

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**  
**«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

Кафедра

кібербезпеки  
(назва кафедри, яка забезпечує викладання дисципліни)

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**  
**РОЗШИРЕНА МЕРЕЖЕВА ТА ХМАРНА БЕЗПЕКА**  
(назва навчальної дисципліни)

рівень вищої освіти другий (магістерський)  
перший (бакалаврський) / другий (магістерський)

галузь знань 12 Інформаційні технології  
(шифр і назва)

спеціальність 125 Кібербезпека  
(шифр і назва)

освітня програма Кібербезпека  
(назви освітньої програми)

вид дисципліни спеціальна (фахова) підготовка; обов'язкова  
(загальна підготовка / спеціальна (фахова) підготовка; обов'язкова/вибіркова)

форма навчання денна  
(денна / заочна/дистанційна)

## ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни Розширена мережева та хмарна безпека  
(назва дисципліни)

Розробники:

к.т.н., с.н.с.  
(посада, науковий ступінь та вчене звання)


  
(підпис)

Андрій ТКАЧОВ  
(ім'я та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри  
кібербезпеки  
(назва кафедри, яка забезпечує викладання дисципліни)

Протокол від “22” серпня 2022 року № 1

Завідувач кафедри

  
(підпис)

Сергій ЄВСЕЄВ  
(ім'я та прізвище)


## ЛИСТ ПОГОДЖЕННЯ

Шифр та назва освітньої програми 125 “Кібербезпека”

---


Кафедра кібербезпеки  
(назва кафедри на якій викладається дисципліна)

Гарант ОП

 22.08.2022р  
(Підпис, дата)

Олександр МІЛОВ  
(ім'я та прізвище)

Завідувач кафедрою

 22.08.2022р  
(Підпис, дата)

Сергій ВСЕЧ  
(ім'я та прізвище)

## ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

№ зп	Дата засідання кафедри-розробника РПНД	Номер протоколу	Підпис завідувача кафедри (яка викладає)	Підпис завідувача кафедри (на якій викладається)	Підпис гаранта освітньої програми
1					
2					
3					
4					
5					

## МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**Мета** навчальної дисципліни "Розширена мережева та хмарна безпека" – отримання студентами загальних відомостей про принципи побудови комплексних систем захисту інформації для формування контуру мережевої та хмарної безпеки в інформаційно-комунікаційних системах на основі Інтернет-технологій та застосунків; придбання навичок з нейтралізації типових мережевих та хмарних загроз, використання протоколів для захисту мереж, захисту від шкідливого програмного забезпечення та мережевого трафіку.

### Компетентності та результати навчання

Компетентності	Результати навчання
<p>КЗ-1. Здатність застосовувати знання у практичних ситуаціях</p>	<p>РН1. 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.</p> <p>РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.</p> <p>РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.</p> <p>РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.</p> <p>РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.</p> <p>РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.</p> <p>РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.</p> <p>РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління,</p>

Компетентності	Результати навчання
	<p>контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.</p> <p>РН13. 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.</p> <p>РН14. 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.</p> <p>РН16. 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.</p> <p>РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та\або кібербезпеки.</p> <p>РН19. 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.</p> <p>РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та\або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.</p> <p>РН21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та\або кібербезпеки.</p> <p>РН23. 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.</p>
<p>КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності)</p>	<p>РН5. 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.</p> <p>РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та\або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>РН15. 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.</p> <p>РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та\або кібербезпеки.</p>

Компетентності	Результати навчання
	<p>РН19. 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.</p> <p>РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.</p>
<p>КФ1. 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</p>	<p>РН1. 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.</p> <p>РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.</p> <p>РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.</p> <p>РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.</p> <p>РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.</p> <p>РН19. 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.</p> <p>РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.</p> <p>РН21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.</p> <p>РН22. 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.</p> <p>РН23. 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.</p>
<p>КФ3. Здатність досліджувати,</p>	<p>РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або</p>

Компетентності	Результати навчання
<p>розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури</p>	<p>кібербезпеки у широких або мультидисциплінарних контекстах.  РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.  РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.  РН16. 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.  РН17. 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.  РН19. 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.  РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.  РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.  РН22. 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.  РН23. 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.</p>
<p>КФ4. 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</p>	<p>РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.  РН12. 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.  РН14. 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.  РН16. 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.</p>



