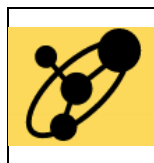


30 лекцій



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



Кафедра інженерії
програмного забезпечення в
енергетиці

БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	121 Інженерія програмного забезпечення
Освітня програма	Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем в енергетиці
Статус дисципліни	Нормативна
Форма навчання	Очна(денна)
Рік підготовки, семестр	4 курс, 7 семестр
Обсяг дисципліни	4 кредити (120 год) 30 годин лекцій, 15 годин практичних робіт
Семестровий контроль/ контрольні заходи	Екзамен
Розклад занять	Науково-педагогічний працівник
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: д.т.н., професор Гаврилко Євген Володимирович, gev.1964@ukr.net , тел. 067-506-91-85 Практика: д.т.н., професор Гаврилко Євген Володимирович, gev.1964@ukr.net , тел. 067-506-91-85
Розміщення курсу	Засоби Google Classroom та E-mail. Викладені матеріали: Лекції, Практики, Лабораторні, Домашні завдання, Література.

Програма навчальної дисципліни

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

Силабус навчальної дисципліни «Безпека програмного забезпечення» (ПО 09) складено відповідно до освітньої програми «Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем в енергетиці» підготовки бакалаврів спеціальності 121 – Інженерія програмного забезпечення.

Метою є формування та закріплення у студентів наступних здатностей: (ФК 1) Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення; (ФК 5) Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу; (ФК 6) Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки); (ФК 17) Здатність реалізовувати застосунки корпоративних систем, інформаційної безпеки програм і даних, зокрема, в кібер-фізичних та енергетичних системах

Предмет навчальної дисципліни – криптографія, криптоаналіз, шифри для захисту програмного забезпечення в кібер-фізичних та енергетичних системах.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (ПРН 3) Знати основні процеси, фази та ітерації життєвого циклу програмного забезпечення (ПРН 11) Вибирати вихідні дані для проектування, керуючись формальними методами опису вимог та моделювання; (ПРН 18) Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних; (ПРН 30) Аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем. (ПРН 31) Реалізовувати застосунки корпоративних систем з інформаційної безпеки програм і даних, зокрема, в кібер-фізичних та енергетичних системах.

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

Дисципліна «Безпека програмного забезпечення» для підготовки бакалаврів зі спеціальності 121 Інженерія програмного забезпечення складена на основі освітньої програми «Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем в енергетиці» та навчального плану кафедри інженерії програмного забезпечення в енергетиці НН ІАТЕ.

У структурно-логічній схемі навчання дисципліна «Безпека програмного забезпечення» розміщена тоді, коли студенти вже прослухали навчальні дисципліни з «Комп'ютерної дискретної математики» (ЗО 1), Основи програмування (ПО 02), Компоненти програмної інженерії (ПО бщо достатньо для виконання практичних робіт з даної дисципліни.

Дисципліна «Безпека програмного забезпечення» забезпечує вивчення забезпечує підготовку до «Переддипломна практика (ПО 10) та «Дипломне проектування» (ПО 11), які викладаються пізніше.

3. Зміст навчальної дисципліни

Розділ 1: ВСТУП ДО БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Лекція 1: Вступ до дисципліни «Безпека програмного забезпечення».

Лекція 2: Математичні основи криптографії.

Лекція 3. Класична криптографія: історія від Цезаря до Хеш-функції.

Розділ 2: СИМЕТРИЧНА ТА АСИМЕТРИЧНА КРИПТОГРАФІЯ

Лекція 4: Симетричне шифрування.

Лекція 5: Асиметричне шифрування.

Лекція 6: Хеш-функції та цифрові підписи.

Лекція 7: Інфраструктура відкритих ключів (PKI) та сертифікати.

Розділ 3: БЕЗПЕКА МЕРЕЖЕВИХ ПРОТОКОЛІВ ТА ЗАХИСТ ДАНИХ.

Лекція 8: Протоколи безпечної передачі даних

Лекція 9: Безпека зберігання даних в ОС.

