ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ЗАТВЕРДЖЕНО
Рішення методичної ради університету
14 лютого 2024 року,
протокол № 5.
Перша проректорка, головуюча на засіданні вченої ради університету, кандидатка наук з державного управління, доцентка

_____ Ірина КОВТУН
(ініціали, прізвище)

22 лютого 2024 року

м.п.

НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ
з навчальної дисципліни
«ІНФОРМАЦІЙНА БЕЗПЕКА БІЗНЕСУ»
для підготовки на першому (освітньому) рівні
здобувачів вищої освіти ступеня бакалавра
за спеціальністю 073 Менеджмент
галузі знань 07 Управління та адміністрування
за денною формою навчання

м. Хмельницький
2024

РОЗРОБНИК ПРОГРАМИ:

Доцент кафедри менеджменту, економіки, статистики та цифрових технологій кандидат економічних наук, доцент _____ Віталій КУДЕЛЬСЬКИЙ
20 січня 2024 року

СХВАЛЕНО

Рішенням кафедри менеджменту, економіки, статистики та цифрових технологій
22 січня 2024 року, протокол № 7.

Завідувачка кафедри, доцентка, кандидатка економічних наук, доцентка

_____ Наталія ЗАХАРКЕВИЧ

22 січня 2024 року

Деканеса факультету управління та економіки, кандидатка економічних наук, доцентка _____ Тетяна ТЕРЕЩЕНКО
23 січня 2024 року

Обліковий обсяг 1,51 ум.др.арк.

ЗМІСТ

1. Структура вивчення навчальної дисципліни

1.1. Тематичний план навчальної дисципліни

№ теми	Назва теми	Кількість годин											
		Денна форма навчання						Заочна форма навчання					
		Усього	у тому числі					Усього	у тому числі				
			Лекції	Сем. (прак).	Лабор.	Ін.зав.	СРС		Лекції	Сем. (прак).	Лабор.	Ін.зав.	СРС
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	Інформаційна безпека: підходи до концептуалізації та індикатори визначення	10	2	2	–	–	6	12	1	1	–	–	10
2.	Інформаційні загрози бізнесу та їх види.	18	4	4	–	–	10	13	1	1	–	–	11
3.	Принципи побудови системи інформаційної безпеки.	10	2	2	–	–	6	11	–	1	–	–	10
4.	Системи та моделі захисту інформації.	13	2	4	–	–	7	12	1	1	–	–	10
5.	Державні інформаційні ресурси.	10	2	2	–	–	6	11	1	–	–	–	10
6.	Конфіденційність документу та комплексний захист інформації.	11	2	2	–	–	7	12	1	1	–	–	10
7.	Системи управління інформаційною безпекою бізнесу.	11	2	2	–	–	7	12	1	1	–	–	10
8.	Політика інформаційної безпеки підприємства.	11	2	2	–	–	7	11	–	1	–	–	10
9.	Контроль стану інформаційної безпеки на підприємстві.	11	2	2			7	11	–	1			10
	Всього годин:	105	20	22	–	–	63	105	6	8	–	–	91

1.2. Лекції

№ з/п	Назва і план теми	Кількість годин
1	2	3
1.	Інформаційна безпека: підходи до концептуалізації та індикатори визначення	2
1.1. 1.2. 1.3.	Інформаційне суспільство. Система забезпечення інформаційної безпеки. Визначення критеріїв захищеної системи обробки інформації та постановка задач	
2.	Інформаційні загрози бізнесу та їх види.	4
2.1. 2.2. 2.3. 2.4. 2.5. 2.6.	Причини порушення інформаційної безпеки. Класифікації загроз інформаційної системи. Засоби і способи захисту інформації. Інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія. Інформаційно-психологічна протидія, контроль каналів передачі інформації, система моніторингу та прогнозування негативних інформаційно-психологічних впливів. Поняття і різновиди загроз інформаційній безпеці.	
3.	Принципи побудови системи інформаційної безпеки.	2
3.1. 3.2. 3.3.	Підходи, принципи і методи забезпечення інформаційної безпеки. Засоби забезпечення інформаційної безпеки. Принципи формування політики інформаційної безпеки підприємства.	
4.	Системи та моделі захисту інформації.	2
4.1. 4.2. 4.3.	Функції системи захисту інформації (ЗІ). Моделі інформаційної безпеки. Стандарти по забезпеченню інформаційної безпеки бізнесу.	
5.	Державні інформаційні ресурси.	2
5.1. 5.2. 5.3.	Державне регулювання інформаційної безпеки. Загрози інформаційній безпеці України. Структура та функції державної системи забезпечення інформаційної безпеки.	
6.	Конфіденційність та комплексний захист інформації.	2
6.1. 6.2. 6.3.	Загальні відомості та задачі комплексного захист інформації (КЗІ). Етапи побудови КЗІ для різних стратегій. Цілі захисту інформації на підприємстві.	
7.	Системи управління інформаційною безпекою бізнесу.	2
7.1. 7.2. 7.3.	Правила управління інформаційною безпекою підприємства. Етапи управління інформаційною безпекою підприємства. Функції технологічного управління інформаційною безпекою.	
8.	Політика інформаційної безпеки підприємства.	2
8.1. 8.2. 8.3.	Інформаційні технології на підприємстві. Правові аспекти інформаційної безпеки бізнесу. Політика інформаційної безпеки (ІБ) бізнесу: цілі, завдання, зміст.	
9.	Контроль стану інформаційної безпеки на підприємстві.	2
9.1. 9.2. 9.3.	Цілі та метод проведення зовнішнього контролю. Принципи контролю інформаційної безпеки. Права працівників на доступ до серверів і баз даних колективного використання.	
	Усього	20

1.3. Семінарські заняття

Семінарське заняття 1

Тема 1. Інформаційна безпека: підходи до концептуалізації та індикатори визначення.

Питання для усного опитування та дискусії

1.1.Інформаційна сфера.

1.2.Інформаційна безпека.

1.3.Національна безпека.

1.4.Кібернетична безпека.

1.5.Підходи до дослідження інформаційної безпеки.

1.6.Сутність категорій: «інформаційна безпека», «політика безпеки», «інформаційна загроза», «інформаційна війна», «інформаційний вплив», «інформаційна зброя».

Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Теми доповідей:

1.Безпека бізнесу в Україні: історія та сучасність.

2.Особливості захисту інформації в комерційній діяльності суб'єктів підприємництва та їх ділових взаємовідносинах.

3.Інформаційні взаємовідносини суб'єктів підприємництва.

Методичні рекомендації

Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є: інформація, безпека, інформаційна сфера, інформаційна безпека, політика безпеки, інформаційна загроза, інформаційна війна, інформаційний вплив, інформаційна зброя, національна безпека, кібернетична безпека.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- інформаційні аспекти;
- інформаційне суспільство;
- інформаційна культура;
- інформаційна подія;
- інформаційне становище;
- рекрутинг інформації;
- інформаційне життя;
- інформаційна конфронтація.

Семінарське заняття 2-3

Тема 2. Інформаційні загрози бізнесу та їх види.

