МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра математичних методів та системного аналізу

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

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВДПП 2.2.7. Кібернетична безпека підприємства
(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

Кібернетична безпека підприємства

(назва навчальної дисципліни)

для студентів ОПП Кібербезпека

за спеціальністю (напрямом підготовки) 125 Кібербезпека

Розробники:

Лазаревська Ю.А., асистент кафедри математичних методів та системного аналізу, Черновол В.С. старший викладач кафедри математичних методів та системного 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)

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 – 4</td><td>Галузь знань:
12 Інформаційні технології
(шифр і назва)</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</td><td rowspan="4">ОПП
Кібербезпека
(назва)
Спеціальність
125 Кібербезпека
(код та найменування спеціальності)</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 5</td><td>2-й</td><td></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 - 120</td><td>4-й</td><td></td></tr>
<tr><td rowspan="12">Тижневих годин для денної форми навчання:
аудиторних – 2
самостійної роботи студента – 4,5</td><td rowspan="12">Освітній рівень:
магістр</td><td colspan="2">Лекції</td></tr>
<tr><td>10</td><td>4</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 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>90 год.</td><td>108 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання</td></tr>
<tr><td colspan="2">1 год.</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">залік</td></tr>
</table>

Примітка.

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

для денної форми навчання 1:4 (25%)

для заочної форми навчання

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є надання майбутньому фахівцеві достатнє уявлення про функціонування та розвиток економічної системи в єдності об'єкта та процесу управління.

Завданням навчальної дисципліни вивчення студентами предмету фундаментальних основ кібернетичної безпеки підприємства, визначення і класифікацію систем, ієрархію економічної системи, як об'єкта кібернетичної безпеки, моделювання об'єктів, принципи, методи і моделі управління.

Місце навчальної дисципліни в освітній програмі: ВК 11. ВДПП 2.2.7.

Передумови для вивчення дисципліни: Методи оптимізації та дослідження операцій, кіберпростір та протидія злочинності, інформаційна безпека держави, нормативно-правове забезпечення інформаційної безпеки.

Результати навчання: критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності; обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування; виконувати декомпозицію ІТС; розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; вибирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах; здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж; виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та

дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ; приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки; на основі політики захисту організації розробляти нормативні документи для її реалізації; впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки; розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем; застосовувати політики, що базуються риск адаптивному контролі доступу; здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками; виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС; використовувати інструментарій для моніторингу даних в ІТС; виконувати аналіз зловмисного програмного коду; характеризувати стан інформаційної безпеки особистості, суспільства та держави; характеризувати основні форми інформаційного протиборства в умовах входження держави в інформаційне суспільство; використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; застосовувати системний підхід та знання основ теорії інформаційної безпеки.

Програма навчальної дисципліни

Змістовий модуль 1. Концептуальні засади забезпечення кібернетичної безпеки підприємств

Тема 1. Основні положення кібернетичної безпеки підприємства.

Концептуальні засади забезпечення кібернетичної безпеки підприємств України. Основні визначення і поняття інформаційної та кібернетичної безпеки. Основні поняття захисту інформації: речова, телекомунікаційна та документована інформація. Інформаційні ресурси й процеси. Основні характеристики інформації: конфіденційність, цілісність та доступність. Методи порушення конфіденційності, цілісності й доступності інформації. Методи і способи захисту інформації. Основні напрями забезпечення безпеки: правовий, організаційний та технічний захист. Керування захистом інформаційних об'єктів.

Тема 2. Методи зламу комп'ютерних мереж.

Інтернет як новітня мережа загальносвітового поширення інформації. Розвиток інформаційних технологій, мережі Інтернет та обумовлені ними проблеми інформаційної безпеки. Електронний екстремізм, електронний тероризм, кіберзлочинність та кібертероризм. Медіа тероризм та Інтернет. Інформаційні загрози мережевих комунікацій. Поняття атаки на комп'ютерну систему. Виконання атак та виявлення методів ненаправлених і направлених хакерських атак.

Тема 3. Організаційно-правове забезпечення захисту інформації.

