МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Кафедра _____*кібербезпеки*_____
(назва кафедри, яка забезпечує викладання дисципліни)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ ПРОГРАМУВАННЯ

(назва навчальної дисципліни)

рівень вищої освіти_____*перший (бакалаврський)*_____
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)

Харків – 2022 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни___ОСНОВИ ПРОГРАМУВАННЯ_____
(назва дисципліни)

Розробники:

___*к.т.н., с.н.с.*_____  *Андрій ТКАЧОВ*
(посада, науковий ступінь та вчене звання) (підпис) (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  *Сергій ЄВСЕЄВ*
(підпис) (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 _____ *Сергій ЄВСЕЄВ*
(Підпис, дата) (ім’я та прізвище)

Завідувач кафедрою _____ 22.08.2022р _____ *Сергій ЄВСЕЄВ*
(Підпис, дата) (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 "Основи програмування" – отримання студентами загальних відомостей про сучасні технології програмування та цілеспрямоване використання розповсюджених мов програмування, а також отримання знань та навичок практичного застосування прийомів програмування при створенні прикладних та системних програмних продуктів.

Компетентності та результати навчання

Компетентності	Результати навчання
КЗ 1. Здатність застосовувати знання у практичних ситуаціях.	РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН–10. виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН–11. виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН–18 використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–21 вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–22 вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних

	системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз. РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних

	(автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	РН–7 діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН–8 готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН-14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН-17. Забезпечувати процеси захисту та

	функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН-18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН-29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН-35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН-53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

	РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз;
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	РН–9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-

	телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17. забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–21. вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–23. реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–24. вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–25. забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–26. впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН–27. вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних

	(автоматизованих) системах; РН–28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН–29. здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35. вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43. застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44. вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН–48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН–49. забезпечувати належне функціонування системи

	моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50. забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52. використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–12 розробляти моделі загроз та порушника; РН–16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-

	телекомунікаційних системах; РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–48 виконувати впровадження та підтримку

	систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН–49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–21вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–28 аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН–29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні

	стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН–11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах; РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених

	компонент; РН–18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–24.Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН–32.Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в

	інформаційно-телекомунікаційних системах; РН–49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–12 розробляти моделі загроз та порушника; РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН–28 аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН–29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих)

	системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Структурно-логічна схема вивчення навчальної дисципліни

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
Алгебра програмування	Інформаційні системи та інтернет технології
Розробка та аналіз алгоритмів	Технології програмування

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Всього (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		Контрольні роботи (кількість робіт)	Залік	Екзамен
1	2	3	4	5	6	7	8	9	10	11
1	**120/4**	**64**	**56**	**32**	**32**	**–**	**–**	**2**	**–**	**+**

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

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ 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)
1	Л СР	2 2	**Тема 1. Вступ до курсу.** Термін програмування. Термін мова програмування. Класифікація мов програмування	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття № 1** Вступ до курсу. Термін програмування. Термін мова програмування. Класифікація мов програмування	
2	Л	2	**Тема 1. Вступ до курсу.** Термін програмування. Термін мова програмування. Класифікація мов програмування	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття № 1** Вступ до курсу. Термін програмування. Термін мова програмування. Класифікація мов програмування	
3	Л СР	2 2	**Тема 2. Компіляція програми з командної строки.** Система котролю версіями git. Makefile. Відлагодження програми. Точки зупинки (breakpoints).	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття №2 .** Компіляція програми з командної строки. Система котролю версіями git. Makefile. Відлагодження програми. Точки зупинки (breakpoints)	
4	Л СР	2 2	**Тема 2. Компіляція програми з командної строки.** Система котролю версіями git. Makefile. Відлагодження програми. Точки зупинки (breakpoints).	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття №2 .** Компіляція програми з командної строки. Система котролю версіями git. Makefile. Відлагодження програми. Точки зупинки (breakpoints)	
5	Л СР	2 2	**Тема 3. Основні типи та структури даних, що застосовуються при програмуванні.** Типи даних та їх розміри. Преобразування типів. Класифікація операторів та їх пріоритети. Змінні в прогамуванні. Структура програми. Розробка лінійних програм. Робота з числовими типами даних. Константи. Коментарі.	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття № 3** Основні типи та структури даних, що застосовуються при програмуванні. Типи даних та їх розміри. Преобразування типів. Класифікація операторів та їх пріоритети. Змінні в прогамуванні. Структура програми. Розробка лінійних програм. Робота з числовими типами даних. Константи. Коментарі	

