ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

ЗАТВЕРДЖУЮ
Декан ФІТ _____ Савенко О.С.
_____ 2022 р.

СИЛАБУС

Навчальна дисципліна ***Проєктування програмних систем захисту інформації***

Освітньо-професійна програма **для всіх ОП**

Рекомендований рівень вищої освіти **другий (магістерський)**

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	**Савенко Олег Станіславович**
Профайл викладача	http://kiis.khmnu.edu.ua/personnel/savenko-oleg-stanislavovych/
E-mail викладача(ів)	savenko_oleg_st@ukr.net
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=8236
Навчальний рік	2022-2023
Консультації	**Очні**: середа, 6-а пара, 1-108; п'ятниця, 6-а пара, 1-108; **онлайн:** за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	1	1	8	240	85	17	34	34		155			+	

Анотація дисципліни

В дисципліні планується освоєння студентами матеріалу з стохастичної комп'ютерної вірусології. загроз інформаційної безпеки, організації заходів безпеки в комп'ютерних системах, критеріїв ефективності антивірусних засобів, принципів побудови систем виявлення вторгнень, технологій побудови систем виявлення атак, перспективних методів протидії зловмисним програмам, методів виявлення аномалій, засобів і методів захисту від програмних закладок, проєктування систем захисту інформації з використанням «приманок» (honeypots, honeynet), методів інтелектуального аналізу даних в системах виявлення вторгнень, технологій безпечного програмування.

Дисципліна викладається для студентів денної форми навчання. При викладанні дисципліни використовуються активні і творчі форми проведення занять.

Мета дисципліни: 1) формування компетентностей, необхідних для абстрактного мислення, аналізу та синтезу на відповідних рівнях розроблення систем захисту інформації та їх компонентів; 2) розвиток у студентів розуміння процесів, які протікають в комп'ютерних системах і мережах, з метою забезпечення безпеки та захисту інформації в них; 3) надання знань, необхідних для подальшого вивчення спеціальних дисциплін та для практичної інженерної діяльності; 4) вироблення у студентів вміння використовувати набуті знання при розробці програмних засобів спеціалізованого призначення.

Завдання дисципліни. Надати студентам знання про організацію захисту інформації та безпеки комп'ютерних систем, а також про проєктування систем виявлення вторгнень і їх елементів.

Очікувані результати навчання.

Студент, який успішно завершив вивчення дисципліни, повинен: аналізувати, оцінювати і застосовувати на системному рівні сучасні програмні та апаратні платформи для ефективного виконання конкретних виробничих задач з програмної інженерії; визначати організаційно-управлінські рішення в умовах невизначеності та зміни вимог; конфігурувати програмне забезпечення, керувати його змінами та розробленням програмної документації на всіх етапах життєвого циклу; набувати нові наукові і професійні знання, вдосконалювати навички, прогнозувати розвиток програмних систем та інформаційних технологій; вміти використовувати методи фундаментальних і прикладних дисциплін інженерії програмного забезпечення при проектуванні та розробленні програмних систем захисту інформації в комп'ютерних системах та мережах, виявлення несанкціонованих вторгнень та аномалій, проявів зловмисного програмного забезпечення, кібер-загроз та кібер-атак.

Тематичний і календарний план вивчення дисципліни

№ тижня	**Тема лекції***	**Тема лабораторного заняття***	**Тема лабораторного заняття***	**Самостійна робота студентів**		
				Зміст	**Год.**	**Література**
1	**2**	**3**	**4**	**5**	**6**	**7**
1	Вступ до інформаційної та кібернетичної безпеки.	Використання програмного забезпечення YARA для виявлення зловмисного програмного забезпечення на основі правил	Ознайомлення з програмним забезпеченням YARA для виявлення зловмисного програмного забезпечення на основі правил	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1. Самостійна робота над розробкою програми до лабораторної роботи №1.	6	[1]-[7]; [9]-[12]
2				Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №1.	6	[1]-[7]; [9]-[12]; [16]
3	Поняття про комп'ютерні атаки.	Використання модулів PE та Cuckoo для YARA	Використання модулів PE та Cuckoo для YARA	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №2. Самостійна робота над розробкою програми до лабораторної роботи №2.	6	[6]- [7]; [9]- [12]; [8]; [14].
4				Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №2.	6	[6]- [7]; [9]- [12]; [8]; [14].

