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

Кафедра штучного інтелекту

# КОМП'ЮТЕРНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

## Робоча програма навчальної дисципліни (Силабус)

| Реквізити навчальної дисципліни | |
|---|---|
| **Рівень вищої освіти** | ***Перший (бакалаврський)*** |
| **Галузь знань** | ***12 Інформаційні технології***[1] |
| **Спеціальність** | ***122 Комп'ютерні науки та інформаційні технології*** |
| **Освітня програма** | ***Системи і методи штучного інтелекту*** |
| **Статус дисципліни** | ***За вибором*** |
| **Форма навчання** | ***очна(денна)*** |
| **Рік підготовки, семестр** | ***4 курс, осінній семестр*** |
| **Обсяг дисципліни** | ***4 кредити (120 годин: лекції 36 годин, практичні заняття 18 годин, самостійна робота студентів 66 годин)*** |
| **Семестровий контроль/ контрольні заходи** | ***залік/модульна контрольна робота, роботи за матеріалом практичних занять*** |
| **Розклад занять** | ***тижневе навантаження: лекції- 2 години, практичні заняття – 1 година*** |
| **Мова викладання** | ***Українська*** |
| **Інформація про керівника курсу / викладачів** | Лектор: **к.т.н., доцент, Коваленко Анатолій Єпіфанович, an20kov@ukr.net** Практичні: **к.т.н., доцент, Коваленко Анатолій Єпіфанович, an20kov@ukr.net** |
| **Розміщення курсу** | https://ecampus.kpi.ua login.kpi.ua, zoom, Google classroom, e-mail, G suit for education Sikorsky |

## Програма навчальної дисципліни

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

Метою кредитного модуля є формування у студентів здатностей на основі загальних компетентностей (ЗК):

ЗК 1 Здатність застосовувати знання в практичних ситуаціях

ЗК 4 Здатність знати та розуміти предметну область і професійну діяльність

ЗК 11 Здатність генерувати нові ідеї (креативність)

Практичні здатності у процесі вивчення полягають у:

- здатності отримувати базові знання особливостей організації і застосування конкретних систем захисту інформації за відповідною довідковою інформацією;
- здатності аналізу студентом принципів побудови сучасних систем захисту інформації з метою їх подальшого вибору і застосування;
- здатності використовувати засоби захисту даних на основі визначення відповідних прав доступу до файлів і низки програм криптографічних алгоритмів;
- здатності виконувати обробку, фільтрацію і захист потоків даних і процесів у комп'ютері під керуванням механізмів захисту системи;

Основою для досягнення мети кредитного модуля є використання аудиторних лекційних занять для отримання базових знань з дисципліни, самостійна робота студентів (СРС) по засвоєнню матеріалу лекційного курсу, аудиторних практичних занять, які передбачають активну

[1]

роботу студентів через виконання індивідуальних завдань і СРС з підготовки необхідних матеріалів звіту з практичних завдань.

Згідно з вимогами програми навчальної дисципліни студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання**: знання**:

- основні поняття захисту інформації;
- основні принципи побудови систем захисту інформації;
- особливості фільтрації даних на різних протокольних рівнях захищеної системи;
- особливості розробки політик безпеки;
- основи використання криптосистем та антивірусних програм;
- можливості системних засобів захисту даних сучасних операційних систем;
- визначати потенційні джерела здійснення мережевих атак і напрямків їх нейтралізації;
- особливості архітектури і захисту інформації електронних платіжних систем

**уміння** за програмними результатами навчання за компонентами освітньо-професійної програми передбачено виконання критерію УМ8 Вміти застосовувати на практиці системи захисту інформації та інформаційні системи і включає складові практичних умінь:

- проводити визначення основних загроз безпеці системи;
- використовувати розмежування доступу і автентифікацію для забезпечення безпеки інформації на основі використання системних засобів операційних систем;
- використовувати засоби взаємної автентифікації на основі сертифікатів;
- створювати і використовувати каталоги і файли з різними атрибутами доступу;
- розробляти мероприємства політики безпеки по виявленню і усуненню наслідків здійснення атак;
- застосовувати системні програмні засоби захисту інформації.

Для активізації самостійної роботи студентів розроблене положення про рейтингову систему оцінки успішності студентів з нарахуванням додаткових балів за активну роботу у семестрі.

Внаслідок вивчення курсу студент повинен бути здатний продемонструвати такий програмний результат навчання ОПП: ПР 13 Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування систем захисту інформації комп'ютерних мереж та їх програмного забезпечення.

## 2. Пререквізити та постреквізити дисципліни

Забезпечуючими дисциплінами є «Дискретна математика», "Математична логіка і теорія алгоритмів", «Методи штучного інтелекту», «Операційні системи».

