Волинський національний університет імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

БЕЗПЕКА ІНФРАСТРУКТУРИ КОМП'ЮТЕРНИХ МЕРЕЖ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека
Форма навчання	Денна
Розробник (викладач)	Пасічник Володимир Володимирович, доктор технічних наук, професор
Контактна інформація	Електронна адреса викладача: icm.ikni@gmail.com Телефон: +38 (032)25-82-551
Семестр, курс	5 семестр, ІІІ курс
Обсяг дисципліни	Загальний обсяг: 4 кредитів / 120 годин. Аудиторних годин: 60; з них: лекцій – 20 год., лабораторних – 40 год. Самостійної роботи: 53 години.
Форма контролю	Екзамен
Час занять	Тижневих годин: 3,5 год. Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація дисципліни	Дисципліна "Безпека інфраструктури комп'ютерних мереж" належить до переліку нормативних навчальних дисциплін за освітнім рівнем "бакалавр" циклу навчальних дисциплін професійної підготовки. Предметом вивчення навчальної дисципліни є основні концепції і принципи безпеки комп'ютерних мереж, виявлення атак на інфраструктуру мережі.
Предреквізити дисципліни	Перелік дисциплін, які мають бути вивчені раніше: Комп'ютерні мережі; Кібернетична безпека; Криптографія; Системи та технології кібербезпеки. До початку вивчення курсу студент має вміти розробляти модель загроз, розробляти модель порушника; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; вибирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки;
Мета вивчення дисципліни	Метою викладання навчальної дисципліни "Безпека інфраструктури комп'ютерних мереж" є дати студентам знання та навички для формування системного підходу до забезпечення безпеки комп'ютерних мереж, навчити планувати і здійснювати організаційні заходи, а так само вибирати і застосовувати основні види технічних засобів захисту інформації. Основне завдання дисципліни дати студентам теоретичну та практичну підготовку з безпеки комп'ютерних мереж. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі. Здатність відновлювати нормальне

	функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов. Результатом вивчення дисципліни є набуття студентами таких компетентностей: – Здатність застосовувати знання у практичних ситуаціях. – Знання та розуміння предметної області та розуміння професії. – Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. – Здатність до пошуку, оброблення та аналізу інформації. – Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. – Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. – Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
Результати навчання	Вивчення дисципліни передбачає наступні результати навчання: – Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. – Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. – Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. – Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. – Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Усього	у тому числі			
		Лекції	Лабораторні заняття	Консультації	Самостійна робота
Змістовий модуль 1. Організаційні засади, методи та засоби безпеки комп'ютерних мереж					
Тема 1. Основні поняття, концепції і принципи безпеки мережевої інфраструктури.	8	2	2		4
Тема 2. Моделі управління мережевими ресурсами	8	2	2		4
Тема 3. Програмно-апаратні засоби забезпечення безпеки мережі	8	2	2		4
Тема 4. Технології забезпечення безпеки мережевої інфраструктури	10	2	4		4
Тема 5. Тенденції розвитку безпекових мережевих технологій	10	2	4		4
Тема 6. Засади організації захисту інформації в корпоративних мережах	10	1	4	1	4
Тема 7. Застосування систем виявлення вторгнень до корпоративних мереж	10	1	4	1	4
Разом за змістовим модулем 1	**64**	**12**	**22**	**2**	**28**
Змістовий модуль 2. Технології безпеки корпоративних мереж					
Тема 8. Захист на канальному і сеансовому рівнях	8	2	2		4
Тема 9. Захист на мережевому рівні – протокол IPSec	8	2	2		4
Тема 10. Інфраструктура захисту на прикладному рівні	8	1	2	1	4
Тема 11. Аналіз захищеності і виявлення атак	10	1	4	1	4
Тема 12. Захист від вірусів	10	1	4	1	4
Тема 13. Методи управління засобами мережевої безпеки	12	1	4	2	5
Разом за змістовим модулем 2	**56**	**8**	**18**	**5**	**25**
Всього годин	**120**	**20**	**40**	**7**	**53**

Оцінювання

Дисципліна складається з двох змістових модулів та її вивчення передбачає виконання лабораторних робіт. У цьому випадку підсумкова оцінка за 100-бальою шкалою складається із сумарної кількості балів за:

- поточне оцінювання з відповідних тем (максимум 40 балів);
- модульні контрольні роботи (максимум 60 балів).

Поточний контроль (40 балів)		**Модульний контроль (60 балів)**		**Загальна кількість балів**
Модуль 1		**Модуль 2**		
Змістовий модуль 1	**Змістовий модуль 2**	**МКР 1**	**МКР 2**	
Т 1-7	Т 8-13	Т 1-7	Т 8-13	100
20	20	30	30	

Якщо студент за період вивчення дисципліни набрав за поточний та модульний контроль мінімум 75 балів і погоджується із цим результатом, то оцінка за семестр може виставлятися без складання екзамену. В іншому випадку студент складає екзамен; максимальна кількість балів, яку можна отримати на екзамені – 60 балів. Оцінка за семестр, у випадку складання екзамену, є сумою балів поточного контролю та балів, отриманих під час екзамену.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття та списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов’язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, виконують всі завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна під час консультацій, одночасно при цьому з’ясувати незрозумілі моменти, задати запитання викладачу.

Перескладання модульних контрольних робіт заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

Рекомендована література

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Со-колов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К. : НАУ. – 2013. – 432 с.
3. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія / Д. В. Дубов. – К.: НІСД, 2014. – 328 с.
4. Жаровський Р.О Конспект лекцій з дисципліни «Захист інформації у комп'ютерних системах» розроблені у відповідності з навчальним планом за спеціальністю 123 "Комп'ютерна інженерія". – Тернопіль, 2019. – 268 с.
5. 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.
6. Олифер, В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. – Москва : Горячая линия-Телеком, 2017. – 644 с.
7. Словник термінів з кібербезпеки / За заг. ред. Копана О.В., Скулиша Є.Д. – К.: ВБ «Аванпост-Прим». – 2012. – 214 с.

Затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 3 від 5 жовтня 2020 р.

Завідувач кафедри  Сачук Ю.В.