Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра системного програмування і спеціалізованих комп'ютерних систем

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*123 - КОМП'ЮТЕРНА ІНЖЕНЕРІЯ*
Освітня програма	*Системне програмування та спеціалізовані комп'ютерні системи*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*3 курс, осінній семестр*
Обсяг дисципліни	*4 кредити, 120 годин*
Семестровий контроль/ контрольні заходи	*РГР, Залік*
Розклад занять	*http://rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор, лабораторні: *д.т.н., проф. Терейковський Ігор Анатолійович, tereikovskyi.ihor@lll.kpi.ua*
Розміщення курсу	https://campus.kpi.ua

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Отримані знання будуть необхідними та корисними для кожного фахівця в області інформаційних технологій, як під час здійснення службових обов`язків, так і в повсякденному житті (наприклад, при використанні сучасних інформаційно-комунікаційних засобів – мережевих месенджерів, електронної пошти, соціальних мереж, різного роду веб-сайтів та ін.).

***Мета** дисципліни: підготовка висококваліфікованих фахівців, які володіють методами побудови систем захисту комп'ютерної інформації, вміють виконувати як моделювання, так і розробку таких систем на основі отриманих теоретичних результатів*

***Предмет** дисципліни: теорія та практика захисту інформації в комп'ютерних системах.*

Основні завдання навчальної дисципліни

Дисципліна підсилює формування наступних компетенцій:

ФК 4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.
ФК 6. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні систем та мережі різного виду та призначення.
ФК 8. Здатність виконувати роботи з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.
ФК 13. Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних

технологій, визначати обмеження цих технологій.

Студент після опанування дисципліни матиме знання

- *Методів та засобів проведення експериментів, збирання даних та моделювання в комп'ютерних системах*
- *Сучасних технологій проектування комп'ютерних систем та мереж.*
- *Структур сучасних операційних систем.*

Студент після опанування дисципліни умітиме

- *Системно мислити та застосовувати творчі здібності для формування нових ідей.*
- *Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення задач спеціальності.*
- *Реалізувати надійне функціонування, а також забезпечити захист інформації в комп'ютерних системах.*

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

***Пререквізити**: мати базові знання отримані при вивченні дисциплін «Теорія ймовірності та математична статистика», «Програмування», «Моделювання», «Системне програмування».*

***Постреквізити**: вирішення практичних задач з захисту комп'ютерної інформації; застосування отриманих знань при вивченні дисциплін пов'язаних з проєктуванням і експлуатацією комп'ютерних систем та мереж.*

3. Зміст навчальної дисципліни

Розділ 1. Основи побудови комплексів засобів захисту в комп'ютерних системах

Тема 1.1. Основні поняття. Нормативна база.

Тема 1.2. Принципи створення комплексної системи захисту інформації.

Тема 1.3. Оптимізація параметрів системи захисту інформації.

Розділ 2. Захист операційних систем

Тема 2.1. Методи та засоби захисту операційних систем.

Розділ 3. Захист систем управління базами даних

Тема 3.1. Методи та засоби захисту систем управління базами даних.

Тема 3.2. Захист офісних та промислових систем управління базами даних.

Розділ 4. Захист від шкідливого програмного забезпечення

Тема 4.1.Загальна характеристика шкідливого програмного забезпечення.

Тема 4.2. Методи та засоби захисту від шкідливого програмного забезпечення.

Розділ 5. Захист комп'ютерних мереж

Тема 5.1. Методи та засоби захисту комп'ютерних мереж.

Тема 5.2. Захист мобільного програмного забезпечення.

Тема 5.3. Захист електронної пошти.

Розділ 6. Розпізнавання атак та вразливостей комп'ютерних систем

Тема 6.1. Принципи створення та використання систем розпізнавання атак та систем розпізнавання вразливостей.

Тема 6.2. Оптимізація параметрів систем розпізнавання атак та систем розпізнавання вразливостей.

Розділ 7. Криптографічні методи і засоби захисту інформації

Тема 7.1. Симетрична криптографія.

Тема 7.2. Асиметрична криптографія.

Розділ 8. Перспективні напрями розвитку засобів захисту інформації

Тема 8.1. Штучний інтелект в засобах захисту інформації.

