ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ЗАТВЕРДЖЕНО
Рішення вченої ради університету
31 січня 2024 року,
протокол № 9.
Ректор, голова вченої ради університету,

доктор юридичних наук, професор

_____ Олег ОМЕЛЬЧУК

31 січня 2024 року

м.п.

РОБОЧА ПРОГРАМА
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

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

ПОГОДЖЕНО

Рішення методичної ради університету
23 січня 2024 року, протокол № 4.
Перша проректорка, голова методичної ради, кандидатка наук з державного управління, доцентка
_____ Ірина КОВТУН
23 січня 2024 року

Обліковий обсяг 0,62 ум.др.арк.

ЗМІСТ

1. Опис навчальної дисципліни

1. Шифр і назва галузі знань	–	07 Управління та адміністрування
2. Код і назва спеціальності	–	073 Менеджмент
3. Назва спеціалізації	–	спеціалізація не передбачена
4. Назва дисципліни	–	Інформаційна безпека бізнесу
5. Тип дисципліни	–	Обов’язкова
6. Код дисципліни	–	ППО 13
7. Освітній рівень, на якому вивчається дисципліна	–	перший
8. Ступінь вищої освіти, що здобувається	–	бакалавр
9. Курс / рік навчання	–	другий
10. Семестр	–	четвертий
11. Обсяг вивчення дисципліни:		
1) загальний обсяг (кредитів ЄКТС / годин)	–	3,5 / 105
2) денна форма навчання:		
аудиторні заняття (годин)	–	42
% від загального обсягу	–	40,0
лекційні заняття (годин)	–	20
% від обсягу аудиторних годин	–	48,0
семінарські заняття (годин)	–	22
% від обсягу аудиторних годин	–	52,0
самостійна робота (годин)	–	63
% від загального обсягу	–	60
тижневих годин:		
аудиторних занять	–	3
самостійної роботи	–	3,5
3) заочна форма навчання:		
аудиторні заняття (годин)	–	14
% від загального обсягу	–	13
лекційні заняття (годин)	–	6
% від обсягу аудиторних годин	–	43
семінарські заняття (годин)	–	8
% від обсягу аудиторних годин	–	57

	самостійна робота (годин)	–	91
	% від загального обсягу	–	87
	тижневих годин:		
	аудиторних занять	–	2,33
	самостійної роботи	–	5,05
12.	Форма семестрового контролю	–	екзамен
13.	Місце дисципліни в логічній схемі:		
	1) супутні дисципліни	–	ППО 6 «Інформаційні технології в менеджменті»
	2) наступні дисципліни	–	ППО 15. Операційний менеджмент ППО 19. HR-менеджмент. ППО 26. Економічне обґрунтування управлінських рішень
14.	Мова вивчення дисципліни	–	українська.

2. Заплановані результати навчання

Програмні компетентності, які здобуваються під час вивчення навчальної дисципліни	**Загальні компетентності** **ЗК 08.** Навички використання інформаційних і комунікаційних технологій**.** **ЗК 15.** Здатність діяти на основі етичних міркувань (мотивів). **Спеціальні компетентності** **СК 1.** Здатність визначати та описувати властивості і характеристики бізнес-середовища та бізнес-структур. **СК 2.** Здатність аналізувати результати діяльності бізнес-структур, зіставляти їх з факторами впливу зовнішнього та внутрішнього середовища. **СК 3.** Здатність визначати перспективи розвитку організації. **СК 6.** Здатність діяти соціально-відповідально і свідомо. **СК 11.** Здатність створювати та організовувати ефективні комунікації в процесі управління **СК 12.** Здатність аналізувати й структурувати проблеми організації, формувати обґрунтовані управлінські рішення.
Результати навчання	**ПР 5.** Описувати зміст функціональних сфер діяльності організації. **ПР 6.** Виявляти навички пошуку, збирання та аналізу інформації, розрахунку показників для обґрунтування управлінських рішень. **ПР 12.** Оцінювати правові, соціальні та економічні наслідки функціонування організації.