Лекція 10: Захист даних засобами і центрами безпеки.

Лекція 11: Захист ідентифікації та автентифікації користувачів.

Модуль 4: ПРАКТИЧНІ АСПЕКТИ ТА СУЧАСНІ ТЕНДЕНЦІЇ БЕЗПЕКИ ПЗ

Лекція 12: Аналіз вразливостей та тестування на проникнення (2 год.)

Лекція 13: Безпека хмарних додатків та контейнеризації.

Лекція 14: Квантова криптографія та постквантова криптографія.

Лекція 15: Правові та етичні аспекти кібербезпеки. Майбутнє безпеки ПЗ.

Лекція 16: Стандарти та вимоги держави щодо захисту інформації

4. Навчальні матеріали та ресурси

1. Фільштінський, В. А., Бережний, А. В. (2011) Математичні основи криптографії: конспект лекцій Сумський державний університет, 2011. – 138 с. <https://essuir.sumdu.edu.ua/bitstream-download/123456789/20822/1/Filsh.pdf;jsessionid=562F54E6557A5B213D7165093E9D26C4>
2. Таненбаум Е. Розподілені системи. Принципи / Е. Таненбаум, М. Ван Стеен. Наука. К, 2022. 877 с.
3. М.Венбо Сучасна криптографія: теорія и практика : пер. с англ. / М.Венбо – К. 2023.768с.
4. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 2021. 248 с.
5. Програмні технології захисту інформації: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти, спеціальності 121 Інженерія програмного забезпечення факультету інформаційних технологій УжНУ / Укладач: д.т.н., доц. Поліщук В.В. – Ужгород: 2023. – 76 с.
6. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2020. – 316 с.
7. Клінцв Л.М. Безпека програм і даних / Л.М. Клінцв Л.М. – Чернігов: ВСП Чернігівський інститут інформації, бізнесу і права, 2017. – 81 с.
8. Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
9. Захист програмного забезпечення. Методичні вказівки до виконання лабораторних робіт [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Системи, технології та математичні методи кібербезпеки» спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад. М. В. Коломицев, С. О. Носок. – Електронні текстові дані (1 файл: 1,1 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 85 с. – Назва з екрана. <https://ela.kpi.ua/handle/123456789/47929>

Навчальний контент

5. Методика опанування навчальної дисципліни(освітнього компонента).

Розділ 1: ВСТУП ДО БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Лекція 1: Вступ до безпеки програмного забезпечення.

Що таке безпека програмного забезпечення: основні принципи (конфіденційність, цілісність, доступність). Виклики та загрози в сучасному світі: типові атаки (SQL-ін'єкції, XSS, переповнення буфера). Життєвий цикл безпечної розробки (SDL): інтеграція безпеки на всіх етапах. Принципи безпечного кодування (OWASP Top 10). Відповідальність розробника за безпеку.

Лекція 2: Математичні основи криптографії. Основні поняття: числа, групи, поля, модульна арифметика. Теорія чисел для криптографії: прості числа, алгоритм Евкліда, китайська теорема про остачі. Криптографічні властивості функцій: одностороння функція, хеш-функція. Поняття складності алгоритмів і обчислювальної стійкості.

Лекція 3: Класична криптографія: історія від Цезаря до Хеш-функції.

Історичний огляд: шифр Цезаря, шифр Віженера, роторні машини (Enigma). Основи заміни та перестановки. Проблеми та вразливості класичних шифрів: частотний аналіз, брутфорс. Злами, інтернет і кібернетична безпека. Перехід до сучасної криптографії.

Розділ 2: СИМЕТРИЧНА ТА АСИМЕТРИЧНА КРИПТОГРАФІЯ

Лекція 4: Симетричне шифрування (4 години).

Принципи симетричного шифрування: єдиний ключ для шифрування та дешифрування. Блочні та потокові шифри. Алгоритми: AES (Advanced Encryption Standard) – детальний розгляд, режими роботи (ECB, CBC, CTR, GCM). DES (Data Encryption Standard)— шифрування певних даних Проблеми розподілу ключів у симетричній криптографії. Практичне застосування симетричного шифрування в ПЗ (наприклад, шифрування файлів, дисків).