Питання для усного опитування та дискусії

2.1. Поняття «загрози безпеки інформації», причини їх виникнення, їх види та особливості прояву.

2.2.Підходів щодо помилок в системах захисту інформації.

2.3.Інформаційне протиборство, інформаційна експансія, інформаційна війна, інформаційний тероризм.

2.4.Принципи інформаційної війни.

2.5.Логіка інформаційної війни.

2.6.Моделі інформаційної війни.

2.7.Різновиди інформаційних воєн.

2.8.Засоби, методи і технології інформаційних воєн.

2.9.Інтернет-ресурси як об'єкти загроз інформаційній безпеці підприємства.

2.10.Система моніторингу Інтернет-ресурсів.

2.11.Актори соціальних Інтернет-сервісів.

2.12.Контент і дані акторів соціальних Інтернет-сервісів.

2.13. Загрози інформаційній безпеці бізнесу у соціальних Інтернет-сервісах.

Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Завдання.1. Обсяг продукції випущеної за квартал (4 місяці) 130000 грн; витрати на придбання інформаційних ресурсів на протязі року склали 5300 грн. Визначити продуктивність інформації.

Завдання.2. Витрати підприємства на захист інформаційних ресурсів 890000 грн; витрати на придбання інформаційних ресурсів -780000 грн. Визначити коефіцієнт захищеності інформації.

Завдання 3. Класифікуйте інформаційні активи, що знаходяться на вашому пристрої (мобільному телефоні, ноутбуці, домашньому ПК і т.д.), сформулюйте потенційні загрози інформації, визначіть методи та засоби їх уникнення. Представити у вигляді таблиці відповідності «інформація-загрози-методи і засоби уникнення».

Методичні рекомендації

***Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є*:** загроза, інформаційне протиборство, інформаційна експансія, інформаційний тероризм, Інтернет-ресурси, актори соціальних Інтернет-сервісів, контент.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- соціально-психологічна стабільність;
- обробка інформації;
- закони поведінки;
- психологічне моделювання;
- логіка речей;
- етичні норми;
- відтінки інформації;
- інформаційна динаміка.

Семінарське заняття 4

Тема 3. Принципи побудови системи інформаційної безпеки.

Питання для усного опитування та дискусії

3.1.Організаційно-технічне забезпечення комп'ютерної безпеки.

3.2.Способи забезпечення інформаційної безпеки економічних систем.

3.3.Принципи забезпечення інформаційної безпеки на основі інженерно-технічного забезпечення.

3.4.Захист від комп'ютерних вірусів.

3.5.Електронний цифровий підпис.

Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Завдання 1. Обсяг продукції випущеної 1300 шт. при ціні 10 грн за одиницю; витрати на придбання інформаційних ресурсів на протязі року склали 15300 грн. Визначити продуктивність інформації.

Методичні рекомендації

Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є: організаційно-технічне забезпечення, комп'ютерна безпека, інформаційна безпека економічних систем, комп'ютерний вірус, електронний цифровий підпис .

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- деталізований опис;
- вибір альтернатив;
- механізм оперативного реагування;
- умови оперативного реагування;
- оцінка ефективність контрзаходів;
- матеріально відповідальна особа (підписант)
- SmartID;

- КЕП.

Семінарське заняття 5-6

Тема 4. Системи та моделі захисту інформації.

Питання для усного опитування та дискусії

4.1.Матриця розподілу доступу.

4.2.Види політики безпеки: виборча політика безпеки, повноважна політика безпеки.

4.3.Політика інформаційної безпеки бізнесу.

4.4.Модель розподілу інформаційних потоків.

4.5.Заходи захисту інформації: організаційно-технічні, адміністративні.

4.6.Вимоги до стандартів з інформаційної безпеки.

4.7.Форми представлення стандартів (документальна, усна).

4.8.Міжнародний стандарт безпеки ISO/IEC 17799.

4.9.Організаційні заходи підприємства щодо забезпечення безпеки.

4.10.Класифікація і управління ресурсами.

4.11.Безпека персоналу.

4.12.Фізична безпека.

4.13.Управління комунікаціями та інформаційними процесами.

4.14. Розробка і технічна підтримка інформаційних систем підприємства. Управління інцидентами інформаційної безпеки. Управління неперервністю бізнесу.

Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Завдання 1. Побудувати модель системи безпеки підприємства в інформаційній сфері.

Завдання 2. Продумати ідею створення власного бізнесу. Дайте відповідь на ключові питання брифу:

1. Інформація про бренд:

1.1. Назва бренду та причина обрання назви.

1.2. Хто є обличчям бренду? Опишіть коротко автобіографію.

1.3. Ніша бренду.

1.4. Цінова стратегія.

1.5. Які проблеми споживачів вирішує ваш товар / послуга.

1.6. Місія бренду.

1.7. Принципи бренду.

2. Інформація про товар / послугу:

2.1. Види (асортимент) товарів / послуг.

2.2. Призначення товарів / послуг.

2.3. Опишіть складові частини товарів / послуг.

2.4. Опишіть етапи виробничого процесу.

2.5. Чи володіє ваш бізнес унікальної методикою та технологіями?

2.6. Переваги вашого продукту порівняно з конкурентами.

2.7. Недоліки вашого продукту порівняно з конкурентами.

2.8. Опишіть упаковку товару / послуги.

2.9. Опишіть супровідне та після продажне обслуговування клієнта.

3. Інформація про цільову аудиторію та клієнтів:

3.1. Виділіть сегменти цільової аудиторії. Опишіть кожен сегмент.

3.2. Пріоритети цільової аудиторії (на що вони звертають увагу).

3.3. На що звертають увагу незадоволені клієнти?

3.4. Чи є серед вашої цільової аудиторії відомі особистості?

3.5. Чи піддаються клієнти емоційним покупкам?

3.6. На що звертають увагу клієнти, приймаючи рішення придбати товару / послугу?

3.7. Які питання найчастіше задають клієнти?

3.8. Чи є ваш товар / послуга сезонною?

3.9. Чи важлива для клієнтів юридична гарантія товару / послуги?

4. Інформація про сервіс:

4.1. Опишіть етапи роботи з клієнтом від першого звернення до завершення покупки.
4.2. Чи супровідне та після продажне обслуговування?
Відповідь опишіть детально.
4.3. Які бонуси, подарунки та знижки передбачаються для клієнтів?
4.4. Опишіть доставку товару.
4.5. Як ви підтримуєте зворотній зв'язок з клієнтами?
4.6. Як ви працюєте з негативними відгуками клієнтів?
4.7. Скільки клієнтів налічує ваш бізнес?
Дані оформіть у вигляді таблиці 1.1

Таблиця 1.1

Бриф

н/п	Питання	Відповідь
1	Назва питання	
2		
3		
4		

Методичні рекомендації

Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є: матриця, доступ, стандарт, бізнес, інформаційний потік, організаційні заходи, безпека, персонал, фізична безпека, комунікація, процес.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- інформаційний план;
- технічні канали;
- комунікаційне обладнання;
- екранове приміщення;
- лінія звязку;
- локальні мережі;
- віртуальні мережі;
- між мережевий екран;
- хибний об’єкт атаки.

