МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра системного аналізу та інформаційних технологій

ЗАТВЕРДЖЕНО
протокол засідання кафедри
«28» серпня 2023 року № 1

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в комп'ютерних системах та мережах
(шифр і назва навчальної дисципліни)

напрям підготовки
(шифр і назва напряму підготовки)

спеціальність 125 Кібербезпека
(шифр і назва спеціальності)

спеціалізація кібербезпека
(назва спеціалізації)

факультет економіко-правовий
(назва факультету)

2023-2024 рік

Робоча програма

Захист інформації в комп’ютерних системах та мережах для студентів
(назва навчальної дисципліни)

для здобувачів вищої освіти ОП 125 Кібербезпека першого (бакалаврського) рівня вищої освіти
Спеціальність 125 Кібербезпека

Розробники:

Дрейс Ю.О., кандидат технічних наук, доцент, доцент кафедри САІТ
(вказати авторів, їхні посади, наукові ступені та вчені звання)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 5</td><td>Галузь знань: 12
Інформаційні технології</td><td colspan="2" rowspan="2">Нормативна</td></tr>
<tr><td>125
Кібербезпека</td></tr>
<tr><td>Семестрових модулів – 1</td><td rowspan="5"></td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</td><td>4-й</td><td>4-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання - вирішення типових завдань за темами змістових модулів</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 240</td><td>7-й</td><td></td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 11</td><td rowspan="10">Освітній ступінь:
бакалавр</td><td>20</td><td></td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>30</td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>100</td><td></td></tr>
<tr><td colspan="2">Індивідуальні завдання: -</td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Примітка.

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

для денної форми навчання – 33%,

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є закладення термінологічного фундаменту, навчання студентів правильному проведенню аналізу погроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах та мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завдання: формування у студентів певних знань та вмінь з теорії та практики захисту інформації, за результатами яких студенти повинні знати сучасні загрози безпеці інформаційним системам; технічні методи і засоби захисту інформації; програмні методи і засоби захисту; методи захисту інформації в розподілених інформаційних системах; організаційно-правове забезпечення захисту інформації; а також вміти аналізувати можливості несанкціонованого здобуття інформації потенційними порушниками; аналізувати вплив комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем; виявляти дії вірусу в операційній системі за допомогою аналізу процесів, що протікають, за допомогою аналізу кодів підозрілих програм, за допомогою антивірусних програм; організовувати та виконувати практичні дій посадових осіб відділу захисту інформації відповідно до інструкцій і обов'язків.

Місце навчальної дисципліни в освітній програмі: ОК 27. ОКПП 1.2.18.

Передумови для вивчення дисципліни: Архітектура комп'ютерних систем, Комп'ютерні мережі, Основи криптографічного захисту інформації, Прикладна криптологія.

Компетентності та результати навчання:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

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

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

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

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

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

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та /або кібербезпекою.

РН 2 організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН 12 розробляти моделі загроз та порушника;
РН 13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
РН 14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
РН 15 використовувати сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних технологій;
РН 19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
РН 25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
РН 27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
РН 28 аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та /або кібербезпеки;
РН 30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
РН 36 виявляти небезпечні сигнали технічних засобів;
РН 37 вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 38 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних- засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
РН 49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
РН 52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;

3. Програма навчальної дисципліни

Змістовий модуль 1. Інформаційна безпека: сутність, поняття, схема забезпечення.

Тема 1. Моделі безпеки та нормативно-правове регулювання інформаційної безпеки.
Модель безпеки CIA (Confidentiality, Integrity, and Availability), інші категорії моделі безпеки. Нормативно-правове регулювання інформаційної безпеки. Типи міжнародних організацій в сфері інформаційної безпеки. Закон України № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах».

Тема 2. Загальні принципи та методи забезпечення інформаційної безпеки.
Вивчення принципів і специфічних методів забезпечення інформаційної безпеки. Принципи побудови системи інформаційної безпеки. Системний підхід до захисту інформації.

Тема 3. Уразливість даних та протидія витоку інформації.
Поняття уразливості і витоку інформації. Види уразливості. Сутність криптографічних методів забезпечення інформаційної безпеки. Організаційно-адміністративні заходи забезпечення комп'ютерної безпеки. Принципи забезпечення інформаційної безпеки на основі інженерно-технічного забезпечення. Дії і події, що порушують інформаційну безпеку. Основні види каналів витоку інформації. Шляхи несанкціонованого доступу до інформації. Стратегія і тактика зловмисника при несанкціонованому доступі.

