СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Ступінь освіти	магістр
Освітня програма	Комп'ютерна інженерія
Тривалість викладання	3, 4 чверті
Заняття:	ІІ семестр 2020/2021 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=1663

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

Кафедра, що викладає Інформаційних технологій та комп'ютерної інженерії

Інформація про викладача:

Викладач:
Панферова Яна Володимирівна
ас. кафедри

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

E-mail:
panforova.ya.v@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.

4. Структура курсу

Лекція 1	**1. Загрози безпеки мережі. Оцінка політики захисту**
	Пояснення причин важливості питань безпеки. Опис загроз безпеки. Види атак.
Лекція 2	**2. Процедури забезпечення безпеки**

	Фізичний захист. Поточні виправлення й оновлення. Антивірусне ПЗ. Антиспам. Програми захисту від шпигунського і рекламного ПО. Засоби блокування спливаючих вікон. Захист даних
Лекція 3	**3. Списки керування доступом (ACL)**
	Призначення списку доступу. Принцип роботи списків управління доступом. Конфігурація списків керування доступом . Типи списків доступу. Правила розміщення списків управління доступом. Зв'язок списку доступу з інтерфейсом.
Лекція 4	**4. Технологія захисту AAA. Налаштування засобів AAA сервера мережевого доступу**
	Архітектура захисту AAA. Методи аутентифікації. Методи авторизації. Методи аудиту.
Лекція 5	**5. Налаштування CiscoSecure ACS і TACACS + / RADIUS**
	Основні особливості ZBF. Визначення класів трафіку. Застосування політик. Self-зона маршрутизатора. Налаштування CiscoSecure ACS і TACACS + / RADIUS.
Лекція 6	**6. Огляд технології шифрування. Застосування шифрування. Криптографія**
	Основні поняття криптографії. Криптографічні протоколи
Лекція 7	**7. Системи IDS IPS**
	Методи виявлення вторгнень. Конфігурація Cisco IPS через Cisco SDM.
Лекція 8	**8. Віртуальні приватні мережі, які використовують IPSec**
	Основи і типи мереж VPN. Загальні відомості про IPsec. Віддалений доступ. Мережі VPN віддаленого доступу з використанням IPsec

ЛАБОРАТОРНІ ЗАНЯТТЯ

Лабораторна робота 1	Налаштування на маршрутизаторах Cisco Syslog, NTP, SSH
Лабораторна робота 2	Конфігурація списків ACL для зменшення атак
Лабораторна робота 3	Налаштування AAA аутентифікації на маршрутизаторах Cisco
Лабораторна робота 4	Конфігурація a Zone-Based Policy Firewall
Лабораторна робота 5	Конфігурація IOS Intrusion Prevention System (IPS) з використанням CLI
Лабораторна робота 6	Конфігурація та перевірка Site-to-Site IPsec VPN з використанням CLI
Лабораторна робота 7	Налаштування GRE поверх IPsec

5 Технічне обладнання та/або програмне забезпечення

Технічні засоби навчання.
Комп’ютерний, клас.
Програмне забезпечення Cisco Packet Tracer 7.3.
Маршрутизатор (Cisco 2801 під керуванням ОС Cisco IOS 15.2(4)).
Комутатор (Cisco 2960 під керуванням ОС Cisco IOS 15.0(2)).
Програмне забезпечення Wireshark.
Дистанційна платформа MOODL.

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. Здобувачі вищої освіти можуть 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	Лабораторна частина		**Разом**
	При своєчасному складанні	При несвоєчасному складанні	
50	50	30	**100**

Лабораторні роботи приймаються за результатами вірних налаштувань мережного обладнання.

Теоретична частина оцінюється за результатами здачі білету диференційного заліку, який містить 25 тестових питань.

6.3. Критерії оцінювання підсумкової роботи

Під час проведення диференційного заліку наприкінці четвертої чверті здобувачі вищої освіти складають відповідні тести, кожен з яких складається з 25 питань. На кожне питання надається 4 варіанти відповіді, серед яких лише 1 – вірний. Максимальна оцінка за тест складає 50 балів. Опитування за тестом проводиться з використанням системи дистанційної освіти Moodle.

6.4. Критерії оцінювання лабораторної роботи

- **100 балів** – робота виконана повністю на 100%
- **90 балів** – робота виконана повністю, але містить неточності та/або недостатньо пояснень;
- **N балів** – відповідно N процентів виконаного завдання.

Максимальна оцінка за лабораторну роботу складає 100 балів. Максимальна оцінка за лабораторний практикум – 50 балів за формулою: (середнє зважене)/2.

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 Політика щодо оскарження оцінювання

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

7.5. 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.

7.6. 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

Базові

1. Платформа дистанційної освіти мережної академії Cisco. Навчальний курс «Big Data & Analytics». [URL: https://www.netacad.com/courses/cybersecurity/ccna-security]
2. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем/ М.В.Гайворонський, О.М. Новіков.–К.: Видавнича група BHV,2009. –608 с., іл
3. 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.
4. Богуш В.М., Довидьков О.А. Основи захищених інформаційних технологій/ В.М.Богуш, О.А.Довидьков. –К.: ДУІКТ, 2005. –450 с.
5. Организация защиты сетей Cisco. : Пер. с анг. – М. : Издательский дом «Вильямс», 2005. – 768 с.

Допоміжні

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учеб. пособие СПб.: Питер, 2006.- 957 с.
2. Введение в криптографию / Под общ. ред. В. В. Ященко. _ 4-е изд., доп. М.: МЦНМО, 2012. _ 348 с.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
4. А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. Основы защиты информации. – М.: «Академия», 2006. – 256 с.
5. Анин Б.Ю. Защита компьютерной информации. − СПб.: БХВ-Санкт-Петербург, 2000. − 384 с.
6. Теоретические основы компьютерной безопасности. : Учеб. пособие для вузов./ Девянин Н.Н., Михальский О.О. и др. − М.: Радио и связь, 2000. − 192 с.