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), з яких 54 години аудиторних (36 год лекції, 18 год практичні), 66 години становить самостійна робота
Семестровий контроль/ контрольні заходи	Екзамен/МКР
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: асистент, аспірант Гейко Олег Олександрович, oleg.63366@gmail.com, тел. 097-305-10-03
Розміщення курсу	Засоби GoogleClassroomта E-mail. Викладені матеріали: Лекції, Практики, Лабораторні, Домашні завдання, Література.

Програма навчальної дисципліни

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

Силабус навчальної дисципліни «Безпека програмного забезпечення» (ПО 09) складено відповідно до освітньої програми «Інженерія програмного забезпечення інтелектуальних кіберфізичних 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 3+) Здатністьрозробляти архітектури, модулі та компоненти*

програмних систем; *(ФК 6+) Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки);(ФК 7) Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних. (фк 14) Здатність до алгоритмічного та логічного мислення;(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 1) Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки; (ПРН 18) Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних; (ПРН 21) Знати, 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 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 постреквізитидисципліни (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 (ЗО 1) Комп'ютерної дискретної математики, (ПО 2.1) «Основи програмування. Частина 1. Базові конструкції», (ПО 2.2) «Основи програмування. Частина 2. Методології програмування», (ПО 6.1) «Компоненти програмної інженерії. Частина 1. Вступ до програмної інженерії», що 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. Базова модель безпеки інформації.

Тема 1.1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки.

Тема 1.2. Базова модель безпеки інформації в програмах і даних.

Тема 1.3. Безпека мережевої інфраструктури.

Тема 1.4. Безпека зберігання даних в ОС Microsoft.

Тема 1.5. Центр забезпечення безпеки Windows SecurityCenterТема 1.6. Центр забезпечення безпеки Windows Defender.

Тема 1.7. Microsoft BaselineSecurityAnalyzer і XSpider.

Тема 1.8. Сканер безпеки XSpider.

Розділ 2. Криптографічні засоби захисту інформації з симетричним ключем.

Тема 2.1. Блокові шифри як основа сучасних криптосистем.

Тема 2.2. Криптосистема DES (DataEncryption Standard).

Тема 2.3. Сучасні симетричні криптосистеми.

Розділ 3. Криптографічні засоби захисту інформації з відкритим ключемТема 3.1. Модель асиметричної системи.

Тема 3.2. Протоколи розподілення ключів на основі центрів довіри .

Тема 3.3. Протоколи асиметричного шифрування.

Тема 3.4. Криптосистема RSA.

Тема 3.5. Цифрові підписи.

Тема 3.6. Програмна реалізація цифрового підпису засобами .NETТема 3.7. Криптографічні Геш-функції.

4. Навчальні матеріали та ресурси

1. *Таненбаум Е. Розподілені системи. Принципи / Е. Таненбаум, М. ван Стеен. К, 2003.877 с.*
2. *М.Венбо Сучасна криптографія: теорія и практика : пер. с англ. / М.Венбо –К. 2005.768с.*
3. *Артем Генкін, АлексейМихеєв. Блокчейн: як цепрацює. –Днепр.:2015. 129*
4. *Вербіцький О. В.Вступ до криптології / О. В. Вербіцький. –Львів : ВНТЛ, 2011. 248 с.*
5. *Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. –Х. : Вид. ХНЕУ, 2010. – 316 с.*
6. *Клінцв Л.М. Безпека програм і даних / Л.М. Клінцв Л.М. –Чернігов: ВСП Чернігівський інститут інформації, бізнесу і права, 2017. –81 с.*
7. *Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. –Київ: КПІ ім. Ігоря Сікорського, 2018. –162 с.*
8. *Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. –Львів : ВНТЛ, 2011. –248 с.*
9. *Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. –Х. : Вид. ХНЕУ, 2010. –316 с.*
10. *Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. –Х. : Вид. ХНЕУ, 2011. –510 с.*

Навчальний контент

1. Методика опанування навчальної дисципліни(освітнього компонента)

Лекції

Розділ 1. Базова модель безпеки інформації.

Тема 1.1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки.

Лекція 1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки.

Вступ до курсу лекцій. Основні поняття та визначення. Правові аспекти захисту інформації.

Властивості інформації з точки зору її захисту. Рівні формування режиму інформаційної безпеки.Тема 1.2. Базова модель безпеки інформації.

