МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра математичних методів та системного аналізу

ЗАТВЕРДЖУЮ
Завідувач кафедри ММСА
_____ Т.В. Шабельник
«__» _____ 2020 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НДПП 1.2.17. Комплексні системи захисту інформації
(шифр і назва навчальної дисципліни)

Освітньо-професійна програма Кібербезпека
(назва)

Спеціальність 125 Кібербезпека
(код та найменування спеціальності)

Спеціалізація _____
(назва спеціалізації)

Факультет Економіко-правовий
(назва факультету)

2020 – 2021 рік

Робоча програма з дисципліни
Комплексні системи захисту інформації
(назва навчальної дисципліни)

для студентів ОП Кібербезпека
за спеціальністю (напрямом підготовки) 125 Кібербезпека

Розробники:
Черновол В.С. ст. викладач кафедри математичних методів та системного аналізу аналізу
Морозова А.О. асистент кафедри математичних методів та системного аналізу аналізу
(вказати авторів, їхні посади, наукові ступені та вчені звання)

Робоча програма затверджена на засіданні
кафедри математичних методів та системного аналізу
Протокол від « 27 » серпня 2020 року, № 1

Завідувач кафедри
математичних методів та системного аналізу


_____ (Т.В. Шабельник)
(підпис) (прізвище та ініціали)

© Черновол В.С. 2020 рік
© Морозова А.О. 2020 рік
© МДУ, 2020 рік

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 8</td><td>Галузь знань:
12 Інформаційні технології
(шифр і назва)</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">ОП
Кібербезпека
(назва)
Спеціальність
125 Кібербезпека
(код та найменування спеціальності)</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>Загальна кількість годин - 240</td><td>8-й</td><td>8-й</td></tr>
<tr><td rowspan="12">Тижневих годин для денної форми навчання:
аудиторних -4
самостійної роботи студента – 8</td><td rowspan="12">Освітній рівень:
магістр</td><td colspan="2">Лекції</td></tr>
<tr><td>40 год.</td><td>16 год.</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>40 год.</td><td>16 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>158 год.</td><td>206 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання</td></tr>
<tr><td colspan="2">2 год.</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">екзамен</td></tr>
</table>

Примітка.

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

для денної форми навчання 33,3 %,

для заочної форми навчання 13,3 %

2. Мета та завдання навчальної дисципліни

Мета навчальної дисципліни: оволодіння студентами комплексом знань у галузі захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових та набуття на основі цих знань практичних навичок та теоретичних знань, необхідних для творчого підходу в питанні сучасного та майбутнього оперативного захисту комп'ютерної техніки й інформації; оволодіння студентами алгоритмами створення сучасних програм захисту, алгоритмами кодування, сучасними методами, технологією, комп'ютерними програмними, технічними засобами у галузі безпеки: операційних систем, текстових редакторів, табличних процесорів, систем управління базами даних, конфіденціальної інформації тощо; набуття на основі вказаних знань практичних навичок, необхідних для розробки систем захисту, керування розробкою систем захисту, а на основі вказаного, нормального забезпечення роботи організацій, зі збереженням характеристик трафіку, швидкості санкціонованого доступу тощо; опанування концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних та глобальних комп'ютерних мережах із метою використання їх, можливостей для покращання показників безпеки в них.

Завдання навчальної дисципліни: студенти повинні здобути знань та практичних навичок щодо засобів дії загроз на об'єкти інформаційної безпеки установ, про правові і нормативні акти, які визначають систему захисту інформації в державі; керівні документи, що визначають ступінь захищеності комп'ютерних систем; методи проведення аналізу надійності системи захисту інформації в комп'ютерних системах; основні методи, технологію, принципи і правила побудови захисту комп'ютерних систем, в тому числі, персональних комп'ютерів, їх елементів і об'єктів комп'ютерних мереж; мати достатньо повне уявлення про алгоритми створення сучасних програм, алгоритми кодування та застосування стандартного програмного забезпечення захисту; методи та технологію захисту операційних систем, текстових редакторів, табличних процесорів, системи управління базами даних, у локальних, корпоративних та глобальних комп'ютерних мережах установ, на основі вивчених алгоритмів вміти розробляти нові програмні складові захисту в майбутньому; здобути практичні навички роботи з концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; роботи з системами й методами визначення захищеності носіїв інформації; створення засобами стандартного програмного забезпечення елементів захисту інформації; формулювати завдання щодо питань захисту інформації та, формалізуючи їх, вказувати шляхи вирішення.

Місце навчальної дисципліни в освітній програмі: ОК 29. НДПП 1.2.17.

Передумови для вивчення дисципліни: " Захист інформації в комп'ютерних системах та мережах ", " Теорія інформації та кодування ", " Основи криптографічного захисту інформації ", " Управління інформаційною безпекою "..

Результати навчання: Уміння організувати власну професійну діяльність,

обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. Здатність аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. Здатність виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. Здатність виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. Використовувати сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних технологій. Здатність реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. Здатність забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. Здатність використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційно- телекомунікаційних (автоматизованих) системах. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. 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. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. - Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. 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. Здатність забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах

3. Програма навчальної дисципліни

Змістовий модуль 1. Етапи проектування КСЗІ.

Тема 1. Поняття КСЗІ, призначення та функції.

Тема 2. Формування загальних вимог до КСЗІ.

Тема 3. Обґрунтування необхідності створення КСЗІ.

Змістовий модуль 2. Основні етапи впровадження КСЗІ.

Тема 4. Обстеження середовищ функціонування

Тема 5. Формування завдання на створення КСЗІ.

Тема 6. Розробка політики безпеки інформації.

Змістовий модуль 2. Організаційні заходи та супровід КСЗІ.

