МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра системного аналізу та інформаційних технологій

ЗАТВЕРДЖЕНО
протокол засідання кафедри
системного аналізу
та інформаційних технологій
«28» серпня 2023 року № 1

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОКПП 1.2.15. Управління інформаційною безпекою

(шифр і назва навчальної дисципліни)

Освітньо-професійна програма /освітньо-наукова Кібербезпека
(назва)

Спеціальність 125 Кібербезпека
(шифр і назва спеціальності)

Спеціалізація
(назва спеціалізації)

факультет економіко-правовий
(назва факультету)

2023-2024 рік

Робоча програма
Управління інформаційною безпекою
(назва навчальної дисципліни)
для здобувачів вищої освіти ОП 125 Кібербезпека першого (бакалаврського) рівня вищої освіти
Спеціальність 125 Кібербезпека

Розробники:
Дрейс Ю.О., доцент кафедри системного аналізу та інформаційних технологій, кандидат технічних наук, доцент

1. Опис навчальної дисципліни

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань: 12
Інформаційні технології</td><td colspan="2">Нормативна</td></tr>
<tr><td>Семестрових модулів – 1</td><td rowspan="5">ОП Кібезбезпека

Спеціальність
125 Кібербезпека</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</td><td>4-й</td><td></td></tr>
<tr><td>Індивідуальне науково-дослідне завдання -</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 150</td><td>8-й</td><td></td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Тижневих годин для денної форми навчання:
аудиторних -4
самостійної роботи студента – 8</td><td rowspan="9">Освітній ступінь:
бакалавр</td><td>20</td><td>12</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>20</td><td>12</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>80</td><td>96</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

Примітка.

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

для денної форми навчання 33 %

для заочної форми навчання 20 %

2. Мета та завдання навчальної дисципліни

Мета дисципліни: надати студентам знання, основні рекомендації та загальні принципи щодо здійснення, підтримки і поліпшення системи управління інформаційною безпекою підприємства на базі міжнародних стандартів серії ISO/IEC, що забезпечують загальне керівництво безпекою інформації на загальноприйнятих показниках.

Завдання дисципліни: забезпечити розуміння концепції менеджменту інформаційної безпеки на базі міжнародних стандартів серії ISO/IEC; надати знань щодо порядку створення системи менеджменту інформаційної безпеки (СМІБ); загальних вимог забезпечення документацією СМІБ; обов'язків керівників СМІБ; порядку проведення внутрішніх та зовнішніх аудитів коректності реалізації СМІБ; цілей управління СМІБ; засобів управління СМІБ; основних понять і визначення моделі оцінки ризику.

Місце навчальної дисципліни в освітній програмі: ОК 24. НДПП 1.2.15.

Передумови для вивчення **дисципліни**: Теорія ймовірностей та математична статистика, Теорія інформації та кодування, Комп'ютерні мережі, Інформаційні технології та системи, Захист інформації в комп'ютерних системах та мережах

Компетентності та результати навчання:

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 7 - діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

РН 8 - готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

РН 9 - впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та /або кібербезпеки;

РН 32 - вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

РН 33 - вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

РН 34 - приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

РН 35 - вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;

РН 39 - проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;

РН 41 - забезпечувати безперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

РН 43 - застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

РН 44 - вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

РН 45 - застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

РН 50 - забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

РН 54 - усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод і громадянина в Україні.

ІК - Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

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 6 – Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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

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

КФ 5 – Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та /або кібербезпеки.

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

3. Програма навчальної дисципліни.

Модуль 1. Основи менеджменту інформаційної безпеки

Тема 1. Ідентифікація середовища.
Основні поняття щодо аудиту та управління ризиками. Важливі терміни та поняття в управління ризиками та аудиті. Місце аудиту та управління ризиками в безпеці**.**Сфера контролю. Охоронний периметр. Загальний регламент про захист даних (GDPR). Процедура Data Protection Impact Assessment (DPIA). Рекомендації щодо оцінки впливу на захист даних (DPIA). Принципи конфіденційності. «Всесвіт аудиту».

