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

Кафедра автоматизації проектування енергетичних процесів і систем

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	**Перший (бакалаврський)**
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітня програма	*Комп'ютерний моніторинг та геометричне моделювання процесів і систем*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*3 курс осінній 1 семестр*
Обсяг дисципліни	*4 кредити (120 год) (лекцій 18 год., лаб. 36 год., 66 СРС)*
Семестровий контроль/ контрольні заходи	*Залік, МКР*
Розклад занять	*http://rozklad.kpi.ua/*
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	Google classroom, e-Кампус

Програма навчальної дисципліни

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

Захист інформації та кібербезпека як такі й їх похідні, що формують окремі важливим напрями діяльності спеціалістів ІТ. Вивчення дисципліни «Безпека інформаційних систем» присвячене різним підходам захисту комп'ютерних програм і інформації від несанкціонованого впливу, внесенню змін, зникненню та крадіжкам.

Метою навчальної дисципліни є формування у студентів здатностей до використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту комп'ютерної інформації, законодавства і стандартів у цій області, сучасних криптосистем; здатність їх застосовувати у професійній діяльності для підтримки інформаційної безпеки об'єктів професійної діяльності.

Завдання. Основні завдання навчальної дисципліни.

Згідно з вимогами освітньо-професійної програми студенти після засвоєння навчальної дисципліни мають уміти забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій і продемонструвати такі результати навчання:

знати:

- основні положення законодавства в галузі захисту інформації,

- основні міжнародні та національні стандарти з безпеки ІС та Т;
- основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки;
- механізми та протоколи забезпечення конфіденційності;
- механізми та протоколи забезпечення автентичності;
- механізми та протоколи забезпечення цілісності даних;
- модель порушника, основні види атак, принципи криптоаналізу;
- механізми та протоколи керування ключами;
- методи та процедури цифрової стеганографії.

та *отримати досвід, який дозволяє*:

- визначати вимоги політики безпеки та формувати профіль захисту відповідно до забезпечення послуг безпеки в інформаційній системі;
- ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в інформаційній системі;
- забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;
- аналізувати технічні параметри діючих протоколів та механізмів захисту інформації з точки зору використання в комп'ютерних системах та мережах, впливу їх характеристик на основні показники інформаційних систем в цілому;
- проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів;
- забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій;
- здійснювати захист даних в корпоративних розподілених інформаційних системах, застосовувати системи криптографії в професійній діяльності.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі програмні результати навчання:

- визначати вимоги політики кібебезпеки та формувати свій профіль захисту відповідно до забезпечення послуг безпеки в інформаційній системі (ПРН4);
- ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в інформаційній системі (ПРН5);
- забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації (ПРН6);
- аналізувати технічні параметри діючих протоколів та механізмів захисту інформації з точки зору використання в комп'ютерних системах та мережах, впливу їх характеристик на основні показники інформаційних систем в цілому (ПРН7);
- проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів (ПРН7);
- забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій (ПРН7);
- здійснювати захист даних в корпоративних розподілених інформаційних системах, застосовувати системи криптографії в професійній діяльності (ПРН8).
-

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

Пререквізити дисципліни. Знання та вміння, отримані при вивченні дисциплін: «Комп'ютерна дискретна математика», «Алгоритмізація та програмування», «Операційні системи», «Об'єктно-орієнтований аналіз та конструювання програмних систем», «Алгоритми та структури даних», «Об'єктно-орієнтоване програмування».

Постреквізити дисципліни. Отримані знання при вивченні дисципліни «Комп'ютерне моделювання та оптимізація» формує базові знання для вивчення дисциплін, пов'язаних з моделюванням, чисельним розв'язком обчислювальних задач, оптимізації та розробки програмного забезпечення систем захисту інформації.

3. Зміст навчальної дисципліни

Розділ 1. Криптографічні засоби захисту інформації з симетричним ключем

Тема 1.1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки.
Тема 1.2. Традиційні криптографічні системи
Тема 1.3. Криптографічна стійкість шифрів
Тема 1.4. Блокові шифри як основа сучасних криптосистем
Тема 1.5. Криптосистема DES (Data Encryption Standard)
Тема 1.6. Сучасні симетричні криптосистеми

Розділ 2. Криптографічні засоби захисту інформації з відкритим ключем

Тема 2.1. Модель асиметричної системи
Тема 2.2. Протоколи розподілення ключів на основі центрів довіри
Тема 2.3. Протоколи асиметричного шифрування
Тема 2.4. Криптосистема RSA
Тема 2.5. Цифрові підписи
Тема 2.6. Програмна реалізація цифрового підпису засобами .NET
Тема 2.7. Криптографічні геш-функції

4. Навчальні матеріали та ресурси

Основна література

1. Венбо М. Современная криптография: теория и практика : пер. с англ. / М.Венбо – М. : Издательский дом "Вильямс", 2005. – 768 с.
2. Клінцв Л.М. Безпека програм і даних / Л.М. Клінцв Л.М. – Чернігов: ВСП Чернігівський інститут інформації, бізнесу і права, 2017. – 81 с.
3. Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
4. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 2011. – 248 с.

Додаткова література

1. Горбатов В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская – М. : Горячая линия – Телеком, 2019. – 248 с.

