РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Загальна інформація про навчальну дисципліну

Повна назва навчальної дисципліни	Захист програм та даних
Повна офіційна назва закладу вищої освіти	Сумський державний університет
Повна назва структурного підрозділу	Навчально-науковий інститут бізнесу, економіки та менеджменту. Кафедра економічної кібернетики
Розробник(и)	Кушнерьов Олександр Сергійович
Рівень вищої освіти	Перший рівень вищої освіти, НРК – 6 рівень, QF-LLL – 6 рівень, FQ-EHEA – перший цикл
Тривалість вивчення навчальної дисципліни	один семестр
Обсяг навчальної дисципліни	Обсяг становить 5 кред. ЄКТС, 150 год. Для денної форми навчання 64 год. становить контактна робота з викладачем (24 год. лекцій, 40 год. практичних занять), 86 год. становить самостійна робота. Для заочної форми навчання 20 год. становить контактна робота з викладачем (8 год. лекцій, 12 год. практичних занять), 130 год. становить самостійна робота.
Мова викладання	Українська

2. Місце навчальної дисципліни в освітній програмі

Статус дисципліни	Обов`язкова навчальна дисципліна для освітньої програми "Кіберспорт та розробка комп`ютерних ігор"
Передумови для вивчення дисципліни	Передумови для вивчення відсутні
Додаткові умови	Додаткові умови відсутні
Обмеження	Обмеження відсутні

3. Мета навчальної дисципліни

Сформувати у здобувача вищої освіти знання, уміння та практичні навички, необхідні для проєктування, розробки, підтримки та оцінювання захищених програмних систем, а також ефективного впровадження заходів із безпеки даних у таких системах. Після освоєння курсу здобувач здатен застосовувати сучасні методи та інструменти забезпечення цілісності, конфіденційності й доступності даних у реальних програмно-апаратних середовищах.

4. Зміст навчальної дисципліни

Тема 1 Вступ до інформаційної безпеки та захисту даних

Вивчаються фундаментальні поняття інформаційної безпеки, основи кіберзагроз для програмного забезпечення та даних, класифікація ризиків і пріоритетів захисту. Аналізується роль нормативно-правових актів у сфері цифрової безпеки, визначаються завдання, стратегії та сучасні підходи до побудови систем захисту, акцентується увага на особливостях регулювання захисту інформації в Україні та світі.

Тема 2 Класифікація загроз та уразливостей програмного забезпечення

Розглядаються зовнішні та внутрішні загрози, технічні й організаційні уразливості, приклади найпоширеніших атак на програмне забезпечення. Студенти опановують методи аналізу та класифікації ризиків, вчаться визначати потенційні вразливості у складних програмних продуктах та застосування стандартів і інструментів оцінки безпеки.

Тема 3 Методи та алгоритми шифрування даних

Тема охоплює основи симетричних та асиметричних алгоритмів шифрування, принципи створення криптографічних систем для передачі й зберігання даних. Студенти вивчають сучасні шифрувальні алгоритми, методи захисту від криптоаналізу, функціонування криптографічних протоколів та їх застосування у різних програмних та апаратних середовищах.

Тема 4 Аутентифікація та авторизація в програмних системах

Висвітлюються принципи аутентифікації та авторизації користувачів, протоколи перевірки ідентичності, технології безпечного управління доступом до даних, впровадження багатофакторної аутентифікації. Вивчаються новітні системи контролю і протидії несанкціонованому доступу, а також формування політик надійної і безпечної роботи користувачів.

Тема 5 Безпека веб-застосунків

Аналізуються типові вразливості веб-додатків (SQL injection, XSS, CSRF), розглядаються механізми захисту проти атак, рекомендації щодо безпечної розробки і тестування, принципи застосування стандартів OWASP. Студенти опановують практики керування ризиками під час розробки і супроводу веб-сервісів.

Тема 6 Резервне копіювання та відновлення даних

Вивчаються принципи побудови ефективної системи резервного копіювання, методи збереження цілісності й доступності даних, підготовка планів дій у разі катастрофи чи інциденту, сучасні технології та засоби автоматизації процесу відновлення, практики вибору типу копій для корпоративних і приватних середовищ.

