ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Савенко О.С.
«_31_» _серпня_ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист та моніторинг комп'ютерних мереж

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека
Рівень вищої освіти	Другий магістерський
Освітньо-професійна програма	Кібербезпека
Обсяг дисципліни	8 кредитів ЄКТС
Мова навчання	Українська
Шифр дисципліни	ВД.06
Статус дисципліни	вибіркова

Факультет інформаційних технологій
Кафедра кібербезпеки

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
Д	-	-	8	240	90	36	54	-	-	150			+	

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

Схвалена на засіданні кафедри кібербезпеки
Протокол № 1 від " 31 " серпня 2022 р.
Зав. кафедри кібербезпеки _____ Ю.П. Кльоц
Підпис | Ініціали, прізвище

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Голова Вченої ради факультету _____ О.С. Савенко
Підпис | Ініціали, прізвище

Хмельницький 2022

ЗАХИСТ ТА МОНІТОРИНГ КОМП'ЮТЕРНИХ МЕРЕЖ

Тип дисципліни	Вибіркова
Освітній рівень	Другий (магістерський)
Мова викладання	Українська
Семестр	-
Кількість встановлених кредитів ЄКТС	8
Форми навчання, для яких викладається дисципліна	Денна

Студент, який успішно завершив вивчення дисципліни, повинен: з*нати* 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: Основні поняття захисту комп'ютерних мереж. Брандмауери та їх функції у задачах захисту мереж. Міжмережні екрани. Безпека віддаленого доступу. Адміністрування мереж. Поняття про мережні протоколи та служби. Основи функціонування протоколу TCP/IP. Служба DNS. Архітектура захищених комп'ютерних мереж. Проектування та монтаж захищених комп'ютерних мереж. Політика інформаційної безпеки мережі підприємства. Методологія атак на комп'ютерні мережі. Класифікація атак на комп'ютерні мережі. Аналіз та моделювання загроз мережної безпеки. Аналіз захищеності комп'ютерних мереж. Технології виявлення атак в комп'ютерних мережах. Методи управління засобами мережної безпеки. Аудит безпеки комп'ютерних мереж.

Запланована навчальна діяльність: не менше 1/3 від запланованого обсягу дисципліни.

Форми (методи) навчання: лекції (з використанням наочних методів (слайдів), пояснення, бесіди); лабораторні роботи (з використанням тренінгів та практикумів), самостійна робота (використання платформи MOODLE ХНУ та опрацювання літературних джерел).

Форми оцінювання результатів навчання: усне опитування перед допуском до лабораторної роботи; захист лабораторних робіт; письмове опитування (тестування).

Вид семестрового контролю: залік.

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. Інформаційна безпека в комп'ютерних мережах: навч. посіб./ [О.А. Смірнов, О.К. Конопліцька-Слободенюк, С.А. Смірнов, К.О. Буравченко та ін.] – Кропивницький: Видавець Лисенко В.Ф., 2020. – 295 с.
3. Інформаційна безпека: навчальний посібник/ [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; 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. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khnu.km.ua.
5. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php

Викладачі: к.т.н, доцент Кльоц Ю.П.

ВСТУП

Дисципліна «Захист та моніторинг комп'ютерних мереж» – вибіркова складова професійної підготовки магістрів спеціальності "125 – Кібербезпека".

Метою викладання навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій, необхідних 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.

Предметом дисципліни є 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.

Завданням дисципліни є забезпечити набуття наступних компетентностей та досягнення наступних програмних результатів навчання:

***компетентності*:**

- Розуміти завдання захисту мережевого трафіку та контролю доступу з використанням існуючих протоколів та інструментів.
- Розуміти методологію атак на комп'ютерні мережі та застосовувати це розуміння на практиці.
- Застосовувати політики безпеки для певного об'єкта (підприємства), щоб запобігти несанкціонованому доступу до комп'ютерних мереж
- Використовувати інструменти та утиліти для адміністрування та обслуговування комп'ютерних мереж відповідно до існуючих політик безпеки.
- Використовувати сучасні інструменти, IDS та SIEM-системи для аудиту, моніторингу процесів та виявлення вторгнень у комп'ютерних мережах.

