СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

Ступінь освіти	магістр
Освітня програма	Комп’ютерна інженерія
Тривалість викладання	3, 4 чверті
Заняття:	ІІ семестр 2024/2025 н.р.
лекції:	1 година
лабораторні заняття:	2 години
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=5137

Інші додаткові ресурси: https://www.netacad.com/courses/cybersecurity/ccna-security

Кафедра, що викладає Інформаційних технологій та комп’ютерної інженерії

Інформація про викладача:

Викладач:
Шедловська Яна Ігорівна
доц. кафедри

Персональна сторінка
https://it.nmu.org.ua/ua/HR_staff/prepods/shedlovska.php

E-mail:
Shedlovska.Y.I@nmu.one

1. Анотація до курсу

Інформаційні процеси, що проходять повсюдно у світі, висувають на перший план, поряд із задачами ефективного опрацювання і передачі інформації, найважливішу задачу забезпечення безпеки інформації. Це пояснюється особливою значимістю для розвитку держави його інформаційних ресурсів, зростанням вартості інформації в умовах ринку, її високою уразливістю і нерідко значним збитком у результаті її несанкціонованого використання.

Курс «Захист інформації в інформаційно-комунікаційних системах» готує слухачів до сертифікаційного іспиту Implementing Cisco Network Security (IINS) (210-260), після якого можна отримати сертифікацію CCNA Security.

2. Мета та завдання курсу

Мета дисципліни – формування теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації, а також умінь та компетенцій, що пов’язані з вивченням основних принципів і методів організації захисту інформації в комп'ютерних системах, розглядаючи сучасні апаратні і програмні засоби, призначені для захисту інформації, основні принципи функціонування систем захисту, розроблених з використанням сучасних методів.

Завдання курсу:

- забезпечення глибокого теоретичного розуміння мережевої безпеки;
- навчання навичок і знань, необхідних для проектування і підтримки систем мережевої безпеки;
- ознайомлення з практичним досвідом з урахуванням галузевих особливостей для підготовки студентів до роботи в сфері мережевої безпеки і виконання робіт на початковому рівні в конкретних галузях;
- надання студентам можливості практичної роботи на IT-обладнанні для підготовки їх до здачі сертифікаційних іспитів і подальшій роботі в якості фахівців з мережевої безпеки.

3. Результати навчання

Студенти

Знають: сучасні загрози, можливі в інфраструктурі обчислювальних мереж, технології безпеки, моніторингу та вирішення проблем мережевих пристроїв для забезпечення цілісності, конфіденційності та доступності даних і пристроїв.

Розуміють: як працювати з технологіями AAA, ACL, Firewall, VPN.

Мають розуміння: про такі поняття, як: розробка політики безпеки для мережі, оцінка уразливостей і боротьба із загрозами мережної безпеки.

Мають базові розуміння: про основоположні принципи інформаційної безпеки необхідні для встановлення, усунення несправностей і моніторингу мережних пристроїв з метою підтримки цілісності, конфіденційності і доступності даних та пристроїв.

Уміють: управляти мережевими пристроями, здійснювати моніторинг активності мережі, а також вибирати відповідне рішення для захисту даних і доступу.

Компетенції:

- студент спроможний розробити комплексну політику мережевої безпеки;
- студент спроможний впровадити модель AAA на мережевих пристроях;
- студент спроможний конфігурувати систему запобігання вторгнень (IPS);
- студент спроможний налаштовувати статичні (site-to-site) VPN з'єднання;
- студент спроможний конфігурувати пристрої локальної мережі для контролю доступу опору атакам, захисту мережевих пристроїв і систем, а також підтримки цілісності і конфіденційності мережевого трафіку.
- студент спроможний виявляти і усувати потенційно небезпечні місця безпеки у комп'ютерних системах
- студент спроможний налаштовувати функціонування міжмережевих екранів на різних рівнях моделі OSI
- студент спроможний застосовувати симетричні та асиметричні алгоритми шифрування даних.
- студент спроможний розробляти та використовувати сучасні засоби та методи криптографічного захисту інформації.