## 3. Зміст навчальної дисципліни

1 ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Визначення інформації. Властивості інформації. Цінність інформації. Достовірність, актуальність інформації. Властивості які підлягають захисту. Властивості конфіденційності, цілісності, доступності, спостережності. Оцінка ризиків порушення безпеки інформації. Джерела порушення безпеки. Аналіз факторів виникнення загроз безпеки інформації. Інформаційні системи. Інформаційна безпека автоматиованих систем оброблки даних. Завдання захисту інформації. Основні задачі, які повинні вирішуватися системою комп'ютерної безпеки. Засоби інформаційного впливу. Класифікація загроз безпеці інформації комп'ютерних систем. Основні види загроз безпеці інформації у комп'ютерних мережах. Характеристика загроз. Характеристика атак. Найбільш поширені атаки на IP мережі.

2 ПОЛІТИКИ БЕЗПЕКИ

Класифікація основних засобів протидії загрозам безпеки. Поняття про інформацію з обмеженим доступом. Визначення конфіденційності і цілісності інформації. Загрози безпеці за об'єктом впливу. Основні типи загроз та боротьба з ними. Структура політики безпеки та її основні частини. Визначення політики безпеки. Фрагментарний і комплексний підходи. Види політики безпеки. Вибіркова (дискреційна) і повноважна (мандатна) політики безпеки. Створення політики безпеки. Етапи програми забезпечення безпеки та основні вимоги. Схема розробки політики безпеки. Визначення рольових функцій. Політика аудиту. Спеціалізовані політики. Механізми захисту інформації у мережах. Комплексний підхід забезпечення інформаційної безпеки. Підтримка політик безпеки в мережах.

3 НОРМАТИВНО-ПРАВОВОВІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

Розділи політики безпеки. Розробка профілю захисту і проекту безпеки об'єкта. Стандарт ISO/IEC 15408. Порядок розробки профілю захисту і проекту забезпечення безпеки. Структура і зміст профілю захисту. Розмежування прав доступу. Стандарт ORANGE BOOK (TCSEC). Основні принципи побудови безпечних систем. Типи вимог безпеки стандарту ISO/IES 15408. Функціональні вимоги. Елементарні сервіси безпеки FAU, FIA, FRU. Сервіси, похідні від елементарних FCO, FPR, FDP, FPT. Вимоги до інфраструктури системи FCS, FMT, FTA, FTP. Сімейства класів FAU, FIA, FRU. Сімейства вимоги гарантій безпеки APE, ASE. Вимоги довіри до етапу розробки ALC, AGD, ATE. Вимоги до оцінки вразливостей класу AVA. Вимоги до постачання та експлуатації класу ADO. Клас AMA (вимоги до підтримки довіри). Рівні оцінки довіри "Загальних критеріїв". Нормативний документ критеріїв НД ТЗІ 2.5-004-99.

4 АНАЛІЗ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ

Оцінка ризиків порушення безпеки інформації. Аналіз факторів виникнення загроз безпеки інформації. Засоби інформаційного впливу. Класифікація загроз безпеці інформації комп'ютерних систем. Основні види загроз безпеці інформації у комп'ютерних мережах. Атаки на IP- мережі і засоби захисту. Характеристика атак. Підслуховування. Аналіз мережного трафіка. Підміна довіреної особи. Посередництво в обміні незашифрованими ключами. Перехоплення сеансу. Відмова в обслуговуванні. Парольні атаки. Атаки на рівні додатків. Мережна розвідка. Зловживання довірою. Комп'ютерні віруси і програми типу «троянський кінь».

5 МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ

Створення політики безпеки. Основні етапи створення політики безпеки. Визначення рольових функцій. Спеціалізовані політики. Адміністративно-організаційна модель керування безпекою. Механізми захисту інформації у мережах. Підтримка політик безпеки в мережах. Застосування механізмів ідентифікації та автентифікації. Поняття ідентифікації, автентифікації та авторизації. Рівні доступу і процеси автентифікації. Рівні безпеки і характеристики процесів автентифікації. Механізми запобігання атак у мережах. Біометрична ідентифікація і автентифікація. Комплексне застосування механізмів захисту.

6 РЕАЛІЗАЦІЯ ПОЛІТИКИ БЕЗПЕКА ЗАСОБАМИ ОПЕРАЦІЙНИХ СИСТЕМ

Загальні принципи застосування операційних систем. Засоби безпеки операційних систем Windows. Система безпеки Windows NT. Налагодження безпеки у клієнтському середовищі. Засоби безпеки систем сім'ї UNIX.

7 ВСТУП ДО КРИПТОЛОГІЇ

Криптографічний захист даних. Криптосистеми шифрування. Характеристика симетричних криптосистем. Обмін секретними ключами у глобальних мережах. Характеристика асиметричних систем. Методи криптографічної автентифікації. Проста автентифікація. Застосування односторонніх функцій. Форми подання об'єктів користувача. Схеми ідентифікації і автентифікації. Взаємна перевірка справжності користувачів. Схема неперервної перевірки справжності користувачів. Керування криптографічними ключами. Генерування ключів. Зберігання ключів. Ієрархія ключів. Схеми генерування ключів. Розподілення ключів. Взаємодія з центром розподілення ключів. Обмін секретними ключами.