Особливості захисту електронної корпоративної інформації. Міжнародні стандарти безпеки інформаційно-обчислювальних систем. Вітчизняні державні стандарти технічного захисту інформації. Законодавча класифікація видів інформації в Україні. Державна таємниця як особливий вид інформації, що захищається. Конфіденційна інформація. Система захисту державної таємниці. Правовий режим захисту державної таємниці. Ліцензійна й сертифікаційна діяльності в сфері інформаційної безпеки. Нормативна база в галузі захисту програмних продуктів від несанкціонованого використання. Правові основи захисту інформації з використанням застосування технічних засобів (захисту від технічних розвідок, застосування й розробка шифрувальних засобів і т. д.). Захист інтелектуальної власності засобами патентного й авторського права. Зарубіжна нормативна база в галузі технічного захисту інформації. Відомі міжнародні стандарти управління інформаційною безпекою: BS 7799 (ISO/IEC 17799 и ISO/IEC 27001), Orange Book, X.800, критерії Європейських держав, Control Objectives for Information and Related Technology (COBIT), IT Infra-structure Library (ITIL) и Statement on Auditing Standards (SAS) No. 70. Критерії, вимоги та категорії систем безпеки «Оранжевої книги».

Тема 4. Побудова систем захисту від загроз порушення конфіденційності інформації.

Перелік конфіденційних відомостей організації. Порядок проведення експертизи з метою визначення конфіденційності інформації. Дослідження структури та умов функціонування ІС організації. Організаційні заходи та заходи забезпечення фізичної безпеки. Захист інформації від витоку технічними каналами. Захист інформації в комп'ютерних системах та мережах. Системи аутентифікації та ідентифікації. Класифікація систем аутентифікації та ідентифікації. Особливості електронних систем аутентифікації та ідентифікації. Використання паролів. Особливості парольних систем аутентифікації. Властивості, достоїнства та недоліки використання парольного захисту. Розрахунок стійкості парольного захисту інформації. Використання парольного захисту інформації в різних системах. Розмежування доступу до інформації в залежності від повноважень користувача. Захист авторських прав в інформаційних системах. Патентне та авторське право в Україні та світовій практиці. Захист елементів інформаційних систем патентами. Комп'ютерні програми і бази даних як об'єкти захисту авторського права.

Змістовий модуль 2. Концепція кібернетичної безпеки підприємств. Програмні засоби захисту інформації.

Тема 5. Побудова систем захисту від загроз порушення цілісності.

Принципи забезпечення цілісності. Структура системи захисту від загроз порушення цілісності. Криптографічні методи забезпечення цілісності інформації. Основи електронного цифрового підпису. Порядок використання цифрового підпису. Правила сертифікації ключів. Поняття про хеш-функції. Коди перевірки автентичності. Методи ідентифікації програм та захист авторських прав. Особливості захисту офісних електронних документів від несанкціонованої модифікації та розповсюдження. Методика та заходи захисту. Оптимізації заходів захисту. Критерії оптимізації. Використання економічного підходу при оптимізації засобів захисту.

Тема 6. Побудова систем захисту від загроз порушення доступності.

Захист мовленнєвої інформації, що передається у відкритих каналах зв'язку. Стеганографічні методи захисту письмової інформації, що передається у відкритих каналах зв'язку. Структура системи захисту від загроз порушення доступності**.** Дублювання шлюзів і міжмережевих екранів. Резервне копіювання інформації. Вибір програм розмежування доступу до інформації. Відмовостійкість дискової підсистеми. Використання RAID технологій. Відмовостійкість серверів. Аналіз існуючих методів і засобів, застосовуваних для контролю й захисту інформації, і розробка пропозицій щодо їхнього вдосконалення й підвищення**.** Методи та засоби захисту систем управління базами даних. Причини, види, основні методи порушення конфіденційності в системах управління базами даних (СУБД). Одержання несанкціонованого доступу до конфіденційної інформації шляхом логічних

висновків. Методи захисту СУБД. Особливості керування доступом: потоковий, контроль висновку, контроль доступу; багаторівневий захист. Підтримка логічної цілісності, транзакції функціонування, синхронізація в розподілених СУБД. Забезпечення безпеки багаторівневих реляційних СУБД. Кластерна організація серверів баз даних. Особливості реалізації механізмів захисту деяких комерційних СУБД.

Тема 7. Аналіз основних загроз інформаційних потоків підприємства.

Концепція безпеки підприємства. Система інформаційної безпеки підприємства. Служба безпеки фірми (підприємства, організації, установи). Недобросовісна конкуренція і захист комерційної таємниці. Ділова (корпоративна) розвідка. Приклади сценаріїв злому інформаційної системи на підприємстві. Наслідки порушення інформаційної безпеки на підприємстві. Основні закони та положення України, які регламентують відповідальність за порушення інформаційної безпеки. Нормативні документи на підприємстві для організації безпеки інформаційних технологій. Основні заходи щодо організації спеціального діловодства з носіями інформації.