Тема 8.2. Нейронні мережі в засобах захисту інформації.

Тема 8.3. Розпізнавання атак на інформацію за допомогою нейронних мереж.

4. Навчальні матеріали та ресурси

Базова література

1. Богуш В.М. Інформаційна безпека від А до Я.: навч. посібник [для студ. вищ. навч. закл.] / В.М. Богуш, А. М. Кудін. – К. : МОУ, 2006. – 456 с.

2. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем [Електронний ресурс] : підручник / М. В. Грайворонський, О. М. Новіков.– Київ : Видавнича група BHV, 2009. – 698 с.

3. Гапак О.М. Комп'ютерна криптографія: навчальний посібник / Гапак О. М. – Ужгород : УжНУ, 2021. – 93 с.

4. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

5. Терейковський, І.А. Захист інформації в комп'ютерних системах [Електронний ресурс] : навчальний посібник / І. А. Терейковський, С.О. Гнатюк; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,67 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 135 с. – Назва з екрана.

Додаткова література

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (1994).

2. Закон України "Про захист персональних даних" (2010).

3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015).

4. Закон України "Про національну безпеку (2018).

5. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016).

6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229.

7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;

8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.

11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.

13. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

14. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.

15. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

16. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

17. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

18. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

19. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

20. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

1. Основні поняття. Нормативна база.

Проблема захисту інформації в комп'ютерних системах: історія, основні тенденції, законодавчий, організаційний та технічний аспекти. Основні визначення. Нормативне забезпечення системи технічного захисту інформації в Україні. Нормативні документи системи криптографічного захисту інформації в Україні. Зарубіжні та міжнародні стандарти щодо захисту інформації в комп'ютерних системах.
Література: 1-6

2. Принципи створення комплексної системи захисту інформації.

Загрози конфіденційності, цілісності, доступності. Спостережність інформації. Джерела загроз. Канали порушення безпеки інформації, їх класифікація та приклади. Політика безпеки інформації. Комплекс засобів захисту і об'єкти комп'ютерної системи. Несанкціонований доступ. Модель порушника. Планування захисту і керування системою захисту. Основні принципи керування доступом: безперервний захист, довірче і адміністративне керування доступом, забезпечення персональної відповідальності. Системність, спеціалізованість та неформальність проектування засобів захисту інформації. Послуги безпеки. Гарантії. Загальні вимоги до засобів захисту інформації.

Література: 1, 2, 9

3. Оптимізація параметрів системи захисту інформації.

Визначення задачі оптимізації захисту інформації у вигляді оберненої задачі оптимізації технічних систем. Економічні та технічні критерії оптимізації системи захисту інформації. Оптимізаційні обмеження. Поняття режиму захисту. Оптимізуємі параметри. Використання моделі зміни рівня захисту. Методи пошуку оптимуму.

Література: 4, 5, 18

4. Методи та засоби захисту операційних систем.

Особливості моделі загроз ресурсам операційних систем (ОС). Основні функції підсистеми захисту ОС. Підходи до створення захищених ОС. Типова структура підсистеми безпеки ОС і виконувані нею функції: ідентифікація й автентифікація, розмежування доступу, аудит, підзвітність дій, повторне використання об'єктів, точність і надійність обслуговування, захист обміну даних. Керування доступом до ресурсів ОС. Сучасні механізми керування доступом. Типова архітектура підсистеми безпеки ОС. Механізми сучасних апаратних платформ, що використовуються для підтримки функціонування підсистеми захисту ОС. Особливості забезпечення безпеки ресурсів ОС сімейств UNIX і Windows. Архітектура безпеки ОС Windows NT/2000/XP/2003 та мереж на її основі.

Література: 1, 2, 4

5. Методи та засоби захисту систем управління базами даних.

Причини, види, основні методи порушення конфіденційності в системах управління базами даних (СУБД). Одержання несанкціонованого доступу до конфіденційної інформації шляхом логічних висновків. Багаторівневі реляційні СУБД. Методи захисту СУБД. Особливості керування доступом. Підтримка логічної цілісності, транзакції функціонування, синхронізація в розподілених СУБД. Забезпечення безпеки багаторівневих реляційних СУБД. Особливості застосування криптографічних методів. Спільне застосування засобів ідентифікації й автентифікації, вбудованих у СУБД і в ОС. Кластерна організація серверів баз даних.

