



**ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ**

Кафедра менеджменту, економіки, статистики та цифрових технологій

ЗАТВЕРДЖЕНО

Рішення кафедри

**менеджменту, економіка, статистики та
цифрових технологій**

27 серпня 2024 року,

протокол № 1 .

**Завідувачка кафедри, доцентка, кандидатка
економічних наук, доцентка**

**_____ Наталія ЗАХАРКЕВИЧ
27 серпня 2024 року**

СИЛАБУС

навчальної дисципліни

«Інформаційна безпека бізнесу»

для підготовки на першому (освітньому) рівні

здобувачів ступеня бакалавра

із спеціальності 073 Менеджмент

галузі знань 07 Управління та адміністрування

заочної форми навчання

РОЗРОБНИК

**Доцент кафедри менеджменту, економіки,
статистики та цифрових технологій
кандидат економічних наук, доцент**

**_____ Віталій КУДЕЛЬСЬКИЙ
26 серпня 2024 року**

ПОГОДЖЕНО

**Деканеса факультету управління та
економіки, кандидатка економічних наук,
доцентка**

**_____ Тетяна ТЕРЕЩЕНКО
28 серпня 2024 року**

Назва навчальної дисципліни	«Інформаційна безпека бізнесу»
Викладач	Лекції, семінарські заняття, консультації: Кудельський Віталій Едуардович (https://univer.km.ua/profile/kudelskyi-vitaliy-eduardovych), доцент кафедри менеджменту, економіки, статистики та цифрових технологій кандидат економічних наук, доцент
Контактна інформація та науковий профіль викладача	Електронна адреса v_kydelskyi@univer.km.ua Профіль у соціальних мережах: https://www.facebook.com/profile.php?id=100042062438545 ORCID: https://orcid.org/0000-0002-7252-6533 GoogleScholar: https://scholar.google.com/citations?user=Qjx5pBMAAAAJ
Інформаційні ресурси	Код для приєднання в Google клас «Інформаційна безпека бізнесу»: cdvdjor Електронна бібліотека: http://elibrary.univer.km.ua/index.php
Консультації	Офлайн консультації: навчальний корпус №2, провулок Володимирський 8/1 кафедра менеджменту, економіки, статистики та цифрових технологій (ауд. 101) Кудельський Віталій Едуардович: середа з 15.00 до 18.00; Онлайн консультації: за попередньою домовленістю електронною поштою у робочі дні з 9.00 до 17.00 Консультації до екзамену: напередодні екзамену згідно із затвердженим розкладом.

Опис навчальної дисципліни

Цілі та особливості навчальної дисципліни	Предметом вивчення навчальної дисципліни є основні терміни, поняття та визначення в галузі безпеки інформаційних систем в бізнесі; головні завдання безпеки інформаційної безпеки; моделі загроз інформації, механізми та сервіси її захисту; криптографічні методи забезпечення конфіденційності, цілісності в інформаційних системах суб'єктів господарювання; аутентифікації суб'єктів та об'єктів інформаційної діяльності в інформаційних системах; електронний цифровий підпис (ЕЦП). Метою дисципліни «Інформаційна безпека бізнесу» є систематизація знань студентів в галузі інформаційної безпеки економічних суб'єктів різних форм власності та вивчення прикладних особливостей застосування методів та засобів захисту інформації.
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 (фахові, предметні) 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 бізнесу. СК 6. Здатність діяти соціально-відповідально і свідомо. СК 11. Здатність створювати та організовувати ефективні комунікації в процесі управління бізнесом. СК 12. Здатність аналізувати й структурувати проблеми організації, формувати обґрунтовані управлінські рішення.
Програмні 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.			
Місце дисципліни в логічній схемі	Обов'язкова навчальна дисципліна, курс навчання – другий-третій, семестр – четвертий-п'ятий. Для успішного опанування дисципліни здобувачі повинні володіти знаннями з таких навчальних дисциплін, як ЗПО 4 «Інформаційні системи та технології», ППО 6 «Інформаційні технології в менеджменті», ППО 9 «Менеджмент». Знання цієї навчальної дисципліни слугуватимуть базою для подальшого вивчення дисциплін (освітніх компонентів): ППО 15. Операційний менеджмент, ППО 19. HR-менеджмент, ППО 26. Економічне обґрунтування управлінських рішень, Виробнича практика 2.			
Обсяг навчальної дисципліни	3,5 кредитів ЄКТС / 105 годин, у тому числі, лекційних - 8 годин; семінарських – 6. самостійної роботи - 91 години,.			
Форма навчання	Заочна			
Тижневе навантаження	2,33 год. аудиторних занять згідно з розкладом, 5,05 год. самостійної роботи на міжсесійний період			
Мова викладання	Українська			
Формат вивчення навчальної дисципліни	Онлайн: лекції, семінарських занять, консультації, екзамен. Для осіб із особливими освітніми потребами, у разі необхідності, розробляється індивідуальний формат вивчення навчальної дисципліни.			
Необхідне обладнання	Комп'ютер.			
Зміст навчальної дисципліни та організація поточного та підсумкового контролю	Години (лек. / сем. / СРС)	Тема	Методи навчання та форми поточного контролю	Максимальна кількість балів
	1/1/10	Тема 1. Інформаційна безпека: підходи до концептуалізації та індикатори визначення	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль.	Лекція – 0,83 Семінарське заняття – 2,5 СРС – 1,66
	1/1/11	Тема 2. Інформаційні загрози бізнесу та їх види.	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль	Лекція –0,83 Семінарське заняття -2,5 СРС – 1,66
	-/1/10	Тема 3. Принципи побудови системи інформаційної безпеки.	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль	Лекція – Семінарське заняття -2,5 СРС – 1,66
	1/1/10	Тема 4. Системи та моделі захисту інформації.	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль	Лекція –0,83 Семінарське заняття -2,5 СРС – 1,66

