(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет
Факультет кібербезпеки та програмної інженерії
Кафедра безпеки інформаційних технологій

УЗГОДЖЕНО
В.о.декана ФКПІ
_____ О. Пономаренко
«23» 02 2024 р.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
_____ А. Полухін
«05» 03 2024 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА
навчальної дисципліни
«Методологія прикладних досліджень у сфері кібербезпеки»

Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека та захист інформації»

Освітньо-професійні програми «Безпека інформаційних і комунікаційних систем»
«Системи технічного захисту інформації, автоматизація її обробки»
«Системи та технології кібербезпеки»

Форма навчання	Семестр	Усього (годин/ кредитів ECTS)	Лекції	Практ. заняття	Лабораторні	Самостійна робота	ДЗ / РГР /К	КР / КПр	Форма сем. контролю
Денна	1	120/4,0	17	-	17	86	-	КП 1с	диф.залік 1с
Заочна	1	120/4,0	6	-	8	106	1 к 1 с	КП 1с	диф.залік 1с

Індекс РМ-14-125-1/23-2.1.2 РМ-14-125-1з/23-2.1.2
РМ-14-125-2/23-2.1.2
РМ-14-125-3/23-2.1.2

	Система менеджменту якості. Робоча програма навчальної дисципліни «Методологія прикладних досліджень у сфері кібербезпеки»	Шифр документа	СМЯ НАУ РП 18.01 – 01-2024
			Стор. 2 із 15

Робоча програма дисципліни «Методологія прикладних досліджень у сфері кібербезпеки» розроблена на основі освітньо-професійної програми «Системи та технології кібербезпеки», «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації, автоматизація її обробки», навчальних та робочих навчальних планів НМ-4-125-1/21-2.1.2, РМ-14-125-1/23-2.1.2, НМ-4-125-2/21-2.1.2, РМ-14-125-2/23-2.1.2, НМ-14-125-3/23-2.1.2, РМ-14-125-3/23-2.1.2, НМ-14-125-1з/23-2.1.2, РМ-14-125-1з/23-2.1.2 підготовки здобувачів вищої освіти освітнього ступеня «Магістр» за спеціальністю 125 «Кібербезпека та захист інформації» та відповідних нормативних документів.

Робочу програму розробили:
професор кафедри безпеки інформаційних технологій _____ О. Корченко
старший викладач кафедри безпеки інформаційних технологій _____ І. Лозова

Робочу програму обговорено та схвалено на засіданні випускової кафедри спеціальності 125 «Кібербезпека та захист інформації» (освітньо-професійної програми «Системи та технології кібербезпеки») – кафедри безпеки інформаційних технологій, протокол №7 від 28.08.2023 р.

Гарант освітньої програми _____ Є. Іванченко
В.о.завідувача кафедри _____ Є. Іванченко

Робочу програму обговорено та схвалено на засіданні випускової кафедри спеціальності 125 «Кібербезпека та захист інформації» (освітньо-професійна програма «Безпека інформаційних і комунікаційних систем») – кафедри безпеки інформаційних і комунікаційних систем, протокол № 2 від 04. 09 .2023р.

Гарант освітньої програми _____ М. Степанов
Завідувач кафедри _____ М. Степанов

Робочу програму обговорено та схвалено на засіданні випускової кафедри спеціальності 125 «Кібербезпека та захист інформації» (освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки») – кафедри засобів захисту інформації, протокол № 1 від 04. 09 .2023р.

Гарант освітньої програми _____ С. Лазаренко
Завідувач кафедри _____ В. Козловський

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету кібербезпеки та програмної інженерії, протокол № 1 від 10. 01 .2024р.

Голова НМРР _____ О. Пономаренко

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

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Методологія прикладних досліджень у сфері кібербезпеки» розроблена на основі «Методичних рекомендацій до розроблення і оформлення робочої програми навчальної дисципліни денної та заочної форм навчання», затверджених наказом ректора від 29.04.2021 № 249/од, та відповідних нормативних документів.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

1.1. Місце, мета, завдання навчальної дисципліни.