Література: 1, 4, 11

6. Захист офісних та промислових систем управління базами даних.

Типові загрози інформації офісних СУБД. Особливості системи захисту офісних СУБД. Особливості розподілу прав доступу до офісних баз даних. Методика та технічні прийоми захисту СУБД MS Access. Типові загрози інформації промислових СУБД. Особливості системи захисту промислових СУБД. Особливості розподілу прав доступу до промислових баз даних. Методика та технічні прийоми захисту СУБД MySQL та MS SQL.

Література: 1, 4, 11

7. Загальна характеристика шкідливого програмного забезпечення.

Руйнуючі програмні засоби. Програми з потенційно шкідливим впливом та їх властивості. Класифікація шкідливого програмного забезпечення. Віруси, трояни, кейлогери. Нормативна база. Задачі захисту програмного забезпечення. Особливості загроз порушення безпеки програмного забезпечення. Злам захисту програмного забезпечення. Комплексність захисту ПЗ.

Література: 1, 4, 8

8. Методи та засоби захисту від шкідливого програмного забезпечення.

Методи і засоби захисту програмного забезпечення. Методи захисту програм від вивчення; захист від програмних впливів, що руйнують. Типова архітектура системи захисту програмного

забезпечення. Інтеграція захисних механізмів до програмного забезпечення. Програмні та апаратні засоби захисту програмного забезпечення. Критерії оцінки ефективності систем захисту від шкідливого програмного забезпечення. Системи антивірусного захисту провідних виробників. Методи ідентифікації програм та захист авторських прав.
Література: 1, 4, 8

9. Методи та засоби захисту комп'ютерних мереж.

Загальні положення про інформаційну безпеку мереж передачі даних. Особливості моделі загроз мереж передачі даних. Формування розподіленої ДВБ та її властивості. Основні типи засобів забезпечення інформаційної безпеки в обчислювальних мережах. Основи технології міжмережних екранів (МЕ). Визначення МЕ та засоби їх реалізації. Принципи побудови та класифікації МЕ. Основи технології віртуальних приватних мереж (ВПМ). Визначення ВПМ та засоби їх реалізації. Принципи побудови та класифікації ВПМ.
Література: 1, 3, 5

10. Захист мобільного програмного забезпечення.

Безпека мобільного програмного забезпечення. Особливості захисту мобільних програмних компонентів та систем мобільних програмних агентів. Особливості архітектури безпеки COM/DCOM, CORBA, ActiveX, Java, Flash Macromedia. Методика оцінки документованих параметрів захисту мобільного програмного забезпечення.
Література: 1, 4, 5

11. Захист електронної пошти.

Типові загрози інформації комп’ютерної системи при використанні електронної пошти. Методи захисту від несанкціонованої передачі даних. Поняття спаму. Фішинг. Види спаму та передумови його існування. Методи захисту від спаму. Характеристика методів захисту на основі чорного та білого списків, ключових словосполучень, байєсовської фільтрації. Особливості сучасних спам-засобів.
Література: 1, 4, 5

12. Принципи створення та використання систем розпізнавання атак та систем розпізнавання вразливостей.

Адаптивні комплекси засобів захисту інформації; системи виявлення вторгнень; системи керування захищеністю; комплекси засобів захисту інформації мобільних програмних систем. Основи систем аналізу вразливостей. Визначення та принципи класифікації. Інформаційні сховища вразливостей та їх застосування. Системи аналізу вразливостей провідних світових виробників. Основи систем виявлення вторгнень. Визначення та принципи класифікації. Три принципи побудови систем виявлення вторгнень. Системи виявлення вторгнень провідних світових виробників.
Література: 1,2 , 4

13. Оптимізація параметрів систем розпізнавання атак та систем розпізнавання вразливостей.

