(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Факультет комп'ютерних наук та технологій
Кафедра технічного захисту інформації

ЗАТВЕРДЖУЮ
Декан ФКНТ
Андрій ФЕСЕНКО
«01» 09 2025 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА
навчальної дисципліни
«Моделювання та оптимізація безпекових процесів авіаційної галузі»

Освітньо професійна програма: «Безпека інформаційних і комунікаційних систем»
«Системи технічного захисту інформації, автоматизація її обробки»
«Системи та технології кібербезпеки»
Галузь знань: F «Інформаційні технології»
Спеціальність: F5 «Кібербезпека та захист інформації»

Форма навчання	Сем.	Усього (год. / кредитів ECTS)	ЛКЦ	ПР.З	Л.З	СРС	ДЗ / РГР / К.р	КР / КП	Форма сем. контролю
Денна	1	180/6	32	-	32	116	1 дз - 1 с	-	екзамен 1с
Заочна	1	180/6	10	-	10	160	1 к - 1 с	-	екзамен 1с

Індекс: № НМ-4-F-1/25-2.1.3, № НМ-4-F-2/25-2.1.3, № НМ-4-F-3/25-2.1.3
Індекс: № НМ-4-F-1з/25-2.1.3

Робочу програму навчальної дисципліни «Моделювання та оптимізація безпекових процесів авіаційної галузі» розроблено на основі освітньо-професійних програм «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації, автоматизація її обробки», «Системи та технології кібербезпеки», навчальних планів №НМ-4-F5-1/25, №НМ-4-F5-2/25, №НМ-4-F5-3/25, № НМ-4-F5-1з/25 та робочих навчальних планів №РМ-4-F5-1/25, №РМ-4-F5-2/25, №РМ-4-F5-3/25 і №РМ-4-F5-1з/25 підготовки здобувачів вищої освіти освітнього ступеня «Магістр» за спеціальністю F5 «Кібербезпека та захист інформації» та відповідних нормативних документів.

Робочу програму розробив
Професор кафедри технічного захисту інформації,
д.т.н., професор:_____ Андрій МІЩЕНКО

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійних програм «Системи технічного захисту інформації, автоматизація її обробки», «Системи та технології кібербезпеки», спеціальності F5 «Кібербезпека та захист інформації» – кафедри технічного захисту інформації, протокол №11 від « 25 » серпня 2025 р.

Гарант освітньо-професійної програми
«Системи технічного захисту інформації,
автоматизація її обробки»_____ Сергій ЛАЗАРЕНКО

Гарант освітньо-професійної програми
«Системи та технології кібербезпеки»_____ Валеріян ШВЕЦЬ

Завідувач кафедри _____ Валерій КОЗЛОВСЬКИЙ

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійної програми «Безпека інформаційних і комунікаційних систем», спеціальності F5 «Кібербезпека та захист інформації» – кафедри кібербезпеки, протокол №11 від « 25 » серпня 2025 р.

Гарант освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»_____ Анна ІЛЬЄНКО

Завідувач кафедри _____ Анна ІЛЬЄНКО

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету комп'ютерних наук та технологій, протокол №10 від «01» вересня 2025 р.

Голова НМРР _____ Оксана ПОЛІЩУК

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

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Моделювання та оптимізація безпекових процесів авіаційної галузі» 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 «Моделювання та оптимізація безпекових процесів авіаційної галузі» належить до циклу професійної підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації». Вона є базовою для формування в студентів системного підходу до застосування методів моделювання та оптимізації для управління ризиками в сфері безпеки критичних інфраструктур авіаційної галузі. Курс охоплює вивчення специфіки авіаційних кіберзагроз, архітектуру вразливих системи керування аеродромом, методи їх моделювання та застосування сучасних алгоритмів оптимізації для розподілу обмежених ресурсів безпеки. Ключовим результатом навчання є розробка комплексного Плану управління безпекою (SMP) для авіаційної організації, що базується на результатах моделювання та оптимізації.

Мета дисципліни — формування у студентів теоретичних знань та практичних навичок з моделювання, аналізу та оптимізації безпекових процесів в авіаційній галузі. Курс спрямований на вивчення сучасних методів забезпечення кібербезпеки, аналізу ризиків та розробки оптимальних рішень для захисту інформаційних систем авіаційних підприємств..