Тема 2. Корпоративне управління, процесний підхід, і виникнення ризиків
Визначення мети діяльності організації та виникнення ризиків. Корпоративне середовище. Виникання ризику. Підходи операційного рівня. Принципи системи внутрішнього контролю. Концепція управління діяльністю організації через три рівні захисту. Моделі систем внутрішнього контролю. Модель внутрішнього контролю COSO. Типи контролю. Стандарт управління ризиками COSO ERM. COBIT 2019. Система та компоненти управління. Моделі спроможності процесів і зрілості діяльності.

Тема 3. Аудит, ризик-орієнтований підхід і відповідність.
Поняття аудиту. Процес аудиту. Види аудиту. Мета аудиту. Кодекс етики аудиту. Алгоритми та принципи аудиту. Незалежний аудит та самооцінка. Закони та положення в галузі аудиту. Етапи аудиту ІС та визначення відповідності організації.

Тема 4. Оцінка ризику
Навички для оцінки ризиків. Профіль ризику, апетит до ризику, толерантність до ризику. Підходи до профілювання. Декларація схильності до ризику: приклад якісної оцінки. Місце ризиків кібербезпеки. Узгодження результатів оцінки з системою управління. Методи оцінки ризику. Як поєднувати методи і моделі. Впровадження кількісної оцінки ризику. Джерела інформації середовища. Джерела інформації в організації. Сценарний підхід. Що враховується в формуванні результатів оцінки. Основи для сценаріїв. Факторний аналіз. Кроки факторного аналізу. Статистичні методи. Чисельні методи. Інструменти аналізу даних

Тема 5. Кількісна оцінка ризику
Дані з фінансової та корпоративної звітності – числа та суть сценарію ризику. Дані середовища для оцінки ймовірності. Дані подібних інцидентів для оцінки наслідків. Як порахувати та з’ясовані параметри розрахунку. Розрахунок наслідків. Розрахунок наслідків інциденту, повне ураження.

Модуль 2. Стандарти та нормативні вимоги до безпеки

Тема 6. Відповідність нормативним вимогам до безпеки.
Звідки беруться стандарти і нормативні вимоги. Що зараз з’являється нормативному полі. Джерела «кращих практик» та як з ними працювати. Регулювання кібербезпеки України. Про ієрархію вимог до безпеки в організації. Проблема з відповідністю вимогам безпеки. Впровадження вимог: безпека за пріоритетами в відкритій системі. Глобальна політика про кіберзлочинність. Що варто враховувати про кіберзброю та захист від неї. Що, куди і коли впроваджувати за вимогами. Процес впровадження кібербезпеки за вимогами. Визначення обсягу впровадження вимог. Організаційні норми. Вимоги безпеки, основне. Вимоги до архітектури мережи.

Тема 7. Впровадження міжнародних стандартів
Навіщо впроваджувати стандарти. Стандарти в роботі. Загальні принципи застосування стандартів. Практика впровадження: ISO 9000, COSO ICF, ISO 27001, ISO 22301 ITIL, ISA, ITAF, IPPF . Зовнішні підтвердження. Демонстрація відповідності. ITAF, структура ITAF, приклади стандартів в ITAF. ISO 27k. Завдання системи управління. Вибір заходів безпеки. Цілі безпеки. Процеси безпеки для досягнення цілей. CIS Critical security controls. KING IV. ISO 38500:2015. NIST SP 800-53 та ін. Приводи для коригування рішень. The ISO 8000 framework. DMBOK

Тема 8. Система управління інформаційною безпекою
Кібербезпека та інші домени безпеки. Кібербезпека один з елементів інформаційної безпеки. Система управління інформаційною безпекою. Порівняння СУІБ та КСЗІ. Сфера використання, кінцева мета впровадження, порівняння, дії при внесенні змін, супроводження та контроль. Впровадження СУІБ. Функціонування СУІБ. Модель ПВПД (PDCA), застосована до процесів СУІБ

