ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету IT
Підпис Олег САВЕНКО Ім'я, ПРІЗВИЩЕ
«31» 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційно-комунікаційних системах

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	10 кредитів ЄКТС
Шифр дисципліни	ОПП.06
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

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

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доц. Юрій КЛЬОЦ
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Третій, четвертий
Кредити ЄКТС	10,0
Форми навчання, для яких викладається дисципліна	Денна

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.

Зміст навчальної дисципліни. Завдання безпеки комп'ютерних мереж. Фізичний захист мереж. Програмні та апаратні засоби захисту мереж. Адміністративні заходи безпеки комп'ютерних мереж. Поняття комп'ютерних мереж. Типи мереж. Апаратні та програмні компоненти комп'ютерних мереж. Мережні топології. Модель OSI. Модель TCP. Мережеві протоколи. Протоколи дротових і бездротових мереж. Стандартні порти. Протоколи WLAN. Протоколи Bluetooth, NFC і RFID. Протоколи Zigbee і Z-Wave. Покоління систем стільникового зв'язку. Мережеві служби. Клієнт-серверна архітектура. DHCP-сервер. DNS сервер. Сервер друку. Файловий сервер. Веб сервер. Поштовий сервер. Проксі сервер. Сервер автентифікації. Syslog сервер. Основні мережеві пристрої. Мережева інтерфейсна карта. Повторювачі, мости та концентратори. Керовані та некеровані комутатори. Бездротові точки доступу. Маршрутизатори. Міжмережеві екрани. Системи виявлення вторгнень IDS. Системи запобігання вторгненням IPS. Пристрої UTM. MAC адреси. IP адреси. Мережеві протоколи. SSL. TSL. SOCS. Мережеві загрози. Нейтралізація мережевих загроз. Призначення адміністративних ролей. Моніторинг пристроїв і керування ними. Використання автоматичних функцій забезпечення безпеки. Захист площини управління. Технології брандмауера. Списки контролю доступу (ACL). Зональні міжмережеві екрани. Призначення AAA. Локальна аутентифікація AAA Серверне рішення AAA. Серверна аутентифікація AAA. Серверна авторизація та облік AAA. Автентифікація RADIUS. Фактори безпеки локальної мережі. Мережі VPN. Протокол IPsec. Компоненти мережі IPsec VPN і їх функціонування. Реалізація мереж IPsec VPN між двома пунктами за допомогою CLI. Системи виявлення та запобігання вторгнень. Моніторинг мережі. Системи керування мережею (NMS). Протокол SNMP. Протокол IP SLA. Тестування безпеки мережі. Розробка комплексної політики безпеки.

Пререквізити: Сигнали і процеси в системах захисту, Операційні системи та технології їх захисту

Кореквізити: Технології виявлення вразливостей та вторгнень, Адміністрування та захист баз і сховищ даних, Виробнича практика, Комплексні системи захисту інформації

Запланована навчальна діяльність: лекції – 35 год., лабораторні роботи – 70 год., самостійна робота – 195 год., разом 300 год.

Методи навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Форми оцінювання результатів навчання: захист лабораторних робіт, тестування, захист курсового проекту, підсумковий контрольний захід (семестровий контроль).
Вид семестрового контролю: іспит – 3,4 семестр, курсовий проект – 4 семестр.

Навчальні ресурси:

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. 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.
3. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с
4. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua.
5. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php.

Викладач: канд. техн. наук, доцент Кльоц Ю.П.

ВСТУП

Дисципліна „Захист інформації в інформаційно-комунікаційних системах” - складова професійної підготовки бакалаврів зі спеціальності „Кібербезпека та захист інформації”, є однією зі спеціальних профілюючих дисциплін.

Метою дисципліни є 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.

Предметом дисципліни є 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.