Завдання дисципліни:

— формування розуміння авіаційної галузі як складної кібер-фізичної системи з точки зору інформаційної безпеки;

— ознайомлення з основними поняттями та апаратом математичного моделювання та оптимізації;

— вивчення принципів побудови математичних моделей різних об'єктів та систем;

— застосування у практичній діяльності, математичного моделювання та методів оптимізації для ключових авіаційних процесів та систем;

— навчити структурувати та оформлювати результати модельно-оптимізаційних досліджень у вигляді стратегічного документу — Плану управління безпекою (SMP), відповідно до вимог ІСАО та національних регуляторів.

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

У результаті вивчення навчальної дисципліни студент повинен набути наступні **результати навчання**.

Освітньо професійна програма: «Безпека інформаційних і комунікаційних систем»

ІК. Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки та захисту інформації.

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.

ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

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.

ФК 11. Здатність проєктувати, розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси і системи засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах на об’єктах критичної інфраструктури держави, включаючи авіаційну галузь.

ФК 12. Здатність до проєктування, впровадження, супроводження інформаційних мереж і ресурсів, з метою забезпечення захисту інформації та безперервного функціонування з використанням сучасних технологій інформаційної безпеки та/або кібербезпеки на об’єктах критичної інфраструктури держави, включаючи авіаційну галузь.

ФК15. Здатність розробляти, впроваджувати та оцінювати ефективність стратегій кіберстійкості інформаційно-комунікаційних систем у контексті концепції сталого розвитку, використовуючи методи мінімізації кіберризиків, сучасні технології захисту та механізми забезпечення безпечного кіберпростору для розвитку цифрового суспільства (Цілі сталого розвитку 9, 11, 16).

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.

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.

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 аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.

ФК12. Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз, зокрема у контексті концепції сталого розвитку.

ФК14. Здатність моделювати безпекові процеси в авіаційній галузі.

Освітньо професійна програма: «Системи та технології кібербезпеки»

ІК. Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки та захисту інформації.

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.

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.

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.

ФК14. Здатність розробляти та впроваджувати стратегії кіберстійкості систем та технологій кібербезпеки у межах концепції сталого розвитку, спрямованої на зменшення кіберризиків в контексті забезпечення захисту критичної інфраструктури та створення безпечного цифрового простору, а також формування компетентності для підтримки інновацій у сфері кібербезпеки (Ціль 9 сталого розвитку) та зміцнення інформаційної безпеки

задля забезпечення довіри у кіберпросторі відповідно до принципів миру, правосуддя та ефективних інституцій (Ціль 16 сталого розвитку).

1.3. Компетентності, які дає можливість здобути навчальна дисципліна.

У результаті вивчення навчальної дисципліни студент повинен набути наступні **компетентності**.

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 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН 5. 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.

ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН 15. 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.

ПРН 16. 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.

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 19. 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.

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

ПРН 21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН 22. 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.

ПРН 23. 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.

ПРН 24. Вирішувати задачі проектування та супроводу захищених інформаційних мереж та комплексів з використанням сучасних методів та технологій забезпечення інформаційної безпеки

та/або кібербезпеки для забезпечення необхідного рівня захищеності на об'єктах критичної інфраструктури держави, включаючи авіаційну галузь.

ПРН28. Аналізувати кіберризики, розробляти та впроваджувати стратегії кіберстійкості інформаційно-комунікаційних систем, застосовуючи сучасні технології захисту та методи забезпечення безперервності функціонування критичних інформаційних ресурсів відповідно до принципів сталого розвитку (Цілі сталого розвитку 9, 11, 16), міжнародних стандартів та регуляторних вимог

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

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 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН 5. 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.

ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

ПРН 10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН 12. 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.

ПРН 14. 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.

ПРН 15. 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.

ПРН 16. 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.

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

ПРН 19. 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.

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

ПРН 21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН 23. 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. Розробляти проєкти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, інформація з обмеженим доступом).

ПРН26. Визначати показники захищеності інформації на об'єкті інформаційної діяльності та можливість (неможливість) створення на ОІД певних технічних каналів витоку інформації.

ПРН27. Вирішувати завдання проєктування та супроводу захищених інформаційних мереж та комплексів з використанням сучасних методів та технологій забезпечення інформаційної безпеки та/або кібербезпеки, для забезпечення необхідного рівня захищеності на об'єктах критичної інформаційної держави, в інтересах її сталого розвитку, включаючи авіаційну галузь.

