Проект
(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»
(найменування освітньо-професійної програми)

Першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)
галузі знань 12 Інформаційні технології
(шифр та найменування галузі)

СМЯ НАУ ОПП 09.01.09. – 03 – 2021

Освітньо-професійна програма
Затверджена Вченою радою Університету
Протокол №___ від_____2021 р.

Вводиться в дію наказом ректора
Ректор
_____ М. Луцький
Наказ №_____ від _____2021 р.

КИЇВ

Стандарт вищої освіти України: перший (бакалаврський) рівень,
галузь знань 12 Інформаціні технології,
спеціальність 125 Кібербезпека
Стандарт вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від «04» 10. 2018 р. № 1074.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО
Науково-методичною радою
Національного авіаційного університету
протокол №_____
від «_____»_____2021 р.
Голова Науково-методичної ради,
проректор з навчальної роботи
_____А. Полухін

ПОГОДЖЕНО
Вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії
протокол №_____
від «_____»_____20___ р.
Голова вченої ради факультету
_____ Нестеренко К.С.

ПОГОДЖЕНО
Кафедрою комп'ютеризованих систем захисту інформації
протокол засідання №_____
від «_____»_____20___ р.
Завідувач кафедри
_____ Казмірчук С.В.

ПОГОДЖЕНО
Студентською радою Факультету кібербезпеки, комп'ютерної та програмної інженерії
протокол №_____
від «_____»_____20___ р.
Голова студентської ради
_____

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності 125 «Кібербезпека) у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

Ільєнко Анна Вадимівна - к.т.н., доц., доцент кафедри комп'ютеризованих систем захисту інформації

підпис гаранта

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

Казмірчук Світлана Володимирівна - д.т.н., доц., завідувач кафедри комп'ютеризованих систем захисту інформації

підпис члена робочої групи

Єлізаров Анатолій Борисович - к.т.н., доц., доцент кафедри комп'ютеризованих систем захисту інформації

підпис члена робочої групи

Дубчак Олена Вікторівна - старший викладач кафедри комп'ютеризованих систем захисту інформації

підпис члена робочої групи

Герасименко Маргарита Костянтинівна - здобувачка вищої освіти

підпис здобувача вищої освіти

ЗОВНІШНІ СТЕЙКХОЛДЕРИ:

Рецензії, відгуки зовнішніх стейкхолдерів (додаються).
Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Національний авіаційний університет, Факультет кібербезпеки, комп'ютерної та програмної інженерії, кафедра комп'ютеризованих систем захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки.
1.3.	Офіційна назва освітньо-професійної програми	Освітньо-професійна програма: Безпека інформаційних і комунікаційних систем.
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС: - 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців навчання (денна форма навчання) / 4 роки 6 місяців навчання (заочна форма навчання)
1.5.	Акредитаційна інституція	Акредитаційна комісія, Міністерство освіти і науки України, сертифікат серія НД №1193809 від 31.10.2017.
1.6.	Період акредитації	До 01.07.2027
1.7.	Цикл/рівень	6 рівень Національної рамки кваліфікацій України (НРК України), перший цикл Європейського простору вищої освіти (FQ-EHEA), 6 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL).
1.8.	Передумови	Вступ на навчання на освітньо-професійну програму обсягом 240 кредитів ЄКТС здійснюється на базі повної загальної середньої освіти
1.9	Форма навчання	Інституційна з елементами дистанційної: очна, заочна
1.10	Мова(и) викладання	Українська
1.11	Інтернет-адреса постійного розміщення опису освітньої програми	http://www.nau.edu.ua http://www.kszi.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціль освітньої-професійної програми «Безпека інформаційних і комунікаційних систем» полягає в підготовці конкурентних на ринку праці професіоналів в галузі інформаційних технологій, здатних розв'язувати складні спеціалізовані завдання або практичні проблеми захисту інформації, використовувати і впроваджувати технології інформаційної та/або кібербезпеки. ОП «Безпека інформаційних і комунікаційних систем» відповідає місії НАУ, у якій наголошується щодо внеску НАУ як у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей на основі інтеграції освіти, досліджень і практики, так і надання високоякісних	

	освітніх та науково-дослідних послуг громадянам України та іноземцям під час підготовки фахівців авіаційно-космічної галузі. У ОП немає аналогів серед ЗВО України щодо врахування галузевого контексту функціонування авіаційного сектору.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (об'єкт діяльності, теоретичний зміст)	**Об'єкти діяльності:** об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси та технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту **Цілі** навчання: підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби 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 проєктування.
3.2.	Орієнтація освітньо-професійної програми	Програма має освітньо-професійну орієнтацію на здобуття студентами знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності; базується на загальновідомих у галузі інформаційних технології наукових результатах, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми	Загальна вища освіта в галузі знань «Інформаційні технології» з поглибленою спеціалізованою підготовкою в сфері безпеки інформаційних і комунікаційних систем.

