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

Емблема кафедри (за наявності)

НН ФТІ Кафедра інформаційної безпеки

Системні технології для застосувань Windows

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	11 Математика і статистика
Спеціальність	113 Прикладна математика
Освітня програма	Математичні методи криптографічного захисту інформації
Статус дисципліни	Вибіркова
Форма навчання	очна(денна)
Рік підготовки, семестр	3 курс, осінній семестр
Обсяг дисципліни	ECTS -4, годин -120 Лекції: 36 Лабораторні: 36 СРС: 48
Семестровий контроль/ контрольні заходи	Залік, модульна контрольна робота
Розклад занять	http://rozklad.kpi.ua
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: кандидат технічних наук, доцент, Гальчинський Леонід Юрійович, hleonid@gmail.com Лабораторні: асистент Ільїн Костянтин Іванович
Розміщення курсу	https://do.ipo.kpi.ua/course/index.php?categoryid=18&browse=courses&perpage=20&page=9

Програма навчальної дисципліни

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

Мета: Основною метою навчальної дисципліни «Системні технології для застосувань Windows» є забезпечення теоретичної підготовки для сучасної технології системного програмування та дати знання і навички для створення системних програмних засобів оцінювання та забезпечення необхідного рівня захищеності інформації.

Предмет. Предметом навчальної дисципліни «Системні технології для застосувань Windows» є технологія спеціальних засобів Windows та їх застосування для кіберзахисту інформаційних систем.

Програмні результати. Процес вивчення дисципліни спрямований на формування наступних знань, умінь та навичок: знання складних програмних механізмів таких як динамічні бібліотеки, UAC, хуків, віддалений виклик та інші, а також набуття умінь та навичок технології розробки програм для безпека об'єктів Windows, програмна анатомія та захист від кейлогерів, асинхронний ввод/вивід Windows, багатопоточне програмування в умовах мереж(Сокети, Виклик віддаленої процедури (Remote Procedure Call); Розподілені обчислення DCOM. Усі ці знання, уміння і навички необхідні фахівцю з кібербезпеки для створення та використання засобів протидії кіберзагрозам.

Загальних компетентностей

ЗК1 – Здатність учитися і оволодівати сучасними знаннями.

ЗК7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК10 – Навички у використанні інформаційних і комунікаційних технологій.

Фахові компетентності

ФК6 – Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, з

використанням стандартних офісних додатків.

ФК7 – Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення.

ФК8 – Здатність використовувати сучасні технології програмування та тестування програмного забезпечення.

Програмні результати навчання

РН11 – Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів.

РН13 – Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп'ютерної математики.

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

Для успішного засвоєння дисципліни треба вміти програмувати на одній з мов структурної парадигми (найкраще С) та знати принципи організації програм, вільне володіння персональними комп'ютерами та іншими комп'ютерними засобами, базові знання дискретної математики, знання англійської мови в обсязі першого курсу. Мінімально необхідний знань та умінь студенти можуть отримати подолавши дисципліни «Програмування», «Системне програмування для багатозадачних операційних систем».

Засвоєні теоретичні знання та отримані практичні навички під час вивчення навчальної дисципліни «Системні технології для застосувань Windows», можна використовувати в подальшому під час навчання всіх навчальних дисциплін циклу навчальних дисциплін професійної та практичної підготовки здобувачів спеціальності 113 Прикладна математика.

3. Зміст навчальної дисципліни

- Розділ 1. Динамічно компоновані бібліотеки
- Розділ 2. Безпека Windows.
- Розділ 3. Асинхронний ввод/вивід Windows
- Розділ 4. Багатопоточне програмування в умовах мереж. Сокети
- Розділ 5. Виклик віддаленої процедури (Remote Procedure Call)
- Розділ 6. Компонентна технологія обробки даних
- Розділ 7. Розподілені обчислення DCOM

4. Навчальні матеріали та ресурси

Базові:

1. Sdk Win32 Api Programming https://pdfprodocs.vip/download/4677773-sdk-win32-api-programming Uploaded: 2022 Jul 03, 02:12
2. Системне програмування: конспект лекцій. Частина 1: Використання командного інтерпретатора CMD та вбудованих системних утиліт ОС Windows (Ukrainian Edition) Paperback – July 23, 2019 Ukrainian Edition by Артем Соколов (Author)
3. Pavel Yosifovich Windows 10 System Programming, Part 2 (2021) Режим доступу https://p302.zlibcdn.com/dtoken/fb4b7ff4e5bfb6236e22136c0199877d

