ПРОЄКТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

першого (бакалаврського) рівня вищої освіти

галузі знань ***F Інформаційні технології***
спеціальності ***F5 Кібербезпека та захист інформації***
освітня кваліфікація ***Бакалавр з кібербезпеки та захисту інформації***

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради
_____ Володимир ОНИЩЕНКО
(протокол № ___ від «___» _____ 2025 р.)

Освітньо-професійна програма вводиться в дію з 01.09.2025

Ректор _____ Володимир ОНИЩЕНКО
(наказ № ___ від «___» _____ 2025 р.)

Полтава, 2025

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

«КІБЕРБЕЗПЕКА»

РІВЕНЬ ВИЩОЇ ОСВІТИ	*Перший (бакалаврський) рівень*
СТУПІНЬ ВИЩОЇ ОСВІТИ	*Бакалавр*
ГАЛУЗЬ ЗНАНЬ	*F Інформаційні технології*
СПЕЦІАЛЬНІСТЬ	*F5 Кібербезпека та захист інформації*
ОСВІТНЯ КВАЛІФІКАЦІЯ	*Бакалавр з кібербезпеки та захисту інформації*

ПОГОДЖЕНО
Проректор з науково-педагогічної та навчальної роботи

_____ Анатолій МАРТИНЕНКО
«____» _____ 2025 р.

ПОГОДЖЕНО
Директор департаменту організації навчального процесу, акредитації та ліцензування

_____ Олег МАКСИМЕНКО
«____»_____2025 р.

РЕКОМЕНДОВАНО
Вченою радою
Навчально-наукового інституту інформаційних технологій та робототехніки
Протокол № __ від «__» _____ 2025 р.
Голова вченої ради інституту
_____ Володимир ПЕНЦ

СХВАЛЕНО
Навчально-методичною комісією
Навчально-наукового інституту інформаційних технологій та робототехніки
Протокол № __ від «__» _____ 2025 р.
Голова НМК інституту
_____ Олександр ШЕФЕР

СХВАЛЕНО
Кафедрою комп'ютерних та інформаційних технологій і систем
Протокол № __ від «__» _____ 2025 р.
Завідувач кафедри
_____ Олена ДВІРНА

РОЗРОБЛЕНО
Проєктною (робочою) групою,
Керівник проєктної (робочої) групи,
гарант освітньо-професійної програми
_____ Юрій ЗДОРЕНКО
«____» _____ 2025 р.

ПЕРЕДМОВА

Освітньо-професійна програма розроблена відповідно до Стандарту вищої освіти України першого (бакалаврського) рівня вищої освіти, галузь знань – F Інформаційні технології, спеціальність F5 Кібербезпека та захист інформації, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 04.10.2018 № 1074 (зі змінами внесеними наказом Міністерства освіти і науки України від 29.10.2024 № 1547) з врахуванням постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1392.

Програму розроблено проєктною (робочою) групою у складі:

Керівник проєктної (робочої) групи:

Здоренко Юрій Миколайович – гарант освітньої програми, доцент кафедри комп'ютерних та інформаційних технологій і систем, кандидат технічних наук;

Члени проєктної (робочої) групи:

Головко Геннадій Вячеславович – доцент кафедри комп'ютерних та інформаційних технологій і систем, кандидат технічних наук, доцент;

Янко Аліна Сергіївна – доцент кафедри комп'ютерних та інформаційних технологій і систем, кандидат технічних наук, доцент

До розробки освітньої програми були долучені:

Ковтун В.В. – керівник навчального центру Software Development Services

Шейко І.О. – директор IT-компанії DIGI CODE

Треумов Д.О. –SEO-спеціаліст компанії IST GrouP

Зовнішні рецензенти:

1. NIXSOLUTIONS, м. Харків
2. Partizan Security Global
3. Харківський IT-кластер

1. Профіль освітньо-професійної програми зі спеціальності F5 Кібербезпека та захист інформації

1.1. Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Полтавська політехніка імені Юрія Кондратюка»; Навчально-науковий інститут інформаційних технологій та робототехніки; Кафедра комп'ютерних та інформаційних технологій і систем
Рівень вищої освіти	Перший (бакалаврський) рівень вищої освіти
Ступінь вищої освіти	Бакалавр
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Назва освітньої програми	Кібербезпека
Інтернет-адреса розміщення освітньої програми	https://nupp.edu.ua/page/litsenzuvannya-ta-akreditatsiya.html
Форми навчання	Денна
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – «Кібербезпека»
Опис предметної області	**Об'єкт(и) вивчення та діяльності:** технології кібербезпеки та захисту інформації; процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання:** підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст складають** принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації.

	Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
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.
Обсяг кредитів за Європейською кредитно-трансферною системою, необхідний для здобуття відповідного ступеня вищої освіти	240 кредитів ЄКТС Термін навчання – 3 роки, 10 місяців
Наявність акредитації	Акредитується вперше
Цикл / рівень	НРК України – 6 рівень, QF-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта (3 рівень НРК) або вищий рівень
Мова(и) викладання	Українська мова
Термін дії освітньої програми	Термін дії освітньої програми – до 30.06.2029
1.2. Мета освітньої програми	
Мета освітньої програми	Мета освітньої програми полягає в підготовці фахівців, здатних вирішувати складні спеціалізовані задачі та практичні проблеми забезпечення інформаційної безпеки та захисту інформаційної та кібернетичної безпеки держави
1.3. Характеристика освітньої програми	
Орієнтація освітньої програми	Освітньо-професійна програма має прикладну орієнтацію і спрямована на вирішенні спеціалізованих та практичних задач з кібербезпеки та захисту інформації.
Основний фокус освітньої програми	Загальна вища освіта в галузі інформаційних технологій, спрямованих на розв’язання задач забезпечення кібернетичної безпеки, набуття професійних навичок фахівця із захисту даних. Акцент на формуванні вмінь застосовувати технології й програмно-технічні засоби проєктування, реалізації, впровадження й супроводження програмних засобів різного призначення, комп’ютерних систем і мереж з врахуванням вимог кібербезпеки та реалізації комплексних систем захисту інформації.

	Ключові слова: кібербезпека, комп'ютерні системи, комп'ютерні мережі, програмування, захист програмного забезпечення, інформаційно-комунікаційні технології, інформаційна безпека, захист інформації
Особливості та відмінності програми	Характерною особливістю даної програми є надання можливості поглибленого вивчення дисциплін, присвячених інформаційній та кібербезпеці, поглиблено вивчати іноземну мову протягом усього терміну навчання. Студенти мають можливість вибудувати унікальну індивідуальну освітню траєкторію шляхом вибору навчальних дисциплін та поглиблювати знання, обираючи один з двох мейджорів – «Захист корпоративних мереж» або «Блокчейн та безпека банківських систем». Здобувачі вищої освіти за цією освітньою програмою мають можливість брати участь в програмах міжнародної академічної мобільності (тривалістю 1 або 2 семестри).
1.4. Придатність випускників освітньої програми до працевлаштування	
Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України (ДК 003:2010): 2139 – фахівець з реагування на інциденти кібербезпеки, 2139 – фахівець з підтримки інфраструктури кіберзахисту, 2139 – фахівець з технічного захисту інформації, 2139 – фахівець з криптографічного захисту інформації, 2139 – фахівець з тестування систем захисту інформації, 2139 – фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139 – фахівець сфери захисту інформації, 2139 – адміністратор безпеки мереж і систем, 2139 – фахівець з питань безпеки (інформаційно-комунікаційні технології), 3439 – фахівець із організації інформаційної безпеки, 3439 – фахівець із організації захисту інформації з обмеженим доступом, 3439 – фахівець з режиму секретності, 3439 – інспектор з організації захисту секретної інформації
1.5. Викладання та оцінювання	
Викладання та навчання	Проведення лекційних, практичних та лабораторних занять, організація майстер-класів, наукових конференцій та семінарів; залучення студентів до участі в проєктних роботах, конкурсах, олімпіадах та науково-дослідних заходах. Залучення до проведення занять кваліфікованих фахівців-практиків. Самостійна робота (підготовка презентацій, рефератів, розрахункових та курсових робіт, підготовка до складання Єдиного державного кваліфікаційного іспиту). Застосовуються інноваційні технології дистанційного

