(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
«___»_____ 2025 р.

КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ

# РОБОЧА ПРОГРАМА
## навчальної дисципліни
## «Безпека в кібернетичному просторі»

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

| Форма здобуття освіти | Сем. | Усього (год. / кредитів ECTS) | ЛКЦ | ПР.З | Л.З | СРС | ДЗ / РГР / К.р | КР / КП | Форма сем. контролю |
|---|---|---|---|---|---|---|---|---|---|
| Денна | 1 | 195/6,5 | 32 | - | 32 | 131 | 1 дз - 1 с | - | Диф залік 1 с |

Індекс: № НМ-4-F5-2/25-2.1.4

Робочу програму навчальної дисципліни «Безпека у кібернетичному просторі» розроблено на основі освітньо-професійних програми «Системи технічного захисту інформації, автоматизація її обробки», навчального плану № НМ-4-F5-2/25 та робочого навчального плану №РМ-4-F5-2/25 підготовки здобувачів вищої освіти освітнього ступеня «Магістр» за спеціальністю F5 «Кібербезпека та захист інформації» та відповідних нормативних документів.

Робочу програму розробив
Завідувач кафедри технічного захисту інформації,
д.т.н., професор_____ Валерій КОЗЛОВСЬКИЙ

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійних програм «Системи технічного захисту інформації, автоматизація її обробки», 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

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» вересня 2025 р.

Голова НМРР _____ Оксана ПОЛІЩУК

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

**ЗМІСТ**

**Вступ** ..... 4

**1. Пояснювальна записка** ..... 4
1.1. Місце, мета, завдання навчальної дисципліни ..... 4
1.2. Результати навчання, які дає можливість досягти навчальна дисципліна ..... 4
1.3. Компетентності, які дає можливість здобути навчальна дисципліна ..... 6
1.4. Міждисциплінарні зв'язки ..... 7

**2. Програма навчальної дисципліни** ..... 7
2.1. Зміст навчальної дисципліни ..... 7
2.2. Модульне структурування та інтегровані вимоги до кожного модуля ..... 7
2.3. Тематичний план ..... 10
2.4. Домашнє завдання ..... 10

**3. Навчально-методичні матеріали з дисципліни** ..... 11
3.1. Методи навчання .....
3.2. Рекомендована література (базова і допоміжна) ..... 11
3.3. Інформаційні ресурси в Інтернет ..... 11
11

**4. Рейтингова система оцінювання набутих студентом знань та вмінь** ..... 12

12

## ВСТУП

Робоча програма (РП) навчальної дисципліни «Безпека в кібернетичному просторі» розроблена на основі «Методичних рекомендацій до розроблення і оформлення робочої програми навчальної дисципліни денної та заочної форм навчання», затверджених наказом ректора від 29.04.2021 No 249/од, та відповідних нормативних документів.

## 1. ПОЯСНЮВАЛЬНА ЗАПИСКА

**1.1. Місце, мета, завдання навчальної дисципліни.**

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

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

— вивчення сучасних інформаційних технологій у галузі інформаційної/кібербезпеки;

— впровадження методів та засобів запобігання несанкціонованому отриманню інформації;

— застосування методів та засобів криптографічного захисту інформації; впровадження технологій захисту інформації в кіберпросторі та виявлення кібератак.

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

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

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

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

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико- математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

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

ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем технологій, бізнес операційних процесів у сфері інформаційної та або кібербезпеки в цілому.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ПРН24. 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)

ПРН25. Проводити спеціальні дослідження засобів обробки інформації, технічних засобів.

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

ПРН27. Вирішувати задачі 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 інфраструктури держави, в інтересах її сталого розвитку, включаючи авіаційну галузь.

**Трудові функції**

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

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

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

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

**1.3. Компетентності, які дає можливість здобути навчальна дисципліна.**

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

**Інтегральну**

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

**Загальні**

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Здатність проводити дослідження на відповідному рівні.