8 СИМЕТРИЧНІ ШИФРОСИСТЕМИ

Симетричні шифри. Перетворення у симетричних алгоритмах шифрування. Мережі Фейстеля. Алгоритм DES. Загальна характеристика. Схема шифрування DES. Схема утворення функції f. Генерування ключів. Дешифрування тексту в DES. Режими використання DES. Режим електронної кодової книги ECB. Режим зчеплення блоків CBC. Режим зворотного зв'язку за

шифротекстом CFB. Режим зворотного зв'язку за виходом OFB. Порівняння режимів DES. Алгоритм Triple DES. Алгоритм AES. Алгоритм IDEA. Загальна характеристика. Схема шифрування. Апаратні реалізації алгоритму IDEA. Алгоритм Blowfish. Алгоритм Twofish.

9 ПОТОКОВІ СИМЕТРИЧНІ АЛГОРИТМИ ШИФРУВАННЯ

Принципи роботи потокових криптосистем. Операції та засоби реалізації потокових шифрів. Реалізація нелінійних функцій. Алгоритм RC4. Алгоритм A5. Алгоритм Phelix. Алгоритм Rabbit. Алгоритми SOBER. Алгоритм Trivium. Алгоритми VEST. Порівняння потокових алгоритмів

10 АСИМЕТРИЧНІ КРИПТОСИСТЕМИ

Типи асиметричних криптосистем. Алгоритми RSA, DH. Основні перетворення. Вимоги до розрядності ключів. Основні принципи застосування. Області застосування асиметричних криптосистем. Алгоритм Ель-Гамаля.

11 ЗАХИСТ ІНФОРМАЦІЇ У ВІДМОВОСТІЙКИХ РОЗПОДІЛЕНИХ СИСТЕМАХ

Системне діагностування відмовостійких систем. Принципи захисту інформації розподілених мобільних систем. Моніторинг і аналіз стану розподілених систем. Моделі системного діагностування. Інтегрована модель процесів діагностування. Особливості подій взаємодіючих процесів. Протоколи процесів системного діагностування і відновлення інформації. Захист інформації розподілених інформаційних систем.

12 ЕЛЕКТРОННІ ПЛАТІЖНІ СИСТЕМИ

Основні характеристики електронних платіжних систем. Аналіз безпеки електронних платіжних систем. Пластикові картки. Загальна характеристика. Картки з магнітною полосою. Смарт- карти. Формування персонального PIN-коду. Системи POS. Загальна схема розрахунку з використанням систем POS. Вимоги до захисту систем POS. Метод виведеного ключа. Метод ключа транзакцій. Метод відкритих ключів. Будова банкомата. Програмне забезпечення банкоматів. Функціонування банкоматів у режимі on-line. Порівняння режимів роботи банкоматів. Захист повідомлень PIN-кодів. Захист каналів передавання даних. Порядок обміну даними між банками.

13 АРХІТЕКТУРИ ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ

Універсальна платіжна система UEPS. Загальна характеристика UEPS. Загальна архітектура UEPS. Структура карт платіжної системи.. Цикл платіжної транзакції. Процедура емісії карт. Сучасні платіжні системи та їх захист.

14 МІЖМЕРЕЖНІ ЕКРАНИ

Загальна структура. Класифікація міжмережних екранів. Безпека міжмережних екранів. Захист на мережному рівні. Протокольні реалізації. Склад міжмережних екранів. Фільтрація пакетів даних. Шлюз сеансового рівня. Екрануючий шлюз. Шлюзи експертного рівня. Реалізації міжмережних екранів. Тунелювання потоків даних у мережах. Тунелювання у мережах VPN.

15 ПРОТОКОЛИ СТРОГОЇ АВТЕНТИФІКАЦІЇ

Загальна характеристика. Протокол Kerberos. Характеристика протоколу Kerberos. Система Kerberos. Послідовність виконання операцій протоколу Kerberos.

16 ПРОТОКОЛИ ЗАХИЩЕНОЇ ВЗАЄМОДІЇ МЕРЕЖНИХ СИСТЕМ

Протокол SSH. Загальна характеристика протоколу SSH. Взаємодія клієнта і сервера SSH. Особливості безпеки застосування SSH. Підключення до SSH – сервера. Протоколи SSL, TLS. Загальна характеристика протоколів SSL, TLS. Цілі застосування протоколів SSL, TLS. Автентифікація у протоколах SSL, TLS. Взаємодія клієнта і сервера SSL. Особливості застосування SSL. Застосування SSL в HTTPS, IPSec, VPN. Застосування NTLM.

17 СПЕЦІЛІЗОВАНИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

Загальна характеристика засобів забезпечення захисту Класифікація систем IDS Класифікація антивірусних програм Системи NIDS Системи HIDS Системи PIDS Системи VMIDS Системи захисту на основі модулів PAM Системи захисту з використанням протоколів Протоколи RADIUS Протоколи DIAMETER Модулі автентифікації. Модулі PAM.

18 СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇЇ НА ОСНОВІ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Моделі штучного інтелекту при фільтрації даних Системи IDES Алгоритми фільтрації і розпізнавання атак Програмна підтримка правил прийняття рішень Програмна підтримка правил прийняття рішень.Використання програмних засобів операційних систем. Пакет OPENSSL..

