МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНЖЕНЕРІЇ ТА УПРАВЛІННЯ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ»

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА

Освітньо-професійний ступінь: Фаховий молодший бакалавр

за спеціальністю: 125 Кібербезпека

галузі знань: 12 Інформаційні технології

кваліфікація: Фаховий молодший бакалавр з кібербезпеки

Затверджено Педагогічною радою
Протокол № 5 від 30 червня 2021 р.
Голова Педагогічної ради
_____ Олександр ПОНОМАРЕНКО

КИЇВ
2021

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	**Повна назва закладу освіти та структурного підрозділу**	Відокремлений структурний підрозділ «Фаховий коледж інженерії та управління Національного авіаційного університету»
1.2.	**Ступінь освіти та назва кваліфікації мовою оригіналу**	Фахова перед вища освіта Фаховий молодший бакалавр з кібербезпеки
1.3.	**Офіційна назва освітньо-професійної програми**	**КІБЕРБЕЗПЕКА**
1.4.	**Тип диплому та обсяг освітньо-професійної програми**	Диплом фахового молодшого бакалавра, одиничний, 180 кредитів ЄКТС, термін навчання 3 роки 10 місяців
1.5.	**Наявність акредитації**	-
1.6.	**Цикл/рівень**	НРК України – 5 рівень, ЄРК – 5 рівень, РК ЄПВО – короткий цикл
1.7.	**Передумови**	Повна загальна середня освіта
1.8.	**Мова(и) викладання**	Українська
1.9.	**Термін дії освітньо-професійної програми**	
1.10	**Інтернет-адреса постійного розміщення опису освітньо-професійної програми**	www.kitu.nau.edu.ua
Розділ 2. Опис предметної області		
2.1.	***Об'єкти професійної діяльності випускників:*** –об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; –технології забезпечення безпеки інформації; –процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. ***Цілі навчання:*** підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. ***Теоретичний зміст предметної області.*** Знання: – 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; –теорії систем управління інформаційною та/або кібербезпекою; –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; –автоматизованих систем проектування. ***Методи, методики та технології:*** Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. ***Інструменти та обладнання:*** –системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; –сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	**Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))**	Галузь знань 12 Інформаційні технології, Спеціальність 125 Кібербезпека
3.2.	**Орієнтація освітньо-професійної програми**	Освітньо-професійна програма фахового молодшого бакалавра, прикладна орієнтація.
3.3.	**Основний фокус освітньо-професійної програми та спеціалізації**	Спеціальна освіта в галузі інформаційних технологій
3.4.	**Особливості освітньо-професійної програми**	Вимагає спеціальної практики
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	**Придатність до працевлаштування**	Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки 2131.2 – Адміністратор бази даних 2131.2 – Адміністратор даних 2131.2 – Адміністратор доступу International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
4.2.	**Академічні права випускників**	Продовження навчання за початковим (короткий цикл) або першим (бакалаврський) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
Розділ 5. Викладання та оцінювання		
5.1.	**Викладання та навчання**	Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції,

		інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка кваліфікаційної роботи молодшого спеціаліста (проекту).
5.2.	**Оцінювання**	Письмові екзамени, практика, есе, презентації, поточний контроль, проектна робота, захист дипломного проекту.
Розділ 6. Програмні компетентності		
6.1.	**Інтегральна компетентність (ІК)**	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки і кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
6.2.	**Загальні компетентності (ЗК)**	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК 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. ЗК 7. 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. ЗК 8. Здатність вчитися і оволодівати сучасними знаннями. ЗК 9. Навички використання інформаційних і комунікаційних технологій.

		ЗК 10. Здатність працювати в команді. ЗК 11. Здатність діяти на основі етичних міркувань (мотивів), прагнення до збереження навколишнього середовища. ЗК 12. Здатність діяти соціально відповідально та свідомо.
6.3.	**Фахові компетентності (ФК)**	ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. ФК 5. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. ФК 10. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-

		телекомунікаційних (автоматизованих) систем. ФК 12. Знання теоретичних та практичних принципів та інструментальних засобів в професійній галузі та уміння їх застосовувати.
Розділ 7. Програмні результати навчання (ПРН)		
7.1.		ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність. ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 8. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН 9. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 10. Розробляти моделі загроз та порушника. ПРН 11. Аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 12. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень. ПРН 13. Реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН 14. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 15. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС. ПРН 16. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. ПРН 17. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки.