5	Принципи побудови систем виявлення вторгнень.	Проєктування та програмна реалізація розподіленої системи виявлення зловмисного програмного забезпечення та комп'ютерних атак в комп'ютерних мережах	Засоби проєктування та програмна реалізація розподіленої системи виявлення зловмисного програмного забезпечення та комп'ютерних атак в комп'ютерних мережах	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №3. Самостійна робота над розробкою програми до лабораторної роботи №3.	6	[6]-[12]; [14].
6				Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3. Самостійне опрацювання теоретичного матеріалу.	6	[6]-[12]; [14].
7	Технології побудови систем виявлення атак.	Реалізація сигнатурного аналізу для виявлення зловмисного програмного забезпечення у виконуваних файлах PE EXE з використанням розподіленої системи виявлення	Реалізація сигнатурного аналізу для виявлення зловмисного програмного забезпечення у виконуваних файлах PE EXE з використанням розподіленої системи виявлення	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №4. Самостійна робота над розробкою програми до лабораторної роботи №4.	6	[6]-[12]; [16].
8				Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4.	6	[6]-[12]; [14].
9	Статистичні методи виявлення аномальної поведінки трафіку мережі.	Реалізація евристичного аналізу для виявлення зловмисного програмного забезпечення у виконуваних файлах PE EXE з використанням розподіленої системи виявлення	Реалізація евристичного аналізу для виявлення зловмисного програмного забезпечення у виконуваних файлах PE EXE з використанням розподіленої системи виявлення	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №5. Самостійна робота над розробкою програми до лабораторної роботи №5.	6	[6]-[12]; [14].
10				Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5. Самостійне опрацювання теоретичного матеріалу.	6	[6]-[12]; [14].

11	Виявлення аномальних викидів мережного трафіку методами кратномасшта бного аналізу.	Реалізація аналізатора мережного трафіку з використанням розподіленої системи виявлення	Реалізація аналізатора мережного трафіку з використанням розподіленої системи виявлення	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №6. Самостійна робота над розробкою програми до лабораторної роботи №6.	6	[6]-[12].
12				Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6. Самостійне опрацювання теоретичного матеріалу.	6	[6]-[12]; [14].
13	Методи інтелектуально го аналізу даних в системах виявлення вторгнень.	Виявлення DDoS атак на основі аналізу мережного трафіку з використанням розподіленої системи виявлення	Засоби виявлення DDoS атак на основі аналізу мережного трафіку з використанням розподіленої системи виявлення	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №7. Самостійна робота над розробкою програми до лабораторної роботи №7.	6	[6]-[12]; [14].
14				Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7. Самостійне опрацювання теоретичного матеріалу.	6	[6]-[12]; [14].
15	Формальні моделі комп'ютерних вірусів, моделі поширення вірусів в комп'ютерних мережах.	Організація політик безпеки комп'ютерних систем та налаштування їх параметрів	Організація політик безпеки комп'ютерних систем та налаштування їх параметрів	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №8. Самостійна робота над розробкою програми до лабораторної роботи №8.	5	[9]-[10]; [13]; [16].
16				Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №8.	5	[9]-[10]; [13].
17	Методи забезпечення безпеки та захисту комп'ютерних систем від різних типів комп'ютерних вірусів.	Залікове заняття	Підсумкове заняття	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу.	5	[6]-[12]; [15].

Політика дисципліни.

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, практичні та лабораторні заняття згідно з розкладом, не запізнюватися на заняття, завдання виконувати відповідно до графіка. Пропущене лабораторне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. Набутті

особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання у ХНУ (http://khnu.km.ua/root/files/01/06/03/006.pdf).

Критерії оцінювання результатів навчання.

Поточний контроль здійснюється під час лекційних, практичних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни. Семестровий контроль проводиться у формі **заліку**. При цьому при виведенні остаточної оцінки враховуються результати поточного контролю.

При викладанні дисципліни використовуються такі види навчальних занять, як лекції, практичні та лабораторні роботи, індивідуальне консультування і керівництво самостійною роботою студента.

Кожний вид роботи з дисципліни оцінюється за *чотирибальною* шкалою. Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав лабораторні роботи, вважається невстигаючим.