Передумови оптимізації параметрів систем розпізнавання атак та вразливостей. Визначення оптимізуємих параметрів. Використання класичних підходів оптимізації режиму контролю та діагностики технічних систем. Методика побудови марківської моделі динаміки параметрів захисту. Особливості збору та обробки статистичних даних для побудови марківської моделі. Приклад створення марківської моделі оптимізації параметрів захисту Веб-серверу.
Література: 1, 2, 9

14. Симетрична криптографія.

Історія криптології. Симетрична криптографія. Методи шифрування заміною, перестановкою та шляхом аналітичних перетворень. Комбіновані методи шифрування. Посимвольне кодування інформації. Кодування за змістом. Інші види криптографічної обробки даних. Елементи криптоаналізу.

Література: 2, 3, 5

15. Асиметрична криптографія.

Принципи асиметричної криптографії. Поняття відкритого та закритого ключів. Інфраструктура відкритого ключа. Поняття цифрового підпису. Поняття та приклади криптографічних протоколів. Організаційне забезпечення засобів асиметричної криптографії. Використання протоколу SSL для безпечного обміну інформацією в мережі.

Література: 2. 3, 5

16. Штучний інтелект в засобах захисту інформації.

Загальна характеристика теорії штучного інтелекту. Мета та задачі застосування методів штучного інтелекту в галузі захисту інформації. Характеристика задач захисту інформації, розв'язання яких потребує застосування методів штучного інтелекту. Розрахунок очікуваного ефекту використання.

Література: 1, 5

17. Нейронні мережі в засобах захисту інформації.

Загальна характеристика теорії нейронних мереж. Мета та задачі застосування методів нейронних мереж в галузі захисту інформації. Характеристика задач захисту інформації, розв'язання яких потребує застосування методів нейронних мереж. Розрахунок очікуваного ефекту використання.

Література: 1, 5

18. Розпізнавання атак на інформацію за допомогою нейронних мереж.

Загальна характеристика задачі розпізнавання атак на комп’ютерну систему. Типи моделей нейронних мереж, які доцільно використовувати для розпізнавання атак. Розпізнавання вірусів за допомогою нейронних мереж. Розпізнавання спаму за допомогою нейронних мереж. Розпізнавання мережевих атак на Веб-сервер за допомогою нейронних мереж.

Література: 1, 5

Лабораторні заняття

1. Захист Веб-серверу Apache

Завдання: встановити Веб-сервер Apache, налаштувати систему його захисту та оцінити відповідність цієї системи вітчизняній нормативній документації

2. Керування системою захисту СУБД MySQL

Завдання: провести настройку системи захисту СУБД MySQL

3. Стеганографічні способи захисту інформації

Завдання: розробити програмне забезпечення для стеганографічного захисту інформації

4. Криптографічні способи захисту інформації

Завдання: розробити програмне забезпечення для криптографічного захисту інформації

6. Самостійна робота студента/аспіранта

У процесі виконання індивідуальних завдань студенти повинні закріпляти знання, отримані під час лекцій та самостійної роботи, самостійно вивчати визначені теми, поглиблювати свої знання для подальшого навчання .

У якості індивідуальних завдань можуть розроблятися окремі питання учбових тем, огляди специфічних методів вимірювань, використання методів та засобів як створення так і обробки різних типів сигналів та зображень, сфери їх використання та інше.

Самостійна робота студентів полягає в наступному:

- *підготовці до лекційних занять по вивченню попереднього лекційного матеріалу;*
- *виконанням лекційних завдань на СРС;*
- *підготовки до лабораторних робіт з вивченням теорії лабораторного заняття з усною відповіддю на наведені питання розділу;*
- *виконанням з оформленням на кожне лабораторне заняття протоколу по попередній темі.*

Контроль знання на лабораторних заняттях здійснюється шляхом перевірки домашніх завдань, опитування, а також через виконання модульних контрольних робіт.