Компетентності	Результати навчання
	<p>РН19. 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.</p>
<p>КФ5. 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</p>	<p>РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.</p> <p>РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.</p> <p>РН16. 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.</p> <p>РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.</p>
<p>КФ7. 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</p>	<p>РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.</p> <p>РН12. 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.</p> <p>РН16. 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.</p> <p>РН19. 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.</p> <p>РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.</p> <p>РН23. 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.</p>
<p>КФ8. Здатність досліджувати, розробляти, впроваджувати та</p>	<p>РН13. 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</p>

Компетентності	Результати навчання
<p>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</p>	<p>інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>РН19. 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.</p> <p>РН21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.</p> <p>РН23. 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.</p>
<p>КФ9. 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</p>	<p>РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.</p> <p>РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.</p> <p>РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.</p> <p>РН14. 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.</p> <p>РН16. 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.</p> <p>РН19. 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.</p> <p>РН23. 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.</p>

## Структурно-логічна схема вивчення навчальної дисципліни

Попередні дисципліни:	Наступні дисципліни:
Веб-безпека	Бездротова та мобільна безпека
Безпека та аудит бездротових та рухомих мереж	Цифрова криміналістика
Безпека в інформаційно-комунікаційних системах	Тестування на проникнення та етичний хакінг
Інформаційні системи та інтернет технології	

## ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Загальний обсяг (годин) / кредитів ECTS	З них		За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль	Семестровий контроль	
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари			Залік	Екзамен
<b>2</b>	<b>90/3</b>	<b>48</b>	<b>42</b>	<b>32</b>	<b>16</b>	-	-	-	-	+

Співвідношення кількості годин аудиторних занять до загального обсягу складає 53,3 (%).

## СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	<p style="text-align: center;">Номер семестру (якщо дисципліна викладається у декількох семестрах).</p> <p style="text-align: center;">Найменування тем та питань кожного заняття.</p> <p style="text-align: center;">Завдання на самостійну роботу.</p>	Рекомендована література (базова, допоміжна)
1	Л	2	<b>Тема 1. Особливості побудови мережевих систем.</b> Особливості побудови мережевих систем.	1, 2
	СР	2		
2	Л	2	<b>Тема 1. Особливості побудови мережевих систем.</b> Особливості побудови мережевих систем.	1, 2
	ЛЗ	2		
	СР	2		
3	Л	2	<b>Тема 2. Особливості побудови хмарних систем.</b>	2, 3, 4

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			Особливості побудови хмарних систем.	
4	СР	2		
	Л	2	<b>Тема 2. Особливості побудови хмарних систем.</b> Особливості побудови хмарних систем.	2, 3, 4
	ЛЗ	2	<b>Лабораторне заняття № 2.</b> Дослідження особливостей побудови хмарних систем	2, 3, 4
5	СР	2		
	Л	2	<b>Тема 3. Модель мережевих та хмарних загроз.</b> Модель мережевих та хмарних загроз.	1, 6, 7
6	СР	2		
	Л	2	<b>Тема 3. Модель мережевих та хмарних загроз.</b> Модель мережевих та хмарних загроз.	1, 6, 7
	ЛЗ	2	<b>Лабораторне заняття № 3.</b> Дослідження моделі мережевих загроз.	1, 6, 7
7	СР	2		
	Л	2	<b>Тема 4. Засоби збору даних.</b> Засоби збору даних.	2, 3, 4, 5
8	СР	2		
	Л	2	<b>Тема 4. Засоби збору даних.</b> Засоби збору даних.	2, 3, 4, 5
	ЛЗ	2	<b>Лабораторне заняття № 4.</b> Дослідження засобів збору даних.	2, 3, 4, 5
	СР	2		
9	СР	2		
	Л	2	<b>Тема 5. Засоби інформаційного аналізу у мережах.</b> Засоби інформаційного аналізу у мережах.	2, 3, 4, 5
10	СР	2		
	Л	2	<b>Тема 5. Засоби інформаційного аналізу у мережах.</b> Засоби інформаційного аналізу у мережах.	2, 3, 4, 5
	ЛЗ	2	<b>Лабораторне заняття № 5.</b> Дослідження засобів інформаційного аналізу у мережах.	2, 3, 4, 5
	СР	2		
11	СР	2		
	Л	2	<b>Тема 6. Засоби інформаційного аналізу у хмарах.</b> Засоби інформаційного аналізу у хмарах.	2, 3, 4, 5
12	СР	2		
	Л	2	<b>Тема 6. Засоби інформаційного аналізу у хмарах.</b> Засоби інформаційного аналізу у хмарах.	2, 3, 4, 5
	ЛЗ	2	<b>Лабораторне заняття № 6.</b> Дослідження засобів інформаційного аналізу у хмарах.	2, 3, 4, 5
	СР	2		