Семінарське заняття 7

Тема 5. Державні інформаційні ресурси.

Питання для усного опитування та дискусії

5.1.Інформаційна безпека та її місце в структурі національної безпеки України.
5.2.Національний інтерес в інформаційній сфері держави.
5.3.Стан та перспективи розвитку інформаційної безпеки держави.
5.4.Державна політика забезпечення інформаційної безпеки бізнесу в Україні
5.5.Особливості реалізації комплексних систем захисту інформації.
5.6.Ліцензування в галузі забезпечення інформаційної безпеки.
5.7.Сертифікація засобів і методів неусвідомлюваного інформаційного впливу.
5.8.Експертиза інформаційної безпеки.
5.9.Контроль за забезпеченням інформаційної безпеки.

.Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Методичні рекомендації

Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є:: національна безпека, національний інтерес, інформаційна сфера, держава, державна політика, ліцензія, сертифікат.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- державні ресурси;
- державні інформаційні ресурси;
- державні електронні інформаційні ресурси;
- органи державної влади;
- Національна програма інформатизації;
- інформаційне суспільство держави;
- масив документів;
- невичерпність інформації;
- національні інформаційні ресурси;
- реєстр інформації;
- Концепції електронного урядування.

Семінарське заняття 8

Тема 6. Конфіденційність та комплексний захист інформації.

Питання для усного опитування та дискусії

6.1.Стратегії комплексного захисту інформації.
6.2.Безпека цінних інформаційних ресурсів.
6.3.Критерії цінності інформації.
6.4.Виявлення та документування конфіденційних відомостей.
6.5.Носії конфіденційних відомостей.
6.6.Розробка комплексної системи захисту інформації на підприємстві від IT Ресурс.

Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Завдання 1. Цифрова безпека бізнесу: як захиститися

Бізнес по всьому світу переживає епоху цифрової трансформації. Це можна порівняти з метаморфозом метелика. Власники бізнесу мусять швидко адаптуватися, поєднуючи традиційні та цифрові методи управління.

Що робити сьогодні, щоб вберегти дані бізнесу? (Відповідно до оорганізаційно-правових форм) Створення бізнес-кейсу захисту інформації по підприємству за прикладом:

1. Створіть стратегію управління ризиками.

1.1.Поставте цілі та створіть бізнес-кейс.

1.2.Пріоритети компанії, її місію та візію в умовах діджиталізації.

1.3. Визначте нові фізичні, мобільні та кіберзасоби контролю безпеки та додайте до вже чинної концепції захисту даних.

1.4.Рорзробіть статут з кібербезпеки, адже зробить вас більш надійним партнером. *2*

2.Розробіть план дій.

2.1.Визначте пріоритетні ризики для вашого бізнесу. За потреби долучіть компанію, що займається кібербезпекою.

2.2.Розробити основні принципи кібергігієни в компанії. Наприклад, які використовувати паролі, логін у відкриті мережі Wi-FI з робочого комп'ютера vs використання захищеної мережі, класифікація документів, доступ до конфіденційної інформації поза межами офісу та багато іншого.

3. Ініціюйте реалізацію.

Поінформуйте співробітників щодо впровадження інструментів кібербезпеки та проведіть навчання, прищеплюйте культуру поваги до безпеки даних компанії. Залучіть новий відділ та експертів з кібербезпеки, встановіть нові ролі та обов'язки в команді. Тренуйте бажані навички, водночас інтегруйте можливі інструменти й технології: від звичайних надійних паролів на робочих комп'ютерах та антивірусних програм, до спеціальних систем захисту даних.

4. Вибудуйте програму та розвивайте її в подальшому

Підтримуйте звітність у процесах захисту даних, проводьте моніторинги. Нехай у вас під рукою буде екстрений план дій у разі виявлення порушень. Для попередження кібератак існують такі технології, як "ханіпоти" (honeypots и honeynets), і більш серйозні превентивні системи DDP (Distributed Deception Platform).

Методичні рекомендації

Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є: стратегія, критерії, документування, конфіденційність, носії конфіденційних відомостей, IT Ресурс.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- несанкціонований доступ;
- комунікативне обладнання;
- периметри інформаційної системи;
- віртуальні мережеві системи;
- система зашумлення;
- модель поведінки;
- моделювання загроз інформаційної безпеки;
- доступ на читання;
- доступ на запис;
- доступ на виконання;
- вбезпечення інформації.

Семінарське заняття 9

Тема 7. Системи управління інформаційною безпекою бізнесу.

Питання для усного опитування та дискусії

7.1.Загальні положення з управління інформаційною безпекою.
7.2.Методи і засоби соціального інжинірингу.
7.3.Етапи розробка політики інформаційної безпеки.
7.4.Система фізичного захисту типові задачі та способи її реалізації.
7.5.Основні характеристики системи фізичного захисту.
7.6.Кількісний і якісний аналіз системи фізичного захисту.
7.7.Інженерно-технічні засоби охорони.

Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Завдання 1.

1.Сформулюйте основні концептуальні положення управління економічною безпекою підприємства.

2. Наведіть приклади факторів, які впливають на стан економічної безпеки підприємства.

3.Визначте елементи світового досвіду забезпечення економічної безпеки підприємства доцільно запровадити в Україні та як їх адаптувати під особливості ведення вітчизняного бізнесу.

4.Визначте основні функціональні цілі економічної безпеки (Таблиця-Функціональні цілі Напрям прояву функціональної цілі економічної безпеки).

5.Оцінка рівня економічної безпеки підприємства.

6.Сформулюйте основні функціональні ознаки фінансової складвої економічної безпеки підприємства (таблиця-Функціональна складова Змістовні ознаки).

7.Сформулюйте основні функціональні ознаки інформаційної складвої економічної безпеки підприємства (таблиця-Функціональна складова Змістовні ознаки).

8.Виділіть основні відмінності між показниками та індикаторами економічної безпеки підприємства.

9.Обгрунтуйте, які методи оцінки економічної безпеки необхідно використовувати на макро-, мезо- та мікро- рівнях економіки?

10. Визначте функції служби безпеки на підприємстві для підтриманню належного рівня економічної та інформаційної безпеки підприємства

Методичні рекомендації

Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є: соціальний інжиніринг, політика, фізичний захист, аналіз, управління, охорона, інженерно-технічні засоби.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- шахраї;
- хакери;
- кіберзлочинність;
- доступ до інформації;
- парольний захист;
- криптографічний захист;
- шифрування;
- моніторинг інформації;
- ISO/IEC 27001;
- ISO 9001:2000.

Семінарське заняття 10

Тема 8. Політика інформаційної безпеки підприємства.

Питання для усного опитування та дискусії

8.1.Сучасне підприємство: бізнес-процеси, інформаційні технології (ІТ), інформаційна та кібернетична безпека.

8.2.Часткові політики інформаційної безпеки.

8.3.Мета та завдання перед проектного етапу: підготовка вихідних даних та обстеження об’єкту інформаційної діяльності.

8.4.Класифікація та оцінка інформаційних ресурсів.

8.5.Задачі моделювання інформації.

8.6.Побудова моделі порушника ІБ.

Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Завдання 1. Розробіть інформаційний буклет «Циганський гіпноз: способи уникнення та протидії».

Завдання 2. Розробіть інформаційний буклет «Як підготуватися до публічного виступу». Запропонуйте програму одноденного тренінгу; мета: розвинути навички переконуючого впливу.

Методичні рекомендації

Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є: підприємство, інформаційні технології (ІТ), бізнес-процес, дані, інформаційна діяльність, інформаційні ресурси, моделювання інформації, модель, порушник.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- інформаційна фіяльність;
- політика економічної безпеки;
- незаконні методи ведення бізнесу;
- недостатня або слабка юридична підтримка;
- зниження лояльності споживачів, зміна трендів на ринку;
- співпраця з підсанкційними контрагентами;
- халатність;
- шахрайство;
- визначення сфер відповідальності;
- порядку обробки персональних даних;
- архівування та зберігання документів;

- обміну документами з працівниками та контрагентами;
- правила зберігання та передачі паролів;
- забезпечення безпеки обладнання підприємства;
- доступ до мережі компанії;
- безпека користування електронною поштою;
- порушення законодавства про захист персональних даних.

Семінарське заняття 11

Тема 9. Контроль стану інформаційної безпеки на підприємстві.

Питання для усного опитування та дискусії

10.1.Контроль систем менеджменту інформаційної безпеки.

10.2.Способи підтвердження входу кожного користувача (аутентифікація).

10.3.Принципи резервного копіювання даних.

10.4.Конфігурація і налаштування мережевих пристроїв, систем зберігання та передачі даних.

10.5.Робота антивірусного і антишпигунського програмного забезпечення, наявність ліцензії.

10.6.Теоретичні та практичні знання працівників підприємства про захист даних.

10.7.Контроль доступу.

10.8.Передумови розвитку послуг із забезпечення інформаційної безпеки та їх структура.

11.9.Інфраструктура публічних ключів.

10.10.Страхування інформаційних ризиків.

10.11.Основи страхування інформаційних ресурсів.

Аудиторна письмова робота

Виконання письмових завдань у тестовій формі за темою заняття.

Завдання 1. Групова робота. У підгрупах визначте, якими рисами та характеристиками має володіти людина, щоб пробуджувати імпульс до наслідування.

Завдання 2. Авторитет комунікатора: чинники та способи формування Способи когнітивної підготовки ідей (презентація - 2 студенти).

Завдання 3. Визначте способи попередження та нейтралізації контраргументів у процесі переконуючого впливу.

Завдання 4. Визначте роль невербальних засобів у процесі аргументації.

Методичні рекомендації

Ключовими термінами, на розумінні яких базується засвоєння навчального матеріалу теми, є: контроль, аутентифікація, принцип, програмне забезпечення, конфігурація, публічний ключ, ризик, страхування.

З метою глибокого засвоєння навчального матеріалу при самостійному вивченні теми студенту варто особливу увагу зосередити на таких аспектах:

- кібергігієна;
- ризику безвідповідальних дій;
- ризику фізичної втрати даних;
- ризику втрати ділової репутації;
- захист інформаційних активів організації;
- забезпечення стабільної діяльності організації;
- мінімізації ризиків інформаційної безпеки;
- створення позитивних для організації інформаційних відносин з партнерами, клієнтами та всередині організації;
- технічні канали витоку інформації;
- обізнаність персоналу;
- віддалений доступ.

1.4. Самостійна робота студентів

Самостійна робота студентів є однією з форм оволодіння матеріалом із навчальної дисципліни «Інформаційна безпека бізнесу». Виконання самостійної роботи дозволяє студентам розвивати самостійне мислення, поглиблювати засвоєні теоретичні знання, опановувати практичні навички з управління інноваціями.

Самостійна робота із навчальної дисципліни «Інформаційна безпека бізнесу» складається з двох окремих завдань: наукової роботи (реферат) та одного індивідуального завдання. Письмова робота та індивідуальне завдання виконується у межах годин, відведених для самостійної роботи навчальним планом.

Студенти виконують наукову роботу та індивідуальне завдання самостійно з одержанням необхідних консультацій від науково-педагогічного працівника протягом семестру. Форма контролю – перевірка письмових робіт та заслуховування доповіді за темою наукової роботи. Питання письмової роботи виносяться на підсумковий семестровий контроль.

1.4.1.Основні вимоги до написання рефератів-оглядів

При виконанні індивідуального Завдання необхідно взяти до уваги, що реферат (лат. refero – доношу, повідомляю, переказую) – це короткий переказ змісту наукової роботи, книги або вчення, оформлене у вигляді письмової публічної доповіді; доповідь на задану тему, зроблена на основі критичного огляду відповідних джерел інформації (наукових праць, літератури по темі).

Зі свого боку, реферат - огляд складається на основі декількох джерел і зіставляє різні точки зору з досліджуваного питання.

Реферат-огляд, незалежно від теми, містить визначені реквізити: титульна сторінка встановленого зразка, вступ, розділи, висновки, список використаних джерел і додатки (у разі необхідності).

Обов’язково в тексті повинні бути посилання на джерела, що були використані при написанні реферату. Посилання подаються у квадратних дужках з вказівкою номера джерела, за яким воно внесене у список використаних джерел, та сторінки (якщо подається точна цитата або числові дані), наприклад [3, с.8].

Технічні вимоги: текст має бути набраний шрифтом Times New Roman, 14 кеглем через 1,5 інтервали. Поля: верхнє – 2,0 см, нижнє – 2,0 см, ліве – 3,0 см, праве – 1,0 см. Загальний обсяг реферату-огляду – до 15 сторінок формату А4.

Теми рефератів-оглядів

1. Інформація як основний об’єкт інформаційних правовідносин: поняття, властивості та види.
2. Інформаційні правовідносини: поняття, структура, характеристика основних елементів.
3. Поняття та види інформаційної діяльності. Інформаційне забезпечення як спосіб організації діяльності підприємства.
4. Право на доступ до інформації про діяльність підприємства.
5. Обов'язок посадових осіб підприємства оприлюднювати офіційну документовану інформацію та інші відомості про свою діяльність.
6. Порядок надання інформації за запитами, зверненнями працівників підприємства
7. Підстави обмеження права на доступ до інформації. Трискладовий тест.
8. Правовий режим конфіденційної інформації.
9. Правовий режим службової інформації посадових осіб організації.
10. Правовий режим таємної інформації фірми.
11. Поняття, сутність та рівні забезпечення інформаційної безпеки.
12. Державна політика України в сфері інформаційної безпеки.
13. Основні загрози та засоби забезпечення інформаційної безпеки України. Інформаційна війна.
14. Міжнародно-правові засади інформаційної безпеки.
15. Кіберзлочинність: поняття та сутність.
16. Поняття комп’ютерної злочинності. Загальна характеристика комп’ютерних злочинів.
17. Кібертероризм: поняття та сутність.
18. Цілі кібертероризму, його відмінність від тероризму.
19. Інформаційна атака як основна форма кібертероризму.

20. Засоби, тактика та прийоми здійснення кібертероризму.

21. Основні напрями боротьби з кібертероризмом.