	навчання з використанням онлайн-платформ для проведення занять.
Оцінювання	**Форми контролю:** письмові екзамени (тестування, вирішення проблемних завдань, розв'язання певної прикладної задачі), усне екзаменування, диф. заліки, проміжні контрольні роботи та опитування, презентації, звіти з практик, публічний захист курсових робіт, складання Єдиного державного кваліфікаційного іспиту. **Види контролю:** поточний та підсумковий контроль **Шкала оцінювання:** оцінювання здійснюється за 100-бальною (рейтинговою) шкалою, шкалою ЄКТС (ECTS), (A, B, C, D, E, FX, F), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно»).
1.6. Програмні компетентності	
Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професійної діяльності. КЗ 3. Здатність спілкуватися державною мовою як усно, так і письмово. КЗ 4. Здатність спілкуватися іноземною мовою. КЗ 5. Здатність вчитися і оволодівати сучасними знаннями. КЗ 6. 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. КЗ 7. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. КЗ 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 (СК)	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності. КФ 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

	КФ 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки й захисту інформації. КФ 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах встановленої політики кібербезпеки та захисту інформації. КФ 5. Здатність відновлювати функціонування інформаційних, інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо. КФ 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. КФ 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. КФ 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. КФ 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

1.7. Програмні результати (ПР)

РН 1 Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків;
РН 2 Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації;
РН 3 Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності;
РН 4 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;
РН 5 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;
РН 6 Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат;

РН 7 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;
РН 9 Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації;
РН 10 Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності;
РН 11 Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації;
РН 12 Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки;
РН 13 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;
РН 14 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;
РН 15 Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи;
РН 16 Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;
РН 17 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;
РН 18 Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності;
РН 19 Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів;
РН 20 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; РН 21 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.	
1.8. Ресурсне забезпечення реалізації програми	
Основні характеристики кадрового забезпечення	До реалізації освітньої програми залучені науково-педагогічні працівники, з яких 87% мають вчені звання та/або наукові ступені. До викладання професійно-орієнтованих дисциплін залучаються викладачі-практики. Частка лекційних годин науково-педагогічних працівників з практичним досвідом роботи складає більше 16%. Освітня та/або професійна кваліфікація науково-педагогічних працівників, що залучені до реалізації освітніх компонентів освітньої програми, повністю відповідає вимогам Ліцензійних умов провадження освітньої діяльності, затверджених постановою Кабінету Міністрів України від 30.12.2015 р. №1187 (в редакції постанови Кабінету Міністрів України від 24.03.2021 №365)
Основні характеристики матеріально-технічного забезпечення	Використання лекційних аудиторій, обладнаних мультимедійною технікою; навчальних аудиторій для проведення практичних та лабораторних занять з використанням персональних комп'ютерів; спеціалізованих навчальних лабораторій Lenovo, Dell, Asus, HP, Cisco.
Основні характеристики інформаційного та навчально-методичного забезпечення	Усі освітні компоненти забезпечені навчально-методичними розробками науково-педагогічних працівників університету – методичними вказівками, навчальними посібниками або підручниками. Навчальні матеріали з кожного освітнього компонента освітньої програми розміщені на платформі дистанційного навчання Moodle. Студенти отримують повний доступ до електронної бібліотеки університету. Індивідуальний навчальний план та персональний розклад занять доступні в особистому електронному кабінеті студента.
1.9. Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність може здійснюватися відповідно до угод Національного університету «Полтавська політехніка імені Юрія Кондратюка» у закладах вищої освіти (наукових установах) – партнерах Національного університету «Полтавська політехніка імені Юрія Кондратюка» в межах України та згідно з Положенням про порядок реалізації права здобувачів вищої освіти Національного університету «Полтавська політехніка імені Юрія Кондратюка» на

	академічну мобільність. https://nupp.edu.ua/uploads/files/0/doc/polozhennia/akademichna-mobilnist.pdf
Міжнародна кредитна мобільність	Може реалізовуватися здобувачами вищої освіти відповідно до укладених угод Національного університету «Полтавська політехніка імені Юрія Кондратюка» та угоди (Еразмус+К1) у закладах вищої освіти (наукових установах) – партнерах поза межами України та згідно з Положенням про порядок реалізації права здобувачів вищої освіти Національного університету «Полтавська політехніка імені Юрія Кондратюка» на академічну мобільність. https://nupp.edu.ua/uploads/files/0/doc/polozhennia/akademichna-mobilnist.pdf
Навчання іноземних здобувачів вищої освіти	Навчання іноземних студентів може здійснюватися згідно з вимогами чинного законодавства

