(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки та програмної інженерії
Кафедра засобів захисту інформації

УЗГОДЖЕНО
Декан
_____ К. Нестеренко
«25» 04 2023 р.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
_____ А. Полухін
«06» 06 2023 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА

навчальної дисципліни
«Безпека в кібернетичному просторі»

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

Форма навчання	Сем.	Усього (год. / кредитів ECTS)	ЛКЦ	ПР.З	Л.З	СРС	ДЗ / РГР / К.р	КР / КП	Форма сем. контролю
Денна	1	105/3,5	17	-	17	71	1	-	Диференційований залік
Заочна	1	105/3,5	6	-	6	93	1	-	

Індекс: НМ-4-125-2/21 - 2.1.4
Індекс: НМ-4-125-2з/21 - 2.1.4

СМЯ НАУ РП 18.03-01-2023

Робочу програму навчальної дисципліни «Безпека в кібернетичному просторі» розроблено на основі освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки», професійних стандартів, навчальних та робочих навчальних планів № НМ-4-125-2/21, № РМ-4-125-2/22 та № НМ-4-125-2з/21, № РМ-4-125-2з/21 підготовки здобувачів вищої освіти освітнього ступеня «Магістр» за спеціальністю 125 «Кібербезпека» та відповідних нормативних документів.

Робочу програму розробив:

Завідувач кафедри засобів захисту інформації

професор _____ Козловський В.В.

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки», спеціальності 125 «Кібербезпека» – кафедри засобів захисту інформації (випускова), протокол № 3 від «20» 03 2023 р.

Гарант освітньо-професійної програми _____ Лазаренко С.В.

Завідувач кафедри _____ Козловський В.В.

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради Факультету кібербезпеки та програмної інженерії, протокол № 3 від «18» 04 2023 р.

Голова НМРР _____ Куклінський М.В.

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

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Безпека в кібернетичному просторі» 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.

Навчальна дисципліна «Безпека в кібернетичному просторі» відноситься до циклу професійної підготовки обов'язкової компоненти та є теоретичною і практичною основою сукупності знань та вмінь, що формують профіль фахівця в галузі інформаційної/кібернетичної безпеки.

Метою навчальної дисципліни є засвоєння основних способів та методів захисту інформації в кібернетичному просторі, протидії кіберзагрозам та несанкціонованому доступу до інформації.

Завданнями вивчення навчальної дисципліни є:

- вивчення сучасних інформаційних технологій у галузі інформаційної/кібербезпеки;
- впровадження методів та засобів запобігання несанкціонованому отриманню інформації;
- застосування методів та засобів криптографічного захисту інформації;
- впровадження технологій захисту інформації в кіберпросторі та виявлення кібератак.

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

За результатами вивчення навчальної дисципліни «Безпека в кібернетичному просторі» студенти набувають таких знань та вмінь:

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

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.

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.

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.

Трудові функції

А. Організовувати та практично реалізовувати заходи з питань безпеки інформаційно-комунікаційних технологій.

В. Здійснювати моніторинг та оцінювання діяльності з питань безпеки інформаційно-комунікаційних технологій.

Г. Забезпечувати контроль/нагляд за діяльністю з питань безпеки інформаційно-комунікаційних технологій.

Д. Організовувати координацію та приймати участь в управлінні діяльністю із забезпечення безпеки інформаційно-комунікаційних технологій.

1.3. Компетентності, які дає можливість здобути навчальна дисципліна.

За результатами вивчення навчальної дисципліни «Безпека інформаційно-комунікаційних систем» студенти повинні здобути наступні програмні компетентності:

Інтегральну

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

Загальні

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

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).

Фахові

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.

1.4. Міждисциплінарні зв'язки

Навчальна дисципліна «Безпека в кібернетичному просторі» базується на знаннях таких дисциплін: «Ділова іноземна мова», «Методи побудови та аналізу криптосистем», «Моделювання та оптимізація безпекових процесів авіаційної галузі» та є базою для вивчення наступних дисциплін: «Автоматизація обробки інформації з обмеженим доступом», проходження виробничих практик, підготовки та захисту магістерської кваліфікаційної роботи.

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 «Забезпечення безпеки у кіберпросторі»;**

– навчального **модуля № 2 «Забезпечення кібербезпеки складних систем».**

Кожен з модулів є логічно завершеною, відносно самостійною, цілісною частиною навчальної дисципліни, засвоєння якої передбачає проведення модульної контрольної роботи та аналіз результатів її виконання.

