(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Факультет комп'ютерних наук та технологій
Кафедра технічного захисту інформації

УЗГОДЖЕНО
Декан
_____ Андрій ФЕСЕНКО
«01» 09 2025 р.

Система менеджменту якості

ПРОГРАМА

Науково-дослідної практики у сфері систем технічного захисту інформації, автоматизації її обробки

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»
Галузь знань: F «Інформаційні технології»
Спеціальність: F5 «Кібербезпека та захист інформації»

Форма навчання	Курс	Семестр	Усього (годин/кредитів ECTS)	Самостійна робота (годин)	Форма семестрового контролю
Денна	1	2	180/6,0	180	Залік

Індекс: НМ-4-F5-2/25 - 2.2.1.1
РМ-4-F5-2/25 - 2.2.1.1

СМЯ КАІ ПП 14.08-01-2025

Київ

Програма Науково-дослідної практики у сфері систем технічного захисту інформації, автоматизації її обробки розроблена на основі навчального плану НМ-4-F5-2/25 та робочого навчального плану РМ-4-F5-2/25 підготовки здобувачів вищої освіти ОС «Магістр», спеціальності F5 «Кібербезпека та захист інформації» освітньо-професійної програми (далі – ОПП) «Системи технічного захисту інформації, автоматизація її обробки».

Програму розробив:
Професор кафедри технічного захисту інформації _____ Сергій ЛАЗАРЕНКО

Гарант ОПП
Професор кафедри
технічного захисту інформації _____ Сергій ЛАЗАРЕНКО

Програму Науково-дослідної практики у сфері систем технічного захисту інформації, автоматизації її обробки обговорено та схвалено на засіданні випускової кафедри технічного захисту інформації, протокол від «25» 08 2025 р. № 11.

Завідувач кафедри _____ Валерій КОЗЛОВСЬКИЙ

Програму Науково-дослідної практики у сфері систем технічного захисту інформації, автоматизації її обробки обговорено та схвалено на засіданні науково-методично-редакційної ради Факультету комп'ютерних наук та технологій, протокол № 10 від «01» вересня 2025 р.

Голова НМРР _____ Оксана ПОЛІЩУК

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

ЗМІСТ

ВСТУП

Програма Науково-дослідної практики у сфері систем технічного захисту інформації, автоматизації її обробки (далі – Науково-дослідна практика) розроблена на основі «Положення про організацію та проведення практик здобувачів вищої освіти Національного авіаційного університету», затвердженого та введеного в дію наказом ректора від 09.12.2021 № 651/од, «Методичних рекомендацій щодо розробки програми практики», затверджених та введених в дію наказом ректора від 13.12.2021 № 659/од, освітньо-професійної програми СМЯ КАІ ОП М ID69363-01-2025 «Системи технічного захисту інформації, автоматизація її обробки», навчального плану НМ-4-F5-2/25, робочого навчального плану РМ-4-F5-2/25 та відповідних нормативних документів.

1. ВІДОМОСТІ ПРО СПЕЦІАЛЬНІСТЬ ТА ПРО ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ

Спеціальність F5 «Кібербезпека та захист інформації» спрямована на захист життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кафедра технічного захисту інформації (далі – ТЗІ) Факультету комп'ютерних наук та технологій (далі – ФКНТ) здійснює підготовку фахівців за ОПП «Системи технічного захисту інформації, автоматизація її обробки» спеціальності F5 «Кібербезпека та захист інформації».

ОПП «Системи технічного захисту інформації, автоматизація її обробки» спеціальності F5 «Кібербезпека та захист інформації» має прикладну орієнтацію, базується на загальновідомих наукових результатах в галузі інформаційних технологій, інформаційної безпеки та/або кібербезпеки у рамках яких можлива подальша професійна кар'єра і подальше навчання.

Метою ОПП є підготовка фахівців, які володіють сучасними загально-науковими й спеціальними знаннями та технологіями інформаційної та/або кібербезпеки, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Опанування специфічних знань особливостей професійної діяльності в авіаційному секторі, застосування яких дозволяє вирішувати практичні завдання підвищення рівня безпеки в авіації.

ОПП «Системи технічного захисту інформації, автоматизація її обробки» відповідає місії Державного університету «Київський авіаційний інститут» (далі - КАІ), в якій наголошується, щодо внеску КАІ у розвиток суспільства на національному та міжнародному рівнях через генерацію нових

знань та інноваційних ідей на основі інтеграції та інтернаціоналізації освіти, досліджень та практики, так і надання високоякісних освітніх та науково-дослідних послуг громадянам України та іноземцям при підготовці фахівців з Кібербезпеки в авіаційно-космічній галузі.