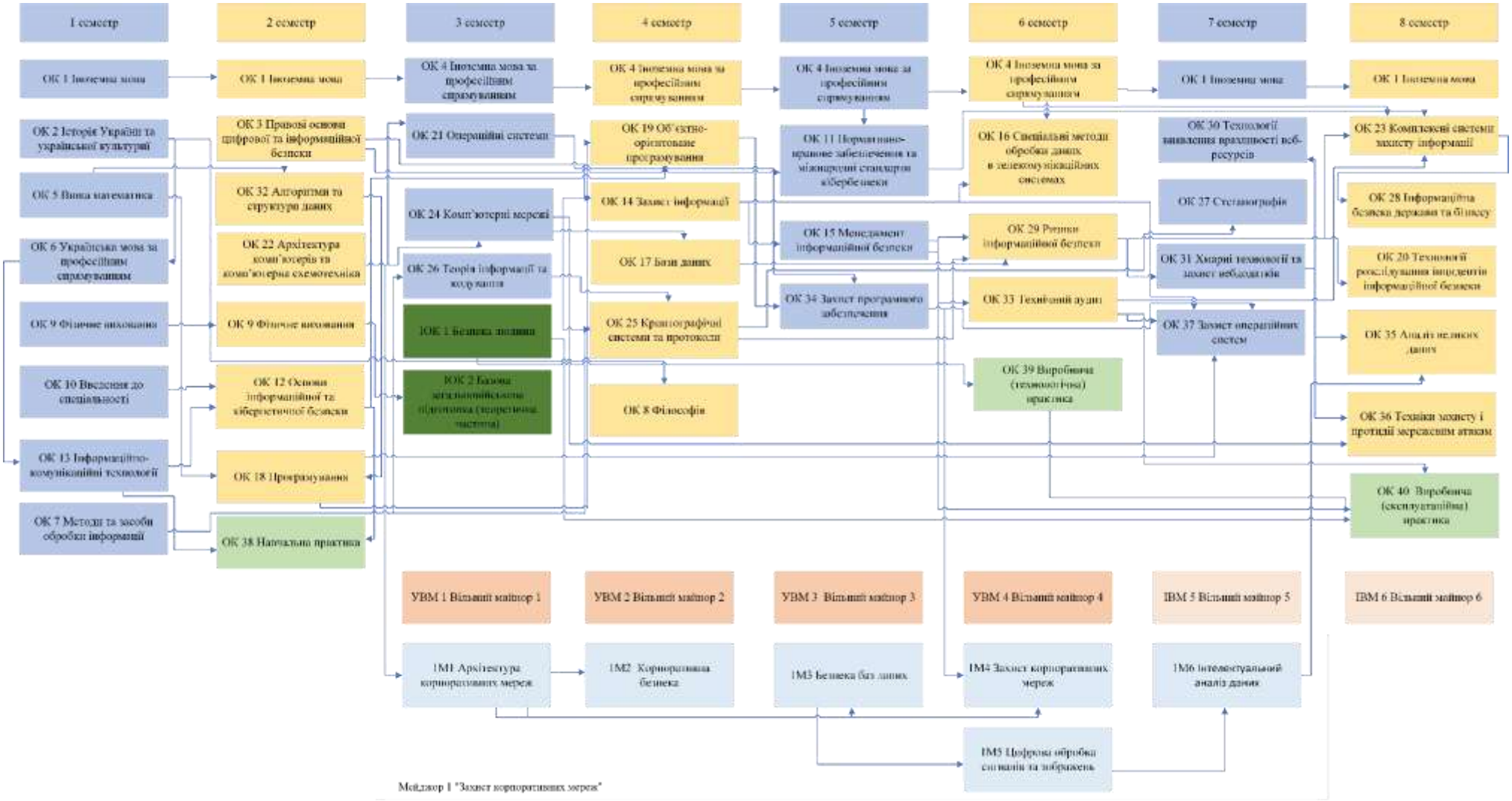
2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент освітньо-професійної програми