Лекція 2. Базова модель безпеки інформації.

Шляхи витоку інформації і несанкціонованого доступу в інформаційних системах.

Архітектура систем безпеки програм та даних.

Тема 1.3. Безпека мережевої інфраструктури.

Лекція 3. Безпека мережевої інфраструктури.

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).

Тема 1.4. Безпека зберігання даних в ОС Microsoft.

Лекція 4. Безпека зберігання даних в ОС Microsoft.

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

Тема 1.5. Центр забезпечення безпеки Windows SecurityCenter.

Лекція 5. Центр забезпечення безпеки Windows SecurityCenter

Центр забезпечення безпеки (Windows SecurityCenter) 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.

Тема 1.6. Центр забезпечення безпеки Windows Defender.

Лекція 6. Центр забезпечення безпеки Windows Defender.

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 (Automaticscanning). Дії за умовчанням (Defaultactions). Параметри захисту в режимі реального часу (Real-timeprotectionoptions). Виявлення підозрілих дій. Робота з карантином. Використання Провідника програмного забезпечення (Software Explorer).

Тема 1.7. Microsoft BaselineSecurityAnalyzer і XSpider.

Лекція 7. Microsoft BaselineSecurityAnalyzer 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.

Тема 1.8. Сканер безпеки XSpider.

Лекція 8. 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-сервисов з їх повною ідентифікацією; проведення перевірок на нестандартні DoS-атаки.

Розділ 2. Криптографічні засоби захисту інформації з симетричним ключем.

Тема 2.1. Блокові шифри як основа сучасних криптосистем.

Лекція 9. Блокові шифри як основа сучасних криптосистем.

Блокові алгоритми і режими шифрування. Режим електронної кодової книги. Режим зціплення блоків по криптотексту. Режим з оберненим зв'язком по виходу. Режим з лічильником. Схема Фейстеля.

Тема 2.2. Криптосистема DES (DataEncryption Standard).

Лекція 10. DataEncryption Standard.

Загальна характеристика DES. Алгоритм шифрування/розшифрування DES. Структура функції шифрування. Криптографічна стійкість DES. Криптосистеми DESX, 3DES. DES і шифрована файлова система EFS. Програмна реалізація симетричних криптографічних алгоритмів DES і 3DES засобами .NET.

Тема 2.3. Сучасні симетричні криптосистеми.

Лекція 11. Сучасні симетричні криптосистеми

Алгоритми блокового симетричного шифрування ДСТУ ГОСТ 28147:2009. Міжнародний стандарт симетричного шифрування AES (AdvancedEncryption Standard). Загальноєвропейський стандарт шифрування IDEA (InternationalDataEncryptionAlgorithm). Програмна реалізація симетричних криптографічних алгоритмів AES засобами .NET.

Розділ 3. Криптографічні засоби захисту інформації з відкритим ключемТема 3.1. Модель асиметричної системи.

Лекція 12. Модель асиметричної системи.

Передумови виникнення асиметричних систем. МодельДіффі-Хеллмана криптосистеми з публічними ключами. Поняття односторонньої функції-пастки. Асиметрична криптосистема на основі використання «задачі рюкзака».

Тема 3.2. Протоколи розподілення ключів на основі центрів довіри.

Лекція 13. Протоколи розподілення ключів на основі центрів довіри.

Проблема розподілення ключів симетричної криптосистем. Протокол широкоротої жаби. Протокол Нідхейма-Шредера. Протокол Отвей-Ріса. Протокол Цербер. Протокол мережної аутентифікаціїKerberos 5 і аутентифікація в Windows.

Тема 3.3. Протоколи асиметричного шифрування.

Лекція 14. Протоколи асиметричного шифрування.

Протокол Діффі-Хеллмана. Шифр Шаміра. Шифр Ель-Гамаля. Програмна реалізація алгоритму Діффі-Хеллмана засобами .NET.

Тема 3.4. Криптосистема RSA

Лекція 15. Криптосистема RSA

Принцип шифрування в RSA. Генерація пари ключів шифрування. Алгоритм шифрування/розшифрування RSA. Програмна реалізація алгоритму RSA засобами .NET.Тема 3.5. Цифрові підписи.

Лекція 16. Цифрові підписи.

Схема застосування цифрового підпису. Цифровий підпис на основі шифру RSA. Цифровий підпис на основі шифру Ель-Гамаля. Алгоритм цифрового підпису DSA (DigitalSignatureAlgorithm). Стандарт ГОСТ Р34.10-94.

