МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра засобів захисту інформації

УЗГОДЖЕНО
Декан факультету

Катерина НЕСТЕРЕНКО

«12» 01 2022 р.

ЗАТВЕРДЖЕНО
Проректор з навчальної роботи

Анатолій ПОЛУХІН

«12» 01 2022 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: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека»

Форма навчання	Курс	Семестр	Усього (годин/кредитів ECTS)	Самостійна робота (годин)	Форма семестрового контролю
Денна	1	2	135/4,5	135	Диференційований залік
Заочна	1	2	135/4,5	135	

Індекс: НМ-4-125-2/21 – 2.2.1.1
РМ-4-125-2/21 – 2.2.1.1
НМ-4-125-2з/21 – 2.2.1.1
РМ-4-125-2з/21 – 2.2.1.1

СМЯ НАУ ПП 09.01.10-01-2022

Київ

Програма Науково-дослідної практики у сфері систем технічного захисту інформації, автоматизації її обробки розроблена на основі навчальних планів НМ-4-125-2/21 та НМ-4-125-2з/21 підготовки здобувачів вищої освіти ОС «Магістр», уведеного в дію наказом ректора від 29.04.2021 № 246/од, та робочих навчальних планів РМ-4-125-2/21 підготовки здобувачів вищої освіти ОС «Магістр», затвердженого проректором з навчальної роботи 28.08.2021 року, РМ-4-125-2з/21 підготовки здобувачів вищої освіти ОС «Магістр», затвердженого проректором з навчальної роботи 15.06.2021 року спеціальності 125 «Кібербезпека» освітньо-професійної програми (далі – ОПП) «Системи технічного захисту інформації, автоматизація її обробки».

Програму розробив:
Професор кафедри засобів захисту інформації _____ ЛАЗАРЕНКО С.В.

Гарант ОПП
Професор кафедри засобів захисту інформації _____ ЛАЗАРЕНКО С.В.

Програму Науково-дослідної практики у сфері систем технічного захисту інформації, автоматизації її обробки обговорено та схвалено на засіданні випускової кафедри засобів захисту інформації, протокол від «13» 12 2021 р. № 19

Завідувач кафедри _____ КОЗЛОВСЬКИЙ В.В.

Програму Науково-дослідної практики у сфері систем технічного захисту інформації, автоматизації її обробки обговорено та схвалено на засіданні науково-методично-редакційної ради Факультету кібербезпеки, комп'ютерної та програмної інженерії, протокол від «20» 12 2021 р. № 12

Голова НМРР
Заступник декана факультету _____ БНАТЮК С.О.

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

ЗМІСТ

сторінка

Вступ 4

1. Відомості про спеціальність та про освітньо-професійну програму 4
2. Відомості про бази практик 5
3. Цілі практики 5
4. Мета практики 6
5. Загальні компетентності 7
6. Фахові компетенції 7
7. Організація проведення практики 8
8. Тематичний план проходження практики 11
9. Підсумки проходження практики 12
10. Інформаційні джерела 15
11. Форма оцінювання проходження практики 17

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» (далі – Положення про організацію практики), 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

Спеціальність 125 «Кібербезпека» спрямована на захищеність 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 і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кафедра засобів захисту інформації (далі – ЗЗІ) Факультету кібербезпеки, комп'ютерної та програмної інженерії (далі – ФККПІ) здійснює підготовку фахівців за ОПП «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 «Кібербезпека».

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.

ОПП «Системи технічного захисту інформації, автоматизація її обробки» відповідає місії НАУ, у якій наголошується, щодо внеску НАУ у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей на основі інтеграції та інтернаціоналізації освіти, досліджень і 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 форми навчання і проводиться на підприємствах, організаціях та установах різних форм власності, а також оснащених відповідним чином структурних підрозділах Університету.

Науково-дослідна практика проводиться згідно з навчальним планом на 1-му курсу, у кінці 2-го семестру в обсязі 135 годин/4,5 кредити (3 тижні).