Додаткові:

1. STRUCTURED COMPUTER ORGANIZATION ANDREW S. TANENBAUM Vrije Universiteit Amsterdam, The Netherlands TODD AUSTIN University of Michigan Ann Arbor, Michigan, United States 801 p. SIXTH EDITION 2013
2. Win32 Api Reference, Режим доступу https://pdfprodocs.vip/download/4677773-win32-api-

reference Uploaded: 2022 Jul 03, 01:39
3. Johnson M. Hart Windows System Programming Fourth Edition, Режим доступу https://fr.ua1lib.org/book/834488/1b7630?dsource=recommend
4. Bob Quinn, David Shute, Windows sockets network programming Режим доступу https://fr.ua1lib.org/book/490687/f2e413?dsource=recommend
5. Pavel Yosifovich Windows 10 System Programming, Part 1 (2020) Режим доступу https://edu.anarcho-copy.org/other/Windows/Windows%2010%20System%20Programming.pdf
6. Pavel Yosifovich Windows Kernel Programmin 2019 g Режим доступу https://p303.zlibcdn.com/dtoken/25b9ac5a56653852add3f8b421822a75
7. Andrea Allievi, Alex Ionescu, Mark Russinovich, David Solomon Windows Internals, Part 2, 7th Edition (2021) Режим доступу https://fr.ua1lib.org/book/17356100/092dac?dsource=recommend
8. Jeffrey Richter Programming Applications for Microsoft Windows ITPro collectionMicrosoft programming series, Seven Edition 1104 p.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Силабус побудований таким чином, що для виконання кожного наступного завдання студентам необхідно відкривати для себе нові поняття та принципи побудови комп'ютерних систем та засвоювати нові навички, опираючись на попередні. Особлива увага приділяється принципу мотивації студентів до активного навчання, у відповідності з яким студенти мають працювати над завданнями лабораторних робіт, які дозволять в подальшому вирішувати реальні проблеми інформаційної кібербезпеки.

Під час навчання студентам прищеплюються ідеї збереження та примноження моральних, культурних, наукових цінностей і досягнення суспільства на основі розуміння закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій. Навчання здійснюється на основі студентоцентрованого підходу та стратегії взаємодії викладача та студента з метою засвоєння студентами матеріалу та розвитку у них практичних навичок.

Для більш ефективного розуміння структури навчальної дисципліни та засвоєння матеріалу використовується електронні засоби, за допомогою яких:

- *спрощується розміщення та обмін навчальним матеріалом;*
- *здійснюється надання зворотного зв'язку студентам стосовно навчальних завдань та змісту навчальної дисципліни;*
- *ведеться облік виконання студентами плану навчальної дисципліни, графіку виконання навчальних завдань та оцінювання студентів.*

Під час навчання та для взаємодії зі студентами використовуються сучасні інформаційно-комунікаційні та мережеві технології для вирішення навчальних завдань, а також обладнання (проектор та електронні презентації для лекційних занять).

В рамках дисципліни заплановано наступні види навчальних занять:

- *лекції;*
- *лабораторні заняття;*
- *самостійна робота.*

Порядок освоєння дисципліни «Системні технології для застосувань Windows» наведений нижче.

№ з/п	Назви тем і питань, що виноситься на заняття	Кількість годин		
		Лек.ї	Лаб.	СРС
1	Розділ 1. Динамічно компоновані бібліотеки Поняття коду "незалежного від позиції" PIC. Схема зв'язування з розділюваними та динамічними бібліотеками. Глобальна таблиця зміщення. Етапи створення DLL. Неявне зв'язування DLL.Мангл і його	2	8	6