Завданням дисципліни є 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.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:			
	лекції	лабораторні роботи	практичні заняття	самостійну роботу
Третій семестр				
Тема 1. Основні поняття комп'ютерних мереж	6	12		33
Тема 2. Безпека мережевих пристроїв	8	12		33
Тема 3. Автентифікація, авторизація та облік	3 (4/2)*	10		33
Разом за 1-й семестр:	**17 (18/16)***	**34**		**99**
Четвертий семестр				
Тема 1. Безпека локальних та віртуальних приватних мереж (LAN, VPN)	6	12		32
Тема 2. Системи виявлення та запобігання вторгнень	4	4		16
Тема 3. Пристрої забезпечення безпеки	2	8		16
Тема 4. Моніторинг мережі	4	4		16
Тема 5. Управління безпекою мережі	2	8		16
Разом за 2-й семестр:	**18**	**36**	-	**96**

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік змістових модулів, тем лекцій, їх анотації	Кількість годин
	Третій семестр	
Тема 1. Основні поняття комп'ютерних мереж		
1	**Поняття комп'ютерних мереж.** Типи мереж. Апаратні та програмні компоненти комп'ютерних мереж. Мережні топології. Модель OSI. Модель TCP. Літ.: [1] с.132-183	2
2	**Основні мережеві пристрої.** Мережева інтерфейсна карта. Повторювачі, мости та концентратори. Керовані та некеровані комутатори. Бездротові точки доступу. Маршрутизатори. Міжмережеві екрани. Пристрої UTM. Літ.: [2] с. 131-144	2
3	Мережева адресація. MAC адреси. IP адреси. Літ.: [2] с.67-96	2
Тема 2. Безпека мережевих пристроїв		
4	Мережеві загрози, нейтралізація мережевих загроз Літ.: [3] с. 5-18; [10] с. 46-109	2
5	Захист доступу до пристроїв, призначення адміністративних ролей Літ.: [8] с. 142-168; [10] с. 111-216;[11] с. 399-466	
6	Моніторинг пристроїв і керування ними Літ.: [9] с.166-206; [11] с. 372-399	2
7	Використання автоматичних функцій забезпечення безпеки Літ.: [11] с. 372-399	2
Тема 3. Автентифікація, авторизація та облік		
8	Призначення AAA. Локальна аутентифікація AAA. Серверна аутентифікація AAA. Літ.: [9] с. 115-166	2

9	Автентифікація RADIUS. Літ.: [9] с. 115-166	2
Разом за 3-й семестр:		**17 (18/16)***
Четвертий семестр		
Тема 1. Безпека локальних та віртуальних приватних мереж (LAN, VPN)		
1	Безпека кінцевих пристроїв. Фактори безпеки локальної мережі Літ.: [11] с.382-399	2
2	Мережі VPN. Протокол IPsec Літ.: [3] с. 43-67; [9] с. 92-115	2
3	Компоненти мережі IPsec. VPN і їх функціонування Літ.: [3] с. 93-113; [9] с. 92-115	2
Тема 2. Системи виявлення та запобігання вторгнень		
4	Технології IDS Літ.: [3] с. 154-189	2
5	Технології IPS. Сигнатури IPS. Впровадження IPS Літ.: [2] с.34-46; [6] с. 7-62	2
Тема 3. Пристрої забезпечення безпеки.		
6	Конфігурація брандмауера ASA. Об'єктні групи, списки контролю доступу, NAT на основі ASA. Конфігурація ASA VPN Літ.: [2] с.63-67 199-250	2
Тема 4. Моніторинг мережі		
7	Системи керування мережею (NMS) Літ.: [2] с.189-198; [7] с. 59-63; [9] с.10-80	2
8	Протокол SNMP. Протокол IP SLA Літ.: [1] с.81-91; [2] с.189-198; [11] с.111-123	2
Тема 5. Управління безпекою мережею		
9	Розробка комплексної політики безпеки. Тестування безпеки мережі Літ.: [3] с. 236-283; [8] с. 177-240; [11] с.134-154	2
Разом за 4-й семестр:		**18**

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

Перелік лабораторних робіт

№ п/п	Тема лабораторної роботи	Кількість годин
Третій семестр		
1	Створення та налаштування мережі в Packet Tracer. Літ.: https://contenthub.netacad.com/itn?lng=uk-UA#10.4.4	4
2	Моніторинг мережевого трафіку Літ.: https://contenthub.netacad.com/itn?lng=uk-UA#3.7.10	4
3	Створення та встановлення SSL/TLS сертифікату. Літ.: [5] с. 447-454	4
4	Дослідження загроз в мережній безпеці Літ.: https://contenthub.netacad.com/itn?lng=uk-UA#16.1	4
5	Дослідження брандмауерів та міжмережних екранів, як засобів захисту мережі від атак Літ.: https://contenthub.netacad.com/itn/16.1.3#16.5.2	4
6	Захист мережних пристроїв Літ.: [2] с.225 – 228	4
7	Налаштування захисту площин контролю та управління Літ.: [2] с.165 – 167	4