22. Інформатизація діяльності органів державної влади та місцевого самоврядування.

23. Перспективи розвитку електронного урядування в Україні.

24. Захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах органів державної влади та місцевого самоврядування.

25. Поняття та основні напрями інформатизації діяльності органів державної влади та місцевого самоврядування.

26. Основні нормативно-правові акти у сфері інформатизації.

27. Державна політика у сфері інформатизації.

28. Інформаційна послуга.

29. Електронна інформаційна система «Електронний Уряд».

30. Компетенція Державного агентства з питань електронного урядування.

31. Інформаційна (автоматизована) система.

32. Телекомунікаційна система.

33. Інформаційно-телекомунікаційна система.

34. Види інформації, що може міститися в інформаційно-телекомунікаційних системах.

35. Державні інформаційні ресурси.

1.4.2.Індивідуальне завдання.

Індивідуальне завдання виконується з прив'язкою до конкретного підприємства: а саме проходження виробничої практики на 2 курсі або підприємства використаного при написанні курсової роботи.

Вимоги: виконання індивідуальної роботи з дисципліни передбачає:

1) самостійне дослідження підприємства;

2) підготовку доповіді з презентацією;

3) відображення результатів проведеного дослідження у схематичному вигляді;

4) захист індивідуальної роботи.

Захист індивідуальної роботи здійснюється у два етапи:

1. Виступ – висвітлення основних положень, висновків з досліджуваної проблематики.

2. Презентація результатів наукового дослідження – подання узагальненого матеріалу у вигляді схеми/таблиці та проектів складеної схеми у друкованому вигляді у кількості, що відповідає кількості студентів академічної групи.

У проекті схеми зазначаються основні дефініції, критерії порівняння і т. п., проте місце для розкриття їх змісту залишається вільним. Заповнення проекту схеми студентами академічної групи відбувається під час виступу доповідача.

Для повноти проведення та виконання індивідуального завдання необхідно відповісти на наступні питання:

1. Зміст принципів відкритості, прозорості та гласності діяльності системи управління інформаційною безпекою бізнесу.

2. Міжнародні стандарти права на інформацію.

3. Нормативно-правове регулювання доступу до публічної інформації в Україні.

4. Нормативно-правове регулювання діяльності засобів масової інформації в Україні.

5. Правове регулювання відносин у мережі Інтернет в зарубіжних країнах та Україні: порівняльно-правова характеристика.

6. Нормативно-правове регулювання захисту персональних даних в Україні.

7. Правовий режим державної таємниці за законодавством України.

8. Правова характеристика основних видів таємної інформації підприємства.

9. Основи кримінальної відповідальності у сфері доступу до інформації.

10. Поняття та ознаки інформаційного суспільства.

11. Нормативно-правове забезпечення інформатизації в Україні.

12. Загальна характеристика основних видів атак на інформаційні системи підприємств.

13. Поняття та компетенція Державного агентства з питань електронного урядування України.

14. Засоби протидії кібезлочинності.

15. Боротьба із кіберзлочинністю: досвід зарубіжних країн.

16. Глобальна інформаційна мережа Інтернет як засіб поширення кібертероризму.

1.5. Підсумковий контроль

Підсумковий семестровий контроль проводиться у формі екзамену.

1.5.1. Питання для підсумкового контролю

1. Інформаційна сфера, інформаційна безпека, національна безпека, кібернетична безпека.
2. Інформаційне суспільство.
3. Підходи до дослідження інформаційної безпеки.
4. Система забезпечення інформаційної безпеки.
5. Сутність категорій: «інформаційна безпека», «політика безпеки», «інформаційна загроза», «інформаційна війна», «інформаційний вплив», «інформаційна зброя».
6. Визначення критеріїв захищеної системи обробки інформації та постановка задач.
7. Поняття «загрози безпеки інформації», причини їх виникнення, їх види та особливості прояву.
8. Причини порушення інформаційної безпеки.
9. Класифікації загроз інформаційної системи.
10. Підходів щодо помилок в системах захисту інформації.
11. Засоби і способи захисту інформації.
12. Поняття і різновиди загроз інформаційній безпеці.
13. Інформаційне протиборство, інформаційна експансія, інформаційна війна, інформаційний тероризм.
14. Інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія.
15. Інформаційно-психологічна протидія, контроль каналів передачі інформації, система моніторингу та прогнозування негативних інформаційно-психологічних впливів.
16. Принципи інформаційної війни.
17. Логіка інформаційної війни.
18. Моделі інформаційної війни.
19. Різновиди інформаційних воєн.
20. Засоби, методи і технології інформаційних воєн.
21. Механізми реагування на загрози інформаційній безпеці.
22. Інтернет-ресурси як об’єкти загроз інформаційній безпеці підприємства.
23. Система моніторингу Інтернет-ресурсів.
24. Актори соціальних Інтернет-сервісів.
25. Контент і дані акторів соціальних Інтернет-сервісів.
26. Загрози інформаційній безпеці бізнесу у соціальних Інтернет-сервісах.
27. Підходи, принципи і методи забезпечення інформаційної безпеки.
28. Засоби забезпечення інформаційної безпеки.
29. Принципи формування політики інформаційної безпеки підприємства.
30. Організаційно-технічне забезпечення комп’ютерної безпеки.
31. Способи забезпечення інформаційної безпеки економічних систем.
32. Принципи забезпечення інформаційної безпеки на основі інженерно-технічного забезпечення.
33. Захист від комп’ютерних вірусів.
34. Електронний цифровий підпис.
35. Структура і задачі служби безпеки.
36. Захист інформації в Інтернеті.
37. Функції системи захисту інформації (ЗІ).
38. Матриця розподілу доступу.