Лекція 5: Асиметричне шифрування.

Принципи асиметричного шифрування: пара ключів (відкритий/приватний). Алгоритми: RSA, Еліптичні криві (ECC). Обмін ключами Діффі-Хеллмана. Переваги та недоліки асиметричного шифрування. Практичне застосування в ПЗ (наприклад, TLS/SSL, PGP).

Лекція 6: Хеш-функції та цифрові підписи

Криптографічні хеш-функції: властивості (односторонність, стійкість до колізій). Алгоритми хешування: SHA-256, SHA-3, MD5 (проблеми та ризики). Цифровий підпис: принципи роботи, призначення (автентифікація, цілісність, незаперечність). Алгоритми цифрового підпису: RSA-PSS, ECDSA. Застосування цифрових підписів у ПЗ (наприклад, підпис коду, документів).

Лекція 7: Інфраструктура відкритих ключів (PKI) та сертифікати

Концепція PKI: компоненти (центр сертифікації, реєстраційний центр). X.509 сертифікати: структура, призначення, ланцюжки довіри. Відкликання сертифікатів: CRL, OCSP. Взаємодія з PKI в програмних системах.

Модуль 3: БЕЗПЕКА МЕРЕЖЕВИХ ПРОТОКОЛІВ ТА ЗАХИСТ ДАНИХ

Лекція 8: Протоколи безпечної передачі даних

Історія та еволюція TLS (SSL). Робота протоколу TLS: етапи рукописання, обмін ключами, шифрування даних. Криптографічні примітиви, що використовуються в TLS. Налаштування TLS у веб-додатках (сервери, клієнти). Поширені вразливості та атаки на TLS (наприклад, Heartbleed, POODLE).

Лекція 9: Безпека зберігання даних в ОС.

Основні поняття операційної системи необхідні для створення систем захисту програмного забезпечення. методи захисту програмного забезпечення. засоби захисту програмного забезпечення

Лекція 10: Захист даних засобами і центрами безпеки.

Принципи роботи систем аналізу захищеності. Microsoft Baseline Security Analyzer. Сканер безпеки Xspider. SIEM системи для ВБОС. Аутентифікація та авторизація API: OAuth

2.0, OpenID Connect, JWT (JSON Web Tokens). Шифрування трафіку API (TLS). Захист від DoS/DDoS атак на API. Принципи безпеки в архітектурі мікросервісів.

Лекція 11: Захист ідентифікації та автентифікації користувачів.

Безпечне зберігання паролів: хешування, солінг, пепперінг, повільні хеші (PBKDF2, bcrypt, scrypt, Argon2). Багатофакторна автентифікація (MFA): TOTP, HOTP, FIDO. Єдиний вхід (Single Sign-On - SSO). Управління сесіями: безпечні токени, захист від фіксації сесій.

Модуль 4: ПРАКТИЧНІ АСПЕКТИ ТА СУЧАСНІ ТЕНДЕНЦІЇ БЕЗПЕКИ ПЗ

Лекція 12: Аналіз вразливостей та тестування на проникнення

Види тестування безпеки: статичний аналіз коду (SAST), динамічний аналіз (DAST). Методології тестування на проникнення (Penetration Testing). Інструменти для аналізу безпеки ПЗ (наприклад, SonarQube, Burp Suite, Zap). Звітування про вразливості та їх усунення. За наявності полігону – захист свого ПЗ.

Лекція 13: Безпека хмарних додатків та контейнеризації.

Модель спільної відповідальності в хмарі. Захист контейнерів (Docker, Kubernetes): образи, реєстри, мережі. Безпека serverless-функцій. Управління секретами в хмарному середовищі.

Лекція 14: Квантова криптографія та постквантова криптографія (4 години).

Основи квантових обчислень та їх вплив на сучасні криптосистеми (алгоритм Шора, Гровера). Принципи квантової криптографії: QKD. Постквантова криптографія (PQC): алгоритми, що витримують атаки квантових комп'ютерів. Стандартизація PQC.