2. Відомості про бази практик

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

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 125 «Кібербезпека».

З базами практики, які відповідають меті, завданням, змісту практики та відповідним вимогам програми, університет завчасно укладає договори на її проведення.

Практиканти можуть пропонувати кафедрі місце проходження науково-дослідної практики. Кафедра дає згоду на проходження практики на таких базах лише за умови, що вони 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.

За результатами проведеної науково-дослідної практики практиканти повинні **знати:**

- спеціальні програмні продукти для проведення математичного моделювання;
- можливі джерела витоку інформації технічними каналами;
- основні організаційні заходи технічного захисту інформації;
- структуру підприємства та його інформаційні процеси;

- принципи роботи та функціональну структуру систем та засобів захисту інформації від несанкціонованого доступу;
- характеристики технічних пристроїв, які використовуються для забезпечення захисту інформації;
- питання розмежування доступу та захисту інформації;
- принципи автоматизації обробки інформації з обмеженим доступом.

Після проходження науково-дослідної практики практиканти повинні **вміти:**

- розробляти та модернізувати засоби обробки інформації з обмеженим доступом;
- самостійно знаходити можливі джерела витоку інформації;
- аналізувати роботу пристроїв захисту інформації;
- розробляти план заходів комплексного 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 і технологічним циклом створення систем захисту інформації, відпрацювання вмінь і навичок зі спеціальності 125 «Кібербезпека», а також збір матеріалу для виконання кваліфікаційних робіт.

Головним завданням 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 галузі кібербезпеки та захисту інформації.

5. Загальні компетентності

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 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

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).

Організаційне та навчально-методичне керівництво науково-дослідною практикою забезпечує кафедра ЗЗІ ФККПІ, яка здійснює наступні заходи:

- організовує проведення зборів практикантів з питань практики за участю керівника практики;
- повідомляє практикантів про систему звітності, а саме: подання письмового звіту, виконаного індивідуального завдання, підготовку доповіді, повідомлення, виступу тощо;
- обговорює підсумки та аналізує виконання програми практики на засіданні кафедри.

Бази практик в особі їх перших керівників разом з Університетом несуть відповідальність за організацію, якість і результати науково-дослідної практики практикантів.

До керівництва науково-дослідною практикою практикантів залучаються досвідчені викладачі кафедри ЗЗІ, які мають науковий ступінь та брали безпосередню участь в навчальному процесі.

Направлення практикантів на базу практики і призначення керівників практики здійснюється кафедрою ЗЗІ і оформлюється наказом ректора Університету.

Науково-дослідна практика передбачає присутність керівника практики тільки для здійснення організаційних, методичних, контролюючих та інших заходів протягом певного часу.

Тривалість робочого часу практикантів під час проходження науково-дослідної практики становить 6 годин на день.

Під час проходження науково-дослідної практики практиканти повинні суворо дотримуватись прийнятих на базі практики правил охорони праці і протипожежної безпеки з обов'язковим проходженням ними інструктажів (вступного і на кожному конкретному місці праці).

Керівник науково-дослідної практики від кафедри ЗЗІ зобов'язаний **до початку практики:**

- ознайомитися з програмою науково-дослідної практики;
- ознайомитися з необхідною навчально-методичною документацією щодо проходження науково-дослідної практики;
- познайомитися зі практикантами, що проходитимуть науково-дослідну практику;
- ознайомити практикантів з програмою науково-дослідної практики;
- провести інструктаж про порядок її проходження та з охорони праці й попередження нещасних випадків (під підпис);
- проконтролювати підготовленість бази практики, та вжити, за необхідності, потрібні заходи щодо її підготовки;
- проінформувати практикантів про систему звітності з практики, прийняту на кафедрі ЗЗІ;
- надати практикантам зразки необхідних документів та консультацію щодо їх оформлення;
- ознайомити керівника від бази практики з програмою науково-дослідної практики й узгодити графік її проходження;
- узгодити з керівником від бази практики індивідуальні завдання з урахуванням особливостей місця проведення практики.

