ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій
_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«29» 08 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист та моніторинг комп'ютерних мереж
Назва дисципліни

Призначення Робочої програми	Для освітніх програм різних спеціальностей
Рівень вищої освіти*	Другий (магістерський)
Мова навчання	Українська
Обсяг дисципліни, кредитів ЄКТС	8
Статус дисципліни	Вибіркова
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма здобуття освіти	Обсяг дисципліни		Кількість годин						Форма семестрового контролю
			Аудиторні заняття					Самостійна робота (в т.ч. ІРЗ)	
	Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття		Залік
Д	8	240	66	32	34			174	+

Примітка: *Вибіркову навчальну дисципліну, яку кафедра рекомендує для певного рівня вищої освіти / спеціальності, мають право вибирати здобувачі інших рівнів та спеціальностей університету.

Робоча програма складена _____ канд. техн. наук, доц. Ігор МУЛЯР
Підпис Науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Схвалена на засіданні кафедри кібербезпеки

Протокол від «29» 08.2025 р. №1

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

2. ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна «Захист та моніторинг комп'ютерних мереж» відноситься до циклу вибіркових дисциплін та охоплює сучасні процеси розробки та проектування захищених комп'ютерних мереж, їх адміністрування та супроводу; міжмережні екрани та схеми їх підключення, протоколи безпеки та їх налаштування, побудову захищених комп'ютерних мереж, безпека віддаленого доступу, розробку політики міжмережної взаємодії, сканери виявлення вразливостей, моніторинг подій та інцидентів в мережах, аналіз загроз інформаційній безпеці в мережах, експертизу захищеності мереж.

Мета дисципліни. Формування у студентів системних знань і практичних навичок з розробки та проектування захищених комп'ютерних мереж, їх адміністрування та супроводу; надання глибоких та міцних знань з питань методології атак на комп'ютерні мережі, аналізу захищеності комп'ютерних мереж та управління їх безпекою.

Предмет дисципліни. Міжмережні екрани та схеми їх підключення, протоколи безпеки та їх налаштування, побудова захищених комп'ютерних мереж, безпека віддаленого доступу, розробка політики міжмережної взаємодії, сканери виявлення вразливостей, моніторинг подій та інцидентів в мережах, аналіз загроз інформаційній безпеці в мережах, експертиза захищеності мереж.

Завдання дисципліни. Формування у майбутніх спеціалістів умінь, навичок та компетентностей для розробки та проектування захищених комп'ютерних мереж, їх адміністрування та супроводу; надання глибоких та міцних знань з питань методології атак на комп'ютерні мережі, аналізу захищеності комп'ютерних мереж та управління їх безпекою.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *знати* основні поняття комп'ютерних мереж та їх компонентів; *захищати* мережевий трафік та *здійснювати* контроль доступу за допомогою існуючих протоколів та інструментів; *розробляти* та *аналізувати* архітектуру мережі, яка відповідає підвищеним вимогам безпеки; *розробляти* політику безпеки на основі моделей атак на певний об'єкт (підприємство); *аналізувати* комп'ютерні мережі за допомогою інструментів для аудиту та моніторингу.

3. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**СРС**
Тема 1. Введення в комп'ютерні мережі	2	4	10
Тема 2. Адміністрування мереж	6	4	32
Тема 3. Методи та засоби захисту комп'ютерних мереж	6	4	31
Тема 4. Розробка та проектування захищених комп'ютерних мереж	6	4	32
Тема 5. Методологія атак на комп'ютерні мережі	4	4	21
Тема 6. Моніторинг безпеки комп'ютерних мереж	4	8	21
Тема 7. Управління безпекою комп'ютерних мереж	4	6	27
Разом:	**32**	**34**	**174**

