(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра засобів захисту інформації

УЗГОДЖЕНО
Декан
_____ Катерина НЕСТЕРЕНКО
«21» 02 2022р.

ЗАТВЕРДЖЕНО
Проректор з навчальної роботи
_____ Анатолій ПОЛУХІН
«21» 02 2022р.

Система менеджменту якості

ПРОГРАМА
Переддипломної практики

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека»

Форма навчання	Курс	Семестр	Усього годин/кредитів ECTS)	Самостійна робота (годин)	Форма семестрового контролю
Денна	1	2	315/10,5	315	Залік
Заочна	1	2	315/10.5	315	

Індекс: НМ-4-125-2/21 – 2.2.1.2
РМ-4-125-2/21 – 2.2.1.2
НМ-4-125-2з/21 – 2.2.1.2
РМ-4-125-2з/21 – 2.2.1.2

СМЯ НАУ НП 09.01.10-03-2021

Програма Переддипломної практики розроблена на основі навчального плану НМ-4-125-2/21 (НМ-4-125-2з/21) підготовки здобувачів вищої освіти ОС «Магістр», уведеного в дію наказом ректора від 29.04.2021 № 246/од, та робочого навчального плану РМ-4-125-2/21 (РМ-4-125-2з/21) підготовки здобувачів вищої освіти ОС «Магістр», затвердженого проректором з навчальної роботи 28.08.2021 року, спеціальності 125 «Кібербезпека» освітньо-професійної програми (далі – ОПП) «Системи технічного захисту інформації, автоматизація її обробки».

Програму розробив:
Професор кафедри
засобів захисту інформації _____ Олександр ТУРОВСЬКИЙ

Гарант ОПП
Професор кафедри
засобів захисту інформації _____ Сергій ЛАЗАРЕНКО

Програму Переддипломної практики обговорено та схвалено на засіданні випускової кафедри засобів захисту інформації, протокол від «13» 12 2021 р. № 19

Завідувач кафедри _____ Валерій Козловський

Програму переддипломної практики обговорено та схвалено на засіданні науково-методично-редакційної ради Факультету кібербезпеки, комп'ютерної та програмної інженерії, протокол № 12 від «20» 12 2021 р.

Голова НМРР _____ Сергій ГНАТЮК

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

ЗМІСТ

ВСТУП

Програма Переддипломної практики 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, та відповідних нормативних документів.

1. ВІДОМОСТІ ПРО СПЕЦІАЛЬНІСТЬ ТА ПРО ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ

Підготовка здобувачів вищої освіти освітнього ступеня «Магістр» другого року навчання за спеціальністю 125 «Кібербезпека» здійснюється на основі освітньо-професійної програми СМЯ НАУ ОПП 09.01.10 –03– 2021 «Системи технічного захисту інформації, автоматизація її обробки», навчальних та робочих навчальних планів № РМ-4-125-2/21, № НМ-4-125-2/21 та № РМ-4-125-2з/21, № НМ-4-125-2з/21 та відповідних нормативних документів.

ОПП «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 «Кібербезпека» 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 загальнонауковими 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.

2. ВІДОМОСТІ ПРО БАЗИ ПРАКТИК

Базами переддипломної практики для здобувачів вищої освіти спеціальності «Системи технічного захисту інформації» можуть бути підприємства, організації та установи будь-яких форм власності, наприклад:

- Служба безпеки України;
- Збройні сили України;
- Національний банк України;
- ДП «Завод №410 ЦА»;
- ДП «Антонов»
- ТОВ «РКІ - Консалтинг»;
- Державна акціонерна холдингова компанія «Артем»;

- Державне підприємство обслуговування повітряного руху України «Украероруx»;
- Департамент інформаційних технологій та митної статистики Державної митної служби України;
- Державна податкова адміністрація України;
- авіакомпанії «Авіалінії України», «Міжнародні Авіалінії України»;
- інші підприємства, профіль яких відповідає вимогам виконання програми практики.

З базами практики, які відповідають вимогам програми, університет завчасно укладає договори на її проведення. Здобувачі вищої освіти – практиканти мають також право самостійно, з дозволу кафедри засобів захисту інформації, вибирати місце проведення практики.