		Ключові слова: кібербезпека, інформаційно-комунікаційні мережі, програмно-апаратне забезпечення, проєктування систем безпеки
3.4.	Особливості освітньо-професійної програми	Програма передбачає підготовку здобувачів вищої освіти щодо 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 і засобів виявлення, управління та ідентифікації ризиків; – методів і засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів і засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проєктування. Врахування вимог національних роботодавців, міжнародних стандартів інформаційної безпеки, тенденцій розвитку IT - галузі. Орієнтація на підготовку фахівця з потужною теоретичною та практичною базою, що здатний адаптуватися до змін технологій.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Професійна діяльність в галузі інформаційної та/або кібербезпеки в установах та організаціях різних форм власності.
4.2.	Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології 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. Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуально-творчий підхід; навчання через лекції, лабораторні роботи, семінари, практичні заняття, проєктну роботу в командах, виробничу, технологічну та переддипломну практики на підприємствах, підготовка кваліфікаційної роботи.
5.2.	Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної навчальної діяльності, спрямовані на опанування навчального навантаження з освітньої програми: поточний, модульний, підсумковий контроль, екзамени, заліки, презентації, диференційований залік з практик, курсова робота, кваліфікаційна робота бакалавра
Розділ 6. Програмні компетентності		
6.1.	Інтегральні компетентності	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. 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 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. ЗК8. Здатність виявляти суспільно значимі ІТ - потреби для їх подальшого задоволення через створення та впровадження сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
6.3.	Фахові компетентності (ФК)	ФК1. 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. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК8 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи

		управління інформаційною та/або кібербезпекою. ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. ФК13. Здатність оцінювати та визначати фізичні процеси, які висвітлюють характеристики та параметри напівпровідникових активних елементів, а також проводити лінійний та нелінійний аналіз електричних схем, схемотехніки різноманітних підсилювальних каскадів, операційних підсилювачів та елементів логіки. ФК14. Здатність застосовувати теоретичні знання та практичні навички із побудови, керування, модернізації, моніторингу та аналізу продуктивності, діагностики та розв`язання проблем сучасних інформаційних і комунікаційних систем та мереж. ФК15. Здатність застосовувати теоретичні знання та практичні навички з організації та функціонування сучасних операційних систем, уміння зі створення та використання ефективного програмного забезпечення для керування обчислювальними ресурсами в багатокористувальницьких операційних системах.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання	ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу

		інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН4. 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. ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних, у галузі інформаційної та/або кібербезпеки. ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки. ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах виявлення ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН12. Розробляти моделі загроз та порушника. ПРН13. Аналізувати проєкти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах, програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН16. Реалізовувати комплексні системи захисту інформації в (автоматизованих) системах (АС) організації (підприємства)

		відповідно до вимог нормативно-правових документів. ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. ПРН20. Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнівних програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. ПРН21. Вирішувати задачі забезпечення та супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН22. Вирішувати задачу управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки. ПРН23. Реалізовувати заходи з протидії отримання несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних інформаційно-телекомунікаційних (автоматизованих) системах. ПРН24. Вирішувати задачу управління доступом до інформаційних ресурсів та процесів інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

		ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах у ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки. ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН33. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків. ПРН34. Брати участь у розробленні та впровадженні стратегії інформаційної безпеки

		та/або кібербезпеки відповідно до цілей і завдань організації. ПРН35. 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. ПРН36. Виявляти небезпечні сигнали технічних засобів. ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю в процесі захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки та розслідування інцидентів. ПРН44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з

		вітчизняними та міжнародними вимогами та стандартами. ПРН45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик - орієнтованому контролю доступу до інформаційних активів. ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН55. Здійснювати вибір і оцінювання систем передачі даних і протоколів, визначати основні параметри каналу зв’язку для подальшої передачі інформації. ПРН56. Здатність демонструвати знання та розуміння основ комп’ютерної схемотехніки та