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
4.1 Зміст лекційного курсу

Перелік лекцій

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Введення в комп'ютерні мережі		**2**
1	**Введення в комп'ютерні мережі** Основи комп'ютерних мереж. Апаратні та програмні компоненти комп'ютерних мереж. Мережні топології. Літ.: [1] с. 8-69; [12] с. 356-371	2
Тема 2. Адміністрування мереж		**6**
2	**Мережні протоколи та служби. Мережні моделі** Завдання та цілі адміністрування мереж. Моделі міжмережної взаємодії. Літ.: [1] с. 132-181; [12] с. 407-461	2
3	**Функціонування протоколу TCP/IP** Адресація вузлів в IP-мережах. Розбиття мереж на підмережі за допомогою маски підмережі. IP-маршрутизація. Служба DNS (простір імен, домени, зони, динамічна реєстрація на сервері). Утиліти діагностування TCP/IP та DNS. Літ.: [2] с. 88-108; Літ.: [3] с. 7-56; [7] с. 10-48; [11] с. 14-60	2
4	**Інші мережні протоколи** Протокол захищеного віддаленого керування SSH. Протокол взаємодії мережного обладнання SNMP. Мережний протокол доступу до текстового інтерфейсу Telnet. Протокол передачі файлів FTP. Поштові протоколи (POP3, IMAP, SMTP). Протоколи передачі гіпертексту HTTP/HTTPS. Міжмережний протокол керуючих повідомлень ICMP. Протоколи захисту транспортного рівня TLS/SSL. Літ.: [7] с. 9-56	2
Тема 3. Методи та засоби захисту комп'ютерних мереж		**6**
5	**Брандмауери та їх функції у задачах захисту мереж** Переваги використання брандмауера у задачах захисту мереж. Види брандмауерів. Літ.: [2] с. 20-39; [10] с. 180-197	2
6	**Міжмережні екрани та міжмережна взаємодія** Міжмережний екран як засіб від вторгнення з Internet. Функціональні вимоги та компоненти міжмережних екранів. Фільтруючі маршрутизатори. Види шлюзів. Основні схеми мережевого захисту на базі міжмережних екранів. Літ.: [2] с. 20-39; [8] с. 434-439	2
7	**Безпека віддаленого доступу** Управління ідентифікацією і доступом. Організація захищеного віддаленого доступу. Моделі управління доступом (мандатні, дискреційні, рольові). Управління доступом за схемою одноразового входу з авторизацією Single Sign - On (SSO). Протокол Kerberos. Літ.: [10] с. 115-167; [12] с. 272-325; [15] с. 315-371	2
Тема 4. Розробка та проектування захищенихкомп'ютерних мереж		**6**
8	**Архітектура захищених комп'ютерних мереж** Параметри (сервіси, метрики, рівні) безпеки мереж. Фізичний захист мереж (кабельна система, системи електропостачання, захист від стихійних лих). Протидія прослуховуванню трафіку. Сегментація мережі [1] с. 183-213; [2] с. 10-34, с. 109-117; [7] с. 56-67	2
9	**Резервування та відновлення роботи мереж**	2