При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на її початку; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи згідно з робочою програмою дисципліни.

Оцінка, яка виставляється за *лабораторне заняття*, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення звіту і графічної частини; вміння студента обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи. Для виконання програми дисципліни студент повинен отримати 8 позитивних оцінок за лабораторні роботи в семестрі. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті.

Пропущене лабораторне заняття студент повинен відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за тиждень до завершення теоретичних занять у семестрі.

При *оцінюванні знань* студентів викладач керується такими критеріями.

Оцінку „відмінно”, за шкалою ECTS – A (див. шкалу оцінок), отримує студент за глибоке і повне опанування змісту навчального матеріалу, в якому він легко орієнтується, понятійного апарату, за уміння зв’язувати теорію з практикою, вирішувати практичні завдання, висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає грамотний, логічний виклад відповіді (як в усній, так і в письмовій формі), якісне зовнішнє оформлення. Студент повинен набути практичних навичок із складання різних алгоритмів та розробки програм за цими алгоритмами. Оцінка "відмінно" виставляється студенту, який глибоко засвоїв предметну область та вміє застосовувати її на практиці. Студент не повинен вагатися при видозміні запитання, повинен робити детальні та узагальнюючі висновки.

Оцінку „добре”, за шкалою ECTS – B, отримує студент за повне засвоєння навчального матеріалу, володіння понятійним апаратом, орієнтування в вивченому матеріалі, свідоме використання знань для вирішення практичних завдань, грамотний виклад відповіді, але у змісті і формі відповіді мали місце окремі неточності (похибки), нечіткі формулювання закономірностей тощо. Відповідь студента повинна будуватись на основі самостійного мислення.

Оцінку „добре”, за шкалою ECTS – C, отримує студент за правильну відповідь з однією суттєвою помилкою.

Оцінки "задовільно", за шкалою ECTS – D, заслуговує студент, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, що справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент слабо знає структуру курсу, допускає помилки у відповіді, засвоїв і набув практичних навичок, але допустив неточності. Вагається при відповіді на видозмінене запитання, разом з тим студент володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Оцінки "задовільно", за шкалою ECTS – E, заслуговує студент за неповне опанування програмного матеріалу, але отримані знання і набуті практичні навички.

Оцінка „незадовільно”, за шкалою ECTS – FX, виставляється, коли студент має розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткових знань з курсу.

Оцінка „незадовільно”, за шкалою ECTS – F, виставляється студенту за повне незнання і нерозуміння навчального матеріалу або відмову від відповіді і передбачає повторне навчання студента з дисципліни.

Кожний вид роботи оцінюється за чотирибальною шкалою. Семестрова підсумкова оцінка визначається

як середньозважена з усіх видів робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

<table>
<tr><td colspan="8">Аудиторна робота</td><td colspan="4">Самостійна, індивідуальна робота</td><td>Форма контрольного заходу</td></tr>
<tr><td colspan="13">1 семестр</td></tr>
<tr><td colspan="4">Лабораторні роботи №:</td><td colspan="4">Практичні роботи №</td><td>Тестовий контроль:</td><td>КР</td><td></td><td>Залік</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">ВК:</td><td colspan="4">1</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Примітка: Т – тема дисципліни; ВК – ваговий коефіцієнт;

Якщо студент отримав негативну оцінку, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

Підсумкова семестрова оцінка за національною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення усіх оцінок до електронного журналу. Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС наведені у наступній таблиці.

Для переходу від вітчизняної оцінки до оцінки за шкалою ECTS необхідно знайти середньоарифметичну оцінку за вітчизняною шкалою, помножити її на відповідний ваговий коефіцієнт і, додавши всі складові, отримаємо суму балів, які визначать конкретну оцінку ECTS.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ECTS	Бали	Вітчизняна оцінка	
A	4,75-5,00	5	ВІДМІННО – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25-4,74	4	ДОБРЕ – повне знання навчального матеріалу з кількома незначними помилками
C	3,75-4,24	4	ДОБРЕ – в загальному правильна відповідь з однією суттєвою помилкою
D	3,25-3,74	3	ЗАДОВІЛЬНО – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00-3,24	3	ЗАДОВІЛЬНО – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00 -2,99	2	НЕЗАДОВІЛЬНО – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00-1, 99	2	НЕЗАДОВІЛЬНО – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ СТУДЕНТІВ

1. Основні поняття і терміни захисту інформації та безпеки комп'ютерних систем. Поняття: інформаційна безпека, кібернетична безпека (кібербезпека), захист інформації.