		описувати в загальних поняттях і термінах характеристики, параметри, фізичні принципи побудови та логічні основи функціонування цифрових елементів; номенклатуру і функціональне призначення інтегральних мікросхем; типові схеми функціональних вузлів комп'ютерів; методику їх аналізу та розрахунку з використанням пакетів програм систем автоматизованого проєктування. ПРН57. Здатність демонструвати знання та розуміння основ побудови комп'ютерних систем захисту інформації та описувати в загальних поняттях і термінах архітектуру, характеристики та принципи їх дії. ПРН58. Здатність демонструвати знання та розуміння основ побудови комп'ютерних мереж та описувати в загальних поняттях і термінах принципи та методи організації мережевих комунікацій; архітектуру та функціонування локальних, комбінованих і глобальних комп'ютерних мереж; систему мережевих стандартів, способи адресації та протоколи маршрутизації; інтерфейси та методи доступу до передавального середовища; технологію автоматизованого проєктування комп'ютерних мереж. ПРН59. Здатність демонструвати знання та розуміння системного програмування, розробляти системні програми, алгоритми обробки різних типів даних та тестування програмного забезпечення. ПРН60. Здатність демонструвати знання та розуміння технологій проєктування комп'ютерних систем захисту інформації та виконувати системне, операційне, функціонально-логічне і технічне проєєстування комп'ютерних пристроїв, використовуючи сучасні засоби автоматизованого проектування.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Штатні науково-педагогічні працівники, які залучені до реалізації освітньої складової ОПП, відповідно до ліцензійних вимог мають науковий ступінь та/або вчене звання, є провідними фахівцями у галузі кібербезпеки, а також мають необхідний стаж наукової та педагогічної роботи.
8.2.	Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо матеріально-технічного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим

		законодавством України. Матеріально-технічне забезпечення спрямоване на ефективне засвоєння студентами теоретичного матеріалу та набуття ними актуальних практичних навичок. Для цього використовуються: мультимедійні лекційні аудиторії, спеціалізовані класи та лабораторії навчально-лабораторного комплексу кафедри. Навчально-лабораторний комплекс кафедри за своєю структурою, обладнанням і призначенням імітує реальне середовище і процеси ІТ-підприємств, що атмосферно сприяє високому рівню підготовленості випускника до практичної діяльності. Наявність вільного доступу до ресурсів глобальних і локальних комп'ютерних мереж забезпечує можливість проведення усіх видів занять в єдиному програмному та інформаційному середовищі. Навчально-лабораторний комплекс кафедри сприяє впровадженню проєктного підходу у навчанні.
8.3	Інформаційне та навчально-методичне забезпечення	Інформаційне забезпечення програми включає загальний фонд навчальної та науково-технічної літератури, навчальні підручники і посібники за напрямком підготовки, інформаційні ресурси мережі Інтернет. Методичне забезпечення створюється відповідно до програми підготовки і включає нормативну програмно-методичну документацію, силабуси та (або) навчально-методичні комплекси дисциплін.
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	На основі договорів між Національним авіаційним університетом та технічними університетами України.
9.2.	Міжнародна кредитна мобільність	У рамках програм подвійного диплому з університетами, зареєстрованими у ERASMUS+
9.3.	Навчання іноземних здобувачів вищої освіти	Створені умови для підготовки іноземних здобувачів вищої освіти.