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

**Фахові**

ФК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

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

ФК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

ФК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

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

ФК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ФК9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки

ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

ФК11. Здатність проводити ліцензування, атестацію та сертифікацію об'єктів інформаційної діяльності.

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

ФК13. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.

ФК14. Здатність моделювати безпекові процеси в авіаційній галузі.

**1.4. Міждисциплінарні зв'язки.**

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

## 2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**2.1. Зміст навчальної дисципліни**

Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох навчальних модулів, а саме:

— навчального модуля №1 «Забезпечення безпеки у кіберпросторі»;

— навчального модуля №2 «Забезпечення кібербезпеки складних систем».

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

**2.2. Модульне структурування та інтегровані вимоги до кожного модуля**

**Модуль №1 "Забезпечення безпеки у кіберпросторі".**

Інтегровані вимоги модуля №1:

**Знати:**

— поняття кіберпростору та кібербезпеки;

— комп'ютерні віруси та вірусоподібні програми;

— сучасні методи автентифікації та ідентифікації;

— принципи забезпечення безпеки програмного забезпечення;

— порядок забезпечення безпеки віддалених інформаційних ресурсів.

**Вміти:**

— використовувати державні нормативно-правові акти та міжнародні стандарти щодо забезпечення кібербезпеки;

— застосовувати методи та засоби забезпечення безпеки програм та даних;

— забезпечувати безпеку віддалених інформаційних ресурсів.

**Тема 1. Основи кібербезпеки та кіберпростору.**

Поняття кіберпростору, кібербезпеки та кіберзлочинності. Аналіз ролі кіберпростору та кібербезпеки як головних ознак сучасної інформаційної цивілізації.

**Тема 2. Загрози, вразливості та кібератаки.**

Розглядаються основні види кіберзагроз, зокрема шкідливе програмне забезпечення, соціальна інженерія, фішинг та інші. Поняття вразливостей інформаційних систем та наводяться приклади кібератак.

**Тема 3. Нормативно-правове регулювання кібербезпеки.**

Державні нормативно-правові акти у сфері кібербезпеки. Також розглядаються міжнародні стандарти та угоди, спрямовані на забезпечення захисту інформаційних ресурсів.

**Тема 4. Механізми та політики захисту даних.**

У темі аналізуються основні підходи до захисту програм та даних за допомогою механізмів розмежування прав доступу. Розглядаються приклади політик безпеки в сучасних інформаційних системах.

**Тема 5. Методи автентифікації та захисту паролів.**

Вивчаються хеш-функції для захисту паролів (на прикладі MD5). Аналізується стійкість паролів до злому та сучасні методи автентифікації користувачів.

**Тема 6. Електронний цифровий підпис та біометричні технології.**

Тема присвячена використанню електронного цифрового підпису як механізму підтвердження достовірності даних. Окремо розглядаються біометричні методи ідентифікації користувачів.

**Тема 7. Безпека веб-застосунків.**

Розглядаються підходи до захисту сесій веб-застосунків. Пояснюються методи контролю коректності введених даних, захист від SQL-ін'єкцій та атак міжсайтового скриптингу (XSS).

**Тема 8. Захист віддалених інформаційних ресурсів.**

У темі описуються методи безпечного конфігурування серверів, установки системи оновлень та контролю системних журналів. Окремо вивчається захист від шкідливих програм, сканування вразливостей та виявлення кібератак.

**Модуль №2 "Забезпечення кібербезпеки складних систем".**

Інтегровані вимоги модуля №2:

**Знати:**

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

**Вміти:**

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

**Тема 1. Забезпечення безпеки кінцевих користувачів у кіберпросторі.**

У темі розглядаються основні засоби захисту користувачів у кіберпросторі. Аналізується використання пасток у «порожній» мережі, перенаправлення шкідливого трафіку та зворотне трасування. Також розглядається важливість роботи з рекомендованими версіями операційних систем та програмного забезпечення, що зменшує кількість вразливостей.

