ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
Тетяна ГОВОРУЩЕНКО
«31» серпня 2024 р.

СИЛАБУС

Навчальна дисципліна: *"Захист інформації в інформаційно-комунікаційних системах "*

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Кльоц Юрій Павлович Стецюк Микола Васильович Мостовий Сергій Володимирович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/sklad-kafedry/
E-mail викладача(ів)	klots@khmnu.edu.ua mykola.stetsiuk@khmnu.edu.ua serhii.mostovyi@khmnu.edu.ua
Контактний телефон	Наявні в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=6483
Навчальний рік, семестр	2024-2025, семестр III(осінньо-зимовий), IV (зимово-весняний)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ОД	2	3	5	150	51	17	34	-	-	99	-	-	-	+
ОД	2	4	5	150	54	18	36	-	-	96	+			+
Разом:			**10**	**300**	**105**	**35**	**70**			**195**				**2**

Анотація дисципліни

Дисципліна викладається для студентів очної денної форми навчання спеціальності «Кібербезпека та захист інформації». При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити: сигнали і процеси в системах захисту інформації; операційні системи та технології їх захисту.

Кореквізити: адміністрування та захист баз і сховищ даних; безпека бездротових мереж та інтернету речей; технології виявлення вразливостей та вторгнень; виробнича практика.

Мета дисципліни. Формування системи знань та розуміння предметної області щодо процесів в галузі інформаційних технологій, що охоплює використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-комунікаційних системах; управління інцидентами, моніторинг процесів функціонування інформаційно-комунікаційних систем.

Предмет дисципліни. Сучасні інформаційно-комунікаційні технології, сучасне програмно-апаратне забезпечення для виявлення та оцінювання можливих загроз, вразливостей та дестабілізуючих чинників в інформаційно-комунікаційних системах та моніторингу процесів функціонування інформаційно-комунікаційних систем, програмні та програмно-апаратні комплекси засобів захисту інформації в інформаційно-комунікаційних системах.

Завдання дисципліни. Забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека та захист інформації»:

компетентності:

ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

результати навчання:

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.

ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

ПРН 17. 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.

ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних

(автоматизованих) системах.

ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Студент, який успішно завершив вивчення дисципліни, повинен: *використовувати* результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності, пов'язаних з захистом інформації, що обробляється в інформаційно-комунікаційних системах; *виконувати* аналіз і декомпозицію інформаційно-телекомунікаційних систем та їх проектів, базуючись на стандартизованих технологіях та протоколах передачі даних; *використовувати* сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій, у тому числі програмні та програмно-апаратні комплекси засобів захисту інформації; *застосовувати* теорії, моделі та методи захисту для забезпечення безпеки інформації в інформаційно-комунікаційних системах; *вирішувати* задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки з метою протидії та попередження отримання несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах; *вирішувати* задачі захисту потоків даних в інформаційно-комунікаційних системах; *забезпечувати* процеси захисту та функціонування інформаційно-комунікаційних систем на основі практик, навичок та знань щодо топології мережі та інформаційних потоків; *підтримувати* працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах з метою *аналізувати*, *виявляти* та *оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки; *забезпечувати* належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-комунікаційних системах та *використовувати* інструментарій для моніторингу процесів функціонування інформаційно-комунікаційних систем; *здійснювати* процедури управління інцидентами, *проводити* розслідування, *надавати* їм оцінку та *забезпечувати* неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