результати навчання:

- 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.

Студент, який успішно завершив вивчення дисципліни, повинен: з*нати* 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.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:		
	лекції	лабораторні роботи	самостійну роботу
Тема 1. Введення в комп’ютерні мережі	2	6	18
Тема 2. Адміністрування мереж	6	6	22
Тема 3. Методи та засоби захисту комп’ютерних мереж	6	6	22
Тема 4. Розробка та проектування захищених комп’ютерних мереж	6	6	22
Тема 5. Методологія атак на комп’ютерні мережі	6	6	22
Тема 6. Моніторинг безпеки комп’ютерних мереж	4	12	24
Тема 7. Управління безпекою комп’ютерних мереж	4	6	20
Разом:	**36**	**54**	**150**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
	Тема 1. Введення в комп'ютерні мережі	
1	**Основи комп'ютерних мереж** 1. Поняття комп'ютерних мереж 2. Апаратні та програмні компоненти комп'ютерних мереж 3. Мережні топології Літ.: [1] с. 8-69; [12] с. 356-371	**2**
	Тема 2. Адміністрування мереж	
2	**Поняття про мережні протоколи та служби. Мережні моделі** 1. Завдання та цілі адміністрування мереж 2. Моделі міжмережної взаємодії (модель OSI, модель TCP/IP) Літ.: [1] с. 132-181; [12] с. 407-461	**2**
3	**Основи функціонування протоколу TCP/IP** 1. Адресація вузлів в IP-мережах 2. Розбиття мереж на підмережі за допомогою маски підмережі 3. Введення в IP-маршрутизацію 4. Служба DNS (простір імен, домени, зони, динамічна реєстрація на сервері) 5. 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 (частина 1)** 1. Протокол захищеного віддаленого керування SSH 2. Протокол взаємодії мережного обладнання SNMP 3. Мережний протокол доступу до текстового інтерфейсу Telnet 4. Протокол передачі файлів FTP Літ.: [7] с. 9-56	**2**
5	**Інші мережні протоколи (частина 2)** 1. Поштові протоколи (POP3, IMAP, SMTP) 2. Протоколи передачі гіпертексту HTTP/HTTPS 3. Міжмережний протокол керуючих повідомлень ICMP 4. Протоколи захисту транспортного рівня TLS/SSL Літ.: [7] с. 9-56	**2**
	Тема 3. Методи та засоби захисту комп'ютерних мереж	
6	**Брандмауери та їх функції у задачах захисту мереж** 1. Переваги використання брандмауера у задачах захисту мереж 2. Види брандмауерів Літ.: [2] с. 20-39; [10] с. 180-197	**2**
7	**Міжмережні екрани та міжмережна взаємодія** 1. Міжмережний екран як засіб від вторгнення з Internet 2. Функціональні вимоги та компоненти міжмережних екранів 3. Фільтруючі маршрутизатори 4. Види шлюзів 5. Основні схеми мережевого захисту на базі міжмережних екранів Літ.: [2] с. 20-39; [8] с. 434-439	**2**
8	**Безпека віддаленого доступу** 1. Управління ідентифікацією і доступом 2. Організація захищеного віддаленого доступу 3. Моделі управління доступом (мандатні, дискреційні, рольові) 4. Управління доступом за схемою одноразового входу з авторизацією	**2**