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

2.1. Перелік компонент ОПП

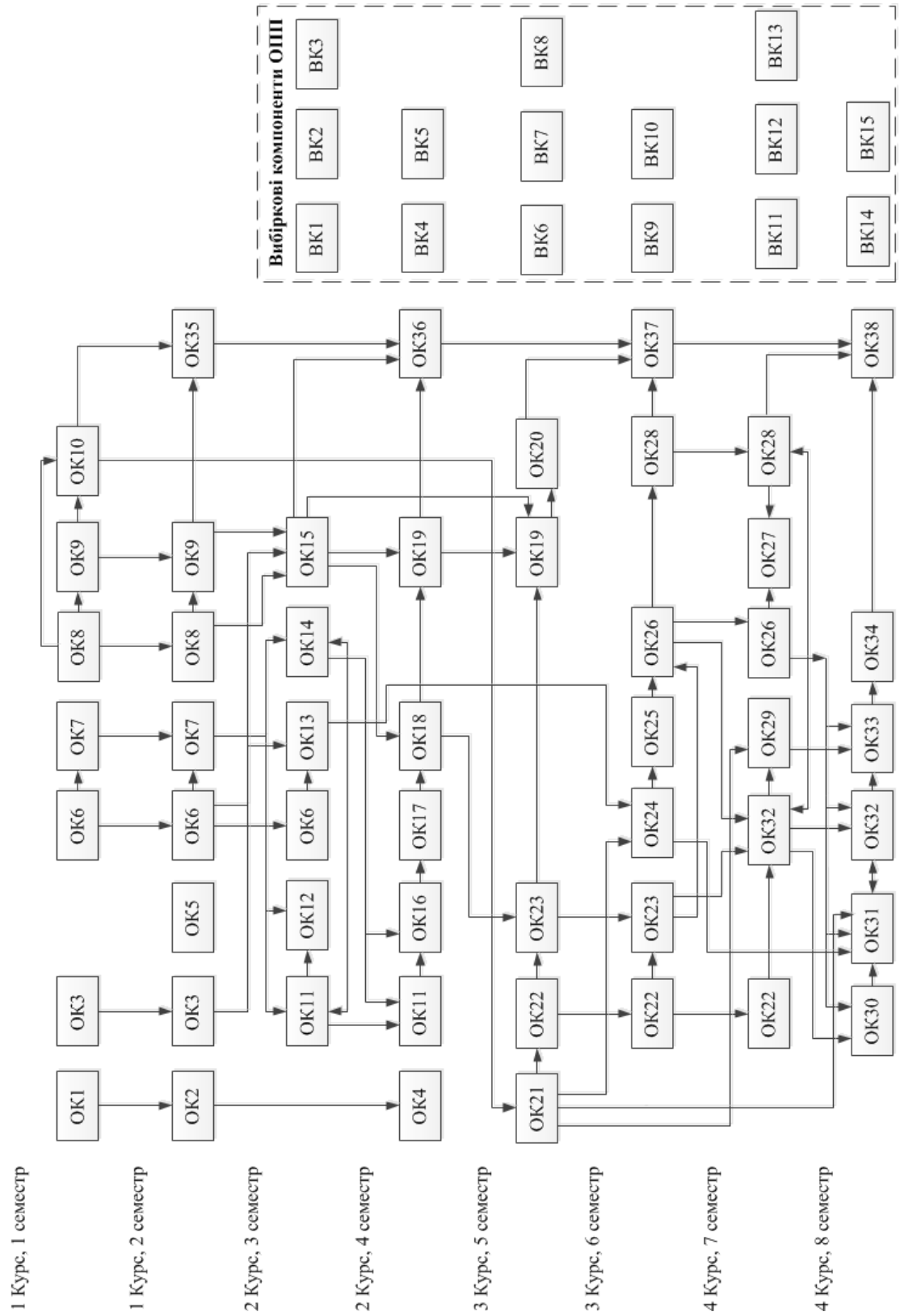
Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
Обов'язкові компоненти ОПП				
ОК1.	Історія української державності та культури	3,0	Екзамен	1
ОК2.	Ділова українська мова	3,0	Екзамен	2
ОК3.	Іноземна мова за професійним спрямуванням	4,5	Диференційований залік Екзамен	1, 2
ОК4.	Філософія	3,5	Екзамен	4
ОК5.	Фізичне виховання та самовдосконалення	3,0	Диференційований залік	2
ОК6.	Вища математика	14,0	Екзамен Диференційований залік	1, 3, 2
ОК7.	Фізика	10,5	Екзамен Диференційований залік	2, 1
ОК8.	Інформаційні технології	11,5	Екзамен Диференційований залік	1, 2
ОК9.	Основи автоматизованої обробки інформації	6,5	Диференційований залік	1,2
ОК10.	Основи кібербезпеки	4,5	Диференційований залік	1
ОК11.	Апаратне забезпечення інформаційних систем	5,0	Диференційований залік Екзамен	3, 4
ОК12.	Курсова робота з дисципіни Апаратне забезпечення інформаційних систем	1,0	Захист	3
ОК13	Основи теорії прийняття рішень у кібербезпеці	4,0	Диференційований залік	3
ОК14.	Компонентна база та схемотехніка в ІКСМ	4,0	Екзамен	3