Науково-дослідна практика здобувачів вищої освіти (далі – практиканти) є невід'ємною складовою процесу підготовки фахівців ОС «Магістр» денної та заочної форм навчання і проводиться на підприємствах, організаціях та установах різних форм власності, а також оснащених відповідним чином структурних підрозділах Університету.

2. ВІДОМОСТІ ПРО БАЗИ ПРАКТИК

Базами практики можуть бути підприємства, організації та установи різних форм власності (далі – бази практики), які відповідають вимогам програми науково-дослідної практики, та структурні підрозділи КАІ (як виняток – на кафедрах КАІ).

Вибір бази практики здійснюється з урахуванням можливості бази практики організувати робоче місце практикантам і забезпечити кваліфіковане керівництво практикою з боку найбільш досвідчених фахівців; науково-дослідних інтересів практикантів; відповідності специфіки бази практики спеціальності F5 «Кібербезпека та захист інформації».

З базами практики, які відповідають вимогам програминауково-дослідної практики, КАІ завчасно укладає договори на її проведення. Практиканти мають також право самостійно, з дозволу кафедри ТЗІ, вибирати місце проведення практики за умови, що такі бази практики відповідають встановленим вимогам для проходження науково-дослідної практики.

3. ЦІЛІ ПРАКТИКИ

Під час проходження науково-дослідної практики практиканти повинні досягти наступних **цілей:**

- засвоїти основні етапи композиції та декомпозиції під час аналізу та створення або модернізації нових пристроїв для захисту інформації;
- практично навчитись користуватися спеціальним програмним забезпеченням для проведення комп'ютерного моделювання;
- оволодіти науковими теоріями та практичними підходами для проведення самостійних досліджень у сфері кібербезпеки та захисту інформації.

У процесі проходження науково-дослідної практики практиканти повинні

Знати:

- законодавчу, нормативно-правову бази України;

- вимоги відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;
- можливі джерела витоку інформації технічними каналами;
- структуру підприємства та його інформаційні процеси;
- принципи роботи та характеристики систем та засобів технічного захисту інформації;
- питання розмежування доступу та захисту інформації в АС;
- принципи автоматизації обробки інформації з обмеженим доступом.

Вміти:

- розв'язувати складні практичні проблеми у галузі забезпечення захисту інформації, що характеризується комплексністю та неповною визначеністю умов.
- аналізувати роботу пристроїв захисту інформації;
- розробляти план заходів із захисту інформації;
- експлуатувати програмні продукти, вміти, за допомогою програм, одержувати якісні результати та впроваджувати їх на підприємстві для забезпечення надійного захисту інформації підприємства;
- використовувати новітні інформаційні технології, які застосовуються на підприємстві;
- вести необхідну технічну та звітну документацію.

4. МЕТА ПРАКТИКИ

Мета науково-дослідної практики – є поглиблення та закріплення теоретичних знань, отриманих практикантами в процесі навчання певного циклу теоретичних дисциплін, ознайомлення безпосередньо в установі, організації на підприємстві з виробничим процесом та технологічним циклом створення систем захисту інформації, відпрацювання вмінь і навичок зі спеціальності F5 «Кібербезпека та захист інформації», а також збір матеріалу для виконання кваліфікаційних робіт.

Головним завданням науково-дослідної практики є набуття необхідних вмінь та досвіду самостійно проводити дослідження та вирішувати задачі наукового спрямування для організації захисту інформації на підприємстві на найвищому рівні. Для цього необхідно ознайомитися з сучасним станом засобів технічного захисту інформації, їх новітніми розробками, оволодіти необхідними науковими підходами та спеціалізованими комп'ютерними програмами для моделювання складних фізичних процесів, що протікають в електричних схемах пристроїв технічного захисту інформації.

На базі здобутих знань та умінь практиканти зможуть вирішувати професійні задачі, що базуються на сучасних технологіях та методах побудови захищених інформаційних систем та технологій.

Знання, одержані під час проходження науково-дослідної практики, є необхідними в подальшому при проектуванні та розробці систем технічного

захисту інформації, проведенні наукових досліджень в сфері кібербезпеки та захисту інформації.

5. ЗАГАЛЬНІ КОМПЕТЕНЦІЇ

Під час проходження науково-дослідної практики практиканти повинні набути наступні інтегральні (далі – ІК) та загальні (далі – ЗК) компетентності:

ІК1. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Здатність проводити дослідження на відповідному рівні.

