Проєктування систем виявлення та запобігання вторгнень

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Шифр і назва спеціальності	123 Комп'ютерна інженерія	**Інститут**	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій
Назва програми	Сучасне програмування, мобільні пристрої та комп'ютерні ігри	**Кафедра**	Комп'ютерна інженерія та програмування
Тип програми	Освітньо-професійна	**Мова навчання**	українська

Викладач

Челак Віктор Володимирович, victor@chelak.com.ua

Аспірант 3 року навчання, асистент кафедри «КІП» НТУ «ХПІ», автор понад 40 наукових праць. Провідний лектор з дисциплін: «Антивірусний захист», «Reverse Programming» (англійською), «Software Means of Information Protection» (англійською), «Проєктування систем виявлення та запобігання вторгнень» та «Штучний інтелект в ігрових програмах».

Загальна інформація про навчальну дисципліну

Анотація	Дисципліна розглядає поняття комп'ютерної атаки, принципи побудови систем виявлення вторгнень, провинений рівень аналізу мережевого трафіку та контенту. Також розглядається інтелектуальний аналіз даних для систем виявлення та запобігання вторгненням. Теоретичний матеріал підкріплюється додатки з прикладами програмного коду, ілюстраціями та спеціально розробленими прикладами для отримання не лише розуміння, а й навичок використання методів виявлення та стратегій запобігання вторгнень у нетривіальних ситуаціях.
Цілі навчальної дисципліни	Формування системи знань з архітектури систем виявлення та запобігання вторгнень, принципів функціонування таких систем та практичні навики розробки систем виявлення та запобігання вторгнень для операційних систем та мережевого захисту.
Формат	Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль – диференційний залік.
Семестр	Шостий

Результати навчання:

N3 – Знати новітні технології в галузі комп'ютерної інженерії;

N8 – Вміти системно мислити та застосовувати творчі здібності до формування принципово нових ідей.

Теми, що розглядаються:

Тема 1. Комп'ютерні атаки.

Тема 2. Реалізація та запобігання комп'ютерним атакам.

Тема 3. Принципи побудови систем виявлення вторгнень.

Тема 4. Технології виявлення аномальної активності.

Тема 5. Технології побудови систем виявлення атак.

Тема 6. Огляд та особливості сучасних систем виявлення атак.

Тема 7. Аналіз мережевого трафіку та контенту (1 частина).

Тема 8. Аналіз мережевого контенту (2 частина).

Тема 9. Системи запобігання вторгнень.

Тема 10. Аналіз методів виявлення вторгнень.

Тема 11. Методи запобігання вторгнень.

Тема 12. Методи пошуку вторгнень

Тема 13. Запобігання вторгнень з використанням методів виявлення аномальних значень трафіка методами кратномасштабного аналізу.

Тема 14. Складні методи виявлення аномальних значень.

Тема 15. Інтелектуальний аналіз даних в системах виявлення та запобігання вторгнень.

Тема 16. Багатоагентні системи та системи аналізу захищеності.

Форма та методи навчання

На лекційних заняттях викладання матеріалу здійснюється в усній формі із записом основних положень лекції у конспект. Для демонстрації презентацій застосовується медіа проектор та комп'ютер.

На практичних заняттях здійснюється вивчення принципів функціонування систем виявлення та запобігання вторгнень, які були викладені на лекційних заняттях, та набуття практичних навиків роботи при проектуванні таких систем.

Під час самостійної роботи вдома студенти виконують завдання практичних робот для закріплення матеріалу, який був викладений на лекційних та практичних заняттях.

Додатково, студенти можуть приймати участь в розробці проектів, які передбачені у програмі «Інноваційний кампус» «НТУ» а також неформальної освіти організацій, які забезпечують надання освітніх послуг (NixSolution, GlobalLogic, EPAM та ін.).

Методи контролю

Поточний контроль реалізується у формі опитування під час проведення практичних занять, виконання домашніх завдань, проведення контрольних робіт (тестування).

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

- з лекційного матеріалу – шляхом перевірки контрольних робіт у формі тестування на кожної лекції;
- з практичних занять – за допомогою перевірки виконаних завдань;
- з домашніх завдань – за допомогою перевірки виконаних завдань.

Семестровий контроль проводиться у формі диференційного заліку у терміни, встановлені навчальним планом.

Підсумкова оцінка за семестр формується за результатами оцінок, отриманих за тестові завдання на кожної лекції та за виконання практичних робіт. Якщо виведена таким чином підсумкова оцінка не задовольняє студента, він має можливість оскаржити результати за процедурою передбаченою документом НТУ «ХПІ» «Положення про організацію освітнього процесу» пункт 8.8 за процедурою розділу 9.

