МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

_____
Каріна НЕМАШКАЛО

ОСНОВИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ

робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "КІБЕРБЕЗПЕКА"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**КІБЕРБЕЗПЕКА**

Статус дисципліни	**обов'язкова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри
кібербезпеки
та інформаційних технологій *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробник:
Шаповалова Олена Олександрівна, к.т.н., доц. кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Завданням навчальної дисципліни «Основи математичного моделювання» є формування навичок та компетентностей в галузі розробки та застосування моделей для дослідження рівня кібербезпеки інформаційних систем. Викладання дисципліни передбачає ознайомлення здобувачів з базовими поняттями математичного моделювання та формалізованого запису правил політик безпеки, набуття ними навичок складання та аналізу математичних моделей на підґрунті обробки статистичних даних, опанування використання класичних моделей: статистичних, регресійних, оптимізаційних, дискреційного, мандатного та рольового доступу тощо.

Навчальна дисципліна «Основи математичного моделювання» є важливою складовою циклу комп'ютерних дисциплін підготовки бакалаврів за спеціальністю "Кібербезпека".

Предметом вивчення дисципліни є математичні моделі кібербезпеки, а також сучасні методи їх побудови і аналізу, зокрема регресійний та кореляційний аналіз даних, техніки розмежування доступу.

Метою навчальної дисципліни "Основи математичного моделювання" є надання здобувачам вищої освіти теоретичних знань з основ математичного моделювання об'єктів з точки зору їх кібербезпеки, засвоєння студентами основних підходів і принципів побудови моделей та надбання навичок їх застосування для аналізу рівня кібербезпеки інформаційних систем; набуття навичок використання методів формулювання та розв'язання задач моделювання та аналізу їх трудомісткості; розуміння сутності математичного забезпечення інформаційних систем; побудова та впровадження математичних моделей процесів обробки інформації, їх оптимізація та визначення напрямків вдосконалення.

Результатами вивчення дисципліни є системні знання та практичні навички в галузі розробки та застосування математичних моделей для обробки статистичних даних, оцінювання якості отриманих моделей та розв'язання задач забезпечення кібербезпеки,

Характеристика навчальної дисципліни

Курс	**3**
Семестр	**1**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення навчальної дисципліни:

Пререквізити	Постреквізити
Вища математика	Основи криптографічного захисту
Методи та засоби комп'ютерних інформаційних технологій	Основи технічного захисту інформації
Технології обробки інформації	Забезпечення інформаційної безпеки

Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 12 – розробляти моделі загроз та порушника;
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних	РН 13 – аналізувати проекти інформаційно - телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах

(автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	передачі даних
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно - телекомунікаційних системах програмно - апаратними засобами та давати оцінку результативності якості прийнятих рішень
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 15 – використовувати сучасне програмно - апаратне забезпечення інформаційно - комунікаційних технологій
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів,	РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

процедур, практичних прийомів та ін.). КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
КЗ 2. Знання та розуміння предметної області та розуміння професії. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 18 – використовувати програмні та програмноапаратні комплекси захисту інформаційних ресурсів
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних	РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно - телекомунікаційних

(автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	системах
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	РН 28 – 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 системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному	РН 35 – 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;

простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
КЗ 2. Знання та розуміння предметної області та розуміння професії. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що	РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління

обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 10. Здатність застосовувати методи та засоби	РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно - телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації

криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 50 – забезпечувати) функціонування програмних та програмно -апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично - сигнатурних)
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Програма навчальної дисципліни

Змістовий модуль 1. Теоретичні основи математичного моделювання

Тема 1. Вступ. Поняття математичного моделювання. Галузь застосування, термінологія. Типи моделей, класифікація, етапи моделювання.

Тема 2. Базові концепції математичного моделювання, обробка статистичних даних. Виявлення кореляції.

Тема 3. Регресійні моделі. Метод найменших квадратів. Лінійна парна регресійна модель. Перевірка її на адекватність

Тема 4. Ідентифікація параметрів математичної моделі. Багатофакторна модель. Перевірка її на адекватність

Тема 5. Умови коректності побудови моделей. Особливі випадки: мультиколінеарність, гетероскедастичність, авторегресія.

Змістовий модуль 2. Моделі безпеки комп'ютерних систем

Тема 6. Тестування даних з метою виявлення гетероскедастичності.

Тема 7. Оптимізаційні моделі

Тема 8. Політики безпеки. Типи моделей

Тема 9. Моделі комп'ютерних систем з дискреційним управлінням доступом

Тема 10. Моделі комп'ютерних систем з мандатним управлінням доступом

Тема 11. Моделі комп'ютерних систем з рольовим управлінням доступом.