під час практики:

- представити практикантів та керівника практики від бази практики і взяти участь у проведенні інструктажу з охорони праці, техніки безпеки, протипожежної безпеки та виробничої санітарії;
- у тісному контакті з керівником від бази практики забезпечити високу якість її проведення згідно з програмою;
- контролювати виконання практикантами правил внутрішнього розпорядку бази практики, вести облік проходження науково-дослідної практики практикантами;

- надавати практикантам необхідні консультації з питань проходження науково-дослідної практики та порядок надання звіту і оформлення;
- брати участь у роботі комісії, призначеної завідувачем кафедри ЗЗІ з проведення захисту звітів з науково-дослідної практики практикантів;
- здійснювати контроль за виконанням програми науково-дослідної практики та строками її проведення;
- проводити обов'язкові консультації щодо обробки зібраного матеріалу та його використання для звіту про науково-дослідну практику, а також у кваліфікаційній роботі;
- надавати методичну допомогу практикантам під час виконання ними індивідуальних завдань і збору матеріалів для кваліфікаційної роботи.

після закінчення практики:

- здати звіти практикантів про проходження практики на кафедру ЗЗІ;
- подати завідувачу кафедри ЗЗІ письмовий звіт про результати науково-дослідної практики із зауваженнями та пропозиціями щодо поліпшення її організації та проведення, який має зберігатися на кафедрі протягом строку, що визначається номенклатурою справ кафедри.

Від бази практики, для безпосереднього керівництва науково-дослідною практикою, призначаються висококваліфіковані фахівці, які ***зобов'язані:***

- забезпечити проведення обов'язкового інструктажу з охорони праці і створити практикантам умови безпечної праці на кожному робочому місці;
- створити всі необхідні умови для виконання практикантами програми практики та індивідуальних завдань;
- надавати, в межах своїх повноважень, практикантам та керівникам практик від Університету можливість користуватися лабораторіями, кабінетами, майстернями, бібліотекою, технічною та іншою документацією, необхідною для виконання програми практики та індивідуальних завдань;
- не допускати використання практикантів для виконання робіт, не передбачених програмою практики;
- інформувати кафедру ЗЗІ про порушення практикантами правил внутрішнього розпорядку бази практики та інші порушення, якщо такі мають місце;
- підготувати відгуки на кожного практиканта за результатами проходження ним практики, перевірити та затвердити його письмовий звіт.

Практиканти зобов'язані

до початку практики:

- ознайомитись з програмою науково-дослідної практики;
- ознайомитись із розробленими кафедрою ЗЗІ методичними рекомендаціями щодо проходження науково-дослідної практики;
- пройти на кафедрі ЗЗІ інструктаж про порядок її проходження та з охорони праці й попередження нещасних випадків (під підпис);
- ознайомитись із системою звітності з науково-дослідної практики;
- одержати від керівника практики від кафедри ЗЗІ зразки необхідних документів та консультацію щодо їх оформлення;

під час практики:

- ознайомитися з правилами внутрішнього трудового розпорядку бази практики;
- вивчити і суворо дотримуватись правил охорони праці;
- повідомляти керівника практики від кафедри ЗЗІ про виникнення труднощів з виконання програми науково-дослідної практики;
- вести щоденник (щоденні записи) про проходження науково-дослідної практики;
- у повному обсязі виконувати всі завдання, передбачені програмою науково-дослідної практики і вказівками її керівника;
- згідно з вимогами скласти звіт про виконання програми науково-дослідної практики і захистити його перед комісією у визначений строк.