Місце даної дисципліни є теоретичною основою сукупності знань та вмінь, що формують профіль професіонала із організації інформаційної безпеки в області в області постановки, організації, планування, виконання і керування науковими дослідженнями, колективною науковою творчістю.

Мета та завдання даної дисципліни полягає в наданні студентам загальних теоретичних знань закономірностей і методів наукової творчості, розвиток в них практичних умінь і навичок рішення реальних задач в області постановки, організації, планування, виконання і керування науковими дослідженнями, колективною науковою творчістю.

Завданнями вивчення навчальної дисципліни є:

– навчити використовувати набуті знання з основних напрямків, закономірностей, змісту і форм наукової творчості, методів планування, організації і керування науковою творчістю, роботи наукових колективів, сучасних теоретичних і експериментальних методів пошуку нових наукових рішень, принципів патентного пошуку, патентування, винахідницької і раціоналізаторської роботи, написання наукових робіт;

– виявити задатки і розвити творчі здібності студентів, виробити основні практичні навички й уміння виконувати наукові дослідження, працювати в наукових колективах.

1.2. Результати навчання, які дає можливість досягти навчальна дисципліна.

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем»:

ПРН 1. 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.

ПРН 2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН 3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

ПРН 17. 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.

ПРН 20. Ставити та вирішувати складні інженерноприкладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

Освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки»:

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.

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.

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

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.

Освітньо-професійна програма «Системи та технології кібербезпеки»

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

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.

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.

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.

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.

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. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки, в тому числі в галузі авіаційної безпеки.

ПРН25. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки, що дозволяє вирішувати практичні завдання підвищення рівня безпекових процесів в тому числі і в сфері авіаційної безпеки.

1.3. Компетентності, які дає можливість здобути навчальна дисципліна.

Компетентності набуті студентом в результаті вивчення дисципліни:

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем»:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Здатність проводити дослідження на відповідному рівні.

ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

ЗК 6. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ФК 10. 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.

Освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки»:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Здатність проводити дослідження на відповідному рівні.

ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

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.

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.

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.

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.

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

Освітньо-професійна програма «Системи та технології кібербезпеки»:

ЗК2. Здатність проводити дослідження на відповідному рівні.

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

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.

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.

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.

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 аргументувати вибір методів розв’язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення.

ФК12. Здатність організовувати роботу колективів виконавців, приймати управлінські рішення в умовах спектра думок, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем захисту інформації.

ФК13. Здатність готувати та здійснювати публічні виступи з презентацією отриманих результатів, готувати науково-технічні публікації (звіти, статті тощо) за результатами виконаних досліджень.

ФК14. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації, а також застосовувати методи і засоби організаційного характеру щодо захисту інформації на об’єктах критичної інфраструктури держави, включаючи авіаційну галузь.

1.4. Міждисциплінарні зв’язки

Навчальна дисципліна «Методологія прикладних досліджень у сфері кібербезпеки» доповнює такі дисципліни, як: «Організаційні моделі кібербезпеки», «Моделювання та оптимізація безпекових процесів авіаційної галузі» «Системи і методи прийняття рішень» та є основою для вивчення таких дисциплін, як: «Інтелектуалізовані системи інформаційної безпеки», «Наукові комунікації у фаховій діяльності» та інших.

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст навчальної дисципліни

Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох навчальних модулів, а саме: навчального **модуля №1 «Методологія**

прикладних досліджень у сфері кібербезпеки», який є логічно завершеною, відносно самостійною, цілісною частиною навчальної дисципліни, засвоєння якої передбачає проведення модульної контрольної роботи та аналіз результатів її виконання. Окремим **модулем №2** є курсовий проект (КП), який здобувач вищої освіти виконує у 1 семестрі. КП є важливою складовою закріплення та поглиблення теоретичних та практичних знань та вмінь, набутих студентом у процесі засвоєння навчального матеріалу дисципліни.

2.2. Модульне структурування та інтегровані вимоги до кожного модуля.

Модуль №1 «Методологія прикладних досліджень у сфері кібербезпеки».