2.2. Модульне структурування та інтегровані вимоги до кожного модуля.

Модуль № 1 «Забезпечення безпеки в кіберпросторі».

Інтегровані вимоги модуля № 1:

знати

- поняття кіберпростору та кібербезпеки;
- комп'ютерні віруси та вірусоподібні програми;
- сучасні методи автентифікації та ідентифікації;
- принципи забезпечення безпеки програмного забезпечення;
- порядок забезпечення безпеки віддалених інформаційних ресурсів.

вміти

- використовувати державні нормативно-правові акти та міжнародні стандарти щодо забезпечення кібербезпеки;
- застосовувати методи та засоби забезпечення безпеки програм та даних;
- забезпечувати безпеку віддалених інформаційних ресурсів.

Тема 1. Поняття кібербезпеки, кіберпростору та кіберзлочинності.

Поняття кібербезпеки, кіберпростору та кіберзлочинності. Кіберпростір та кібербезпека як головні ознаки нової інформаційної цивілізації. Загрози, вразливості та атаки. Державні нормативно-правові акти та міжнародні стандарти у галузі кібербезпеки.

Тема 2. Безпека програм та даних на основі механізмів та політик розмежування прав доступу до даних.

Використання хеш функцій (на прикладі MD5), оцінка стійкості паролю до зламу. Сучасні методи автентифікації та ідентифікації користувачів для захисту даних – електронний цифровий підпис, біометричні методи автентифікації.

Тема 3. Забезпечення безпеки програмних застосунків у кіберпросторі.

Захист сесій веб-застосунків. Контроль коректності даних, що вводяться (SQL-захист від інжекції). Забезпечення безпеки скриптів (захист від атак міжсайтового скриптингу). Аудит коду і незалежне тестування програмного коду. Підтвердження достовірності провайдера для споживачів.

Тема 4. Забезпечення безпеки віддалених інформаційних ресурсів у кіберпросторі.

Безпечне конфігурування серверів. Установка системи оновлень безпеки. Контроль системних журналів. Захист від шкідливих програм. Регулярне сканування контенту на наявність шкідливих програм. Регулярне сканування уразливостей сайту і додатків. Виявлення спроб злому та кібератак.

Модуль № 2 «Забезпечення кібербезпеки складних систем».

Інтегровані вимоги модуля № 2:

знати

- порядок забезпечення безпеки користувачів у кіберпросторі;
- методи та засоби криптографічного захисту інформації;
- поняття соціальної інженерії та способи захисту від соціоатак;
- методи та способи кібербезпеки складних систем.

вміти

- класифікувати віддалені атаки на кінцевих користувачів в інформаційно-комунікаційних системах та кіберпросторі;
- застосовувати методи криптографічного захисту інформації;
- забезпечувати захист від соціоатак;
- забезпечувати захист складних систем.

Тема 1. Забезпечення безпеки кінцевих користувачів у кіберпросторі.

Використання пасток в «порожній» мережі. Перенаправлення шкідливого трафіку. Зворотне трасування. Використання рекомендованих версій операційних систем, програмних додатків. Використання антивірусних засобів. Налаштування веб-браузерів в безпечному режимі, використання додаткових механізмів безпеки веб-браузерів. Використання фільтрів фітинг. Використання міжмережевих екранів і систем виявлення вторгнень. Використання автоматичних оновлень довірених програм.

Тема 2. Методи криптографічного захисту даних.

Шифри та їх використання. Методи шифрування даних в комп'ютерних системах загального призначення, симетричні та асиметричні алгоритми шифрування. Асиметричні методи шифрування та їх підтримка в бібліотеках мов програмування. Методи приховування інформації в потоках даних. Стеганографія.

Тема 3. Захист від атак методами соціальної інженерії у кіберпросторі.

Розробка і впровадження політик безпеки. Категорування та класифікація інформації. Соціальна інженерія, як метод розвідки. Моніторинг соціальних мереж. Використання технічних механізмів контролю.

Тема 4. Забезпечення кібербезпеки різних систем.

Забезпечення кібербезпеки в медицині, енергетиці, мобільних телефонах. Кібербезпека систем - банкінгу, електронної комерції, інтернет речей, соціальних мереж, хмарних застосунків.

2.3. Тематичний план.