3. ЦІЛІ ПРАКТИКИ

Під час проходження переддипломної практики здобувачів вищої освіти – практиканти повинні досягнути наступних цілей:

Знати:

- організацію, управління кадрами, економічні затрати для систем захисту інформації з обмеженим доступом на підприємстві;
- принципи дії апаратури захисту інформації;
- принципи функціонування спеціалізованого програмного забезпечення захисту інформації з обмеженим доступом;
- принципи функціонування автоматизованих систем обробки інформації з обмеженим доступом;
- основи захисту інформації в комп'ютерних системах та мережах;
- функціональні обов'язки та особливості первинних посад випускника освітньо-кваліфікаційного рівня магістр;
- чинне законодавство України, нормативні та інструктивні матеріали з питань організації та ведення обліку документів з обмеженим доступом.

Вміти:

- виконувати функціональні обов'язки фахівця освітньо-кваліфікаційного рівня магістр на відповідних первинних посадах;
- застосовувати отримані теоретичні знання та наявні вміння при розробці організаційно-технічних заходів захисту інформації з обмеженим доступом, досліджувати резерви підвищення ефективності систем захисту інформації;
- оцінювати рівень організації виробництва та управління.

4. МЕТА ПРАКТИКИ

Метою переддипломної практики є поглиблення та закріплення теоретичних знань, отриманих здобувачами вищої освіти в процесі навчання певного циклу теоретичних дисциплін; оволодіння сучасними методами і

формами організації професійної діяльності та знаряддями праці, що забезпечують здатність розв'язання задач дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки в авіаційній галузі, збір матеріалу для виконання дипломних (курсових) робіт (проєктів)

5. ЗАГАЛЬНІ КОМПЕТЕНЦІЇ

Загальні компетенції (далі –ЗК), яких повинні досягти практиканти:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Здатність проводити дослідження на відповідному рівні.

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

К34. 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

Фахові компетенції (далі –ФК), яких повинні досягти практиканти:

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 галузіінформаційної 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 проводити ліцензування, атестацію та сертифікацію об'єктів інформаційної діяльності.

ФК12. Здатність розробляти проектну документацію, програми та методики випробувань та організовувати тестування і налагодження комплексів засобів захисту та охорони об'єктів інформаційної діяльності.

7. ОРГАНІЗАЦІЯ ПРОВЕДЕННЯ ПРАКТИКИ

7.1.Організаційні питання

Тривалість практики: усього 315 годин / 10.5 кредитів ECTS (4 тижні).

Практика проводиться на другому курсі навчання у третьому семестрі.

Організація та керівництво переддипломною практикою здійснюється відповідно до «Положення про організацію проходження практик здобувачів вищої освіти Національного авіаційного університету» СМЯ НАУ П 03.01(20)-02-2021.

7.2. Обов'язки керівника практики від університету

Обов'язки здобувача вищої освіти, 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.

8. ТЕМАТИЧНИЙ ПЛАН ПРОХОДЖЕННЯ ПРАКТИКИ

Види робіт, які виконують практиканти під час проходження науково-дослідної практики, розробляються кафедрою ЗІ у взаємодії з базою практик.

Теми, які розглядаються під час проходження практики:
– Проблеми забезпечення безпеки інформаційно-комунікаційних систем;
– Захист інформації в системах зв'язку та передавання даних;
– Нормативно-правові акти з основних положень інформаційної безпеки;
– Ліцензування господарської діяльності з надання послуг у галузі криптографічного та технічного захисту інформації.

З метою активізації творчого мислення практикантів, підвищення ініціативи і здатності самостійно досліджувати, аналізувати та узагальнювати підсумки, забезпечувати проходження переддипломної практики більш конкретним та цілеспрямованим, практикантам видаються індивідуальні завдання. Такі завдання направлені на отримання умінь та навичок наукового дослідження, самостійного розв'язання виробничих проблем. Виконання індивідуальних завдань активізує діяльність практикантів, розширює їх світогляд, підвищує ініціативу і робить проходження переддипломної практики більш цілеспрямованим. Індивідуальні завдання конкретизуються та уточнюються під час проходження преддипломної практики.

В процесі підготовки індивідуального завдання практикант напрацьовує матеріал відповідно теми магістерської роботи. Направленість матеріалу – практична реалізація запропонованих рекомендацій та шляхів удосконалення процесів, що передбачаються до дослідження в ході підготовки магістерської роботи.