**Тема 2. Технічні засоби безпеки для кінцевих користувачів.**

Вивчається роль антивірусних засобів, налаштування веб-браузерів у безпечному режимі та використання додаткових механізмів захисту браузерів. Окремо розглядаються фільтри фішингу, міжмережеві екрани, системи виявлення вторгнень та механізми автоматичного оновлення програм.

**Тема 3. Основи криптографічного захисту даних.**

Розглядаються поняття шифрів та їх застосування у комп'ютерних системах. Аналізуються методи шифрування, що використовуються для забезпечення конфіденційності інформації.

**Тема 4. Симетричні та асиметричні алгоритми шифрування.**

У темі приділяється увага симетричним і асиметричним методам шифрування, їх перевагам та недолікам. Окремо досліджується підтримка асиметричних алгоритмів у бібліотеках сучасних мов програмування.

**Тема 5. Методи приховування інформації.**

Розглядаються принципи приховування інформації у потоках даних та можливості стеганографії. Наводяться приклади використання цих методів для захисту інформації та прихованого обміну даними.

**Тема 6. Захист від соціальної інженерії.**

Основи соціальної інженерії як методу розвідки та впливу на користувачів. Пояснюється важливість розробки політик безпеки, категорування та класифікації інформації. Розглядається роль моніторингу соціальних мереж і технічних механізмів контролю.

**Тема 7. Кібербезпека в критичних сферах.**

Тема присвячена особливостям забезпечення кібербезпеки в медицині та енергетиці. Аналізуються основні загрози для цих галузей та сучасні методи їх подолання.

**Тема 8. Кібербезпека сучасних цифрових систем.**

Питання безпеки мобільних пристроїв, банківських систем, електронної комерції, інтернету речей, соціальних мереж та хмарних застосунків. Наголошується на важливості комплексного підходу до захисту таких систем.

**2.3. Тематичний план.**

| № з/п | Назва теми | Обсяг навчальних занять (год.) Денна форма здобуття освіти | | | |
|---|---|---|---|---|---|
| | | Усього | Лекції | Лабор. заняття | СРС |
| **Модуль № 1 «Забезпечення безпеки у кіберпросторі»** | | | | | |
| | | **2 семестр** | | | |
| 1.1 | Тема 1. Основи кібербезпеки та кіберпростору | 9 | 2 | - | 7 |
| 1.2 | Тема 2. Загрози, вразливості та кібератаки. | 12 | 2 | 2 | 8 |
| 1.3 | Тема 3. Нормативно-правове регулювання кібербезпеки. | 11 | 2 | 2 | 7 |
| 1.4 | Тема 4. Механізми та політики захисту даних. | 11 | 2 | 2 | 7 |
| 1.5 | Тема 5. Методи автентифікації та захисту паролів. | 12 | 2 | 2 | 8 |
| 1.6 | Тема 6. Електронний цифровий підпис та біометричні технології. | 12 | 2 | 2 | 8 |
| 1.7 | Тема 7. Безпека веб-застосунків. | 11 | 2 | 2 | 7 |
| 1.8 | Тема 8. Захист віддалених інформаційних ресурсів. | 11 | 2 | 2 | 7 |
| 1.9 | Модульна контрольна робота № 1 | 7 | - | 1 | 6 |
| | **Усього за модулем № 1** | **96** | **16** | **15** | **65** |
| **Модуль № 2 «Забезпечення кібербезпеки складних систем»** | | | | | |
| 2.1 | Тема 1. Забезпечення безпеки кінцевих користувачів у кіберпросторі. | 11 | 2 | 2 | 7 |
| 2.2 | Тема 2. Технічні засоби безпеки для кінцевих користувачів. | 12 | 2 | 2 | 8 |
| 2.3 | Тема 3. Основи криптографічного захисту даних | 11 | 2 | 2 | 7 |
| 2.4 | Тема 4. Симетричні та асиметричні алгоритми шифрування. | 12 | 2 | 2 | 8 |
| 2.5 | Тема 5. Методи приховування інформації | 11 | 2 | 2 | 7 |
| 2.6 | Тема 6. Захист від соціальної інженерії | 12 | 2 | 2 | 8 |
| 2.7 | Тема 7. Кібербезпека в критичних сферах. | 10 | 2 | 2 | 6 |
| 2.8 | Тема 8. Кібербезпека сучасних цифрових систем | 9 | 2 | 2 | 5 |
| 2.9 | Домашнє завдання | 8 | - | - | 8 |
| 2.10 | Модульна контрольна робота №2 | 2 | - | 1 | 1 |
| | **Усього за модулем № 2** | **99** | **16** | **17** | **66** |
| | **Усього за навчальною дисципліною** | **195** | **32** | **32** | **131** |