## 4. Навчальні матеріали та ресурси

### Базова література


1. .Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов,С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
2. Коваленко А.Є. Сучасні криптографічні засоби систем захисту інформації : навчально-методичний посібник із самостійної роботи студентів / Уклад. А.Є.Коваленко.- К.:НТУУ «КПІ» ННК «ІПСА», 2012.-119 с. (НТБ ім. Г.І. Денисенка)
3. Коваленко А.Є. Операційні системи : навч. посібн. / Коваленко А.Є. – К.: НТУУ «КПІ», 2010. – 248 с. (НТБ ім. Г.І. Денисенка)
4. Коваленко А.Є. Розподілені інформаційні системи : навч. посібн / Коваленко А.Є. – К.: НТУУ «КПІ», 2008 - 244с.с. (НТБ ім. Г.І. Денисенка)


### Допоміжна література


5. Антонюк А.О. Основи захисту інформації в автоматизованих системах.—К.:»КМ Академія». 2003.—244 с.
6. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. —НД ТЗІ 1.1-001-98, ДСТСЗІ СБ України, Київ, 1998.
7. Закон України про захист інформації в автоматизованих системах, від 05.07.94.
8. Tanenbaum Andrew S. Modern operating systems / Tanenbaum Andrew S., Herbert Bos.-4-th ed.-Upeer Saddle River, New Jersey.: Prentice- Hall, 2015.
9. Stallings W. Operating systems: internals and design principles.- 8-th ed.-Upeer Saddle River, New Jersey.: Prentice- Hall, 2015.-800 p.
10. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с. http://ir.polissiauniver.edu.ua/bitstream/123456789/3073/1/Zahyst_informacii_ASU.PDF


**Навчальний контент**

## 5. Методика опанування навчальної дисципліни

В результаті вивчення дисципліни " КОМП'ЮТЕРНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА " студенти повинні знати: основні поняття захисту інформації; основні принципи побудови систем захисту інформації; особливості фільтрації даних на різних протокольних рівнях захищеної системи; особливості розробки політик безпеки; основи використання криптосистем та антивірусних програм; можливості системних засобів захисту даних сучасних операційних систем; визначати потенційні джерела здійснення мережевих атак і напрямків їх нейтралізації; особливості архітектури і захисту інформації електронних платіжних систем

Для отримання знань і оволодіння необхідними уміннями передбачено проведення контрольних робіт і виконання індивідуальних завдань.

Для активізації самостійної роботи студентів застосвують рейтингову систему оцінки успішності студентів з нарахуванням додаткових балів за активну роботу у семестрі. Кожний студент отримує свій підсумковий рейтинг з дисципліни. Якщо цей рейтинг його задовольняє, то він отримує залік «автоматом».

Для виконання самостійної роботи студент використовує навчальні посібники, які зберігаються у бібліотеці ІПСА, в комп'ютерній мережі кафедри ММСА, та на сайті кампусу НТУУ «КПІ ім. Ігоря Сікорського» та в ресурсах Інтернет.

Приблизний перелік завдань практичних занять включає вивчення і засвоєння наступних питань

Розробка криптографічних засобів захисту інформації.

Використання системних програмних засобів для реалізації політики безпеки.

Спеціалізовані системи захисту інформації.

Криптоаналіз сучасних криптосистем розподілених систем.

Дослідження моделей системного діагностування систем захисту інформації

Розробка політики безпеки корпоративної мережі організації

Використання сертифікатів у системах захисту з відкритими ключами

Форма організації їх засвоєння може передбачати кілька індивідуальних завдань у межах кожної роботи..

Виконання циклу робіт пратичних занять забезпечує формування практичного досвіду розробки , створення командних файлів, налагодження і застосування програмного забезпечення керування ресурсами і захисту інформації.

## 6. Самостійна робота студента

Метою індивідуальних семестрових завдань є опрацювання тем лекційного курсу, та тем, винесених на самостійну роботу студентів.. Методичні вказівки зберігаються на сайті кампуса НТУУ «КПІ ім.. Ігоря Сікорського».

На самостійну роботу студентів винесено підготовку до виконання контрольних робіт, залікової контрольної роботи, розв'язання типових задач.

У семестрі проводять одну модульну контрольну роботу.

Критерії оцінювання для кожної роботи визначаються складністю задач і завдань в межах сумарного вагового балу.

Варіанти модульної контрольної роботи відповідають тематиці лекційного курсу та індивідуальним завданням практичних занять. Форму проведення контрольної роботи (зокрема, у письмовому вигляді, за тестами) визначає викладач за тиждень до її проведення..

## Політика та контроль

### 7. Політика навчальної дисципліни (освітнього компонента)

Рейтинг студента з дисципліни складається з балів, які він отримує за:

1) Виконання однієї модульної контрольної роботи
2) виконання та захист трьох робіт за тематикою практичних занять.

До загального рейтингу можуть додаватись бали, отримані за необов'язкові складові.

Система вимог, які викладач ставить перед студентом, визначається системою РСО.