№ 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)
6	Л	2	**<u>Тема 3.</u> Основні типи та структури даних, що застосовуються при програмуванні.** Типи даних та їх розміри. Преобразування типів. Класифікація операторів та їх пріоритети. Змінні в прогамуванні. Структура програми. Розробка лінійних програм. Робота з числовими типами даних. Константи. Коментарі.	1-8, 9-12
	СР	2		
	ЛЗ	2	**Лабораторне заняття № 3** Основні типи та структури даних, що застосовуються при програмуванні. Типи даних та їх розміри. Преобразування типів. Класифікація операторів та їх пріоритети. Змінні в прогамуванні. Структура програми. Розробка лінійних програм. Робота з числовими типами даних. Константи. Коментарі	
	СР	2		
7	Л	2	**<u>Тема 3.</u> Основні типи та структури даних, що застосовуються при програмуванні.** Типи даних та їх розміри. Преобразування типів. Класифікація операторів та їх пріоритети. Змінні в прогамуванні. Структура програми. Розробка лінійних програм. Робота з числовими типами даних. Константи. Коментарі.	1-8, 9-12
	СР	2		
	ЛЗ	2	**Лабораторне заняття № 3** Основні типи та структури даних, що застосовуються при програмуванні. Типи даних та їх розміри. Преобразування типів. Класифікація операторів та їх пріоритети. Змінні в прогамуванні. Структура програми. Розробка лінійних програм. Робота з числовими типами даних. Константи. Коментарі	
	СР	2		
8	Л	2	**<u>Тема 4.</u> Використання умовного оператора if**. Логічні операції. Тернарний оператор. Оператор вибору (case). Опис оператору вибору в вигляді схеми алгоритмів за умов присутності та відсутності оператору break.	1-8, 9-12
	СР	2		
	ЛЗ	2	**Лабораторне заняття № 4** Використання умовного оператора if. Логічні операції. Тернарний оператор. Оператор вибору (case). Опис оператору вибору в вигляді схеми алгоритмів за умов присутності та відсутності оператору break.	
	СР	2		
9	Л	2	**<u>Тема 4.</u> Використання умовного оператора if**. Логічні операції. Тернарний оператор. Оператор вибору (case). Опис оператору вибору в вигляді схеми алгоритмів за умов присутності та відсутності оператору break.	1-8, 9-12

№ 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)
	ЛЗ СР	2 2	**Лабораторне заняття № 4** Використання умовного оператора if. Логічні операції. Тернарний оператор. Оператор вибору (case). Опис оператору вибору в вигляді схеми алгоритмів за умов присутності та відсутності оператору break.	
10	Л СР	2 2	**<u>Тема 5.</u> Робота з операторами циклу (for, while-do, do-while).** Оператори break та continue.	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття № 5** Робота з операторами циклу (for, while-do, do-while). Оператори break та continue.	
11	Л	2	**<u>Тема 5.</u> Робота з операторами циклу (for, while-do, do-while).** Оператори break та continue.	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття № 5** Робота з операторами циклу (for, while-do, do-while). Оператори break та continue.	
12	Л СР	2 2	**<u>Тема 6.</u> Робота з масивами.** Об‘ява. Ініціалізація. Індексація. Алгоритм сортування типу «бульбашка». Одновимірні та багатовимірні масиви.	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття № 6** Робота з масивами. Об‘ява. Ініціалізація. Індексація. Алгоритм сортування типу «бульбашка». Одновимірні та багатовимірні масиви.	
13	Л	2	**<u>Тема 6.</u> Робота з масивами.** Об‘ява. Ініціалізація. Індексація. Алгоритм сортування типу «бульбашка». Одновимірні та багатовимірні масиви.	1-8, 9-12
	ЛЗ СР	2 2	**Лабораторне заняття № 6** Робота з масивами. Об‘ява. Ініціалізація. Індексація. Алгоритм сортування типу «бульбашка». Одновимірні та багатовимірні масиви.	
14	Л СР	2 2	**<u>Тема 7.</u> Введення до модульного програмування.** Робота з функціями. Їх призначення. Створення власної функції. Передача аргументів в функцію. Сигнатура функції. Попередня об‘ява функції. Повернення значення з функції. Область видимості змінних. Передача аргументів з значення за замовчуванням. Робота з функціями. Бібліотечні функції. Перевантаження функції. Рекурсивні функції. Генератор псевдовипадкових чисел. Варіативні функції. Розмір типів даних (sizeof).	1-8, 9-12
	ЛЗ	2	**Лабораторне заняття № 7** Введення до модульного програмування. Робота з функціями. Їх призначення. Створення власної функції. Передача аргументів в функцію. Сигнатура функції. Попередня об‘ява функції.	