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

6. ФАХОВІ КОМПЕТЕНЦІЇ

Під час проходження науково-дослідної практики практиканти повинні набути наступні фахові компетентності (далі – ФК):

ФК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ФК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

ФК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ФК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ФК8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ФК9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

ФК11. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.

ФК12. Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз, зокрема у контексті концепції сталого розвитку.

ФК13. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.

ФК14. Здатність моделювати безпекові процеси в авіаційній галузі.

7. ОРГАНІЗАЦІЯ ПРОВЕДЕННЯ ПРАКТИКИ

7.1.Організаційні питання

Тривалість практики: усього 180 годин / 6.0 кредитів ECTS.

Практика проводиться на першому курсі навчання у другому семестрі.

Організація та керівництво науково-дослідною практикою здійснюється відповідно до «Положення про організацію та проведення практик здобувачів вищої освіти Національного авіаційного університету», затвердженого та введеного в дію наказом ректора від 09.12.2021 № 651/од (далі – Положення про проведення практик).

7.2. Обов'язки керівника практики від університету

Обов'язки практикантів, керівників практики від університету та від бази практики висвітлені у Розділі 4 «Положення про організацію проходження практик здобувачів вищої освіти Національного авіаційного університету» СМЯ НАУ П 03.01(20)-02-2021.

Практиканти повинні суворо дотримуватися прийнятих на базі практики правил охорони праці та протипожежної безпеки з обов'язковим проходженням ними інструктажів (вступного і на кожному конкретному місці праці).

Під час проходження науково-дослідної практики передбачені різні форми та методи поточного контролю. Щоденний поточний контроль здійснюється керівником від бази практики та полягає у контролі часу початку та закінчення роботи, відомості щодо особистої участі кожного практиканта у виконанні необхідного обсягу робіт, дотримання вимог інструкцій з техніки безпеки та охорони праці на робочих місцях, ведення щоденника практики тощо.

Підсумковий контроль полягає у перевірці щоденника практики та звіту про виконання індивідуального завдання в рамках програми практики, що має бути підготовлений практикантом особисто та складання диференційного заліку.

8. ТЕМАТИЧНИЙ ПЛАН ПРОХОДЖЕННЯ ПРАКТИКИ

Тематика занять

У період проходження науково-дослідної практики передбачається проведення теоретичних навчальних занять у вигляді лекцій або бесід та організація виробничих екскурсій. Все це має за мету дати практикантам знання по основним питанням технології, організації проектування виробництва, економіки, наукової організації праці тощо.

Навчальні заняття проводяться кваліфікованими інженерно-технічними працівниками та провідними спеціалістами підприємства. Планування і проведення занять проводиться спільно з керівником практики від університету та бази практики.

Тематика навчальних завдань при проведенні практики:

– аналіз правових актів забезпечення кібербезпеки та захисту інформації;

– дослідження каналів витоку інформації;

– дослідження ефективності застосування методів, механізмів та пристроїв технічного захисту інформації;

– порядок ведення технічної документації та звітності відповідно до вітчизняних та міжнародних стандартів.

Остаточна тематика лекцій (бесід) уточнюється в процесі проведення практики. З метою надбання практикантами найбільш повного уявлення про базу практики, її структуру, взаємодію її структурних підрозділів, діючу

систему управління, під час практики проводяться екскурсії. Час, що надається на навчальні заняття та екскурсії, не повинен перевищувати 6 годин на тиждень на одну групу студентів.

Індивідуальні завдання

Зміст індивідуального завдання конкретизується і уточняється керівниками практики під час її проходження.

Індивідуальні завдання, зміст яких встановлює керівник практики по узгодженню з керівником практики від виробництва, конкретизуються і уточнюються під час проходження науково-дослідної практики. В індивідуальних завданнях можуть бути відображені питання, які відповідають інтересам роботи практикантів в студентському науково-технічному товаристві (СНТТ), кафедральних науково-дослідних робіт (НДР) та ін. Результати, отримані практикантами під час виконання індивідуальних завдань, можуть бути в подальшому використані при виконанні кваліфікаційних робіт, підготовці доповідей на наукових конференціях, опублікуванні наукових публікацій тощо.

Результати виконання індивідуального завдання входять до письмового звіту з практики.

9. ПІДСУМКИ ПРОХОДЖЕННЯ ПРАКТИКИ

За результатами проходження науково-дослідної практики практикант повинен досягнути наступних програмних результатів (далі – ПРН):

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплі-нарних контекстах.

ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

ПРН24. Розробляти проєкти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, інформація з обмеженим доступом)

ПРН25. Проводити спеціальні дослідження засобів обробки інформації, технічних засобів.