Одному або двом кращим студентам може додаватись 1 заохочувальний бал за оригінальні нестандартні розв'язки задач підвищеної складності під час занять.

До необов'язкових складових віднесено:

- участь у модернізації індивідуальних завдань практичних занять:
- доповіді на наукових студентських семінарах, конференціях, якщо робота мала відношення до теорії інформації і кодування;

За їх виконання студент може отримати до 10 заохочувальних балів ( у межах максимального числа 10 заохочувальних балів на повний рейтинг 100 балів).

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

Варіанти контрольних робіт передбачають теоретичні питання і індивідуальні задачі практичних занять та поточних тем лекційного курсу.

Залікова контрольна робота дозволяє отримати залік або покращити рейтинг, отриманий протягом семестру. Кількість завдань і критерії оцінювання залікової контрольної роботи визначаються в межах навчального матеріалу всього навчального курсу.

**Система рейтингових балів**

Рейтинг студента з кредитного модуля складається з балів, які він отримує за:

1. Виконання однієї модульної контрольної роботи.
2. Виконання трьох робіт практичних занять

До загального рейтингу можуть додаватись бали, отримані за необов'язкові складові.

1. Модульна контрольна робота.
   - «відмінно», повна відповідь (не менше 90% потрібної інформації) – 36-40 балів;
   - «добре», достатньо повна відповідь (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 30-35 балів;
   - «задовільно», неповна відповідь (не менше 60% потрібної інформації) та незначні помилки – 24-29 балів;
   - «незадовільно», незадовільна відповідь (не відповідає вимогам на «задовільно») – 0 балів
2. виконання та захист вправ і завдань практичних занять (ЗПЗ):
   - «відмінно», коректне повне, вчасне виконання індивідуальних вправ ЗПЗ, правильне та своєчасне оформлення вправ ЗПЗ, демонстрація вільного володіння теоретичним матеріалом при захисті виконаних вправ ЗПЗ і самостійне виконання завдання (не менше 90% потрібної інформації) 18-20 балів;
   - «добре», коректне повне, вчасне виконання індивідуальних вправ ЗПЗ, правильне та своєчасне оформлення вправ ЗПЗ, демонстрація вільного володіння теоретичним матеріалом при захисті виконаних вправ ЗПЗ і самостійне виконання завдання з можливими незначними неточностями і зауваженнями (не менше 75% потрібної інформації) - 15-17 балів;
   - «задовільно», неповна відповідь, невчасне або зі значними неточностями виконання індивідуальних вправ ЗПЗ з підготовки і виконання, відповідь на половину питань з теми роботи під час захисту ЗПЗ (не менше 60% потрібної інформації)– 12-14 балів;
   - «незадовільно», незадовільна відповідь (не відповідає вимогам на бали «задовільно») – 0 балів

Одному або двом кращим студентам можуть додаватися 1 заохочувальний бал за оригінальні нестандартні розв'язки задач підвищеної складності під час занять.

До необов'язкових складових віднесено:

- участь у модернізації завдань практичних занять:
- доповіді на наукових студентських семінарах, конференціях, якщо робота мала відношення до теорії інформації і кодуванню.

За їх виконання студент може отримати до 10 заохочувальних балів ( у межах максимального числа 10 заохочувальних балів на повний рейтинг 100 балів).

За результатами роботи за перші 7 тижнів студент може набрати до 39 балів. На першій атестації (8-й тиждень) студент отримує зараховано, якщо його поточний рейтинг балів не менше 19 балів.

За результатами роботи за перші 13 тижнів студент може набрати до 72 балів. На другій атестації (13-й тиждень) студент отримує зараховано, якщо його поточний рейтинг балів не менше 36 балів.

Рейтингова оцінка ( $RD$ ) з кредитного модуля, семестрова атестація з якого передбачена у вигляді заліку, формується як сума всіх рейтингових балів $r_K$ , а також заохочувальних $r_З$

$$RD = \sum_k r_K + \sum_k r_Ç$$

Максимальна сума балів складає 100 балів. Необхідною умовою допуску до заліку є 40 балів рейтингу за умови виконання ЗПЗ.

Для отримання заліку з кредитного модуля «автоматом» потрібно мати рейтинг не менше 60 балів. Необхідною умовою допуску до заліку є не менше 40 балів рейтингу.

Студенти, які мають наприкінці семестру рейтинг менше 60 балів, а також ті, хто хоче підвищити оцінку в системі ECTS, виконують залікову контрольну роботу. При цьому до балів за ЗПЗ ($r_{зпз}$) додають бали за контрольну роботу і ця рейтингова оцінка є остаточною.

Завдання контрольної роботи складається з трьох питань різних розділів робочої програми із наданого переліку до засвоєння кредитного модуля. Кожне питання контрольної роботи $r_1, r_2. r_3$ оцінюється у 13 балів відповідно до системи оцінювання:

– «відмінно», повна відповідь (не менше 90% потрібної інформації) – 12-13 балів;

– «добре», достатньо повна відповідь (не менше 75% потрібної інформації або незначні неточності) – 10-11- балів;

– «задовільно», неповна відповідь (не менше 60% потрібної інформації та деякі помилки) – 8-9 балів;

– «незадовільно», незадовільна відповідь – 0 балів.