8. Тематичний план проходження практики

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

Теми, які розглядаються під час науково-дослідної практики:

- аналіз структури підприємства, функціонального призначення структурних підрозділів, технічних характеристик засобів захисту інформації;
- дослідження інформаційних потоків та стану документообігу, порядок обігу конфіденційної інформації;
- дослідження систем контролю та управління доступом, програмних засобів захисту та організаційних заходів, інженерно-технічного забезпечення захисту інформації;
- дослідження етапів організації комплексної системи захисту інформації на підприємстві;
- аналіз функціонування комплексу технічного захисту інформації;
- аналіз основних напрямків подальшого розвитку підприємства, за необхідності формування пропозицій щодо поліпшення стану організації та забезпечення кібербезпеки на підприємстві.

Індивідуальні завдання

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

Індивідуальні завдання конкретизуються та уточнюються під час проходження науково-дослідної практики. 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.

Тематика занять та екскурсій

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 та інше.

Приблизна тематика навчальних завдань при проведенні науково-дослідної практики може бути наступна:

- законодавчо-правові основи забезпечення інформаційної/кібербезпеки;
- організаційні основи забезпечення інформаційної/кібербезпеки;
- побудова комплексної системи захисту інформації на підприємствах;
- побудова комплексів технічного захисту інформації на підприємствах;
- технологія застосування методів, механізмів та пристроїв технічного захисту інформації;
- аналіз можливих каналів витоку інформації;
- дослідження ефективності впроваджених правових, організаційних та технічних заходів із захисту інформації;
- правила розробки технічної (спеціалізованої) документації.

Основна тематика лекцій (бесід) уточнюється в процесі проходження науково-дослідної практики. Під час проходження науково-дослідної практики практикантам проводять екскурсії з метою надбання практикантами найбільш повного уявлення про базу практики, її структуру, взаємодію її структурних підрозділів, діючу систему управління. Час, що надається на навчальні заняття та екскурсії, не повинен перевищувати 6 годин на тиждень на одну групу практикантів.

9. Підсумки проходження практики

Під час науково-дослідної практики практиканти повинні щодня коротко записувати в щоденник усе, що він робив за день для виконання плану проходження науково-дослідної практики.

Щоденник (щоденні записи) – основний документ практикантів під час проходження науково-дослідної практики, що оформлюється в довільній формі (*орієнтовний зразок оформлення наведено в Додатку 3 Положення про організацію практики)* та додається до звіту про практику.

Не рідше одного разу на тиждень практиканти зобов'язані подавати щоденники на перегляд керівнику практики від кафедри ЗІІ, який перевіряє щоденник, дає письмові зауваження, додаткові запитання й візує записи, що їх зробили практиканти.

Без заповненого і підписаного щоденника практика не зараховується.

Не пізніше ніж за день до закінчення науково-дослідної практики практикант повинен отримати характеристику з місця проходження практики, підписану керівником підприємства та в обов'язковому порядку завірену печаткою бази практики.

У кінці строку проходження науково-дослідної практики практиканти оформлюють письмовий звіт про виконання програми науково-дослідної практики та індивідуального завдання (*орієнтовний зразок оформлення наведено в Додатку 4 Положення про організацію практики)*.

Для узагальнення матеріалу, напрацьованого практикантами під час науково-дослідної практики і підготовки звіту, передбачений час у її останні два-три дні.

В останні дні строку проходження практики практиканти повинні захистити звіти про практику.

Звіт з практики перевіряється та затверджується її керівниками від бази практики та кафедри ЗІІ, доповнюється відгуком керівника від бази практики і повертається практиканту для підготовки до захисту.

Звіт з практики захищається практикантом (з диференційною оцінкою) в комісії, призначеній завідувачем кафедри ЗІІ.

До складу комісії входять керівники практики від кафедри ЗІІ і, за можливості, від бази практики, а також викладачі кафедри ЗІІ, які були задіяні в освітньому процесі.

Робота комісії здійснюється у останні дні строку проходження науково-дослідної практики.

Під час захисту практикант має особисто охарактеризувати та критично оцінити виконану роботу, показати знання з теорії і практики організації роботи на базі практики, запропонувати і довести обґрунтованість та доцільність своїх пропозицій щодо її вдосконалення.