Освітньо професійна програма: «Системи та технології 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 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН 5. 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.

ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН 10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН 12. 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.

ПРН 13. 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.

ПРН 14. 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.

ПРН 15. 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.

ПРН 16. 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.

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 19. 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.

ПРН 21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

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.

ПРН26. Розробляти та впроваджувати стратегії кіберстійкості систем та технологій кібербезпеки, спрямовані на захист критичної цифрової інфраструктури, підвищення стійкості інформаційних систем до атак, мінімізацію кіберризиків та розвиток ефективних механізмів реагування на кіберзагрози, необхідні для забезпечення безпечного цифрового середовища, розвитку інновацій у сфері кібербезпеки (Ціль 9 сталого розвитку), підвищення рівня захищеності міських цифрових екосистем (Ціль 11 сталого розвитку) та зміцнення інституційних механізмів протидії кіберзлочинності відповідно до принципів миру, правосуддя та ефективного управління (Ціль 16 сталого розвитку).

1.4. Міждисциплінарні зв'язки.

Дана дисципліна доповнює такі дисципліни як «Автоматизація обробки інформації з обмеженим доступом», «Інтелектуалізовані системи інформаційної безпеки», «Організаційні моделі кібербезпеки», «Технології захисту мережевих інфраструктур», «Технології створення та застосування систем захисту кіберпростору», та інші з «Циклу дисциплін вільного вибору студента».

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст навчальної дисципліни

Навчальний матеріал дисципліни структурований за модульним принципом і складається з одного навчального модуля,№ 1 «Моделювання та управління безпековими процесами авіаційної галузі», який є логічною завершеною, самостійною, цілісною частиною навчального плану, засвоєння якої передбачає проведення модульної контрольної роботи та аналіз результатів її виконання.

2.2. Модульне структурування та інтегровані вимоги до кожного модуля

Інтегровані вимоги модуля №1:

Знати:

- основні поняття та категорії авіаційної безпеки (АБ), безпеки польотів (БП) та кібербезпеки (КБ), а також взаємозв'язок між ними;

- ключові нормативно-правові акти та міжнародні стандарти у сфері авіаційної безпеки та кіберзахисту (ICAO, EASA, Державіаслужба України);
- цілі кібербезпеки в авіації (конфіденційність, цілісність, доступність, стійкість до атак);
- особливості архітектури авіаційних систем: бортових, наземних, інформаційно-комунікаційних;
- основні загрози та вразливості авіаційних інформаційних систем, у т.ч. зовнішні (GPS spoofing, DDoS, атаки на системи управління польотами) і внутрішні (інсайдери, людський фактор);
- структуру та принципи функціонування систем управління безпекою (SMP, ICAO Doc 9859).
- принципи математичного і комп'ютерного моделювання безпекових процесів;
- основні положення теорії ймовірностей, необхідні для кількісної оцінки ризиків;
- моделі теорії масового обслуговування та їхнє застосування для аналізу навантаження в авіаційних системах;
- основи дискретного моделювання та теорії графів для аналізу критичних вузлів у мережевих структурах;
- методи теорії ігор для аналізу взаємодії атакуючих і захисників у кіберпросторі;
- методи прийняття рішень в умовах невизначеності та кризових ситуаціях;
- принципи детермінованої оптимізації (лінійне, нелінійне програмування);
- еволюційні та метаевристичні методи (генетичні алгоритми, рої частинок, нейронні мережі);
- концепції оптимізації захисту (редундантність, ізоляція, принцип найменших привілеїв);
- основи BCP (Business Continuity Planning) та DRP (Disaster Recovery Planning), показники RTO/RPO, вартість простою;
- принципи побудови оптимальної архітектури безпеки авіапідприємств та інтеграції SMP з корпоративними системами.

