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

ЗАТВЕРДЖУЮ
Декан ФКНТ
_____ Андрій ФЕСЕНКО
«____» _____ 2025 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА
навчальної дисципліни
«Методи побудови та аналізу криптосистем»

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 ргр - 1с	-	екзамен 1с
Заочна	1	180/6	10	-	10	160	1 к - 1 с	-	екзамен 1с

Індекс: № НМ-4-F5-1/25-2.1.1, № НМ-4-F5-2/25-2.1.1, НМ-4-F5-3/25-2.1.1
Індекс: № НМ-4-F5-1з/25-2.1.1

Робочу програму навчальної дисципліни «Методи побудови та аналізу криптосистем» 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 і № 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
Завідувач кафедри кібербезпеки,
к.т.н., доцент: _____ Анна ІЛЬЄНКО

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» 08 2025 р.

Гарант освітньо-професійної програми _____ Анна ІЛЬЄНКО

Завідувач кафедри _____ Анна ІЛЬЄНКО

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» 08 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 науково-методично-редакційної ради факультету комп'ютерних наук та технологій, протокол № 10 від «01» 09 2025 р.

Голова НМРР _____ Оксана ДОЛІЙЧУК

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

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Назва дисципліни» 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 «Методи побудов та аналізу криптосистем» належить до циклу професійної підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації». Вона є базовою для формування фахових компетентностей, пов'язаних із забезпеченням інформаційної та кібербезпеки, зокрема шляхом застосування сучасних криптографічних засобів, протоколів та криптоаналітичних методів. Здобуті знання та практичні навички дозволять майбутньому фахівцю вирішувати професійні завдання із захисту інформації в інформаційно-телекомунікаційних системах з використанням сучасних криптографічних методів і засобів.

Мета дисципліни — формування у здобувачів знань та практичних навичок щодо побудови, функціонування, аналізу та застосування сучасних криптографічних систем і протоколів, а також уміння здійснювати оцінку їх стійкості і застосовувати ці знання для підвищення рівня кіберзахисту в інформаційно-телекомунікаційних системах.

Завдання дисципліни:

— ознайомлення зі структурою, компонентами і принципами функціонування криптографічних систем;

— опанування конструкції та властивостей сучасних криптографічних протоколів;

— набуття навичок аналізу криптосистем і оцінки їх криптостійкості;

— формування практичних навичок застосування криптографічних засобів у реальних інформаційно-телекомунікаційних середовищах.

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»

1. ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки та захисту інформації.
2. ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
3. ЗК 2. Здатність проводити дослідження на відповідному рівні.
4. ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу.
5. 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.
6. 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.
7. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
8. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

9. 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.

10. 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»

1. ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки та захисту інформації.
2. ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
3. ЗК 2. Здатність проводити дослідження на відповідному рівні.
4. ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу.
5. 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.
6. 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.
7. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
8. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
9. 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.

Освітньо професійна програма: «Системи та технології кібербезпеки»

1. ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки та захисту інформації.
2. ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
3. ЗК 2. Здатність проводити дослідження на відповідному рівні.
4. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
5. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
6. 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.

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»

1. 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.
2. ПРН 2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
3. 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.
4. ПРН 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
5. ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. ПРН 28. 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»

1. 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.

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

3. 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.

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

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

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

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

Освітньо професійна програма: «Системи та технології кібербезпеки»

1. 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.

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

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

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

5. 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.

6. 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.

7. 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.

8. 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 «Моделювання та оптимізація безпекових процесів авіаційної галузі», «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 «Сучасні криптографічні системи: математичні основи, класифікація та характеристика»,** який є логічно 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:

– структуру, принципи роботи та класифікацію сучасних криптографічних систем (симетричних, асиметричних, комбінованих);

– структуру та функціонування інфраструктури відкритих ключів (PKI), зокрема компоненти, формати сертифікатів та нормативне забезпечення;

– математичні основи та властивості сучасних криптографічних протоколів (включаючи нульове розголошення, підпис, автентифікацію, розподіл секрету);

– методи забезпечення автентичності, цілісності та конфіденційності інформації;

– принципи та методи криптографічного аналізу (класичного та сучасного), включаючи статистичний, диференціальний, алгебраїчний, лінійний аналіз;

– принципи шифрування даних при передачі у протоколах TLS/SSL, VPN, IPsec;

– основи квантової криптографії та протоколів квантового розподілу ключів (BB84, E91, інші).

