МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«Ужгородський національний університет»

ЗАТВЕРДЖЕНО
Протокол Вченої ради
ДВНЗ «Ужгородський
національний університет»
28.03. **2024 р. №** 4

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

Першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

Кваліфікація: Бакалавр з кібербезпеки та захисту інформації

УВЕДЕНО В ДІЮ
Наказ ректора ДВНЗ
«Ужгородський національний
університет
04.04. **2024 р. №** 250/01-04

ЗМІНИ ДО ОСВІТНЬОЇ ПРОГРАМИ

ЗАТВЕРДЖЕНО
Протокол Вченої ради ДВНЗ «УжНУ»
28.01 2025 р. № 1

УВЕДЕНО В ДІЮ
Наказ ректора ДВНЗ «УжНУ»
28.01 2025 р. № 181/01-04

Ужгород 2025

АРКУШ ПОГОДЖЕННЯ
освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»

1. **Ректор** **Володимир СМОЛАНКА**

28.01. **2025 р.**

2. **Гарант освітньо-професійної програми** **Олександр ЧОБАЛЬ**

20 грудня **2024 р.**

3. **Декан структурного підрозділу** **Володимир ЛАЗУР**

20 грудня **2024 р.**

4. **Керівник робочої групи** **Олександр ЧОБАЛЬ**

20 грудня **2024 р.**

5. **Начальник навчальної частини** **Анатолій ШТИМАК**

27.01. **2025 р.**

ПЕРЕДМОВА

Освітньо-професійна програма "Безпека інформаційних і комунікаційних систем" підготовки здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека та захист інформації розроблена згідно з вимогами Закону України «Про вищу освіту» та відповідно до нової редакції стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології для першого (бакалаврського) рівня, затвердженого й введеного в дію наказом Міністерства освіти і науки України № 1547 від 29.10.2024 р.

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ: Чобаль Олександр Ілліч, кандидат фіз.-мат. наук, доцент, доцент кафедри твердотільної електроніки та інформаційної безпеки;

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

1. Різак Василь Михайлович, доктор фіз.-мат. наук, професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки;

2. Січка Михайло Юрійович, кандидат фіз.-мат. наук, доцент, доцент кафедри твердотільної електроніки та інформаційної безпеки;

3. Маркевич Петро Вікторович, начальник Управління державної служби спеціального зв'язку та захисту інформації України в Закарпатській області

4. Попович Владислава Володимирівна, здобувачка першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації, голова студентської ради фізичного факультету ДВНЗ "УжНУ".

Рецензії-відгуки зовнішніх стейкхолдерів:

Корченко Олександр Григорович, перший проректор Державного університету інформаційно-комунікаційних технологій, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, доктор технічних наук (05.13.21 - Системи захисту інформації), професор.

Танчинець Михайло Михайлович, заступник начальника відділу протидії кіберзлочинам в Закарпатській області Департаменту кіберполіції Національної поліції України

1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Державний вищий навчальний заклад «Ужгородський національний університет», фізичний факультет, кафедра твердотільної електроніки та інформаційної безпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти: бакалавр. Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС. Термін навчання 3 роки 10 місяців.
Наявність акредитації	Акредитаційна комісія України Сертифікат про акредитацію серія НД № 0791769 Термін дії сертифікату до 01.07.2025 р.
Цикл/рівень	Національна рамка кваліфікацій України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень.
Передумови	Наявність повної загальної середньої освіти. Умови вступу визначаються «Правилами прийому до Ужгородського національного університету»
Мова(и) викладання	Українська
Термін дії освітньої програми	До чергового перегляду
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.uzhnu.edu.ua/uk/infocentre/15068
2 – Мета освітньої програми	
Навчання та підготовка конкурентних на ринку праці фахівців в галузі інформаційних технологій, здатних розробляти, використовувати і впроваджувати технології кібербезпеки та захисту інформації для вирішення низки актуальних завдань у сфері інформаційної безпеки. Засвоїти знання з основ законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації

	Обсяг освітньої програми бакалавра: – на базі повної загальної середньої освіти з терміном навчання 11 років – 240 кредитів ЄКТС – на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти. Для здобуття ступеня бакалавра на основі ступеня молодшого бакалавра, фахового молодшого бакалавра або ОКР молодшого спеціаліста ЗВО має право скорочувати обсяг освітньої програми. При цьому програма має забезпечувати набуття визначених стандартом вищої освіти результатів навчання, а її загальний обсяг має бути не меншим, ніж 120 кредитів. Об’єкти вивчення: – об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології; – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації. Цілі навчання: підготовка фахівців, здатних розробляти, використовувати і впроваджувати технології кібербезпеки та захисту інформації, а також розв’язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної діяльності Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної безпеки та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою;

	– процесів функціонування системи управління інформаційною безпекою та/або кібербезпекою, а також основ теорії ризиків; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Програма має освітньо-професійну орієнтацію на здобуття студентами знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності у галузі кібербезпеки та захисту інформації; базується на загальновідомих у галузі інформаційних технології наукових результатах, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта в галузі знань «Інформаційні технології» з поглибленою спеціалізованою підготовкою в сфері безпеки інформаційних і комунікаційних систем. Ключові слова: кібербезпека, інформаційно-комунікаційні системи, програмно-апаратне забезпечення, проєктування систем кібербезпеки та захисту інформації
Особливості програми	Програма передбачає вивчення: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – методів і засобів виявлення, управління та ідентифікації ризиків; – методів і засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних систем; – сучасних програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації. Освітня програма враховує вимоги національних роботодавців, міжнародних стандартів інформаційної та кібербезпеки, а також тенденції розвитку IT - галузі.

Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Професійна діяльність в галузі інформаційної та/або кібербезпеки в установах, підприємствах та організаціях різних форм власності на посадах, що передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації
Подальше навчання	Можливість навчання на другому (магістерському) рівні вищої освіти. Навчання за перехресним вступом, здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та лабораторні заняття, самонавчання, проектно-орієнтоване навчання, консультації із науково-педагогічними працівниками, проведення наукових досліджень. Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуально-творчий підхід, навчання через виробничу та педагогічну практики.
Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної навчальної діяльності, спрямовані на опанування навчального навантаження освітньої програми: поточні контроль та оцінювання, поетапний, модульний, підсумковий контроль; екзамени; заліки, презентації, курсовий проект, єдиний державний кваліфікаційний іспит. Проміжкове та підсумкове оцінювання знань відбувається на засадах студентоорієнтованого особистісного підходу з використанням сучасних методик та практик. Оцінювання знань здобувачів вищої освіти відбувається згідно: Положення про організацію освітнього процесу в Державному вищому навчальному закладі «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/31357 Положення про порядок та методику проведення семестрових (курсових) екзаменів і заліків в Ужгородському національному університеті https://www.uzhnu.edu.ua/uk/infocentre/get/5952, Положення про атестацію здобувачів вищої освіти та екзаменаційну комісію у Державному вищому навчальному закладі «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/11070

	з дотриманням норм академічної доброчесності відповідно до Положення про академічну доброчесність в Ужгородському національному університеті https://www.uzhnu.edu.ua/uk/infocentre/get/12223. Перезарахування кредитів відбувається на основі Положення про визнання (перезарахування) кредитів ЄКТС для учасників програм академічної мобільності у Державному вищому навчальному закладі «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/20131. Процедура оцінювання здобувачів вищої освіти також враховує результати неформальної освіти згідно Положення про порядок визнання Державному вищому навчальному закладі «Ужгородський національний університет» результатів навчання, здобутих у неформальній освіті https://www.uzhnu.edu.ua/uk/infocentre/get/22966. Наявна чітка процедура розгляду апеляцій здобувачів вищої освіти, яка описана в Положенні про порядок застосування заходів з врегулювання конфліктів та спорів (суперечок) у діяльності співробітників та здобувачів вищої освіти Державного вищого навчального закладу «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/22964 та Положенні про порядок оскарження результатів (апеляція) оцінювання в Державному вищому навчальному закладі «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/22967
Програмні компетентності	
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 і 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.
Фахові компетентності (ФК)	– ФК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. – ФК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. – ФК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. – ФК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. – ФК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. – ФК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів, тощо). – ФК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. – ФК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

	– ФК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. – ФК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
Програмні результати навчання	
– РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. – РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. – РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. – РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. – РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. – РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. – РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. – РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. – РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. – РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. – РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. – РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.	

– РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно- комунікаційних систем та\або інфраструктури організації в цілому. – РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. – РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. – РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. – 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.	
Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація освітньої програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають Ліцензійним умовам провадження освітньої діяльності на першому (бакалаврському) рівні вищої освіти. Склад робочої групи освітньої програми та професорсько-викладацький склад, що задіяний до викладання навчальних дисциплін, постійно

	проходять стажування та підвищення кваліфікації, що відповідає Положенню про підвищення кваліфікації та стажування педагогічних та науково-педагогічних працівників ДВНЗ ”УжНУ” . https://www.uzhnu.edu.ua/uk/infocentre/get/5950
Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо матеріально-технічного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України. Освітня програма забезпечена необхідним матеріально - технічним комплексом засобів та систем для її реалізації: навчальними приміщеннями, комп’ютерними робочими місцями, лабораторіями, мультимедійним обладнанням, устаткуванням, контрольно-вимірювальними приладами необхідними для виконання навчальних планів. Наявні засоби обчислювальної техніки з прикладним та спеціалізованим програмним забезпеченням, спеціальні радіовимірювальні пристрої, засоби технічного захисту інформації, спеціалізовані апаратно-програмні комплекси. Наявна вся необхідна соціально-побутова інфраструктура. Для проведення практичних і лабораторних робіт, інформаційного пошуку та обробки результатів наявні спеціалізовані комп’ютерні класи факультету з необхідним програмним забезпеченням та необмежено відкритим доступом до Інтернет-мережі.
Інформаційне та навчально-методичне забезпечення	– офіційний веб-сайт http://www.uzhnu.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти; – необмежений доступ до мережі Інтернет, фондів та електронних каталогів наукової бібліотеки ДВНЗ «УжНУ», а також до електронного репозитарію ДВНЗ «УжНУ» (https://dspace.uzhnu.edu.ua/jspui/), де містяться навчально-методичні матеріали з дисциплін навчального плану; – наукова бібліотека, читальні зали; – навчальні і робочі плани; – графіки навчального процесу; – дидактичні матеріали для самостійної та індивідуальної роботи студентів з дисциплін, програми практик; – сайт електронного навчання ДВНЗ “УжНУ” (https://moodle.uzhnu.edu.ua/).

Академічна мобільність	
Національна кредитна мобільність	Академічна мобільність студентів здійснюється на основі двосторонніх угод, укладених між ДВНЗ «Ужгородський національний університет» та закладами вищої освіти України.
Міжнародна кредитна мобільність	Відповідно до Положення про академічну мобільність студентів у ДВНЗ «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/21269 , встановлено загальний порядок організації академічної мобільності студентів. Започатковано програми міжнародної академічної мобільності «Еразмус +».
Навчання іноземних здобувачів вищої освіти	До ДВНЗ «УжНУ» приймаються іноземні громадяни, а також особи без громадянства, які проживають на території України на законних підставах. Особливості вступу та навчання визначаються Положенням про навчання іноземних громадян у ДВНЗ «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/9378