Тематичний і календарний план вивчення дисципліни

Номер тижня	Номер теми	Тема лекції	Тема лабораторної роботи	Самостійна робота студента		
				Зміст	Години	Література
Перший семестр						
1	1	Поняття комп'ютерних мереж	**ЛР1.** Створення та налаштування мережі в Packet Tracer.	Опрацювання лекційного матеріалу, підготовка до виконання ЛР1.	5	[1] с.132-183 https://contenthub.netacad.com/itn?lng=uk-UA#10.4.4
2	1			Опрацювання лекційного матеріалу, підготовка до захисту ЛР1.	6	[1] с.132-183 https://contenthub.netacad.com/itn?lng=uk-UA#10.4.4
3	1	Основні мережеві пристрої	**ЛР2.** Моніторинг мережевого трафіку	Опрацювання лекційного матеріалу, підготовка до виконання ЛР2.	5	[2] с. 131-144 https://contenthub.netacad.com/itn?lng=uk-UA#3.7.10
4	1			Опрацювання лекційного матеріалу, підготовка до захисту ЛР2.	6	[2] с. 131-144 https://contenthub.netacad.com/itn?lng=uk-UA#3.7.10
5	1	Мережева адресація. MAC адреси. IP адреси.	**ЛР3.** Створення та встановлення SSL/TLS сертифікату.	Опрацювання лекційного матеріалу, продовження підготовки підготовка до виконання ЛР3.	5	[2] с.67-96 [5] с. 447-454
6	1			Опрацювання лекційного матеріалу, підготовка до захисту ЛР3.	6	[2] с.67-96 [5] с. 447-454
7	2	Мережеві загрози, нейтралізація мережевих загроз	**ЛР4.** Дослідження загроз в мережній безпеці	Опрацювання лекційного матеріалу, підготовка до виконання ЛР4.	4	[3] с. 5-18; [10] с. 46-109, https://contenthub.netacad.com/itn?lng=uk-UA#16.1
8	2			Опрацювання лекційного матеріалу, підготовка до захисту ЛР4.	4	[3] с. 5-18; [10] с. 46-109, https://contenthub.netacad.com/itn?lng=uk-UA#16.1
9	2	Захист доступу до пристроїв, призначення адміністративних ролей	**ЛР5.** Дослідження брандмауерів та міжмережних екранів, як засобів захисту мережі від атак	Опрацювання лекційного матеріалу, підготовка до виконання ЛР5.	4	[8] с. 142-168; [10] с. 111-216;[11] с. 399-466 Літ.: https://contenthub.netacad.com/itn/16.1.3#16.5.2
10	2			Опрацювання лекційного матеріалу, підготовка до захисту ЛР5.	4	[8] с. 142-168; [10] с. 111-216;[11] с. 399-466 Літ.: https://contenthub.netacad.com/itn/16.1.3#16.5.2
11	2	Моніторинг пристроїв і керування ними	**ЛР6.** Захист мережних пристроїв	Опрацювання лекційного матеріалу, підготовка до виконання ЛР6.	4	[9] с.166-206; [11] с. 372-399, [2] с.225 – 228
12	2			Опрацювання лекційного матеріалу, підготовка до захисту ЛР6.	4	[9] с.166-206; [11] с. 372-399, [2] с.225 – 228
13	2	Використання автоматичних функцій забезпечення безпеки	**ЛР7.** Налаштування захисту площин контролю та управління	Опрацювання лекційного матеріалу, підготовка до виконання ЛР7.	4	[11] с. 372-399, [2] с.165 – 167
14	2			Опрацювання лекційного матеріалу, підготовка до захисту ЛР7.	5	[11] с. 372-399, [2] с.165 – 167