Вміти:

- аналізувати співвідношення між АБ, БП і КБ у контексті комплексної безпеки авіаційної галузі;
- ідентифікувати та класифікувати основні кіберзагрози та вразливості в авіаційних інформаційних системах;
- застосовувати базові методи аналізу ризиків для оцінювання ймовірності та наслідків кіберінцидентів у авіації;
- орієнтуватися в міжнародних і національних нормативних документах, що регламентують авіаційну безпеку та кіберзахист;
- формувати базове уявлення про структуру та функції Security Management Plan і його інтеграцію в діяльність авіапідприємства;
- узагальнювати та інтерпретувати приклади реальних кіберінцидентів в авіаційній сфері для визначення кращих практик захисту.
- будувати математичні та імітаційні моделі для оцінки ризиків і прогнозування кіберзагроз;
- застосовувати ймовірнісні та статистичні методи для аналізу безпеки авіаційних систем;
- моделювати процеси функціонування авіаційних служб та систем із використанням СМО;
- використовувати графові моделі для виявлення критичних залежностей і вузлів у мережевій інфраструктурі;
- застосовувати ігрові моделі для обґрунтування стратегій кіберзахисту;
- розробляти алгоритми прийняття рішень у кризових умовах та оцінювати їхню ефективність;
- використовувати методи лінійної, нелінійної та багатокритеріальної оптимізації для розподілу ресурсів безпеки;
- застосовувати еволюційні й метаевристичні методи для вирішення складних задач кіберзахисту;

- розробляти заходи з підвищення відмовостійкості та зменшення вразливості авіаційних систем;
- формувати комплексні плани забезпечення безперервності бізнесу та відновлення після інцидентів;
- інтегрувати SMP з іншими системами управління безпекою підприємства та адаптувати архітектуру безпеки до сучасних викликів.

Модуль 1. Моделювання та управління безпековими процесами авіаційної галузі

Тема 1. Структура курсу, мета та короткий огляд.

Визначення місця дисципліни у підготовці магістрів кібербезпеки для авіаційної галузі. Розмежування понять: авіаційна безпека (АБ), безпека польотів (БП) і кібербезпека (КБ). Розгляд міжнародних нормативних документів ICAO, EASA та Державіаслужби України. Обговорення місця SMP (Security Management Plan) у системі управління безпекою підприємства.

Тема 2. Цілі кібербезпеки в авіації. Базові поняття.

Розгляд класичних принципів CIA triad (Confidentiality, Integrity, Availability) у контексті авіаційних систем. Визначення специфічних цілей кіберзахисту для авіації: стійкість до атак, безперервність авіаційних процесів, збереження довіри пасажирів. Аналіз архітектури: бортові системи, наземна інфраструктура, канали обміну даними (ACARS, ADS-B).

Тема 3. Основні загрози та вразливості авіаційних систем.

Класифікація кіберзагроз для авіаційної галузі: зовнішні атаки (GPS spoofing, DDoS, вторгнення у системи управління польотами), внутрішні загрози (інсайдери, помилки персоналу), людський фактор. Огляд реальних інцидентів (наприклад, атаки на системи польотного планування чи витоки даних авіакомпаній). Методи аналізу ризиків.

Тема 4. Вступ до систем управління безпекою.

Зміст і структура SMP (Security Management Plan) відповідно до ICAO Doc 9859. Принципи інтеграції безпеки у всі операційні процеси. Взаємозв’язок між SMP і корпоративними планами управління безпекою (ISMS, ISO/IEC 27001).

Тема 5. Моделювання як мова безпеки.

Роль математичного та комп’ютерного моделювання для прогнозування кіберзагроз. Класифікація моделей: імовірнісні, детерміновані, ігрові, симуляційні. Приклади застосування в авіаційній галузі.

Тема 6. Імовірнісні моделі для кількісної оцінки ризиків.

Використання законів розподілу (експоненційний, нормальний, Пуассона) для оцінки ймовірності кіберінцидентів. Моделювання ризику відмов критичних систем. Розрахунок показників MTBF, MTTF, MTTR.

Тема 7. Моделі теорії масового обслуговування (СМО).

Аналіз навантаження на системи управління авіаційним трафіком, диспетчерські служби та інформаційні системи аеропортів. Використання СМО для оптимізації ресурсів і зменшення ризиків перевантаження.

Тема 8. Дискретні моделі: теорія графів.

Моделювання авіаційних комунікаційних мереж як графів. Визначення критичних вузлів і каналів, оцінка стійкості до відмов. Методи пошуку мінімальних відрізних множин та аналіз зв’язності мережі.

Тема 9. Моделі теорії ігор.

Застосування стратегічних ігор для моделювання протистояння «зловмисник – захисник». Розробка оптимальних стратегій захисту. Приклади: ігри з нульовою сумою, повторювані ігри, моделювання сценаріїв Red Team vs Blue Team.

