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

Кафедра інженерії програмного забезпечення в енергетиці (ІПЗЕ)

Методи і засоби протидії злоякісному програмному забезпеченню

Робоча програма навчальної дисципліни

(Силабус)

Реквізитинавчальної дисципліни

Рівень вищої освіти	другий (магістерський)
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем в енергетиці*
Статус дисципліни	*вибіркова*
Форма навчання	*Очна(денна)*
Рік підготовки, семестр	*1 курс весняний семестр*
Обсяг дисципліни	4кредити, 120 годин, з яких 54 години аудиторних (36 год лекції, 18 год лабораторні), 66 години становить самостійна робота
Семестровий контроль/ контрольні заходи	*Залік*
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* Лабораторні заняття: д.т.н., *професор Гаврилко Євген Володимирович, gev.1964@ukr.net, тел. 067-506-91-85*
Розміщення курсу	*Googleclassroom, Zoom, еКампус, Телеграмм*

Програманавчальної дисципліни

1. Описнавчальної 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 «Методи і засоби протидії злоякісному програмному забезпеченню» присвячене різним підходам захисту комп'ютерних програм і інформації від несанкціонованого впливу, внесенню змін, зникненню, крадіжкам.

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

Завдання. *Основними завданнями вивчення дисципліни " є отримання магістром компетенцій для того, щоб приймати участь у проектуванні інформаційних систем, розглянуті загальні питання криптоаналізу, зокрема типи криптоаналізу з точки зору інформації, яку має криптоаналітик; надана класифікація шифросистем стосовно захищеності (стійкості до криптоаналізу). Наведені приклади зламування шифросистем. Значна увага приділяється електронному цифровому підпису, який підтверджує дійсність і цілісність документа та засвідчує авторство, реалізації дискретних структур різних типів, створення складних процедур обробки. В результаті вивчення дисципліни у студентів повинні сформуватися наступні компетентності:*

В результаті вивчення дисципліни у студентів повинні сформуватися наступні компетентності:

загальні:

- Здатність до абстрактного мислення, аналізу та синтезу (ЗК1),
- Здатність спілкуватися іноземною мовою як усно, так і письмово (ЗК2),
- Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами інших галузей знань/видів економічної діяльності) (ЗК4).

фахові:

- Здатність розробляти, аналізувати та застосовувати специфікації, стандарти, правила і рекомендації в сфері інженерії програмного забезпечення (ФК5);
- Здатність проектувати архітектуру програмного забезпечення, моделювати процеси функціонування окремих підсистем і модулів (ФК3);
- Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах (ФК7);

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

- визначати вимоги політики безпеки та формувати свій профіль захисту відповідно до забезпечення послуг безпеки в інформаційній системі (ПРН1);
- ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в інформаційній системі (ПРН3);
- забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації (ПРН5);
- 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 ПЗ, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів (ПРН7);
- забезпечувати захист програмного забезпечення від несанкціонованих дій (ПРН12).

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», «Захист комп'ютерних програм».

***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 для систем захисту у бездротових, мобільних та хмарних системах накопичення, зберіганні і передавання інформації.

3. Зміст навчальної дисципліни

Зміст навчальної дисципліни

Розділ 1. Модель безпеки програмного забезпечення.

В ході вивчення дисципліни магістр розгляне основні аспекти захисту програмного забезпечення (ПЗ) і даних, що циркулюють в інфокомунікаційних системах. На початку вивчення дисципліни будуть розглянуті основні історичні аспекти захисту ПЗ. Буде вивчена Базова модель безпеки інформації в програмах і даних. Основним аспектом стане вивчення і відпрацювання підходів забезпечення безпеки мережевої інфраструктури, безпеки зберігання даних в ОС Microsoft, Linux. Також ми згадаємо порядок функціонування центру забезпечення безпеки Windows Security Center, центру забезпечення безпеки Windows Defender, Microsoft Baseline Security Analyzer і XSpider та сканеру безпеки XSpider. Коротко розглянемо мережеві антивірусні програмні засоби захисту ПЗ.

Розділ 2. Криптографічні засоби захисту інформації з симетричним ключем.

Для забезпечення захисту програм і даних використовується широкий арсенал криптосистем. Буде вивчено Блокові шифри як основа сучасних криптосистем, Криптосистема DES (Data Encryption Standard), 3DES, AES, SHA128, SHA128 та сучасні симетричні криптосистеми, в тому числі і на інших принципах.

Розділ 3. Криптографічні засоби захисту інформації з відкритим ключем.

На основі вивчення Моделей асиметричної системи будуть розглянуті протоколи розподілення ключів на основі центрів довіри, протоколи асиметричного шифрування. Основою стане Криптосистема RSA та цифровий підпис. Програмна реалізація цифрового підпису засобами .NET та криптографічні дайджести та Геш-функції. Крім того будуть розглянуті підходи, програмні засоби блокчейн.

Заплановані види навчальної діяльності та методи навчання

Планується проведення навчальних занять у виді лекцій та лабораторних занять. Основний змістовний матеріал дисципліни викладається на лекціях. Лабораторні заняття проводяться з метою закріплення знань з основних тем дисципліни; формування у студентів навичок і вмінь з використання технологій захисту інформації Web-рисурсів.

4. Навчальні матеріали та ресурси

HTML5 SecurityCheatsheet [Електронний ресурс]. – Режим доступу: https://html5sec.org.