8	Налаштування автентифікації Літ.: [2] с. 225 – 232	4
9	Підсумкове заняття.	2
	Разом за 3-й семестр:	**34**
	Четвертий семестр	
1	Налаштування VPN тунелю між двома мережами. Літ.: [2] с. 225 – 232	4
2	Дослідження протоколу IPsec. Літ.: [1] с.199-221	4
3	Створення мережі IPsec VPN Літ.: [3] с. 93-113	4
4	Налаштування Cisco IOS IPS Літ.: https://contenthub.netacad.com/sec/8.4.1#8.4.3	4
5	Налаштування політики доступу на Cisco ASA Літ.: https://contenthub.netacad.com/sec/9.2.1#9.2.4	4
6	Налаштування брандмауера на основі ідентифікації Cisco ASA Літ.: https://contenthub.netacad.com/sec/9.3.1#9.3.5	4
7	Моніторинг мережевого обладнання з використанням протоколу SNMP Літ.: https://contenthub.netacad.com/sec/9.3.1#9.3.5	4
8	Дослідження інструментів тестування мережевої безпеки. Літ.: [2] с.183-186	4
9	Підсумкове заняття. Тестування	4
	Разом за 4-й семестр:	**36**

ЗМІСТ САМОСТІЙНОЇ (ІНДИВІДУАЛЬНОЇ) РОБОТИ

Об'єм самостійної роботи у першому семестрі становить 180 годин, у другому семестрі становить 99 годин. Він включає опрацювання лекційного матеріалу, підготовку до виконання лабораторних робіт і їх захисту, виконання практичних завдань, підготовку до поточного контролю (тестування), роботу над курсовим проектом та підготовку до його захисту. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час, в тому числі із застосуванням технологій інтерактивного та дистанційного навчання.

Номер тижня	Теми самостійної роботи	Кількість годин
Третій семестр		
1	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №1.	5
2	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1	6
3	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №2.	5
4	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №2	6
5	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №3.	5
6	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 3.	6
7	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №4.	4
8	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4.	4
9	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 5.	4
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 5	4
11	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 6.	4
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 6	4
13	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 7.	4
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної №7	5
15	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи № 8.	11
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 8	11
17	Опрацювання лекційного матеріалу.	11
	Разом за 3-й семестр:	**99**
Четвертий семестр		
1	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №1	6
2	Підготовка до захисту лабораторної роботи №1	6
3	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №2. Робота над курсовим проектом.	6
4	Підготовка до захисту лабораторної роботи №2. Робота над курсовим проектом.	6
5	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №3. Робота над курсовим проектом.	6

6	Підготовка до захисту лабораторної роботи №3. Робота над курсовим проектом.	6
7	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №4. Робота над курсовим проектом.	5
8	Підготовка до захисту лабораторної роботи №4. Робота над курсовим проектом.	5
9	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №5	5
10	Підготовка до захисту лабораторної роботи №5. Робота над курсовим проектом.	5
11	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №6. Робота над курсовим проектом.	5
12	Підготовка до захисту лабораторної роботи №6. Робота над курсовим проектом.	5
13	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №7. Робота над курсовим проектом.	5
14	Підготовка до захисту лабораторної №7. Робота над курсовим проектом.	5
15	Опрацювання лекційного матеріалу. Підготовка до виконання лабораторної роботи №8. Робота над курсовим проектом.	5
16	Підготовка до захисту лабораторної роботи №8. Підготовка до захисту курсового проекту.	5
17	Опрацювання лекційного матеріалу. Підготовка до тестування. Підготовка до захисту курсового проекту.	5
18	Опрацювання лекційного матеріалу. Підготовка до тестування. Підготовка до захисту курсового проекту.	5
	Разом за 4-й семестр:	**96**

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

Навчальним планом дисципліни передбачено курсовий проєкт, на виконання якого виділяється 2 кредити ЄКТС (60 год.) самостійної роботи студента під керівництвом викладача та з консультуванням за графіком.