Тема 10. Моделі прийняття рішень у кризах.

Методи багатокритеріального вибору (AHP, ELECTRE, TOPSIS). Використання сценарного аналізу для управління кризами в авіаційній галузі. Оцінка варіантів дій в умовах невизначеності.

Тема 11. Детерміновані моделі оптимізації.

Лінійне та нелінійне програмування для розподілу ресурсів безпеки (персонал, техніка, фінанси). Задачі оптимізації для підвищення ефективності реагування на інциденти.

Тема 12. Еволюційні та метаевристичні методи.

Природоподібні підходи до пошуку оптимальних рішень у складних, багатокритеріальних задачах для ефективного дослідження простору варіантів безпекових заходів.

Тема 13. Оптимізація захисту: редундантність, ізоляція, принцип найменших привілеїв.

Проектування архітектури високої відмовостійкості. Методи резервування, сегментації систем, обмеження доступив. Приклади архітектурних патернів захисту.

Тема 14. Оптимізація відродження систем.

Планування безперервності бізнесу (BCP) і відновлення після аварій (DRP). Визначення цільових показників відновлення (RTO, RPO). Аналіз впливу простоїв на фінансові та безпекові показники.

Тема 15. Оптимізація архітектури безпеки.

Інтеграція SMP з корпоративними ISMS. Побудова багаторівневої архітектури безпеки, що враховує технічні, організаційні та людські фактори. Приклади best practices з авіаційної галузі.

Тема 16. Огляд сучасних трендів.

Огляд сучасних викликів і перспектив кіберзахисту в авіації.

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 «Моделювання та управління безпековими процесами авіаційної галузі»									
1.1	Структура курсу, мета та короткий огляд	**1 семестр**				**1 семестр**			
		8	2	-	6	10	-	-	10
1.2	Цілі кібербезпеки в авіації. Базові поняття.	8	2	-	6	12	2	-	10
1.3	Основні загрози та вразливості авіаційних систем	12	2	2 2	6	12	-	2	10
1.4	Вступ до систем управління безпекою	8	2	-	6	12	2	-	10
1.5	Моделювання як мова безпеки	10	2	2	6	10	-	-	10
1.6	Імовірнісні моделі для кількісної оцінки ризиків	10	2	2	6	14	2	2	10
1.7	Моделі теорії масового обслуговування (СМО).	12	2	2 2	6	14	2	2	10
1.8	Дискретні моделі: теорія графів	10	2	2	6	10	-	-	10
1.9	Моделі теорії ігор	10	2	2	6	10	-	-	10
1.10	Моделі прийняття рішень у кризах	10	2	2	6	10	-	-	10
1.11	Детерміновані моделі оптимізації	10	2	2	6	10	-	-	10
1.12	Еволюційні та метаевристичні методи	10	2	2	6	10	-	-	10
1.13	Оптимізація відродження систем	10	2	2	6	10	-	-	10
1.14	Оптимізація архітектури безпеки	28	2	2 2 2 2	18	18	2	2 2	12
1.15	Огляд сучасних трендів	12	2	-	10	10	-	-	10
1.16	Виконання та захист домашнього завдання	8	-	-	8	-	-	-	-
1.17	Виконання контрольної роботи (ЗФН)	-	-	-	-	8	-	-	8
1.18	Модульна контрольна робота №1	4	2	-	2	-	-	-	-
Усього за модулем №1		**180**	**32**	**32**	**116**	**180**	**10**	**10**	**160**
Усього за навчальною дисципліною		**180**	**32**	**32**	**116**	**180**	**10**	**10**	**160**

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

Домашнє завдання (ДЗ) з дисципліни виконується в першому семестрі, відповідно до затверджених в установленому порядку методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та вмінь студента в області моделювання та оптимізація безпекових процесів і є складовою модулю №1 «Моделювання та управління безпековими процесами авіаційної галузі».

Конкретною метою ДЗ є з'ясування, що для ефективної протидії необхідно впроваджувати комплексний, системний підхід, який визначається як Комплексний план управління безпекою (Security Management Plan, SMP).

Виконання, оформлення та захист ДЗ здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій.

Час, потрібний для виконання ДЗ, - до 8 годин самостійної роботи.