Інтегровані вимоги модуля №1:

Знати:

– місце, предмет, основну мету, головні задачі і методи наукової творчості;

– основні напрямки, проблеми і перспективи розвитку науки і техніки за фахом, у тому числі за тематикою магістерської роботи;

– принципи та засоби пошуку наукової і патентної інформації у тому числі автоматизованого;

– методику і техніку оформлення результатів наукового дослідження.

Вміти:

– самостійно планувати та виконувати наукові дослідження, пошук нових наукових рішень;

– працювати в наукових колективах;

– працювати з науково-технічною літературою і патентною інформацією, оформляти результати наукових досліджень із забезпеченням авторських прав;

– виконувати патентний пошук, розробляти, оформляти і подавати заявки на одержання патентів

Тема 1. Місце дисципліни в системі підготовки професіонала із організації інформаційної безпеки. Технічні аспекти і основні закономірності розвитку науки.

Предмет і сутність науки як сфери людської діяльності. Понятійний апарат, зміст та класифікація наук. Організація наукової діяльності в Україні.

Тема 2. Методи наукового дослідження. Загальні закономірності розвитку науки.

Методологія і логіка наукових досліджень. Загальнонаукові методи досліджень. Розвиток методів науки. Наука як система. Класифікація наук. Організаційні основи наукових досліджень. Загальні питання управління наукою. Підготовка наукових кадрів. Науково-дослідна робота студентів.

Тема 3. Вибір напрямку наукового дослідження та етапи науково-дослідної роботи.

Класифікація науково-дослідних робіт. Вибір і оцінка тем наукових досліджень. Етапи науково-дослідної роботи. Етапи дослідно-конструкторських розробок.

Тема 4. Пошук, нагромадження і обробка наукової інформації.

Особливості науково-технічної інформації. Наукові документи і видання. Системи науково-технічної інформації. Аналіз інформації і формулювання задач наукового дослідження.

Тема 5. Проведення експерименту.

Поняття експерименту і його класифікація. Методика проведення експерименту. Метрологічне забезпечення експериментальних досліджень. Вплив організації робочого місця і психологічних факторів на хід і якість експерименту.

Тема 6. Усне представлення наукової інформації.

Види і форми усних представлень наукової інформації. Підготовка до виступу. Постановка питань і формулювання відповідей. Діалектика і психологія суперечки: принципи, правила, вимоги.

Тема 7. Методика і техніка оформлення результатів дослідження.

Основи методики оформлення. Послідовність і стиль викладу матеріалу. Структура і техніка оформлення наукового документа (дисертаційні та магістерські роботи, науковий звіт, наукові статті, реферати, анотації, матеріали конференцій, тези доповідей). Депонування рукописних робіт. Винаходи та раціоналізаторські пропозиції. Довідково-бібліографічне оформлення наукового документа.

Тема 8. Правова охорона наукової творчості

Авторське право. Право на відкриття. Право на винахід, раціоналізаторську пропозицію.

Модуль №2 Курсовий проект.

Курсовий проект (КП) з дисципліни виконується у 1 семестрі. Курсовий проект представляє собою комплексну роботу, що охоплює кілька підрозділів програми. Тематика роботи спрямована на написання наукової статті відповідно до вимог ВАК України; формули винаходу; експертизи формули винаходу. Має за мету застосування на практиці теоретичних знань з оформлення результатів наукових досліджень із забезпеченням авторських прав та з виконання патентного пошуку, розробки, оформлення і подачі заявки на одержання патентів. За навчальною програмою для виконання курсового проекту передбачено 45 години самостійної роботи студента.

Звітом про виконаний курсовий проект є пояснювальна записка, що містить стислі теоретичні відомості, постановку задачі на написання наукової статті відповідно до вимог ВАК України; формули винаходу; експертизи формули винаходу та опису процесу їх розробки.

Виконання, оформлення та захист КП здійснюється студентом в індивідуальному порядку.