Тема 7 Захист програмного коду та обфускація

Опанування технологій захисту коду від аналізу, реверс-інжинірингу та несанкціонованого використання, ознайомлення із сучасними методами обфускації, мініфікації, криптографічного підпису. Вивчаються реальні інструменти захисту комерційних програмних продуктів та засоби відкритого програмного забезпечення, принципи побудови стійких захисних систем для коду.

Тема 8 Захист даних у хмарних та мобільних середовищах Тема присвячена практикам захисту інформації у хмарних інфраструктурах, особливостям апаратно-програмної безпеки мобільних пристроїв. Аналізуються актуальні загрози, використовуються стандарти безпеки для SaaS/PaaS/IaaS-рішень, методи та засоби захисту даних для Android/iOS, порівнюються технології шифрування, багатофакторної аутентифікації та захисту каналів зв'язку.
Тема 9 Аудит інформаційної безпеки Вивчаються принципи організації аудиту безпеки, процедура планування та проведення аудиту у програмних й апаратних системах. Студенти оволодівають техніками ідентифікації вразливостей, підготовки аудиторської документації, розробки рекомендацій щодо усунення ризиків, зачіпають міжнародні стандарти ефективного аудиту.
Тема 10 Захист даних у корпоративних мережах і системах Охоплюються сучасні механізми захисту корпоративних мереж: мережеве сегментування, моніторинг та реагування на інциденти, принципи впровадження політик безпеки для підприємств, методи контролю доступу і управління подіями безпеки, актуальні питання застосування SIEM/SOAR систем.
Тема 11 Безпека при розробці програмного забезпечення (SDLC) Студенти оволодівають методиками інтеграції безпеки у всі стадії життєвого циклу (SDLC) створення програм, моделювання загроз, автоматизованого контролю/перевірки коду, засобів безпечного програмування. Вивчаються сучасні інструменти розробки і системи безперервного тестування, принципи DevSecOps.
Тема 12 Соціальна інженерія та захист від неї Ознайомлення з основними способами соціальної інженерії, аналіз прикладів атак через психологічний вплив. Вивчаються стратегії протидії, практики підвищення захищеності користувачів та компаній, формування політик інформаційної стійкості, тренування із кіберкультури та запобігання інцидентам у реальних й віртуальних середовищах.

5. Очікувані результати навчання навчальної дисципліни

Після успішного вивчення навчальної дисципліни здобувач вищої освіти зможе:

РН1	Надавати вичерпне пояснення основних концепцій та принципів інформаційної безпеки програмного забезпечення та даних, розуміти ключові загрози та методи їх усунення.
РН2	Визначати та застосовувати відповідні технології обробки, зберігання та передачі даних з урахуванням вимог інформаційної безпеки, забезпечувати їх цілісність та конфіденційність.
РН3	Використовувати методи верифікації та валідації програмного забезпечення для забезпечення його надійності та безпеки, відповідно до сучасних стандартів і найкращих практик.

6. Роль навчальної дисципліни у досягненні програмних результатів

Програмні результати навчання, досягнення яких забезпечує навчальна дисципліна.
Для спеціальності 121 Інженерія програмного забезпечення:

ПР7	Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення.
ПР13	Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань.
ПР18	Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.
ПР21	Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

7. Роль навчальної дисципліни у досягненні програмних компетентностей

Програмні компетентності, формування яких забезпечує навчальна дисципліна:
Для спеціальності 121 Інженерія програмного забезпечення:

ПК1	ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.
ПК2	ЗК02. Здатність застосовувати знання у практичних ситуаціях.
ПК3	ЗК06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ПК4	ЗК07. Здатність працювати в команді.
ПК5	ЗК08. Здатність діяти на основі етичних міркувань.
ПК6	ЗК10. Здатність діяти соціально відповідально та свідомо.
ПК7	ФК1. Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.
ПК8	ФК6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (у тому числі кібербезпеки).
ПК9	ФК14. Здатність до алгоритмічного та логічного мислення.

8. Види навчальних занять

Тема 1. Вступ до інформаційної безпеки та захисту даних
Лк1 "Вступ до інформаційної безпеки та захисту даних" Ця лекція знайомить студентів із базовими поняттями інформаційної безпеки, типами загроз для програмного забезпечення та даних, а також ключовими концепціями захисту інформації у сучасному цифровому середовищі. Розглядаються приклади реальних інцидентів порушення безпеки, методи аналізу ризиків, основні завдання захисту даних. Окрему увагу приділено нормативно-правовим актам та міжнародним стандартам у галузі кібербезпеки, що регламентують діяльність IT-фахівця під час роботи з чутливою інформацією.