Вміти:

– застосовувати методи та засоби криптографічного захисту інформації в IT-середовищі;

– проектувати криптографічні системи для інформаційно-телекомунікаційних систем відповідно до вимог безпеки;

– використовувати сучасні криптографічні протоколи для забезпечення автентифікації, цілісності, розподілу ключів та електронного підпису;

– застосовувати компоненти інфраструктури відкритих ключів для управління сертифікатами та ключами;

– здійснювати криптографічний аналіз з метою оцінки стійкості та виявлення вразливостей криптографічних систем і протоколів;

– обґрунтовувати доцільність використання квантових підходів до захисту інформації у перспективних системах.

Модуль 1. Сучасні криптографічні системи: математичні основи, класифікація та

характеристика

Тема 1. Основи побудови сучасних криптографічних систем.

Вступ. Загальні поняття про криптографічні системи. Симетричні, асиметричні та комбіновані криптографічні системи. Поняття ідеальних криптографічних систем та їх особливості застосування. Функції криптографічних систем. Класифікація криптографічних шифрів та характеристика їх параметрів.

Тема 2.Інфраструктура відкритих ключів.

Основні поняття та визначення. Нормативно-правове забезпечення в сфері інфраструктури відкритих ключів. Компоненти, архітектура та функції сучасної інфраструктури відкритих ключів. Поняття та класифікації сертифікатів відкритих ключів. Структура та формат сертифікату X.509.

Тема 3. Методи автентифікації і контролю цілісності інформації на основі криптографічних перетворень.

Завдання автентифікації інформації. Імітозахист інформації. Контроль цілісності потоку повідомлень. Криптографічні методи контролю цілісності. Коди автентифікації повідомлень. Код виявлення маніпуляцій з даними. Коди MAC, MDC, HMAC, CMAC. Автентифікація суб'єкта та об'єкта з використанням криптографічних перетворень.

Тема 4. Криптографічні протоколи.

Основні поняття, класифікація та функції криптографічних протоколів. Поняття примітивних та прикладних криптографічних протоколів. Докази з нульовим розголошенням. Протоколи підкидання монети. Протоколи бітових зобов'язань. Протоколи розподілу секрету. Протоколи електронного підпису. Класифікація атак на схеми електронного підпису. Особливі схеми електронного підпису. Протоколи віддаленої автентифікації. Симетричні та асиметричні методи автентифікації. Класифікація та математичні основи проведення криптографічного аналізу криптопротоколів.

Тема 5. Управління криптографічними ключами.

Розрядність ключа. Генерація ключів. Неоднорідне ключовий простір. Зберігання ключів. Розподіл ключів. Час життя ключів.

Тема 6. Криптографічний аналіз сучасних криптосистем.

Загальна поняття проведення криптографічного аналізу. Історія криптоаналізу. Класифікація сучасних методів криптоаналізу. Статистичний криптоаналіз. Алгебраїчний криптоаналіз. Диференціальний (або різницевий) криптоаналіз. Лінійний криптоаналіз. Процедури проведення криптографічного аналізу симетричних та асиметричних криптографічних систем. Оцінка криптографічної стійкості.

Тема 7. Шифрування даних при передачі.

Протоколи TLS/SSL, VPN, IpSec. Значення шифрування даних при передачі. Протоколи TLS/SSL. Порушення безпеки на різних етапах процесу передачі даних. VPN. IPSec. Стандарти, що вимагають шифрування при передачі даних

Тема 8. Квантова криптографія: основні визначення та поняття.

