МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"

Проректор з навчально-методичної роботи

_____

Каріна НЕМАШКАЛО

Технології програмування

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробник:
Міхєєв І.А., к.т.н., доцент кафедри кібербезпеки та інформаційних технологій.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Методологія програмування є фундаментом, на якому будуються конкретні технології програмування до яких відноситься сукупність виробничих процесів, що приводить до створення необхідного програмного забезпечення, а також опис цієї сукупності процесів. В технології програмування акцент робиться саме на процесах розробки програм (технологічних процесах) у порядку їх проходження. Для однієї методології може існувати декілька технологій програмування.

Предметом навчальної дисципліни є основні поняття та методи алгоритмізації та програмування, навики написання та налагодження програм мовою Python, створення структур даних, оволодіння методологією проектування програмних засобів.

Метою навчальної дисципліни є вивчення основних положень мови програмування Python, придбання студентами знань і навиків в області розробки алгоритмів, створення, трансляції та налагодження прикладних програм, застосування бібліотек та модулів Python для створення програмного забезпечення для вирішення задач аналізу та захисту інформаційних систем, що необхідно для професійної підготовки бакалаврів зі спеціальності «Кібербезпека».

Результатами вивчення дисципліни є набуття практичних навичок з розроблення алгоритмів вирішення задач згідно з технічним завданням, коду на мові програмування Python, з визначення структури програмного забезпечення комп'ютерних інформаційних систем, використовуючи інформацію про математичне, технічне, інформаційне забезпечення, проведення тестування програмних модулів в процесі відлагодження програмного забезпечення, визначення ефективності алгоритмів та програм.

Характеристика навчальної дисципліни

Курс	**2**
Семестр	**3, 4**
Кількість кредитів ECTS	**12**
Форма підсумкового контролю	Залік, екзамен

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Основи програмування	**Основи криптографічного захисту**
Розробка та аналіз алгоритмів	**Основи побудови та захисту сучасних операційних систем**
	Основи побудови та захисту мікропроцесорних систем

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. 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. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

метою реалізації встановленої політики інформаційної та/або кібербезпеки. 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.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. 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	
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.) 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–12 розробляти моделі загроз та порушника.
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. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. 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.) 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–16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
КЗ 2. Знання та розуміння предметної області та розуміння професії. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	РН–17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	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.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	РН–27 вирішувати задачі захисту потоків даних в інформаційних,

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	РН–31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. 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. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. 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.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. 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–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 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	РН–37 вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та

	визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	РН–38 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку., КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку., КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих)	РН–49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

систем згідно встановленої політики інформаційної та/або кібербезпеки.	
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку., КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН–52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. 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–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Програма навчальної дисципліни

Змістовий модуль 1. Основи роботи з Python
Тема 1. *Вступ до Python*
Тема 2. *Основи роботи з Python*
Тема 3. *Списки, кортежи та словники*
Тема 4. *Робота із рядками*
Тема 5. *Робота з файлами*
Змістовий модуль 2. Особливості та приклади застосування об'єктно-орієнованого підходу
Тема 6. *Об'єктно-орієнтоване програмування в Python*
Тема 7. *Основні модулі Python*
Тема 8. *Основи роботи з датами та часом*
Змістовий модуль 3. Основи криптографії з Pyhon. Шифри підстановки
Тема 9. *Шифри підстановок*
Тема 10. *Аналіз алгоритму шифрування ROT13*
Тема 11. *Аналіз шифру підстановок*
Змістовий модуль 4. Шифрування та дешифрування даних
Тема 12. *Шифрування та дешифрування за допомогою шифру підстановок*
Тема 13. *Граматичний аналіз шифрів*
Тема 14. *Основи криптоаналізу шифру*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

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 проблемні лекції, презентації, бесіди, індивідуальні та групові міні-проекти.

Викладання дисципліни передбачає залучання пояснювально-ілюстративного, репродуктивного, дослідницького методів, а також методів проблемного навчання. Так під час проведення лекційних занять викладач надає здобувачам певний обсяг теоретичного матеріалу з синтаксису мови програмування Python (Тема 1-14), з наданням пояснень у графічному вигляді (презентації) та за допомогою прикладів програмного коду (Тема 1-14). На лабораторних роботах здобувачі мають змогу отримати практичні навички розробки програмного забезпечення на підставі проблеми, сформульованої за тематикою заняття (Тема 1-14). Вдосконалення практичних навичок відбувається під час виконання індивідуальних завдань та самостійної роботи (Тема 1-14).

Наведені методи навчання спрямовані на формування у здобувачів здатності розробляти програмне забезпечення за різними технологіями та парадигмами програмування.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

- поточний контроль, що здійснюється протягом 3-го семестрі під час проведення лекційних та лабораторних робіт і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що надає студенту поставити залік – 60 балів);
- поточний контроль, що здійснюється протягом 4-му семестрі під час проведення лекційних та лабораторних робіт і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що надає студенту поставити залік – 36 балів);

− підсумковий/семестровий контроль у 4 семестрі, що проводиться у формі екзамену, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і практичних занять проводиться за такими критеріями:

- обробляти дані представляти результати за допомогою розробки процедурних програм;
- вміння аналізувати та використовувати інформаційні ресурси з розробки програмного забезпечення;
- вміння розробити алгоритм для рішення певного завдання;
- знання основ організації середовища розробки програмного забезпечення;
- знання методології та технік з розроблення сучасних програмних рішень;
- знати особливості сучасних мов програмування та сферу їх застосування;
- використовувати технології розробки у середовищі спеціалізованих веб-сервісів;
- знання щодо структур даних, файлових структур та архітектуру комп'ютера;
- вміння використовувати знання щодо розробки нескладних програм;
- вміння застосовувати інструментальні засоби розробки програмного забезпечення.