	Single Sign - On (SSO) 5. Протокол Kerberos Літ.: [10] с. 115-167; [12] с. 272-325; [15] с. 315-371	
Тема 4. Розробка захищених комп'ютерних мереж		
9	**Архітектура захищених комп'ютерних мереж** 1. Параметри (сервіси, метрики, рівні) безпеки мереж 2. Фізичний захист мереж (кабельна система, системи електропостачання, захист від стихійних лих) 3. Протидія прослуховуванню трафіку 4. Сегментація мережі [1] с. 183-213; [2] с. 10-34, с. 109-117; [7] с. 56-67	**2**
10	**Резервування та відновлення роботи мереж** 1. Резервування мережного обладнання та каналів зв'язку 2. Системи архівування та дублювання інформації 3. 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	**2**
11	**Політика інформаційної безпеки мережі підприємства** 1. Структура політики безпеки підприємства 2. Класифікація складових мережі з точки зору інформаційної безпеки 3. Матриця управління доступом та розподіл інформаційних потоків і ролей Літ.: [8] с. 177-240	**2**
Тема 5. Методологія атак на комп'ютерні мережі		
12	**Проблеми інформаційної безпеки мереж** 1. Прояви загроз мережній безпеці 2. Стратегії зломщиків та порушників 3. Огляд основних інструментів злому Літ.: [12] с. 27-38; [14] с. 46-109	**2**
13	**Класифікація атак на комп'ютерні мережі** 1. Атаки доступу (Sniffing, Hijacking, Session Hijacking) 2. Атаки модифікації (зміна, додавання, видалення даних) 3. Атаки типу «відмова в обслуговуванні» 4. 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**
14	**Аналіз та моделювання загроз мережної безпеки** 1. Загрози, їх джерела та вразливості 2. Загрози та їх класифікація, як об'єкт моделювання 3. Узагальнений підхід щодо побудови моделей загроз в комп'ютерних мережах Літ.: [8] с. 116-177;	**2**
Тема 6. Моніторинг безпеки комп'ютерних мереж		
15	**Аналіз захищеності комп'ютерних мереж** 1. Технологія аналізу захищеності 2. Засоби аналізу захищеності мереж, мережних протоколів і сервісів (сканери уразливостей) Літ.: [4] с. 154-203	**2**
16	**Технології виявлення атак в комп'ютерних мережах** 1. Класифікація систем виявлення атак IDS (Intrusion Detection System) 2. Компоненти і архітектура IDS	**2**

	3. Системи SIEM 4. Методи реагування на атаки Літ.: [1] с. 71-131; [10] с. 197-206	
Тема 7. Управління безпекою комп'ютерних мереж		
17	**Аудит безпеки комп'ютерних мереж (частина 1)** 1. Цілі та завдання аудиту 2. Етапність аудиту Літ.: [4] с. 205-231; [8] с. 348-357; [18] с. 7-103	**2**
18	**Аудит безпеки комп'ютерних мереж (частина 2)** 1. Відповідність мережі вимогам стандарту 2. Ризик-менеджмент 3. Вироблення рекомендацій Літ.: [8] с. 348-357; [18] с. 7-103	**2**
	Разом за семестр:	**36**

Перелік лабораторних робіт

№ п/п	**Теми лабораторних робіт**	**Кількість годин**
1	Проектування комп'ютерної мережі підприємства	**6**
2	IP-адресація та IP-маршрутизація в комп'ютерних мережах. Адміністрування комп'ютерних мереж TCP/IP-утилітами, TCP/IP-сервісами та засобами доменних групових політик	**6**
3	Дослідження брандмауерів та міжмережних екранів, як засобів захисту мережі від атак	**6**
4	Налаштування та управління віддаленим доступом засобами ОС сімейства Windows	**6**
5	Дослідження технологій злому комп'ютерних мереж, збирання технічної та чуттєвої інформації, аналіз мережного трафіку	**6**
6	Дослідження вразливостей комп'ютерних мереж, сканування мережних протоколів	**6**
7	Моніторинг інцидентів та подій у комп'ютерних мережах	**6**
8	Управління ризиками інформаційної безпеки мережі з використанням програмних засобів	**6**
9	Контрольні заходи за пройденим теоретичним матеріалом (тестування)	**6**
	Разом за семестр:	**54**