	Резервування мережного обладнання та каналів зв'язку. Системи архівування та дублювання інформації. Відновлення функціонування комп'ютерних мереж після здійснення кібератак, збоїв та відмов різних класів та походження [1] с. 183-213; [2] с. 10-34, с. 109-117; [5] с. 22-134	
10	**Політика інформаційної безпеки мережі підприємства** Структура політики безпеки підприємства. Класифікація складових мережі з точки зору інформаційної безпеки. Матриця управління доступом та розподіл інформаційних потоків і ролей Літ.: [8] с. 177-240	2
Тема 5. Методологія атак на комп'ютерні мережі		**4**
11	**Класифікація атак на комп'ютерні мережі** Атаки доступу (Sniffing, Hijacking, Session Hijacking). Атаки модифікації (зміна, додавання, видалення даних). Атаки типу «відмова в обслуговуванні». Комбіновані атаки (підміна довіреного суб'єкту, Man-in-theMiddle, експлойти, парольні атаки, атаки на рівні застосувань, аналіз мережного трафіку, Phishing, Pharming, ботнети, крадіжка конфіденційних даних). Літ.: [4] с. 5-18; [10] с. 206-227; [12] с. 373-381	2
12	**Аналіз та моделювання загроз мережної безпеки** Прояви загроз мережній безпеці. Стратегії зломщиків та порушників. Огляд основних інструментів злому. Загрози та їх класифікація, як об'єкт моделювання. Узагальнений підхід щодо побудови моделей загроз в комп'ютерних мережах. Літ.: [8] с. 116-177; [12] с. 27-38; [14] с. 46-109	2
Тема 6. Моніторинг безпеки комп'ютерних мереж		**4**
13	**Аналіз захищеності комп'ютерних мереж** Технологія аналізу захищеності. Засоби аналізу захищеності мереж, мережних протоколів і сервісів (сканери уразливостей). Літ.: [4] с. 154-203	2
14	**Технології виявлення атак в комп'ютерних мережах** Класифікація систем виявлення атак IDS (Intrusion Detection System). Компоненти і архітектура IDS. Системи SIEM. Методи реагування на атаки. Літ.: [1] с. 71-131; [10] с. 197-206	2
Тема 7. Управління безпекою комп'ютерних мереж		**4**
15	**Аудит безпеки комп'ютерних мереж** Цілі та завдання аудиту. Етапність аудиту. Літ.: [4] с. 205-231; [8] с. 348-357; [18] с. 7-103	2
16	**Аудит безпеки комп'ютерних мереж (продовження)** Відповідність мережі вимогам стандарту. Ризик-менеджмент. Вироблення рекомендацій. Літ.: [8] с. 348-357; [18] с. 7-103	2
	Разом за семестр:	**32**

4.2 Зміст лабораторних робіт

Перелік лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
Тема 1. Введення в комп'ютерні мережі		**4**
1	Проектування комп'ютерної мережі підприємства	4

Тема 2. Адміністрування мереж		**4**
2	IP-адресація та IP-маршрутизація в комп'ютерних мережах. Адміністрування комп’ютерних мереж TCP/IP-утилітами, TCP/IPсервісами та засобами доменних групових політик Літ.: [1]	4
Тема 3. Методи та засоби захисту комп’ютерних мереж		**4**
3	Дослідження брандмауерів та міжмережних екранів, як засобів захисту мережі від атак	4
Тема 4. Розробка та проектування захищенихкомп’ютерних мереж		**4**
4	Сегментація мережі, канали резервування та розробка політики безпеки	4
Тема 5. Методологія атак на комп’ютерні мережі		**4**
5	Дослідження технологій злому комп’ютерних мереж, збирання технічної та чуттєвої інформації, аналіз мережного трафіку	4
Тема 6. Моніторинг безпеки комп’ютерних мереж		**8**
6	Дослідження вразливостей комп’ютерних мереж, сканування мережних протоколів	4
7	Моніторинг інцидентів та подій у комп’ютерних мережах	4
Тема 7. Управління безпекою комп’ютерних мереж		**6**
8	Управління ризиками інформаційної безпеки мережі з використанням програмних засобів	4
9	Узагальнення матеріалу. Тестування	2
	Разом за семестр:	**34**

4.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у опрацюванні теоретичного матеріалу з відповідних джерел інформації, підготовці до виконання та захисту лабораторних робіт, до тестування тощо. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи (І семестр)	Кількість годин
1	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	10
2	Опрацювання теоретичного матеріалу лекції №2. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	11
3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2.	10
4	Опрацювання теоретичного матеріалу лекції №4. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	11
5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3.	10
6	Опрацювання теоретичного матеріалу лекції №6. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	11
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4.	10
8	Опрацювання теоретичного матеріалу лекції №8. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	11
9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5.	10
10	Опрацювання теоретичного матеріалу лекції №10. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	11
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6.	10
12	Опрацювання теоретичного матеріалу лекції №12. Оформлення	11

	звіту та підготовка до захисту лабораторної роботи №6.	
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7.	10
14	Опрацювання теоретичного матеріалу лекції №14. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	11
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8.	10
16	Опрацювання теоретичного матеріалу лекції №16. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	11
17	Підготовка до тестування за пройденим теоретичним матеріалом.	6
	Разом за семестр:	**174**

5. ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів; лабораторні роботи – з використанням практичних та частково-пошукових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, тестування), з використанням пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

6. МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів захисту лабораторних робіт;
- тестовий контроль теоретичного матеріалу;

Підсумкова семестрова оцінка виставляється за результатами поточного контролю. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

7. ПОЛІТИКА ДИСЦИПЛІНИ

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, активно працювати на занятті, якісно підготувати звіт (відповідно до теми роботи), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене лабораторне заняття здобувач зобов'язаний відпрацювати

в лабораторіях кафедри у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами тестування.

Здобувач вищої освіти, виконуючи лабораторні роботи, тестування з дисципліни з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення плагіату в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (за наявності такого переліку, доцільно вказати рекомендовані курси), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

8. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ОСВІТИ

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Залежно від важливості окремих видів навчальної роботи, і їх ролі у формуванні компетентностей і результатів навчання, визначених освітньою програмою, розробники Робочої програми присвоюють кожному виду навчальної роботи (структурній одиниці) з дисципліни певну кількість балів. При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності ***не допускаються***.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти 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 мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, 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 правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві***

	помилки.
Задовільно (достатній)	Здобувач вищої освіти 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 здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, 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 (недостатній)	Здобувач вищої освіти 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 здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів

Аудиторна робота								**Контрольні заходи**	**Семестровий контроль**
Лабораторні роботи №:								Тестовий контроль:	Залік
1	2	3	4	5	6	7	8	Т 1-7	
Кількість балів за вид навчальної роботи (мінімум-максимум)									
6-10	6-10	6-10	6-10	6-10	6-10	6-10	6-10	12-20	За рейтингом
48-80								**12-20**	**60-100***

Примітки: Т – тема навчальної дисципліни;

*За набрану з будь-якого виду роботи (дисципліни) кількість балів нижче встановленого мінімуму здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; якість оформлення звіту; вільне володіння здобувачем спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів навчання з теоретичного матеріалу

Тест, передбачений Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	0-59	60-65		66-72	73-82		83-89	90-100		
Кількість балів	-	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни**	
		Залік	**Іспит/диференційований залік**
A	90-100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		
D	66-72		***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
E	60-65		
FX	40-59	Незараховано	***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання з усіх видів робіт до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС у наведеній нижче таблиці.

Семестровий залік виставляється на останньому занятті за умови якщо загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

9. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Задачі захисту комп'ютерних мереж
2. Фізичний захист мереж (кабельна система, системи електропостачання, захист від стихійних лих)

3. Огляд програмних та програмно-апаратних методів захисту мереж (захист від мережних вірусів, захист від несанкціонованого доступу)

4. Адміністративні заходи

5. Використання брандмауера у задачах захисту мереж

6. Види брандмауерів

7. Міжмережний екран як засіб від вторгнення з Internet

8. Функціональні вимоги та компоненти міжмережних екранів

9. Фільтруючі маршрутизатори

10. Види шлюзів

11. Основні схеми мережевого захисту на базі між мережних екранів

12. Управління ідентифікацією і доступом

13. Організація захищеного віддаленого доступу

14. Моделі управління доступом (мандатні, дискреційні, рольові)

15. Управління доступом за схемою одноразового входу з авторизацією Single Sign – On (SSO)

16. Протокол Kerberos

17. Інфраструктура управління відкритими ключами PKI (Public Key Infrastructure)

18. Мережні протоколи та служби

19. Завдання та цілі адміністрування мереж

20. Моделі міжмережної взаємодії (модель OSI, модель TCP/IP)