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
13	Л	2	<b>Тема 7. Моделі атак на мережи та хмари.</b> Моделі атак на мережи та хмари.	1, 5
	СР	2		
14	Л	2	<b>Тема 7. Моделі атак на мережи та хмари.</b> Моделі атак на мережи та хмари.	1, 5
	СР	2		
	ЛЗ	2	<b>Лабораторне заняття № 7.</b> Дослідження моделей атак на мережи та хмари.	1,5
	СР	2		
15	Л	2	<b>Тема 8. Засоби захисту мережевих та хмарних систем.</b> Засоби захисту мережевих та хмарних систем.	2,3,4
	СР	2		
16	Л	2	<b>Тема 8. Засоби захисту мережевих та хмарних систем.</b> Засоби захисту мережевих та хмарних систем.	2,3,4
	СР	2		
	ЛЗ	2	<b>Лабораторне заняття № 8.</b> Дослідження засобів захисту мережевих та хмарних систем.	2,3,4
	СР	2		
<b>Разом (годин)</b>		<b>90</b>		

## САМОСТІЙНА РОБОТА

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час.

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацювання лекційного матеріалу	26
2	Підготовка до практичних(лабораторних, семінарських)занять	16
	<b>Разом</b>	<b>42</b>

## ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Не передбачено навчальним планом.

## МЕТОДИ НАВЧАННЯ

На лекційних заняттях викладання матеріалу здійснюється в усній формі із записом основних положень лекції у конспект.

На практичних заняттях здійснюється підготовка до виконання лабораторних робіт: вирішуються типові завдання згідно темам лабораторних робіт.

Під час самостійної роботи вдома студенти виконують додаткові завдання, навчаються використовувати інструментальні засоби для підвищення практичних навичок.

На лабораторних заняттях студенти виконують та демонструють індивідуальні завдання. Для цього вони використовують необхідні програмні та апаратні інструментальні засоби: Internet, ОС Linux/Windows, VisualStudioCode, Kali Linux, персональні комп'ютери.

Студенти мають можливість навчатися та розробляти реальні проекти, взявши участь у програмі «Інноваційний кампус» НТУ «ХПІ».

Додаткові знання студенти отримують у рамках неформальної освіти, завдяки організаціям, що забезпечують надання освітніх послуг.

## МЕТОДИ КОНТРОЛЮ

Поточний контроль при вивченні дисципліни реалізується у формі опитувань на лекційних заняттях, захисту лабораторних робіт, проведення контрольних робіт.

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

- з лекційного матеріалу – шляхом проведення тестування, презентацій докладів за темами лекційних занять;
- з лабораторних завдань – за допомогою перевірки виконаних завдань.

Семестровий контроль проводиться у формі екзамену відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом.

Семестровий контроль проводиться по екзаменаційних білетах в письмовій формі за контрольними завданнями, а також шляхом тестування з використанням технічних засобів.

Результати поточного контролю враховуються як допоміжна інформація для виставлення оцінки з даної дисципліни.

Студент вважається допущеним до семестрового екзамену з навчальної дисципліни за умови повного відпрацювання усіх лабораторних робіт, виконання контрольних робіт та тестових опитувань.

## РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів для оцінювання успішності студента для іспиту

Контрольні роботи	Лабораторні роботи	РГЗ	Індивідуальні завдання	Тощо	Іспит	Сума
20	40	-	-	-	40	100

## Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під **системою оцінювання** розуміють сукупність методів (письмові, усні і практичні тести, екзамени, проекти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними **критеріями оцінювання** для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

**Критерії оцінювання** – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв'язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об'єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100 бальної шкали (табл. 2). Оцінки обов'язково переводять у національну шкалу (з виставленням державної семестрової оцінки „відмінно”, „добре”, „задовільно” чи „незадовільно”) та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ЄКТС

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
90-100	A	Відмінно	- <b>Глибоке знання</b> навчального матеріалу, що містяться в <b>основних і додаткових літературних джерелах;</b> - <b>вміння аналізувати</b> явища, які вивчаються, в їхньому взаємозв'язку і розвитку; - <b>вміння проводити теоретичні розрахунки;</b> - <b>відповіді</b> на запитання <b>чіткі,</b>	Відповіді на запитання можуть містити <b>незначні неточності</b>