15	3	Призначення AAA. Локальна аутентифікація AAA. Серверна аутентифікація AAA.	**ЛР8.** Налаштування автентифікації	Опрацювання лекційного матеріалу, підготовка до виконання ЛР8.	11	[2] с. 225 – 232, [9] с. 115-166
16	3			Опрацювання лекційного матеріалу, підготовка до захисту ЛР8.	11	[2] с. 225 – 232, [9] с. 115-166
17	3	Автентифікація RADIUS.	**Підсумкове заняття.**	Опрацювання лекційного матеріалу.	11*	[9] с. 115-166
Другий семестр						
1	1	Безпека кінцевих пристроїв. Фактори безпеки локальної мережі	**ЛР1.** Налаштування VPN тунелю між двома мережами.	Опрацювання лекційного матеріалу, підготовка до виконання ЛР1. Виконання КП.	5	[2] с. 225 – 232 [11] с.382-399
2	1			Опрацювання лекційного матеріалу, підготовка до захисту ЛР1. Виконання КП.	6	[2] с. 225 – 232 [11] с.382-399
3	1	Мережі VPN. Протокол IPsec	**ЛР2.** Дослідження протоколу IPsec.	Опрацювання лекційного матеріалу, підготовка до виконання ЛР2. Виконання КП.	5	[1] с.199-221 [3] с. 43-67 [9] с. 92-115
4	1			Опрацювання лекційного матеріалу, підготовка до захисту ЛР2. Виконання КП.	6	[1] с.199-221 [3] с. 43-67 [9] с. 92-115
5	1	Компоненти мережі IPsec. VPN і їх функціонування	**ЛР3.** Створення мережі IPsec VPN	Опрацювання лекційного матеріалу, продовження підготовки підготовка до виконання ЛР3. Виконання КП.	5	[3] с. 93-113 [9] с. 92-115
6	1			Опрацювання лекційного матеріалу, підготовка до захисту ЛР3. Виконання КП.	5	[3] с. 93-113 [9] с. 92-115
7	2	Технології IDS	**ЛР4.** Налаштування Cisco IOS IPS	Опрацювання лекційного матеріалу, підготовка до виконання ЛР4. Виконання КП.	4	[3] с. 154-189 https://contenthub.netacad.com/sec/8.4.1#8.4.3
8	2			Опрацювання лекційного матеріалу, підготовка до захисту ЛР4. Виконання КП.	4	[3] с. 154-189 https://contenthub.netacad.com/sec/8.4.1#8.4.3
9	2	Технології IPS. Сигнатури IPS. Впровадження IPS	**ЛР5.** Налаштування політики доступу на Cisco ASA	Опрацювання лекційного матеріалу, підготовка до виконання ЛР5. Виконання КП.	4	[2] с.34-46; [6] с. 7-62 https://contenthub.netacad.com/sec/9.2.1#9.2.4
10	2			Опрацювання лекційного матеріалу, підготовка до захисту ЛР5. Виконання КП.	4	[2] с.34-46; [6] с. 7-62 https://contenthub.netacad.com/sec/9.2.1#9.2.4
11	3	Конфігурація брандмауера ASA. Об'єктні групи, списки контролю доступу, NAT на основі ASA. Конфігурація ASA VPN	**ЛР6.** Налаштування брандмауера на основі ідентифікації Cisco ASA	Опрацювання лекційного матеріалу, підготовка до виконання ЛР6. Виконання КП.	8	[2] с.63-67, 199-250 https://contenthub.netacad.com/sec/9.3.1#9.3.5
12	3			Опрацювання лекційного матеріалу, підготовка до захисту ЛР6. Виконання КП.	8	[2] с.63-67, 199-250 https://contenthub.netacad.com/sec/9.3.1#9.3.5
13	4	Системи керування мережею (NMS)	**ЛР7.** Моніторинг мережевого обладнання з використанням протоколу SNMP	Опрацювання лекційного матеріалу, підготовка до виконання ЛР7. Виконання КП.	5	[2] с.189-198; [7] с. 59-63; [9] с.10-80 https://contenthub.netacad.com/sec/9.3.1#9.3.5

14	4			Опрацювання лекційного матеріалу, підготовка до захисту ЛР7. Виконання КП.	6	[2] с.189-198; [7] с. 59-63; [9] с.10-80 https://contenthub.netacad.com/sec/9.3.1#9.3.5
15	4	Протокол SNMP. Протокол IP SLA	**ЛР8.** Дослідження інструментів тестування мережевої безпеки.	Опрацювання лекційного матеріалу, підготовка до виконання ЛР8. Виконання КП.	5	[2] с.183-186 [1] с.81-91; [2] с.189-198; [11] с.111-123
16	5			Опрацювання лекційного матеріалу, підготовка до захисту ЛР8. Виконання КП.	6	[2] с.183-186 [1] с.81-91; [2] с.189-198; [11] с.111-123
17	5	Розробка комплексної політики безпеки. Тестування безпеки мережі	Підсумкове заняття. Захист КП.	Захист курсового проекту.	6	[3] с. 236-283; [8] с. 177-240; [11] с.134-154
18	5		Підсумкове заняття. Захист КП.	Захист курсового проекту.	5	[3] с. 236-283; [8] с. 177-240; [11] с.134-154

***** Зменшення годин самостійної роботи через збільшення часу аудиторних занять за чисельником / за знаменником (розрахунок здійснено відповідно до розкладу)

Завдання до виконання курсового проекту з дисципліни

Комплексне завдання:

- розробити топологію інформаційно-комунікаційної мережі для підприємства згідно свого варіанту;
- змоделювати зазначену мережу в САПР Packet Tracer;
- провести аналіз та оцінювання загроз, уразливостей та дестабілізуючих чинників розробленої мережі, визначити рівень захищеності мережі та запропонувати до неї відповідні політики безпеки.

