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 «ТЕХНОЛОГІЇ ПРОТИДІЇ ЗЛОЯКІСНОМУ ПРОГРАМНОМУ КОДУ»

для студентів

спеціальності	125 Кібербезпека та захист інформації
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0190/23
(підпис) (прізвище, ініціали)
«____» _____ 2023 р.

2023 – 2024 навчальний рік

Розробник:

Соколов Володимир Юрійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Соколов Володимир Юрійович, кандидат технічних наук, доцент, доцент 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 _____(підпис)_____ Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми ___(підпис)___ Володимир СОКОЛОВ

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____(підпис)_____ Євген ІВАНІЧЕНКО

Пролонговано:

на 2023/2024 н.р. _____ (Складанний П.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	
Загальний обсяг кредитів / годин	5 / 150	
Курс	2	
Семестр	3	
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	48	
Модульний контроль	8	
Семестровий контроль	30	
Самостійна робота	64	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Технології протидії злоякісному програмному коду» 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 другого (магістерського) рівня відповідно до навчальних планів спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.02 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 «Технології протидії злоякісному програмному коду» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Технології протидії злоякісному програмному коду» складається з 4-х змістових модулів: 1. Поняття злоякісного програмного коду. 2. Функціональні різновиди злоякісного програмного коду. 3. Способи внесення і запуску злоякісних програмних засобів і програмного коду. 4. Способи і засоби виявлення і протидії злоякісному програмному коду. Обсяг дисципліни – 150 год (5 кредитів).

Метою викладання навчальної дисципліни «Технології протидії злоякісному програмному коду» є отримання компетентностей в області технологій протидії злоякісному програмному коду.

Завдання:

- надання студентам теоретичних знань щодо проблем, завдань і особливостей технологій протидії злоякісному програмному коду;
- формування у студентів категоріальних понять з основ процесів, що притаманні функціонуванню технологій протидії злоякісному програмному коду і забезпечення безпеки функціонування програмних засобів;
- формування у студентів знань і умінь щодо протидії злоякісному програмному коду;
- стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів розвитку у сфері захисту інформації.

У результаті вивчення навчальної дисципліни формуються загальні компетентності:

ЗК-1: здатність застосовувати знання у практичних ситуаціях;

ЗК-2: здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях;

ЗК-3: здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням;

фахові компетентності:

КФ-1: Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації.

КФ-5: Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, розробки і тестування програмних засобів таких систем, супроводження та їх експлуатації.

3. Результати навчання за дисципліною

При вивченні курсу «протидії злоякісному програмному коду» студенти повинні

знати:

- про технології протидії злоякісному програмному коду;
- про правові і нормативні акти, які визначають систему захисту інформації в державі;
- про основні методи, технології, принципи і правила протидії злоякісному програмному коду;
- про технології розробки, тестування і супроводження програмних засобів протидії злоякісному програмному коду.

уміти:

- використовувати технології протидії злоякісному програмному коду;
- розробляти, тестувати і супроводжувати програмні засоби протидії злоякісному програмному коду.

та досягнути наступні ***програмні результати***:

РН-2: вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки; вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації; знати уразливості й методи їх застосування в різних телекомунікаційних технологіях; знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж; вміти проектувати, розробляти, тестувати і супроводжувати програмні засоби забезпечення безпеки інформаційно-комунікаційних систем і мереж; знати методи організації захищеної передачі даних у незахищеному середовищі;

РН-3: знати уразливості й методи їх застосування в інформаційно-комунікаційних і обчислювальних системах та мережах; вміти розробляти, тестувати і супроводжувати програмні засоби відповідно до моделі їх життєвого циклу; знати спеціалізоване мережеве обладнання, що застосовується для забезпечення мережевої безпеки; вміти розробляти і тестувати програмні засоби забезпечення безпеки обчислювальних і інформаційно-комунікаційних систем та мереж;

РН-7: знати технології розробляти і тестувати програмні засоби забезпечення безпеки обчислювальних і інформаційно-комунікаційних систем та мереж; вміти знаходити шляхи для їх усунення;

РН-9: володіти практичними навичками розробки і тестування програмних засобів забезпечення безпеки обчислювальних і інформаційно-комунікаційних систем та мереж;

РН-24: знати уразливості й методи їх застосування в різних телекомунікаційних технологіях та SMART-інфраструктурі. Вміти проектувати захищені (з урахуванням загроз) проводові і

безпроводові телекомунікаційні та SMART-системи.