Зміст самостійної (у т.ч. індивідуальної) роботи

Об'єм самостійної роботи з дисципліни "Захист та моніторинг комп'ютерних мереж" становить 150 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	8
2	Опрацювання теоретичного матеріалу лекції №2. Підготовка до захисту лабораторної роботи №1.	8
3	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2.	8
4	Опрацювання теоретичного матеріалу лекції №4. Підготовка до захисту лабораторної роботи №2.	8
5	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3.	8
6	Опрацювання теоретичного матеріалу лекції №6. Підготовка до захисту лабораторної роботи №3.	8
7	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4.	8
8	Опрацювання теоретичного матеріалу лекції №8. Підготовка до захисту лабораторної роботи №4.	8
9	Опрацювання теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5.	8
10	Опрацювання теоретичного матеріалу лекції №10. Підготовка до захисту лабораторної роботи №5.	8
11	Опрацювання теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6.	8
12	Опрацювання теоретичного матеріалу лекції №12. Підготовка до захисту лабораторної роботи №6.	9
13	Опрацювання теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7.	9
14	Опрацювання теоретичного матеріалу лекції №14. Підготовка до захисту лабораторної роботи №7.	9
15	Опрацювання теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8.	9
16	Опрацювання теоретичного матеріалу лекції №16. Підготовка до захисту лабораторної роботи №8.	9
17	Опрацювання теоретичного матеріалу лекції №17.	8
18	Опрацювання теоретичного матеріалу лекції №17. Підготовка до контрольного заходу за пройденим матеріалом.	9
	Разом за семестр:	**150**

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться словесними методами з супроводом презентаційних матеріалів, лабораторні заняття проводяться з використанням сучасних інформаційних технологій та прикладних програм і мають за мету – набуття студентами практичних навичок забезпечення захисту та моніторингу сучасних комп'ютерних мереж.

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; інтерактивне спілкування з проблемних питань під час лекцій, прилюдні захисти лабораторних робіт 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; обмежений час на виконання лабораторних робіт, контрольних завдань, чітко визначені і надані в силабусі 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 https://www.khnu.km.ua/root/files/01/06/03/006.pdf.

МЕТОДИ КОНТРОЛЮ

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

При цьому використовуються такі методи поточного контролю:

- усне опитування перед допуском до лабораторної роботи;
- захист лабораторної роботи;
- письмовий контроль (тестування).

Семестровий контроль проводиться у формі заліку. Підсумкова семестрова оцінка виставляється на основі результатів поточного контролю.

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**
Вид заняття	Лабораторні роботи	Тестування	Семестровий контроль (залік)
Тема	1-7	1-7	-
Ваговий коефіцієнт	0,8	0,2	0

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 звіту; вільне володіння студентом спеціальною термінологією і уміння професійно 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.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з п'ятдесяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 50.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–25	26–38	39–47	48–50
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 50 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 50 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в онлайн-режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни не пізніше ніж через 10 днів після проходження тестування.

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

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 оцінку «незадовільно» за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

Студент, який не набрав позитивний середньозважений бал за поточну роботу або не виконав індивідуальний план з дисципліни повністю, вважається невстигаючим.

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».

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	Зараховано	***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	Незараховано	***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

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, збоїв та 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

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Захист та моніторинг комп'ютерних мереж» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