ОК15	Основи програмування ****	4,0	Екзамен	3
ОК16	Сигнали та процеси у системах захисту інформації	3,5	Екзамен	4
ОК17.	Курсова робота з дисципіни Сигнали та процеси у системах захисту інформації	1,0	Захист	4
ОК18.	Основи мережевих технологій **	4,5	Диференційований залік	4
ОК19.	Технології програмування	7,5	Диференційований залік Екзамен	4, 5
ОК20.	Курсова робота з дисципіни Технології програмування	1,0	Захист	5
ОК21.	Нормативно-правове забезпечення кібербезпеки	4,5	Екзамен	5
ОК22.	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	10,5	Екзамен Диференційований залік	5, 6, 7
ОК23.	Захищені комп'ютерні системи та мережі **	8,0	Диференційований залік Екзамен	5, 6
ОК24.	Управління інформаційною безпекою	3,0	Екзамен	6
ОК25.	Курсова робота з дисципіни Управління інформаційною безпекою	1,0	Захист	6
ОК26.	Прикладна криптологія	7,5	Екзамен	6, 7
ОК27.	Курсова робота з дисципіни Прикладна криптологія	1,0	Захист	7
ОК28.	Операційні системи та технології їх захисту ***	7,0	Диференційований залік Екзамен	6, 7
ОК29.	Системи технічного захисту інформації	3,5	Екзамен	7
ОК30.	Технології безпечного доступу	4,0	Диференційований залік	8
ОК31.	Комплексні системи захисту інформації	4,0	Екзамен	8
ОК32.	Безпека інформаційно-комунікаційних систем та мереж	7,0	Диференційований залік Екзамен	7, 8
ОК33.	Програмні засоби захисту інформації	3,0	Екзамен	8
ОК34.	Курсова робота з дисципіни Програмні засоби захисту інформації	1,0	Захист	8
ОК35.	Фахово-ознайомлювальна практика	3.0	Диференційований залік	2
ОК36.	Комп'ютерна практика	3.0	Диференційований залік	4
ОК37.	Технологічна практика	3.0	Диференційований залік	6
ОК38.	Кваліфікаційна робота	7.5	Захист	8

Загальний обсяг обов'язкових компонент:		**180 кредитів ЄКТС**		
Вибіркові компоненти *				
ВК 1.		4,0	Диф.залік	3
ВК 2.		4,0	Диф.залік	3
ВК 3.		4,0	Диф.залік	3
ВК 4.		4,0	Диф.залік	4
ВК 5.		4,0	Диф.залік	4
ВК 6.		4,0	Диф.залік	5
ВК 7.		4,0	Диф.залік	5
ВК 8.		4,0	Диф.залік	5
ВК 9.		4,0	Диф.залік	6
ВК 10.		4,0	Диф.залік	6
ВК 11.		4,0	Диф.залік	7
ВК 12.		4,0	Диф.залік	7
ВК 13.		4,0	Диф.залік	7
ВК 14.		4,0	Диф.залік	8
ВК 15.		4,0	Диф.залік	8
Загальний обсяг вибіркових компонент		**60 кредитів ЄКТС**		
Загальний обсяг освітньо-професійної програми		**240 кредитів ЄКТС**		

**Реалізація права здобувачів вищої освіти на вільний вибір навчальних дисциплін та створення індивідуальної освітньої траєкторії регламентується Законом України «Про вищу освіту» та внутрішніми нормативними актами НАУ. Вибіркові компоненти обираються здобувачами вищої освіти із каталогів рекомендованих та альтернативних вибіркових дисциплін.*

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	**Кваліфікаційна робота**
Вимоги до кваліфікаційної роботи	Атестація повинна здійснюватися у формі публічного захисту кваліфікаційної роботи. Кваліфікаційна робота має передбачати розв'язання кваліфікаційної задачі галузі інформаційної та/або кібербезпеки. Кваліфікаційна робота має бути перевірена на плагіат. Оприлюднення на сайті.