№ варіан-ту	**Тип**	**Кількість основних провайдерів**	**Кількість резервних провайдерів**	**Кількість груп примі-щень**	**Характеристика підмереж**	**Кількість приміщень**	**Відстань до окремого приміщення**
1	Мініготель	1	0	1	Відеоспостереження, гостьова, IOT обладнання, адміністрації і персоналу	6	
2	Магазин і офіс, склад (окремий провайдер)	2	1 (для магазину і офісу)	2	Відеоспостереження магазину і складу з переглядом адміністрацією, робоча з сервером 1С, wi-fi на складі	7	10км
3	Магазин з офісом	1	1	2	Відеоспостереження магазину з переглядом адміністрацією, робоча з сервером 1С, гостьова	5	300м
4	Юридична компанія	1	1	1	Локальна з доступом в інтернет, локальна з доступом до внутрішніх ресурсів (веб), гостьова	9	
5	Відділення банку	2 (балансування навантаження)		1	Відеоспостереження, гостьова, адміністрації, персоналу	6	
6	Супермар-кет	2 (балансування навантаження)	1	1	Відеоспостереження, гостьова, локальна з доступом в інтернет, локальна з доступом до внутрішніх ресурсів (веб)	5	
7	IT компанія	2 (балансування навантаження)		1	Локальна з доступом в інтернет, локальна з доступом до внутрішніх ресурсів, гостьова	8	
8	Мінішкола	1	0	1	Відеоспостереження, вчителів і адміністрації, учнів	9	

					(локальні ресурси, дозволені зовнішні ресурси)		
9	Датацентр (Офіс, Безносе-редньо серверна)	2 (балансування навантаження) підключення до датацентру, офіс підключений через датацентр		2	Зовнішня з доступом до серверів, локальна з доступом до серверів для службових операцій, локальна співробітників з доступом до інтернету, відеоспостереження, логування доступу і кодових замків	5	300м

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 і лабораторні роботи згідно з розкладом, не запізнюватися на заняття, курсовий проект виконувати відповідно до графіка. Пропущені лабораторні роботи студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До лабораторних робіт студент має підготуватися за відповідною темою і проявляти активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ.

Оцінювання результатів навчання студентів

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

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

Аудиторна робота		**Підсумковий контрольний захід**
IV семестр		
Лабораторні роботи №:		Семестровий контроль (іспит)
1 – 8		0,4
ВК:	0,6	
V семестр		
Лабораторні роботи №:		Семестровий контроль (іспит)
1 – 8		0,4
ВК:	0,6	

Умовні позначення: Т – тема дисципліни; ВК – ваговий коефіцієнт.

Календарний план виконання курсового проєкту

Зміст етапу	Термін виконання
1 Вибір та затвердження теми курсового проєкту; розробка завдання на курсовий проєкт; складання календарного графіка виконання курсового проєкту	1-2 тиждень
2 Аналіз об'єкта захисту та аналіз захищеності його інформації від несанкціонованого втручання	3-4 тиждень
3 Аналіз та опис наявної системи захисту інформації	5-8 тиждень
4 Проєктування пропонованої КСЗІ	9-12 тиждень
5 Написання тексту пояснювальної записки та розробка	13-14 тиждень

графічних матеріалів	
6 Остаточне коригування курсового проєкту з урахуванням зауважень керівника; оформлення курсового проєкту, як документа відповідно до вимог	15 тиждень
7 Підготовка до захисту та захист курсового проєкту	16 тиждень

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами (курсове проектування)

1 етап	2 етап	3 етап	4 етап	5 етап	Захист КП
ВК:0,1	ВК:0,2	ВК:0,1	ВК:0,2	ВК:0,2	ВК:0,2

При оцінюванні курсового проекту враховується дотримання в ній ряду вимог. Виконання курсового проекту передбачає ґрунтовне вивчення літературних джерел з обраної теми, теоретичні знання та практичні навички, аналізу особисто зібраного фактичного матеріалу, або опрацювання матеріалів інших дослідників, власне творче бачення студента. При проведенні захисту та оцінюванні курсових робіт (проектів) необхідно керуватися такими критеріями.

Оцінка «відмінно» виставляється, якщо: курсовий проект виконаний в повному обсязі відповідно до завдань, робота демонструє творчий підхід, технічно досконала. У пояснювальній записці теоретичний матеріал подано послідовно, грамотно використано спеціальну термінологію. Результат виконаної роботи повністю відповідає чинним якісним та кількісним показникам або може бути кращий від них. Під час захисту курсового проекту на всі запитання дано вичерпну відповідь.