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

Викладання дисципліни передбачає залучання пояснювально-ілюстративного, репродуктивного, дослідницького методів, а також методів проблемного навчання. Так під час проведення лекційних занять викладач надає здобувачам значний обсяг теоретичного матеріалу з наданням пояснень з залученням графічного подання (схеми, таблиці, презентації), доказів математичних гіпотез та формул, прикладів розв’язання задач (Тема 2,3,4,5,6). Протягом лабораторних занятть здобувачі мають змогу отримати практичні навички розв’язання задач на підставі проблеми, сформульованої за тематикою заняття. Вдосконалення практичних навичок відбувається під час виконання завдань за такими методами навчання як: індивідуальні завдання (Теми 2,3, 4, 5, 6) та самостійна робота (Теми 7, 8, 9, 10, 11)

Наведені методи навчання спрямовані на формування у здобувачів здатності розв’язувати складні комплексні задачі в галузі математичного моделювання.

Порядок оцінювання результатів навчання

Програма навчальної дисципліни передбачає лекційні, лабораторні та самостійні види робіт. Знання та компетентності, отримані здобувачами під час лекційних занять, оцінюються за написання контрольних робіт та складання тестів, навички, отримані під час лабораторних занять, оцінюються за розв’язанням задач, передбачених тематикою занять. Самостійна робота окремо не оцінюється, оскільки вона полягає у підготовці до інших видів занять і є невід’ємною складовою здобуття освіти. Оцінювання сформованих компетентностей здобувачів здійснюється за рейтинговою накопичувальною 100-бальною системою. Контрольні заходи включають:

- поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що надає студенту можливість складати залік, – 60 балів);

- модульний контроль передбачає виконання підсумкових контрольних завдань, які можуть включати творчу дослідницьку складову та потребують знань та навичок отриманих під час вивчення сукупності матеріалу за тематикою модуля.

За поточного контролю знання здобувачів оцінюються за такими критеріями:

– вільне володіння навчальним матеріалом в повному обсязі, з розумінням прикладів та можливістю наведення власних прикладів для пояснення сутності матеріалу;

– демонстрація навичок застосування методів побудови математичних моделей для розв’язання прикладних задач;

– демонстрація навичок застосування інноваційних методів роботи під час розв’язання задач;

– демонстрація навичок пошуку та аналізу джерел інформації, обґрунтування отриманих результатів та формування висновків за роботою;

– демонстрація навичок командної роботи під час розв’язання комплексних завдань з розробки та аналізу математичних моделей.

Формування завдань та контроль за їх виконанням мають за мету сприяння набуття здобувачами навичок активного творчого мислення, прищеплення когнітивних навичок та норм доброчесної співпраці. Головною вимогою до виконання завдань є самостійність їх виконання або визначення відсотку вкладу за умови командної роботи.

Розподіл балів поточного оцінювання за видами робіт є наступним.

Лекційні заняття: рівень оволодіння теоретичними знаннями визначається під час захисту виконання лабораторних робіт, за написання контрольних робіт (максимальна кількість балів становить – 20).

Лабораторні заняття: рівень набутих навичок застосування знань для розв’язання задач визначається правильністю виконання завдань лабораторних робіт (максимальна кількість балів становить 80).

Самостійна робота: рівень оволодіння навичками використання новітніх знань, методології та методів проведення наукових досліджень визначається за ступенем підготовки здобувача до виконання лабораторних та написання контрольних робіт (в Рейтинг-плані навчальної дисципліни додаткових балів на цей вид робіт не передбачено).

Здобувача слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 60 балів.. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**	**Форми оцінювання**	**Макб**

				а л
Тема 1	*Аудиторна робота*			
	Лекція	Лекція 1″ Вступ. Поняття математичного моделювання. Галузь застосування, термінологія. Типи моделей, класифікація, етапи моделювання.″		
	Лабораторне заняття	Лабораторна робота 1. Обробка статистичних даних.		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	*Аудиторна робота*			
	Лекція	Лекція 2 ″ Базові концепції математичного моделювання, обробка статистичних даних. Виявлення кореляції″		
	Лабораторне заняття	Лабораторна робота 1. Обробка статистичних даних та виявлення кореляції.		8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	*Аудиторна робота*			
	Лекція	Лекція 3 «Регресійні моделі. Метод найменших квадратів. Лінійна парна регресійна модель. Багатофакторна модель. Оцінка якості моделювання»		