2. Властивості інформаційної безпеки. Принципи забезпечення інформаційної безпеки. Критерії оцінки інформаційної безпеки.

3. Методологічна база для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступеня захищеності. Чотири групи вимог захисту проти певних типів загроз. Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій».

4. Загрози безпеці інформації. Види захисту інформації. Руйнуючі програмні впливи. Причини трудомісткості рішення задачі забезпечення безпеки програмних систем. Зловмисне програмне забезпечення та комп'ютерні атаки.

5. Методи захисту від руйнуючих програмних впливів та їх виявлення. Покоління антивірусних програм. Типова архітектура програмних засобів антивірусного захисту. Недоліки існуючих засобів захисту та перспективні методи захисту від руйнуючих програмних впливів.

6. Критерії ефективності програмних засобів антивірусного захисту. ROC-аналіз в задачах виявлення зловмисного програмного забезпечення та комп'ютерних атак.

7. Поняття про комп'ютерні атаки.

8. Міжмережні екрани (firewall), антивіруси, системи виявлення атак (СВА) (Intrusion Detection System, IDS), системи контролю цілісності, криптографічні засоби захисту.

9. Типи атак. Моделі атак. Класифікація комп'ютерних атак. Основні типи аномалій в IP-мережах. Етапи реалізації атак.

10. Основні механізми реалізації атак. Вивчення оточення. Ідентифікація топології мережі. Ідентифікація вузлів. Ідентифікація сервісів або сканування портів. Ідентифікація операційної системи. Визначення ролі вузла. Визначення вразливості вузла. Реалізація атак: проникнення, встановлення контролю. Цілі реалізації атак. Завершення атаки. Засоби досягнення мети атаки.

11. Застосування технологій безпечного програмування.

12. Принципи побудови систем виявлення вторгнень.

13. Основні поняття про системи виявлення вторгнень. Класифікація систем виявлення атак.

14. Системи виявлення атак рівня мережі. Класифікація систем виявлення вторгнень.

15. Характеристики систем виявлення вторнень. Системи контролю цілісності. Монітори реєстраційних файлів.

16. Архітектура систем виявлення вторгнень. Основні елементи локальної та глобальної архітектур систем виявлення вторгнень.

17. Технології побудови систем виявлення атак.

18. Основні поняття про системи виявлення атак і технології виявлення. Існуючі технології систем виявлення вторгнень.

19. Методи, які використовують сигнатури вторгнень. Продукційні (експертні) системи виявлення вторгнень. Виявлення вторгнень, що базується на моделі. Аналіз переходу системи із стану в стан. Контроль натиснення клавіш.

20. Концепція виявлення комп'ютерних загроз. Підвищення ефективності систем виявлення атак.

21. Фазовий простір комп'ютерних атак.

22. Характеристика напрямків і груп методів виявлення вторгнень. Типова архітектура системи виявлення атак.

23. Групи методів з виявлення аномалій і зловживань: з контрольованим навчанням («навчання з учителем») і з неконтрольованим навчанням («навчання без учителя»).

24. Некомерційні системи виявлення комп'ютерних атак.

25. Аналіз мережного трафіку і контенту. Програми аналізу та моніторингу мережного трафіку. Отримання і підготовка вихідних даних для аналізу властивостей аномалій трафіку. Аналіз зразків трафіку. Траси і їх аналіз.

26. Тестування програмного забезпечення. Мережні атаки Portsweep, Neptune, Nmap, Mailbomb, Smurf. Типи сканування портів.

27. Застосування статичних методів в системах виявлення вторгнень. Статистичні методи виявлення аномальної поведінки. Профіль типової поведінки об'єкту.

28. Методи математичної статистики. Класифікація методів виявлення змін.

29. Помилки першого і другого роду в оцінці ефективності алгоритмів виявлення.

30. Рівень значущості і потужність критерію.

31. Статистичні тести. Критерії відповідності та однорідності. Критерій хі-квадрат. Критерії згоди.