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
			лаконічні, логічно послідовні; - вміння вирішувати складні практичні задачі.	
82-89	B	Добре	- Глибокий рівень знань в обсязі обов'язкового матеріалу, - вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; - вміння вирішувати складні практичні задачі.	Відповіді на запитання містять певні неточності;
75-81	C	Добре	- Міцні знання матеріалу, що вивчається, та його практичного застосування; - вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; - вміння вирішувати практичні задачі.	- невміння використовувати теоретичні знання для вирішення складних практичних задач.
64-74	D	Задовільно	- Знання основних фундаментальних положень матеріалу, що вивчається, та їх практичного застосування; - вміння вирішувати прості практичні задачі.	Невміння давати аргументовані відповіді на запитання; - невміння аналізувати викладений матеріал і виконувати розрахунки; - невміння вирішувати складні практичні задачі.
60-63	E	Задовільно	- Знання основних фундаментальних положень - вміння вирішувати найпростіші практичні задачі.	Незнання окремих (непринципових) питань з матеріалу модуля; - невміння послідовно і аргументовано висловлювати думку; - невміння застосовувати теоретичні положення при розв'язанні практичних задач



Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
35-59	FX (потрібне додаткове вивчення)	Незадовільно	Додаткове вивчення матеріалу може бути виконане в терміни, що передбачені навчальним планом.	Незнання основних фундаментальних положень навчального матеріалу модуля; - істотні помилки у відповідях на запитання; - невміння розв'язувати прості практичні задачі.
1-34	F (потрібне повторне вивчення)	Незадовільно		- Повна відсутність знань значної частини навчального матеріалу модуля; - істотні помилки у відповідях на запитання; - незнання основних фундаментальних положень; - невміння орієнтуватися під час розв'язання простих практичних задач

## НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Стандарт вищої освіти галузі знань 12 “Інформаційні технології” для другого (магістерського) рівня вищої освіти, який затверджено наказом Міністерства освіти і науки України від 18.03.2021 р. № 332 та введено в дію з 2021/2022 навчального року.

2. Робоча програма навчальної дисципліни.

3. Силабус навчальної дисципліни.

4. Персональні навчальні системи кафедри кібербезпеки НТУ “ХП”:

[https://iiii-](https://iiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8)

[my.sharepoint.com/personal/serhii\\_yevseiev\\_khpi\\_edu\\_ua1/\\_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8](https://iiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8)

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА

### Базова література

1	Безпека хмарного середовища [Електронний ресурс]. – Режим доступу : <a href="https://www.netacad.com/ru/courses/cybersecurity/cloud-security">https://www.netacad.com/ru/courses/cybersecurity/cloud-security</a>
2	Amazon Web Services (AWS) [Електронний ресурс]. – Режим доступу : <a href="https://www.checkpoint.com/solutions/amazon-aws-security/">https://www.checkpoint.com/solutions/amazon-aws-security/</a>
3	Microsoft Azure (Azure) [Електронний ресурс]. – Режим доступу : <a href="https://www.checkpoint.com/solutions/microsoft-azure-security/">https://www.checkpoint.com/solutions/microsoft-azure-security/</a>
4	Google Cloud Platform (GCP) [Електронний ресурс]. – Режим доступу : <a href="https://www.checkpoint.com/solutions/google-cloud-platform-security/">https://www.checkpoint.com/solutions/google-cloud-platform-security/</a>
5	Kali Linux [Електронний ресурс]. – Режим доступу : <a href="https://www.kali.org/">https://www.kali.org/</a>

### Допоміжна література

6	Cloud Computing Security [Електронний ресурс]. – Режим доступу : <a href="https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.htm">https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.htm</a>
7	Computer Network Security [Електронний ресурс]. – Режим доступу : <a href="https://www.javatpoint.com/computer-network-security">https://www.javatpoint.com/computer-network-security</a>

## ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. [https://www.google.com/search?q=%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&rlz=1C1SQJL\\_enUA886UA886&oq=%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&aqs=chrome..69i57j0i512l4j69i6l13.4705j0j7&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&rlz=1C1SQJL_enUA886UA886&oq=%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&aqs=chrome..69i57j0i512l4j69i6l13.4705j0j7&sourceid=chrome&ie=UTF-8)

2. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ”:  
[https://iiii-my.sharepoint.com/personal/serhii\\_yevseiev\\_khpi\\_edu\\_ua1/\\_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8](https://iiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8)