Пр1 "Аналіз нормативно-правових актів у галузі інформаційної безпеки"

Заняття присвячене системному огляду та аналізу основних нормативних документів, які визначають вимоги до захисту даних в Україні та світі. Студенти знайомляться із законами, стандартами ISO/IEC, внутрішніми політиками організацій, механізмами впровадження процедур і аудиту відповідності. Практикується критичний аналіз типових ситуацій та кейсів, здійснюється порівняння міжнародних і національних підходів до організації безпеки.

Тема 2. Класифікація загроз та уразливостей програмного забезпечення

Лк2 "Класифікація загроз та уразливостей програмного забезпечення"

Лекція охоплює типи загроз, такі як зовнішні, внутрішні, технічні, організаційні — для програмного забезпечення. Студенти опановують основи класифікації, аналізують механізми атаки та можливості впливу на систему. Вивчаються сучасні уразливості, їх типові прояви, моделі виявлення, методи оцінки критичності. Акцент на формуванні навичок системного аналізу безпеки та прогнозування нових ризиків.

Пр2 "Виявлення уразливостей у програмному забезпеченні"

Практичне заняття орієнтовано на застосування спеціалізованих інструментів для сканування уразливостей (наприклад, Nessus, OpenVAS, Burp Suite), роботу з результатами сканування, аналіз виявлених проблем і рекомендації щодо їх усунення. Студенти навчаються працювати зі звітами, розвивають навички аудиту та оцінки ризиків для реальних проєктів у сфері програмного забезпечення.

Тема 3. Методи та алгоритми шифрування даних

Лк3 "Методи та алгоритми шифрування даних"

Лекція поглиблено розкриває основи сучасної криптографії, порівнює симетричні (AES, DES) та асиметричні (RSA, ECC) алгоритми шифрування. Вивчаються принципи забезпечення конфіденційності, цілісності та автентичності даних при передачі та зберіганні. Дається огляд криптографічних протоколів, їх впровадження у різних типах програмних систем та реальних додатків.

Пр3 "Реалізація симетричних алгоритмів шифрування"

Студенти розробляють прості програми для шифрування/дешифрування даних на основі алгоритму AES, аналізують ефективність алгоритму та його стійкість до атак. У рамках практики реалізується тестування, порівнюється швидкодія, надійність та масштабується застосування у різних середовищах роботи з даними.

Тема 4. Аутентифікація та авторизація в програмних системах

Лк4 "Аутентифікація та авторизація в програмних системах" (денна)

Лекція розкриває основи організації систем ідентифікації та управління доступом, розглядає структуру механізмів аутентифікації (паролі, токени, біометрія, багатофакторні підходи). Вивчаються питання побудови політик доступу, захисту від атак типу вгадування, replay, соціальної інженерії. Окремо аналізуються сучасні протоколи: OAuth, Kerberos, SAML.