Знання та компетенції, які студенти отримають на зовнішніх курсах компаній (GlobalLogic, EPAM та ін.) а також завдяки участі у програмі «Інноваційний кампус» НТУ «ХПІ» при відповідності освітньому компоненту, можуть бути частково зараховані у вигляді балів за практичну роботу, яка має прямий зв'язок з проектом, знанням та компетенцією, який студент розробив, отримав.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів для оцінювання успішності студента для диференційного заліку

Контрольні роботи	Практичні заняття	Сума
30	70	100

Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під системою оцінювання слід розуміти сукупність методів (письмові, усні і практичні тести, екзамени, проекти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними критеріями оцінювання для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

Критерії оцінювання – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв'язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об’єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100-бальної шкали (табл. 2). Оцінки обов’язково переводять у національну шкалу (з виставленням державної семестрової оцінки «відмінно», «добре», «задовільно» чи «незадовільно») та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ECTS

Рейтингова оцінка, бали	**Оцінка ECTS та її визначення**	**Національна оцінка**	**Критерії оцінювання**	
			позитивні	**негативні**
1	2	3	4	5
90-100	A	Відмінно	- **глибоке знання** навчального матеріалу модуля, що містяться в **основних і додаткових літературних джерелах;** - **вміння аналізувати** явища, які вивчаються, в їхньому взаємозв’язку і розвитку; - **вміння** проводити **теоретичні розрахунки**; - **відповіді** на запитання **чіткі**, **лаконічні, логічно послідовні;** **- вміння вирішувати складні практичні задачі.**	- відповіді на запитання можуть містити **незначні неточності**
82-89	B	Добре	- **глибокий рівень знань** в обсязі **обов’язкового матеріалу**, що передбачений модулем; - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **складні практичні задачі.**	- відповіді на запитання містять **певні неточності**
75-81	C	Добре	- м**іцні знання** матеріалу, що вивчається, та його **практичного застосування;** **-** вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **практичні задачі.**	**-** невміння використовувати теоретичні знання для вирішення **складних практичних задач**

1	2	3	4	5
64-74	D	Задовільно	- знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**; - вміння вирішувати прості **практичні задачі**.	- невміння давати **аргументовані відповіді** на запитання; - невміння **аналізувати** викладений матеріал і **виконувати розрахунки;** - невміння вирішувати **складні практичні задачі.**
60-63	E	Задовільно	- знання **основних фундаментальних положень** матеріалу модуля, - вміння вирішувати найпростіші **практичні задачі**.	- незнання **окремих (непринципових) питань** з матеріалу модуля; - невміння **послідовно і аргументовано** висловлювати думку; - невміння застосовувати теоретичні положення при розв'язанні **практичних задач**
35-59	FX (потрібне додаткове вивчення)	Незадо-вільно	**- додаткове вивчення** матеріалу модуля може бути виконане **в терміни, що передбачені навчальним планом**.	- незнання **основних фундаментальних положень** навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; - невміння розв'язувати **прості практичні задачі**
1-34	F (потрібне повторне вивчення)	Незадо-вільно	–	- повна **відсутність знань** значної частини навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; - незнання основних фундаментальних положень; - невміння орієнтуватися під час розв'язання **простих практичних задач**

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплект методичних матеріалів по дисципліні «Проєктування систем виявлення та запобігання вторгнень» знаходиться на сервері та сайті кафедри. Він вміщує: робочу програму та літературу.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1.1	О.І. Шелухін. Виявлення вторгнень в комп'ютерних мережах / О.І. Шелухін., Д. Ж. Сакалема та А.С. А.С. Філінова // 2013 .– 212р.
1.2	Tripathy, B. and Acharjya, D., 2014. Advances in secure computing, internet services, and applications. Hershey, PA: Information Science Reference.
1.3	Farooq Anjum; Petros Mouchtaris, "Intrusion Detection Systems," in Security for Wireless Ad Hoc Networks , Wiley, 2007, pp.120-159, doi: 10.1002/9780470118474.ch5.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

http://web.kpi.kharkov.ua/otp/ - сайт кафедри Комп'ютерної інженерії та програмування НТУ «ХПІ»

https://victor.chelak.com.ua/ - Сайт Челака Віктора (Лектора).

Структурно-логічна схема вивчення навчальної дисципліни

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
ВВП14 Антивірусний захист	ВВП12 Захист інформації в комп'ютерних мережах
СП9 Системне програмування	

Провідний лектор: _асист. каф. «КІП» Віктор ЧЕЛАК____