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

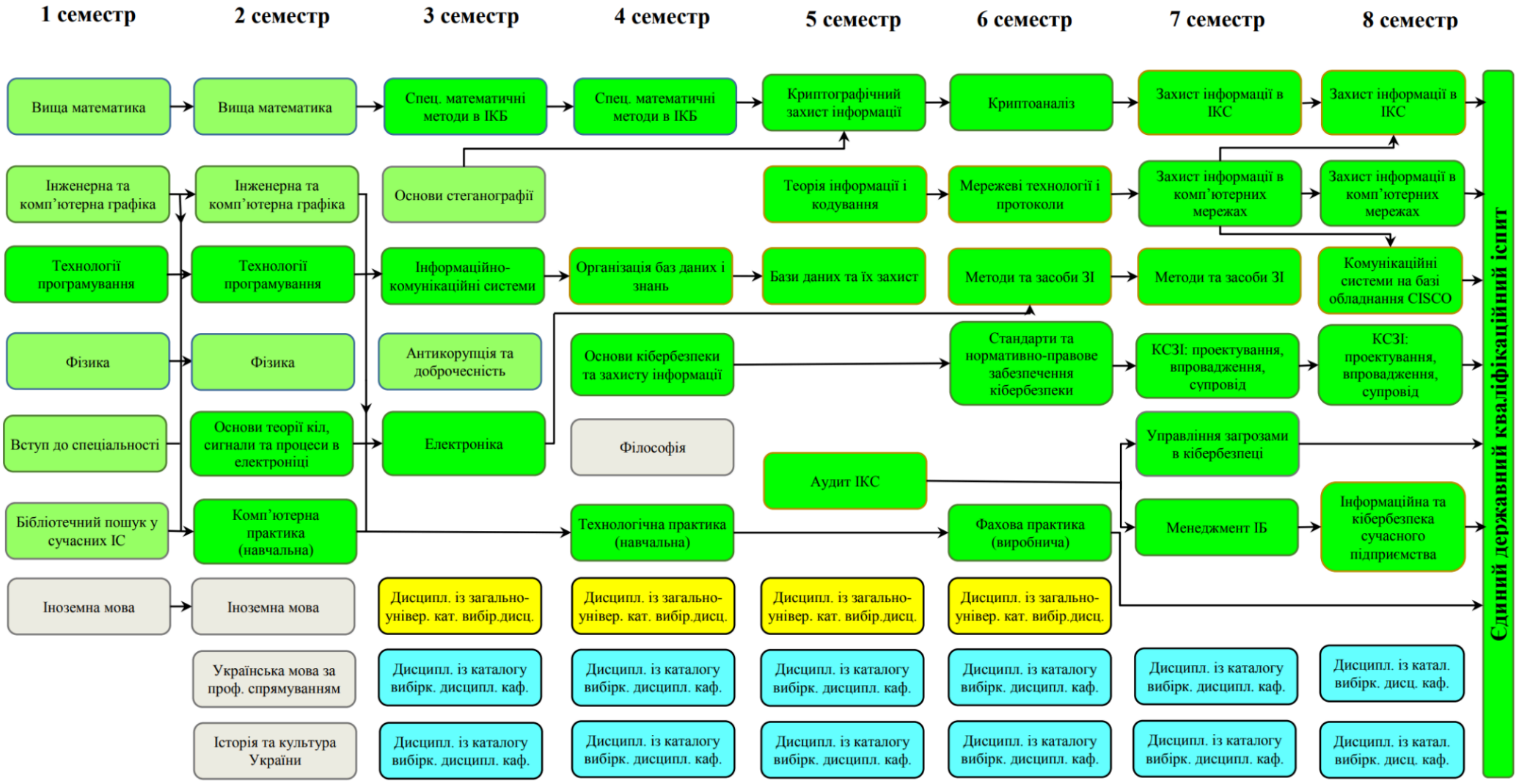
2.1. Перелік компонентів освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	**2**	**3**	**4**
Обов'язкові компоненти ОПП			
ОК1	Іноземна мова	6	Залік, іспит
ОК2	Історія та культура України	3	Залік
ОК3	Українська мова за професійним спрямуванням	3	Залік
ОК4	Вступ до спеціальності	3	Залік
ОК5	Фізика	7	Іспит, залік
ОК6	Вища математика	7	Іспит
ОК7	Бібліотечний пошук у сучасних інформаційних системах	3	Залік
ОК8	Антикорупція та доброчесність	3	Залік
ОК9	Технології програмування	11,5	Іспит
ОК10	Інженерна та комп'ютерна графіка	10,5	Залік
ОК11	Основи теорії кіл, сигнали та процеси в електроніці	3	Залік
ОК12	Філософія	3	Залік
ОК13	Спеціальні математичні методи в інформаційній та кібербезпеці	6	Іспит
ОК14	Основи стеганографії	4,5	Залік
ОК15	Інформаційно-комунікаційні системи	5,5	Іспит
ОК16	Електроніка	3	Іспит
ОК17	Основи кібербезпеки та захисту інформації	4	Іспит
ОК18	Організація баз даних і знань	3	Іспит
ОК19	Криптографічний захист інформації	6	Іспит
ОК20	Криптоаналіз	3	Іспит
ОК21	Мережеві технології і протоколи	3	Іспит