За дисципліною передбачені такі методи поточного нормативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення слухачами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лабораторні заняття:

3 семестр – максимальна кількість балів становить 100 (виконання та захист лабораторних робіт – 50, контрольні робота – 50), а мінімальна – 60;

4 семестр – максимальна кількість балів становить 60 (виконання та захист лабораторних робіт – 30, контрольні робота – 30), а мінімальна – 36.

Самостійна робота у 3 та 4 семестрах: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями та контрольних робіт за лабораторними роботами дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль у третьому семестрі: проводиться з урахуванням отриманих балів у продовж семестру.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумковий контроль у четвертому семестрі: проводиться з урахуванням іспиту.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни. Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню програмного коду за задачею, виконання його оцінюється 10 балами; третє завдання – відлагодження програмного коду, виконання його оцінюється 10 балами.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Рейтинг-план навчальної дисципліни

3 семестр

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1	***Аудиторна робота***			
	Лекція	Лекція *"Вступ до Python"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №1. *Основи введення/виведення даних*	Захист лабораторної роботи № 1	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Лекція	Лекція *"Основи роботи з Python"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №2. Організація обробки даних	Захист лабораторної роботи № 2	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Списки, кортежи та словники"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №3. *Організація роботи з циклами*	Захист лабораторної роботи № 3	5
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *"Робота зі строками"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 5. *Обробка рядків*	Захист лабораторної роботи № 4	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція "*Робота з файлами"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 5. *Робота з файлами*	Захист лабораторної роботи № 5	5
			Контрольна робота 1	25
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *"Об'єктно-орієнтоване програмування в Python"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №6 Робота з класами та об’єктами	Захист лабораторної роботи № 6	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція "*Основні модулі Python"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота № 7. *Розробка модульної структури*	Захист лабораторної роботи № 7	10
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Основи роботи з датами та часом"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №8. *Робота з датами та часом*	Захист лабораторної роботи № 8	5
			Контрольна робота 1	25
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Залік				

Рейтинг-план навчальної дисципліни

4 семестр

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 9	***Аудиторна робота***			
	Лекція	Лекція "*Шифри підстановок"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 9. Криптографія з Python – зворотний шифр, шифр Цезаряю. Злом шифру	Захист лабораторної роботи № 9	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція *"Аналіз алгоритму шифрування ROT13"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 11. Аналіз алгоритму шифрування ROT13	Захист лабораторної роботи № 10	5
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 11	***Аудиторна робота***			
	Лекція	Лекція "Аналіз шифру підстановок"	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 11. Аналіз шифру підстановок	Захист лабораторної роботи № 11	5
			Контрольна робота 3	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 12	***Аудиторна робота***			
	Лекція	Лекція "Шифрування та дешифрування за допомогою шифру підстановок"	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 12. Шифрування та дешифрування за допомогою шифру підстановок	Захист лабораторної роботи № 12	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 13	***Аудиторна робота***			
	Лекція	Лекція *"Граматичний аналіз шифрів"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота 13. *Граматичний аналіз шифрів*	Захист лабораторної роботи № 13	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 14	***Аудиторна робота***			
	Лекція	Лекція *"Основи криптоаналізу шифру"*	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №14 *Основи криптоаналізу шифру*	Захист лабораторної	5

			роботи № 14	
			Контрольна робота 1	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Екзамен				40

Рекомендована література

Основна

1. Підручник з Python [Електронний ресурс] / Підручник з Python — Python 3.10.6 documentation. – Режим доступу: https://docs.python.org/uk/3.10/tutorial/index.html
2. Креневич А.П. Python у прикладах і задачах. Частина 1. Структурне програмування Навчальний посібник із дисципліни "Інформатика та програмування" – К.: ВПЦ "Київський Університет", 2017. – 206 с.
3. Креневич А.П. Python у прикладах і задачах. Частина 2. Об’єктно-орієнтоване програмування. Навчальний посібник – К.: ВПЦ "Київський Університет", 2020. – 152 с.
4. Висоцька В.А., Оборська О.В. Python: алгоритмізація та програмування: навчальний посібник – Львів: Видавництво «Новий Світ – 2000», 2021. – 514 с.

Додаткова

5. Копей В.Б. Мова програмування Python для інженерів і науковців: Навчальний посібник. Івано-Франківськ : ІФНТУНГ, 2019. 274с.
6. Мокін, Б. І. М 74 Навчальний посібник для опанування студентами способів розв’язання задач з функціонального аналізу мовою Python. Частина 1 / Б. І. Мокін, В. Б. Мокін, О. Б. Мокін. – Вінниця : ВНТУ, 2022. – 124 с.
7. Бріггс Джейсон Р. Python для дітей (веселий вступ до програмування). / перекладачка з англійської Олександра Гордійчук. Львів : Видавництво старого Лева, 2019. 400 с
8. Доля П. Г. Вступ у науковий Python. Харків : ХНУ ім. Каразіна, 2016. 265 с.
9. Задачі з програмування. Мова програмування Python. Навчальний посібник [Електронний ресурс] / [О. В. Обвінцев, А. П. Креневич, Б. П. Довгий та ін.]. – 2022. – Режим доступу до ресурсу: http://matfiz.univ.kiev.ua/userfiles/files/Zadachi_z_programuvannya_3.pdf.
10. Козуб Г.О. Програмування : метод. рек. до лаб. робіт для студ. спец. 121 – „Інженерія програмного забезпечення” / Г. О. Козуб, Н. А. Семенов; Держ. закл. „Луган. нац. ун-т імені Тараса Шевченка”. – Старобільськ : ДЗ „ЛНУ імені Тараса Шевченка”, 2020. – 108 с.

Інформаційні ресурси

11. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Технології програмування" https://pns.hneu.edu.ua.