32. Критерій Колмогорова-Смірнова.

33. Критерії оцінювання однорідності Вілкоксона-Манна-Уїтні.

34. Параметричний метод реєстрації змін.

35. Контрольні карти. Контрольні карти Шухарта, CUSUM.

36. Виявлення DDoS-атак із застосуванням алгоритму CUSUM.

37. Розподілене вторгнення. Три основні групи методів виявлення DDoS-атак. Виявлення DDoS-атак на основі відповідності між з'єднаннями, що встановлюються і закриваються. Вибір параметрів алгоритму CUSUM. Моніторинг різних IP-адрес у вхідному трафіку.

38. Непараметричні багатовимірні CUSUM тести для швидкого виявлення DoS-атак в комп'ютерних мережах. Непараметричний багатовимірний CUMSUM алгоритм.

39. Непараметричні методи. Контрольні карти EWMA.

40. Критерії аномальної поведінки та їх практичне застосування. Відсоткове відхилення. Ентропія. Методи описової статистики. Показник активності. Розподіл активності в записах аудиту. Вимірювання категорій. Порядкові виміру. Пошук і оцінка аномалій мережного трафіку на основі циклічного аналізу. Перевірка циклів з точки зору статистичної значущості. Комбінування і проектування циклів в майбутнє.

41. Виявлення аномалій методом головних компонент.

42. Сингулярний спектральний аналіз.

43. Метод головних компонент і виявлення аномалій у великих розподілених системах.

44. Переваги та недоліки статистичних методів.

45. Проєктування систем виявлення вторгнень із застосуванням статистичних методів виявлення аномальної поведінки мережного трафіку.

46. Застосування методів кратномасштабного аналізу в системах виявлення вторгнень.

47. Основи теорії вейвлетів. Неперервне вейвлет-перетворення. Дискретне вейвлет-перетворення. Алгоритм Малла.

48. Аналіз методів виявлення аномалій мережного трафіку на основі вейвлет.

49. Алгоритм виявлення аномалій методом дискретного вейвлет-перетворення.

50. Алгоритм виявлення аномалій за критерієм Фішера для викидів дисперсій.

51. Алгоритм виявлення аномалій на основі критерію Кохрана–Кокса.

52. Алгоритм виявлення аномалій за критерієм Фішера для викидів середніх значень. Вибір порогів виявлення.

53. Дискретне вейвлет-пакетне перетворення.

54. Виявлення DoS- і DDoS-атак методами мультифрактального аналізу. Фрактальні властивості телекомунікаційного трафіку.

55. Використання методів інтелектуального аналізу даних при проєктуванні підсистем систем виявлення вторгень. Методи Data Mining. Метод опорних векторів.

56. Виявлення аномалій трафіку із застосуванням нейронних мереж. Виявлення аномалій мережної активності із застосуванням апарату штучних нейронних мереж. Застосування нейронних мереж в задачах виявлення вторгнень. Архітектурні рішення СВВ. Результати експериментів.

57. Методи штучного інтелекту в задачах забезпечення безпеки комп'ютерних мереж.

58. Багатоагентні системи. Системи аналізу захищеності.

59. Методи штучних імунних систем і нейронних мереж для виявлення комп'ютерних атак. Побудова штучної імунної системи для виявлення комп'ютерних атак. Метод функціонування імунних нейромережних детекторів. Алгоритм функціонування системи виявлення вторгнень на основі штучних імунних систем і нейронних мереж.

60. Візуальний аналіз даних. Аналіз методів візуалізації.

61. Математичні аспекти безпеки та захисту комп’ютерних систем.

62. Формальні моделі комп’ютерних вірусів. Визначення комп’ютерного вірусу на основі модельного підходу. Моделі Ф. Коена. Модель Л. Адлемана. «Французька» модель. Інші формальні моделі. Модель китайських авторів Z. Zuo і M. Zhou. Векторна модель Д. Зегжди. Моделі на основі абстрактних «обчислювачів».

63. Моделі поширення вірусів в комп'ютерних мережах. Проста SI-модель експоненціального розмноження. SI-модель розмноження в умовах обмеженості ресурсів. SIS-модель примітивного протидії. SIR-модель кваліфікованої боротьби. Інші моделі епідемій.