Лекція 15: Правові та етичні аспекти кібербезпеки. Майбутнє безпеки ПЗ.

Законодавство у сфері захисту даних. ДСТУ та міжнародні стандарти в сфері безпеки програмного забезпечення. Відповідальність розробників та компаній. Етичні питання в кібербезпеці. Перспективи розвитку безпеки ПЗ: AI/ML у кібербезпеці, поведінковий аналіз, Zero Trust. Кар'єрні можливості у сфері безпеки ПЗ.

Практичні заняття

Практична робота 1. Тема: Шифр Цезаря. Мета: Розробити криптосистему на основі історичного шифру Цезаря.

Практична робота 2. Тема: Шифр Тритеміуса. Мета: Розробити криптосистему на основі шифру Тритеміуса.

Практична робота 3. Тема: Книжковий шифр. Мета: Розробити криптосистему на основі використання віршованого фрагменту в якості ключа шифрування.

Практична робота 4. Тема: Шифр гамування. Мета: Розробити криптосистему на основі шифру гамування.

Практична робота 5. Тема: Шифр DES Мета: Розробити криптографічний код Алгоритму симетричного шифрування DES (Data Encryption Standard).

Практична робота 6. Тема: Шифрування з відкритим ключем на основі задачі рюкзака. Мета: розробити асиметричну криптосистему на базі алгоритмів типу рюкзак.

Практична робота 7. Тема: Шифрування з відкритим ключем на основі алгоритму RSA. Мета: Ознайомитись з використанням криптопровайдерів для побудови асиметричної криптосистеми.

Практична робота 8. Тема: Електронно-цифровий підпис на основі алгоритму RSA. Мета: Ознайомитись з порядком утворення підпис на основі алгоритму RSA.

Практична робота 9. Тема: Шифрування за допомогою SHA256. Мета: Ознайомитись з порядком утворення блокчейн.

6. Самостійна робота студента

Розділ 1. Базова модель безпеки інформації.

Актуальність проблеми забезпечення безпеки програм та даних. (2 години) Загальна характеристика дисципліни. Нормативно-правова база для організації і проведення заходів щодо безпеки програм та даних. Шляхи витоку інформації і несанкціонованого доступу в інформаційних системах. Архітектура систем безпеки програм та даних.

Сервіси безпеки, механізми їх реалізації. Атаки. Модель мережевої взаємодії. Організаційно-технічні заходи щодо забезпечення безпеки Основні механізми розгортання ОС, які застосовуються для ОС Microsoft (4 години): метод дублювання дисків з використанням утиліти Sysprep та метод віддаленої установки з використанням сервера віддаленої установки (RIS).

Безпека зберігання даних в ОС Microsoft. Технологія тіньового копіювання даних. Архівація даних. Створення відмовостійких томів для зберігання даних. Робота з томами RAID.

Центр забезпечення безпеки (Windows Security Center) в операційній системі Windows. Три основні компоненти безпеки ОС: брандмауер, антивірус, система автоматичного оновлення. Параметри безпеки. Налаштування безпеки Internet Explorer. Створення виключення для програми. Створення виключення для порту.

Основні механізми розгортання ОС, які застосовуються для ОС Microsoft: метод дублювання дисків з використанням утиліти Sysprep та метод віддаленої установки з використанням сервера віддаленої установки (RIS).

Забезпечення безпеки зберігання даних в ОС Microsoft. Ознайомлення з можливостями ОС Microsoft Windows 2003/XP/2007/2010 по забезпеченню безпеки зберігання даних в цілому, не дивлячись на їх важливість. Розглянуто рішення, що надаються ОС Microsoft Windows в цьому діапазоні: технологія тіньового копіювання даних; архівація даних; створення відмовостійких томів для зберігання даних.

Обмеження тіньового копіювання томів. Стратегії архівації (повна архівація, повна архівація з подальшою додатковою, повна архівація з подальшою різницевою, щоденна архівація). Відновлення даних. Види відмовостійких томів для зберігання даних. Класифікація RAID.

