Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ПРИКЛАДНІ АСПЕКТИ ПРОГРАМУВАННЯ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ»

для студентів

спеціальності 125 Кібербезпека
освітнього рівня першого (бакалаврського)
освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0239/23
(підпис) (прізвище, ініціали)
«___» _____ 2023 р.

Розробник:

ТаджДіні Махіяр, старший викладач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

ТаджДіні Махіяр, старший викладач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми _____ Артем ПЛАТОНЕНКО
(підпис)

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ Євген ІВАНІЧЕНКО
(підпис)

Пролонговано:

на 2023/2024 н.р. _____ Благодарний В.І., «23» 08 2023 р., протокол № 8
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська / англійська	
Загальний обсяг кредитів / годин	5 / 150	
Курс	4	
Семестр	7	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	30	
Самостійна робота	56	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Прикладні аспекти програмування в системах ІКБ» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Прикладні аспекти програмування в системах ІКБ» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Прикладні аспекти програмування в системах ІКБ» складається з трьох змістових модулів: «Поняття безпеки та безпровідних технологій, їх аналіз», «Дизайн безпеки, огляд дизайну безпеки, його процес та оцінка», «Реалізація безпечного програмування». Обсяг дисципліни – 150 год. (5 кредитів).

Метою викладання навчальної дисципліни «Прикладні аспекти програмування в системах ІКБ» є формування у студентів уміння вирішувати задачі адміністрування безпровідних і мобільних мереж і систем, застосовувати нормативно-правові, організаційні та технічні процедури при роботі бездротових і мобільних технологій.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері бездротових і мобільних технологій, інформаційної та кібернетичної безпеки та набуття **наступних компетентностей**:

Фахові компетентності

КФ-3 — здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ-5 — здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації**.**

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен
знати:

- коди загроз;
- безпечний розвиток найкращий практик;
- концепцію безпечного програмування.

уміти:

- аспекти безпечного програмування та кодів;
- тестування та віднаходження слабкі місця безпеки у кодах;
- планування мітігешену;
- дизайн безпечного застосунку.

та досягти наступних **програмних результатів навчання:**

ПРз-8 — вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки; забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.

ПРз-9 — володіти практичними навичками проведення аудиту безпеки ІКС, їх адміністрування та експлуатації; вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Поняття безпеки та безпровідних технологій, їх аналіз							
Тема 1. Розуміння безпеки: компетентності та недосконалості, надійність та конфіденційність.	4	2		2			2
Тема 2. Загрози: моделі загроз, атаки, пом'якшення загроз.	7				2		3
Тема 3. Мітігейшн: структурні стратегії пом'якшення загроз, мінімізація можливостей атак, політика та контроль доступу.	10	2		2	2		5
Тема 4. Паттерни: атрибути дизайну, збій в роботі, глибинний захист інформації.	9				2		5
Тема 5. Криптографія: інструменти криптографії інформації, псевдовипадкові числа, коди автентифікації повідомлень.	8			2	2		5
Модульний контроль	2						
Разом	40	4		6	8		20
Змістовий модуль 2. Дизайн безпеки, огляд дизайну безпеки, його процес та оцінка							

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Тема 4. Безпека дизайну: інтеграція безпеки в дизайн, визначення сфери застосування, встановлення вимог безпеки, моделювання загроз, проектування обробки даних.	12	1		2	2		7
Тема 5.Огляд дизайну безпеки: коли його проводити, документація, процес, оцінювання, 4 питання керівництва, огляди конфіденційності.	10	1		2	2		5
Модульний контроль	2						
Разом	24	2		4	4		12
Змістовий модуль 3. Реалізація безпечного програмування							
Тема 6. Безпечне програмування: ланцюги уразливостей, помилки та ентропія, уразливість кодування.	10	2		2	2		4
Тема 7. Помилки кодування низького рівня: арифметичні уразливості, уразливості точності з плавучою точкою, доступ до пам’яті, переповнення буфера.	9	1		2	2		4
Тема 8. Недовірений вхід: уразливості та проблеми входу.	10	1		2	2		5
Тема 9. Тестування безпеки: функціональне тестування, GotoFail, XXS, Fuzz Testing, тести регресії безпеки.	13	1		2	4		6
Тема 10. Практичні навички безпечного доступу: обробка винятків помилок, якість коду, кодекс гігієни, вибір безпечних компонентів, сортування уразливостей.	10	1		2	2		5
Модульний контроль	4						
Разом	56	6		10	12		24
Підготовка та проходження контрольних заходів	30						
Усього	150	12		20	24		56