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

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

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

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

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

Час, потрібний для виконання домашнього завдання, контрольної (домашньої) роботи - до 8 годин самостійної роботи.

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

## 3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

### 3.1. Методи навчання

При вивченні навчальної дисципліни «Безпека в кібернетичному просторі» використовуються навчальні технології, що застосовуються для активізації навчально-пізнавальної діяльності студентів, а саме: робота в малих групах, семінар-дискусія, мозкова атака, кейс, презентація, рольова гра, дидактична гра тощо.

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

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

### 3.2. Рекомендована література

**Базова література**

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

3.2.2. Закон України «Про захист персональних даних».

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

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

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

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

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

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

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

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

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

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

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

**Допоміжна література**

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

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

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

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

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

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

**3.3. Інформаційні ресурси в інтернеті**

3.3.1. http://zakon.rada.gov.ua. 3.3.2. http://scholar.google.com.ua/

3.3.2. http://www.dstszi.gov.ua/dstszi/control/uk/index. 3.3.4. http://www.nau.edu.ua.

3.3.3. https://www.coursera.org/learn/r-programming/.

3.3.4 . http://prometheus.org.ua/dataanalysis/.

Відповідне інформаційне навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment).

Електронний репозитарій наукової бібліотеки КАІ: er.kai.edu.ua.

## 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 здобуття освіти |
| | 1 семестр |
| **Модуль № 1 «Забезпечення безпеки в кіберпросторі»** | |
| Виконання та захист лабораторних робіт | 35 |
| *Для допуску до виконання модульної контрольної роботи № 1 студент має набрати не менше* | *21* |
| Виконання модульної контрольної роботи № 1 | 10 |
| **Усього за модулем № 1** | **45** |

| **Модуль № 2 «Забезпечення кібербезпеки складних систем»** | |
|---|---|
| Виконання та захист лабораторних робіт | 40 |
| Виконання домашнього завдання | 5 |
| Виконання контрольної (домашньої) роботи | - |
| *Для допуску до виконання модульної контрольної роботи № 2 студент має набрати не менше* | *19* |
| Виконання модульної контрольної роботи № 2 | 10 |
| **Усього за модулем № 2** | **55** |
| **Усього за модулем № 1, 2** | **100** |
| **Усього за дисципліною** | **100** |

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

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

4.4. 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.

4.5. 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 підсумкової семестрової контрольної роботи** | **Виконання та захист домашнього завдання, (контрольної (домашньої) роботи (ЗФН)** | **Виконання модульної роботи** | |
| 32-35 | 36-40 | 18-20 | 27-30 | 9-10 | Відмінно |
| 27-31 | 30-35 | 15-17 | 23-26 | 8 | Добре |
| 21-26 | 24-29 | 12-14 | 18-22 | 6-7 | Задовільно |
| менше 21 | менше 24 | менше 12 | менше 18 | менше 6 | 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 | 03.02 | 02.09.25 | Федоренко К.Я. | | |
| | | | | | |
| | | | | | |

(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 | | | | |