Тема 9. Забезпечення професійної думки.
Засоби обґрунтування професійної думкиє. Аудиторські докази: ITAF. Докази. Види доказів Отримання доказів. Оцінка доказів. Підготовка аудиторської документації. Виконання та нагляд. Цифровий ланцюг зберігання. Ланцюг опіки. Форма ланцюга опіки. Про реалії електронних доказів в законодавстві України. Якість даних в управлінні ризиками. Прийняття обґрунтованих рішень. Метрики якості даних. Забезпечення якості даних. Подальший контроль за якістю даних, методологія. Процедури контролю за якістю даних. Структура опису процедури подальшого контролю за якістю даних в інформаційних системах.

Модуль 3. Обробка ризиків та аудиторські рекомендації

Тема 10. Обробка ризиків і аудиторські рекомендації
Обробка ризику. Аудиторські рекомендації. Функціонування заходів. Оцінка впливу невідповідності. Суттєвість зауваження. План заходів за результатом зауважень ВА. Взаємодія зацікавлених сторін. Впровадження аудиторських рекомендацій

Тема 11. Безперервність.
Аварійне відновлення. Мета. Терміни та скорочення. Управління безперервністю. Процес BCP. Політика безперервності бізнесу. Непередбачені обставини. Правові режими НС. Обставини непереборної сили. Надзвичайний стан. Військовий стан. Управління інцидентами BCP. Критерії настання інцидента. Додаткові параметри. Підготовка до непередбачених обставин. Стратегії відновлення. Альтернативи відновлення.

Тема 12. Звітність щодо безпеки
Місце звітності в системі управління. Загальні принципи в системі управління.
Особливості інтерпретації звітів про безпеку. Безпека: стан справ. Ризики: управлінська звітність. Стрес-тестування ризику. KRI. Звідки брати KRI. Аудиторські звіти.
Методологія внутрішнього аудиту.

Тема 13. Комунікація в організації.
Комунікація в організації. Предмет комунікації фахівців з аудиту та ризиків. Форми комунікації. Комунікація з вищим керівництвом. Логіка взаємодії: організаційні структури. Про структуру управління: потенційні адресати комунікації аудиту та ризиків. Ролі та відповідальність в процесі. Ролі в організації щодо управління ризиками.

Тема 14. Моделі та критерії зрілості

Логіка моделей зрілості. Структурована діяльність: процеси. Спроможність процеса. Зрілість діяльності. Критерії вимірювання діяльності. Активності на різних рівнях спроможності. Спроможність безпеки. Перелік моделей зрілості. Результат застосування моделі зрілості.

Тема 15. Постійне вдосконалення діяльності

Управління змінами та трансформація. Загальний процес змін. Управління технологічними змінами. Контрольні самооцінки. Самооцінка за і проти. Напрямки оцінки СУІБ. Процедури оцінки СУІБ. Перегляд СУІБ. Рівні зрілості процесу [УІБ]. Методика вимірювання ефективності. Ризик моніторинг. Процес моніторингу KRI. Документація індикатора ризику. ВА – процес моніторингу рекомендацій.

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.
Модуль 1. Основи менеджменту інформаційної безпеки												
Тема 1. Ідентифікація середовища	7	1				6	8					8
Тема 2. Корпоративне управління, процесний підхід, і виникнення ризиків	7	1				6	8					8
Тема 3. Аудит, ризик-орієнтований підхід і відповідність.	7	1				6	8	2				6
Тема 4. Оцінка ризику	13	1		10		2	8	2		6		8
Тема 5. Кількісна оцінка ризику	14	2		10		2	8	2		6		8
Разом за змістовим модулем 1	48	6		20		22	56	6		12		38
Модуль 2. Стандарти та нормативні вимоги до безпеки												
Тема 6. Відповідність нормативним вимогам до безпеки.	8	2				6	8	2				6
Тема 7. Впровадження міжнародних стандартів	8	2				6	8	2				6
Тема 8. Система управління інформаційною безпекою	8	2				6	8	2				6
Тема 9. Забезпечення професійної думки.	8	2				6	6					6
Разом за змістовим модулем 2	32	8				24	38	6				24
Модуль 3. Обробка ризиків та аудиторські рекомендації												