Вступ до квантової криптографії. Квантовий розподіл ключа. Квантовий прямий безпечний зв□язок. Квантове розділення секрету. Квантове шифрування. Протоколи квантового розподілу ключів: BB84, E91 та інші. Мета та важливість КРК. Протокол BB84. Протокол E91. Протокол B92. Протокол СВК. Порівняння протоколів квантового розподілу ключів.

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 «Сучасні криптографічні системи: математичні основи, класифікація та характеристика»									
1.1	Основи побудови сучасних криптосистем	32	6	2 2 2 2	18	32	2 2	2 2 2 2	20
1.2	Інфраструктура відкритих ключів	24	4	2 2	16	20	2	2	16
1.3	Методи автентифікації і контролю цілісності інформації на основі криптографічних перетворень	38	4	2 2 2 2 2 2	22	20	-	-	20
1.4	Криптографічні протоколи	16	2	2 2	10	30	-	-	30
1.5	Управління криптографічними ключами	16	2	2 2	10	12	2	-	10
1.6	Криптографічний аналіз сучасних криптосистем	12	4	-	8	24	-	-	24
1.7	Шифрування даних при передачі	14	4	-	10	12	2	-	10
1.8	Квантова криптографія: основні визначення та поняття.	14	4	-	10	22	-	-	22
1.9	Виконання та захист розрахунково-графічної роботи	10	-	-	10	-	-	-	-
1.10	Виконання контрольної (домашньої) роботи (ЗФН)	-	-	-	-	8	-	-	8
1.11	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. Розрахунково-графічна робота, завдання на контрольну (домашню) роботу (ЗФН).

Розрахунково-графічна робота (РГР) 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 реалізації криптографічного захисту інформації і є складовою модулю №1 «Сучасні криптографічні системи: математичні основи, класифікація та характеристика».

Конкретною метою РГР є застосування на практиці та в професійній діяльності теоретичних знань з принципів побудови і використання криптографічних систем для організації захисту інформації в інформаційно-телекомунікаційних системах.

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

Час, потрібний для виконання РГР, - до 10 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.

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. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.

3.2.2. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120 с.

3.2.3. Anubhab Baksi. Classical and Physical Security of Symmetric Key Cryptographic Algorithms (Computer Architecture and Design Methodologies). Springer. 2022 . – 300 p.

3.2.4. Dr.Sonali Ridhorkar. Elliptic Curve Cryptography: Implementation Issues: Key Establishment Protocol. LAP LAMBERT Academic Publishing. 2021. – 152 p.

3.2.5. Aiden A. Bruen, Mario A. Forcinito, James M. McQuillan Cryptography, Information Theory, and Error-Correction. Wiley. 2021. – 688 p.

3.2.6. Duncan Buell. Fundamentals of Cryptography: Introducing Mathematical and Algorithmic Foundations. Springer. 2021. – 296 p.

3.2.7. Lisa Bock. Modern Cryptography for Cybersecurity Professionals. Packt Publishing. 2021. – 286 p.

Допоміжна література

3.2.8. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: монографія. – Харків, ХНУРЕ, Форт, 2012. – 868 с.

3.2.9.Корченко О.Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.:іл.

3.2.10. Задірака В.К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С.Олексюк. К. -Тернопіль: Підручники і посібники, 2007. – 272 с.

3.2.11. Jean-Philippe Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption Paperback. Kindle Edition, 2017. – 313 pages.

3.2.12. Mollin, R. A. Introduction to Cryptography. — CRC Press, 2007. — P. 80.— 413 p. — ISBN 1584886188.

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.cryptography.org
3.3.7.www.iso.org
3.3.8. www.cryptography.com
3.3.9. www.springerlink.com
3.3.10. www.financialcryptography.com
3.3.12. www.cryptonessie.org
3.3.13. 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	Мах кількість балів	
	Денна форма навчання	Заочна форма навчання
1 семестр		
Модуль №1 «Сучасні криптографічні системи: математичні основи, класифікація та характеристика»		
Виконання та захист лабораторних робіт	6б×8 = 48	10б×3 = 30
Виконання та захист розрахунково-графічної роботи	20	–
Виконання та захист домашнього завдання (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		**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

(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				