі в галузі кібербезпеки та захисту інформації. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Перевірка на плагіат проводиться згідно з Кодексом академічної доброчесності Державного університету інформаційно-комунікаційних технологій, введеного в дію наказом ректора від 14 серпня 2023 року № 111. Кваліфікаційна робота розміщується на офіційному сайті (або репозитарії) Державного університету інформаційно-комунікаційних технологій. Атестація здійснюється відкрито і гласно.

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	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	
OK.01	+					+														
OK.02	+						+			+	+	+								
OK.03	+	+	+																	
OK.04	+			+																
OK.05	+				+															
OK.06	+			+																
OK.07	+	+	+					+	+											
OK.08	+		+					+	+	+										
OK.09	+							+		+										
OK.10	+								+											
OK.11	+	+							+											
OK.12	+		+						+											
OK.13																				
OK.14	+	+	+			+												+		
OK.15	+	+	+			+														
OK.16	+						+			+										
OK.17	+			+					+		+									
OK.18	+																		+	
OK.19	+										+		+							
OK.20	+	+							+									+		
OK.21	+										+									
OK.22	+														+			+		
OK.23	+	+	+								+									
OK.24	+		+				+	+		+										
OK.25	+		+				+	+		+										
OK.26	+											+				+				
OK.27	+															+				
OK.28	+															+				
OK.29	+										+			+						
OK.30	+											+								
OK.31	+										+			+						
OK.32	+											+	+							
OK.33	+	+			+		+	+												
OK.34	+																		+	
OK.35	+	+	+		+					+										
OK.36	+									+		+				+				
OK.37	+	+	+				+		+	+	+									
OK.38	+	+	+			+	+	+	+	+	+	+								
OK.39	+	+	+			+	+	+	+	+	+	+	+	+						
OK.40	+	+	+			+	+	+	+	+	+	+	+	+		+			+	

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

Освітні компоненти	Результати навчання																				
	РН 1	РН 2	РН 3	РН 4	РН 5	РН 6	РН 7	РН 8	РН 9	РН 10	РН 11	РН 12	РН 13	РН 14	РН 15	РН 16	РН 17	РН 18	РН 19	РН 20	РН 21
OK.01								+													
OK.02									+	+	+										
OK.03				+																	
OK.04	+																				
OK.05		+																			
OK.06	+																				
OK.07			+	+																	
OK.08			+			+															
OK.09								+													
OK.10								+													
OK.11									+												
OK.12		+				+															
OK.13																					
OK.14					+			+												+	
OK.15					+			+													
OK.16									+												
OK.17						+				+											
OK.18																					+
OK.19										+		+	+								
OK.20								+										+	+		
OK.21										+											
OK.22																+				+	
OK.23					+					+											
OK.24			+	+	+				+												
OK.25			+	+	+				+												
OK.26		+									+							+			
OK.27																		+			
OK.28																		+			
OK.29										+				+	+						
OK.30											+										
OK.31										+		+	+								
OK.32											+	+	+								
OK.33	+	+	+																		
OK.34																					+
OK.35		+		+					+												
OK.36									+		+							+			
OK.37				+		+			+	+											
OK.38			+	+		+	+	+	+	+	+										
OK.39			+	+		+	+	+	+	+	+	+	+	+	+						
OK.40			+	+		+	+	+	+	+	+	+	+	+	+		+				+

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