4. Структура курсу

Лекція 1	**Вступ**
	Мета і завдання дисципліни “ Захист інформації в комп'ютерних системах”. Базові поняття. Загальна схема процесу забезпечення безпеки. Порушення комп'ютерних систем. Методи протидії порушенням.
Лекція 2	**Програмне забезпечення захисту в комп'ютерних системах**
	Комп'ютерні віруси та проблеми антивірусного захисту. Класифікація комп'ютерних вірусів. Життєвий цикл вірусів. Основні канали розповсюдження шкідливих програм. Антивірусні програми у комп’ютерних системах
Лекція 3	**Міжмережеві екрани**
	Функції міжмережевих екранів. Фільтрація трафіку. Особливості функціонування міжмережевих екранів на різних рівнях моделі OSI. Екрануючий маршрутизатор. Шлюз сеансового рівня. Прикладний шлюз. Шлюз експертного рівня. Схеми мережевого захисту на базі міжмережевих екранів.
Лекція 4	**Захист інформації у IP-мережах**
	Протокол захисту електронної пошти S/MIME. Система PGP. Інфраструктура захисту на прикладному рівні. Основи і типи мереж VPN. Загальні відомості про IPsec. Віддалений доступ. Мережі VPN віддаленого доступу з використанням IPsec.
Лекція 5	**Захист на канальному та сеансовому рівнях**
	Протоколи формування захищених каналів на канальному рівні: PPTP, L2F та L2TP. Протоколи формування захищених каналів на сеансовому рівні: SSL, TLS, SOCKS. Захист безпровідних мереж.
Лекція 6	**Технологія захисту AAA. Налаштування засобів AAA сервера мережевого доступу**
	Архітектура захисту AAA. Методи аутентифікації. Методи авторизації. Методи аудиту.
Лекція 7	**Методи виявлення кібератак у комп’ютерних системах**.
	Класифікація кібератак в комп’ютерних системах. Стек протоколів IoT Методи виявлення DoS/DDoS атак в комп’ютерних системах мережах IoT.
Лекція 8	**Основні поняття криптографічного захисту інформації**
	Симетричні криптосистеми шифрування. Основні режими роботи та особливості застосування блочного симетричного алгоритму. Алгоритм шифрування DES. Американський стандарт шифрування AES. Схема Фейстеля. Шифр Blowfish
Лекція 9	**Асиметричні шифри**
	Розподілення ключів по схемі Діффі-Хеллмана. Криптографічна система RSA. Криптографічна система Эль-Гамаля.
Лекція 10	**Методи шифрування інформації**
	Сумісне використання симетричних та асиметричних шифрів. Алгоритм SHA-1. Хэш-функції з ключем

ЛАБОРАТОРНІ ЗАНЯТТЯ

Лабораторна робота 1	Дослідження найпоширеніших типів вірусів. Встановлення та налаштування антивірусного програмного забезпечення
Лабораторна робота 2	Дослідження функціональних можливостей міжмережевих екранів

Лабораторна робота 3	Використання програми Wireshark для перегляду мережевого трафіку
Лабораторна робота 4	Дослідження TCP та UDP протоколів за допомогою програми Wireshark
Лабораторна робота 5	Дослідження захищених сокетів (протокол SSL)
Лабораторна робота 6	Дослідження головних особливостей DDoS (Distributed Denial of Service) атак та методи захисту від них
Лабораторна робота 7	Дослідження алгоритмів криптографічного захисту на основі підстановок та перестановок. Блочні шифри
Лабораторна робота 8	Дослідження процедур шифрування та дешифрування в криптосистемі RSA

5 Технічне обладнання та/або програмне забезпечення

1.Персональний комп'ютер або ноутбук зі сталим доступом до мережі Інтернет

2.Активований акаунт університетської пошти (student.i.p.@nmu.one) на Офіс365.

3.Активний обліковий запис у системі дистанційної освіти Moodle.

4.Програмне забезпечення:

- Платформа Windows 10
- Програмне забезпечення Wireshark.
- Програмне забезпечення Oracle Virtual Box.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
75 – 89	добре
60 – 74	задовільно
0 – 59	незадовільно

6.2. Підсумкова оцінка. Здобувач вищої освіти може отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Поточна успішність складається з оцінок за лекційну частину курсу та лабораторний практикум. Отримані бали додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

Максимальне оцінювання:

Теоретична частина	**Практична частина**		**Разом**
	При своєчасному складанні	**При несвоєчасному складанні**	
40	60	50	100

Лабораторні роботи приймаються за контрольними запитаннями до кожної з роботи.