	ПРН 18. Здійснювати протидію отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 19. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 20. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН 21. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 22. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН 23. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 24. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 25. Здійснювати аналіз ризиків обробки інформації в ІТС. ПРН 26. Вирішувати задачі аналізу програмного коду на наявність можливих вразливостей.	
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	**Кадрове забезпечення**	Педагогічний склад, задіяний до викладання циклу дисциплін професійної підготовки
8.2.	**Матеріально-технічне забезпечення**	Матеріально-технічна база коледжу володіє достатнім аудиторним фондом. Освітній процес підготовки молодших спеціалістів з кібербезпеки забезпечується спеціалізованими кабінетами: інформаційної безпеки, мережевих технологій, програмування та спеціалізованими комп'ютерними лабораторіями: технологій програмування, мережевого обладнання та технологій, програмування для Інтернет, комп'ютерної графіки та інформаційних систем.
8.3	**Інформаційне та навчально-методичне забезпечення**	Використання електронної бібліотеки коледжу та авторських методичних розробок викладацького складу. Бібліотека КІтУ НАУ, бібліотека НАУ.

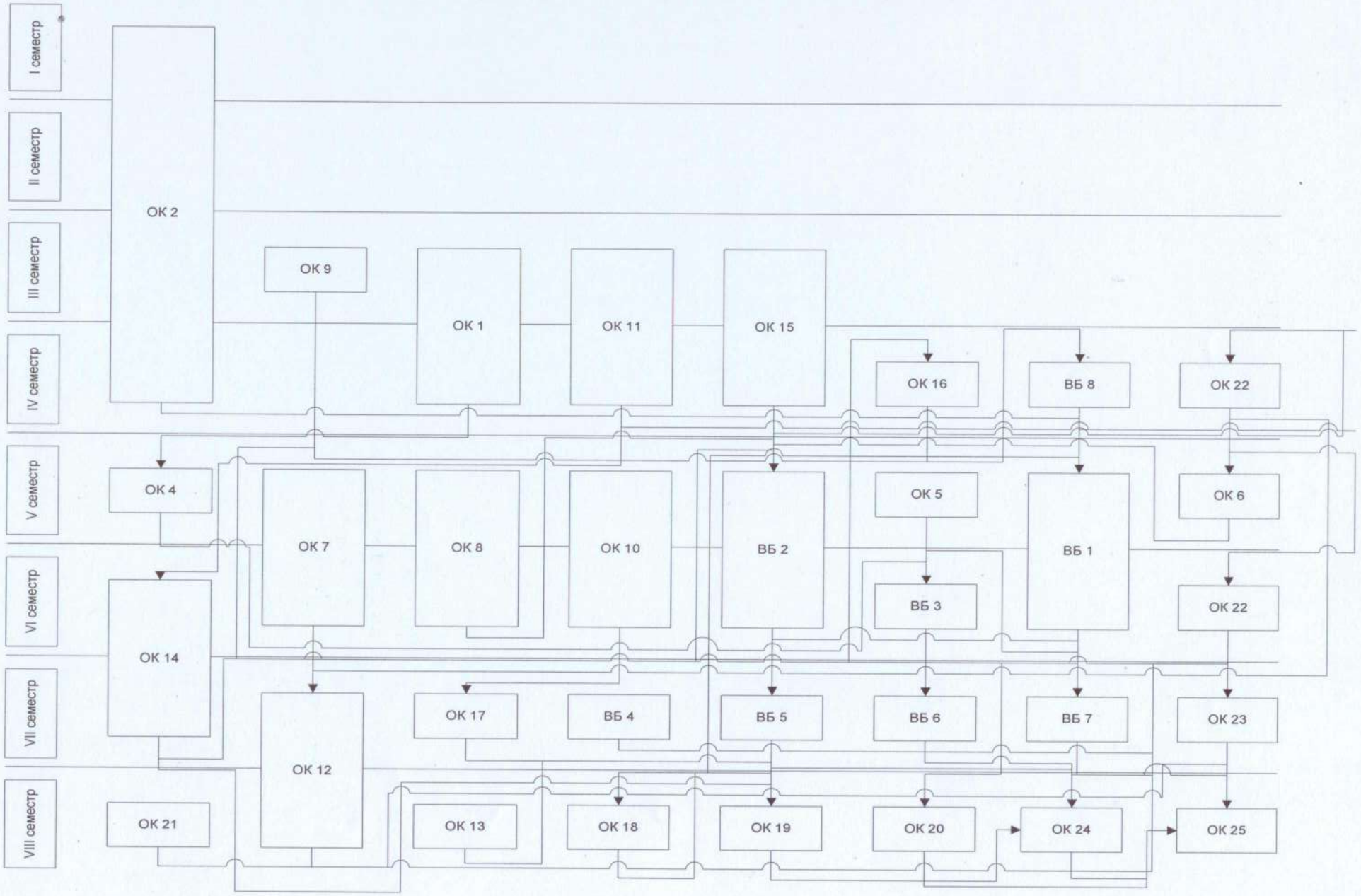
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю/КП, КР
1	2	3	4
Обов'язкові компоненти ОПП			
ОК1	Стандарти інформаційної безпеки	4	Екзамен
ОК2	Інформаційні технології та основи програмування	9	Екзамен
ОК3	Операційні системи та системне програмне забезпечення	6	Екзамен
ОК4	Основи інформаційної безпеки держави	4	Екзамен
ОК5	Історія та культура України	3	Залік
ОК6	Архітектура апаратного забезпечення комп`ютера	8	Екзамен/КР
ОК7	Комп`ютерна дискретна математика	6	Екзамен
ОК8	Вища математика	10	Екзамен
ОК9	Вища фізика	8	Залік
ОК10	Фізичне виховання	4	Залік
ОК11	Іноземна мова (за професійним спрямуванням)	6	Екзамен