	подолання.Завантаження ресурсів з DLL. Плагіни. Поняття та використання			
2	Розділ 2. Безпека Windows. Спеціальні компоненти підсистеми захисту Windows. Модулі компонент підсистеми захисту Windows. Компоненти системи безпеки Windows. Схема взаємодії компонент системи безпеки Windows. Активні суб'єкти моделі безпеки Windows. Призначення маркера доступу (access token). Різновиди контролю доступу до об'єктів Windows. Програмний механізм вибіркового доступу до об'єктів Windows. Захищений виклик. Структура SECURITY_ATTRIBUTES . Анатомія дескриптора безпеки. Ідентифікатори безпеки(SID). Списки контролю доступу.Взаємодія маркера доступу та атрибутами безпеки об'єкта. Права об'єктів і доступ до об'єктів. Робота з ACL. Зв'язування списку ACL з SD. Програмна реалізація доступу до файлів. Програмна реалізація доступу до іменованих каналів. Реалізація захисту власних об'єктів Програмна реалізація надання привілеїв. Протокол Kerberos. Технологія перехоплення викликів функцій в чужих процесах – хуки.API-функції для хуків.Сутність хукінгу - підміна адрес бібліотек.Схема реалізації хукінгу. Методи реалізації перехоплення-перелік. Метод раннього зв'язування. Метод пізнього зв'язування. Метод модифікації машинного коду прикладної програми. Метод модифікації таблиці імпорту. Метод перехоплення функцій в режимі ядра. Використання WindowsHookEx для ін'єкції DLL в Windows . Фільтруючі функції хуків. Хукінг таблиці дескрипторів сервісних послуг. Пряма маніпуляція об'єктом ядра (DKOM). Приховування процесів у Windows. Бібліотека Detours . Цільова функція та функція батута. Використання бібліотеки Detours. Побудова кейлогера. Обробка даних, введених за допомогою клавіатури в Windows. Архітектура інтерактивних пристроїв введення Набір драйверів для системних пристроїв введення. Сирий вхідний потік (дані, отримані від драйвера) . Масив стану клавіатури клавіатури Особливості кейлогерів режиму ядра. Хуки клавіатури. Реалізація функції-фільтра. Виявлення перехоплювачів клавіатурних повідомлень	10	10	10
3	Розділ 3. Асинхронний ввод/вивід Windows Модель В/В Windows. Відносини об'єктів WINDOWS. Пакет запитів IO (IRP). Шляхи асинхронних IO запитів.Програмна реалізація асинхронного ВВ . Перевірка безпеки та доступу. Нативні IO API. Причини уповільнення виконання операцій введення і виведення властива. Організація асинхронного виклику. Різновиди методів асинхронного вводу /виводу Windows. Структура OVERLAPPED. Асинхронний багатопотоковий В/В. Попереджувальний В/В. Порти завершення вводу/виводу.	4		4
4	Розділ 4. Багатопоточне програмування в умовах мереж. Сокети Клієнт/ Серверна Модель обміну в мережі. Характеристики клієнта та сервера. Поняття протоколу. Модель ISO OSI. Сокети. Адресації та типи взаємодії. Сокети Берклі. Сокети та бібліотеки сокетів Ідентифікація сокетів. Виклик bind (). Структури адресації сокетів Типи сокетів. Сокети.Сімейства адресації і типи взаємодії. Сімейства адресації. Сокеты. Типи взаємодії. Процедури, які реалізують API Socket. Інтерфейс Winsock Windows. Мережеві API Windows. Windows Sockets API(загальні). Ініціалізація Winsock. Створення сокета. Серверні функції сокета. Функції listen та accept. Клієнтські функції сокета send і recv. Порівняння іменованих каналів і сокетів.	8	10	10

	Моделі вводу/виводу в Winsock 2.0. Модель блокування воду/виводу Модель мультиплексування вводу/виводу . Мультиплексування вводу/виводу за допомогою select() на блокуючому або не блокуючому сокеті. Мультиплексування вводу/виводу за допомогою функції WSAAsyncSelect (). Модель мережевого I/O з використанням WSAEventSelect() .Модель з перекриттям - Overlapped I/O Модель порту завершення Протоколи, орієнтовані на повідомлення			
5	Розділ 5. Виклик віддаленої процедури (Remote Procedure Call) Ідея виклику віддаленої процедури(RPC). Виклик функції за правилами C . Віддалений виклик. Поняття пари заглушок RPC. RPC – реалізація. Модель RPC. Структура виклику версії RPC Маршалінг аргументів. Реалізація віддаленого виклику. процедури.Заглушка клієнта. Реалізація віддаленого виклику процедури.Заглушка сервера. Транспортування виклику віддаленої процедури. Традиційний RPC. Асинхронний RPC. Мова визначення інтерфейсу IDL. Мова Microsoft Interface Definition Language (MIDL)	4		4
	Розділ 6. Компонентна технологія обробки даних Проблема інтеграції даних. Канонічна схема структурованої обробки даних. Вимоги до програмних компонент. Технології розподілених компонент. Поняття складеного документу. Технологія DDE (Dynamic Data Exchange). Технологія Object Linking and Embedding(OLE) . COM - Component Object Model, модель компонентних об'єктів. Множинне успадкування інтерфейсів COM Поняття автоматизації в COM. Перманентність даних COM-об'єкта Уніфікованою передача даних (Uniform Data Transfer) COM. COM і технології Інтернету. Технологія OLE DB. Технології доступу до даних Microsoft. Інтерфейс та коклас об'єктів COM Призначення глобально унікальний ідентифікатор (globally unique identifier – GUID. інтерфейс COM як абстрактний клас. Специфікація інтерфейсу COM. Сервери об'єктів COM. COM і багатопотопотоковість Поняття фабрики класу. Модифікація методів COM-об'єктів. Модель сервісів COM. COM і об'єктно-орієнтований підхід. Розробка клієнта COM. OLE Automation . Інтерфейс Idispatch. Методи диспінтерфейсу Метод Invoke . Клієнти та компоненти автоматизації. Раннє зв'язування в автоматизації. Пізнє зв'язування в автоматизації Автоматизація Microsoft Office. Тип автоматизації VARIANT Структура VARIANT. Модель об'єктів MS EXCEL. Microsoft Word - скорочена об'єктна модель.	4	8	10
	Розділ 7. Розподілені обчислення DCOM Основні поняття DCOM.. Архітектура DCOM. Служби (сервіси) DCOM. Безпека доступу до віддаленого об'єкту. Програмування DCOM	4		4
	Разом годин	36	36	48