21. Адресація вузлів в IP-мережах

22. Публічні і приватні IP-адреси

23. Відображення IP-адрес на фізичні адреси

24. Розбиття мереж на підмережі за допомогою маски підмережі

25. Введення в IP-маршрутизацію

26. Утиліти діагностування TCP/IP та DNS

27. Простір імен, домени і зони

28. Алгоритми роботи ітеративних і рекурсивних запитів DNS

29. Налаштування вузлів для виконання динамічної реєстрації на сервері DNS

30. Архітектура захищених комп'ютерних мереж

31. Параметри (сервіси, метрики, рівні) безпеки мереж

32. Протидія прослуховуванню трафіку

33. Сегментація мережі

34. Резервування мережного обладнання та каналів зв'язку

35. Системи архівування та дублювання інформації в мережах

36. Відновлення функціонування комп'ютерних мереж після здійснення кібератак, збоївта відмов різних класів та походження

37. Проектування та монтаж захищених комп'ютерних мереж: загальні вимоги та вихідні дані проекту

38. Проектування та монтаж захищених комп'ютерних мереж: проектна документація на створення мережі.

39. Проектування та монтаж захищених комп'ютерних мереж: вибір архітектури та структури мережі.

40. Структура політики безпеки підприємства

41. Класифікація складових мережі з точки зору інформаційної безпеки

42. Матриця управління доступом та розподіл інформаційних потоків і ролей

43. Проблеми інформаційної безпеки мереж

44. Прояви загроз мережній безпеці

45. Стратегії зломщиків та порушників

46. Огляд основних інструментів злому

47. Класифікація атак на комп'ютерні мережі

48. Загрози, їх джерела та вразливості проводових та безпроводових мереж

50. Узагальнений підхід щодо побудови моделей загроз в комп'ютерних мережах

51. Концепція адаптивного управління безпекою

52. Технологія аналізу захищеності

53. Засоби аналізу захищеності мереж, мережних протоколів і сервісів (сканери уразливостей, сніфери, системи SIEM)
54. Технології виявлення атак в комп'ютерних мережах
55. Методи аналізу мережної інформації
56. Класифікація систем виявлення атак IDS (Intrusion Detection System)
57. Компоненти і архітектура IDS
58. Методи реагування на атаки, ведення журналів реєстрації
59. Завдання управління системою мережної безпеки
60. Архітектура управління засобами мережної безпеки
61. Функціонування системи управління засобами мережної безпеки
62. Аудит безпеки комп'ютерних мереж
63. Ризик-менеджмент у комп'ютерних мережах

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі для навчання: https://msn.khmnu.edu.ua/course/view.php?id=8036.

11. МАТЕРІАЛЬНО-ТЕХНІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Інформаційна та комп'ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями.

Спеціальне та прикладне програмне забезпечення: OS Kali Linux, OS Ubuntu, OS MS Windows 10 або вище, OS FreeBSD, Oracle Virtual Box, Cisco Packet Tracer, Honeyd, Metasploit, MS Visual Studio 19 або вище, MS Visio 2019 або вище, Web Application Firewall, Ettercap, Wireshark, Nessus, Snort/Suricata, Nmap (Zenmap), CORAS Tools тощо.

Спеціальне апаратне забезпечення: маршрутизатори Cisco S4400, комутатори C2960, міжмережні екрани Cisco ASA/CISCO Fortinet та інше мережеве обладнання.

12. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Тестування на проникнення: навч. посіб. Ч.1/ Є.О. Живило. П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 134 с.
2. Тестування на проникнення: навч. посіб. Ч.2/ Є.О. Живило. П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 239 с.
3. OSINT у кібербезпеці: навч. пос./ Ланде Д.В. Київ: ТОВ «Інжиніринг», 2024. 522 с.
4. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с.
5. Організація баз даних: навчальний посібник/ Я.І. Соколовський, М.В. Дендюк, І.М. Крошний, І.Б.Пірко, М.М. Паславський. Видавництво Wydawnictwo GSW, 2023. 466 с.
6. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч. посіб./ В.М.Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2023. 508 с.