Оцінка «добре» виставляється, якщо: студент виконав поставлені завдання на належному рівні та показав володіння системними професійними знаннями в повному обсязі. Проект виконана з врахуванням встановлених вимог, демонструє творчий підхід, але має незначні технічні недоліки. Під час захисту курсового проекту у відповідях можливі 1-2 неточності в термінології і другорядних висновках.

Оцінка «задовільно» виставляється, якщо: студент при виконанні курсового проекту на різних етапах припускався помилок і неточностей, які частково виправляв самостійно та після консультації з керівником. Проект має окремі недоліки, але в цілому має завершений вигляд. Під час захисту курсового проекту студент на частину поставлених запитань не дав відповіді, або ж відповіді були не повні.

Оцінка «незадовільно» виставляється, якщо курсовий проект виконаний не у повному обсязі та з відхиленням від визначеної тематики. Проект не відповідає встановленим вимогам, містить грубі помилки, під час захисту курсового проекту студент не дав відповіді на більшість поставлених запитань. Такий курсовий проект потребує переробки.

Оцінювання лабораторних робіт. 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; вільне володіння студентом спеціальною термінологією і уміння фахово обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні

підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань,
	передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив 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 додаткової роботи з вивчення дисципліни.

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

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані

терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно”.

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**	
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 двома-трьома суттєвими помилками
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 здобутих студентами результатів навчання

Третій семестр

1. Завдання безпеки комп’ютерних мереж. Фізичний захист мереж.
2. Програмні та апаратні засоби захисту мереж.
3. Адміністративні заходи безпеки комп’ютерних мереж.
4. Поняття комп’ютерних мереж.
5. Типи мереж.
6. Апаратні та програмні компоненти комп’ютерних мереж.
7. Мережні топології.
8. Модель OSI.
9. Модель TCP.
10. Мережеві протоколи.
11. Протоколи дротових і бездротових мереж.
12. Стандартні порти.
13. Протоколи WLAN.
14. Протоколи Bluetooth, NFC і RFID.
15. Протоколи Zigbee і Z-Wave.
16. Покоління систем стільникового зв'язку.
17. Мережеві служби.
18. Клієнт-серверна архітектура.
19. DHCP-сервер.
20. DNS сервер.
21. Сервер друку.
22. Файловий сервер.
23. Веб сервер.
24. Поштовий сервер.
25. Проксі сервер.
26. Сервер автентифікації.
27. Syslog сервер.
28. Основні мережеві пристрої.
29. Мережева інтерфейсна карта.
30. Повторювачі, мости та концентратори.
31. Керовані та некеровані комутатори.
32. Бездротові точки доступу.
33. Маршрутизатори.
34. Міжмережеві екрани.
35. Системи виявлення вторгнень IDS.
36. Системи запобігання вторгненням IPS.
37. Пристрої UTM.
38. MAC адреси.
39. IP адреси.
40. Мережеві протоколи. SSL. TSL. SOCS.
41. Безпека мережевих пристроїв
42. Мережеві загрози
43. Нейтралізація мережевих загроз
44. Захист доступу до пристроїв
45. Призначення адміністративних ролей
46. Моніторинг пристроїв і керування ними
47. Використання автоматичних функцій забезпечення безпеки
48. Захист площини управління
49. Технології брандмауера.
50. Списки контролю доступу (ACL).
51. Зональні міжмережеві екрани
52. Автентифікація, авторизація та облік

53. Призначення AAA.
54. Локальна аутентифікація AAA
55. Серверне рішення AAA.
56. Серверна аутентифікація AAA.
57. Серверна авторизація та облік AAA.
58. Автентифікація RADIUS.

Четвертий семестр

1. Безпека локальних та віртуальних приватних мереж (LAN, VPN)
2. Безпека кінцевих пристроїв
3. Фактори безпеки локальної мережі
4. Мережі VPN
5. Протокол IPsec
6. Компоненти мережі IPsec VPN і їх функціонування
7. Реалізація мереж IPsec VPN між двома пунктами за допомогою CLI
8. Системи виявлення та запобігання вторгнень
9. Технології IDS
10. Технології IPS. Сигнатури IPS. Впровадження IPS
11. Пристрої забезпечення безпеки
12. Cisco Adaptive Security Appliance
13. Конфігурація брандмауера ASA
14. Об’єктні групи, списки контролю доступу, NAT на основі ASA
15. Конфігурація ASA VPN
16. Моніторинг мережі
17. Системи керування мережею (NMS)
18. Протокол SNMP
19. Протокол IP SLA
20. Управління безпекою мережею
21. Тестування безпеки мережі
22. Розробка комплексної політики безпеки