Пр4 "Налаштування та використання засобів аутентифікації" (денна) Студенти налаштовують та інтегрують програми для здійснення однокрокової чи багатофакторної аутентифікації користувачів, тестують стійкість системи до різних типів атак, налаштовують політики паролів, вчаться інтегрувати методи авторизації (RBAC, ABAC) у прикладних системах.
Тема 5. Безпека веб-застосунків
Лк5 "Безпека веб-застосунків" (денна) Охоплює вивчення типових вразливостей веб-застосунків (SQL injection, XSS, CSRF та інші), аналізу методів їх виявлення і нейтралізації. Акцент на принципах безпечної розробки, розгортанню захисних механізмів, стандартам OWASP Top 10, впровадженню сучасних практик тестування, аудитах і тактиках швидкої реагування.
Пр6 "Захист від SQL ін'єкцій" (денна) Студенти проводять тестування веб-застосунків на уразливість до SQL injection за допомогою фреймворків і утиліт, вивчають типові патерни атак і методи захисту — підготовлені запити, фільтрація вводу, аудит коду. Практичні кейси дозволяють оцінити ефективність захисту і рекомендації для покращення стійкості системи.
Пр6 "Впровадження захисту від XSS атак" (денна) Практика з аналізу ризиків XSS — міжсайтового скриптингу. Студенти ідентифікують уразливі точки у коді, впроваджують заходи (escaping, контекстна фільтрація, CSP), тестують робочі сценарії для захисту. Оцінка результатів дозволяє запропонувати оптимальні підходи для реальних проєктів веб-розробки.
Пр7 "Проведення пентесту програмного забезпечення" (денна) Практичне заняття присвячено комплексному тестуванню програмного забезпечення на проникнення із використанням сучасних інструментів (Nmap, Nessus, Metasploit, Burp Suite, Kali Linux). Студенти моделюють реальні атаки, збирають інформацію про цільову систему, виконують сканування портів, виявляють уразливості, застосовують експлойти для демонстрації ризиків. Відпрацьовуються етапи пентесту: розвідка, сканування, експлуатація, аналіз результатів, підготовка звіту та розробка рекомендацій щодо усунення вразливостей.
Пр8 "Використання автоматичних інструментів аналізу безпеки" (денна) Заняття фокусує увагу на застосуванні автоматизованих сканерів безпеки для перевірки вихідного коду, веб-застосунків і систем. Студенти працюють із інструментами SonarQube, Nessus, OpenVAS, Burp Suite; налаштовують завдання сканування, аналізують результати, визначають критичність знайдених уразливостей. Вивчаються алгоритми статичного та динамічного аналізу, принципи автоматизації і інтеграції засобів безпеки у CI/CD-процеси командного проекту.
Тема 6. Резервне копіювання та відновлення даних

Лк6 "Резервне копіювання та відновлення даних" (денна)

Лекція присвячена принципам організації резервного копіювання в різних програмно-апаратних середовищах. Студенти знайомляться з видами бекапів — повний, диференційований, інкрементальний, стратегіями тестування процедур відновлення. Розглядаються питання вибору сховищ (локальних та хмарних), створення робочого плану реагування на катастрофи, дотримання вимог доступності й цілісності даних.

Пр9 "Розробка плану резервного копіювання" (денна)

Практикум передбачає розробку плану резервного копіювання для реального програмного чи корпоративного середовища: вибір типу копій, налаштування розкладу, тестування процесу відновлення після збою. Студенти аналізують типові помилки, проводять оцінювання ефективності декількох стратегій, документують план для впровадження у хмарній чи локальній інфраструктурі.

Пр10 "Реагування на інциденти інформаційної безпеки" (денна)

Комплексне практичне заняття, яке охоплює розробку, впровадження і тестування плану реагування на інциденти кібербезпеки, аналіз кейсів порушення захисту. Студенти моделюють інциденти, виконують збір артефактів, фіксують сценарії реагування, розробляють коригувальні заходи (patch management, ізоляція, відновлення), готують внутрішні звіти для IT-команди компанії.

Тема 7. Захист програмного коду та обфускація

Лк7 "Захист програмного коду та обфускація" (денна)

Лекція знайомить із найбільш ефективними підходами захисту вихідного коду — реверс-інжиніринг, обфускація, криптографічний підпис, використання ліцензування. Розглядаються засоби обфускації для різних мов (Dotfuscator, ProGuard), їх переваги й недоліки, кейси реального захисту комерційних і open-source програмних продуктів, стандарти безпеки коду.

Пр11 "Реалізація обфускації коду" (денна)

Практична робота зі застосування сучасних засобів обфускації: студенти порівнюють функціонал популярних інструментів (Dotfuscator, ProGuard), тестують захищеність та декомпіляцію різних варіантів коду, аналізують результати і розробляють рекомендації щодо впровадження обфускації у своїх проєктах.

Пр12 "Проведення стрес-тестування програмного забезпечення" (денна)

Студенти моделюють навантаження й атаки, тестують стійкість програм при пікових навантаженнях, працюють з інструментами JMeter, Locust, розширюють функціонал тестів. Аналізується поведінка додатків при обмежених ресурсах, впроваджуються сценарії аномальних вхідних даних, результати використовуються для покращення надійності та стійкості продукту.