5. Програма навчальної дисципліни

Змістовий модуль 1. Поняття безпеки та безпровідних технологій, їх аналіз

Основні питання:

- Розуміння безпеки та довіри, компетентності та недосконалості, прийняття рішення довіри, неявно довірені компоненти, надійність, C-I-A в інформаційній безпеці, золотий стандарт та конфіденційність.
- Загрози, змагальна перспектива, чотири основні питання, моделювання загроз, розробка з точки зору моделі, визначення активів, просторів атак, межі довіри та загроз, пом’якшення загроз, конфіденційність та моделювання загроз.

● Мітігейшн загроз: звернення до загроз, структурні стратегії пом’якшення та мінімізація можливостей атаки, вузькі вікна вразливості, мінімізація доступу до даних, політика та контроль доступу до даних, інтерфейси, спілкування та зберігання даних.
● Паттерни: атрибути, економіка та прозорість дизайну, мінімізація експозиції, мінімум привілеїв та інформації, безпека за замовчуванням, дозволені списки над списками блокування, уникнення передбачуваності, збій безпеки, повна медіація, найменш поширений механізм, глибинний захист, поділ привілеїв, небажання довіряти та прийнятна відповідальність за безпеку, анти-паттерни, сторонні компоненти та компоненти, які не підлягають виправленню.
● Криптографія: криптографічні інструменти, випадкові числа, псевдовипадкові числа, коди автентифікації повідомлень, використання MACів для запобігання фальсифікації, повторні атаки, безпечний зв’язок MAC, симетричне/асиметричне цифрування, використання симетричної криптографії, криптосистема RSA, цифрові підписи та сертифікати, обмін ключами, використання Crypto.

Змістовий модуль 2. Дизайн безпеки, огляд дизайну безпеки, його процес та оцінка
Основні питання:
● Введення в безпечний дизайн, інтеграція безпеки в дизайні, визначення сфери застосування, встановлення вимог безпеки, моделювання загроз.
● Архітектура дизайну, проектування інтерфейсів та обробка даних, інтеграція конфіденційності в дизайн, планування повного життєвого циклу програмного забезпечення, компромісність та простота дизайну.
● Огляд дизайну безпеки: логістика SDR, навіщо SDR проводити та коли це робити. Документування SDR.
● Процес SDR: вивчення, запитання, ідентифікація, співпраця, відгуки.
● Методи оцінки безпеки дизайну, використання чотирьох основних запитань керівництва.

Змістовий модуль 3. Реалізація безпечного програмування
Основні питання:
● Введення в концепції безпечного програмування, уразливості та їх ланцюги, помилки та ентропія.
● GotoFail, однорядкова вразливість та уразливості кодування, часові атаки.
● Помилки кодування низького рівня, арифметичні вразливості, уразливості точності з плаваючою точкою, уразливості доступу до пам’яті, управління пам'яттю, переповнення буфера, Heartbleed
● Недовірений вхід, визначення терміну дії, критерії підтвердження, відхилення неправильного введення, виправлення неправильного введення, уразливості рядка символів, проблеми Unicode, SQL Injection, Небезпека XML.
● Тестування безпеки, перевірка безпеки уразливості GotoFail, функціональне тестування та функціональне тестування з уразливістю, тестові випадки безпеки, межі тестів безпеки, написання тестових випадків безпеки.
● Перевірка введення, тестування на наявність уразливостей XSS, Fuzz Testing, тести регресії безпеки, тестування доступності.
● Споживання ресурсів, порогове тестування, поширені атаки відмови в обслуговуванні, найкращі методи тестування безпеки, розробка, орієнтована на тестування, використання інтеграційного тестування.
● Практичні практики безпечного розвитку, якість коду, обробка винятків і помилок, документування безпеки, огляд коду безпеки. Вибір безпечних компонентів, інтерфейси безпеки, боротьба із Legacy Security, сортування вразливостей, оцінки DREAD. Прийняття рішень про сортування, підтримка безпечного середовища розвитку, забезпечення інструментів розробки.