	1/-/10	Тема 5. Державні інформаційні ресурси.	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль	Лекція – 0,83 Семінарське заняття - СРС – 1,66
	1/1/10	Тема 6. Конфіденційність документу та комплексний захист інформації.	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль	Лекція – 0,83 Семінарське заняття – 2,5 СРС – 1,66
	1/1/10	Тема 7. Системи управління інформаційною безпекою бізнесу.	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль	Лекція – 0,85 Семінарське заняття – 2,5 СРС – 1,66
	-/1/10	Тема 8. Політика інформаційної безпеки підприємства.	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль	Лекція – Семінарське заняття -2,5 СРС – 1,66
	-/1/10	Тема 9. Контроль стану інформаційної безпеки на підприємстві.	Реферативні повідомлення, дискусійне обговорення проблемних питань, індивідуальні завдання, презентації, тестовий контроль.	Лекція – Семінарське заняття -2,5 СРС – 1,66
			індивідуальне завдання	25
Рекомендовані джерела для вивчення навчальної дисципліни	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. 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 .			
	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 Ліпа-К. 2021. 412 с. URL:https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsId=AfmBOopJU4tK16kgRXX0Lg03QIoD2DIyajXd8zmRtZ4VtZ5sYYnybyl. 9. 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. 10. 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/problem-pratidii-negativnim-informatsiynim-vplivam-ta-zakhistu-informatsiynoi-bezpeki-lyudini-i-sus.
Методи навчання та форми поточного контролю	Методи навчання та форми поточного контролю, порядок накопичення балів визначені у робочій програмі та навчально-методичних матеріалах навчальної дисципліни «Інформаційна безпека бізнесу» (розміщені у бібліотеці університету (http://elibrary.univer.km.ua/index.php)) Під час лекційних занять застосовуються: 1) традиційний усний виклад змісту теми; 2) створення проблемних ситуацій; 3) слайдова презентація; 4) діалог, дискусія; 5) методи активного слухання та методи зворотного зв'язку. На семінарських заняттях застосовуються: 1) дискусійне обговорення проблемних питань; 2) методи активного слухання, диференціації та методи рефлексії. Поточний контроль знань фахівців вищої освіти може проводитися у формах: 1) усне або тестове опитування у Гугл-формі на семінарських заняттях; 2) захист підготовленої презентації; 3) реферативне повідомлення.
Політика щодо дедлайнів та здобуття балів за пропущені заняття	Перескладання лекцій та семінарських занять відбувається у порядку, визначеному 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) (http://www.univer.km.ua/studentu/ofis-studenta/ofis-studenta). Перескладання лекцій: в усній формі. Перескладання семінарських занять: виконання тестових завдань, реферативних повідомлень, індивідуальних завдань розміщених за кожною темою у Google класі «Інформаційна безпека бізнесу» (код приєднання: cdvdjor).
Критерії оцінювання	1. 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) (http://www.univer.km.ua/studentu/ofis-studenta/ofis-studenta). 2. Положення про систему рейтингового оцінювання результатів освітньої діяльності здобувачів вищої освіти у Хмельницькому університеті управління та права, введене в дію наказом від 19.02.2019 р. № 74/19 (http://www.univer.km.ua/studentu/ofis-studenta/ofis-studenta).

Політика академічної доброчесності	Розділ «Етика, академічна доброчесність та антикорупційна політика» на сайті Університету (https://univer.km.ua/pro-universytet/etyka-akademichna-dobrochesnist-ta-antykorrupsiyna-polityka-0)
Політика врегулювання конфліктів	Етичний кодекс Хмельницького університету управління та права імені Леоніда Юзькова, затверджений рішенням вченої ради університету 27 травня 2020 року, протокол № 9, введений в дію наказом від 27.05.2020 р. № 201/20 (http://univer.km.ua/doc/Etichniy_kodeks.pdf).
Зворотній зв'язок	1) Під час аудиторних занять, консультацій. 2) За допомогою анкетування після завершення вивчення навчальної дисципліни, регулярних анкетувань студентів, що проводяться в університеті.
Політика академічної доброчесності	Розділ «Етика, академічна доброчесність та антикорупційна політика» на сайті Університету (https://univer.km.ua/pro-universytet/etyka-akademichna-dobrochesnist-ta-antykorrupsiyna-polityka-0)

Обліковий обсяг – 0,32 ум.др.арк.