Тема 8. Захист даних у хмарних та мобільних середовищах

Лк8 "Захист даних у хмарних та мобільних середовищах" (денна)

Лекція структурно висвітлює сучасні методи та засоби забезпечення безпеки у хмарних сховищах (AWS, Azure, Google Cloud), особливості організації захисту мобільних застосунків, політики шифрування й автентифікації. Надаються стандарти хмарної безпеки, аналізуються кейси критичних інцидентів, практичні стратегії розгортання захисту у мобільних серверних та клієнтських середовищах.

Пр13 "Забезпечення безпеки на мобільних пристроях" (денна)

Практичне заняття орієнтовано на аналіз мобільних додатків на предмет типових загроз (вразливості Android/iOS), впровадження інструментів шифрування, аутентифікації й захисту каналів передачі. Студенти розробляють політики безпеки, здійснюють аудит застосунків, готують рекомендації для адміністраторів і кінцевих користувачів, тестують API та сценарії безпеки для мобільних систем.

Пр14 "Інтеграція засобів захисту у розробку ПЗ"

Практичне заняття охоплює впровадження бібліотек і API для захисту програм під час розробки: інтеграція засобів аналізу коду (SAST/DAST), налаштування криптографічних функцій, моніторинг активності, контроль доступу та журналювання подій. Студенти опановують принципи DevSecOps — автоматизацію перевірок безпеки на різних етапах CI/CD, налаштовують тестування коду, моделюють інтеграцію RASP для активного захисту застосунків. Окрему увагу приділено вибору ефективних засобів і оптимізації процесу безпечної розробки.

Тема 9. Аудит інформаційної безпеки

Лк9 "Аудит інформаційної безпеки" (денна)

Лекція розкриває мету й принципи аудиту ІБ, міжнародні й вітчизняні стандарти (ISO/IEC 27001, NIST, GDPR). Вивчаються класичні та сучасні процедури, етапи підготовки аудиту системи захисту програм та даних, принципи складання чек-листів, кейси з виявлення невідповідностей, типи аудиторських звітів і механізми розробки рекомендацій для підвищення безпеки IT-систем, продуктів та організацій.

Пр15 "Проведення аудиту безпеки програмного забезпечення" (денна)

Студенти проєктують і виконують аудит конкретного ПЗ чи IT-сервісу: формують план аудиту, обирають критерії, аналізують код та архітектуру, оцінюють відповідність стандартам. Працюють із документуванням виявлених ризиків і невідповідностей, розробляють рекомендації щодо підвищення захищеності, оцінюють виконання рекомендацій. Практика включає підготовку та захист аудиторського звіту.

Тема 10. Захист даних у корпоративних мережах і системах

Лк10 "Захист даних у корпоративних мережах і системах"

Лекція охоплює сучасні механізми захисту даних: сегментування корпоративної мережі, потоковий моніторинг подій, впровадження SIEM/IDS/IPS систем. Аналізуються методи контролю доступу, реагування на інциденти, політики безпеки для корпоративного ПЗ, розглядаються принципи впровадження засобів контролю і забезпечення комплексної безпеки мережевих і серверних середовищ.

Пр16 "Впровадження засобів моніторингу та контролю доступу"

Студенти налаштовують і тестують роботу SIEM-систем, засобів моніторингу, IDS/IPS, впроваджують політики управління доступом (ACL, RBAC), здійснюють аудит і оцінювання стану корпоративної безпеки. Демонструється взаємодія з реальними корпоративними мережами, аналізуються типові атаки та сценарії реагування.

Пр17 "Розробка політик інформаційної безпеки" (денна)

Практичне заняття з розробки внутрішніх політик і регламентів для управління інформаційною безпекою: студенти створюють шаблони документації для організацій/ПЗ, визначають структуру політик, описують механізми реагування та управління ризиками, інтегрують стандарти захисту для відповідності галузевим вимогам.

Тема 11. Безпека при розробці програмного забезпечення (SDLC)

Лк11 "Безпека при розробці програмного забезпечення (SDLC)" (денна)

Лекція присвячена вбудованій безпеці у SDLC: принципи безпечного програмування, інтеграція контролю коду, моделювання загроз, автоматизоване сканування та тестування на всіх етапах розробки. Вивчаються сучасні практики DevSecOps, SSDLC, засоби та підходи до організації процесу захисту ПЗ, забезпечення відповідності міжнародним стандартам, підготовка до комплексного аудиту.