Тема 8. Організація інформаційної безпеки на підприємстві.

Поняття політики безпеки (ПБ) на підприємстві. Служби інформаційної безпеки (ІБ) на підприємстві. Типові функціональні обов'язки співробітників служби ІБ. Методика розробки ПБ на підприємстві. Основні етапи реалізації ПБ в умовах сучасного бізнесу. Типова структура підсистеми безпеки ОС і функції, які виконуються: ідентифікація й аутентифікація, розмежування доступу, аудит, підзвітність дій, повторне використання об'єктів, точність і надійність обслуговування, захист обміну даних. Реалізація підсистеми ІБ на підприємстві. Порядок проведення робіт з технічного захисту інформації. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. Роботи, які пов'язані із розробкою й аналізом засобів забезпечення інформаційної безпеки комп'ютерних систем на основі розроблених програм і методик, у тому числі із забезпеченням вимог, що випливають із документів, що регламентують режим дотримання державної таємниці. Організація оптимального використання парольного захисту інформації на підприємстві. Організація на підприємстві групи влагоджування інцидентів комп'ютерної безпеки. Її права, статус, обов'язки. Порядок й організація проведення розслідування за фактом комп'ютерного інциденту.

Тема 9. Захист від шкідливого програмного забезпечення.

Особливості забезпечення захисту ком'ютерних систем сполучених з глобальною мережею Інтернет. Типи та класифікація загроз, відповідно популярним сервісам. Вразливості протоколів Інтернет. Особливості загрози типу „відмова в обслуговувані". Характеристика інструментальних засобів захисту. Політика безпеки при використанні ресурсів мережі Інтернет. Руйнуючі програмні засоби. Програми з потенційно шкідливим впливом та їх властивості. Основні класи руйнуючих програм. Захист інформації у комп'ютерах від вірусів. Методи захисту від шкідливих програм. Тестовий

вірус. Програмні засоби захисту інформації. Вибір та застосування антивірусних програм. Політика безпеки при опрацюванні електронної пошти. Захист електронної пошти від спаму. Визначення та класифікація спаму. Особливості „фішінгу". Модель загроз від спаму. Методи розпізнавання спаму: чорні та білі списки, баєсовський підхід. Використання методів штучного інтелекту для розпізнавання спаму. Методи та засоби протидії спаму.

Тема 10. Перспективні напрями розвитку комплексів засобів захисту інформації.

Адаптивні комплекси засобів захисту інформації: активні системи захисту, системи виявлення вторгнень; системи керування захищеністю; комплекси засобів захисту інформації мобільних програмних систем. Передумови створення активних систем захисту інформації. Методика зменшення ефективності атак та збільшення ефективності захисту за рахунок використання обчислювальних ресурсів порушника. Основи систем аналізу вразливостей. Інформаційні сховища вразливостей та їх застосування. Системи аналізу вразливостей провідних світових виробників. Основи систем виявлення вторгнень. Системи виявлення вторгнень провідних світових виробників. Використання засобів штучного інтелекту для діагностики вразливостей та вторгнень в розподілені системи та мережі. Механізми та засоби захисту програм та електронного документообігу від несанкціонованої модифікації та розповсюдження. Безпека мобільного програмного забезпечення та мобільних пристроїв. Характеристика специфічних загроз. Особливості захисту мобільних програмних компонентів та систем мобільних програмних агентів. Задачі захисту мобільного програмного забезпечення та платформи його функціонування. Особливості системи безпеки COM/DCOM, ActiveX, Java, Framework, Flash Macromedia. Оцінка техніко-економічного рівня й ефективності запропонованих і реалізованих організаційно-технічних рішень, пов'язаних із застосуванням програмно-технічних засобів інформаційної безпеки, з урахуванням перспектив та напрямків їхнього вдосконалення.