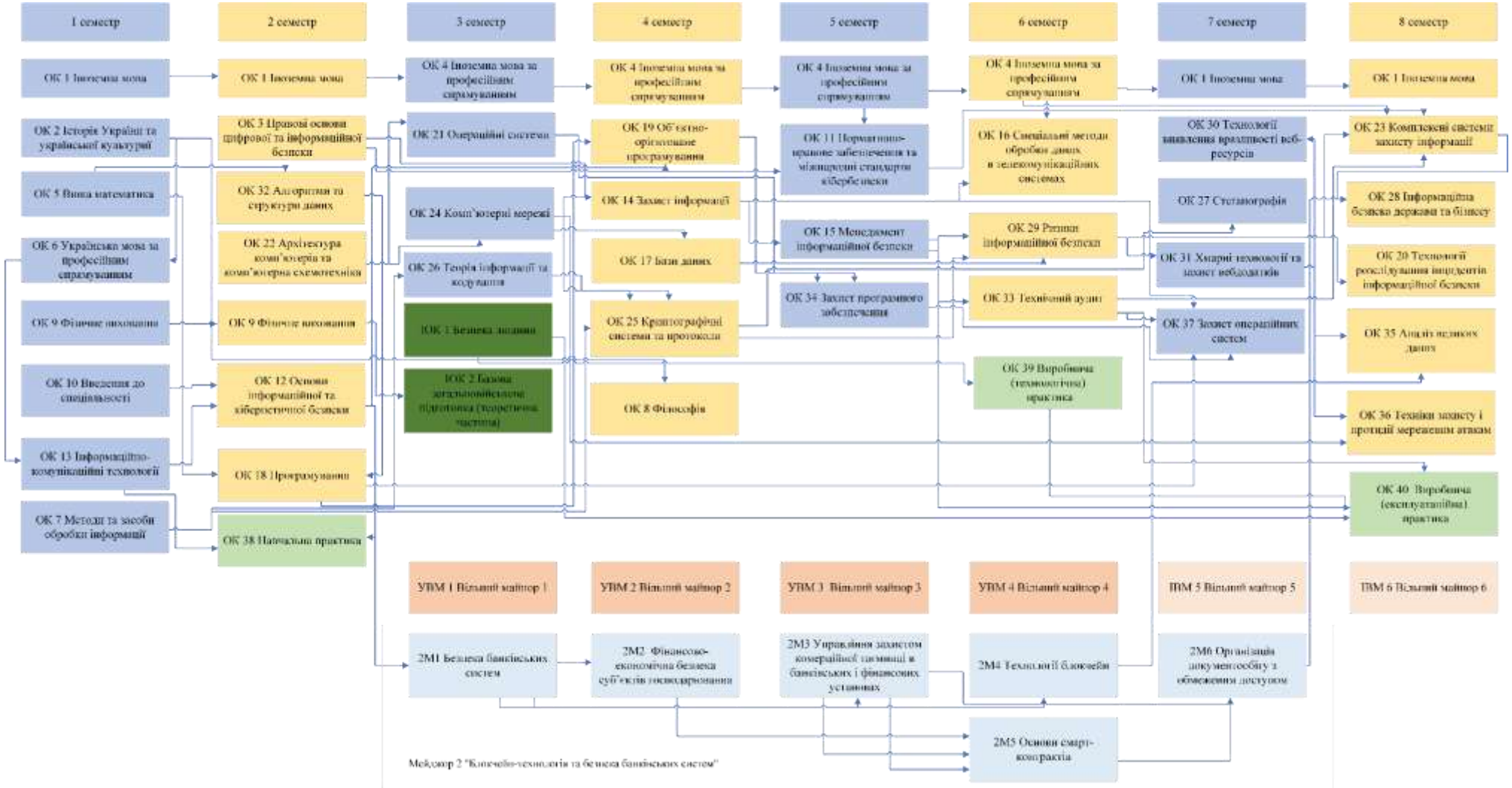
Код о/к	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
І. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОК 1.	Іноземна мова	8	екзамен
ОК 2	Історія України та української культури	3	екзамен
ОК 3	Правові основи цифрової та інформаційної безпеки	4	диф. залік
ОК 4.	Іноземна мова за професійним спрямуванням	8	екзамен
ОК 5.	Вища математика	6	екзамен
ОК 6.	Українська мова за професійним спрямуванням	3	екзамен
ОК 7	Методи та засоби обробки інформації	4	диф. залік
ОК 8	Філософія	3	екзамен
ОК 9	Фізичне виховання	4	диф. залік
Загальний обсяг обов'язкових компонент загальної підготовки:		**43**	
ІІ. ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОК 10	Введення до спеціальності	3	екзамен
ОК 11	Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки	5	екзамен
ОК 12	Основи інформаційної та кібернетичної безпеки	5	екзамен
ОК 13	Інформаційно-комунікаційні технології	4	диф. залік
ОК 14	Захист інформації	4	КР, екзамен
ОК 15	Менеджмент інформаційної безпеки	5	екзамен
ОК 16	Спеціальні методи обробки даних в телекомунікаційних системах	3	екзамен
ОК 17	Бази даних	5	екзамен
ОК 18	Програмування	6	екзамен
ОК 19	Об'єктно-орієнтоване програмування	5	екзамен
ОК 20	Технології розслідування інцидентів інформаційної безпеки	4	екзамен
ОК 21	Операційні системи	4	екзамен
ОК 22	Архітектура комп'ютерів та комп'ютерна схемотехніка	5	екзамен
ОК 23	Комплексні системи захисту інформації	5	КР, екзамен
ОК 24	Комп'ютерні мережі	4	КР, екзамен
ОК 25	Криптографічні системи та протоколи	4	диф. залік
ОК 26	Теорія інформації та кодування	4	екзамен
ОК 27	Стеганографія	4	екзамен
ОК 28	Інформаційна безпека держави та бізнесу	4	екзамен
ОК 29	Ризики інформаційної безпеки	3	екзамен
ОК 30	Технології виявлення вразливості веб-ресурсів	3	диф. залік
ОК 31	Хмарні технології та захист вебдодатків	4	екзамен
ОК 32	Алгоритми та структури даних	6	диф. залік
ОК 33	Технічний аудит	3	КР,екзамен
ОК 34	Захист програмного забезпечення	5	КР,екзамен
ОК 35	Аналіз великих даних	4	диф. залік
ОК 36	Техніки захисту і протидії мережевим атакам	4	диф. залік
ОК 37	Захист операційних систем	4	диф. залік
ОК 38	Навчальна практика	3	диф. залік