● Прийняття рішень про сортування, підтримка безпечного середовища розвитку, відокремлення розвитку від виробництва, забезпечення інструментів розробки.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми-емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	1	1	3	3
Відвідування семінарських занять	1						
Відвідування практичних занять	1	3	3	2	2	5	5
Відвідування лабораторних занять	1	4	4	2	2	6	6
Робота на семінарському занятті	10						
Робота на практичному занятті	10	3	30	2	20	5	50
Лабораторна робота (в тому числі допуск, виконання, захист)	10	4	40	2	20	6	60
Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
Виконання модульної роботи	25	1	25	1	25	1	25
Виконання ІНДЗ	30						
Разом		-	114	-	80	-	159
Максимальна кількість балів: 353							
Розрахунок коефіцієнта: 353/60=5,88							

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Поняття безпеки та безпровідних технологій, їх аналіз		20	10
1	Проаналізуйте код та загрози, запропонуйте план мітігейшну, застосуйте паттерн та додайте криптографію: • виконання завдань відповідно до теми; • опрацювання фахових видань.	20	10
Змістовий модуль 2. Дизайн безпеки, огляд дизайну безпеки, його процес та оцінка		12	10
2	Створіть дизайн документу та застосунку, базуючись на стандартах безпеки: • виконання завдань відповідно до теми; • опрацювання фахових видань.	12	10
Змістовий модуль 3. Реалізація безпечного програмування		24	10
3	Протестуйте застосунок, віднайдіть проблеми у безпеці та запропонуйте ваші варіанти рішення проблем: • виконання завдань відповідно до теми;	24	10

	• опрацювання фахових видань.		
	Разом	56	30

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отримання студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Іспит оцінюється у 40 балів за розподілом: 10 балів – комплексний тест з дисципліни; 30 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з навчальної дисципліни.

Оцінювання практичного завдання відбувається в межах від 0 до 30 балів, згідно критеріїв оцінювання. Бали за виконання тесту та бали за виконання практичного завдання додаються.

Орієнтовний перелік питань для семестрового контролю

1. Розуміння безпеки та довіри.
2. Компетентність і недосконаліть.
3. Вміння довіряти рішенням.
4. Неявно довірені компоненти.
5. Надійність та безпечність.
6. C-I-A в інформаційній безпеці.
7. Золотий стандарт.
8. Конфіденційність.
9. Загрози, змагальна перспектива.
10. Чотири основні питання загроз.
11. Моделювання загроз.
12. Робота з моделі.
13. Визначення активів, поверхонь атаки, меж довіри та загроз. Уміння пом'якшити загрози, моделювання загроз, звернення до загроз.
14. Конфіденційність.
15. Структурні стратегії пом'якшення, мінімізація поверхонь атаки.

16. Вузькі вікна вразливості, мінімізація доступу до даних, політика доступу та контроль доступу.
17. Інтерфейси
18. Паттерни. Атрибути, економіка дизайну. Прозорий дизайн.
19. Мінімізація експозиції. Мінімум привілей та інформації.
20. Безпека за замовчуванням.
21. Дозволені списки над списками блокування.
22. Уникнення передбачуваності.
23. Збій безпеки. Чіткість виконання необхідних дій, повне посередництво, найменш поширений механізм, глибинний захист, довіра та відповідальність прийнятих рішень.
24. Анти-паттерни. Зворотний потік довіри. Компоненти, які не підлягають виправленню.
25. Криптографія, крипто-інструменти, випадкові числа, псевдовипадкові числа, криптографічно захищені псевдовипадкові числа, коди автентифікації повідомлень.
26. Використання MACів для запобігання фальсифікації. Повторні атаки. Безпечний зв'язок MAC.
27. Симетричне/асиметричне шифрування. Одноразовий блокнот. Розширений стандарт шифрування. Використання симетричної криптографії.
28. Криптосистема RSA. Цифрові підписи. Цифрові сертифікати. Обмін ключами. Використання Crypto.
29. Безпечний дизайн. Інтеграція безпеки в дизайн. Явні припущення проекту. Визначення сфери застосування. Встановлення вимог безпеки. Моделювання загроз. Пом'якшення загроз.
30. Проектування інтерфейсів. Проектування обробки даних. Інтеграція конфіденційності в дизайн. Планування повного життєвого циклу програмного забезпечення. Укладання компромісів. Простота дизайну.
31. Огляд дизайну безпеки: Логістика SDR – навіщо, що це та коли проводити? Процес SDR. Оцінка безпеки дизайну. Використання чотирьох питань як керівництва. Де копати.
32. Огляди конфіденційності. Перегляд оновлень. Управління розбіжностями. Ескалація розбіжностей.
33. Реалізація безпечного програмування. Шкідливий вплив. Уразливості – це помилки.