№ пор	Назва теми (тематичного розділу)	Обсяг навчальних занять (год.)							
		Денна форма навчання				Заочна форма навчання			
		Усього	Лекції	Лаб./прак. заняття	СРС	Усього	Лекції	Лаб./прак. заняття	СРС
		1 семестр				1 семестр			
1	2	3				4			
Модуль № 1 «Забезпечення безпеки в кіберпросторі»									
1.1	Тема 1. Поняття кібербезпеки, кіберпростору та кіберзлочинності.	11	2	2	7	12	2	-	10
1.2	Тема 2. Безпека програм та даних на основі механізмів та політик розмежування прав доступу до даних.	11	2	2	7	12	-	2	10
1.3	Тема 3. Забезпечення безпеки програмних застосунків у кіберпросторі.	11	2	2	7	10	-	-	10
1.4	Тема 4. Забезпечення безпеки віддалених інформаційних ресурсів у кіберпросторі.	11	2	2	7	10	-	-	10
1.5	Модульна контрольна робота № 1	4	1	-	3	-	-	-	-
Усього за модулем № 1		**48**	**9**	**8**	**31**	**44**	**2**	**2**	**40**

1	2	3				4			
Модуль № 2 «Забезпечення кібербезпеки складних систем»									
2.1	Тема 1. Забезпечення безпеки кінцевих користувачів у кіберпросторі.	11	2	2	7	10	-	-	10
2.2	Тема 2. Методи криптографічного захисту даних.	11	2	2	7	16	2	2	12
2.3	Тема 3. Захист від атак методами соціальної інженерії у кіберпросторі.	11	2	2	7	10	-	-	10
2.4	Тема 4. Забезпечення кібербезпеки різних систем.	11	2	2	7	14	2	1	11
2.5	Модульна контрольна робота № 2	5	-	1	4	-	-	-	-
2.6	Домашнє завдання	8	-	-	8	-	-	-	-
2.7	Контрольна (домашня) робота	-	-	-	-	8	-	-	8
2.8	Підсумкова семестрова контрольна робота	-	-	-	-	3	-	1	2
Усього за модулем № 2		**57**	**8**	**9**	**40**	**61**	**4**	**4**	**53**
Усього за навчальною дисципліною		**105**	**17**	**17**	**71**	**105**	**6**	**6**	**93**

2.4. Домашнє завдання, завдання на контрольну (домашню) роботу.

Домашнє завдання, завдання на контрольну (домашню) роботу з дисципліни «Безпека в кібернетичному просторі» виконується самостійно кожним студентом і є важливим етапом у засвоєнні навчального матеріалу.

Домашнє завдання, завдання на контрольну (домашню) роботу охоплює всі основні теми дисципліни «Безпека в кібернетичному просторі» та виконується з метою закріплення та поглиблення теоретичних знань та вмінь студентів щодо безпеки в кібернетичному просторі.

Питання для виконання домашнього завдання доводяться викладачем до студента індивідуально і виконуються відповідно до розроблених провідним викладачем методичних матеріалів, затверджених протоколом кафедри розробника.

Завдання для виконання контрольної (домашньої) роботи розробляються автором робочої програми. Навчальні матеріали затверджуються протоколом засідання випускової кафедри, доводяться до відома студента індивідуально і виконуються відповідно до методичних рекомендацій.

Час, потрібний для виконання домашнього завдання, контрольної (домашньої) роботи – до 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 вивченні навчальної дисципліни «Безпека в кібернетичному просторі» використовуються навчальні технології, що застосовуються для активізації навчально-пізнавальної діяльності студентів, а саме: робота в малих групах, семінар-дискусія, мозкова атака, кейс, презентація, рольова гра, дидактична гра тощо.

Використання технології *дистанційного навчання* реалізуються за допомогою комп'ютерної техніки, шляхом проведення занять з використанням чат-технологій, дистанційних занять, конференцій, семінарів, ділових ігор, лабораторних робіт, практикумів й інших форм навчальних занять, які проводяться за допомогою засобів телекомунікацій з використанням веб-технологій.

Також, використовується *проблемно-орієнтоване навчання* (яке передбачає формулювання та вирішення проблеми під час лекцій, розв`язання ситуативних задач на семінарах, практичних заняттях, дослідження проблеми під час самостійної роботи студентів) та *практико-орієнтоване навчання* (здійснюється через різні види практик на підприємствах, установах та організаціях різних форм власності).

3.2. Рекомендована література (базова і допоміжна)

Базова література

3.2.1. Закон України «Про захист інформації в інформаційно-комунікаційних системах».

3.2.2. Закон України «Про захист персональних даних».