Центр забезпечення безпеки (Windows Security Center) в операційній системі Windows. Три основні компоненти безпеки ОС: брандмауер, антивірус, система автоматичного оновлення. Параметри безпеки. Налаштування безпеки Internet Explorer. Створення виключення для програми. Створення виключення для порту.

Windows Defender. Захист від шкідливого програмного забезпечення. Технологія безпеки, що захищає комп'ютер від програм-шпигунів і інших видів небажаних програм. Установка Windows Defender, вимоги до системи. Налаштування Windows Defender. Автоматична перевірка (Automatic scanning). Дії за умовчанням (Default actions). Параметри захисту в режимі реального часу (Real-time protection options). Виявлення підозрілих дій. Робота з карантинном. Використання Провідника програмного забезпечення (Software Explorer).

Microsoft Baseline Security Analyzer і XSpider. Системи аналізу захищеності корпоративної мережі (виявлення уразливостей). Принципи роботи систем аналізу захищеності. Вибір комп'ютера і опцій сканування в програмі MBSA. Опис перевірок, виконуваних MBSA.

Сканер безпеки XSpider. Можливості програми: повна ідентифікація сервісів на випадкових портах; евристичний метод визначення типів і імен серверів (HTTP, FTP, SMTP, POP3, DNS, SSH) незалежно від їх відповіді на стандартні запити; обробка RPC- сервісів з їх повною ідентифікацією; проведення перевірок на нестандартні DoS-атаки.

Розділ 2. Криптографічні засоби захисту інформації з симетричним ключем.

DES (Data Encryption Standard) - Симетричний алгоритм шифрування. (4 години) Мережа Фейстеля. Схема шифрування алгоритму DES. Генерування ключів. Режими використання DES: ECB — Electronic Code Book, CBC — Cipher Block Chaining, CFB — Cipher Feed Back, OFB — Output Feed Back. Переваги і недоліки режимів.

Алгоритми блокового симетричного шифрування ДСТУ ГОСТ 28147:2009. Міжнародний стандарт симетричного шифрування AES (Advanced Encryption Standard). Загальноєвропейський стандарт шифрування IDEA (International Data Encryption Algorithm). Програмна реалізація симетричних криптографічних алгоритмів AES засобами .NET.

Розділ 3. Криптографічні засоби захисту інформації з відкритим ключем

RSA - криптографічний алгоритм з відкритим ключем. Необхідні поняття. Алгоритм створення відкритого і секретного ключів. Шифрування і дешифрування. Цифровий підпис. Швидкість роботи алгоритму RSA. Криптоаналіз RSA. Елементарні атаки.

GnuPG -- інструмент для шифрування і цифрового підпису. Налаштування. Створення ключа. Обмін ключами. Захист листування.

Блокчейн. Інструменти та засоби функціонування децентралізованих застосунків. Застосунки на основі P2P.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування лекційних та практичних занять є обов'язковим за винятком поважних причин (хвороби, форс-мажорних обставин).

В разі пропущення занять з поважних причин викладач надає можливість студенту виконати усі або деякі лабораторні завдання (винятком є виконання деяких завдань у зв'язку із закінченням навчального процесу).

В разі пропущення занять без поважних причин, а також через порушення граничного терміну виконання завдання (deadline) студент може отримати зменшену кількість балів від максимальної оцінки за відповідне завдання.

Протягом семестру студенти:

- вивчають лекції, посібники;
- виконують та захищають лабораторні роботи у відповідні терміни;
- пишуть 2 модульні контрольні роботи;
- повинні позитивно закрити календарні контролі;
- по закінченні навчального процесу складають іспит.

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

Поточний контроль: тестування або експрес-опитування за кожним Розділом навчального матеріалу, Модульна контрольна робота, виконання завдань до практичних занять.

Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог Силабусу.

Модульна контрольна робота складається з тесту за матеріалом Розділів 1, та 2,3.

Семестровий контроль: екзамен.

Умови допуску до семестрового контролю: семестровий рейтинг більше 40 балів.