Теми лабораторних занять

№	Теми *лабораторних* занять	Кількість ауд. годин
1.	Створення динамічних бібліотек в середовищі WIN 32	8
2.	Реалізація захисту доступу до файлів та іменованих каналів для Windows.	10
3.	Багатопоточне програмування в умовах мереж шляхом використання Winsock 2.0	10
4.	Програмування в середовищі Component Object Model, модель компонентних об'єктів	8

6. Самостійна робота здобувача

Самостійна роботи студента в основному концентрується на вирішенні завдань комп'ютерних практикумів згідно індивідуального варіанта для кожного студента, що потребує суттєвих зусиль, а також підготовці та оформлення звітності , яка потрібна при захисті кожного комп'ютерного практикуму. Крім того заохочується підготовка до лекційних занять та прочитання додаткових джерел. Терміни зазначені у календарному плані.

Назва розділу, теми, що виноситься на самостійне опрацювання	Кількість годин СРС
Плагіни. Поняття та використання	6
Набір драйверів для системних пристроїв введення. Сирий вхідний потік (дані, отримані від драйвера) . Масив стану клавіатури клавіатури Особливості кейлогерів режиму ядра. Хуки клавіатури. Реалізація функції-фільтра. Виявлення перехоплювачів клавіатурних повідомлень	6
Різновиди методів асинхронного вводу /виводу Windows. Структура OVERLAPPED Асинхронний багатопотоковий В/В. Попереджувальний В/В Порти завершення вводу/виводу.	6
Мультиплексування вводу/виводу за допомогою функції WSAAsyncSelect (). Модель мережевого I/O з використанням WSAEventSelect() .	6
Асинхронний RPC. Мова визначення інтерфейсу IDL. Мова Microsoft Interface Definition Language (MIDL	6
Мультиплексування вводу/виводу за допомогою функції WSAAsyncSelect (). Модель мережевого I/O з використанням WSAEventSelect() .Модель з перекриттям - Overlapped I/O Модель порту завершення Протоколи, орієнтовані на повідомлення	6
Автоматизація Microsoft Office. Тип автоматизації VARIANT Структура VARIANT. Модель об'єктів MS EXCEL. Microsoft Word - скорочена об'єктна модель	6
Безпека доступу до віддаленого об'єкту. Програмування DCOM.	6
Всього	48

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Студентам рекомендується відвідувати заняття, як лекції, на яких концентровано викладається теоретичний матеріал, так і лабораторні роботи, де розвиваються практичні навички та обговорюються теоретичний матеріал під час захисту робіт. Активним студентам можуть бути виставлені заохочувальні бали.

Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, які здатні розвинути практичні уміння та навички. Правила поведінки на аудиторних заняттях та контрольних заходах передбачають відключення телефонів та використання засобів зв'язку для пошуку інформації в Інтернеті. Захист лабораторних робіт /комп'ютерних практикумів проводиться в індивідуальному порядку при наявності документованої звітності (протокола), який проводиться у два етапи:

1. Демонструється робота завдання

2. Якщо демонстрація показала працездатність, проводиться співбесіда з метою перевірити рівень розуміння студентом представленої роботи та системних , програмних механізмів, на основі яких представлена.

На підставі цих трьох компонент : документування, демонстрації та відповідей під час співбесіди проставляється оцінка.