2. Гребенчук В. Г. Цифровая стеганография / В. Г. Гребенчук, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2012. – 272 с.
3. Грибунин В. Г. Цифровая стеганографія / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Прес, 2012. – 272 с.
4. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – 2-е изд. – СПб. : БХВ-Петербург, 2013. – 368 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. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.
7. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. Т.II. Информационная безопасность. – К. : Арий, 2008. – 344 с.
8. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров – М. : ДМК, 2000. – 448 с.
9. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 1. – 292 с.
10. Поповский В. В. Защита информации в телекоммуникационных системах : учебник : в 2 т. / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 2. – 252 с.
11. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд. / В. Столлингс; пер. с англ. – М. : Издательский дом "Вильямс", 2001. – 672 с.
12. Хайнс Б. Руководство по безопасности Windows Server 2008 / Б. Хайнс, Б. Курри, Д. Стин, Р. Харриссон. – Microsoft, 2008. – 326 с.
13. Хорошко В. А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с.
14. Чмора А.Л. Современная прикладная криптография / А. Л. Чмора. – М. : Гелиос АРВ, 2001. – 256 с.
15. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и Техника, 2004. – 384 с.

Навчальний контент

5. Методика опанування навчальної дисципліни(освітнього компонента)

Розділ 1. Криптографічні засоби захисту інформації з симетричним ключем.

Тема 1.1. Лекція 1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки. Основні поняття та визначення. Правові аспекти захисту інформації. Властивості інформації з точки зору її захисту. Рівні формування режиму інформаційної безпеки.

Тема 1.2. Лекція 1.Традиційні криптографічні системи. Криптографія і її основні поняття. Модель симетричної криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем. Види історичних шифрів.

Тема 1.3. Лекція 2. Криптографічна стійкість шифрів. Поняття криптографічної стійкості шифру. Обчислювальна складність алгоритму, основні класи складності. Межі застосування «грубої сили» до атак на шифри. Абсолютна криптостійкість шифрів, шифр Вернама. Поняття квантової криптографії.

Тема 1.4. Лекція 3. Блокові шифри як основа сучасних криптосистем. Блокові алгоритми і режими шифрування. Режим електронної кодової книги. Режим зціплення блоків по криптотексту. Режим зціплення блоків по криптотексту. Режим з оберненим зв'язком по виходу. Режим з лічильником. Схема Фейстеля.

Тема 1.5. Криптосистема DES (Data Encryption 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 1.6. Сучасні симетричні криптосистеми. 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 2. Криптографічні засоби захисту інформації з відкритим ключем

Тема 2.1. Модель асиметричної системи. Передумови виникнення асиметричних систем. Модель Діффі-Хеллмана криптосистеми з публічними ключами. Поняття односторонньої функції-пастки. Асиметрична криптосистема на основі використання «задачі рюкзака».

Тема 2.2. 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 аутентифікації Kerberos 5 і аутентифікація в Windows.

Тема 2.3. Протоколи асиметричного шифрування. Протокол Діффі-Хеллмана. Шифр Шаміра. Шифр Ель-Гамаля. Програмна реалізація алгоритму Діффі-Хеллмана засобами .NET.

Тема 2.4. Криптосистема RSA.Принцип шифрування в RSA. Генерація пари ключів шифрування. Алгоритм шифрування/розшифрування RSA. Програмна реалізація алгоритму RSA засобами .NET.

Тема 2.5. Цифрові підписи. Схема застосування цифрового підпису. Цифровий підпис на основі шифру RSA. Цифровий підпис на основі шифру Ель-Гамаля. Алгоритм цифрового підпису DSA (Digital Signature Algorithm). Стандарт ГОСТ Р34.10-94.

Тема 2.6. Програмна реалізація цифрового підпису засобами .NET

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

Тема 2.7. Криптографічні геш-функції

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

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 карантином. 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.

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

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування лекційних та практисчних 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 граничноготерміну виконання завдання (deadline)студент може отримати зменшену кількість балів від максимальної оцінки за відповідне завдання.

Протягом семестру студенти:

- виконують та захищають лабораторні роботи у відповідні терміни,
- пишутьмодульнуконтрольну роботу,
- повинні позитивно закрити дві атестації (в кінці березня та в серединітравня),
- по закінченні навчального процесу складають залік.

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

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 лабораторних робіт,
- модульну контрольну роботу (МКР) тривалістю 1 акад. година.

1. <u>Виконання завдань лабораторних робіт</u>

Завдання лабораторної роботи являє собою індивідуальне виконання робіт, що пов'язані з рішенням на ЕОМ заданої задачі комп’ютерного моделювання.

Вагові бали завдань наведено у таблиці.

Види завдань	*Внесок до семестрового рейтингу балів*
Виконання лабораторних робіт	
Завдання №1. Класичні і історичні шифри. Шифр Цезаря, Шифр Тритеміуса	*5*
Завдання №2. Класичні і історичні шифри. Шифр Гамування	*5*
Завдання №3. Класичні і історичні шифри. Шифр Книжковий	*10*
Завдання №4. Симетричні криптосистеми. Алгоритм DES.	10
Завдання №5. Шифрування з відкритим ключем на основі задачі рюкзака	5
Завдання №6. Асиметричні криптосистеми. Алгоритм RSA.	10
Завдання №7. Електронно-цифровий підпис на основі алгоритму RSA	5
Завдання №8. Хеш функція на основі RSA	10

Максимальна кількість балів за всі завдання дорівнює 60 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. Модульний контроль

Ваговий бал – 40.

Контрольна робота складається з 20 тестових завдань. За кожну вірну відповідь на запитання надається 2 бали.

Сума вагових балів контрольних заходів протягом семестру складає:

R= 60 + 40 = 100 балів.

Необхідною умовою допуску до заліку є зарахування усіх лабораторних 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

Робочу програму навчальної дисципліни (силабус):

Складенодоцент, д.т.н., професор Гаврилко Є.В.

Ухвалено кафедрою АПЕПС (протокол № _16__ від _18.06.2021 р._)

Погоджено Методичною комісією ТЕФ КПІ ім. Ігоря Сікорського [1] (протокол № 11 від 24.06.2021 р.)

[1] Методичною радою університету – для загальноуніверситетських дисциплін.