У період проходження переддипломної практики передбачається проведення теоретичних та практичних навчальних заходів та організація виробничих екскурсій. Все це має за мету дати практикантам знання по основним питанням технології, організації проектування виробництва, економіки, наукової організації праці та інше на об'єкті проведення практики.

9. ПІДСУМКИ ПРОХОДЖЕННЯ ПРАКТИКИ

У результаті проходження переддипломної практики здобувач вищої освіти – 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.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

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

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

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.

ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

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.

ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

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.

ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

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.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

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.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ПРН24. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.

ПРН25. Організовувати внутрішньо-об'єктовий та пропускний режими на підприємстві.

ПРН26. Здійснювати оцінювання захищеності інформації, що циркулює на об'єкті інформаційної діяльності.

ПРН27. Використовувати методи та засоби пошуку закладних пристроїв.

10. ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. Закон України "Про інформацію".
2. Закон України "Про державну таємницю".

3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

4. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

5. 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.

6. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

7. НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

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

9. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації. Навчальний посібник.- Київ: НАУ, 2012.- 207 с.

10. Методы и средства защиты информации Хорошко В.А., Чекатков А.А. – К.: ЮНИОР, 2003.

11. Максименко Г.А., Хорошко В.О. Методи виявлення, обробки та ідентифікації сигналів радіозакладних приладів. - К.: ООО „Поліграф Консалтинг", 2004.-317 ст.

12. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО „ТИД „ДС", 2002. – 688 с.

13. Домарев В.В. Безопасность информационных технологий. Системный подход. К.: ООО „ТИД „ДС", 2014. – 992 с.

14. Системы и устройства информационной безопасности. Учебное пособие / под ред. проф. В.А. Хорошко/ Соавторы: А.П. Провозин. О.В. Рыбальский, В.А.Хорошко, Д.В. Чирков/- К. ДУИКТ, 2007.

15. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

16. http://www.czo.gov.ua/index.php?page=docs&id=41.

17. http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=97BBACF714A05BF6459C5F476282F024?art_id=39738&cat_id=38835.

18. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article;jsessionid=BA075F688F4E729D7C88A20E1C636EA4?art_id=40393&cat_id=38835.

19. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074.

20. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40396&cat_id=38835.

20. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835.

21. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40381&cat_id=38835.

22. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40374&cat_id=38835.

23. http://tzi.com.ua/rubzh-rso-versya-20.html.

24. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074.

25.11. https://metod.onat.edu.ua.

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 здобувачем вищої освіти 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 практики.

Таблиця 1

Вид навчальної роботи	Max кількість балів	
	Денна форма навчання	Заочна форма навчання
Модуль № 1 «Забезпечення інформаційна безпека інформаційно-комунікаційних систем методами спеціальних вимірювань»		
Тема 1. Проблеми забезпечення безпеки інформаційно-комунікаційних систем	15	15
Тема 2. Захист інформації в системах зв'язку та передавання даних.	10	10
Усього за модулем № 1	**25**	**25**
Модуль № 2 «Нормативно правове регулювання заходів інформаційної безпеки»		
Тема 1. Нормативно-правові акти з основних положень інформаційної безпеки.	20	20
Тема 2. Ліцензування господарської діяльності з надання послуг у галузі криптографічного та технічного захисту інформації.	15	15
Усього за модулем № 2	**35**	**35**
Усього за модулями № 1, № 2	**60**	**60**
Індивідуальне завдання	**40**	**40**
Усього за дисципліною	**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	
23 - 25	32 - 35	36 - 40	Відмінно
19 - 22	26 - 34	31 - 35	Добре
15 - 18	21 - 25	24 - 30	Задовільно
менше 9	менше 9	менше 9	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 переддипломну 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./А, 87/Добре/В, 79/Добре/С, 68/Задов./D, 65/Задов./Е*** тощо.

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	НВ	22.01.2022	Гузовська О.Б		

(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		25.01.2022	
2.	Козловський В.В		26.01.2022	
3.	Темников В.О.		28.01.2022	
4.	Швець В.О.		28.01.2022	
5.	Щербак Т.Л.		28.01.2022	
6.	Журовський О.Л.		28.01.2022	

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності
1.	Муровський О. Л	29.08.2022		Актуально на 2022 - 2023 н.р.
2.	Кохоренко С.В.	28.08.2023		Актуально на 2023 - 2024 н.р.

(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				