Лекційні завдання на СРС

1. Типове положення про службу захисту інформації в автоматизованій системі
2. Методика керування засобами захисту
3. Пошук оптимуму методом дихотомії
4. Критерії оцінки ефективності функціонування підсистеми захисту ОС.
5. Використання «ролей» для розподілу доступу в СУБД
6. Особливості захисту СУБД Oracle
7. Веб-орієнтоване шкідливе програмне забезпечення
8. Захист від Веб-орієнтованого шкідливого програмного забезпечення
9. Захист мереж Cisco
10. Особливості захисту ActiveX
11. Захист від спаму на основі семантичного аналізу тексту листа
12. Система виявлення вторгнень Snort
13. Визначення оптимального періоду контролю вразливостей
14. Методи криптоаналізу
15. Програмні засоби для створення цифрового підпису
16. Використання семантичних мереж
17. Методика функціонування мережі APT.
18. Використання мережі PNN.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Всі студенти повинні відвідувати лекційні та лабораторні заняття, на яких потрібно активно працювати над засвоєнням навчального матеріалу. За об'єктивних причин (наприклад - хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі індивідуально за погодженням із керівником курсу.

Всі індивідуальні лабораторні роботи потрібно розрахувати і у вигляді окремого файлу надати викладачеві на наступному після видачі лабораторному занятті. Практичні результати виконання лабораторної роботи потрібно підтвердити знанням теоретичного матеріалу за темою при захисті.

Політика щодо дедлайнів та перескладання:

Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності:

Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт заборонені (в т. ч. із використанням мобільних пристроїв)

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Рейтинг студента з дисципліни складається з балів, що він отримує за:
- виконання та захист 4 лабораторних робіт;
- виконання та захист розрахунково-графічної роботи;
- усну відповідь на заліку.

Система рейтингових (вагових) балів та критерії оцінювання
1. Лабораторні роботи
Ваговий бал – 10. Максимальна кількість балів за всі лабораторні роботи дорівнює 10 балів х 4 = 40 балів.
Критерії оцінювання лабораторної роботи:
оцінюється:

- *Чіткість у визначені предметної області (або постановка задачі).*
- *Якість програми.*
- *Екрані форми.*
- *Знання теоретичних засад.*
- *Вчасність здачі лабораторної роботи.*

Критерії оцінювання:
9-10 балів – всі вимоги виконані;
6-8 бали – виконані усі вимоги, але немає чіткості у поясненнях або робота здана пізніше ніж за тиждень після запланованої дати;
1-5 бали – не всі вимоги виконані, зокрема, немає програмного забезпечення , або воно працює невірно, або робота здана пізніше ніж за 2 тижні після запланованої дати;
0 балів – робота не виконана.

2. Бали за розрахунково-графічну роботу
Максимальна кількість балів за розрахункову роботу: 20 балів.
Бали нараховуються за:
- відповідь під час захисту розрахункової роботи: 0-8 бали;
- якість виконання розрахункової роботи: 0-12 балів.
Критерії оцінювання відповіді:
7-8 балів – відповідь вірна, добре аргументована;
5-6 балів – відповідь вірна, але не дуже добре аргументована;

3-4 бали – в цілому відповідь вірна, але має недоліки;
1-2 бали – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.
Критерії оцінювання якості виконання:
10-12 балів – робота виконана на високому рівні, в повному обсязі;
5-9 бали – робота виконана в повному обсязі, але містить незначні помилки;
1-4 бали – робота виконана не в повному обсязі, містить суттєві помилки;
0 балів – робота не виконана.

3. Усна відповідь на заліку.
Правильний захист кожного з 4-х теоретичних питань дає 10 балів:
4 бали х 10 = 40 балів

Розрахунок шкали (R) рейтингу:
Сума вагових балів контрольних заходів протягом семестру складає:
RC = 40 + 20 + 40 = 100 балів.

Таким чином, рейтингова шкала з дисципліни складає R = RC = 100 балів.

Семестровий контроль: залік
Умови допуску до семестрового контролю:

- *мінімально позитивна оцінка за розрахунково-графічну роботу;*
- *зарахування усіх лабораторних робіт;*
- *семестровий рейтинг більше 30 балів.*

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Варіанти завдань для розрахункової роботи представлено у додатку А.
Перелік запитань, які виносяться на семестровий контроль представлено у додатку Б.