AndrewHoffman .WebApplicationSecurity: ExploitationandountermeasuresforModernWebApplications, - :,2021.—336c.

Heiderich M., Nava E., Heyes G., Lindsay D. WebApplicationObfuscation. – ISBN-10: 1597496049.

McNab C. NetworkSecurityAssessment : KnowYourNetwork, secondedition. – ISBN-10:0-596-51030-6.

OWASP Foundation. OWASP TestingGuide v4.0 [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/Web_Application_Penetration_ Testing.

Ristic I. Bulletproof SSL and TLS: Understandinganddeploying SSL/TLS and PKI tosecureserversandWebapplications. – ISBN-10: 1907117040.

Stuttard D., Pinto M. TheWebApplicaionHackers'sHandbook: FindingandExploitingSecurityFlaws. – ISBN-10: 1118026470.

Zalewski M. TheTangledWeb: A GuidetoSecuringModernWebApplications. – ISBN-10: 1593273886.

Джонсон Дэн Берг, ДеоганДэниел, СаванаДэниел /Безопасноbydesign/. — Днепр:, 2021. — 432 с.

Домарев В. В. Защитаинформации и безопасностькомпьютерных систем / В. В. Домарев. – К. : Диа-софт, 2009. – 234 с.

Защита в виртуальнойсреде: чеклистугроз [Електронний ресурс]. – Режим доступу: https://habr.com/company/croc/blog/140044.

Інформаційна стійкість комп'ютерних технологій і мереж : навч. посіб. / А. В. Луговой, О. Г. Славко, П. П. Костенко, М. І. Гученко, М. М. Гузій. – Кременчук : Вид-во ПП Щербатих О. В., 2015. – 350 с.

Лисиченко М. Л. Методичні рекомендації щодо механізму перевірки письмових робіт на плагіат / М. Л. Лисиченко, В. І. Жила, А. В.Левкін. – Х.: ХНТУСГ, 2017. – 28 с.

Тарасюк О. М. Безопасность и устойчивостьWeb- и облачных систем. Практикум / О. М. Тарасюк, А. В. Горбенко; под ред. В. С. Харченко. – Министерствообразования и науки Украины, Национальныйаэрокосмическийуниверситетим. Н. Е. Жуковского «ХАИ», 2017. – 40 с.

Троян С. О. Захист інформаційних ресурсів: навчально-методичний посібник до курсу «Захист інформаційних ресурсів» / С. О. Троян. – Умань: [б. в.], 2012. – 120 с.

Навчальний контент

5. Методика опанування навчальної дисципліни(освітнього компонента)

Зміст навчальної дисципліни

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 Security Center.
Лекція 5. Центр забезпечення безпеки Windows Security Center
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.
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 (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).
Тема 1.7. Microsoft Baseline Security Analyzer і XSpider.
Лекція 7. 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.

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.

Блокові алгоритми і режими шифрування. Режим електронної кодової книги. Режим зціплення блоків по криптотексту.

Лекція 10. Блокові шифри.

Режим зціплення блоків по криптотексту. Режим з оберненим зв'язком по виходу. Режим з лічильником. Схема Фейстеля.

Тема 2.2. Криптосистема DES (Data Encryption Standard).

Лекція 10. 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 2.3. Сучасні симетричні криптосистеми.

Лекція 11. 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 3. Криптографічні засоби захисту інформації з відкритим ключем

Тема 3.1. Модель асиметричної системи.

Лекція 12. 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 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 аутентифікації Kerberos 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 (Digital Signature Algorithm). Стандарт ГОСТ Р34.10-94.
Тема 3.6. Програмна реалізація цифрового підпису засобами .NET.
Лекція 16. 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. Безключові геш-функції. Програмна реалізація алгоритмів гешування в .NET.

6. Самостійна робота студента

1. Розділ 1. Історія захисту ПЗ
2. Розділ 2. Безпека мережевої інфраструктури.
3. Розділ 3. Microsoft Baseline Security Analyzer і XSpider.
4. Розділ 4. Сканер безпеки XSpider.

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 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*
Завдання №1. Розробити технологію віддаленого виклику типу GRPC.процедур .	10
Завдання №2. Робота з брокерами повідомлень.	10
Завдання №3. На основі створеної **GRPC** *розробити децентралізовану систему.*	10

Максимальна кількість балів за всі завдання дорівнює 30 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 – 10.

Контрольна робота складається з 10 тестових завдань. За кожну вірну відповідь на запитання надається 1 бал.

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

Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль

1. *Істрія появи проблематики і необхідності захисту ПЗ.*

2. *Інфокомункаційні мережі та протоколи..*
3. *Асиметричні і семеричні шифри: особливості, подібності і відмінності.*
4. *Оцінка вразливості архітектури ПЗ.*
5. *Підходи проведення порівняння сучасних та ранніх версій додатків Windows Security Center..*
6. *Що має на озброєнні Windows Defender Baseline Security Analyzer і XSpider*
7. *Механізми сканеру безпеки XSpider.*

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри ІПЗЕ, д.т.н., професор Гаврилком Є.В.

Ухвалено кафедрою ІПЗЕ (протокол № 1 від 2.07.2022 р.)

Погоджено Методичною комісією ННІАТЕ КПІ ім. Ігоря Сікорського [1] (протокол № __ від _____.2022 р.)

1 Методичною радою університету– для загальноуніверситетських дисциплін.