	Лабораторне заняття	Лабораторнаробота 2. Лінійна парна регресійна модель.	Захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція 4″ Умови коректності побудови моделей. Особливі випадки: мультиколінеарність, гетероскедастичність, авторегресія.″	Контрольна робота 1	5
	Лабораторне заняття	Лабораторна робота 3. Регресійні моделі. Обчислення параметрів парної регресії, перевірка якості моделі.	Захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція 5″Тестування даних з метою виявлення мультиколінеарності та її усунення»		
	Лабораторне заняття	Лабораторна робота 4. Регресійні моделі. Обчислення параметрів багатофакторної регресії, перевірка якості моделі.	Захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Тема 6	***Аудиторна робота***			
	Лекція	Лекція 6″ Тестування даних з метою виявлення гетероскедастичності ″		
	Лабораторне заняття	Лабораторна робота 5. Виявлення мультиколінеарності в даних та її усунення	Захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція 7″ Оптимізаційні моделі ″	Контрольна робота 1	5
	Лабораторне заняття	Лабораторна робота 6. Тестування даних з метою виявлення гетероскедастичності	Захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція 8 ″ Політики безпеки. Типи моделей ″		
	Лабораторне заняття	Лабораторна робота 7. Оптимізаційні моделі. Оптимізація планування виробництва	Захист лабораторної роботи	8
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 9	***Аудиторна робота***			
	Лекція	Лекція 9″ Моделі комп'ютерних систем з дискреційним управлінням доступом. Модель ХРУ ″		
		Лекція 10″ Моделі комп'ютерних систем з дискреційним управлінням доступом. Модель Take-Grand ″		
	Лабораторне заняття	Лабораторна робота 8. Оптимізаційні моделі. Транспортна задача	Захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція 11 ″ Моделі комп'ютерних систем з мандатним управлінням доступом. Модель Белла-ЛаПадули ″		
	Лабораторне заняття	Лабораторна робота 9. Моделі комп'ютерних систем з дискреційним управлінням доступом. Модель ХРУ. Модель Take-Grand	Захист лабораторної роботи	8
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 11	***Аудиторна робота***			
	Лекція	Лекція 12″ Модель рольового доступа″	Контроль на робота 3	10
	Лабораторне заняття	Лабораторна робота 10. Модель мандатного доступу. Модель Белла-ЛаПадули		8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до		

Рекомендована література

Основна

1. Ільїн К.І., Стьопочкіна І.В. Безпека інформаційних систем. Лабораторний практикум: навчальний посібник. – Київ: КПІ ім. Ігоря Сікорського, 2020. – 60 с.

2. Методичні вказівки до виконання лабораторних робіт із дисципліни «Методи оптимізації» Розділ 1: «Математичне програмування» для студентів спеціальності 122 – «Комп'ютерні науки», Харків: ХНУБА, 2019 – 75с.

3. Методичні вказівки до виконання лабораторних робіт із дисципліни «Методи оптимізації» Розділ 2: «Регресійні моделі» », Харків: ХНУБА, 2019 - 71с.

4. Сізова Н.Д., Шаповалова О.О. Математичні моделі і методи прийняття рішень. Лабораторний практикум для здобувачів вищої освіти спеціальностей 122, 126.- Харків: ХНУБА, 2021 – 140с.

5. Новіков О. М., Стьопочкіна І. В. Методи штучного інтелекту в кібербезпеці: навчальний посібник/ – Київ : КПІ ім. Ігоря Сікорського, 2022. – 82 с.

Додаткова

6. Карпович І. ., Гладка О. , Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. Технічні науки та технології, (1(23), 62–68.

7. Росомахін С., Будянська К., Уранова А., Багмут М. Математична модель біометричної системи автентифікації відбитків пальців // Комп'ютерні науки та кібербезпека. 2019. № 1. С. 4-16.

8. Кузнецов О., Григоренко В., Дьяченко А., Багмут М. Дисперсійний аналіз мережевого трафіку для виявлення вторгнень в Smart Grids // Комп'ютерні науки та кібербезпека. 2019. № 1. С. 62-74.

9. Щебланін Ю., Рабчун Д. Математична модель порушника інформаційної

безпеки. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка". 1, 1 (Вер 2018), 63-72. DOI:https://doi.org/10.28925/2663-4023.2018.1.6372.

10. Ніколаєва О.Г., Шаповалова О.О. Лабораторний практикум з дисциплін «Імітаційне моделювання» та «Системний аналіз»: Навчально-методичний посібник. - Харків: ХНУБА, 2020 – 110с.

5.3.Інформаційні ресурси в мережі Інтернет

11. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Основи математичного моделювання" https://pns.hneu.edu.ua/course/view.php?id=8924