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 злоякісного програмного коду							
Тема 1. Поняття про небезпечну комп'ютерну інформацію.	14	2		2	2		8
Тема 2. Антивірусні програмні засоби.	14	2		2	2		8
Модульний контроль	2						
Разом	30	4		4	4		16
Змістовий модуль 2. Функціональні різновиди злоякісного програмного коду							
Тема 3**.** Функціональні види злоякісного програмного забезпечення і програмного коду.	14	2		2	2		8
Тема 4. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків.	14	2		2	2		8
Модульний контроль	2						
Разом	30	4		4	4		16
Змістовий модуль 3. Способи внесення і запуску злоякісних програмних засобів і програмного коду							
Тема 5. Способи впровадження і запуску злоякісного програмного коду.	14	2		2	2		8
Тема 6. Механізми приховування злоякісних програм і програмного коду.	14	2		2	2		8
Модульний контроль	2						
Разом	30	4		4	4		16
Змістовий модуль 4. Способи і засоби виявлення і протидії злоякісному програмному коду							
Тема 7. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду.	14	2		2	2		8
Тема 8. Технології проактивного виявлення і протидії злоякісному програмному коду.	14	2		2	2		8
Модульний контроль	2						
Разом	30	4		4	4		16
Підготовка та проходження контрольних заходів	30						
Усього	150	16		16	16		64

5. Програма навчальної дисципліни

Змістовий модуль 1. Поняття злоякісного програмного коду

Тема 1. Поняття про небезпечну комп'ютерну інформацію.

Небезпечні дані; інструменти створення злоякісних програм; стиль «небезпечного» програмування; склад злоякісних програм і команд; виконуємі та інтерпретуємі програми; програмне управління комп'ютером в рещимі командної строки; управління програмами в графічному режимі.

Тема 2. Антивірусні програмні засоби.

Сканування; моніторинг; контроль; імунізація; оновлення баз даних антивірусів і ресурсів злоякісного програмного коду.

Змістовий модуль 2. Функціональні різновиди злоякісного програмного коду

Тема 3. Функціональні види злоякісного програмного забезпечення і програмного коду.

Комп'ютерні віруси; програмні закладки; «логічні бомби»; злоякісні програми «віддаленого адміністрування»; «мережеві хробаки»; «жадібні» програми; міфічні злоякісні програми.

Тема 4. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків.

Блокування комп'ютерної інформації; несанкціоноване видалення комп'ютерної інформації; злоякісна модифікація комп'ютерної інформації; несанкціоноване копіювання комп'ютерної інформації; порушення роботи комп'ютера; несанкціонований характер запуску злоякісних програм.

Змістовий модуль 3. Способи внесення і запуску злоякісних програмних засобів і програмного коду

Тема 5. Способи впровадження і запуску злоякісного програмного коду.

Впровадження і запуск на етапі само тестування комп'ютера; впровадження і запуск на етапі завантаження операційної системи; мережеве впровадження і запуск; запуск при завантаженні CD ROM;запуск шляхом модифікації типу і піктограм файлу; впровадження і запуск програм за допомогою «троянських» оболонок; впровадження і запуск небезпечних команд з використанням ярликів.

Тема 6. Механізми приховування злоякісних програм і програмного коду.

Форми статичного приховування файлів злоякісних програм від антивірусного сканування; форми динамічного приховування виконуємих програм; механізми приховування небезпечних програм на рівні ядра.

Змістовий модуль 4. Способи і засоби виявлення і протидії злоякісному програмному коду

Тема 7. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду.

Проактивний захист; антивірусні програми; виявлення аномалій; вивлення з використанням сигнатур; виявлення з використанням емуляції; програма-ревізор;мережеві системи виявлення атак; сигнатурні атаки; системи виявлення вторгнень; хостові системи виявлення вторгнень; евристичне сканування; активна система виявлення небезпечних серверів; технології CVP.

Тема 8. Технології проактивного виявлення і протидії злоякісному програмному коду.

Евристичний аналіз; емуляція коду; аналіз поведінки; песочниця; віртуалізація робочого оточення; використання проактивних технологій.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної 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, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *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		Модуль 4	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	2	2	2	2	2	2
Відвідування семінарських занять									
Відвідування практичних занять	1	2	2	2	2	2	2	2	2
Відвідування лабораторних занять	1	2	2	2	2	2	2	2	2
Робота на семінарському занятті									
Робота на практичному занятті	10	2	20	2	20	2	20	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10	2	20	2	20	2	20	2	20
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25
Разом		-	76	-	76	-	76	-	76
Максимальна кількість балів: 304									
Розрахунок коефіцієнта: 304/60=5,07									