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. Концептуальні засади забезпечення кібернетичної безпеки підприємств												
Тема 1. Основні положення кібернетичної безпеки підприємства.	**9**	2	2			5	12		2			10
Тема 2. Методи зламу комп'ютерних мереж.	**9**	2	2			5	12	2				10
Тема 3. Організаційно-правове забезпечення захисту інформації.	**14**	2	2			10	12					10
Тема 4. Побудова систем захисту від загроз порушення конфіденційності інформації.	**12**		2			10	12					10
Разом за змістовим модулем	**44**	**6**	**8**			**30**	**48**	**2**	**2**			**40**
Змістовий модуль 2. Концепція кібернетичної безпеки підприємств. Програмні засоби захисту інформації												
Тема 5. Побудова систем захисту від загроз порушення цілісності.	**14**	2	2			10	**12**	2	2			12
Тема 6. Побудова систем захисту від загроз порушення доступності.	**14**	2	2			10	**12**		2			12
Тема 7. Аналіз основних загроз інформаційних потоків підприємства.	**12**		2			10	**12**					12
Тема 8. Організація інформаційної безпеки на підприємстві.	**12**		2			10	**12**					12
Тема 9. Захист від шкідливого програмного забезпечення	**12**		2			10	**12**		2			10

Тема 10. Перспективні напрями розвитку комплексів засобів захисту інформації.	**12**		2			**10**	**11**					10
Разом за змістовим модулем	**76**	**4**	**12**			**60**	**71**	**2**	**6**			**68**
Усього годин	**120**	**10**	**20**			**90**	**120**	**4**	**8**			**108**

1

3. Теми практичних занять

Денна форма навчання

№ з/п	Назва теми	Кількість годин
1	Основні положення теорії інформаційної та кібернетичної безпеки	2
2	Аналіз ризиків та основні принципи забезпечення інформаційної безпеки	2
3	Контроль доступу користувачів до інформаційно-телекомунікаційної системи. Парольна аутентифікація	2
4	Моделювання процедури надання доступу до автоматизованої інформаційної системи. Основні моделі безпеки	2
5	Нормативно-правовий підхід до забезпечення інформаційної безпеки України та провідних країн світу	2
6	Інформаційна безпека на рівні операційної системи Windows	2
7	Комп’ютерні віруси та інше шкідливе програмне забезпечення. Боротьба з malware	2
8	Основи забезпечення мережевої безпеки інформаційно-телекомунікаційної системи	2
9	Політика інформаційної безпеки віртуального підприємства	2
10	Побудова політики безпеки підприємства	2
	Усього	20

Заочна форма навчання

№ з/п	Назва теми	Кількість годин
1	Основні положення теорії інформаційної та кібернетичної безпеки	2
2	Аналіз ризиків та основні принципи забезпечення інформаційної безпеки	2
3	Виявлення ата Аналіз ризиків та основні принципи забезпечення інформаційної безпеки	2
4	Нормативно-правовий підхід до забезпечення інформаційної безпеки України та провідних країн світу	2
	Усього	8

4. Самостійна робота

Денна форма навчання

№ з/п	Назва теми	Кількість годин
1	Основні положення кібернетичної безпеки підприємства.	5
2	Методи зламу комп'ютерних мереж.	5
3	Організаційно-правове забезпечення захисту інформації	10
4	Побудова систем захисту від загроз порушення конфіденційності інформації.	10
5	Побудова систем захисту від загроз порушення цілісності.	10
6	Побудова систем захисту від загроз порушення доступності.	10
7	Аналіз основних загроз інформаційних потоків підприємства	10
8	Організація інформаційної безпеки на підприємстві.	10
9	Захист від шкідливого програмного забезпечення	10
10	Перспективні напрями розвитку комплексів засобів захисту інформації	10
	Усього	90

Заочна форма навчання

№ з/п	Назва теми	Кількість годин
1	Основні положення кібернетичної безпеки підприємства.	10
2	Методи зламу комп'ютерних мереж.	10
3	Організаційно-правове забезпечення захисту інформації	10
4	Побудова систем захисту від загроз порушення конфіденційності інформації.	10
5	Побудова систем захисту від загроз порушення цілісності.	12
6	Побудова систем захисту від загроз порушення доступності.	12
7	Аналіз основних загроз інформаційних потоків підприємства	12
8	Організація інформаційної безпеки на підприємстві.	12
9	Захист від шкідливого програмного забезпечення	10
10	Перспективні напрями розвитку комплексів засобів захисту інформації	10
	Усього	108

5. Індивідуальні завдання

Підготовка тез доповіді на конференції/статті з обраної теми.

Вирішення типових завдань за темами змістових модулів.

6. Методи навчання

Викладання дисципліни здійснюється через лекційні та практичні заняття, індивідуальні та групові консультації, самостійну роботу здобувачів освіти з виконання практичних завдань по кожній темі по індивідуальним варіантам, захист практичних робіт, тестування.

Усі теми дисципліни згруповані у 5 змістових модулях.