3.2.3. Закон України «Про основні засади забезпечення кібербезпеки України».

3.2.4. Постанова КМУ від 19.06.2019 № 518 «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури»

3.2.5. Постанова КМУ від 19.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту».

3.2.6. Наказ Адміністрації Держспецзв'язку від 26.03.2007 № 45 «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сферах технічного захисту інформації», зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587.

3.2.7. Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», зареєстрований в Міністерстві юстиції України 28.01.2015 за № 90/26535.

3.2.8. ДСТУ ISO/IEC 15408-1:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель».

3.2.9. ДСТУ ISO/IEC 15408-2:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги».

3.2.10. ДСТУ ISO/IEC 15408-3:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки».

3.2.11. ДСТУ ISO/IEC 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки».

3.2.12. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник /Даник Ю.Г., Воробієнко П.П., Чернега В.М.// – Видання друге, перероб. та доп. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. - 320 с

3.2.13. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.

Допоміжна література

3.2.14. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Електронний ресурс]. – Режим доступу до ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11423.

3.2.15. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanoviz-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii.

3.2.16. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Електронний ресурс]. – Режим доступу до ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11425 .

3.2.17. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Електронний ресурс]. – Режим доступу до ресурсу: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr- 13335-4-2005.

3.2.18. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Електронний ресурс]. – Режим доступу до ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11427.

3.2.19. ISO 270032:2012 Information technology – Security techniques – Guidelines for cybersecurity. – Офіц. вид. – Режим доступу до ресурсу: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375.

3.3. Інформаційні ресурси в Інтернет

3.3.1. http://zakon.rada.gov.ua.
3.3.2. http://scholar.google.com.ua/
3.3.3. http://www.dstszi.gov.ua/dstszi/control/uk/index.
3.3.4. http://www.nau.edu.ua.
3.3.5. http://www.kzzi.nau.edu.ua.
3.3.6. https://www.coursera.org/learn/r-programming/.
3.3.7. http://prometheus.org.ua/dataanalysis/.

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.

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

4.1. Методи контролю та схема нарахування балів.

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

Таблиця 4.1

Вид навчальної роботи	Мах кількість балів	
	Денна форма навчання	Заочна форма навчання
	1 семестр	1 семестр
Модуль № 1 «Забезпечення безпеки в кіберпросторі»		
Виконання та захист лабораторних робіт	32	20
Для допуску до виконання модульної контрольної роботи № 1 студент має набрати не менше	*19*	*12*
Виконання модульної контрольної роботи № 1	15	-
Усього за модулем № 1	**47**	**20**
Модуль № 2 «Забезпечення кібербезпеки складних систем»		
Виконання та захист лабораторних робіт	32	20
Виконання домашнього завдання	6	-
Виконання контрольної (домашньої) роботи	-	30
Для допуску до виконання модульної контрольної роботи № 2 студент має набрати не менше	*19*	*12*
Виконання підсумкової семестрової контрольної роботи	-	30
Виконання модульної контрольної роботи № 2	15	-
Усього за модулем № 2	**53**	**80**
Усього за модулем № 1, 2	**100**	**100**
Усього за дисципліною	**100**	

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

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

Таблиця 4.2

Відповідність рейтингових оцінок за окремі види навчальної роботи в балах оцінкам за національною шкалою

Рейтингова оцінка в балах						Оцінка за національною шкалою
Виконання та захист лабораторної роботи		Виконання контрольної (домашньої) роботи	Виконання домашнього завдання	Виконання підсумкової семестрової контрольної роботи	Виконання модульної Контрольної роботи	
18 - 20	29 - 32	27 - 30	6	27 - 30	14 - 15	Відмінно
15 - 17	24 - 28	23 - 26	5	23 - 26	12 - 13	Добре
12 - 14	19 - 23	18 - 22	4	18 - 22	9 - 11	Задовільно
менше 12	менше 19	менше 18	менше 4	менше 18	менше 9	Незадовільно

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. Підсумкова семестрова рейтингова оцінка, перераховується в оцінку за національною шкалою та шкалою ECTS (табл. 4.3).

Таблиця 4.3

Відповідність підсумкової семестрової 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)

4.5. 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.

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

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	03.02	06.06.23	Федоренко І.А.		

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки
1	Кожухівський В.В.		8.06.2023	
2.	Федоренко І.А.		12.06.2023	

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності
1.	Кормовський В.В	28.05.2023		Актуальна 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				