Сума балів за кожне з трьох запитань контрольної роботи та сумарний бал за виконані усіх ЗПЗ переводиться до залікової оцінки згідно з таблицею.

| **Рейтингові бали,** $RD$ **RD= $r_{зпз}$ + $r_1$ + $r_2$ + $r_3$** | **Оцінка за університетською шкалою** |
|---|---|
| 95-100 | Відмінно |
| 85-94 | Дуже добре |
| 75-84 | Добре |
| 65-74 | Задовільно |
| 60-64 | Достатньо |
| Менше 60 | Не зараховано |
| Менше 40 | Не допущено |

Складено
доцентом кафедри ММСА, к.т.н., доц. Коваленко Анатолієм Єпіфановичем

Ухвалено кафедрою кафедрою штучного інтелекту (протокол № 14 від 24.05.2023)
Погоджено Методичною комісією ННІПСА (протокол № 4 від 16.06.2023)

**Питання до модульної контрольної роботи**

1. Предмет захисту даних в комп'ютерних системах і мережах
2. Передумови забезпечення безпеки систем оброблення даних.
3. Поняття конфіденційності інформації.
4. Поняття цілісності інформації.
5. Основні шляхи реалізації загроз безпеці системи та типи загроз.
6. Основні умисні загрози банківським системам.
7. Загрози безпеці системам і мережам.
8. Ризики. і оцінка втрат
9. Модель порушника безпеки
10. Властивості інформації: цінність інформації.
11. Властивості інформації: вибірковість інформації.
12. Властивості інформації: достовірність інформації.
13. Поняття перехоплення сеансу, відмови в обслуговуванні, парольної атаки та засоби
14. Аналіз факторів порушення безпеки інформації
15. Класифікація загроз безпеці інформації комп'ютерних систем
16. Основні види загроз безпеці інформації у комп'ютерних мережах
17. Атаки на IP мережі і засоби захисту. Форми реалізації. Засоби протидії.
18. Підслуховування (sniffing - сніфінг), Форми реалізації. Засоби протидії.
19. IP- спуфінг Форми реалізації. Засоби протидії.
20. Парольні атаки Форми реалізації. Засоби протидії.
21. Мережна розвідка Форми реалізації. Засоби протидії.
22. Зловживання довірою Форми реалізації. Засоби протидії.
23. Визначення політики безпеки
24. Основні етапи створення політики безпеки
25. Визначення рольових функцій
26. Спеціалізовані політики
27. Адміністративно-організаційна модель керування безпекою
28. Механізми захисту інформації у мережах
29. Підтримка політик безпеки в мережах
30. Поняття ідентифікації, автентифікації та авторизації
31. . Рівні доступу і процеси автентифікації
32. Рівні безпеки і характеристики процесів автентифікації
33. Механізми запобігання атак у мережах
34. Біометрична ідентифікація і автентифікація
35. Комплексне застосування механізмів захисту
36. Архітектура і застосування протоколу IPSec.
37. Протокол Kerberos. Система Kerberos
38. Порядок формування повідомлень у системі Kerberos
39. Технології міжмережних екранів. Класифікації.
40. Схеми мережного захисту на базі міжмережних екранів.
41. Основні дії фільтрів міжмережних екранів і критерії фільтрації.
42. Функції між мережної резидентної програми. Основні проблеми застосування міжмережних екранів.
43. Екрани рівнів OSI ISO. Поля фільтрації.
44. Загальна схема фільтрації пакетів у екрануючому маршрутизаторі. Переваги і недоліки екрануючих маршрутизаторів.
45. Призначення і схема функціонування шлюзу сеансового рівня. Порядок роботи. Переваги і недоліки.
46. Основні функції і схема екрануючого шлюзу. Схема функціонування прикладного шлюзу і функції посередників.
47. Основні параметри, переваги і недоліки використання шлюзу прикладного рівня. Принципи роботи шлюзу експертного рівня.
48. Основні функції, переваги і недоліки застосування шлюзів експертного рівня.