Теоретична частина оцінюється за результатами здачі заліку, який містить 2 питання.

6.3. Критерії оцінювання теоретичної частини курс.

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

40 балів – дана розгорнута відповідь на два питання.

30 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання.

15 балів – два повна відповідь на одне питання або на два питання зі значними помилками.

5 балів – відповідь на одне питання із значними помилками.

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання звіту з практичної роботи.

З кожної практичної роботи здобувач вищої освіти отримує 6 запитань з переліку контрольних запитань. Відповідь на питання оцінюється максимально у 1 бал, причому:

– **1 бал** – відповідь вірна:

– **0,5 бала** – відповідь вірна, але не повна; відповідь вірна, але містить неточності та/або помилки;

– **0 балів** – відповідь невірна.

Максимальна оцінка за роботу складає 6 балів.

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2. Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

7.5. Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.6. Студентоцентрований підхід

Для врахування інтересів та потреб студентів на початку вивчення курсу здобувачам вищої освіти пропонується відповісти у системі Moodle на низку питань щодо інформаційного наповнення курсу. Відповідно до результатів опитування формується траєкторія навчання з урахуванням потреб студентів.

Під час навчання студенти реалізують своє право вибору індивідуальних завдань лабораторних робіт.

Наприкінці вивчення курсу та перед початком сесії здобувачам вищої освітим пропонується анонімно заповнити у системі Moodle електронні анкети для оцінки рівня задоволеності методами навчання і викладання та врахування пропозицій стосовно покращення змісту навчальної дисципліни. За результатами опитування вносяться відповідні корективи у робочу програму та силабус.

8 Рекомендовані джерела інформації

Основні:

1. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах: навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с.
2. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологія і мережах [Електронний ресурс] : навч. посіб. дл студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак – Київ : КПІ ім. Ігоря Сікорського, 2020. – 78 с.
3. Платформа дистанційної освіти мережної академії Cisco. Навчальний курс «Big Data & Analytics». [URL: https://www.netacad.com/courses/cybersecurity/ccna-security]
4. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем/ М.В.Гайворонський, О.М. Новіков.–К.: Видавнича група BHV,2009. – 608 с., іл
5. Юдін О.К., Конахович Г.Ф., Корченко О.Г., Захист інформації в мережах передачі даних: підручник/О.К. Юдін, Г.Ф.Конахович, О.Г.Корченко. –К: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. –714с., іл.

Додаткові:

1. Kizza J. M. Guide to Computer Network Security Springer. Series Title: Computer Communications and Networks, London 2015, 545 p. https://doi.org/10.1007/978-1-4471-6654-2
2. Olifer V. G., Olifer N. A. Computer networks: principles,technologies and protocols for network. Wiley India Pvt. Limited, ISBN 8126509171, 2006 – 1000 p.
3. Miller, A. R. The Cryptographic Mathematics of Enigma, Center for Cryptologic History National Security Agency [Электронний ресурс] / A. R. Miller // Google Диск. – 2019. – Режим доступу: https://drive.google.com/file/d/1By1nea1BhIiNwCfykdmQAawkyh5QT_hr/view. – Дата доступа: 20.02.2020.
4. Soni, A., Upadhyay, R., Jain, A. (2017). Internet of Things and Wireless Physical Layer Security: A Survey. In: Satapathy, S., Bhateja, V., Raju, K., Janakiramaiah, B. (eds) Computer Communication, Networking and Internet Security. Lecture Notes in Networks and Systems, vol 5. Springer, Singapore. **https://doi.org/10.1007/978-981-10-3226-4_11**
5. Shivanna, K., Deva, S.P., Santoshkumar, M. Privacy Preservation in Cloud Computing with Double Encryption Method. In: Satapathy, S., Bhateja, V., Raju, K., Janakiramaiah, B. (eds) Computer Communication, Networking and Internet Security. Lecture Notes in Networks and Systems, vol 5. Springer, Singapore, (2017) https://doi.org/10.1007/978-981-10-3226-4_12