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	ОК38	ВБ 1	….	ВБ 15
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК1	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК2		+				+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК3	+	+	+					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК4								+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК5	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК6	+																				+														+			+			
ЗК7	+	+			+																																	+			
ЗК8								+	+	+			+		+			+	+	+		+	+	+	+	+	+			+	+	+	+	+	+		+	+			
ФК1										+											+	+		+	+						+	+			+			+			
ФК2								+	+				+					+				+	+	+	+			+		+	+	+	+	+	+	+		+			
ФК3								+			+	+		+	+			+	+	+		+	+			+	+	+	+	+	+	+	+	+	+	+		+			
ФК4										+	+	+	+		+			+	+	+	+		+	+	+	+	+	+	+	+	+	+	+				+			
ФК5										+					+				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+							
ФК6											+	+		+				+					+					+			+	+					+	+			
ФК7										+	+	+				+	+				+	+	+			+	+	+	+	+	+	+						+			
ФК8													+								+	+	+	+	+					+	+								+			
ФК9										+			+								+	+	+	+	+							+							+			
ФК10						+					+	+		+	+	+	+		+	+			+			+	+	+	+	+		+	+	+				+			
ФК11										+	+	+				+	+				+	+	+	+	+	+	+	+		+		+						+			
ФК12										+								+			+	+	+	+	+				+	+	+	+						+			
ФК13						+	+	+			+	+		+		+	+												+									+			
ФК14													+		+	+	+	+	+	+			+					+		+	+	+	+	+				+			
ФК15						+									+				+	+			+			+	+	+			+	+	+	+				+			

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	ОК38	ВБ 1	……	ВБ 15
ПРН1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН2		+	+					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН3								+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН4								+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН5								+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН6								+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН7								+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН8																					+			+	+					+								+			
ПРН9													+						+	+		+	+	+	+	+	+		+	+	+	+						+			
ПРН10																		+				+	+	+	+			+	+		+	+						+			
ПРН11																		+				+								+	+	+					+	+			
ПРН12											+							+			+	+	+	+	+			+	+	+	+	+					+	+			
ПРН13																		+				+	+	+	+				+	+	+	+	+	+			+	+			
ПРН14														+		+	+					+							+			+					+	+			
ПРН15											+	+									+	+							+	+	+	+					+	+			
ПРН16																		+			+	+									+	+					+	+			
ПРН17								+	+		+	+	+	+		+	+					+						+			+	+						+			
ПРН18											+	+	+	+	+				+	+			+					+	+		+	+	+	+			+	+			
ПРН19															+			+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+			+	+			
ПРН20															+				+	+			+			+	+	+			+	+	+	+				+			
ПРН21																					+	+		+	+						+	+						+			
ПРН22																						+	+					+			+	+	+				+	+			
ПРН23															+			+	+	+			+			+	+	+	+	+	+	+	+	+			+	+			
ПРН24																							+							+	+	+						+			
ПРН25																							+							+	+	+						+			
ПРН26																						+							+	+								+			
ПРН27															+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+			+	+			
ПРН28																					+	+	+	+					+	+	+							+			
ПРН29																						+	+	+					+		+							+			
ПРН30																						+	+	+	+			+	+	+	+	+					+	+			
ПРН31													+		+	+	+	+	+	+		+	+			+	+	+	+	+	+	+	+	+			+	+			
ПРН32																						+	+					+	+	+		+					+	+			
ПРН33																								+	+													+			
ПРН34																					+	+		+	+													+			
ПРН35																						+	+	+	+				+	+	+	+	+	+				+			
ПРН36														+			+	+											+									+			
ПРН37														+			+	+											+									+			

ПРН38													+			+	+			+								+								+			
ПРН39																				+								+								+	+			
ПРН40													+			+	+			+								+								+	+			
ПРН41																	+				+	+	+	+			+		+	+	+	+	+			+	+			
ПРН42																					+	+	+	+	+	+	+	+	+	+	+	+	+			+	+			
ПРН43									+											+	+	+	+	+												+	+			
ПРН44									+											+	+	+	+	+												+	+			
ПРН45																					+	+	+	+												+	+			
ПРН46																					+	+	+	+	+	+	+	+	+	+	+	+			+	+			
ПРН47																									+	+										+				
ПРН48																						+			+	+			+	+	+					+				
ПРН49																						+						+	+	+	+					+				
ПРН50																						+						+	+	+	+					+				
ПРН51																						+						+	+	+	+					+				
ПРН52												+		+	+	+	+	+	+	+		+			+	+	+	+	+	+	+	+			+	+			
ПРН53																	+	+	+						+	+						+	+			+	+			
ПРН54	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПРН55														+								+							+	+	+					+	+			
ПРН56		+	+							+			+		+	+						+						+							+	+	+			
ПРН57		+	+																			+						+			+	+	+	+	+	+	+			
ПРН58		+	+					+									+				+	+					+								+	+			
ПРН59		+	+					+						+					+	+						+	+						+	+			+	+			
ПРН60		+	+											+			+	+	+			+			+	+	+		+	+	+	+	+			+	+			

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				