При оцінці підсумків роботи практиканта комісія бере до уваги зміст звіту, хід його захисту та відгук керівника від бази практики.

Оцінка за науково-дослідну практику вноситься до заліково-екзаменаційної відомості та до індивідуального навчального плану студента за підписом керівника практики від кафедри ЗІІ.

Після захисту звіт практиканта зберігається на відповідній кафедрі протягом одного року.

Практикант, який не виконав програму практики з неповажних причин або за підсумками її повторного проходження отримав в комісії незадовільну оцінку, **відраховується з Університету**.

За результатами проходження науково-дослідної практики практиканти повинні досягти наступні програмні результати навчання (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.

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

10. Інформаційні джерела

Рекомендована література (базова і допоміжна):

Базова

1. Бабуров Э.Ф., Куликов Э.Л., Маригодов В.К. Основы научных исследований: Учебн. пособ. - К.: Высш. шк. Головное изд-во, 1988. - 230 с.

2. Ворожко В.П., Корченко О.Г. Захист інформації з обмеженим доступом. Збірник нормативних документів. - К.: КМУЦА, 1999. - 283 с.

3. Головань С.М. Ведення документів, що містять інформацію з обмеження доступу: Навч.-метод. посіб. - К.: ІВЦ «Політехніка», 2001. - 88 с.

4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. - К.: ООО «ТИД ДС», 2001. - 688 с.

5. Хорошко В.О., Темніков В.О., Самохвалов Ю.Я. Організаційно-технічне забезпечення захисту інформації: Навч. посіб. / За ред. проф. В.О. Хорошка. - К.: НАУ, 2002. - 207 с.

6. Єріна А.М., Захожай В. Б., Єрін Д. Л. Методологія наукових досліджень: Навчальний посібник. -Київ: Центр навчальної літератури, 2004,-212с.

7. Мочерний С.В. Методологія економічного дослідження. - Л.: Світ, 2001. - 419 с.

8. Стіченко Д.М. Методологія наукових досліджень: Підручник. – К.: Знання-Прес, 2005. – 300с.

9. Сурмін Ю.Г. Майстерня вченого: Підручник. – К. : Знання-Прес, 2006. – 280 с.

10. Шейко В.М., Кушнаренко Н.М. Методика науково-дослідницької діяльності: Підручник. – К.: Знання-Прес, 2002. – 295с.

11. ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення».

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

13. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

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

Допоміжна

15. Жильцов О. Б. Математичне програмування (з елементами інформаційних технологій): Навч. посіб. / О. Б. Жильцов, В. Р. Кулян, О. О. Юнькова; За ред. О. О. Юнькової. – К.: МАУП, 2006. – 186 с.

16. Компьютерное моделирование бизнес-процессов: [учеб. пособие для студентов высш. учеб. заведений] / Сериков А. В., Титов Н. В., Белоцерковский А.В. и др.; Харьк. гос. техн. ун-т стр-ва и архитектуры. — Х.: Бурун Книга, 2007. – 320 с.

17. Кузьмичов А. І., Медведєв М. Г. Математичне програмування в Excel: Навч. посіб. – К.: Вид-во Європ. ун-ту, 2005. – 320 с.

18. Лудченко А.А. и др. Основы научных исследований: Учеб. пособие / Под ред. А.А. Лудченко. - К.: Т-во «Знання», КОО, 2000. - 114 с.

19. Філіпенко А.С. Основи наукових досліджень. Конспект лекцій: Посібник. - К.: Академвидав, 2004. - 208 с.

20. Закон України «Про вищу освіту».

21. Закон України «Про наукову і науково-технічну діяльність»

22. Основи методології та організації наукових досліджень: Навч. посіб. для студентів, курсантів, аспірантів і ад'юнктів / за ред. А. Є. Конверського. — К.: Центр учбової літератури, 2010. — 352 с.