Тема 7. Розробка технічного завдання на створення КСЗІ

Тема 8. Розробка проекту КСЗІ.

Тема 9. Введення КСЗІ в дію та оцінка захищеності інформації. Супроводження КСЗІ.

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	сем	інд	с.р.
Модуль 1												
Змістовий модуль 1. Етапи проектування КСЗІ												
Тема 1. Поняття КСЗІ, призначення та функції.	**21**	2		4		15	**22**	1		1		20
Тема 2. Формування загальних вимог до КСЗІ.	**25**	4		6		15	**23**	2		1		20
Тема 3. Обґрунтування необхідності створення КСЗІ.	**29**	4		5		20	**23**	1		2		20
Разом за змістовим модулем 1	**75**	**10**		**15**		**50**	**68**	**4**		**4**		**60**
Змістовий модуль 2. Основні етапи впровадження КСЗІ												
Тема 4. Обстеження середовищ функціонування.	**31**	5		6		20	**34**	2		2		30
Тема 5. Формування завдання на створення КСЗІ	**24**	5		4		15	**24**	2		2		20
Тема 6. Розробка політики безпеки інформації.	**25**	5		5		15	**40**	2		2		36
Разом за змістовим модулем 2	**80**	**15**		**15**		**50**	**98**	**6**		**6**		**86**
Змістовий модуль 3. Організаційні заходи та супровід КСЗІ												
Тема 7. Розробка технічного завдання на створення КСЗІ	29	5		4		20	**24**	2		2		20
Тема 8. Розробка проекту КСЗІ	27	5		2		20	**24**	2		2		20
Тема 9. Введення КСЗІ в дію та оцінка захищеності інформації. Супроводження КСЗІ.	27	5		4		18	**24**	2		2		20
Разом за змістовим модулем 3	**83**	**15**		**10**		**58**	**72**	**6**		**6**		**60**
Модуль 2												
ІНДЗ	**2**				**2**		**2**				**2**	
Усього годин	**240**	**40**		**40**	**2**	**158**	**240**	**16**		**16**	**2**	**206**

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження структури об’єкту захисту	6
2	Розробка політики інформаційної безпеки	6
3	Моделі загроз. Класифікації моделі	8
4	Протокол випробувань комплексних систем захисту інформації	6
5	Документація на етапі експлуатації КСЗІ	8
6	Програма та методика попередніх випробувань комплексної системи захисту інформації	6
	Усього	40

6. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Поняття КСЗІ, призначення та функції.	20
2	Формування загальних вимог до КСЗІ.	20
3	Обґрунтування необхідності створення КСЗІ	20
4	Обстеження середовищ функціонування.	20
5	Формування завдання на створення КСЗІ.	20
6	Розробка політики безпеки інформації.	10
7	Розробка технічного завдання на створення КСЗІ.	20
8	Розробка проекту КСЗІ.	18
9	Введення КСЗІ в дію та оцінка захищеності інформації. Супроводження КСЗІ.	10
	Усього	158

7. Індивідуальні завдання

Підготовка тез доповіді на конференції/статті з обраної теми. Вирішення типових завдань за темами змістових модулів.

8. Методи навчання

Викладання дисципліни здійснюється через лекційні та практичні заняття, індивідуальні та групові консультації, самостійну роботу студентів з виконання практичних завдань по кожній темі по індивідуальним варіантам, захист практичних робіт, тестування. Усі теми дисципліни згруповані у 2 змістових модуля.

9. Критерії оцінювання

Критерії поточного оцінювання знань студентів**.**

Усний виступ та виконання письмового 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

Письмова контрольна робота або тестування	Критерії оцінювання
21-25	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.

17-21	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.
14-17	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.
10-14	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.
10	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. Засоби оцінювання

Поточний контроль знань студентів здійснюється за допомогою тестів, опитувань по темам, захисту звітів про виконання лабораторних робіт. Модульний контроль здійснюється із застосуванням тестів. Підсумковий контроль здійснюється у формі екзамену.

Завданням поточного контролю знань студентів є перевірка розуміння та запам'ятовування певного теоретичного матеріалу, умінь самостійної роботи зі спеціальною літературою, набуття практичних навичок роботи з ПК і окремими програмними засобами, вміння пояснити і захистити свою роботу.

11. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота										Екзамен	Сума в балах
Змістовний модуль 1			Змістовний модуль 2			Змістовний модуль 3					
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Тести		
2	2	2	4	4	4	8	8	6	10	50	100

Т1, Т2, ... – змістові теми

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, які обладнано мережею комп’ютерів платформи x86.

13. Рекомендовані джерела інформації

Основні:

1Закон України "Про інформацію".

2Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

3Закон України "Про основи національної безпеки".

4Постанова Кабінету Міністрів України від 27.11.1998 № 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».

5 Порядок захисту державних інформаційних ресурсів в інформаційнотелекомунікаційних системах.

6ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.

7ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

8ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

9НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

10 НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

11 НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

12 НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

13 НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

14 НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

15 НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

16 НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Додаткова:

1. Хорошко В.О, Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки : К.: ДУІКТ, 2008. – 186 с.
2. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник. – К.: "МК-Прес", 2005. – 432 с.
3. Расторгуев С.П. Основы информационной безопасности. – М.: „Академия", 2007. – 187 с.
4. Бузов О.О. Защита информации от утечки по техническим каналам. Учебное пособие. М.: Гостехкомисия Росии, 2005. - 435 с.
5. Хорев А.А. Техническая защита информации: учеб. Пособие для студентов вузов. В 3 т. Т.1. Технические каналы утечки информации. – М.: НПЦ "Аналитика", 2008. – 436 с.