49. Тунелювання потоків даних у мережах. Формат пакету. Тунелювання у мережах VPN
50. Основні типи вірусів, приклади, механізми дії
51. Шляхи проникнення і ознаки появи вірусу у комп'ютер
52. Антивірусні засоби. Детектори. Фаги.
53. Антивірусні засоби. Ревізори. Сканери.
54. Антивірусні засоби. Монітори. Вакцини.
55. Порівняльний аналіз антивірусних програм.
56. Визначити поняття: критпологія, криптографія, стеганографія, криптоаналіз.
57. Описати особливості асиметричних криптосистем
58. Основні вимоги до асиметричної системи, визначені Діффі і Хеллманом для забеспечення безпеки
59. Схема простої автентифікації на основі багаторазових паролів
60. Описати сутність метода збереження і передачі паролів з використанням односторонніх функцій.
61. Описати процедуру рукостискання взаємної автентифікації
62. Що таке мережі Фейстеля ? В чому полягає зворотне перетворення Фейстеля. Описати схему шифрування DES
63. Понятт, загальна структура іпринципи функціонування електронних платіжних систем.
64. Роль банків емітентів і еквайерів. Взаємодія через процесинговий центр.
65. Проблеми, які виникають при застосування електронних платіжних систем і основні механізми їх захисту.
66. Електронні пластикові карти. Активні і пасивні картки.
67. Смарт-карти. Будова і основні характеристистики апаратури і програмного забезпечення.
68. Персональний ідентифікаційний номер PIN. Способи формування пін-коду.
69. Взаємодія і забезпечення безпеки платіжних систем з POS.
70. Схема системи POS. Основні вимоги до захисту.
71. Безпека банкоматів. Робота в режимах on-line та off-line
72. Режими роботи банкоматів. Структура повідомлень банкомата і банка.
73. Схема проходження даних про PIN клієнта до банка.
74. Ключі і коди шифрування і дешифрування повідомлень у платіжних системах.
75. Універсальна платіжна система UEPS. Архітектура, типи карток.
76. Функції центру емісії системи UEPS.
77. Структура карт системи UEPS. Ключі

**Додаток А**

## Перелік теоретичних контрольних питань.

1. Призначення операційної системи Передумови створення операційних систем
2. Оболонки операційних систем
3 Класифікація редакторів операційних систем
4. Текстові рядкові редактори Потокові редактори і процесори
5. Машинні мови . Платформи машинних мов. Мови асемблера
6. Принципи класифікації операційних систем
7. Серверні операційні системи. Мультипроцесорні операційні системи
8. Операційні системи персональних комп'ютерів
9. Операційні системи долоневих комп'ютерів Вбудовані операційні системи
10. Сенсорні операційні системи
11. Операційні системи реального часу Операційні системи смарткарток
12. Режим пакетного оброблення даних Режим багатозадачного оброблення даних
13. Моделі операційних систем Монолітні системи
14. Моделі операційних систем Багаторівневі системи
15. Моделі операційних систем Віртуальні машини
16. Моделі операційних систем Системи за моделлю клієнт  сервер
17. Поняття процесуУмови створення процесу
18. Концепція потоків Основні переваги потоків
19. Класифікація процесів Класифікація процесів за часом розвитку
20. Класифікація процесів за місцем реалізації
21. Класифікація процесів за способами зв'язків процесів
22. Функції ядра Типи переривань
23. Архітектура ядра операційної системи BSD
24. Керування файловою системою
25. Керування взаємодією оперативної і зовнішньої пам'яті
26. Оброблення апаратних та емульованих переривань
27. Операційні системи Unix, BSD, Linux
28. Особливості розвитку Linux. Версії Linux
29. Інтерфейси користувача і оболонки за стандартом POSIX 1003.2
30. Передумови створення операційних систем WINDOWS 9x
31. Операційні системи WINDOWS NT
32. Модель операційної системи Windows NT Windows NT Server
33. Робочі і доменні групи Windows NT Server
34. ОПЕРАЦІЙНІ СИСТЕМИ Windows 10 Загальна характеристика Версії
35. Архітектура ядра Windows 8
36. Основні характеристики WindowsServer 2016
37. ОПЕРАЦІЙНІ СИСТЕМИ BSD Загальні відомості та історія створення
38. Версії BSD Версія Ghost BSD Версії BSD Free BSD
39. Загальна характеристика Chrome OS Етапи розвитку Chrome OS
40. ОПЕРАЦІЙНІ СИСТЕМИ LINUX MINT Версії Linux Mint
41. ОПЕРАЦІЙНІ СИСТЕМИ WINDOWS CE Загальна характеристика
42. Архітектура Windows CE 8.Системні виклики API Windows CE 8.0
43. Загальна характеристика Android Призначення Android
44. Android 9.0 Pie Основні відмінності від попередніх версій Ядро та архітектура
45. Android 8.0 Oreo Загальна характеристика і архітектура
46. ОПЕРАЦІЙНІ СИСТЕМИ DARWIN Загальна характеристика і застосування
47. ОПЕРАЦІЙНА СИСТЕМА MAC OS X Загальна Ядро XNU
48. Ядро Mach Версії Mac OS X
49. ОПЕРАЦІЙНІ СИСТЕМИ IOS Загальна характеристика iOS