Пр18 "Впровадження безпечного SDLC" (денна)

Студенти виконують проєкти із використанням безпечних підходів у життєвому циклі розробки: моделюють загрози, аналізують ризики, інтегрують SAST/DAST у CI/CD пайплайн, розробляють сценарії захисту і моніторингу. Оцінюється ефективність впроваджених заходів, формуються рекомендації для підвищення стійкості проекту.

Пр19 "Оцінка і управління ризиками для програмного забезпечення" (денна)

Практика із застосування моделей оцінки ризиків: студенти виконують ідентифікацію й якісну/кількісну оцінку ризиків для своїх проектів, використовують стандарти (ISO 31000, OCTAVE), розробляють стратегії управління, документують ризики, формують плани запобігання та реагування.

Тема 12. Соціальна інженерія та захист від неї

Лк12 "Соціальна інженерія та протидія їй" (денна)

Лекція розкриває сутність соціальної інженерії: методи впливу на користувачів для отримання доступу до ПЗ і даних, класифікацію атак (фішинг, вішинг, бейтинг), кейси успішних атак. Описуються сучасні стратегії протидії психологічному впливу, формування кіберкультури, механізми навчання й самозахисту у корпоративних і персональних середовищах.

Пр20 "Моделювання атак соціальної інженерії"

Практичне заняття передбачає імітацію різних атак (фішинг, спершу, телефонні пошуки тощо), аналіз захисних реакцій користувачів, розробку навчальних матеріалів та тренінгів із протидії соціальній інженерії для підвищення стійкості організації. Студенти опрацьовують засоби тестування сценаріїв та розробляють політики інформування персоналу про загрози соціальної інженерії.

9. Стратегія викладання та навчання

9.1 Методи викладання та навчання

Дисципліна передбачає навчання через:

МН1	Лекційне навчання
МН2	Практикоорієнтоване навчання

Лекції надають студентам матеріали з основ захисту програмного забезпечення та даних, включаючи основні загрози, методи їх усунення, та сучасні технології інформаційної безпеки. Лекції забезпечують теоретичну базу, яка є основою для самостійного навчання здобувачів вищої освіти. Лекції доповнюються практичними заняттями, що дозволяють студентам застосовувати отримані теоретичні знання на реальних прикладах. Зміст практичних робіт спрямований на практико-орієнтоване навчання, яке передбачає проведення аналізу уразливостей програмного забезпечення, впровадження заходів захисту даних та перевірку ефективності цих заходів.

9.2 Види навчальної діяльності

НД1	Самостійна виконання та підготовка до захисту практичних робіт
НД2	Захист практичних робіт
НД3	Підготовка та виконання індивідуального завдання

10. Методи та критерії оцінювання

10.1. Критерії оцінювання

Визначення	Чотирибальна національна шкала оцінювання	Рейтингова бальна шкала оцінювання
Відмінне виконання лише з незначною кількістю помилок	5 (відмінно)	$90 \leq RD \leq 100$
Вище середнього рівня з кількома помилками	4 (добре)	$82 \leq RD < 89$
Загалом правильна робота з певною кількістю помилок	4 (добре)	$74 \leq RD < 81$
Непогано, але зі значною кількістю недоліків	3 (задовільно)	$64 \leq RD < 73$
Виконання задовольняє мінімальним критеріям	3 (задовільно)	$60 \leq RD < 63$
Можливе повторне складання	2 (незадовільно)	$21 \leq RD < 59$
Можливе одноразове повторне складання	2 (незадовільно)	$0 \leq RD < 20$

10.2 Методи поточного формативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**

МФО1 Настанови викладача в процесі виконання практичних завдань	Пояснення в процесі виконання практичних завдань	16	Під час практичних занять
МФО2 Виконання роботи у визначений термін (soft skills)	Виконання завдань практичної роботи згідно з графіком виконання	16	Платфора MIX
МФО3 Надання зворотного зв'язку про результати перевірки виконання індивідуальних завдань здобувачем	Інформування про результати перевірки виконання практичних завдань	16	Результати перевірки практичних завдань