Тема 10. Обробка ризиків і аудиторські рекомендації	10	2		2		6	6					6
Тема 11. Безперервність.	6					6	6					6
Тема 12. Звітність щодо безпеки	8	2				6	6					6
Тема 13. Комунікація в організації	6					6	6					6
Тема 14. Моделі та критерії зрілості	8	2				6	4					4
Тема 15. Постійне вдосконалення діяльності	4					4	6					6
Разом за змістовим модулем 3	32	12		2		34	34					34
Усього годин	**120**	**20**		**20**		**80**	**120**	**12**		**12**		**96**

5. Перелік тем і зміст лабораторних занять

№ з/п	Назва теми та стислий зміст роботи	Мета	Кількість годин денна /заочна	Результат навчання (РН) за ОП
1	Протокол стрес-тестування операційного ризику	Навчитися формувати протокол стрес-тестування інформаційного ризику за сценарієм безпеки	2/-	РН2, РН7, РН8, РН9, РН32, РН33, РН34, РН35, РН39, РН41, РН 43, РН 44, РН 45, РН50, РН54
2	Модель розвитку подій, без врахування заходів безпеки	Навчитися рахувати модель розвитку подій, без врахування заходів безпеки	4/2	РН2, РН7, РН8, РН9, РН32, РН33, РН34, РН35, РН39, РН41, РН 43, РН 44, РН 45, РН50, РН54
3	Модель розвитку подій, враховуючи заходи безпеки	Навчитися рахувати модель розвитку подій, враховуючи заходи безпеки	4/2	РН2, РН7, РН8, РН9, РН32, РН33, РН34, РН35, РН39, РН41, РН 43, РН 44, РН 45, РН50, РН54

4	Розрахунок впливу, без врахування заходів безпеки	Навчитися розраховувати вплив, без врахування заходів безпеки	4/2	РН2, РН7, РН8, РН9, РН32, РН33, РН34, РН35, РН39, РН41, РН 43, РН 44, РН 45, РН50, РН54
5	Розрахунок впливу, враховуючи впроваджені заходи безпеки	Навчитися розраховувати вплив, враховуючи впроваджені заходи безпеки	4/4	РН2, РН7, РН8, РН9, РН32, РН33, РН34, РН35, РН39, РН41, РН 43, РН 44, РН 45, РН50, РН54
6	Оцінка суттєвості впливу на фінансовий стан та ліквідність. План заходів	Навчитися проводити оцінку суттєвості впливу на фінансовий стан та ліквідність	2/2	РН2, РН7, РН8, РН9, РН32, РН33, РН34, РН35, РН39, РН41, РН 43, РН 44, РН 45, РН50, РН54
Всього			20/12	

6. Самостійна робота

Денна форма навчання

№ з/п	Зміст роботи	Кількість годин
1	Підготовка до лекційних занять	15
2	Підготовка до лабораторних занять	30
3	Підготовка до екзамену	35
	Разом	80

Заочна форма навчання

№ з/п	Зміст роботи	Кількість годин
1	Підготовка до лекційних занять	12
2	Підготовка до лабораторних занять	40
3	Підготовка до екзамену	44
	Разом	96

7. Індивідуальні завдання

Підготовка тез доповідей на конференцію.

8. Методи навчання

Викладання дисципліни здійснюється через лекційні та практичні роботи, індивідуальні та групові консультації, самостійну роботу студентів з виконання практичних завдань по темам, 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 практичних робіт, експрес-контроль), підсумкового контролю – у формі заліку.