Тема 4. Способи практичної реалізації механізмів захисту інформації.
Шкідливе програмне забезпечення (malware), його види. Організація конфіденційного діловодства. Структура і функції служби інформаційної безпеки компанії. Забезпечення інформаційної безпеки автоматизованих банківських систем. Інформаційна безпека електронної комерції. Електронний цифровий підпис та особливості його застосування. Інформаційна безпека користувачів мобільних пристроїв. Протоколи мережевого доступу AAA (Authentication, Authorization, Accounting).

Змістовий модуль 2. Технології взаємодії між інформаційними системами та UNIX-подібні системи.

Тема 5. Основні поняття і концепції UNIX-подібних систем.
UNIX-подібні системи: історія, основні особливості та області використання. Базові команди і утиліти Linux. Розмежування прав доступу в UNIX-подібній системі.

Тема 6. Основи програмування на shell. Створення скриптів для моніторингу і управляння процесами в UNIX-подібній системі.
Командні інтерпретатори, їх різновиди та відмінності. Оболонки (shells). Конвеєри і перенаправлення вводу-виводу. Налаштування shell. Взаємодія shell-скриптів з користувачем. Умовні оператори, цикли в програмах на shell. Створення функцій у програмах на shell. Процеси і їх ідентифікатори. Взаємодія процесів в UNIX-подібній системі.

Тема 7. Файлові підсистеми UNIX-подібного оточення.
Сучасні файлові підсистеми, що використовуються у UNIX-подібних системах та їх особливості. Робота з таблицями розділів MBR і GPT. Відновлення таблиць розділів в разі збоїв. Пошук у файловій системі і в текстовому файлі. Утиліти find і grep.

Тема 8. Налаштування і використання мережевих комунікацій в UNIX-подібних системах.
Багаторівневий підхід до організації мережевих взаємодій. Засоби налаштування мережевої підсистеми Linux. Доступ до локальної мережі засобами Linux. Команди налаштування

протоколу IP. Постійні мережеві конфігурації (на прикладі Debian/GNU Linux). Базова діагностика мережевих підключень. Транспортний і прикладний рівні моделі мережевої взаємодії. Налаштування деяких мережевих служб в Debian/GNU Linux. Маршрутизація в Linux. Забезпечення доступу до мережі Інтернет.

Змістовий модуль 3. Прикладні аспекти захисту інформації.

Тема 9. Маніпуляції з локальними даними: виявлення скритих або видалених даних, їх відновлення та шифрування.

Комп'ютерна криміналістика (форензіка): вирішувані завдання і методи. Відновлення даних. Утиліти TestDisk, PhotoRec, Extundelete, Foremost. Симетричні алгоритми шифрування даних. Асиметричні алгоритми шифрування даних. Шифрування даних. PGP / GPG: можливості та особливості програмного забезпечення. Шифрування даних. TrueCrypt: можливості, особливості, нюанси програми. Специфікація шифрування диску / блочного пристрою LUCKS/dm-crypt (Linux Unified Key Setup).

Тема 10. Підходи до забезпечення інформаційної безпеки у мережі.

Призначення, цілі, опис ідентифікатора MAC. Засоби отримання MAC-адреси стороннього пристрою. Мотивація зловмисника при отриманні MAC-адреси чужого пристрою. Статичний і динамічний IP-адреси. Метод сканування протоколів IP. Основні методи сканування Nmap. Призначення, цілі, опис Honeypot. Способи виявлення Honeypot. Недоліки Honeypot. Проблеми, які можуть виникнути при його використанні. RPC-сервіси. Цілі RPC-сканування. Важливість інформації щодо активності та розміщення таких сервісів. Балансування навантаження (load balancing). Методи балансування навантаження на веб-сервер. DoS / DDoS-атаки. Чотири основні класи атак, що відповідають рівням моделі ISO OSI. Виявлення ознак DDoS-атаки. Основні способи захисту від DDoS-атак. Брандмауер: призначення. Принцип роботи Netfilter. Таблиці брандмауера Netfilter, їх призначення.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
Змістовний модуль 1. Інформаційна безпека: сутність, поняття, схема забезпечення.												
Тема 1. Моделі безпеки та нормативно-правове регулювання інформаційної безпеки.	**11**	1				10						
Тема 2. Загальні принципи та методи забезпечення інформаційної безпеки.	**11**	1				10						
Тема 3. Уразливість даних та протидія витоку інформації.	**11**	1				10						
Тема 4. Способи практичної реалізації механізмів захисту інформації.	**11**	1				10						
Разом за модулем 1	**44**	**4**				**40**						
Змістовий модуль 2. Технології взаємодії між інформаційними системами та UNIX-подібні системи.												
Тема 5. Основні поняття і концепції UNIX-подібних систем.	**16**	2		4		10						
Тема 6. Основи програмування на shell. Створення скриптів для моніторингу і управляння процесами в UNIX-подібній системі.	**14**	2		2		10						
Тема 7. Файлові підсистеми UNIX-подібного оточення.	**18**	2		6		10						
Тема 8. Налаштування і використання мережевих комунікацій в UNIX-подібних системах.	**30**	4		6		10						
Разом за модулем 2	**78**	**10**		**18**		**40**						