Тема 3.6. Програмна реалізація цифрового підпису засобами .NET.

Лекція 17. Програмна реалізація цифрового підпису засобами .NET.

Реалізація цифрового підпису на основі RSA. Використання криптопровайдера цифрового підпису на основі DSA.

Тема 3.7. Криптографічні геш-функції.

Лекція 18. Криптографічні геш-функції.

Геш-функції і їх призначення. Ключові геш-функції. Безключовігеш-функції. Програмна реалізація алгоритмів геширування в .NET.

Практичні заняття

1. *Практична робота 1. Тема: Шифр Цезаря. Мета: Розробити криптосистему на основі історичного шифру Цезаря.*
2. *Практична робота 2. Тема: Шифр Тритеміуса. Мета: Розробити криптосистему на основі шифру Тритеміуса.*
3. *Практична робота 3. Тема: Криптосистема Хілла. Мета: Розробити криптосистему на основі Криптосистема Хілла.*
4. *Практична робота 4. Тема: Книжковий шифр. Мета: Розробити криптосистему на основі використання віршованого фрагменту в якості ключа шифрування.*
5. *Практична робота 5. Тема: Шифр гамування. Мета: Розробити криптосистему на основі шифру гамування.*
6. *Практична робота 6. Тема: Шифр DES Мета: Розробити криптографічний код Алгоритму симетричного шифрування DES (DataEncryption Standard).*
7. *Практична робота 7. Тема: Шифрування з відкритим ключем на основі задачі рюкзака. Мета: Розробити асиметричну криптосистему на базі алгоритмів типу рюкзак.*
8. *Практична робота 8. Тема: Шифрування з відкритим ключем на основі алгоритму RSA. Мета: Ознайомитись з використанням криптопровайдерів для побудови асиметричної криптосистеми.*
9. *Практична робота 9. Тема: Електронно-цифровий підпис на основі алгоритму RSA. Мета: Ознайомитись з порядком утворення підпис на основі алгоритму RSA.*

2. 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 безпекиОсновні 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. Технологіятіньового копіювання даних. Архівація даних. Створення відмовостійких томів для зберігання даних. Робота з томами RAID.

Центр забезпечення безпеки (Windows SecurityCenter) 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 зберіганняданих.

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 SecurityCenter) 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 (Automaticscanning). Дії за умовчанням (Defaultactions). Параметри захисту в режимі реального часу (Real-timeprotectionoptions). Виявлення підозрілих дій. Робота з карантином. Використання Провідника програмного забезпечення (Software Explorer).

Microsoft BaselineSecurityAnalyzer 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 (DataEncryption Standard) - Симетричний алгоритм шифрування. (4 години) Мережа Фейстеля. Схема шифрування алгоритму DES. Генерування ключів. Режими використання DES: ECB —ElectronicCodeBook, CBC —CipherBlockChaining, CFB — CipherFeedBack, OFB —OutputFeedBack. Переваги і недоліки режимів.

Алгоритми блокового симетричного шифрування ДСТУ ГОСТ 28147:2009. Міжнародний стандарт симетричного шифрування AES (AdvancedEncryption Standard). Загальноєвропейський стандарт шифрування IDEA (InternationalDataEncryptionAlgorithm). 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. Елементарніатаки.

GnuGPG -- 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

1. 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 студентувиконати 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.*

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

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.*

<u>Виконання завдань практичних робіт</u>

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 поєднаю з рішеннями практик.

Вагові бали завдань наведено у таблиці.

Види завдань	*Внесок до семестрового рейтингу балів*
1	2
Практична робота 1. Тема: Шифр Цезаря. Мета: Розробити криптосистему на основі історичного шифру Цезаря.	*5*
Практична робота 2. Тема: Шифр Тритеміуса. Мета: Розробити криптосистему на основі шифру Тритеміуса.	*5*
Практична робота 3. Тема: Криптосистема Хілла. Мета: Розробити криптосистему на основі Криптосистема Хілла.	*5*