ОК22	Стандарти та нормативно-правове забезпечення кібербезпеки	3	Залік
ОК23	Бази даних та їх захист	3	Іспит
ОК24	Теорія інформації і кодування	6	Іспит
ОК25	Аудит інформаційно-комунікаційних систем	4	Іспит
ОК26	Методи та засоби захисту інформації	10	Іспит
ОК27	Управління загрозами в кібербезпеці	3	Іспит
ОК28	Захист інформації в інформаційно-комунікаційних системах	6,5	Іспит
ОК29	Комплексні системи захисту інформації: проектування, впровадження, супровід	10	Залік, іспит
ОК30	Захист інформації в комп'ютерних мережах	6,5	Іспит
ОК31	Менеджмент інформаційної безпеки	3	Залік
ОК32	Комунікаційні системи на базі обладнання CISCO	3	Залік
ОК33	Інформаційна та кібербезпека сучасного підприємства	6	Залік
ОК34	Комп'ютерна практика (навчальна)	3	Диференційований залік
ОК35	Технологічна практика (навчальна)	6	Диференційований залік
ОК36	Фахова практика (виробнича)	6	Диференційований залік
ОК37	Єдиний державний кваліфікаційний іспит		Іспит
Загальний обсяг обов'язкових компонентів:		**180 кредитів**	
Вибіркові компоненти ОПП			
ВК1	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік

ВК2	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
ВК3	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
ВК4	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
ВК5	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК6	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК7	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК8	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК9	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК10	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК11	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК12	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК13	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК14	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК15	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК16	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
Загальний обсяг вибіркових компонентів:		**60 кредитів**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ:		**240 кредитів**	

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Атестація здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації в межах освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» здійснюється у формі єдиного державного кваліфікаційного іспиту (ЄДКІ). За умови успішного проходження атестації університет видає документ встановленого зразка про присудження ступеня бакалавра із присвоєнням освітньої кваліфікації: бакалавр з кібербезпеки та захисту інформації.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 Кібербезпека та захист інформації, а також освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем».

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	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**
ЗК1					+	+	+		+										+		+			+		+	+		+	+	+	+	+	+	+	+
ЗК2					+				+							+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК3			+						+																											+
ЗК4	+		+		+											+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+			+
ЗК5			+		+		+		+	+	+	+	+	+			+		+		+	+			+		+		+	+	+						+
ЗК6		+	+		+			+																													+
ЗК7								+																													+
ЗК8				+				+				+			+																						+
ФК1					+				+					+		+		+					+	+	+	+	+	+									+

ФК2					+				+					+		+		+					+		+	+	+	+									+
ФК3											+													+												+
ФК4					+									+		+		+				+			+	+	+	+								+
ФК5													+								+	+									+			+		+	+	+
ФК6																+									+		+		+				+				+	+
ФК7																			+						+		+	+			+					+	+	+
ФК8															+										+	+	+		+						+			+
ФК9														+								+			+		+		+				+					+
ФК10									+							+		+							+	+	+	+							+			+

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

	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**
ПРН1			+	+					+													+					+										+
ПРН2	+		+						+							+			+				+				+				+				+	+	+
ПРН3									+					+			+					+						+		+			+		+	+	+
ПРН4			+																		+				+						+				+	+	+
ПРН5																	+			+							+		+					+			+
ПРН6																+						+				+		+				+					+
ПРН7																					+				+				+						+	+	+
ПРН8																			+					+		+				+		+			+	+	+
ПРН9																+				+										+			+		+	+	+

ПРН10																		+	+			+		+		+			+		+			+		+
ПРН11																+				+			+				+	+			+	+				+
ПРН12															+		+				+			+										+		+
ПРН13																		+			+	+	+			+		+	+				+	+	+		+
ПРН14																			+												+				+		+
ПРН15																					+	+		+												+	+
ПРН16					+					+		+			+				+				+		+		+	+			+		+			+	+
ПРН17														+									+	+	+				+				+			+	+
ПРН18															+				+		+		+														+
ПРН19			+			+			+															+	+	+				+							+	+
ПРН20																+				+											+				+		+	+
ПРН21																		+	+			+		+			+		+			+		+			+	+