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
Модуль 1. Основи менеджменту інформаційної безпеки			
Тема 1. Ідентифікація середовища			
лекційні	2	0,06	
Тема 2. Корпоративне управління, процесний підхід, і виникнення ризиків			
лекційні	2	0,06	
Тема 3. Аудит, ризик-орієнтований підхід і відповідність.			
лекційні	2	0,06	
Тема 4. Оцінка та оцінка ризику			
лекційні	2	0,06	
практичні заняття	14	0,42	10
Тема 5. Кількісна оцінка ризику			
лекційні	2	0,06	
практичні заняття	14	0,42	10
Модуль 2. Стандарти та нормативні вимоги до безпеки			
Тема 6. Відповідність нормативним вимогам до безпеки.			
лекційні	2	0,06	
Тема 7. Впровадження міжнародних стандартів			
лекційні	2	0,06	
Тема 8. Система управління інформаційною безпекою			
лекційні	2	0,06	
Тема 9. Забезпечення професійної думки.			
лекційні	2	0,06	
Тестування з модулю			10
Модуль 3. Обробка ризиків та аудиторські рекомендації			
Тема 10. Обробка ризиків і аудиторські рекомендації			
лекційні	2	0,06	
практичні заняття	2	0,06	2
Тема 11. Безперервність.			
лекційні	2	0,06	

Тема 12. Звітність щодо безпеки			
лекційні	2	0,06	
Тема 13. Комунікація в організації			
лекційні	2	0,06	
Тема 14. Моделі та критерії зрілості			
лекційні	2	0,06	
Тема 15. Постійне вдосконалення діяльності			
лекційні	2	0,06	
Тестування з модулю			8
Підготовка тез доповідей			10
Підготовка та складання екзамену			50
Підсумок			100

11. 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

12. Інструменти, обладнання та програмне забезпечення:

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

13. Рекомендовані джерела інформації:

Обов’язкова література:

1. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. / Ю.П. Лісовська / - К. : Видавничий дім «КОНДОР», 2019. 272 с.

2. Корченко О.Г. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2019. – 408 с.

3. КорченкоО.Г . Аудит та управління інцидентами інформаційної безпеки: навч. посіб.Електронний ресурс / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.- пр.видань НАСБ України, 2014. – 190 с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf

4. Богуш, В.М. Інформаційна безпека держави : навч. посібник [Електронний ресурс] / В.М. Богуш, О.К. Юдін. К.: «МК-Прес», 2005. 432 с. – Режим доступу: https://studfiles.net/preview/5376129/ ; https://studfiles.net/preview/5376129/

5. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки: навч. посібник. / Кононович В.Г., Гладиш С.В. / Затверджено Міністерством транспорту та зв'язку України / за ред. В.Г. Кононовича. – Одеса: ОНАЗ, – 2009. – 208 с. – Режим доступу: https://old.onat.edu.ua/?pg=biblio_kaf_ib_pd.

6. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник [Електронний ресурс] / [В.Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа], заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с. – Режим доступу: http://www.dut.edu.ua/uploads/p_303_79299367.pdf .

7. «Про аудит фінансової звітності та аудиторську діяльність», Закон України, ВР від 21.12.2017р. № 2258-VIII. [Електронний ресурс], Режим доступу: http://search.ligazakon.ua/ l_doc2.nsf/ link1/T172258.html (26 січня 2019).

Додаткова література:

8. Стратегія національної безпеки України. Затверджено Указом Президента України від 26 травня 2015 року № 287/2015 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015 .

9. Тардаскіна Т.М., Кононович В.Г. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посібник. Затверджено Міністерством освіти та науки України як навчальний посібник для студентів вищих навчальних закладів [Лист № 1/11-7791 від 13 серпня 2010 року] / – Одеса: ОНАЗ, – 2010. – 268 с.

10. Про національну безпеку України: Закон України [Електронний ресурс] / Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. Затверджено Указом Президента України від 21 червня 2018 року № 2469-VIII – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19.

11. ДСТУ ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель.

12. ДСТУ ISO 15408-2: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 2. Функціональні вимоги безпеки.

13. ДСТУ ISO 15408-3: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 3. Вимоги до забезпечення захисту.

14. ДСТУ ISO 17799: 2005. Інформаційні технології. Методи захисту. Практичні рекомендації з управління інформаційної безпеки.