№ 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)
	СР	2	Повернення значення з функції. Область видимості змінних. Передача аргументів з значення за замовчуванням. Робота з функціями. Бібліотечні функції. Перевантаження функції. Рекурсивні функції. Генератор псевдовипадкових чисел. Варіативні функції. Розмір типів даних (sizeof).	
15	Л	2	**<u>Тема 7.</u> Введення до модульного програмування.** Робота з функціями. Їх призначення. Створення власної функції. Передача аргументів в функцію. Сигнатура функції. Попередня об‘ява функції. Повернення значення з функції. Область видимості змінних. Передача аргументів з значення за замовчуванням. Робота з функціями. Бібліотечні функції. Перевантаження функції. Рекурсивні функції. Генератор псевдовипадкових чисел. Варіативні функції. Розмір типів даних (sizeof).	1-8, 9-12
	СР	2		
	ЛЗ	2	**Лабораторне заняття № 7** Введення до модульного програмування. Робота з функціями. Їх призначення. Створення власної функції. Передача аргументів в функцію. Сигнатура функції. Попередня об‘ява функції. Повернення значення з функції. Область видимості змінних. Передача аргументів з значення за замовчуванням. Робота з функціями. Бібліотечні функції. Перевантаження функції. Рекурсивні функції. Генератор псевдовипадкових чисел. Варіативні функції. Розмір типів даних (sizeof).	
	СР	2		
16	Л	2	**<u>Тема 3.</u> Основа роботи з документацією.** Введення до Блок-схем алгоритмів (БСА). Опис основних дій в програмуванні за допомогою БСА. Опис низькорівневої схеми алгоритмів операторів циклу. Doxygen коментарі. Оформлення лабораторних робіт. Markdown, СТВУЗ ХПІ. Стандарти оформлення коду на мові С.	1-8, 9-12
	СР	2		
	ЛЗ	2	**Лабораторне заняття № 8** Введення до Блок-схем алгоритмів (БСА). Опис основних дій в програмуванні за допомогою БСА. Опис низькорівневої схеми алгоритмів операторів циклу. Doxygen коментарі. Оформлення лабораторних робіт. Markdown, СТВУЗ ХПІ. Стандарти оформлення коду на мові С.	
	СР	2		
Разом (годин)		**120**		

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	Опрацьовування лекційного матеріалу	24
2	Підготовка до лабораторних занять	32
	Разом	**56**

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Не передбачено навчальним планом

МЕТОДИ НАВЧАННЯ

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

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, проєкти, 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
1	2	3	4	5
90-100	A	Відмінно	- **Глибоке знання** навчального матеріалу, що містяться в **основних і додаткових літературних джерелах;** - **вміння аналізувати** явища, які вивчаються, в їхньому взаємозв'язку і розвитку; - **вміння** проводити **теоретичні розрахунки**; - **відповіді** на запитання **чіткі**, **лаконічні, логічно послідовні;** **- вміння вирішувати складні практичні задачі.**	Відповіді на запитання можуть містити **незначні неточності**
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	Д	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**

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
1	2	3	4	5
				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 розвязанні **практичних задач**
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 фундаментальни

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
1	2	3	4	5
				х 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 першого (бакалаврського) рівня вищої освіти, який затверджено наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074 та введено в дію з 2018/2019 навч. року.

2. Робоча програма навчальної дисципліни.

3. Силабус навчальної дисципліни.

4. Персональні навчальні системи кафедри кібербезпеки НТУ "ХПІ": https://iiiii-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	Python 3.10.2 documentation [Електронний ресурс]. – Режим доступу : https://docs.python.org/3/
2	Java Platform Standard Edition 8 Documentation [Електронний ресурс]. – Режим доступу : https://docs.oracle.com/javase/8/docs/
3	Microsoft C++, C, and Assembler documentation [Електронний ресурс]. – Режим доступу : https://docs.microsoft.com/en-us/cpp/?view=msvc-170

Допоміжна література

4	Python Tutorial [Електронний ресурс]. – Режим доступу : https://www.tutorialspoint.com/python/index.htm
5	Java Tutorial [Електронний ресурс]. – Режим доступу : https://www.tutorialspoint.com/java/index.htm
6	C++ Tutorial [Електронний ресурс]. – Режим доступу : https://www.tutorialspoint.com/cplusplus/index.htm

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..69i57j0i512l4j69i61l3.4705j0j7&sourceid=chrome&ie=UTF-8
2. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ”: https://iiiii-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