ОК12	Українська мова (за професійним спрямуванням)	3	Залік
ОК13	Технології програмування	8	Екзамен/КП
ОК14	Основи системного аналізу	5	Екзамен
ОК15	Системи розмежування доступу	5	Залік
ОК16	Основи охорони праці та БЖД	3	Залік
ОК17	Захищені комп`ютерні системи та мережі	8	Екзамен/КП
ОК18	Управління ресурсами інформаційних систем	5	Екзамен
ОК19	Практика навчальна	7,5	Залік
ОК20	Практика технологічна	7,5	Залік
ОК21	Практика переддипломна (виробнича)	12	Залік
ОК22	Атестація (Кваліфікаційна робота)	1	
Загальний обсяг обов'язкових компонент:		**133**	
Вибіркові компоненти ОПП			
Вибірковий блок за вибором закладу освіти ВБ 1			
ВБ 1.1	Економікс	3	Залік
ВБ 1.2	Основи правознавства	3	Залік
ВБ 1.3	Інженерна та комп`ютерна графіка	4	Залік
ВБ 1.4	Філософія	3	Залік
ВБ 1.5	Бази даних	4	Залік
ВБ 1.6	Економіка в галузі інформаційної безпеки	4	Залік
ВБ 1.7	Соціологія	3	Залік
ВБ 1.8	Оцінка та управління ризиками	4	Залік
Загальний обсяг вибіркових компонент ВБ 1:		**28**	
Вибірковий блок за вибором здобувачів освіти ВБ 2			
ВБ 2.1	Інтернет-технології	4	Залік
ВБ 2.2	Технології штучного інтелекту	4	Залік
ВБ 2.3	Інформаційно-психологічні впливи у кіберпросторі	4	Залік

ВБ 2.4	Випробування систем захисту інформації	4	Залік
ВБ 2.5	Організація секретного діловодства	3	Залік
ВБ 2.6			
ВБ 2.7			
ВБ 2.8			
ВБ 2.9			
ВБ 2.10			
Загальний обсяг вибіркових компонент ВБ 2:		**19**	
Загальний обсяг вибіркових компонент:		**47**	
Загальний обсяг освітньо-професійної програми:		**180**	

2.2. Структурно-логічна схема ОПП



3. Форма атестації здобувачів освіти

Атестація випускників освітньо-професійної програми Кібербезпека спеціальності 125 Кібербезпека проводиться у формі публічного захисту (демонстрації) кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження освітнього ступеня фахового молодшого бакалавра із присвоєнням кваліфікації: фаховий молодший бакалавр з кібербезпеки за спеціальністю 125 Кібербезпека.

У кваліфікаційній роботі не може бути академічного плагіату, фальсифікації та списування.

Атестація здійснюється відкрито і публічно.