Робочу програму навчальної дисципліни (силабус):

Складено професор, д. т. н., проф., Терейковський Ігор Анатолійович

Ухвалено кафедрою системного програмування і спеціалізованих комп'ютерних систем

(протокол № 6 від 03.01.24)

Погоджено Методичною комісією факультету (протокол № 6 від 12.01.24)

ДОДАТОК А.

ВАРІАНТИ ЗАВДАНЬ ДЛЯ РОЗРАХУНКОВОЇ РОБОТИ

Варіант 1.
Настроїти систему захисту операційної системи.

Варіант 2.
Розробити додаткові компонентів захисту операційної системи.

Варіант 3.
Настроїти систему захисту електронної пошти від спаму.

Варіант 4.
Розробити систему захисту електронної пошти від спаму.

Варіант 5.
Настроїти мережевий екран.

Варіант 6.
Розробити додаткові компонентів захисту мережевих екранів.

Варіант 7.
Дослідити систему розповсюдження спаму, з метою виявлення їх вразливостей.

Варіант 8.
Дослідити мережеві сканери та розробити відповідну систему захисту.

Варіант 9.
Дослідити Dos та Ddos атаки та розробити систему захисту від них.

Варіант 10.
Дослідити особливості програмного забезпечення мобільних пристроїв.

Варіант 11.
Настроїти систему захисту СУБД.

Варіант 12.
Розробити додаткові компоненти захисту СУБД.

Варіант 13.
Розробити засоби захисту СУБД від SQL ін’єкцій.

Варіант 14.
Настроїти антивірусні засоби.

Варіант 15.
Розробити систему антивірусного захисту.

Варіант 16.
Настроїти систему захисту від кейлогерів.

Варіант 17.
Розробити компонент захисту від кейлогерів.

Варіант 18.
Настроїти захист віртуальної мережі.

Варіант 19.
Дослідити засоби зламу парольного захисту операційних систем та розробити відповідну систему захисту.

Варіант 20.
Розробити систему захисту офісних документів від несанкціонованого копіювання.

Варіант 21.
Настроїти систему захисту програм та даних від несанкціонованого розповсюдження.

Варіант 22.
Настроїти систему резервного копіювання інформації операційної системи.

Варіант 23.
Дослідити стійкість віртуальної машини Java від атаки на відмову в обслуговуванні.

Варіант 24.
Дослідити стійкість Framework від атаки на відмову в обслуговуванні.

Варіант 25.
Настроїти систему безпеки Веб-серверів.
Варіант 26.
Розробити додаткові модулі захисту Веб-серверів.
Варіант 27.
Дослідити засоби зламу захисту програм з метою розробки відповідних систем захисту.
Варіант 28.
Розробити систему захисту програм від вивчення.
Варіант 29.
Настроїти систему виявлення вторгнень.
Варіант 30.
Настроїти систему виявлення вразливостей.
Варіант 31.
Розробити систему виявлення вторгнень.
Варіант 32.
Розробити систему виявлення вразливостей.
Варіант 33.
Дослідити вразливості програмного забезпечення мобільних пристроїв з метою розробки системи їхнього захисту.

ДОДАТОК Б.