2.3. Тематичний план

№ п/п	Назва теми	Обсяг навчальних занять (год.)							
		Денна форма навчання				Заочна форма навчання			
		Усього	Лекції	Лабор. заняття	СРС	*Усього*	Лекції	Лабор. заняття	СРС
1	2	3	4	5	6	7	8	9	10
Модуль №1 «Методологія прикладних досліджень у сфері кібербезпеки»									
1.1	Місце дисципліни в системі підготовки професіонала із організації інформаційної безпеки. Технічні аспекти і основні закономірності розвитку науки	1 семестр				1 семестр			
		8	2	2	4	6	–	–	6
1.2	Методи наукового дослідження. Загальні закономірності розвитку науки	8	2	2	4	9	2	1	6
1.3	Вибір напрямку наукового дослідження та етапи науково-дослідної роботи	9	2	2	5	6	–	–	6
1.4	Пошук, нагромадження і обробка наукової	9	2	2	5	8	–	2	6

1	2	3	4	5	6	7	8	9	10
	інформації								
1.5	Проведення експерименту	9	2	2	5	11	2	2	7
1.6	Усне представлення наукової інформації	9	2	2	5	6	–	–	6
1.7	Методика і техніка оформлення результатів дослідження	11	2	2 1	6	12	2	2	8
1.8	Правова охорона наукової творчості	9	2	2	5	6	–	–	6
1.9	Виконання контрольної роботи	–	–	–	–	8	–	–	8
1.10	Модульна контрольна робота №1	3	1	–	2	–	–	–	–
1.11	Підсумкова семестрова контрольна робота	–	–	–	–	3	–	1	2
Усього за модулем №1		***75***	***17***	***17***	***41***	***75***	***6***	***8***	***61***
Модуль №2 «Курсовий проект»									
Написання наукової статті. Оформлення та експертиза заявки на винахід		45	–	–	45	45	–	–	45
Усього за модулем №1		***45***	–	–	***45***	***45***	–	–	***45***
Усього за навчальною дисципліною		***120***	***17***	***17***	***86***	***120***	***6***	***8***	***106***

2.4. Завдання на контрольну (домашню) роботу (ЗФН).

Контрольна (домашня) робота (ЗФН).

Контрольна (домашня) робота з дисципліни виконується у першому семестрі, відповідно до затверджених в установленому порядку методичних рекомендацій, **з метою** закріплення та поглиблення теоретичних знань та вмінь здобувача вищої освіти при вивченні дисципліни.

Теми та завдання для виконання практичної частини контрольної (домашньої) роботи здійснюється здобувачем вищої освіти в індивідуальному порядку відповідно до методичних рекомендацій, розроблених провідними викладачами кафедри.

Час, потрібний для виконання контрольної складає 8 годин самостійної роботи.

2.5. Перелік питань для підготовки до підсумкової контрольної роботи

Перелік питань та зміст завдань для підготовки до підсумкової контрольної роботи, розробляються провідним викладачем кафедри відповідно до робочої програми, затверджується на засіданні кафедри та доноситься до відома студентів.

3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.1. Методи навчання.

При вивчення навчальної дисципліни використовуються наступні методи навчання:

– пояснювально-ілюстративний метод;

– метод проблемного викладу;

– репродуктивний метод;

– дослідницький метод.

Реалізація цих методів здійснюється при проведенні лекцій, демонстрацій, самостійному вирішенні задач, роботі з навчальною літературою, аналізі та вирішенні задач з прикладних досліджень у сфері кібербезпеки.

3.2. Рекомендована література.

Базова література.

3.2.1. Основи наукових досліджень: навчальний посібник / О. М. Сінчук, Т. М. Берідзе, М. Л. Барановська, О.В. Данілін, Д.О. Кальмус. Кременчук: ПП Щербатих О. В., 2022. 196 с.

3.2.2. Марта Мальська, Наталія Паньків. Основи наукових досліджень : навчальний посібник. Львів : Видавництво ЛНУ імені Івана Франка, 2020. 226 с.

3.2.3. Вітченко А. О., Вітченко А. Ю. Основи наукових досліджень у вищій школі : підруч. Київ : ФОП Ямчинський О.В., 2020. 272 с.

3.2.4. Самсонов В.В., Сільвестров А.М., Тачиніна О.М. Методологія наукових досліджень та приклади її використання: Навч. посібник. К.:НУХТ, 2022. 385 с.

3.2.5. Данильян О. Г., Дзьобань О. П. Методологія наукових досліджень : підручник. Харків: Право, 2019. 368 с.