У випадку проявлення студента творчих елементів , оригінальних рішень можуть бути проставлені додаткові бали.

Неналежне оформлення звітності враховується в загальну оцінку, оскільки цього вимагають стандарти ДСТУ. Під час виконання практичних робіт а також під час контрольних заходів здобувачи повинні дотримуватись політики академічної доброчесності, згідно Кодексу Честі НТУУ "КПІ".

При виявленні порушення академічної доброчесності, зокрема при списуванні чужих робіт до студента можуть бути застосовані санкції аж до недопуску до захисту.

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

Поточний контроль:

№ з/п	Контрольний захід	%	Ваговий бал	Кіл-ть	Всього
1.	Лабораторна робота	20	20	4	80
2.	Модульна контрольна робота (МКР)	6	16	1	16
3.	Активність на лекційних та семінарських заняттях	10	0,22	36	4
	Всього				100

Штрафні та заохочувальні бали:

Заохочувальні бали		Штрафні бали	
Критерій	Ваговий бал	Критерій	Ваговий бал
Конспект лекційних занять[1]	3 бали	Порушення термінів виконання (лабораторнаробота) (за кожну таку лабораторну роботу)	-2 бали
Участь науково-технічнихконференціях з виступом та опублікуванням тез(за тематикою спеціальності)	2-5 балів	Невідповідність виконаногозавдання лабораторної роботи поставленому у варіанті.	-5 бали
Участь в університетських, міжнародних, всеукраїнських олімпіадах та/або конкурсах (за тематикою навчальної дисципліни)	1-10 балів		-2 бали за кожен тиждень

[1] *Мають бути законспектовані всі лекції власноруч, після перевірки конспекту лекційних занять конспект позначається для запобігання його передачі іншим студентам.*

Пропущені контрольні заходи

Результат модульної контрольної роботи для студента(-ки), який не з'явився на контрольний захід, є нульовим Повторне написання модульної контрольної роботи на підвищення оцінки не допускається.

Результати лабораторних робіт та тематичних завдань оголошуються кожному студенту окремо у присутності або в дистанційній формі та супроводжуються оціночними листами, в яких студенти можуть побачити свою оцінку за певними критеріями.

Результати семестрового індивідуального завдання оголошуються кожному студенту окремо у присутності або в дистанційній формі та супроводжуються позитивними коментарями та зауваженнями стосовно помилок. Оцінка на екзамені є сумою балів, отриманих за семестрову активність та оцінкою за відповідь на питання, включені у перелік для екзамену у пропорції 1 до 2.

– **Семестровий контроль: залік**

- *Здобувачі, що мають рейтинг ≥60 балів отримують залік без додаткових випробувань. Зі здобувачами, які мають рейтингову оцінку менше 60 балів, а також з тими, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті з дисципліни в семестрі викладач проводить семестровий контроль у вигляді співбесіди.*
- *Попередній рейтинг здобувача у цьому випадку скасовується (за винятком балів за семестрове індивідуальне завдання). Бали, отримані за виконання МКР, ЛР, Практ. (комп.практ) та штрафні і заохочувальні бали не входять до переліку індивідуальних семестрових завдань. Розмір шкали оцінювання додаткової контрольної роботи зменшується зі 100 балів на максимальне значення балів, передбачених за виконання відповідного індивідуального семестрового завдання.*
- Таблиця переведення рейтингових балів до оцінок за університетською шкалою:

Рейтингові бали, RD	Оцінка за університетською шкалою	Можливість отримання оцінки «автоматом»
95 ≤ RD ≤ 100	Відмінно	-
85 ≤ RD ≤ 94	Дуже добре	-
75 ≤ RD ≤ 84	Добре	-
65 ≤ RD ≤ 74	Задовільно	-
60 ≤ RD ≤ 64	Достатньо	-
RD < 60	Незадовільно	-

9. Додаткова інформація з дисципліни (освітнього компонента)

- *перелік питань, які виносяться на семестровий контроль (наприклад, як додаток до силабусу);*
- *можливість зарахування сертифікатів проходження дистанційних чи онлайн курсів за відповідною тематикою;*
- *інша інформація для студентів щодо особливостей опанування навчальної дисципліни.*

Робочу програму навчальної дисципліни (силабус):
Складено доцент, к.т.н., доцент Гальчинський Леонід Юрійович
Ухвалено кафедрою ІБ (протокол № 5 від 22.06.2022)
Погоджено Методичною комісією ННФТІ (протокол № 6__ від _30.06.2022)