Після завершення вивчення дисципліни здобувач повинен продемонструвати такі результати навчання:	
1. Знання	
1.1)	відтворювати передумови еволюції інформаційної безпеки бізнесу;
1.2)	називати етапи розвитку інформаційної безпеки бізнесу;
1.3)	характеризувати управлінську інформацію та її вплив на розвиток бізнесу;
1.4)	встановлювати інформаційний зв'язок між людськими відносинами та системою управління;
1.5)	описувати інформаційні підходи до управління безпекою бізнесу.
2. Розуміння	
2.1)	пояснювати зміст основних термінів інформаційної безпеки бізнесу;
2.2)	класифікувати загрози інформаційної безпеки;
2.3)	пояснювати особливості розвитку системи управління інформаційною безпекою

	бізнесу;
2.4)	пояснювати теоретичні засади інформаційної безпеки бізнесу;
2.5)	з’ясовувати базові аспекти лідерських якостей керівника в управлінні інформаційною безпекою підприємства.
	3. Застосування знань
3.1)	будувати ефективну систему управління інформаційною безпекою;
3.2)	системно аналізувати діяльність підприємства в інформаційній безпеці;
3.3)	будувати організаційні структуру інформаційної безпеки бізнесу;
3.4)	з’ясовувати особливості бізнесу в інформаційній безпеці
3.5)	розробляти програми управління інформаційною безпекою.
	4. Аналіз
4.1)	аналізувати умови виникнення та розвитку теорії управління інформаційною безпекою бізнесу;
4.2)	системно аналізувати діяльність підприємства в інформаційній безпеці;
4.3)	здійснювати розподіл завдань між виконавцями;
4.4)	спів ставляти технології розробки різних видів інформації;
4.5)	визначати ефективність системи комунікації в інформаційній безпеці.
	5. Синтез
5.1)	проектувати систему комунікацій в управлінні інформаційною безпекою;
5.2)	узагальнювати сучасні підходи до інформаційної безпеки бізнесу;
5.3)	установлювати інформаційний зв'язок між структурними підрозділами підприємства;
5.4)	спів ставляти очікувані результати затрат з орієнтацією на досягнення необхідного результату;
5.5)	інтегрувати сучасні підходи в практику управління інформаційною безпекою бізнесі.
	6. Оцінювання
6.1)	оцінювати ефективність менеджерських якостей в управлінні інформаційною безпекою;
6.2)	розробляти сучасні системи контролю інформаційними потоками;
6.3)	оцінити ефективність системи управління інформаційною безпекою бізнесу;
6.4)	пропонувати новітні системи ефективного захисту інформації
6.5)	оцінити вплив системи управління інформаційною безпекою з урахуванням галузевих особливостей.
	7. Створення (творчість)
7.1)	створювати сучасні системи мотивації праці при управлінні інформаційною безпекою підприємства;
7.2)	розробляти сучасні системи контролю за дотримання інформаційної безпеки;
7.3)	проектувати системи управління інформаційною безпекою бізнесу із врахуванням сучасних технологій;
7.4)	пропонувати новітні системи ефективного захисту інформаційної безпеки;
7.5)	пропонувати власні варіанти системи управлінням інформаційною безпекою бізнесу з урахуванням галузевих особливостей.

3. Програма навчальної дисципліни

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

Інформаційна сфера, інформаційна безпека, національна безпека, кібернетична безпека. Інформаційне суспільство. Підходи до дослідження інформаційної безпеки. Система забезпечення інформаційної безпеки. Сутність категорій: «інформаційна безпека», «політика безпеки», «інформаційна загроза», «інформаційна війна», «інформаційний вплив», «інформаційна зброя». Визначення критеріїв захищеної системи обробки інформації та постановка задач.

Тема 2. **Інформаційні загрози бізнесу та їх види.**

Поняття «загрози безпеки інформації», причини їх виникнення, їх види та особливості прояву. Причини порушення інформаційної безпеки. Класифікації загроз інформаційної системи. Підходів щодо помилок в системах захисту інформації. Засоби і способи захисту інформації. Поняття і різновиди загроз інформаційній безпеці. Інформаційне протиборство, інформаційна експансія, інформаційна війна, інформаційний тероризм. Інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія. Інформаційно-психологічна протидія, контроль каналів передачі інформації, система моніторингу та прогнозування негативних інформаційно-психологічних впливів. Принципи інформаційної війни. Логіка інформаційної війни. Моделі інформаційної війни. Різновиди інформаційних воєн. Засоби, методи і технології інформаційних воєн. Механізми реагування на загрози інформаційній безпеці. Інтернет-ресурси як об'єкти загроз інформаційній безпеці підприємства. Система моніторингу Інтернет-ресурсів. Актори соціальних Інтернет-сервісів. Контент і дані акторів соціальних Інтернет-сервісів. Загрози інформаційній безпеці бізнесу у соціальних Інтернет-сервісах.