ОК 39	Виробнича (технологічна) практика	6	диф. залік
ОК 40	Виробнича (експлуатаційна) практика	6	диф. залік
Загальний обсяг обов'язкових компонент професійної підготовки:		**134**	
Загальний обсяг обов'язкових компонент загальної та професійної підготовки:		**177**	
ВИБІРКОВІ КОМПОНЕНТИ			
І. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
УВМ1	Вільний майнор 1	4	диф. залік
УВМ 2	Вільний майнор 2	4	диф. залік
УВМ 3	Вільний майнор 3	4	диф. залік
УВМ 4	Вільний майнор 4	4	диф. залік
Загальний обсяг вибіркових компонент загальної підготовки:		**16**	
ІІ. ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ІВМ1	Вільний майнор 5	4	
ІВМ2	Вільний майнор 6	4	
Мейджор 1 «Захист корпоративних мереж» (Блок вибіркових дисциплін №1 за освітньою програмою)			
1 ММ 1	Архітектура корпоративних мереж	6	диф. залік
1 ММ 2	Корпоративна безпека	6	диф. залік
1 ММ 3	Безпека баз даних	6	диф. залік
1 ММ 4	Захист корпоративних мереж	6	диф. залік
1 ММ 5	Цифрова обробка сигналів та зображень	6	диф. залік
1 ММ 6	Інтелектуальний аналіз даних	6	диф. залік
Мейджор 2 «Блокчейн-технологія та безпека банківських систем» (Блок вибіркових дисциплін №2 за освітньою програмою)			
2 ММ 1	Безпека банківських систем	6	диф. залік
2 ММ 2	Фінансово-економічна безпека суб'єктів господарювання	6	диф. залік
2 ММ 3	Управління захистом комерційної таємниці в банківських і фінансових установах	6	диф. залік
2 ММ 4	Технології блокчейн	6	диф. залік
2 ММ 5	Основи смарт-контрактів	6	диф. залік
2 ММ 6	Організація документообігу з обмеженим доступом	6	диф. залік
Мейджор 3 «Кібербезпека об'єктів критичної інфраструктури» (Блок вибіркових дисциплін №3 за освітньою програмою)			
3 ММ 1	Безпека об'єктів критичної інфраструктури	6	диф. залік
3 ММ 2	Системи електронного документообігу	6	диф. залік
3 ММ 3	Управління ризиками інформаційної безпеки	6	диф. залік
3 ММ 4	Нормативно-правове забезпечення інформаційної безпеки об'єктів критичної інфраструктури	6	диф. залік
3 ММ 5	Спеціальні та інтелектуальні системи інформаційної безпеки	6	диф. залік
3 ММ 6	Технічний захист інформації на об'єктах критичної інфраструктури	6	диф. залік
Загальний обсяг вибіркових компонент професійної підготовки:		**44**	
Загальний обсяг вибіркових компонент загальної та професійної підготовки		**60**	
ІНШІ ОСВІТНІ КОМПОНЕНТИ			
ІОК1	Безпека людини	**3**	диф. залік
ІОК2	Базова загальновійськова підготовка		
ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		**240**	