Інформаційні ресурси в інтернеті

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

- http://www.nau.edu.ua;
- http://www.kzzi.nau.edu.ua.

Також, для навчання використовується:

- https://www.coursera.org/learn/r-programming/;
-http://prometheus.org.ua/dataanalysis/.

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

Оцінювання окремих видів виконаної практикантом роботи, під час проходження науково-дослідної практики, здійснюється в балах відповідно до табл. 11.1.

Рейтингова оцінка за захист звіту науково-дослідної практики визначається (в балах та за національною шкалою) за результатами виконання всіх видів робіт протягом науково-дослідної практики.

Таблиця 11.1

Вид навчальної роботи	Max кількість балів	
	Денна форма навчання	Заочна форма навчання
	2 семестр	2 семестр
Модуль № 1 «Дослідження кібербезпеки об'єктів інформаційної діяльності»		
Аналіз структури підприємства, функціонального призначення структурних підрозділів, технічних характеристик засобів захисту інформації	10	6
Дослідження інформаційних потоків та стану документообігу, порядок обігу конфіденційної інформації	10	6
Дослідження систем контролю та управління доступом, програмних засобів захисту та організаційних заходів, інженерно-технічного забезпечення захисту інформації	10	6
Дослідження організації комплексної системи захисту інформації на підприємстві	10	8
Аналіз функціонування комплексу технічного захисту інформації	10	8
Аналіз основних напрямків подальшого розвитку підприємства, за необхідності формування пропозицій щодо поліпшення стану організації та забезпечення кібербезпеки на підприємстві	10	6
Виконання індивідуального завдання	20	20
Усього за модулем № 1	**80**	**60**
Захист звіту науково-дослідної практики	**20**	**40**
Усього за науково-дослідну практику	**100**	

Виконані види робіт науково-дослідної практики зараховуються практиканту, якщо він отримав за них позитивну рейтингову оцінку (табл. 11.2).

Сума підсумкової модульної рейтингової оцінки та рейтингової оцінки за захист звіту науково-дослідної практики, у балах (табл. 11.3, 11.4), становить підсумкову рейтингову оцінку за науково-дослідну практику, яка перераховується в оцінки за національною шкалою та шкалою ECTS (табл. 11.5).

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

Таблиця 11.2

Відповідність рейтингових оцінок за окремі види робіт науково-дослідної практики в балах оцінкам за національною шкалою

Рейтингова оцінка в балах				Оцінка за національною шкалою
Виконання окремих видів робіт науково-дослідної практики			Виконання індивідуального завдання	
6	8	9 - 10	18 - 20	Відмінно
5	6 - 7	8	15 - 17	Добре
4	5	6 - 7	12 - 14	Задовільно
менше 4	менше 5	менше 7	менше 12	Незадовільно

Таблиця 11.3

Відповідність підсумкової модульної рейтингової оцінки в балах оцінкам за національною шкалою

Оцінка в балах		Оцінка за національною шкалою
72 - 80	54 - 60	Відмінно
60 - 71	45 - 53	Добре
48 - 59	36 - 44	Задовільно
менше 48	менше 44	Незадовільно

Таблиця 11.4

Відповідність рейтингової оцінки за захист звіту в балах оцінці за національною шкалою

Оцінка в балах		Оцінка за національною шкалою
18 - 20	36 - 40	Відмінно
15 - 17	30 - 35	Добре
12 - 14	24 - 29	Задовільно
менше 12	менше 24	Незадовільно

Таблиця 11.5

Відповідність підсумкової рейтингової оцінки за науково-дослідну практику 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)

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	НВ	13.01.2022	Гузовська О.Б.	[signature]	

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки
1	Лазаренко Сергій Володимирович	[signature]	20.01.2022	
2	Козловський В.В.	[signature]	20.01.2022	

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності
1	Лазаренко С.В	23.08.2023		Актуальна по 2024/2025 н.р
2	Лазаренко С.В	28.08.2023		Актуальна на 2024/2025 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				