Система рейтингових (вагових) балів та критерії оцінювання

Максимальна кількість балів з кредитного модуля дорівнює 100.

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

- виконання та захист практичних робіт,
- модульну контрольну роботу (МКР) тривалістю 1 акад. година.

Виконання завдань практичних робіт

Завдання практичні роботи являє собою індивідуальне виконання робіт, що пов'язані з рішенням на ЕОМ заданої задачі шляхом розробки модулю і його інтерфейсу. Інтерфейс повинен бути поєднано з рішеннями практик.

Вагові бали завдань наведено у таблиці.

Види завдань		Внесок до семестрового рейтингу балів
1.	Практична робота 1. Тема: Шифр Цезаря. Мета: Розробити криптосистему на основі історичного шифру Цезаря.	5
2.	Практична робота 2. Тема: Шифр Тритеміуса. Мета: Розробити криптосистему на основі шифру Тритеміуса.	5
3.	Практична робота 3. Тема: Книжковий шифр. Мета: Розробити криптосистему на основі використання віршованого фрагменту в якості ключа шифрування.	5
4.	Практична робота 4. Тема: Шифр гамування. Мета: Розробити криптосистему на основі шифру гамування.	5
5.	Практична робота 5. Тема: Шифр DES Мета: Розробити криптографічний код Алгоритму симетричного шифрування DES (Data Encryption Standard).	5

6.	Практична робота 6. Тема: Шифрування з відкритим ключем на основі задачі рюкзака. Мета: розробити асиметричну криптосистему на базі алгоритмів типу рюкзак.	5
7.	Практична робота 7. Тема: Шифрування з відкритим ключем на основі алгоритму RSA. Мета: Ознайомитись з використанням криптопровайдерів для побудови асиметричної криптосистеми.	5
8.	Практична робота 7. Тема: Електронно-цифровий підпис на основі алгоритму RSA. Мета: Ознайомитись з порядком утворення підпис на основі алгоритму RSA.	5
Контрольна робота		10
Контрольна робота 2		10
Екзамен		40

Максимальна кількість балів за всі завдання дорівнює 50 балів.

Критерії оцінювання

Підготовка до роботи (у відсотках від максимальної кількості балів за відповідну роботу):

- протокол відповідає вимогам, охайний – 20 %;
- протокол відповідає вимогам, але є чисельні виправлення – 10 %;

Виконання завдання лабораторної роботи:

- робота виконана повністю і вірно протягом відведеного часу – 50 %;
- робота виконана пізніше зазначеного терміну – 20 %;

Якість захисту роботи:

- студент вірно і повністю відповів на запитання – 30 %;
- студент при відповіді допустив несуттєві неточності – 20 %;
- студент при відповіді на запитання допустив суттєві неточності, але самостійно виправив їх – 10 %.

2. Екзамен

Ваговий бал – 40.

Контрольна робота складається з 5 тестових завдань. За кожну вірну відповідь на запитання надається 8 бали.

Сума вагових балів контрольних заходів протягом семестру складає:

$$R = 40 + 20 + 40 = 100 \text{ балів.}$$

Необхідною умовою допуску до заліку є зарахування усіх практичних робіт, а також стартовий рейтинг (r_c) не менше 40% від R, тобто 40 балів.

Сума балів переводиться до залікової оцінки згідно з таблицею:

Бали (RD)	Традиційна оцінка
95...100	Відмінно
85...94	Дуже добре
75...84	Добре
65...74	Задовільно

60...64	Достатньо
$RD \leq 60$	Незадовільно
$RD < 40$ або не виконані інші умови допуску до заліку	Не допущений

9. Додаткова інформація з дисципліни (освітнього компонента)

Вимоги до спеціального матеріально-технічного та/або інформаційного забезпечення:

Наявність діючих облікових записів: Користувача на Платформі дистанційного навчання "Сікорський" та Сервісів Google;

Вимоги до мережевої інфраструктури: достатні для отримання доступу до <https://google.com/> та <https://do.ipokpi.ua>.