Ланцюги уразливостей. Помилки та ентропія. GotoFail: однорядкова вразливість. Уроки від GotoFail. Уразливості кодування. Атомність. Часові атаки. Серіалізація. Звичайні підозрювані.

34. Помилки кодування низького рівня. Арифметичні вразливості. Цілі уразливості фіксованої ширини. Уразливості точності з плаваючою точкою.
35. Нижній потік із плаваючою точкою. Переповнення цілого числа. Безпечна арифметика.
36. Уразливості доступу до пам’яті. Управління пам'яттю. Переповнення буфера. Вразливості виділення пам’яті. Heartbleed.
37. Недовірений вхід. Перевірка введення. Визначення терміну дії. Критерії підтвердження. Відхилення неправильного введення. Виправлення неправильного введення.
38. Уразливості рядка символів. Проблеми з довжиною. Проблеми Unicode. Уразливості ін’єкцій. SQL Injection. Обхід шляху. Регулярні вирази. Небезпека XML. Пом’якшення ін’єкційних атак.
39. Тестування безпеки. Що таке тестування безпеки? Перевірка безпеки уразливості GotoFail. Функціональне тестування. Функціональне тестування з уразливістю. Тестові випадки безпеки. Межі тестів безпеки. Написання тестових випадків безпеки. Перевірка перевірки введення.
40. Тестування на наявність уразливостей XSS. Fuzz Testing. Тести регресії безпеки. Тестування доступності. Споживання ресурсів. Порогове тестування.
41. Поширені атаки відмови в обслуговуванні. Найкращі методи тестування безпеки. Розробка, орієнтована на тестування. Використання інтеграційного тестування. Тестування безпеки.

42. Практичні практики безпечного розвитку. Якість коду. Кодекс гігієни. Обробка винятків і помилок. Документування безпеки. Огляд коду безпеки. Залежності.
43. Вибір безпечних компонентів. Інтерфейси безпеки. Не винаходьте колеса безпеки. Боротьба із Legacy Security. Сортування вразливостей. Оцінки DREAD.
44. Створення робочих подвигів. Прийняття рішень про сортування. Підтримка безпечного середовища розвитку. Відокремлення розвитку від виробництва. Забезпечення інструментів розробки. Випуск продукту

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре — достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре — в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно — посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо — мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання — незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу — досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 150 год., лекції – 12 год., практичні заняття – 20 год., лабораторні роботи – 24 год., модульний контроль – 8 год., самостійна робота – 56 год.