ЗАПИТАННЯ (ЗАДАЧІ) ДО ЗАЛІКУ

1. *Охарактеризуйте проблему захисту інформації в комп'ютерних системах.*
2. *Наведіть основні визначення в області захисту інформації.*
3. *Охарактеризуйте нормативне забезпечення системи технічного захисту інформації в Україні.*
4. *Охарактеризуйте нормативні документи системи криптографічного захисту інформації в Україні.*
5. *Охарактеризуйте зарубіжні та міжнародні стандарти щодо захисту інформації в комп'ютерних системах.*
6. *Охарактеризуйте загрози конфіденційності, цілісності, доступності.*
7. *Охарактеризуйте канали порушення безпеки інформації.*
8. *Охарактеризуйте політику безпеки інформації.*
9. *Охарактеризуйте комплекс засобів захисту і об'єкти комп'ютерної системи.*
10. *Що таке несанкціонований доступ?*
11. *Охарактеризуйте модель порушника.*
12. *Охарактеризуйте планування захисту і керування системою захисту.*
13. *Охарактеризуйте основні принципи керування доступом.*
14. *Охарактеризуйте послуги безпеки.*
15. *Охарактеризуйте загальні вимоги до засобів захисту інформації.*
16. *Охарактеризуйте економічні та технічні критерії оптимізації системи захисту інформації.*
17. *Охарактеризуйте поняття режиму захисту.*
18. *Охарактеризуйте особливості моделі загроз ресурсам ОС.*
19. *Охарактеризуйте основні функції підсистеми захисту ОС.*
20. *Охарактеризуйте типову структуру підсистеми безпеки ОС.*
21. *Охарактеризуйте керування доступом до ресурсів ОС.*
22. *Охарактеризуйте особливості забезпечення безпеки ресурсів ОС сімейств Windows.*
23. *Охарактеризуйте особливості забезпечення безпеки ресурсів ОС сімейств UNIX.*
24. *Охарактеризуйте причини, види, основні методи порушення конфіденційності в СУБД.*
25. *Охарактеризуйте методи захисту СУБД.*
26. *Охарактеризуйте типові загрози інформації офісних СУБД.*
27. *Охарактеризуйте особливості системи захисту офісних СУБД.*
28. *Охарактеризуйте типові загрози інформації промислових СУБД.*

29. Що таке руйнуючі програмні засоби?
30. Охарактеризуйте підходи до класифікація шкідливого програмного забезпечення.
31. Охарактеризуйте методи і засоби захисту програмного забезпечення.
32. Охарактеризуйте методи захисту програм від вивчення.
33. Охарактеризуйте типову архітектуру системи захисту програмного забезпечення.
34. Охарактеризуйте критерії оцінки ефективності систем захисту від шкідливого програмного забезпечення.
35. Охарактеризуйте системи антивірусного захисту провідних виробників.
36. Охарактеризуйте загальні положення про інформаційну безпеку мереж передачі даних.
37. Охарактеризуйте особливості моделі загроз мереж передачі даних.
38. Охарактеризуйте технологію міжмережних екранів.
39. Охарактеризуйте технологію віртуальних приватних мереж (ВПМ).
40. Охарактеризуйте особливості захисту мобільних програмних компонентів.
41. Охарактеризуйте особливості архітектури безпеки COM/DCOM, CORBA, ActiveX, Java, Flash Macromedia.
42. Охарактеризуйте типові загрози інформації комп'ютерної системи при використанні електронної пошти?
43. Охарактеризуйте методи захисту від несанкціонованої передачі даних?
44. Охарактеризуйте поняття спаму.
45. Охарактеризуйте основні методи захисту від спаму.
46. Охарактеризуйте методи захисту від спаму на основі чорного та білого списків.
47. Охарактеризуйте методи захисті від спаму на основі ключових словосполучень.
48. Охарактеризуйте метди захисту від спаму на основі байєсовської фільтрації.
49. Охарактеризуйте особливості сучасних спам-засобів.
50. Охарактеризуйте системи виявлення вторгнень.
51. Охарактеризуйте системи керування захищеністю.
52. Охарактеризуйте системи аналізу вразливостей.
53. Охарактеризуйте системи виявлення вторгнень.
54. Охарактеризуйте підходи до оптимізації параметрів систем розпізнавання атак та вразливостей?
55. Охарактеризуйте методологію побудови марківської моделі динаміки параметрів захисту.
56. Охарактеризуйте приклад створення марківської моделі оптимізації параметрів захисту Веб-серверу.
57. Що таке симетрична криптографія?
58. Охарактеризуйте методи шифрування заміною.
59. Охарактеризуйте методи шифрування перестановкою
60. Охарактеризуйте методи шифрування шляхом аналітичних перетворень.
61. Що таке крипто аналіз?
62. Охарактеризуйте принципи асиметричної криптографії?
63. Охарактеризуйте поняття цифрового підпису?
64. Охарактеризуйте поняття криптографічних протоколів.
65. Охарактеризуйте використання протоколу SSL для безпечного обміну інформацією в мережі.
66. Охарактеризуйте задачі захисту інформації, розв'язання яких потребує застосування методів штучного інтелекту.
67. Охарактеризуйте приклади використання нейронних мереж в задачах захисту інформації.