Методичне забезпечення

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі на сторінці дисципліни

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
2. Організація комп’ютерних мереж: підручник/ Ю.А. Тарнавський, І.М. Кузьменко. – Київ: КПІ ім. І. Сікорського, 2018. – 259 с.
3. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
4. Сучасні інформаційно-комунікаційні технології: Навчальний посібник. / Г.Г.Швачич, В.В.Толстой, Л.М.Петречук, Ю.С.Іващенко, О.А.Гуляєва, Соболенко О.В. – Дніпро: НМетАУ, 2017. –230 с.
5. Проектування та монтаж локальних комп’ютерних мереж/ І. М. Журавська. – Миколаїв: Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.

6. Defensive Security Handbook/ Lee Brotherston, Amanda Berlin. - O'Reilly Media, Inc., 2017. – 247 p.
7. Технології та протоколи інфокомунікаційних мереж. Частина 1[Електронний ресурс]/ О.Л. Недашківський. – Київ, 2017. - http://www.dut.edu.ua/uploads/l_1799_76743031.pdf
8. Моделювання систем захисту інформації/А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. - 273 с.
9. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с.
10. 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.
11. Технології захисту інформації: навчальний посібник/ С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
12. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання. – Видання друге (доповнене)/ За загальною ред. Довгого С.О. – К.: «Азитут-Україна». – 2013. – 608 с.
13. Комп'ютерні мережі та Інтернет. Навчальний посібник/ В.М. Франчук. – К.: НПУ імені М.П. Драгоманова, 2015 р. – 141 с.

Додаткова

14. Unix and Linux system administration handbook. Fifth edition/ E. Nemeth, G. Snyder, T. R. Hein, B. Whaley, D. Mackin. – Pearson Education, Inc, 2018. – 1179 p.
15. Operating System Concepts Essentials. Second Edition/ A. Silberschatz, P. B. Galvin, G. Gagne. – John Wiley & Sons, Inc, 2014. – 760 p.
16. Unix and Linux System Administration and Shell Programming. – PR NTR KMT, 2014. – 328 p.
17. The Practice of System and Network Administration. Volume 1. Third Edition/ Th. A. Limoncelli, Ch. J. Hogan, S. R. Chalup. – Virtual.NET Inc., Lumeta Corporation, 2017. – 1426 p.
18. Linux Command Line. A Beginner's Guide/ Ray Yao. – Ray Yao, USA, 2014. – 90 p.
19. Network Security Assessment. Third edition/ Ch. McNab. – O'Reilly Media, Inc., 2017. – 546 p.
20. Wireless Networks [Електронний ресурс]/ J. Salazar. – Czech Technical University of Prague, 2017. – режим доступу: http://standardsoui.ieee.org/oui/oui.txt
21. Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. – Software Architecture. – 2016. – P. 274-290.
22. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення/ Бурячок В. Л. та ін. /Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. – №3. – С. 48-61.
23. Уязвимости корпоративных информационных систем [Електронний ресурс]. – Positive Technologies, 2017. – режим доступу: https://www.ptsecurity.com/upload/ corporate/ru-ru/analytics/Corp-Vulnerabilities-2017-rus.pdf
24. Комп'ютерні мережі. Книга 1/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2013. – 256 с.
25. Комп'ютерні мережі. Книга 2/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2014. – 312 с.
26. Основи інформаційної та кібернетичної безпеки. Навчальний посібник/ В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання MOODLE (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань) Доступ до ресурсу: https://msn.khmnu.edu.ua.

2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php.

Розробник	_____	к.т.н., доцент	Ю.П. Кльоц
	Підпис	Вчений ступінь, звання	Ініціали, прізвище викладача(ів)

Погоджено

Гарант освітньої програми	_____	к.т.н., доцент	В.М. Чешун
	Підпис	Вчений ступінь, звання	Ініціали, прізвище

Зав. кафедри кібербезпеки	_____	к.т.н., доцент	Ю.П. Кльоц
	Підпис	Вчений ступінь, звання	Ініціали, прізвище