Тема 3. **Принципи побудови системи інформаційної безпеки.**

Підходи, принципи і методи забезпечення інформаційної безпеки. Засоби забезпечення інформаційної безпеки. Принципи формування політики інформаційної безпеки підприємства. Організаційно-технічне забезпечення комп'ютерної безпеки. Способи забезпечення інформаційної безпеки економічних систем. Принципи забезпечення інформаційної безпеки на основі інженерно-технічного забезпечення. Захист від комп'ютерних вірусів. Електронний цифровий підпис. Структура і задачі служби безпеки. Захист інформації в Інтернеті.

Тема 4. **Системи та моделі захисту інформації.**

Функції системи захисту інформації (ЗІ). Матриця розподілу доступу. Моделі інформаційної безпеки. Види політики безпеки: виборча політика безпеки, повноважна політика безпеки. Політика інформаційної безпеки бізнесу. Модель розподілу інформаційних потоків. Заходи захисту інформації: організаційно-технічні, адміністративні.

Стандарти по забезпеченню інформаційної безпеки бізнесу. Вимоги до стандартів з інформаційної безпеки. Форми представлення стандартів (документальна, усна). Міжнародний стандарт безпеки ISO/IEC 17799. Організаційні заходи підприємства щодо забезпечення безпеки. Класифікація і управління ресурсами. Безпека персоналу. Управління комунікаціями та інформаційними процесами. Розробка і технічна підтримка інформаційних систем підприємства. Управління інцидентами інформаційної безпеки. Управління неперервністю бізнесу.

Тема 5. Д**ержавні інформаційні ресурси.**

Державне регулювання інформаційної безпеки. Інформаційна безпека та її місце в структурі національної безпеки України. Загрози інформаційній безпеці України. Національний інтерес в інформаційній сфері держави. Стан та перспективи розвитку інформаційної безпеки держави. Державна політика забезпечення інформаційної безпеки бізнесу в Україні

Особливості реалізації комплексних систем захисту інформації. Структура та функції державної системи забезпечення інформаційної безпеки. Ліцензування в галузі забезпечення інформаційної безпеки. Сертифікація засобів і методів неусвідомлюваного інформаційного впливу. Експертиза інформаційної безпеки. Контроль за забезпеченням інформаційної безпеки.

Тема 6. **Конфіденційність та комплексний захист інформації.**

Загальні відомості та задачі комплексного захист інформації (КЗІ). Стратегії комплексного захисту інформації. Етапи побудови КЗІ для різних стратегій. Безпека цінних інформаційних ресурсів. Критерії цінності інформації. Виявлення та документування конфіденційних відомостей. Носії конфіденційних відомостей. Цілі захисту інформації на підприємстві. Розробка комплексної системи захисту інформації на підприємстві від IT Ресурс

Тема 7. **Системи управління інформаційною безпекою бізнесу.**

Правила управління інформаційною безпекою підприємства. Етапи управління інформаційною безпекою підприємства. Функції технологічного управління інформаційною безпекою. Загальні положення з управління інформаційною безпекою. Методи і засоби

соціального інжинірингу. Етапи розробка політики інформаційної безпеки. Система фізичного захисту типові задачі та способи її реалізації. Основні характеристики системи фізичного захисту. Кількісний і якісний аналіз системи фізичного захисту. Інженерно-технічні засоби охорони.

Тема 8. **Політика інформаційної безпеки підприємства.**

Сучасне підприємство: бізнес процеси, інформаційні технології (ІТ), інформаційна та кібернетична безпека. Інформаційні технології на підприємстві. Правові аспекти інформаційної безпеки бізнесу. Політика інформаційної безпеки (ІБ) бізнесу: цілі, завдання, зміст. Часткові політики інформаційної безпеки. Мета та завдання перед проектного етапу: підготовка вихідних даних та обстеження об'єкту інформаційної діяльності. Класифікація та оцінка інформаційних ресурсів. Задачі моделювання інформації. Побудова моделі порушника ІБ.

Тема 9. **Контроль стану інформаційної безпеки на підприємстві.**

Цілі та метод проведення зовнішнього контролю. Контроль систем менеджменту інформаційної безпеки. Принципи контролю інформаційної безпеки. Права працівників на доступ до серверів і баз даних колективного використання. Способи підтвердження входу кожного користувача (аутентифікація). Принципи резервного копіювання даних. Конфігурація і налаштування мережевих пристроїв, систем зберігання та передачі даних. Робота антивірусного і антишпигунського програмного забезпечення, наявність ліцензії. Теоретичні та практичні знання працівників підприємства про захист даних. Контроль доступу.

Передумови розвитку послуг із забезпечення інформаційної безпеки та їх структура. Інфраструктура публічних ключів. Страхування інформаційних ризиків. Основи страхування інформаційних ресурсів.