Згідно з навчальним планом підготовки бакалаврів за спеціальністю «Кібербезпека та захист інформації» курсовий проєкт виконується у 4 семестрі поетапно, відповідно до календарного плану.

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 графічних матеріалів	13-14 тиждень
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

Завдання на курсовий проєкт базується на матеріалі, який опрацьовується під час лекційних, лабораторних та самостійних занять в ході вивчення дисципліни. Тематика курсового проєкту

пов’язана з майбутньою спеціальністю студентів. В курсовому проєкті студент повинен показати свої знання в галузі захисту інформації в інформаційно-комунікаційних системах. Крім того, в якості об’єкту для курсового проєкту можуть бути дослідження та впровадження відомих технології проєктування засобів захисту, реалізація тестових програм тощо.

Розробка повинна бути представлена у вигляді інформаційно-комунікаційної мережі і супроводжуватись пояснювальною запискою, яка б повинна бути обсягом ***50-60 сторінок.*** Обов’язковим є креслення зазначеної мережі, а також таблиця, де містяться загрози, їх джерела та вразливості, через які зазначені загрози можуть бути реалізовані, та засоби протидії виявленим вразливостям.

Завдання до виконання курсового проєкту 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, адміністарції 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, адміністарції, 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 (локальні ресурси, дозволені зовнішні ресурси)	9	
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

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів, зокрема: лекції проводяться з використанням пояснювально-ілюстративних методів, лабораторні роботи та практичні заняття проводяться з використанням практичних, продуктивних, репродуктивних, тренінгових методів та з застосуванням інформаційно-комп'ютерних технологій (автоматизована система проектування Cisco Packet Tracer тощо).

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: виконання частини лабораторних робіт передбачає роботу у малих групах з призначенням тім-лідера, що сприяє розвитку лідерських якостей у студентів, здатності до спілкування і організації командної роботи над спільними задачами, а змінюваність складу робочих груп між лабораторними роботами сприяє розвитку навичок адаптованості, гнучкості, комунікативності і оперативного налагоджування міжособистісних відносин в різних колективах; прилюдні захисти лабораторних робіт і виступи під час практичних занять з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни, що передбачає рішення проблемних завдань із застосуванням творчих підходів в синтезі і аналізі програмних рішень і орієнтацію на роботу з постійно оновлюваними технологіями програмування; обмежений час на виконання лабораторних робіт, практичних і тестових завдань, чітко визначені терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час практичних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторної роботи;
- виконання практичних завдань;
- тестування.

Семестровий контроль проводиться у формі іспиту та курсового проекту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

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		Контрольні заходи	Підсумковий контрольний захід
III семестр			
Лабораторні роботи №:			Семестровий контроль (іспит)
1 - 8			0,4
ВК:	0,6		
IV семестр			
Лабораторні роботи №:			Семестровий контроль (іспит)
1 – 8			0,4
ВК:	0,6		

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

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. 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 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 інституційної 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 повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

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. Комп'ютерні мережі та Інтернет. Навчальний посібник/ В.М. Франчук. – К.: НПУ імені М.П. Драгоманова, 2015 р. – 141 с.

Додаткова

12. 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.
13. Operating System Concepts Essentials. Second Edition/ A. Silberschatz, P. B. Galvin, G. Gagne. – John Wiley & Sons, Inc, 2014. – 760 p.
14. Unix and Linux System Administration and Shell Programming. – PR NTR KMT, 2014. – 328 p.
15. 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.
16. Linux Command Line. A Beginner's Guide/ Ray Yao. – Ray Yao, USA, 2014. – 90 p.
17. Network Security Assessment. Third edition/ Ch. McNab. – O'Reilly Media, Inc., 2017. – 546 p.
18. Wireless Networks [Електронний ресурс]/ J. Salazar. – Czech Technical University of Prague, 2017. – режим доступу: http://standardsoui.ieee.org/oui/oui.txt
19. Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. – Software Architecture. – 2016. – P. 274-290.
20. 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.
21. 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. Доступ до ресурсу: https://msn.khmnu.edu.ua.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/.