7. Критерії оцінювання

Критерії поточного оцінювання знань здобувачів освіти**.**

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 здобувачі освіти, 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 здобувачі освіти, 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 здобувачі освіти, які своїм запитанням до виступаючого суттєво і конструктивно можуть доповнити хід обговорення теми.

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

Експрес-контроль***:***

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

1 бал отримують здобувачі освіти, 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.

Здобувачам освіти пропонується скласти словник основних термінів з конкретної теми на останніх сторінках опорного конспекту лекцій.

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

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

Ведення опорного конспекту лекції***:***

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

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

Підготовка творчих завдань(есе, дайджест):

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

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

Підсумковий модульний контроль знань здобувачів освіти**.**

Критерії підсумкового модульного оцінювання знань здобувачів освіти

Письмова контроль на 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, и 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.

8. Засоби оцінювання

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

Завданням поточного контролю знань ЗВО 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.

9. Розподіл балів, які отримують здобувачі освіти

Поточне тестування та самостійна робота											Сума (в балах)
Змістовий модуль №1				Змістовий модуль №2							
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Тези/ наук. стаття	
5	5	5	5	10	5	10	10	10	5	30	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

10. Інструменти, обладнання та програмне забезпечення:

Під час викладання дисципліни для занять використовується лабораторна база комп'ютерних класів МДУ, які обладнано мережею комп'ютерів IBM Pentium.

11. Рекомендовані джерела інформації:

Основна:

1. Бедрій Я. І. Івах Р. М., Рощин В. О., Ємкало В. М. Цивільна оборона України : навч. Посібник. Київ: Кондор, 2011. 358 с.
2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.
3. Концепція розвитку цифрової економіки та суспільства України на 2018- 2020 роки : розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/67-2018-%D1%80/page
4. Крегул Ю. І., Зубок М. І., Банк Р. О. Комерційна розвідка та внутрішня безпека на підприємстві : навч. посібник / за ред. Ю. І. Крегула. Київ: КНТЕУ, 2014. 176 с.
5. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. Посібник. Київ: КНТ, 2006. 280с.
6. Мазаракі А. А., Корольчук О. П., Мельник Т. М. та ін. Економічна безпека України в умовах глобалізаційних викликів : монографія / за заг. ред. А. А. Мазаракі. Київ: КНТЕУ, 2010. 718 с.
7. Облік послуг з охорони на підприємстві. Вісник податкової служби України. 2013. № 32. С.12-23.
8. Скібіцька Л. І. Організація праці менеджера : навч. Посібник. Київ: Центр учбової літератури, 2010. 360 с.
9. Стратегія кібербезпеки України (Україна), 15 березня 2016, № 96/2016. URL: http://zakon2.rada.gov.ua/laws/show/96/2016

Додаткова:

10. Бабенко О. Безпека систем дистанційного банківського обслуговування. Фінансовий ринок України. 2012. №5. С.30-31.
11. Бєгун А. Безпека Web-сайтів економічних об'єктів. Ринок цінних паперів України. 2012. №9. С.115-120.
12. Боднар І. Р. Пріоритетні напрями держави в сфері інформаційної безпеки. Економіка & держава. 2012. №2. С.27-29.
13. Бурячок, В. Л., & Богуш, В. М. (2014). Рекомендації щодо розробки та запровадження профілю навчання «Кібернетична безпека» в Україні. Безпека інформації, 20(2), 126–131. doi: 10.18372/2225-5036.20.7297

14. Волох, О. К. (2016). Питання кібернетичної безпеки в умовах розбудови інформаційного суспільства. Юридичний науковий електронний журнал, 4, 104–107.

15. Гахов, С. О. (2016). Застосування методів правового регулювання під час здійснення організаційних заходів щодо кібернетичного захисту інформаційних систем підприємств, установ та організацій. Сучасний захист інформації, 3, 67–71.

16. Герасименко О. М. Інформаційна безпека торговців цінними паперами. Економіка, фінанси, право. 2010. №1. С.18-21.

17. Деркач Т. Інформаційна безпека в Україні: огляд законодавчих змін. Бухгалтерія. 2014. № 29. С.51-55.

18. Дешко Л. М., Бондарєва К. Д. Кібербезпека в Україні: національна стратегія та міжнародне співробітництво [Електронний ресурс] // Електронне наукове фахове видання «Порівняльно-аналітичне право». – 2018. - №2. – с.379-382. – Режим доступу: http://www.pap.in.ua/2_2018/112.pdf.