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом позааудиторної 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
<u>Змістовий модуль 1</u>. Поняття злоякісного програмного коду		16	5
1	Тема 1. Поняття про небезпечну комп’ютерну інформацію. Тема 2. Антивірусні програмні засоби.	16	5
<u>Змістовий модуль 2</u>. Функціональні різновиди злоякісного програмного коду		16	5
2	Тема 3. Функціональні види злоякісного програмного забезпечення і програмного коду. Тема 4. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків.	16	5
<u>Змістовий модуль 3.</u> Способи внесення і запуску злоякісних програмних засобів і програмного коду		16	5
3	Тема 5. Способи впровадження і запуску злоякісного програмного коду. Тема 6. Механізми приховування злоякісних програм і програмного коду.	16	5
<u>Змістовий модуль 4</u>. Способи і засоби виявлення і протидії злоякісному програмному коду		16	5
4	Тема 7. Методи і технології виявлення і протидії злоякісним	16	5

№ з/п	Назва теми	Кількість годин	Бали
	програмним засобам і програмному коду. Тема 8. Технології проактивного виявлення і протидії злоякісному програмному коду.		
	Разом	64	20

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, обгрунтованість 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 – модульна контрольна зі звітом в електронній формі.

Модульна контрольна робота оцінюється у 3 бали.

Форми проведення семестрового контролю та критерії оцінювання

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

Форма проведення іспиту – комбінована. Екзамен оцінюється у 40 балів за розподілом: 30 балів – теоретичні питання з дисципліни; 10 балів – виконання практико-орієнтованого завдання.

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

Оцінювання практичного завдання відбувається в межах від 0 до 10 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь.

Орієнтовний перелік питань для семестрового контролю

1. Поняття про небезпечну комп'ютерну інформацію. Небезпечні дані.
2. Поняття про небезпечну комп'ютерну інформацію. Інструменти створення злоякісних програм.
3. Поняття про небезпечну комп'ютерну інформацію. Стиль «небезпечного» програмування.
4. Поняття про небезпечну комп'ютерну інформацію. Склад злоякісних програм і команд.
5. Поняття про небезпечну комп'ютерну інформацію. Виконуємі та інтерпретуємі програми.
6. Поняття про небезпечну комп'ютерну інформацію. Програмне управління комп'ютером в рещимі командної строки.
7. Поняття про небезпечну комп'ютерну інформацію. Управління програмами в графічному режимі.
8. Антивірусні програмні засоби. Сканування.
9. Антивірусні програмні засоби. Моніторинг.
10. Антивірусні програмні засоби. Контроль.

11. Антивірусні програмні засоби. Імунізація.
12. Антивірусні програмні засоби. Оновлення баз даних антивірусів і ресурсів злоякісного програмного коду.
13. Функціональні різновиди злоякісного програмного коду. Комп'ютерні віруси.
14. Функціональні різновиди злоякісного програмного коду. Програмні закладки.
15. Функціональні різновиди злоякісного програмного коду. «Логічні бомби».
16. Функціональні різновиди злоякісного програмного коду. Злоякісні програми «віддаленого адміністрування».
17. Функціональні різновиди злоякісного програмного коду. «Мережеві хробаки».
18. Функціональні різновиди злоякісного програмного коду. «Жадібні» програми.
19. Функціональні різновиди злоякісного програмного коду. Міфічні злоякісні програми.
20. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків. Блокування комп'ютерної інформації.
21. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків. Несанкціоноване видалення комп'ютерної інформації.
22. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків. Злоякісна модифікація комп'ютерної інформації.
23. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків. Несанкціоноване копіювання комп'ютерної інформації.
24. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків. Порушення роботи комп'ютера.
25. Дії злоякісних програм і програмного коду, що призводить до небезпечних наслідків. Несанкціонований характер запуску злоякісних програм.
26. Способи впровадження і запуску злоякісного програмного коду. Впровадження і запуск на етапі самотестування комп'ютера.
27. Способи впровадження і запуску злоякісного програмного коду. Впровадження і запуск на етапі завантаження операційної системи.
28. Способи впровадження і запуску злоякісного програмного коду. Мережеве впровадження і запуск.
29. Способи впровадження і запуску злоякісного програмного коду. Запуск при завантаженні CD ROM.
30. Способи впровадження і запуску злоякісного програмного коду. Запуск шляхом модифікації типу і піктограм файлу.
31. Способи впровадження і запуску злоякісного програмного коду. Впровадження і запуск програм за допомогою «троянських» оболонок.
32. Способи впровадження і запуску злоякісного програмного коду. Впровадження і запуск небезпечних команд з використанням ярликів.
33. Механізми приховування злоякісних програм і програмного коду**.** Форми статичного приховування файлів злоякісних програм від антивірусного сканування.
34. Механізми приховування злоякісних програм і програмного коду**.** Форми динамічного приховування виконуємих програм.
35. Механізми приховування злоякісних програм і програмного коду**.** Механізми приховування небезпечних програм на рівні ядра.
36. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Проактивний захист.
37. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Антивірусні програми.
38. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Виявлення аномалій.
39. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Ввивлення з використанням сигнатур.
40. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Виявлення з використанням емуляції.

41. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Програма-ревізор.
42. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Мережеві системи виявлення атак.
43. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Сигнатурні атаки.
44. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Системи виявлення вторгнень.
45. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Хостові системи виявлення вторгнень.
46. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Евристичне сканування.
47. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Активна система виявлення небезпечних серверів.
48. Методи і технології виявлення і протидії злоякісним програмним засобам і програмному коду. Технології CVP.
49. Технології проактивного виявлення і протидії злоякісному програмному коду. Евристичний аналіз.
50. Технології проактивного виявлення і протидії злоякісному програмному коду. Емуляція коду.
51. Технології проактивного виявлення і протидії злоякісному програмному коду. Аналіз поведінки.
52. Технології проактивного виявлення і протидії злоякісному програмному коду. Песочниця.
53. Технології проактивного виявлення і протидії злоякісному програмному коду. Віртуалізація робочого оточення.
54. Технології проактивного виявлення і протидії злоякісному програмному коду. Використання проактивних технологій.

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 карта дисципліни

Разом: 150 год., лекції – 16 год., практичні заняття – 16 год., лабораторні роботи – 16 год., модульний контроль – 10 год., самостійна робота – 92 год., семестровий контроль – 30 год.

Модулі (назви, бали)	**Змістовий модуль 1. Поняття злоякісного програмного коду** (76 балів)		**Змістовий модуль 2. Функціональні різновиди злоякісного програмного коду** (76 балів)		**Змістовий модуль 3. Способи внесення і запуску злоякісних програмних засобів і програмного коду** (76 балів)		**Змістовий модуль 4. Способи і засоби виявлення і протидії злоякісному програмному коду** (76 балів)	
Лекції (теми, бали)	1. Тема 1 (1 бал)	2. Тема 2 (1 бал)	3.Тема 3 (1 бал)	4. Тема 4 (1 бал)	5. Тема 5 (1 бал)	6. Тема 6 (1 бал)	7. Тема 7 (1 бал)	8. Тема 8 (1 бал)
Лабораторні заняття (теми, бали)	1. (11 балів)	2. (11 балів)	3. (11 балів)	4. (11 балів)	5. (11 балів)	6. (11 балів)	7. (11 балів)	8. (11 балів)
Практичні заняття (теми, бали)	1. (11 балів)	2. (11 балів)	3. (11 балів)	4. (11 балів)	5. (11 балів)	6. (11 балів)	7. (11 балів)	8. (11 балів)
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 1 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)							

8. Рекомендовані джерела

Основна

1. Бакланов В.В. Захист комп'ютерної інформації у клієнтських додатках: навч. посіб. / В.В. Бакланов. – К.: ГОУ ВПО УГТУ, 2005. – 84 с.
2. Білліг В.А. VBA в Office 2000. Офісне програмування / В.А. Білліг. – Х.: «ІЗОТЕК», 1999. – 480 с.
3. Борн Г. Керівництво розробника на Microsoft Windows Script Host 2.0 Майстер-клас. – Х.: Діалог-МІФІ, 2001. – 480 с.
4. Глушаков С.В., Мельников В.В., Сурядний А.С. Програмування у середовищі Windows: Навчальний курс / С.В. Глушаков, В.В. Мельников, А.С. Сурядний. – Х.: Фоліо, 2001. – 487 с.
5. Глушаков С.В., Хачиров Т.С., Соболев Р.О. Таємниці хакера. Захист та атака / С.В. Глушаков, Т.С. Хачиров, Р.О. Соболев. – Х.: Фоліо, 2004. – 414 с.
6. Дунаєв С.Б. Технології Інтернет-програмування / С.Б. Дунаєв. – К.: Видавничий дім «Вільямс», 2001. – 480 с.
7. Макнамара Д. Таємниці комп'ютерного шпіонажу: тактика і контрміри / Д. Макнамара; Пер. з англ.; За ред. С.М. Молявко. – К.: Діалектика, 2004. – 536 с.
8. Несвижський В. Програмування апаратних засобів у Windows / В. Несвижський. – Х.: «ІЗОТЕК», 2004. – 880 с.
9. Пирогов В.Ю. Асемблер для Windows/ В.Ю. Пирогов. 3-е вид., перероб. і доп. – Х.: «ІЗОТЕК», 2005. – 864 с.
10. Фленов М.Є. Програмування на C++ очима хакера / М.Є. Фленов. – Х.: Фоліо, 2004. – 336 с.

Додаткова

1. Блек Р. Ключові процеси тестування. Планування, підготовка, проведення, удосконалення. – К.: Лорі, 2006.
2. Дастін Е., Решка Д., Пол Д. Автоматизоване тестування програмного забезпечення: Пер. з англ. – К.: Лорі, 2003 – 568с
3. Стотлемаєр Д. Тестування Web-додатків. Пер. з англ. – Х.: Фоліо, 2003. – 240 с.