Змістовий модуль 3. Прикладні аспекти захисту інформації.											
Тема 9. Маніпуляції з локальними даними: виявлення скритих або видалених даних, їх відновлення та шифрування.	**20**	4		6		10					
Тема 10. Підходи до забезпечення інформаційної безпеки у мережі.	**18**	2		6		10					
Разом за модулем 3	**38**	**6**		**12**		**29**					
Усього годин	**150**	**20**		**30**		**100**					

5. Перелік тем і зміст лабораторних занять

№ з/п	Назва теми та стислий зміст роботи	Мета	Кількість годин	Результат навчання (РН) за ОП
1	Вивчення базових команд Linux.	Первинне знайомство з командним інтерпретатором. Вивчення базових команд операційної системи Linux.	4	РН2, РН12, РН13, РН 14, РН15, РН19, РН25, РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52
2	Розмежування прав доступу.	Вивчення механізмів управління доступом до ресурсів, прав доступу. Осягнення поняття користувача і групи. Набуття практичних навичок управління користувачами за допомогою консольних утиліт. Придбання навичок роботи з правами користувачів і правами на файли, каталоги за допомогою консольних утиліт.	2	РН2, РН12, РН13, РН 14, РН15, РН19, РН25, РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52
3	Файлові підсистеми.	Отримання теоретичних та практичних навичок роботи з таблицями розділів (MBR і GPT), створення розділів і файлових систем.	6	РН2, РН12, РН13, РН 14, РН15, РН19, РН25, РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52
4	Відновлення даних.	Отримання теоретичних та практичних навичок програмного відновлення даних.	6	РН2, РН12, РН13, РН 14, РН15, РН19, РН25, РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52
5	Шифрування даних.	Отримання теоретичних та практичних навичок роботи з програмними засобами шифрування даних.	6	РН2, РН12, РН13, РН 14, РН15, РН19, РН25, РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52
6	Honeypot, Nmap.	Отримання практичних і	6	РН12, РН13, РН14,

		теоретичних навичок роботи з honeypot, способами і методами сканування мережі.		РН15, РН19, РН25, РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52
7	LAN, веб-сервер з CMS.	Отримання теоретичних та практичних навичок побудови локальної комп'ютерної мережі та веб-сервера на прикладі установки CMS.	6	РН2, РН12, РН13, РН 14, РН15, РН19, РН25, РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52
8	Тестування навантаження веб-сервера.	За допомогою систем навантажувального тестування визначити продуктивність web-серверів Apache та Nginx, домогтися відмови в обслуговуванні.	6	РН2, РН12, РН13, РН 14, РН15, РН19, РН25, РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52

6. Самостійна робота

№ з/п	Зміст роботи	Кількість годин
1	Підготовка до лекційних занять	15
2	Підготовка до лабораторних занять	20
3	Виконання індивідуальних завдань (забезпечення цілісності та доступності даних: Raid, LVM; робота з пісочницями та файловими антивірусами. Sandbox; захист від спаму: антиспам (ASSP); управління інформаційною безпекою та подіями безпеки: SIEM; налаштування веб-серверу на UNIX-подібній системі; DDoS-атаки – основні особливості їх організації та захисту від них; мережеві системи виявлення та запобігання вторгнень: NIPS/NIDS: Snort; правила брандмауера: створення правил для брандмауера утилітою Iptables; міжмережеві екрани WAF (Web Application Firewall); пісочниця (sandbox): принцип роботи, приклади використання, переваги та недоліки пісочниць, альтернативи використанню пісочниць)	30
4	Підготовка до поточного модульного контролю	15
5	Підготовка до екзамену	20
	Разом	100

7. Індивідуальні завдання

Реферативне дослідження з обраної теми. Вирішення типових розрахункових завдань за темами змістових модулів.