14. Політика навчальної дисципліни

1. Академічна доброчесність здобувачів є важливою умовою для опанування результатів навчання за навчальною дисципліною і отримання задовільної оцінки з поточного та підсумкового контролю.

Дотримання академічної доброчесності здобувачами освіти передбачає:

- Самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання;
- Посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- Дотримання норм законодавства про авторське право і суміжні права;

- Надання достовірної інформації про результати власної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

МДУ виступає за дотримання принципів академічної доброчесності, тому обов'язково використовується сервіс з перевірки робіт здобувачів вищої освіти на плагіат – Unicheck, а також доступний безкоштовний сервіс, який здійснює перевірку на плагіат письмових робіт – EduBirdie https://edubirdie.com/perevirka-na-plagiat.

Порушенням академічної доброчесності, згідно із Законом України «Про освіту» (ст. 42 п. 4) вважається:

- **академічний плагіат** – оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та / або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

- **самоплагіат** – оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

- **фабрикація** – вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

- **фальсифікація** – свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

- **списування** – виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання;

- **обман** – надання завідомо неправдивої інформації щодо власної освітньої (наукової, творчої) діяльності чи організації освітнього процесу; формами обману є, зокрема, академічний плагіат, самоплагіат, фабрикація, фальсифікація та списування;

- **хабарництво** – надання (отримання) учасником освітнього процесу чи пропозиція щодо надання (отримання) коштів, майна, послуг, пільг чи будь-яких інших благ матеріального або нематеріального характеру з метою отримання неправомірної переваги в освітньому процесі;

- **необ'єктивне оцінювання** – свідоме завищення або заниження оцінки результатів навчання здобувачів освіти.

Наведений перелік не є остаточно вичерпним і не охоплює всіх діянь, що можуть містити ознаки порушення академічної доброчесності.

За порушення академічної доброчесності здобувачі вищої освіти можуть бути притягнені до наступної академічної відповідальності:

- повторне проходження оцінювання (поточний, підсумковий контроль, залік, іспит тощо);

- проведення додаткової перевірки всіх робіт авторства порушника;

- позбавлення наданих МДУ пільг з оплати навчання;

- оголошення догани із занесенням до особової справи порушника;

- відрахування з МДУ;

- інші, відповідно до вимог чинного законодавства та нормативних локальних актів МДУ.

Більш детально тут

Анкетування з академ доброчесності: https://docs.google.com/forms/d/1VHzYkdFEGivtVl-dsENos1SCDRHfUpGia1YklgQK8j0/edit

2. Здобувач має право на оскарження процедури проведення та результатів контрольних заходів згідно Положення про організацію контролю та оцінювання успішності навчання здобувачів вищої освіти в МДУ.

3. Участь в анкетуванні. Наприкінці навчального семестру здобувачам буде запропоновано заповнити анонімну анкету щодо якості викладання вивчених навчальних дисциплін.

Заповнення анкети є важливою для вдосконалення освітнього процесу та системи внутрішнього забезпечення якості освіти МДУ та дозволить оцінити дієвість застосованих методів викладання та врахувати вашу думку стосовно покращення змісту навчальних дисциплін.

4. Неформальна освіта. Це освіта, яка здобувається, як правило, за освітніми програмами та не передбачає присудження визнаних державою освітніх кваліфікацій за рівнями освіти, але може завершуватися присвоєнням професійних та/або присудженням часткових освітніх кваліфікацій. Здобувач вищої освіти, який виявив бажання щодо визнання результатів, отриманих у неформальній освіті, звертається із відповідною заявою про визнання результатів, отриманих у неформальній освіті, в цілому для навчальної дисципліни

/змістового модулю /практичних завдань з навчальної дисципліни/ завдань з практики тощо для здобувачів вищої освіти, до деканату факультету, на якому викладається навчальна дисципліна. Процедура зарахування здійснюється згідно Порядку визнання результатів навчання, отриманих у неформальній освіті МДУ.