50. Операційні системи iPhone OS Операційні системи iOS
51. Архітектура операційної системи iOS 11.x.
52. ОБОЛОНКИ UNIX – ПОДІБНИХ ОПЕРАЦІЙНИХ СИСТЕМ Типові команди
53. Системні каталоги UNIX Системні виклики при роботі з каталогами
54. Системні виклики при роботі з процесами UNIX
55. Оболонка Bash Загальна характеристика
56. Синтаксис Bash Версії Bash Команди Bash Скрипти для Bash
57. Характеристики Windows PowerShell Командлети PowerShell
58. PowerShell для Windows Server 2016 Системні функції
59. Особливості організації і виконання ріре у PowerShell.
60. Програмування, скрипти і функції PowerShell.
61. Якими є основні і додаткові стани процесу ?
62. Як описують життєвий цикл процесу за допомогою діаграм станів ? Приклад.
63. Якими є основні типи зв'язків процесів під час їх взаємодії ?
64. Як описують основні проблеми синхронізації процесів ?
65. Якими є основні умови сумісного використання ресурсів процесами?
66.Як використовують примітиви sleep, wakeup у реалізації проблеми «виробник-споживач»?
67. Як виникають стани одночасного очікування у програмній реалізації проблеми «виробник-споживач» при застосуванні примітивів sleep, wakeup?
68. Якими є недоліки активного очікування процесів ?
69. Що таке мютекс і яким є мехінізм використання його процедур ?
70. Що таке монітор і як його реалізують ?
71. Як виконується взаємодія процесів через повідомлення із застосуванням send, receive ?
72. Які є способи передавання повідомлень у разі взаємодії процесів?
73. В чому полягають дві схеми організації скриньок для проблеми "виробник-споживач" ?
74. Якими є умови виникнення взаємного блокування процесів ?
75. Що описують вершини і ребра графової моделі Холта ?
76. Як визначають види процесів з обмеженими можливостями ? Які процеси домінують і чому ?
77. Описати ситуації прийняття рішень при плануванні процесів. У чому полягають відмінності планування для пріоритетних і непріоритетних алгоритмів ?
78. Як розрізняють середовища планування за вимогами ?
79. Якими є спільні вимоги планування для всіх середовищ ?
80. Описати рівні трирівневого планування і для яких середовищ їх застосовують?
81. Яку моделі планування і які алгоритми застосовують для інтерактивних систем ?
82. Чим відрізняється реалізація планування в системах реального часу? За якими критеріями воно виконується ? Які алгоритми застосовують ?
84. Як побудована ієрархія пам'яті в комп'ютері ?
85. Що лежить в основі поняття «підкачування» і «віртуальної» пам'яті? Роль ущільнення.
86. Описати схеми розподілу пам'яті багатозадачних систем зі стеками і переваги.
87. Які застосовують принципи перетворення віртуальної адреси у фізичну застосовують?
88. Як здійснюється функціонування MMU?
89. Порівняти особливості однорівневої і багаторівневої таблиці сторінок. Структура запису таблиці сторінок.
90. В чому полягає поняття сегментації? Переваги і недоліки сегментації.
91. В чому полягають відмінності віртуальної пам'яті і сегментації?
92. Для яких цілей застосовують буфер TLB та асоціативну пам'ять?
93. Призначення і будова селектора, таблиць LDT, GDT Pentium?
94. Описати структуру дескриптора таблиці дескрипторів.
95. Яка схема формування лінійної адреси Pentium?
96. Яка структура фізичної лінійної адреси Pentium?
97. Які рівні захисту застосовують при використанні Pentium? Принципи доступу процесів до даних різних рівнів.
98. У чому полягають відмінності між блочними і символьними пристроями?. Як виконується доступ до пристрою?

99. Що собою являють контролери прямого доступу до памяті? Описати послідовність керування роботою контролера DMA.
100. Дати поняття семафора і характеристику його операцій.
101. Програмне забезпечення пристроїв введення/виведення.
102. Організація підсистеми введення/виведення. Універсальні інтерфейси введення виведення.
103. Способи буферування даних.
104. Методи і засоби захисту.
105. Методи ідентифікації і автентифікації.
106. Криптографічний захист даних. Політики безпеки .
107. Рівні захисту операційних систем.
108. Засоби безпеки операційних систем Windows NT.
109. Засоби безпеки операційних систем сімейства UNIX.
110. Засоби захисту файлів операційних систем сімейства UNIX.
111. Політики безпеки UNIX.
112. Засоби безпеки UNIX. Програмне забезпечення шифрування і дешифрування даних.
113. Будова каталогів файлових систем. Атрибути файлів.
114. Файлові системи Ext2, ext3, ext4, Reizer ОС Linux.
115. Мережна файлова система NFS.
116. Файлові системи операційних систем WINDOWS.
117. Система NTFS.
118. Файлова система ISO 9660 та її модифікації.
119. Підходи до оцінки продуктивності операційних систем. Моделі оцінки продуктивності.
120. Поняття відмово стійкості. Надійність і відмовостійкість систем.
121. Відмовостійкість процесів.
122. Виявлення непрацездатних станів і моделі системного діагностування відмовостійких систем.
123. Планування процесів у мультимедійних системах. Кодування звуку і зображень. Ущільнення відеоінформації.
124. Алгоритми планування реального часу мультимедійних систем.
125. Процеси розподілених систем. Потоки виконання.
126. Процеси клієнтів і серверів.
127. Перенесення коду. Програмні агенти.
128. Синхронізація процесів. Синхронізація годинників.
129. Логічні годинники. Глобальний стан. Алгоритми голосування.
130. Розподілені файлові системи Система CODA.
131. Система PLAN 9.
132. Файлова система xFS. Захищена файлова система SFS.
133. Система Lotus Notes.