8. Методи навчання

Викладання дисципліни здійснюється через лекційні та лабораторні заняття, індивідуальні та групові консультації, самостійну роботу студентів з виконання практичних завдань по кожній темі по індивідуальним варіантам, тестування. Усі теми дисципліни згруповані у 3 змістових модуля.

9. Засоби діагностики результатів навчання

Діагностика результатів навчання відбувається у формі поточного модульного контролю (тестування за змістовими модулями, усне опитування, захист лабораторних робіт, експрес-контроль), підсумкового контролю – у формі письмового екзамену. Критерії оцінювання

Критерії поточного оцінювання знань студентів.

Усний виступ та захист практичного завдання, тестування	**Критерії оцінювання**
5	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
4	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.
3	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
2	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
1	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.

Доповнення виступу*:*

2 бали – отримують студенти, які глибоко володіють матеріалом, чітко визначили його зміст; зробили глибокий системний аналіз змісту виступу, виявили нові ідеї та положення, що не були розглянуті, але суттєво впливають на зміст доповіді, надали власні аргументи щодо основних положень даної теми.

1 бал отримують студенти, які виклали матеріал з обговорюваної теми, що доповнює зміст виступу, поглиблює знання з цієї теми та висловили власну думку.

Суттєві запитання до доповідачів*:*

2 бали отримують студенти, які своїм запитанням до виступаючого суттєво і конструктивно можуть доповнити хід обговорення теми.

1 бал отримують студенти, які у своєму запитанні до виступаючого вимагають додаткової інформації з ключових проблем теми, що розглядається.

Експрес-контроль:

2 бали нараховуються студентам, які вільно володіють усім навчальним матеріалом, орієнтуються в темі та аргументовано висловлюють свої думки.

1 бал отримують студенти, які частково володіють матеріалом та можуть окреслити лише деякі проблеми теми.

Складання словника основних термінів**,** що визначені програмою курсу (за темами): Програмою курсу визначено перелік ключових термінів, що розкривають зміст кожної теми. Студентам пропонується скласти словник основних термінів з конкретної теми на останніх сторінках опорного конспекту лекцій.

2 бали нараховуються студентам, які не лише склали повний перелік визначених термінів з конкретної теми, а й можуть вільно розтлумачити їх зміст.

1 бал нараховуються студентам, які склали неповний перелік визначених термінів з конкретної теми і не можуть їх розтлумачити без конспекту.

Ведення опорного конспекту лекції:

2 бали нараховуються студентам, які в повному обсязі самостійно і творчо опрацювали всі питання лекції і вільно володіють її змістом.

1 бал нараховується студентам, які опрацювали лише окремі питання лекції і не достатньо вільно володіють її змістом.

Підготовка творчих завдань(есе, дайджест):

2 бали отримують студенти, які можуть виокремити з різних джерел основні положення, структурно об'єднати їх, коротко проаналізувати кожне з них та зробити ґрунтовні узагальнюючі висновки.

1 бал отримують студенти, які в цілому правильно виокремили основні положення кожного з джерел, але не зробили їх відповідного аналізу та узагальнюючих висновків. Ведення конспекту першоджерел.

2 бали отримують студенти, які опрацювали всю необхідну обов'язкову літературу, засвоїли її основні теоретичні положення, вміють їх пояснити і розтлумачити.

1 бал отримують студенти, котрі опрацювали не всю необхідну літературу, не завжди розуміють її вихідні теоретичні положення, поверхово їх пояснюють.

Підсумковий модульний контроль знань студентів.
Критерії підсумкового модульного оцінювання знань студентів

Екзаменаційна робота	Критерії оцінювання
45-50	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
35-44	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.
25-34	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
15-24	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому

	суттєві неточності, правильно вирішив меншість тестових завдань.
1-14	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