4. Структура вивчення навчальної дисципліни

4.1. 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

4.2. Аудиторні заняття

4.2.1. Аудиторні заняття (лекції, семінарські заняття) проводяться згідно з темами та обсягом годин, передбачених тематичним планом.

4.2.2. Плани лекцій з передбачених тематичним планом тем визначаються в підрозділі 1.2 навчально-методичних матеріалів з дисципліни.

4.2.3. Плани семінарських занять з передбачених тематичним планом тем, засоби поточного контролю знань та методичні рекомендації для підготовки до занять визначаються в підрозділі 1.3 навчально-методичних матеріалів з дисципліни.

4.3. Самостійна робота студентів

4.3.1. Самостійна робота студентів денної форми навчання включає завдання до окремих тем та індивідуальні завдання.

4.3.2. Завдання для самостійної роботи студентів та методичні рекомендації до їх виконання визначаються в підрозділі 1.4 навчально-методичних матеріалів з дисципліни.

4.3.3. Студенти денної форми навчання виконують індивідуальні завдання у формі рефератів та індивідуальних науково-дослідних завдань.

4.3.4. Тематика індивідуальних завдань та методичні рекомендації до їх виконання визначаються в підрозділі 1.5 навчально-методичних матеріалів з дисципліни.

4.3.5. Індивідуальні завдання виконуються в межах часу, визначеного для самостійної роботи студентів, та оцінюються частиною визначених в розділі 6 цієї програми кількості балів, виділених для самостійної роботи.

5. Методи навчання та контролю

Під час лекційних занять застосовуються:

1) традиційний усний виклад змісту теми;

2) слайдова презентація.

На семінарських та практичних заняттях застосовуються:

- дискусійне обговорення проблемних питань;
- вирішення розрахункових та ситуаційних завдань;
- повідомлення про виконання індивідуальних завдань.

Поточний контроль знань студентів з навчальної дисципліни проводиться у формах:

1) усне або тестове опитування у Гугл-формі щодо засвоєння матеріалу;

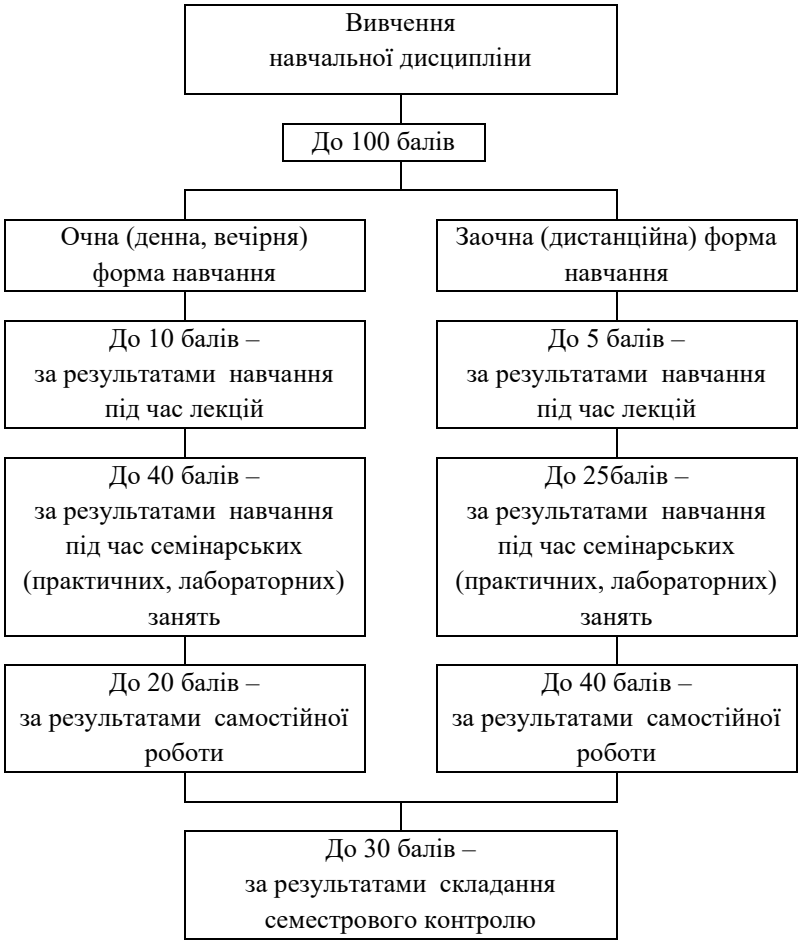
2) усне або тестове опитування у Гугл-формі на семінарських заняттях усне або письмове (у тому числі тестове) опитування на семінарських заняттях;

3) виконання поточних контрольних робіт у формі тестування.