1	2
Практична робота 5. Тема: Книжковий шифр. Мета: Розробити криптосистему на основі використання віршованого фрагменту в якості ключа шифрування.	*5*
4.Практична робота 5. Тема: Шифр гамування. Мета: Розробити криптосистему на основі шифру гамування.	*5*
Практична робота 6. Тема: Шифр DES Мета: Розробити криптографічний код Алгоритму симетричного шифрування DES (DataEncryptionStandard).	*5*
Практична робота 7. Тема: Шифрування з відкритим ключем на основі задачі рюкзака. Мета: розробити асиметричну криптосистему на базі алгоритмів типу рюкзак.	*5*
Практична робота 8. Тема: Шифрування з відкритим ключем на основі алгоритму RSA. Мета: Ознайомитись з використанням криптопровайдерів для побудови асиметричної криптосистеми.	*5*
Практична робота 9.Тема: Електронноцифровий підпис на основі алгоритму RSA. Мета: Ознайомитись з порядком утворення підпис на основі алгоритму RSA.	*5*
Контрольна робота 1	*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 %.

<u>Екзамен</u>

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 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<=60	*Незадовільно*
RD < 40 або не виконані інші умови допуску до заліку	*Не допущений*

Додаткова інформація з дисципліни (освітнього компонента)

1. *Що означає «Інформаційна безпека».*
2. *Що передбачає «Захист інформації».*
3. *Назвіть властивості інформації з точки зору захисту інформації, відповідь можна викласти у вигляді схеми?*
4. *Які рівні формування режиму інформаційної безпеки з точки зору ЗІ. Необхідно розкрити їх зміст?*
5. *Які в залежності від загроз інформаційній безпеці існують рівні ЗІ?*
6. *Дайте визначення криптографії.*
7. *Дайте визначення основним поняттям криптографії.*
8. *У чому полягає принцип Керкхоффса. Дати визначення?*
9. *Як здійснюється шифрування за допомогою стовпчикової перестановки? Представити у вигляді схеми.*
10. *Криптосистема Хілла. Як формується ключ шифра?*
11. *Як влаштований шифр матричної перестановки? Представити у вигляді схеми.*
12. *Як здійснюється шифрування за допомогою шифру заміни? Представити у вигляді схеми.*
13. *У чому сутність шифру поліалфавітної заміни? Представити у вигляді схеми.*
14. *У чому сутність шифру за допомогою Поворотної решітки Кардинала Решелье? Представити у вигляді схеми.*
15. *У чому сутність шифру за допомогою Шифра Віженера? Представити у вигляді схеми.*
16. *Як здійснюється шифрування за допомогою шифру Цезаря?*
17. *Як здійснюється шифрування за допомогою шифру гамування?*
18. *Як здійснюється шифрування за допомогою книжкового шифру?*
19. *Що таке рівень криптостійкості? Надати поняття класу складності обчислення.*
20. *Дати визначення загальному методу повного перебору.*
21. *Які шифри називаються абсолютно крипостійкими?*
22. *Як працює шифр Вермана?*
23. *Показати схематично які дії реалізуються в алгоритмі DES.*
24. *Показати схематично на прикладі DES як побудовані шифри 3DES, DES-EEE3, DES-EDE3, DES-EEE2.*
25. *Дати приклад роботи моделі криптосистеми з публічними ключами.*

26. Як здійснюється шифрування за допомогою шифру рюкзака?

27. Як на основі задачі рюкзака побудувати асиметричну криптосистему?

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

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

30. Який головний недолік протоколу Діффі-Хеллмана?

31. Як здійснюється шифрування за шифром Шаміра, шифром Ель-Гамаля?

32. Як здійснюється шифрування за допомогою шифру RSA.

33. Що представляє собою цифровий підпис?

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

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

36. Що дозволяє використання Електронного цифрового підпису.

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

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

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

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

41. Що знаходиться в основі протоколу Електронного цифрового підпису.

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

43. Назвати властивості цифрових сертифікатів Електронного цифрового підпису.

44. Назвіть сфери використання хеш-функцій.

45. Назвати властивості, які притаманні криптографічним хеш-функцій.

46. Назвіть усі типи криптографічних хеш-функцій.

Робочу програму навчальної дисципліни (силабус):

Складено заступником директора НН ІАТЕ з НВР, професором кафедри ІПЗЕ д.т.н., професором Гаврилком Є.В.

Ухвалено кафедрою ІПЗЕ (протокол № 34 від 10.05.2024 р.)

Погоджено Методичною комісією ННІАТЕ КПІ ім. Ігоря Сікорського (протокол №9 від 31.05.2024 р.)