Операційна система: не специфікується;

Інтернет браузер: не специфікується;

Текстовий редактор: не специфікується;

Перелік питань, які виносяться на семестровий контроль

Що означає «Інформаційна безпека».

Що передбачає «Захист інформації».

Назвіть властивості інформації з точки зору захисту інформації, відповідь можна викласти у вигляді схеми?

Які рівні формування режиму інформаційної безпеки з точки зору ЗІ. Необхідно розкрити їх зміст?

Які в залежності від загроз інформаційній безпеці існують рівні ЗІ?

Дайте визначення криптографії.

Дайте визначення основним поняттям криптографії.

У чому полягає принцип Керкхоффа. Дати визначення?

Як здійснюється шифрування за допомогою стовпчикової перестановки? Представити у вигляді схеми.

Як влаштований шифр матричної перестановки? Представити у вигляді схеми.

Як здійснюється шифрування за допомогою шифру заміни? Представити у вигляді схеми.

У чому сутність шифру поліалфавітної заміни? Представити у вигляді схеми.

У чому сутність шифру за допомогою Поворотної решітки Кардинала Решельє? Представити у вигляді схеми.

У чому сутність шифру за допомогою Шифра Віженера? Представити у вигляді схеми.

Як здійснюється шифрування за допомогою шифру Цезаря?

Як здійснюється шифрування за допомогою шифру гамування?

Як здійснюється шифрування за допомогою книжкового шифру?

Що таке рівень криптостійкості? Надати поняття класу складності обчислення.

Дати визначення загальному методу повного перебору.

Які шифри називаються абсолютно криптостійкими?

Як працює шифр Вермана?

Показати схематично які дії реалізуються в алгоритмі DES.

Показати схематично на прикладі DES як побудовані шифри 3DES, DES-EEE3, DES-EDE3, DES-EEE2.

Дати приклад роботи моделі криптосистеми з публічними ключами.

Як здійснюється шифрування за допомогою шифру рюкзака?

Як на основі задачі рюкзака побудувати асиметричну криптосистему?

Що зараз вивчає сучасна криптографія. Дати пояснення основним розділам сучасної криптографії.

Що таке протокол Діффі-Хеллмана? В чому полягає Алгоритм сеансового ключа в симетричному алгоритмі.

Який головний недолік протоколу Діффі-Хеллмана?

Як здійснюється шифрування за шифром Шаміра, шифром Ель-Гамала?

Як здійснюється шифрування за допомогою шифру RSA.

Що представляє собою цифровий підпис?

Як реалізується цифровий підпис на основі шифру RSA.? Показати алгоритм підпису RSA.

Дати визначення Електронний підпис та Електронний цифровий підпис. Яка різниця між ними з огляду на криптографію.

Що дозволяє використання Електронного цифрового підпису.

Назвати Схеми побудови цифрового електронного підпису. Недоліки і переваги симетричної схеми.

Назвати Схеми побудови цифрового електронного підпису. Назвати процеси асиметричної схеми.

Що таке криптографічна хеш-функція? Назвіть переваги хеш-функції.

Особливості SHA256, переваги і недоліки?

Як вирішуються завдання зберігання закритого ключа в схемі Цифрового електронного підпису.

Що знаходиться в основі протоколу Електронного цифрового підпису.

Навести назви і схеми стандартних протоколів узгодження ключів Електронного цифрового підпису.

Назвати властивості цифрових сертифікатів Електронного цифрового підпису.

Назвіть сфери використання хеш-функцій.

Особливості квантової криптографії і постквантової криптографії.

Назвати властивості, які притаманні криптографічним хеш-функцій.

Назвіть усі типи криптографічних хеш-функцій.

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри інженерії програмного забезпечення в енергетиці НН ІАТЕ, д.т.н., проф., Гаврилком Євгеном Володимировичем.

Ухвалено кафедрою інженерії програмного забезпечення в енергетиці НН ІАТЕ (протокол № 43 від 24.06.2023 р.)

Погоджено Методичною комісією НН ІАТЕ (протокол № 9-від 26.06.2026 р.)