Додаткова

7. Penetration Testing For Dummies/ Robert Shimonski. John Wiley & Sons, Inc., Hoboken, New Jersey. 2020. 334 p.
8. Practical Binary Analysis/ Dennis Andriesse. San Francisco. 2020. 493 p.
9. OWASP Top 10 API Security Risks – 2023 [Електронний ресурс]. Режим доступу: https://surl.li/esffdo
10. Web Application Security Testing v4.2 [Електронний ресурс]. Режим доступу: https://surl.li/mjbsxb

11. A Guide to Penetration Testing [Електронний ресурс]. Режим доступу: https://surl.li/uoqvpd
12. Penetration Testing Execution Standard (PTES) [Електронний ресурс]. Режим доступу: http://www.pentest-standard.org/
13. NIST Technical Guide to Information Security Testing [Електронний ресурс]. Режим доступу: https://surl.li/hzlwdh
14. Пентест від А до Я: посібник з тестування на проникнення [Електронний ресурс]. Режим доступу: https://surl.li/vjvbgr
15. Maltego Handbook for Cyber Threat Intelligence [Електронний ресурс]. Режим доступу: https://surl.li/vzafzr
16. OSINT Академія [Електронний ресурс]. Режим доступу: https://surl.li/qufgzc
17. Kali Docs [Електронний ресурс]. Режим доступу: https://www.kali.org/docs/
18. Kali Tools [Електронний ресурс]. Режим доступу: https://www.kali.org/tools/
19. Metasploit Documentation [Електронний ресурс]. Режим доступу: https://docs.metasploit.com
20. Посібники про Honeypot. Від А до Я [Електронний ресурс]. Режим доступу: https://surl.li/oaizik
21. Приманки для лову хакерів (Комплексні системи розгортання приманок) [Електронний ресурс]. Режим доступу: https://surl.li/zxtiyg
22. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
23. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в КС від НСД.
24. YARA's documentation [Електронний ресурс]. Режим доступу: https://yara.readthedocs.io/en/stable/

13. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=8036
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

ЗАХИСТ ТА МОНІТОРИНГ КОМП'ЮТЕРНИХ МЕРЕЖ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	-
Кількість встановлених кредитів ЄКТС	8
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *знати* основні поняття комп'ютерних мереж та їх компонентів; *захищати* мережевий трафік та *здійснювати* контроль доступу за допомогою існуючих протоколів та інструментів; *розробляти* та *аналізувати* архітектуру мережі, яка відповідає підвищеним вимогам безпеки; *розробляти* політику безпеки на основі моделей атак на певний об'єкт (підприємство); *аналізувати* комп'ютерні мережі за допомогою інструментів для аудиту та моніторингу.

Зміст навчальної дисципліни. Введення в комп'ютерні мережі. Адміністрування мереж. Мережні протоколи. Методи та засоби захисту комп'ютерних мереж. Міжмережні екрани та міжмережна взаємодія. Безпека віддаленого доступу. Розробка та проектування захищених комп'ютерних мереж. Архітектура захищених комп'ютерних мереж. Резервування та відновлення роботи мереж. Методологія атак на комп'ютерні мережі. Моніторинг безпеки комп'ютерних мереж. Управління безпекою комп'ютерних мереж.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для другого (магістерського) рівня вищої освіти за денною формою здобуття освіти становить 8 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів); лабораторні роботи (з використанням практичних та частково-пошукових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій); самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт; тестовий контроль теоретичного матеріалу.

Вид семестрового контролю: залік.

Навчальні ресурси:

1. Тестування на проникнення: навч. посіб. Ч.1/ Є.О. Живило. П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 134 с.
2. Тестування на проникнення: навч. посіб. Ч.2/ Є.О. Живило. П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. 239 с.
3. OSINT у кібербезпеці: навч. пос./ Ланде Д.В. Київ: ТОВ «Інжиніринг», 2024. 522 с.
4. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с.
5. Організація баз даних: навчальний посібник/ Я.І. Соколовський, М.В. Дендюк, І.М. Крошний, І.Б.Пірко, М.М. Паславський. Видавництво Wydawnictwo GSW, 2023. 466 с.
6. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч. посіб./ В.М.Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2023. 508 с.
7. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=8036
8. Електронна бібліотека ХНУ. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладач: канд. техн. наук, доц. Муляр І.В.