10.3 Методи підсумкового сумативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**
МСО1 Виконання практичних робіт	Виконання роботи відбувається студентом самостійно піля отримання завдання від лектора	1 - 16	Viber, mix.sumdu.edu.ua
МСО2 Звіт за результатами виконання практичних робіт	Виконання роботи відбувається студентом самостійно піля отримання завдання від лектора	1 - 16	Viber, mix.sumdu.edu.ua
МСО3 Захист індивідуального завдання	Виконання роботи відбувається студентом самостійно піля отримання завдання від лектора	15	Viber, mix.sumdu.edu.ua
МСО4 Складання комплексного письмового модульного контролю	Виконання роботи відбувається студентом самостійно піля отримання завдання від лектора	16	Viber, mix.sumdu.edu.ua

Контрольні заходи:

		Максимальна кількість балів	Можливість перескладання з метою підвищення оцінки
Перший семестр вивчення		**100 балів**	
МСО1. Виконання практичних робіт		**60**	
	10х6	60	Так
МСО2. Звіт за результатами виконання практичних робіт		**20**	
	10х2	20	Так
МСО3. Захист індивідуального завдання		**5**	
		5	Так
МСО4. Складання комплексного письмового модульного контролю		**15**	
		15	Ні

Дисципліна передбачає такі методи узагальнюючої підсумкової оцінки, як захист практичних робіт, перевірка та оцінка індивідуальної роботи. Форма підсумкового контролю - диференційований залік. Загальну позитивну оцінку дисципліни можна отримати, якщо за завдання набрано щонайменше 60% балів.

11. Ресурсне забезпечення навчальної дисципліни

11.1 Засоби навчання

ЗН1	Комп’ютери, комп’ютерні системи та мережи
ЗН2	Oracle VM VirtualBox

11.2 Інформаційне та навчально-методичне забезпечення

Основна література	
1	Кушнерьов, О. С. Безпека інформації [Електронний ресурс] : конспект лекцій / О. С. Кушнерьов. — Суми : СумДУ, 2021. — 99 с.
2	Інформаційно-аналітична система оцінювання відповідності сучасним вимогам навчального контенту спеціальності кібербезпека [Електронний ресурс] / А. С. Довбиш, І. В. Шелехов, Ю. О. Хібовська, О. В. Матяш // Радіоелектронні і комп'ютерні системи. — 2021. — № 1. — С. 70-80.
3	Інформаційна безпека : підручник / [В. В. Остроухов, М. М. Присяжнюк та ін.] — Київ : Ліра К, 2021. — 412 с.
Допоміжна література	

1	Операційні системи [Електронний ресурс] : навч. посіб. / І. М. Федотова-Півень, І. В. Миронець, О. Б. Півень та ін. ; за ред. В. М. Рудницького. — Харків : ДІСА ПЛЮС, 2019. — 216 с.
2	Cybersecurity and innovative digital educational environment [Електронний ресурс] = Кібербезпека та інноваційне цифрове освітнє середовище / O. Burov, O. Butnik-Siversky, O. Orliuk, K. Horska // Інформаційні технології і засоби навчання. — 2020. — Вип. 6 (80). — С. 414-430.
3	Основи кіберпростору, кібербезпеки та кіберзахисту : навчальний посібник / [Богуш В.М., Богуш В.В., Бровко В.Д., та ін.] — Київ : Ліра К, 2021. — 554 с.
Інформаційні ресурси в Інтернеті	
1	Oracle VM VirtualBox [Електронний ресурс]. - Режим доступу: https://www.virtualbox.org/wiki/Documentation
2	Офіційному сайті Кіберполіції україни [Електронний ресурс]. – Режим доступу: https://cyberpolice.gov.ua/
3	Офіційному сайті Урядової команди реагування на комп’ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв’язку та захисту інформації України [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п	Програма навчальної дисципліни	Усього годин	Навчальна робота, аудиторних годин				Самостійна робота здобувача вищої освіти за видами, годин					
			Усього, ауд. год.	Лекції	Практичні заняття	Лабораторні роботи	Усього, год.	Самостійне опрацювання матеріалу	Підготовка до практичних занять	Підготовка до лабораторних робіт	Підготовка до контрольних заходів	Виконання самостійних позааудиторних завдань
1	2	3	4	5	6	7	8	9	10	11	12	13
денна форма навчання												
1	Вступ до інформаційної безпеки та захисту даних	5	4	2	2	0	1	0.5	0.5	0	0	0
2	Класифікація загроз та уразливостей програмного забезпечення	5	4	2	2	0	1	0.5	0.5	0	0	0
3	Методи та алгоритми шифрування даних	5	4	2	2	0	1	0.5	0.5	0	0	0
4	Аутентифікація та авторизація в програмних системах	5	4	2	2	0	1	0.5	0.5	0	0	0
5	Безпека веб-застосунків	12.5	10	2	8	0	2.5	0.5	2	0	0	0
6	Резервне копіювання та відновлення даних	7.5	6	2	4	0	1.5	0.5	1	0	0	0
7	Захист програмного коду та обфускація	7.5	6	2	4	0	1.5	0.5	1	0	0	0
8	Захист даних у хмарних та мобільних середовищах	7.5	6	2	4	0	1.5	0.5	1	0	0	0
9	Аудит інформаційної безпеки	5	4	2	2	0	1	0.5	0.5	0	0	0
10	Захист даних у корпоративних мережах і системах	7.5	6	2	4	0	1.5	0.5	1	0	0	0
11	Безпека при розробці програмного забезпечення (SDLC)	7.5	6	2	4	0	1.5	0.5	1	0	0	0
12	Соціальна інженерія та захист від неї	5	4	2	2	0	1	0.5	0.5	0	0	0
Контрольні заходи												
1	диференційний залік	6	0	0	0	0	6	0	0	0	6	0
Індивідуальні завдання												