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

Конкретною метою контрольній (домашній) роботи є з'ясування, що для ефективної протидії необхідно впроваджувати комплексний, системний підхід, який визначається як Комплексний план управління безпекою (Security Management Plan, SMP). Ця концепція є ключовим елементом дисципліни "Математичне моделювання та оптимізація інформаційно-безпекових процесів", оскільки вона формує стратегічну основу, в рамках якої застосовуються всі технічні, математичні та аналітичні методи. SMP представляє собою не просто документ, а сукупність принципів, процедур, політик та ресурсів, спрямованих на постійне управління ризиками, що пов'язані з кібербезпекою.

Завдання для виконання практичної частини контрольної (домашньої) роботи здійснюється студентом 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 екзамену.

Перелік питань та зміст завдань для підготовки до екзамену, розробляються провідними викладачами та затверджуються протоколом засідання кафедри та доводяться до відома студентів.

3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.1. Методи навчання

При вивченні навчальної дисципліни використовуються наступні методи навчання: пояснювально-ілюстративний метод; метод проблемного викладання; репродуктивний метод; дослідницький метод. Реалізація цих методів здійснюється при проведенні лекцій, демонстрацій, самостійному розв'язанні завдань, роботі з навчальною літературою, аналізі та розв'язанні завдань.

3.2. Рекомендована література

Базова література

3.2.1. ICAO. Global Aviation Security Plan (GASP). 2020.
3.2.2. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. 2012.
3.2.3. ISO/IEC 27001:2022. Information security management systems.
3.2.4. FAA. Cybersecurity Best Practices for Aviation Stakeholders. 2023.
3.2.5. EASA. CS-ACS: Cybersecurity Requirements for Aircraft Systems. 2022.
3.2.6. Кравченко О.В. Кібербезпека в авіації: проблеми та шляхи вирішення. Київ, 2024.
3.2.7. Хоменко В.М. Математичне моделювання систем безпеки. Львів, 2021.
3.2.8. Математичне моделювання систем і процесів: навч. посіб. – К. : НАУ, 2017. – 392 с.
3.2.9. Методи оптимізації та пошуку оптимальних рішень: навч.посіб. – К. : КПІ ім.. Ігоря Сікорського. 2023. – 73 с.
3.2.10. Taha H.A. Operations Research: An Introduction. Pearson, 2020.
3.2.11. Ross S.M. Introduction to Probability Models. Academic Press, 2022.

Допоміжна література

3.2.12. MITRE ATT&CK Framework for Aviation Sector
3.2.13. IATA Security Manual
3.2.14. ENISA Threat Landscape Reports

3.3. Інформаційні ресурси в інтернеті

3.3.1. www.rsasecurity.com

3.3.2. www.nist.gov
3.3.3. www.eprint.iacr.org
3.3.4. www.citeseerx.ist.psu.edu
3.3.5. www.ansi.org
3.3.6.www.iso.org
3.3.7. Методичні розробки кафедри (в електронному вигляді).

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

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

Таблиця 4.1

Вид навчальної роботи	Max кількість балів	
	Денна форма навчання	Заочна форма навчання
1 семестр		
Модуль №1 «Моделювання та управління безпековими процесами авіаційної галузі»		
Виконання та захист лабораторних робіт	6б×8 = 48	10б×3 = 30
Виконання та захист домашнього завдання	20	–
Виконання та захист контрольної роботи (ЗФН)	–	30
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше	*41 балу*	–.
Виконання модульної контрольної роботи №1	12	–
Усього за модулем №1	**80**	**60**
Семестровий екзамен	**20**	**40**
Усього за дисципліною	**100**	

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

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 підсумкової семестрової модульної та **екзаменаційної** рейтингових оцінок, у балах становить підсумкову семестрову рейтингову оцінку, яка перераховується в оцінки за національною шкалою та шкалою ECTS (табл. 4.3)

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.

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 лабораторних робіт		**Виконання та захист розрахунково-графічної роботи**	**Виконання та захист домашнього завдання, (контрольної (домашньої) роботи (ЗФН)**	**Виконання модульної роботи**	
6	9-10	18-20	27-30	11-12	Відмінно
5	8	15-17	23-26	9-10	Добре
4	6-7	12-14	18-22	7-8	Задовільно
менше 4	менше 6	менше 12	менше 18	менше 9	Незадовільно

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)

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	кафедра №143	01.09.25	Ємченко В.В.		

(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				