64. «Екзотичні» віруси. Міфічні віруси. Batch-віруси. Віруси в початкових текстах. Графічні віруси. Віруси в інших операційних системах. Віруси в UNIX-подібних системах. Віруси для мобільних телефонів. Інша вірусна «екзотика».

65. Поширення вірусів. Епідемії мережних worm-вірусів Моделювання заходів пасивної протидії. Моделювання «контрчервя». Епідемії поштових worm-вірусів, файлових і завантажувальних вірусів. Епідемії мобільних worm-вірусів.

66. Методи забезпечення безпеки та захисту комп'ютерних систем від різних типів комп'ютерних вірусів.

67. Виявлення комп'ютерних вірусів. Аналіз непрямих ознак. Прості сигнатури. Контрольні суми. Питання ефективності. Вибір файлових позицій. Фільтр Блума. Метод половинного ділення. Розбиття на сторінки. Використання сигнатур для детектування поліморфних вірусів. Апаратне трасування. Емуляція програм. Протидія емуляції. «Глибина» трасування і емуляції.

68. «Рентгеноскопія» поліморфних вірусів.

69. Метаморфні віруси і їх детектування.

70. Етап «виділення та збору характеристик». Етап «обробки і аналізу». Аналіз статистичних закономірностей. Евристичні методи детектування вірусів. Виділення характерних ознак.

71. Логічні методи. Синтаксичні методи. Методи на основі формули Байеса. Методи, які використовують штучні нейронні мережі.

72. Концепція сучасного антивірусного детектора. Боротьба з вірусами без використання антивірусів. Файлові «ревізори».

73. Політики розмежування доступу. Криптографічні методи. Гарвардська архітектура ЕОМ. Перспективи розвитку і використання комп'ютерних вірусів. Віруси як «кіберзброя». Корисні застосування вірусів.

74. Засоби і методи захисту від програмних закладок. Проєктування систем захисту інформації з використанням «приманок» (honeypots, honeynet).

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою в модульному середовищі.

1.**Засоби захисту інформації** : методичні вказівки до виконання лабораторних робіт для магістрів спеціальностей "Комп'ютерна інженерія" та "Інженерія програмного забезпечення" / С. М. Лисенко, О. С. Савенко, К. Ю. Бобровнікова– Хмельницький : ХНУ, 2017. – 42 с.

2.**Безпека та захист комп'ютерних систем**: методичні вказівки до виконання лабораторних робіт для студентів спеціальності "Комп'ютерна інженерія"/ О. С. Савенко, А. О. Нічепорук, Д. М. Медзатий. – Хмельницький: ХНУ, 2021. – 86 с.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література.

1. Стратегія кібербезпеки України: Затверджено Указом Президента України від 15.03.2016 р. № 96/2016 // Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899.
2. ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) {Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241}
3. Міжнародний стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity: [Електронний ресурс]. – Режим доступу: https://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf.
4. National Institute of Standards and Technology (NIST). (2010a). Guide to Aplying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37.
5. National Institute of Standards and Technology (NIST). (2010b). Security and Privacy Controls for Federal Information Systems and Organizations, Building Effective Security Assessment Plans, NIST Special Publication 800-53A.

6. Богуш В.М., Довидьков О.А., Кривуца В. Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с. ISBN 978-966-2970-49-4.
7. Лукова-Чуйко Н.В. Методологічні основи забезпечення функціональної стійкості розподілених інформаційних систем до кібернетичних загроз / Дис. на здобуття наук. ступеня докт. техн. наук за спеціальністю 05.13.06 інформаційні технології. - Київ. Державний університет телекомунікацій. – 2018.
8. S. Lysenko, O. Savenko, K. Bobrovnikova, A. Kryshchuk. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks / Communications in Computer and Information Science, 2018.- 860, - Pp. 385-401.
9. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник] / В.Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко. – К.: ДУТ-КНУ, 2016. –178 с. ISBN 978–617–7092–78–9.
10. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с. ISBN № 978–966–2970–81–4.
11. Основи криптографічного захисту інформації: підручник / Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук / Вінниця: ВНТУ, 2011. – 199 с. ISBN 978-966-641-430-7.
12. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с. ISBN 978–617–7092–64–2.
13. Sergii Lysenko. Detection of the botnets' low-rate DDoS attacks based on self-similarity / Lysenko, S., Bobrovnikova, K., Matiukh, S., Hurman, I., Savenko, O. // International Journal of Electrical and Computer Engineering. – 2020. – Vol. 10., №4 – PP.-3651-3659, ISSN: 2088-8708.
14. Markowsky G. The technique for metamorphic viruses' detection based on its obfuscation features analysis / G. Markowsky, O. Savenko, S. Lysenko, A. Nicheporuk // CEUR-WS, ISSN: 1613–0073. – 2018. – Vol. 2104. – Pp. 680–687.
15. R. C. Joshi, A. Sardana. Honeypots A New Paradigm to Information Security. USA: Science Publishers. - 2011. - 339 p. ISBN 978-1-57808-708-2.
16. Савенко О.С. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах / Дис. на здобуття наук. ступеня докт. техн. наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Львів. Національний університет «Львівська політехніка». – 2019.