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. Адміністрування комп'ютерних мереж та операційних систем [Електронний ресурс]/ В.В. Поліщук. – Ужгород: 2019. – режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/24567/1/Методичне%20видання%20адміністрування%20КМ%20і%20ОС.pdf
4. Інформаційна безпека в комп'ютерних мережах: навч. посіб./ О.А. Смірнов, О.К. Конопліцька-Слободенюк, С.А. Смірнов, К.О. Буравченко, Т.В. Смірнова, Л.І. Поліщук. – Кропивницький: Видавець Лисенко В.Ф., 2020. – 295 с. http://dspace.kntu.kr.ua/jspui/bitstream/123456789/9799/1/Inform_bezp_komp_mer.pdf
5. Проектування та монтаж локальних комп'ютерних мереж/ І. М. Журавська. – Миколаїв: Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.
6. Комп'ютерні мережі: навч. посіб./ Б.Ю. Жураковський, І.О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 213 с. https://ela.kpi.ua/bitstream/123456789/36689/1/Zhurakovkyi_Zeniv_Kompiuterni_merezhi_lab.pdf
7. Технології та протоколи інфокомунікаційних мереж. Частина 1[Електронний ресурс]/ О.Л. Недашківський. – Київ, 2017. – режим доступу: 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. Моделирование системы защиты информации. Практикум: Учеб. пособие./ Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2015. - 120 с.
10. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с
11. Комп'ютерні мережі та Інтернет. Навчальний посібник/ В.М. Франчук. – К.: НПУ імені М.П. Драгоманова, 2015 р. – 141 с.
12. Інформаційна безпека: навчальний 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.
13. Інформаційна безпека держави: методичні вказівки до виконання лабораторних робіт/ уклад. О.А. Смірнов, О.К. Конопліцька-Слободенюк, В.Д. Хох, С.А. Смірнов/ – Кропивницький: ЦНТУ – 2017. – 90 с.
14. 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. http://www.dgma.donetsk.ua/docs/kafedry/avp/metod/_БКМ%20Пос_бник.pdf
15. Технології захисту інформації: навчальний посібник/ С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. http://kist.ntu.edu.ua/textPhD/tzi.pdf
16. Апаратно-програмні засоби захисту інформації у корпораціях: навчально-методичний посібник [Електронний ресурс]/ В.Г. Крижановський, С.П. Сергієнко. – Вінниця : ДонНУ

імені Василя Стуса, 2019. – режим доступу: https://r.donnu.edu.ua/bitstream/123456789/111/1/Методичка%20Засоби%20захисту%20інформації%20у%20корпораціях.pdf
17. IBM QRadar. Installation Guide [Електронний ресурс]. – IBM Corp., 2019. – режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_siem_inst.pdf
18. Аудит та управління інцидентами інформаційної безпеки: навчальний посібник/ О.Г. Корченко, С.О. Гнатюк С.О, С.В. Казмірчук та ін. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.

Додаткова

16. 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.
17. Operating System Concepts Essentials. Second Edition/ A. Silberschatz, P. B. Galvin, G. Gagne. – John Wiley & Sons, Inc, 2014. – 760 p.
18. Unix and Linux System Administration and Shell Programming. – PR NTR KMT, 2014. – 328 p.
19. 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.
20. Linux Command Line. A Beginner's Guide/ Ray Yao. – Ray Yao, USA, 2014. – 90 p.
21. Mastering Windows Server 2019. Second Edition/ J. Krause. – Packt Publishing Ltd, 2019. – 1010 p.
22. Network Security Assessment. Third edition/ Ch. McNab. – O'Reilly Media, Inc., 2017. – 546 p.
23. Wireless Networks [Електронний ресурс]/ J. Salazar. – Czech Technical University of Prague, 2017. – режим доступу: http://standardsoui.ieee.org/oui/oui.txt
24. Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. – Software Architecture. – 2016. – P. 274-290.
25. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів: Монографія./ В.Л. Бурячок, В.Ю. Соколов. – Київ : КУБГ, 2019. - 164 с.
26. 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.
27. 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
28. Комп'ютерні мережі. Книга 1/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2013. – 256 с.
29. Комп'ютерні мережі. Книга 2/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2014. – 312 с.
30. Основи інформаційної та кібернетичної безпеки. Навчальний посібник/ В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
31. Безпека безпроводових і мобільних мереж: Навчальний посібник/ В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. – 2 вид., доп. – К.: КУБГ, 2019. – 130 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.