39. Моделі інформаційної безпеки.
40. Види політики безпеки: виборча політика безпеки, повноважна політика безпеки.
41. Політика інформаційної безпеки бізнесу.
42. Модель розподілу інформаційних потоків.
43. Заходи захисту інформації: організаційно-технічні, адміністративні.
44. Стандарти по забезпеченню інформаційної безпеки бізнесу.
45. Вимоги до стандартів з інформаційної безпеки.
46. Форми представлення стандартів (документальна, усна).
47. Міжнародний стандарт безпеки ISO/IEC 17799.
48. Організаційні заходи підприємства щодо забезпечення безпеки.
49. Класифікація і управління ресурсами.
50. Безпека персоналу.
51. Управління комунікаціями і процесами.
52. Розробка і технічна підтримка інформаційних систем підприємства.
53. Управління інцидентами інформаційної безпеки.
54. Управління неперервністю бізнесу.
55. Державне регулювання інформаційної безпеки.
56. Інформаційна безпека та її місце в структурі національної безпеки України.
57. Загрози інформаційній безпеці України.
58. Національний інтерес в інформаційній сфері держави.
59. Стан та перспективи розвитку інформаційної безпеки держави.
60. Державна політика забезпечення інформаційної безпеки бізнесу в Україні/
61. Особливості реалізації комплексних систем захисту інформації.
62. Структура та функції державної системи забезпечення інформаційної безпеки.
63. Ліцензування в галузі забезпечення інформаційної безпеки.
64. Сертифікація засобів і методів неусвідомлюваного інформаційного впливу.
65. Експертиза інформаційної безпеки.
66. Контроль за забезпеченням інформаційної безпеки.
67. Загальні відомості та задачі комплексного захист інформації (КЗІ).
68. Стратегії комплексного захисту інформації.
69. Етапи побудови КЗІ для різних стратегій.
70. Безпека цінних інформаційних ресурсів.
71. Критерії цінності інформації.
72. Виявлення та документування конфіденційних відомостей.
73. Носії конфіденційних відомостей.
74. Цілі захисту інформації на підприємстві.
75. Розробка комплексної системи захисту інформації на підприємстві від IT Ресурс/
76. Правила управління інформаційною безпекою підприємства.
77. Етапи управління інформаційною безпекою підприємства.
78. Функції технологічного управління інформаційною безпекою.
79. Загальні положення з управління інформаційною безпекою.
80. Методи і засоби соціального інжинірингу.
81. Етапи розробка політики інформаційної безпеки.
82. Система фізичного захисту типові задачі та способи її реалізації.
83. Основні характеристики системи фізичного захисту.
84. Кількісний і якісний аналіз системи фізичного захисту.
85. Інженерно-технічні засоби охорони.
86. Сучасне підприємство: бізнес процеси, інформаційні технології (IT), інформаційна та кібернетична безпека.
87. Поняття про бізнес-процеси підприємства.
88. Інформаційні технології на підприємстві.
89. Правові аспекти інформаційної безпеки бізнесу.
90. Політика інформаційної безпеки (ІБ) бізнесу: цілі, завдання, зміст.
91. Часткові політики інформаційної безпеки.

92. Мета та завдання перед проектного етапу: підготовка вихідних даних та обстеження об’єкту інформаційної діяльності.

93. Класифікація та оцінка інформаційних ресурсів.

94. Задачі моделювання інформації.

95. Побудова моделі порушника ІБ.

96. Цілі та метод проведення зовнішнього контролю.

97. Контроль систем менеджменту інформаційної безпеки.

98. Принципи контролю інформаційної безпеки.

99. Права працівників на доступ до серверів і баз даних колективного використання.

100. Способи підтвердження входу кожного користувача (аутентифікація).

101. Принципи резервного копіювання даних.

102. Конфігурація і налаштування мережевих пристроїв, систем зберігання та передачі даних.

103. Робота антивірусного і антишпигунського програмного забезпечення, наявність ліцензії.

104. Теоретичні та практичні знання працівників підприємства про захист даних.

105. Контроль доступу.

106. Передумови розвитку послуг із забезпечення інформаційної безпеки та їх структура.

107. Інфраструктура публічних ключів.

108. Страхування інформаційних ризиків.

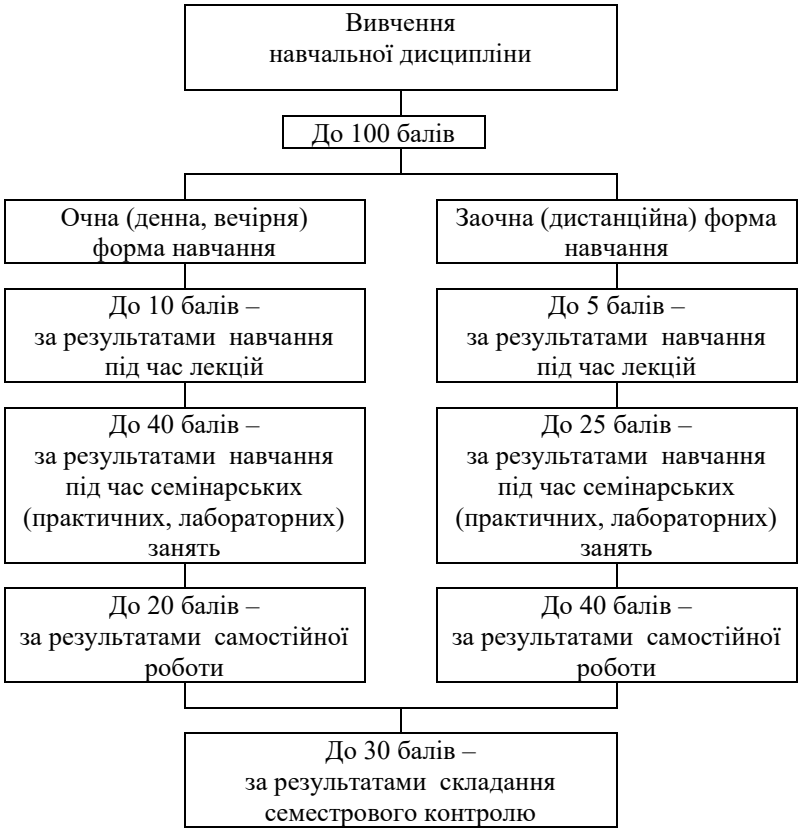
109. Страхування інформаційних ресурсів.

1.5.2. Структура екзаменаційного білета

1. Питання 1. Причини порушення інформаційної безпеки.
2. Тести. Виберіть позначення з правильною відповіддю:
    1. Інформаційна безпека забезпечується:
       А. Інформаційною діяльністю. Б. Інформаційним забезпеченням. В. Системою збереження інформаційної безпеки. Г. Мінімізація ризиків інформаційної діяльності.
    2. За ступенев вливу на інформаційну безпеку загрози поділяються:
       А. Активні. Б. Пасивні. В. Загальні. Г. Штучні.
    3. За розташуванням інормаційної безпеки загрози поділяються на:
       А. Внутрішні. Б.Зовнішні. В. Загальні. Г. Індивідуальні.
    4. За мотивами порушень інформаціційної безпеки виділяють порушників: А.Месник. Б.Технік. В. Кріт. Г. Агент.
    5. Загрози інформаційної безпеки за типом збитків поділяються на:
       А. Моральні. Б. Граничні. В. Матеріальні. Г. Персональні.
    6. ……
3. Завдання. Обсяг продукції випущеної за квартал (4 місяці) 130000 грн; витрати на придбання інформаційних ресурсів на протязі року склали 5300 грн. Визначити продуктивність інформації.

2. Схема нарахування балів

2.1. Нарахування балів студентам з навчальної дисципліни здійснюється відповідно до такої схеми:



2.2. Обсяг балів, здобутих слухачем під час лекцій з навчальної дисципліни, обчислюється у пропорційному співвідношенні кількості відвіданих лекцій і кількості лекцій, передбачених навчальним планом, і визначається згідно з додатком 1 2 до Положення про організацію освітнього процесу в Хмельницькому університеті управління та права (затвердженого 29 травня 2017 року, протокол № 14).

З навчальної дисципліни «Інформаційна безпека бізнесу» для студента денної форми навчання передбачено проведення 10 лекційних занять. Отже, студент може набрати під час лекцій таку кількість балів (табл. 2.1).