Додаткова література.

17. Center for Strategic & International Studies (CSIS). (2012). Twenty Critical Scurity Controls for Effective Cyber Defense: Consensus Audit Guidelines. Retrieved from SANS.org website January 24, 2013 at http://www.sans.org/critical-security-controls/
18. McAfee, Inc. (2009). Virtual Criminology Report – Cybercrime: The Next Wave. Santa Clara, CA. Retrieved February 2, 2010 from the McAfee websitehttp://www.mcafee.com/us/research/criminology _ report/default.html
19. Carlin D. Dynamic Analysis of Malware Using Run-Time Opcodes/ D. Carlin, P. O'Kane, S.Sezer // Data Analytics and Decision Support for Cybersecurity. – 2017. – Pp. 99-125.
20. Kotenko I. Modeling the Impact of Cyber Attacks / I. Kotenko, I. Saenko, O. Lauta // Cyber Resilience of Systems and Networks. – 2019. – Pp. 135-169.
21. Sochor T. Analysis of attackers against windows emulating honeypots in various types of networks and regions/ T. Sochor, M. Zuzcak, P. Bujok// 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). – Vienna (Austria), July 5-8, 2016. – Pp. 863-868.
22. Дудикевич В. Б. Квінтесенція інформаційної безпеки кіберфізичної системи / В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. — Львів: Видавництво Львівської політехніки, 2018. – № 887. – С. 58–68.
24. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
25. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
26. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

27. НД ТЗІ 2.5-008-02. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
28. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
29. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

Інформаційні ресурси

Електронний університет:

1. Модульне середовище для навчання (розміщені усі необхідні навчальні матеріали з дисципліни).
2. Електронна бібліотека університету.

Електронні ресурси:

3. AV-TEST | Antivirus & Security Software & AntiMalware Reviews. https://www.av-test.org/en/
4. Avast! [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.avast.com/index (Viewed on April 2, 2019). – Title from the screen.
5. AVG [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.avg.com (Viewed on April 2, 2019). – Title from the screen.
6. Avira [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.avira.com (Viewed on April 2, 2019). – Title from the screen.
7. ClamAV [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.clamav.net/ (Viewed on April 2, 2019). – Title from the screen.
8. DAMBALLA. Botnet communication topologies. Understanding the intricacies of botnet command-and-control [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.damballa.com/downloads/r_pubs /WP_Botnet_Communications_Primer.pdf (Viewed on April 2, 2019). – Title from the screen.
9. DAMBALLA. Botnet detection for communications service providers [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https:// www.damballa.com/ downloads/r_pubs/WP_Botnet_Detection_for_CSPs. pdf (Viewed on April 2, 2019). – Title from the screen.
10. https://www.virusbulletin.com/
11. ESET Endpoint Security [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: http://www.eset.com/ (Viewed on April 2, 2019). – Title from the screen.
12. Symantec Endpoint Protection [Electronic resource]: [Web-site]. – Electronic data. – Mode of access: https://www.anti-malware.ru/reviews/ Symantec_Endpoint_Protection (Viewed on April 2, 2019). – Title from the screen.

Розробник: д.т.н., проф. Савенко О.С.

Погоджено:
Зав. каф. КІІС: д.т.н., проф. Говорущенко Т.О.