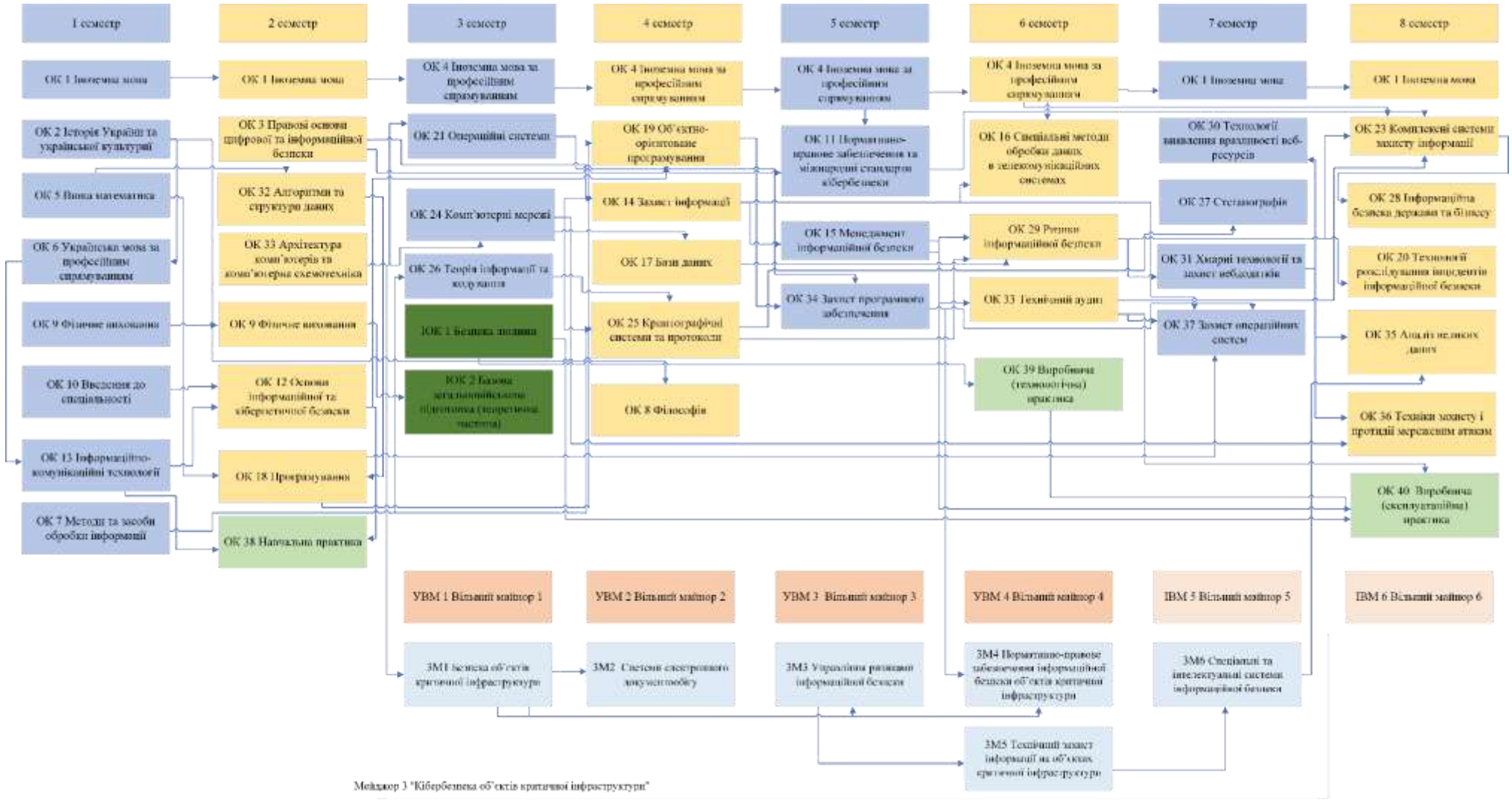
2.2. Структурно-логічна схема ОП (індивідуальна освітня траєкторія за мейджором 1 «Захист корпоративних мереж»)