19. Диба М., Яременко С. Економічна безпека банків: стан та проблеми. Банківська справа. 2013. №4. С.3-9.

20. Дудатьєв А. В., Войтович О. П., Каплун В. А. Захист комп'ютерних мереж. Теорія та практика: навч. посібник. Вінниця: ВНТУ, 2009. 219 с.

21. Забара І. Розвиток правового регулювання інформаційної безпеки в Європейському Союзі. Право України. 2012. №7. С.106-117.

22. Зубок М. І. Інформаційна безпека : навч. Посібник. Київ: КНТЕУ, 2009. 133 с.

23. Іващенко Г. А., Воронюк, Є. В. (2017). Кібернетична безпека в системі діагностики та аналізу економічної безпеки підприємства. Молодий вчений, 1, 605–608

24. Кириченко О. А., Шикова О. М. Теоретичні засади інформаційної безпеки держави. Економіка & держава. 2011. №3. С.26-29.

25. Копитко С. Б. Апробація комплексу економіко-математичних моделей управління ефективністю системи захисту комп'ютерної інформації. Актуальні проблеми економіки. 2013. №12. С.235-244.

26. Корченко О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О.Г. Корченко, В. Л. Бурячок, С.О. Гнатюк // Безпека інформації. – 2013. – Т. 19, № 1.

27. Мєзєнцева Н. Б. До питання наукового обґрунтування політики і методології державної системи інформаційної безпеки. Економіка & держава. 2013. №3. С.142-144.

28. Мороз, Ю. Ю., & Цаль-Цалко, Ю. С. (2017). Облікова політика підприємства та її кібербезпека. Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства, 4(1), 8–11.

29. Нога, І. М., Скриньковський, Р. М., & Павловські, Г. (2016). Діагностика ефективності застосування інформаційних технологій в управлінні підприємствами. Бізнес Інформ, 9, 241–245.

30. Панфілов О. Ю. До проблеми оцінки сучасного рівня інформаційної безпеки України. Зовнішня торгівля: економіка, фінанси,

право. 2012. №3. С.226-235.

31. Ситніченко В., Кісельова Г., Стоякін Є. Формування інформаційної безпеки на основі стандарту ISO/IEK 27001:2005. Стандартизація, сертифікація, якість. 2010. №2. С.50-56.

32. Скриньковський, Р. М., Крамар, Р. І., & Гарасим, П. С. (2016). Діагностика ефективності системи захисту інформації на підприємстві та відповідальність за порушення законодавства про комерційну таємницю. Порівняльно-аналітичне право, 1, 225–228

Нормативно-правові

33. Конституція України: Закон України від 28 червня 1996 р. №254к/96-ВР / Верховна Рада України. Відомості Верховної Ради України. 1996. №30.

34. Про державну таємницю: Закон України від 21 січня 1994 року №3855-XII. / База даних «Законодавство України. URL: http://zakon4.rada.gov.ua/laws/show/3855-12

35. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. №851-IV. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T030851.html

36. Про електронний цифровий підпис: Закон України від 22 травня 2003 р. №851-IV. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T030852.html

37. Про захист інформації в автоматизованих системах. Закон України від 05.07.94р. / Відомості Верховної Ради України. 1994.

38. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 31.05.2005 №2594-IV-ВР. / База даних «Законодавство України. URL: http://zakon4.rada.gov.ua/laws/show/80/94

39. Про національну програму інформатизації: Закон України від 04.02.1998 №74/98 – ВР. / Відомості Верховної Ради України. 1998. №27-28. Ст. 181.

40. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017р. №2163-VIII. Відомості Верховної Ради. 2017. №45. Ст.403.

41. Про основні засади розвитку інформаційного суспільства в України 2007-2015 роки: Закон України від 09 січня 2007. / Відомості Верховної Ради України. 2007. № 12. – Ст. 102.

42. Про основи національної безпеки України: Закон України від 19 червня 2003 р. / Голос України. 2003. №134.

43. Про порядок здійснення криптографічного захисту інформації в Україні: Указ президента України від 22 травня 1998 р. №505/98. URL: http://www.uapravo.net/akty/ministerstvo-main/akt9pprs7f.htm

44. Про положення про технічний захист інформації в Україні: Указ президента України від 27 вересня 1999 р. №1229. / База дани «Законодавство України. URL:http://zakon4.rada.gov.ua/laws/show/1229/99

45. Управління боротьби з кіберзлочинністю // Міністерство внутрішніх справ України [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/ publish/article/544754