1	2	3	4	5	6	7	8	9	10	11	12	13
1	інші індивідуальні завдання	64	0	0	0	0	64	0	0	0	0	64
Всього з навчальної дисципліни (денна форма навчання)		*150*	*64*	*24*	*40*	*0*	*86*	*6*	*10*	*0*	*6*	*64*

№ з/п	Програма навчальної дисципліни	Усього годин	Навчальна робота, аудиторних годин				Самостійна робота здобувача вищої освіти за видами, годин					
			Усього, ауд. год.	Лекції	Практичні заняття	Лабораторні роботи	Усього, год.	Самостійне опрацювання матеріалу	Підготовка до практичних занять	Підготовка до лабораторних робіт	Підготовка до контрольних заходів	Виконання самостійних позааудиторних завдань
1	2	3	4	5	6	7	8	9	10	11	12	13
заочна форма навчання												
1	Вступ до інформаційної безпеки та захисту даних	5	4	2	2	0	1	0.5	0.5	0	0	0
2	Класифікація загроз та уразливостей програмного забезпечення	5	4	2	2	0	1	0.5	0.5	0	0	0
3	Методи та алгоритми шифрування даних	5	4	2	2	0	1	0.5	0.5	0	0	0
4	Аутентифікація та авторизація в програмних системах	5	0	0	0	0	5	5	0	0	0	0
5	Безпека веб-застосунків	12.5	0	0	0	0	12.5	12.5	0	0	0	0
6	Резервне копіювання та відновлення даних	7.5	0	0	0	0	7.5	7.5	0	0	0	0
7	Захист програмного коду та обфускація	7.5	0	0	0	0	7.5	7.5	0	0	0	0
8	Захист даних у хмарних та мобільних середовищах	7.5	2	0	2	0	5.5	5	0.5	0	0	0
9	Аудит інформаційної безпеки	5	0	0	0	0	5	5	0	0	0	0
10	Захист даних у корпоративних мережах і системах	7.5	4	2	2	0	3.5	3	0.5	0	0	0
11	Безпека при розробці програмного забезпечення (SDLC)	7.5	0	0	0	0	7.5	7.5	0	0	0	0
12	Соціальна інженерія та захист від неї	5	2	0	2	0	3	2.5	0.5	0	0	0
Контрольні заходи												
1	диференційний залік	6	0	0	0	0	6	0	0	0	6	0
Індивідуальні завдання												

1	2	3	4	5	6	7	8	9	10	11	12	13
1	інші індивідуальні завдання	64	0	0	0	0	64	0	0	0	0	64
Всього з навчальної дисципліни (заочна форма навчання)		*150*	*20*	*8*	*12*	*0*	*130*	*57*	*3*	*0*	*6*	*64*