2.2. Структурно-логічна схема ОП (індивідуальна освітня траєкторія за мейджором 2 «Блокчейн-технологія та безпека банківських систем»)



2.3. Структурно-логічна схема ОП (індивідуальна освітня траєкторія за мейджором 3 «Кібербезпека об’єктів критичної інфраструктури»)



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ІК	КЗ 1.	КЗ 2.	КЗ 3.	КЗ 4	КЗ 5.	КЗ 6.	КЗ 7.	КЗ 8.	КФ 1.	КФ 2.	КФ 3.	КФ 4.	КФ 5.	КФ 6.	КФ 7.	КФ 8.	КФ 9.	КФ 10.
ОК 1	*	*		*	*														
ОК 2	*						*		*										
ОК 3	*	*					*	*		*					*				
ОК 4	*	*		*	*														
ОК 5	*	*															*		
ОК 6	*	*		*	*														
ОК 7	*					*									*				
ОК 8	*						*		*										
ОК 9	*								*										
ОК 10	*		*				*	*	*	*									
ОК 11	*	*					*	*		*					*				
ОК 12	*		*																*
ОК 13	*		*								*								
ОК 14	*	*	*									*	*						
ОК 15	*											*		*	*	*			
ОК 16	*																		*
ОК 17	*		*			*													
ОК 18	*	*				*													
ОК 19	*			*	*														*
ОК 20	*		*			*				*		*		*					
ОК 21	*			*	*														*
ОК 22	*													*					*
ОК 23	*	*	*								*	*			*			*	
ОК 24	*	*									*								*
ОК 25	*		*										*				*		
ОК 26	*												*				*		
ОК 27	*		*														*		
ОК 28	*		*							*									*
ОК 29	*		*			*						*							*
ОК 30	*					*													
ОК 31	*					*											*		
ОК 32	*	*				*													
ОК 33	*	*				*													*
ОК 34	*	*											*			*	*	*	*
ОК 35	*					*													*
ОК 36	*		*										*	*		*		*	
ОК 37	*		*										*			*		*	
ОК 38	*	*																	
ОК 39	*	*																	
ОК 40	*	*																	
ІОК 1	*	*					*		*										

5. Матриця відповідності програмним результатів компонентам освітньої програми

	ПРН 1	ПРН 2	ПРН 3	ПРН 4	ПРН 5	ПРН 6	ПРН 7	ПРН 8	ПРН 9	ПРН 10	ПРН 11	ПРН 12	ПРН 13	ПРН 14	ПРН 15	ПРН 16	ПРН 17	ПРН 18	ПРН 19	ПРН 20	ПРН 21
ОК 1	*	*					*	*	*												
ОК 2			*																		
ОК 3			*						*												
ОК 4	*	*					*	*	*												
ОК 5										*											
ОК 6	*	*	*																		
ОК 7					*																
ОК 8			*																		
ОК 9				*		*	*	*													
ОК 10						*															
ОК 11					*	*			*						*	*					
ОК 12									*						*						*
ОК 13										*											
ОК 14				*								*						*	*		*
ОК 15				*	*						*	*		*				*			
ОК 16																					
ОК 17																					
ОК 18																					
ОК 19																					
ОК 20					*										*						
ОК 21															*						*
ОК 22										*											
ОК 23				*										*	*	*	*			*	
ОК 24				*																	
ОК 25																			*		
ОК 26																			*		
ОК 27																			*		
ОК 28											*										
ОК 29											*	*			*		*	*		*	
ОК 30															*						
ОК 31																					*
ОК 32																					
ОК 33				*																*	
ОК 34				*									*								*
ОК 35																					
ОК 36													*							*	*
ОК 37																					*
ОК 38																	*				
ОК 39																	*				
ОК 40							*	*									*				
ІОК 1			*			*	*	*													