Модулі (назви, бали)	**Змістовий модуль 1. Поняття безпеки та безпровідних технологій, їх аналіз (114 балів)**					**Змістовий модуль 2. Дизайн безпеки, огляд дизайну безпеки, його процес та оцінка (80 балів)**		**Змістовий модуль 3. Реалізація безпечного програмування (159 балів)**				
Лекції (теми, бали)	Безпека: компетентності та недосконалості, надійність та конфіденційність (1 бал)	Загрози: моделі загроз, атаки пом'якшення загроз (1 бал)	Мітігейшн: стратегії, мінімізація атак, політика та контроль доступу (0,5 балів)	Паттерни: атрибути дизайну, збій в роботі, глибинний захист інформації (0,5 балів)	Криптографія: її інструменти псевдовипадкові числа, коди автентифікації повідомлень (1 бал)	Безпека дизайну: інтеграція безпеки, сфери застосування, вимоги безпеки, моделювання загроз, проектування обробки даних (1 бал)	Огляд дизайну безпеки: коли проводити, документація, процес, оцінювання, 4 питання керівництва, конфіденційність. (1 бал)	Безпечне програмування: ланцюги уразливостей, помилки та ентропія, уразливість кодування. (2 бали)	Помилки кодування низького рівня: арифметичні уразливості, точності з плавучою точкою, доступ до пам'яті, переповнення буфера (1 бал)	Недовірений вхід: уразливості та проблеми входу. (1 бал)	Тестування безпеки: функціональне тестування, GotoFail, XXS, Fuzz Testing, тести регресії безпеки. (1 бал)	Практичні навички безпечного доступу: обробка винятків помилок, якість коду, вибір безпечних компонентів, сортування уразливостей. (1 бал)
Практичні заняття (теми, бали)	Принципи поширення C-I-A у безпечному програмному забезпеченні . Модель загрози для існуючого програмного забезпечення (11 балів)		Бібліотеки для застосування політики розширеного доступу до існуючого API даних (11 балів)	Розробка дизайну сайту, на основі шаблону. Визначення кількості паттернів розділу для забезпечення його	максимальної безпеки. Покращення крипто API (11 балів)	Ознайомлення з інструкціями Google щодо написання документів (11 балів)	Визначення слабких/сильних сторін в існуючих проектах (11 балів)	Тошук помилок безпеки у проектах програмного забезпечення студентів (11 балів)	Ознайомлення з інструментами аналізу – Valgrind (11 балів)	Теревірка введених даних на достовірність (11 балів)	Пошук надважливих областей безпеки у коді та розробка додаткових тестів безпеки (11 балів)	Вивчення простих способів поступового покращення якості коду та перевірки тестового покриття помилок і обробки винятків. (11 балів)
Лабораторні заняття (теми, бали)		Атаки, пом'якшення загроз (11 балів)	Технології злому WEP та WPS (11 балів)	Атрибути дизайну глибинний захист інформації (11 балів)	Інструменти криптографії, коди автентифікації (11 балів)	Інтеграція безпеки дизайну та сфери застосування (11 балів)	Чотири питання керівництва, конфіденційність дизайну безпеки (11 балів)	Безпечне програмування, ланцюги уразливостей (11 балів)	Помилки кодування низького рівня, доступ до пам'яті, буфер обміну (11 балів)	Недовірний вхід, уразливості та проблеми (11 балів)	Тестування безпеки: GotoFail, XXS, Fuzz Testing (22 бали)	Навички безпечного доступу, якість коду, вибір компонентів (11 балів)
Самостійна робота	Самостійна робота (10 балів)					Самостійна робота (10 балів)		Самостійна робота (10 балів)				
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)					Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)				
Підсумковий контроль (вид, бали)	Екзамен (40 балів)											

8. Рекомендовані джерела

Основна (базова):

1. Коноваленко І.В. Програмування мовою C# 6.0. Навчальний посібник для технічних спеціальностей вищих навчальних закладів. - Тернопіль.: ТНТУ, 2016. – 229 с.
2. Голуб Б.М. C#. Концепція та синтаксис. Навчальний посібник. - Львів.: ЛНУ, 2006. – 136 с.
3. DESIGNING SECURE SOFTWARE by Loren Kohnfelder, 2021.
4. Cyber Security Source-Code Defender by cybertrining365.

Додаткова:

1. Ховард М., Лебланк Д., Вієга Д. Як написати безпечний код на C++, Java, Perl, PHP, ASP.NET. – К.: Видавництво ДМК Пресс, 2014. – 288 с.
2. Камаєв В.А., Костерин В.В. Технології програмування: Посібник – Харків: Вища школа, 2006. — 454 с.
3. Ховард М., Лебланк Д., Вієга Д. 19 смертних гріхів, що загрожують безпеці програм. Як не допустити типових помилок. – К.: Видавництво ДМК Пресс, 2006. — 288с.

Додаткові ресурси:

1. OWASP Top 10 (англ.) [Електронний ресурс]. – Режим доступу: https://owasp.org/Top10/
2. Visual Studio 2017 (англ.) [Електронний ресурс]. – Режим доступу: https://docs.microsoft.com/en-us/visualstudio/?view=vs-2017
3. ВікіПідручник C Sharp 2017 (укр.) [Електронний ресурс]. – Режим доступу: https://uk.wikibooks.org/wiki/C_Sharp
4. C# : Використання баз даних (укр.) [Електронний ресурс]. – Режим доступу: http://programmersworld.xyz/article/4/92
5. Керівництво по ASP.NET Core 2.0 (укр.) [Електронний ресурс]. – Режим доступу: https://metanit.com/sharp/aspnet5/