Підсумковий семестровий контроль проводиться у формі екзамену. Структура екзаменаційного білету включає 1 теоретичне питання, 20 тестових завдань та практичну ситуацію.

6. Схема нарахування балів

6.1. Нарахування студентам балів за результатами навчання здійснюється за схемою, наведеною на рис.



6.2. Обсяг балів, здобутих студентом під час лекцій, семінарських занять, самостійної роботи студентів та виконання індивідуальних завдань визначаються в навчально-методичних матеріалах з цієї дисципліни.

7. Рекомендовані література

7.1. Нормативно-правові акти

1. Господарський кодекс України. Закон України від 16.01.2003 р. № 436-IУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15 .

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

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

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

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

6. Цивільний кодекс України. Закон України від 16.01.2003 р. № 435-IУ. URL: https://zakon.rada.gov.ua/ laws/show/436-15.

7.2. Монографії

7. 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.

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.

7.3. Підручники та навчальні посібники

9. 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.

10. 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

11. 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

12. 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.

13. 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 .

14. 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).

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

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

7.4. Допоміжні джерела

17. Арістова І.В., Баранов О.А., Дзьобань О.П. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології. За заг. ред. проф. К.І. Бєлякова. Монографія. Київ: КВІЦ, 2019. 344 с. (Розділ 4. Характеристика

галузевих видів юридичної відповідальності за інформаційні делікти.) URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf .

18. Ахрамович В. М., Амелькін С. В. Система захисту інформації приватного підприємства. Організація служби захисту інформації приватного підприємства. *Сучасний захист інформації*.2019.№1(37).С.21–27.

19. Баранов О. А. Соціальні та цифрові трансформації: нова парадигма кібербезпеки. Монографія. Київ: 2021. 86 с. URL: https://ippi.org.ua/sotsialni-ta-tsifrovi-transformatsii-nova-paradigma-kiberbezpeki.

20. Баранов О. А. Трансформація: соціальна & цифрова & правова: монографія у 3-х т. Т. 1. Порятунок цивілізації: економіка результату. Одеса: Видавничий дім «Гельветика», 2022. 272 с. URL: https://ippi.org.ua/transformatsiya-sotsialna-tsifrova-pravova.

21. Варічева Р. В. Захист інформаційних даних управлінського обліку: організаційно-кадрова складова. *Проблеми і перспективи економіки та управління.* 2015. № 3(3). С. 308–312.

22. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань». Монографія. Київ-Одеса : Фенікс. 2021. 176 с. URL: http://ippi.org.ua/kiberbezpeka-%C2%ABsuspilstva-znan%C2%BB.

23. 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.

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

25. 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.

26. Легенчук С. Ф., Назаренко Т. П., Царук І. М. Принципи захисту даних у системі обліку: управлінські аспекти. *Економіка, управління та адміністрування.* 2021. № 2(96). С. 61–69.

27. Національна безпека: світоглядні та теоретико-методологічні засади: монографія. за заг. ред. О. П. Дзьобаня. Харків: Право, 2021. 776 с. URL: http://ippi.org.ua/natsionalna- bezpeka-svitoglyadni-ta-teoretiko-metodologichni-zasadi.

28. Осмятченко В. О., Склярук І. П. Сучасні ІТ-рішення для обліку та управління бізнесом. *Підприємництво і торгівля.* 2022. № 34. С. 41–46. URL: http://journals-lute.lviv.ua/index.php/pidpr-torgi/article/view/1219/1149.

29. Скрипник С. В., Франчук І. Б., Шепель І.В. Особливості автоматизації обліку підприємств в сучасних умовах. *Економіка та держава*. 2020. № 10. С. 39–45. URL: http://www.economy.in.ua/pdf/10_2020/9.pdf.

30. Смотрич Д.В. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету.* Серія ПРАВО. Випуск 77: частина 2. 2023. С. 121-126. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/22-2.pdf.

31. Шишкова Н. Л. Засоби підвищення керованості безпекою облікової інформації. *Економічний вісник.* 2016. № 3. С. 119–127. URL: http://nbuv.gov.ua/UJRN/evngu_2016_3_17.

32. Ясінська А.І. Проблеми та перспективи електронного документообігу в умовах цифрової трансформації. *Молодий вчений*. 2022. № 11(111). С. 128–134. URL: https://molodyivchenyi.ua/index.php/journal/article/view/5653/5531

8. 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.