ПРН26. Визначати показники захищеності інформації на об'єкті інформаційної діяльності та можливість (неможливість) створення на ОІД певних технічних каналів витоку інформації.

10. ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. Закон України «Про інформацію».

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

3. ДСТУ 3396.1-96. «Захист інформації. Технічний захист інформації. Порядок проведення робіт».

4. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку // 2015 - Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074.

5. НД ТЗІ 1.4-001-2000. «Типове положення про службу захисту інформації в автоматизованій системі».

6. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

7. НД ТЗІ 2.5-005-99. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

8. НД ТЗІ 2.5-008-02. «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2».

9. НД ТЗІ 2.5-010-03. «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».

10. НД ТЗІ 3.7-001-99. «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».

11. НД ТЗІ 1.1-002-99. «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

З урахуванням специфіки технологічних процесів, що забезпечуються підприємством – базою практики, до переліку інформаційних джерел можуть бути додані спеціальні вітчизняні та міжнародні стандарти, описи, наочні посібники, програми технічної експлуатації тощо.

Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment).

Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua.

Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua.

11. ФОРМА ОЦІНЮВАННЯ ПРОХОДЖЕННЯ ПРАКТИКИ ЗГІДНО ПОЛОЖЕННЯ ПРО РСО

Оцінювання окремих видів виконаної практикантом навчальної роботи здійснюється в балах відповідно до табл. 1.

Залікова рейтингова оцінка визначається (в балах та за національною шкалою) за результатами виконання всіх видів навчальної роботи протягом науково-дослідної практики.

Таблиця 1

Вид навчальної роботи	Мах кількість балів
	Денна форма навчання
	2 семестр
Модуль № 1 «Забезпечення кібербезпеки об'єктів інформаційної діяльності»	
Аналіз правових актів забезпечення кібербезпеки та захисту інформації	15
Дослідження каналів витоку інформації	15
Усього за модулем № 1	**30**
Модуль № 2 «Дослідження кібербезпеки об'єктів інформаційної діяльності»	
Дослідження ефективності застосування методів, механізмів та пристроїв технічного захисту інформації	15
Порядок ведення технічної документації та звітності відповідно до вітчизняних та міжнародних стандартів	15
Виконання індивідуального завдання	20
Усього за модулем № 2	**50**
Усього за модулем № 1, 2	**80**
Захист звіту науково-дослідної практики	**20**
Усього за науково-дослідну практику	**100**

Виконані види навчальних заходів зараховуються практиканту, якщо він отримав за них позитивну рейтингову оцінку (Табл. 2).

Таблиця 2

Відповідність рейтингових оцінок за окремі види навчальних заходів в балах оцінкам за національною шкалою

Рейтингова оцінка в балах				Оцінка за національною шкалою
Виконання навчальних заходів. Модуль 1	Виконання навчальних заходів. Модуль 2	Індивідуальне завдання	Захист звіту переддипломної практики	
27 - 30	45 - 50	18 - 20	18 - 20	Відмінно
23 - 26	38 - 44	15 - 17	15 - 17	Добре
18 - 22	30 - 37	12 - 14	12 - 14	Задовільно
менше 18	менше 30	менше 12	менше 12	Незадовільно

Сума рейтингових оцінок, отриманих практикантом за окремі види виконаних навчальних заходів становить підсумкову оцінку, що заноситься до відомості заліку яка перераховується в оцінки за національною шкалою та шкалою ECTS (Табл. 3).

Таблиця 3

Відповідність підсумкової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	**Відмінно**	**A**	**Відмінно** (відмінне виконання лише з незначною кількістю помилок)
82-89	**Добре**	**B**	**Дуже добре** (вище середнього рівня з кількома помилками)
75-81		**C**	**Добре** (в загальному вірне виконання з певною кількістю суттєвих помилок)
67-74	**Задовільно**	**D**	**Задовільно** (непогано, але зі значною кількістю недоліків)
60-66		**E**	**Достатньо** (виконання задовольняє мінімальним критеріям)
35-59	**Незадовільно**	**FX**	**Незадовільно** (з можливістю повторного складання)
1-34		**F**	**Незадовільно** (з обов'язковим повторним курсом)

Підсумкова рейтингова оцінка за науково-дослідну практику в балах, за національною шкалою та шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та індивідуального навчального плану студента, наприклад, так: ***92/Відм./A, 87/Добре/B, 79/Добре/C, 68/Задов./D, 65/Задов./E*** тощо.

(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
1	Лазаренко С.В	[signature]	01.09.25	

(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				