3.2.6. Медвідь В. Ю., Данько Ю. І., Коблянська І. І. Методологія та організація наукових досліджень (у структурно-логічних схемах і таблицях): навч. посіб. Суми: СНАУ, 2020. 220 с.

Допоміжна література.

3.2.7. Основи наукових досліджень. Курс лекцій. [Електронний ресурс]: навч. посіб. для здобувачів ступеня магістра за спеціальністю 172 Електронні комунікації та радіотехніка / О. Б. Шарпан (уклад.). К.: КПІ ім. Ігоря Сікорського, 2023. 89 с.

3.2.8. Вегеш Микола. Основи наукових досліджень. Методичний посібник для студентів спеціальності 052 "Політологія". Ужгород. 2021. 67 с.

3.3. Інформаційні ресурси в Інтернет.

3.3.1. Національна бібліотека України імені В. І. Вернадського [Електронний ресурс]: [Веб-сайт]. Електронні дані. Київ: НБУВ. Режим доступу: www.nbuv.gov.ua – Назва з екрана.

3.3.2. Електронний каталог Національної бібліотеки України імені Ярослава Мудрого [Електронний ресурс]: [політемат. база даних містить відом. про вітчизн. та зарубіж. кн., брош., що надходять у фонд НБУ України]. Електронні дані (803 438 записів). Київ: Нац. б-ка України ім.Я. Мудрого. Режим доступу: http://catalogue.nlu.org.ua/. – Назва з екрана.

3.3.3. Державне підприємство "Український інститут інтелектуальної власності" [Електронний ресурс]: [Веб-сайт]. Електронні дані. Київ: УІІВ, 2024. Режим доступу: https://ukrpatent.org/uk – Назва з екрана.

3.3.4. Методичні розробки кафедри (в електронному вигляді).

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

4.1. Оцінювання окремих видів виконаної студентом навчальної роботи здійснюється в балах відповідно до табл. 4.1.

Таблиця 4.1

	Максимальна кількість балів	
	Денна форма	**Заочна форма**
Вид навчальної роботи	**Модуль №1**	
Виконання та захист лабораторних робіт	**1 семестр**	**1 семестр**
	8×10б = 80	4×10б = 40
Виконання та захист контрольної (домашної) роботи	-	30
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше 48 балів		-
Виконання модульної контрольної роботи №1	20	-
Підсумкова семестрова контрольна робота	-	30
Усього за модулем №1	100	100
Усього за дисципліною	**100**	

	Модуль №2	
	1 семестр	**1 семестр**
Виконання курсового проекту	60	60
Захист курсового проекту	40	40
Виконання та захист курсового проекту	**100**	

4.2. Виконані види навчальної роботи зараховуються студенту, якщо він отримав за них позитивну рейтингову оцінку.

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

4.3. Сума рейтингових оцінок, отриманих студентом за окремі види виконаної навчальної роботи, становить поточну модульну рейтингову оцінку, яка заноситься до відомості модульного контролю.

4.4. Сума поточної та контрольної модульних рейтингових оцінок становить підсумкову модульну рейтингову оцінку, яка в балах та за національною шкалою заноситься до відомості модульного контролю.

4.5. Підсумкова модульна рейтингова оцінка у балах становить підсумкову семестрову модульну рейтингову оцінку, яка перераховується в оцінку за національною шкалою.

4.6. Сума підсумкової семестрової модульної та екзаменаційної рейтингових оцінок, у балах становить підсумкову семестрову рейтингову оцінку, яка перераховується в оцінки за національною шкалою та шкалою ECTS.

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

4.8. Підсумкова рейтингова оцінка з дисципліни дорівнює підсумковій семестровій рейтинговій оцінці. Зазначена підсумкова рейтингова оцінка з дисципліни заноситься до Додатку до диплома.

4.9. Підсумкова модульна рейтингова оцінка, отримана здобувачем вищої освіти за результатами виконання та захисту курсового проекту, крім відомості модульного контролю, заноситься також до навчальної картки, залікової книжки та Додатку до диплома, наприклад, так: ***92/Відм./A, 87/Добре/B, 79/Добре/C, 68/Задов./E*** тощо.

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

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

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

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

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

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

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

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

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				