Таблиця 2.1

Розподіл балів для лекцій з навчальної дисципліни «Інформаційна безпека бізнесу»

№ з/п	Форма навчання	Кількість лекцій за планом	Кількість відвіданих лекцій/балів									
			1	2	3	4	5	6	7	8	9	10
1.	Денна	10	1,0	2,0	3,0	4,0	5,0	6,0	7,0	8,0	9,0	10,0

2.3. З навчальної дисципліни «Інформаційна безпека бізнесу» для студентів за спеціальністю 073 «Менеджмент» денної форми навчання передбачено проведення 11 семінарських занять.

За результатами семінарського заняття кожному слухачу до відповідного документа обліку успішності виставляється кількість балів від 0 до 5 числом, кратним 0,5, яку він отримав протягом заняття.

2.4. Обсяг балів за самостійну роботу з навчальної дисципліни «Інформаційна безпека бізнесу» для студентів розподіляється пропорційно за виконання наукової роботи та індивідуального завдання.

Критерії поточного оцінювання знань здобувачів наведені у п.4.3.8. Положення про організацію освітнього процесу у ХУУП, затверджене рішенням вченої ради від 05.07.2016 р.,

протокол №16, введене в дію наказом від 08.06.2016 р. № 359/16 (в редакції рішення вченої ради ХУУП імені Леоніда Юзькова від 28 серпня 2020 року, протокол № 1, з 01 вересня 2020 року, наказ ХУУП імені Леоніда Юзькова від 28 серпня 2020 року № 312/20)2.4. Обсяг балів за самостійну роботу з навчальної дисципліни «Інформаційна безпека бізнесу» для студентів розподіляється пропорційно за виконання наукової роботи та індивідуального завдання.

Індивідуальне завдання виконане за пропонованою темою та обирається студентом самостійно, оцінюються окремо та складає не більше 14 балів. Загалом за виконання самостійної роботи студент денної форми навчання може одержати максимально 20 балів.

Перерозподіл балів, в межах максимально можливої кількості їх одержання за виконану самостійну роботу, наведено в табл. 2.2.

Таблиця 2.2

Розподіл балів для самостійної роботи з навчальної дисципліни «Інформаційна безпека»

№ з/п	Алгоритм нарахування балів	Кількість балів	Разом балів
1	Максимальна кількість балів за індивідуальне завдання, виконане у вигляді наукової роботи (реферат)	6,0	6,0
2	Максимальна кількість балів за індивідуальне завдання, виконане у вигляді наукової роботи	14,0	14,0
	Усього балів		20,0

2.5. За семестровий контроль, що проводиться у формі семестрового екзамену з навчальної дисципліни «Інформаційна безпека бізнесу», студент денної форми навчання може максимально одержати 30 балів.

Перерозподіл балів, в межах максимально можливого одержання їх кількості за надані слухачами бакалаврату відповіді в усній та письмовій формі відповідно на питання, тестові завдання залікового білета та завдання, наведено в табл. 2.3.

Таблиця 2.3

Розподіл балів для семестрового контролю з навчальної дисципліни «Інформаційна безпека бізнесу»

№ з/п	Алгоритм нарахування балів	Номер питань залікового білета			Разом балів
		1	2	3	
1.	Максимальна кількість балів за усну відповідь на кожне питання залікового білета	5,0	-	-	5,0
2.	Максимальна кількість балів за письмову відповідь на тестові завдання	-	10,0	-	10,0
3.	Максимальна кількість балів за практичне завдання	-	-	15,0	15,0
	Усього балів	5,0	10,0	15,0	30,0

3. Рекомендовані джерела

Тема 1

1. Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/ show/2657-12#Text.
2. Закон України «Господарський кодекс України» від 16.01.2003 р. № 436-IУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15 .
3. Постанова КМУ «Про перелік відомостей, ще не становлять комерційної таємниці» від 09.08.1993 р. № 61. URL: https://zakon.rada.gov.ua/go/611-93-%D0BF .
4. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.
5. Кавун С.В. Інформаційна безпека: підручник. Харків : ХНЕУ. 2013. 213с. URL: http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/3068/1A1.%D0%92..pdf.
6. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання: посібник; за заг. ред. Д. В. Ланде. Київ-Одеса : Фенікс. 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf .
7. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).
8. Остапов С.Е. Технології захисту інформації: навчальний посібник. Чернівці: Видавничий дім «Родовід». 2014. 471с. URL:http://kist.ntu.edu.ua/textPhD/tzi.pdf.
9. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf? srsltid=AfmBOopJUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl.
10. Тихомиров О.О. Права людини: інформаційний вимір. Монографія. Одеса: Видавництво «Юридика». 2023. 304с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf
11. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія за заг. ред. В. Пилипчука. Київ - Одеса: Фенікс. 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus.

Тема 2

1. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-УІ. URL: https://zakon.rada.gov.ua/go/2297-17.
2. Закон України «Цивільний кодекс України» від 16.01.2003 р. № 435-IУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15.
3. Закон України «Господарський кодекс України» від 16.01.2003 р. № 436-IУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15 .
4. Постанова КМУ «Про перелік відомостей, ще не становлять комерційної таємниці» від 09.08.1993 р. № 61. URL: https://zakon.rada.gov.ua/go/611-93-%D0BF .
5. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.
6. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник . Харків: ХНУ імені В. Н. Каразіна. 2013. 632с. URL: https://old.karazin.ua/images/redactor/news/2013-03-01/Esin.pdf
7. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання: посібник; за заг. ред. Д. В. Ланде. Київ-Одеса : Фенікс. 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf .
8. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).
9. Остапов С.Е. Технології захисту інформації: навчальний посібник. Чернівці: Видавничий дім «Родовід». 2014. 471с. URL:http://kist.ntu.edu.ua/textPhD/tzi.pdf.

10. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf? srsltid=AfmBOopJUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl.

11. Тихомиров О.О. Права людини: інформаційний вимір. Монографія. Одеса: Видавництво «Юридика». 2023. 304с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf

12. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія за заг. ред. В. Пилипчука. Київ - Одеса: Фенікс. 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus.

Тема 3

1. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.

2. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. ун- т внутріш. справ, 2020. 144 с. URL: https://vstup.htek.com.ua/wp-content/uploads/2024/10/34.1-Grebenyuk.pdf

3. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник . Харків: ХНУ імені В. Н. Каразіна. 2013. 632с. URL: https://old.karazin.ua/images/redactor/news/2013-03-01/Esin.pdf.

4. Іжевський П., Самарічева Т. А., Кудельський В.Е. Цифрові інновації в розвитку малого бізнесу. *Економіка та суспільство.* 2024. № 63. URL: https://economyandsociety.in.ua/index.php/journal/issue/view/63.

5. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання: посібник; за заг. ред. Д. В. Ланде. Київ-Одеса : Фенікс. 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf .

6. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).

7. Остапов С.Е. Технології захисту інформації: навчальний посібник. Чернівці: Видавничий дім «Родовід». 2014. 471с. URL:http://kist.ntu.edu.ua/textPhD/tzi.pdf.

8. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf? srsltid=AfmBOopJUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl.

9. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія за заг. ред. В. Пилипчука. Київ - Одеса: Фенікс. 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus.

Тема 4

1. Закон України «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-УІ. URL: https://zakon.rada.gov.ua/laws/show/2939-17.

2. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-УІ. URL: https://zakon.rada.gov.ua/go/2297-17.

3. Закон України «Цивільний кодекс України» від 16.01.2003 р. № 435-ІУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15.

4. Закон України «Господарський кодекс України» від 16.01.2003 р. № 436-ІУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15.

5. Постанова КМУ «Про перелік відомостей, ще не становлять комерційної таємниці» від 09.08.1993 р. № 61. URL: https://zakon.rada.gov.ua/go/611-93-%D0BF .

6. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.

7. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник . Харків: ХНУ імені В. Н. Каразіна. 2013. 632с. URL: https://old.karazin.ua/images/redactor/news/2013-03-01/Esin.pdf

8. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).

9. Остапов С.Е. Технології захисту інформації: навчальний посібник. Чернівці: Видавничий дім «Родовід». 2014. 471с. URL:http://kist.ntu.edu.ua/textPhD/tzi.pdf.

10. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf? srsltid=AfmBOop JUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl

11. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія за заг. ред. В. Пилипчука. Київ - Одеса: Фенікс. 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus.

Тема 5

1. Закон України «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-УІ. URL: https://zakon.rada.gov.ua/laws/show/2939-17.

2. Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/ show/2657-12#Text.

3. Закон України «Цивільний кодекс України» від 16.01.2003 р. № 435-ІУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15.

4. Закон України «Господарський кодекс України» від 16.01.2003 р. № 436-ІУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15 .

5. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.

6. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. ун- т внутріш. справ, 2020. 144 с. URL: https://vstup.htek.com.ua/wp-content/uploads/2024/10/34.1-Grebenyuk.pdf.

7. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання: посібник; за заг. ред. Д. В. Ланде. Київ-Одеса : Фенікс. 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf.

8. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).

9. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AfmBOop JUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl.

10. Тихомиров О.О. Права людини: інформаційний вимір. Монографія. Одеса: Видавництво «Юридика». 2023. 304с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf.

Тема 6

1. Постанова КМУ «Про перелік відомостей, ще не становлять комерційної таємниці» від 09.08.1993 р. № 61. URL: https://zakon.rada.gov.ua/go/611-93-%D0BF .

2. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.

3. Кавун С.В. Інформаційна безпека: підручник. Харків : ХНЕУ. 2013. 213с. URL: http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/3068/1A1.%D0%92..pdf.

4. Кудельський В.Е.Українські стартапи в умовах війни. Міжнародний науковий періодичний журнал, що рецензується *«ScientificWorldJournal»* 2024. Випуск №25. (Болгарія, Copernicus, GScholar). С.172-180.

5. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання: посібник; за заг. ред. Д. В. Ланде. Київ-Одеса : Фенікс. 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf .

6. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).

7. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AfmBOopJUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl

8. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія за заг. ред. В. Пилипчука. Київ - Одеса: Фенікс. 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus.

Тема 7

1. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf..

2. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. ун- т внутріш. справ, 2020. 144 с. URL: https://vstup.htek.com.ua/wp-content/uploads/2024/10/34.1-Grebenyuk.pdf

3. Кавун С.В. Інформаційна безпека: підручник. Харків : ХНЕУ. 2013. 213с. URL: http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/3068/1A1.%D0%92..pdf.

4. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання: посібник; за заг. ред. Д. В. Ланде. Київ-Одеса : Фенікс. 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf .

5. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).

6. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AfmBOopJUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl.

7. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія за заг. ред. В. Пилипчука. Київ - Одеса: Фенікс. 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus.

Тема 8

1. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-УІ. URL: https://zakon.rada.gov.ua/go/2297-17.

2. Закон України «Цивільний кодекс України» від 16.01.2003 р. № 435-ІУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15.

3. Закон України «Господарський кодекс України» від 16.01.2003 р. № 436-ІУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15 .

4. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.

5. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. ун- т внутріш. справ, 2020. 144 с. URL: https://vstup.htek.com.ua/wp-content/uploads/2024/10/34.1-Grebenyuk.pdf.

6. Кудельський В.Е. Виклик інформаційного суспільства - маніпуляція свідомістю. THEORETICAL METHODS OF RESEARCH OF THE LATEST PROBLEMS *Abstracts of XXI International Scientific and Practical Conference Prague*, Czech Republic (May 27-29, 2024). с.290-292.

7. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання: посібник; за заг. ред. Д. В. Ланде. Київ-Одеса : Фенікс. 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf .

8. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).

9. Остапов С.Е. Технології захисту інформації: навчальний посібник. Чернівці: Видавничий дім «Родовід». 2014. 471с. URL:http://kist.ntu.edu.ua/textPhD/tzi.pdf.

10. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AfmBOopJUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl.

11. Тихомиров О.О. Права людини: інформаційний вимір. Монографія. Одеса: Видавництво «Юридика». 2023. 304с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf.

12. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія за заг. ред. В. Пилипчука. Київ - Одеса: Фенікс. 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus.

Тема 9.

1. Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/ show/2657-12#Text.

2. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-УІ. URL: https://zakon.rada.gov.ua/go/2297-17.

3. Закон України «Цивільний кодекс України» від 16.01.2003 р. № 435-ІУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15.

4. Закон України «Господарський кодекс України» від 16.01.2003 р. № 436-ІУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15 .

5. Постанова КМУ «Про перелік відомостей, ще не становлять комерційної таємниці» від 09.08.1993 р. № 61. URL: https://zakon.rada.gov.ua/go/611-93-%D0BF .

6. Бобало Ю. Я. Інформаційна безпека : навчальний посібник. Львів: Видавництво Львівської політехніки. 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf.

7. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. ун- т внутріш. справ, 2020. 144 с. URL: https://vstup.htek.com.ua/wp-content/uploads/2024/10/34.1-Grebenyuk.pdf.

8. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник. Київ. 2018. 105 с. URL:http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne).

9. Остапов С.Е. Технології захисту інформації: навчальний посібник. Чернівці: Видавничий дім «Родовід». 2014. 471с. URL:http://kist.ntu.edu.ua/textPhD/tzi.pdf.

10. Остроухов В. В. Інформаційна безпека: підручник . Київ. Видавництво Ліра-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf? srsltid=AfmBOopJUt4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl.

11. Тихомиров О.О. Права людини: інформаційний вимір. Монографія. Одеса: Видавництво «Юридика». 2023. 304с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf

12. Уханова Н. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія за заг. ред. В. Пилипчука. Київ - Одеса: Фенікс. 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus.

4. Інформаційні ресурси в Інтернеті

1. Офіційний сайт Президента України. URL: http://www.president.gov.ua/.
2. Офіційний сайт Верховної Ради України. URL: http://www.zakon.rada.gov.ua/.
3. Офіційний сайт Урядового порталу. URL: http://www.kmu.gov.ua/.
4. Офіційний сайт Міністерства освіти і науки України URL: http://mon.gov.ua.
5. Офіційний сайт Національної бібліотеки України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua/.
6. Пошукова система Google Scholar URL: http://scholar.google.com.ua/.
7. Пошукова система Scopus URL: http://www.scopus.com/home.url.