10. Розподіл балів, які отримують студенти

Вид роботи	Кількість годин	Обсяг кредитів	Кількість балів
Змістовний модуль 1. Інформаційна безпека: сутність, поняття, схема забезпечення.			
Тема 1. Моделі безпеки та нормативно			
лекційні	1	0,03	1
Тема 2. Загальні принципи та методи забезпечення інформаційної безпеки.			
лекційні	1	0,03	1
Тема 3. Уразливість даних та протидія витоку інформації.			
лекційні	1	0,03	1
Тема 4. Способи практичної реалізації механізмів захисту інформації.			
лекційні	1	0,03	1
Змістовий модуль 2. Технології взаємодії між інформаційними системами та UNIX-подібні системи.			
Тема 5. Основні поняття і концепції UNIX-подібних систем.			
лекційні	2	0,06	
лабораторні заняття	4	0,12	6
Тема 6. Основи програмування на shell. Створення скриптів для моніторингу і управляння процесами в UNIX-подібній системі.			
лекційні	2	0,06	
лабораторні заняття	2	0,06	6
Тема 7. Файлові підсистеми UNIX-подібного оточення.			
лекційні	2	0,06	
лабораторні заняття	6	0,18	6
Тема 8. Налаштування і використання мережевих комунікацій в UNIX-подібних системах.			
лекційні	4	0,12	
лабораторні заняття	6	0,18	6
Тестування з модулю			5
Змістовий модуль 3. Прикладні аспекти захисту інформації.			
Тема 9. Маніпуляції з локальними даними: виявлення скритих або видалених даних, їх відновлення та шифрування.			
лекційні	4	0,12	
лабораторні заняття	6	0,18	6

Тема 10. Підходи до забезпечення інформаційної безпеки у мережі.			
лекційні	2	0,06	
лабораторні заняття	6	0,18	6
Тестування з модулю			5
Підготовка і складання екзамену			50
Підсумок			100

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 - 100	**A**	відмінно	зараховано
82 - 89	**B**	добре	
74 - 81	**C**		
70 - 74	**D**	задовільно	
64 - 73	**E**		
35 - 59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0 - 34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

11.Інструменти, обладнання та програмне забезпечення:

Під час викладання дисципліни для занять використовується лабораторна база комп’ютерних класів МДУ.

Перелік програмного забезпечення:

KVM (Kernel-based Virtual Machine), VirtualBox, dd, TestDisk, PhotoRec, Extundelete, Foremost, mdadm, lvm, parted, TrueCrypt, LUCKS/dm-crypt (cryptsetup), gpg, Nmap, honeyd, Apache benchmark (ab), httperf, Siege, iptraf, ksysguard.

12. Рекомендовані джерела інформації:

Обов’язкова література:

1. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с.

2. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с.

3. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

4. Захист інформації в автоматизованих системах управління: навч. посібник / Уклад.

І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

5. Інформаційна безпека України: теорія і практика : підручник / В.В. Лизанчук. – Львів : ЛНУ імені Івана Франка, 2017. – 728 с.

6. Криворучко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с..

7. Телекомунікаційні системи передавання інформації. Методи кодування [Текст] : навч. посібник / Р. А. Бурачок, М. М. Климаш, Б. В. Коваль. – Львів : Вид-во Львів. політехніки, 2015. – 476 с.

8. 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.

Додаткова література:

1. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни та визначення. – К. : Укр. НДІССІ, 1997. – 11 с.

2. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.

3. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.

4. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.

5. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.

6. . НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999 р. ДСТСЗІ СБУ. – К., 1999. – 34 с.

7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 18.04.2006, – К. : Урядовий кур'єр. – 2006. № 73 – 74.

8. Про інформацію : Закон України від 03.04.1997. – К. : Урядовий кур'єр. – 1997. – № 62.

14. Політика навчальної дисципліни

Політика навчальної дисципліни «Захист інформації в комп'ютерних системах та мережах» заснована на положеннях Етичного кодексу, Положенні про організацію контролю та оцінювання успішності навчання здобувачів вищої освіти, Положенні про комплекс навчально-методичного забезпечення навчальної дисципліни, Положенні про академічну доброчесність, Положенні щодо політики розвитку soft skills в Маріупольському державному університеті.

Вивчення дисципліни потребує підготовки до лекційних та лабораторних занять, виконання науково-дослідного завдання (реферативне дослідження або участь у конференції з публікацією тез), опрацювання рекомендованої основної та додаткової літератури.

Підготовка та виконання лабораторних робіт передбачає: ознайомлення з програмою навчальної дисципліни та планами лабораторних занять; вивчення теоретичного матеріалу; виконання завдань, запропонованих для самостійного опрацювання.

Відповідь здобувача повинна демонструвати ознаки самостійності виконання поставлених завдань, відсутність ознак повторюваності та плагіату. Присутність здобувачів вищої освіти на заняттях є обов'язковою. Пропущені з поважних причин заняття мають бути відпрацьовані.

Здобувач вищої освіти повинен дотримуватися навчально-академічної етики та графіка навчального процесу.