СИЛАБУС

навчальної дисципліни

«Управління інформаційною безпекою підприємства»

Спеціальність	073 «Менеджмент»
Освітня програма	Бізнес-адміністрування
Рівень вищої освіти	Перший (бакалаврський)
Статус навчальної дисципліни	вибіркова
Код навчальної дисципліни відповідно до освітньо-професійної програми	ВК 2
Семестр вивчення	4-й семестр
Кількість кредитів ЄКТС / годин	4 / 120
Розподіл за видами занять та годинами навчання	Лекції - 48 год.
	Практичні, семінарські заняття - 32 год.
	Самостійна робота - 40 год.
Вид індивідуального завдання	Практичні завдання, доповідь
Форма підсумкового контролю	залік
Кафедра (назва, № кабінету, контактний телефон, e-mail)	Кафедра Менеджменту і адміністрування
Викладач /і:	
Контактна інформація викладача/ів:	
Дні занять	Згідно з розкладом
Консультації	Очні консультації: згідно з графіком Дистанційні: електронна пошта, групи у Вайбері, Телеграмі

Анотація навчальної дисципліни

Зміни, що відбуваються в суспільстві призвели до значного зростання обсягів інформації у різних сферах. Крім того, ця інформація характеризується не лише швидкоплинністю, а й дуже динамічно змінюється та «старіє». Перед керівниками сучасних підприємницьких структур постає питання відбору саме корисної інформації, яка б дозволила ухвалювати ефективні управлінські рішення для реалізації визначених підприємством цілей. В умовах жорсткої конкуренції особливої уваги заслуговує інформація, яка характеризує певні технології, методи управління, тому власники такої інформації вимушені вживати відповідні заходи та технології для її захисту.

Мета навчальної дисципліни:

Формування у студентів сучасного управлінського мислення щодо управління інформаційною безпекою, застосування комплексного підходу із забезпечення інформаційної безпеки в різних сферах діяльності.

Мета орієнтована на формування у студентів таких компетентностей:

ЗК4. Здатність застосовувати знання у практичних ситуаціях

ЗК6. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК8. Навички використання інформаційних і комунікаційних технологій.

ЗК14. Здатність працювати у міжнародному контексті.

СК13. Розуміти принципи і норми права та використовувати їх у професійній діяльності.

СК17. Уміння використовувати законодавчі та інші нормативні акти державного і регіонального рівнів.

Програмні результати навчання (відповідно до освітньо-професійної програми)

ПРН 3. Демонструвати знання теорій, методів і функцій менеджменту, сучасних концепцій лідерства

ПРН 5. Описувати зміст функціональних сфер діяльності організації

ПРН 12. Оцінювати правові, соціальні та економічні наслідки функціонування організації

ПРН 13. Демонструвати здатність грамотно спілкуватись в усній та письмовій формі державною та іноземною мовами

ПРН 15. Демонструвати здатність діяти соціально відповідально та громадсько свідомо на основі етичних міркувань (мотивів), повагу до різноманітності та міжкультурності

ПРН 16. Демонструвати навички самостійної роботи, гнучкого мислення, відкритості до нових знань, бути критичним і самокритичним

Очікувані результати навчання

Вільно володіти основними термінами та визначеннями, що стосуються питань управління інформаційною безпекою підприємства;

Застосовувати набуті знання щодо формування вимог до інформації, яка використовується на підприємстві;

Забезпечувати заходи із формування політики безпеки підприємства;

Попереджати джерела та причини витоку інформації;

Передбачати різні способи охорони конфіденційної інформації;

Оцінювати структуру управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства;

Робити висновки щодо оптимального функціонування комп'ютерної системи підприємства та комплексної системи захисту інформації;

Формулювати основні завдання підрозділу захисту інформації;

Аналізувати результати аудиту стану інформаційної безпеки на підприємстві.

Зміст навчальної дисципліни:

Змістовий модуль 1

ТЕМА 1. ОСНОВИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА.

Інформація, її сутність. Основні ознаки та властивості інформації. Вимоги до інформації.

Загальна класифікація інформації. Класифікаційні ознаки інформації.

Основні вимоги до інформації у сучасній системі управління. Класифікація інформації в управлінні.

Тема 2. ІНФОРМАЦІЙНА БЕЗПЕКА: ОСНОВНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ.

Необхідність забезпечення інформаційної безпеки підприємства.

Безпека, інформаційна безпека. Інформаційне середовище. Об'єкти і суб'єкти інформаційної безпеки. Групи об'єктів інформаційної безпеки. Види інформаційної безпеки.

Сучасні особливості інформаційного розвитку підприємництва. Інформація як умова ефективного здійснення підприємницької діяльності. Структура інформаційної безпеки суб'єкта підприємництва. Основні принципи організації інформаційної безпеки. Вимоги надійності та ефективності інформаційної безпеки. Види інформаційної безпеки підприємництва. Структура процесу організації інформаційної безпеки суб'єкта підприємництва. Основні принципи побудови системи інформаційної безпеки.

Основні задачі інформаційної безпеки.

Тема 3. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА РІВНІ ПІДПРИЄМСТВА

Необхідність розробки і впровадження політики інформаційної безпеки. Передумови розробки політики безпеки підприємства.

Структура організаційної діяльності у сфері інформаційної безпеки на підприємстві.

Три її основні рівні політики безпеки: верхній, середній і нижній. Кроки при розробка політики безпеки. Правила розробки політики безпеки. Загальний життєвий цикл політики інформаційної безпеки.

Тема 4. ЗАГРОЗИ БЕЗПЕЦІ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

Базові терміни та визначення. Інформаційний простір. Інформаційний ресурс. Інформаційна інфраструктура. Інформаційна безпека. Загрози інформаційній безпеці. Захист інформації. Основні задачі забезпечення інформаційної безпеки.

Причини виникнення загрози інформаційній безпеці підприємства. Класифікація загроз безпеці. Джерела загроз. *Засоби впливу* загроз на інформаційну безпеку. Сучасні засоби захисту інформації в бізнес-середовищі. Методи запобігання та ліквідації загроз інформаційній безпеці. принципи захисту інформації.

Тема 5. ЗАГАЛЬНІ ПИТАННЯ ОХОРОНИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Мета захисту інформації. Поділ інформаційних ресурсів за критеріями.

Категорії інформації. Поняття конфіденційної інформації. Проблеми, пов'язані із захистом інформації.

Комерційна таємниця, основні поняття та умови охорони. Види відомостей, що становлять комерційну таємницю. Комерційна інформація. Секрети виробництва. Організаційно-управлінська діяльність підприємства.

ТЕМА 6. ДЖЕРЕЛА ТА ПРИЧИНИ ВИТОКУ ІНФОРМАЦІЇ.

Можливі канали просочування інформації. Аналіз документації підприємства як канал просочування інформації. Персонал підприємств як основне джерело просочування цінної інформації. Технічні засоби втрати інформації.

Основні причини витоку інформації: Персонал. Проблеми підбору кадрів. Відрядження. Співпраця з іншими компаніями. Використання складних IT-інфраструктур. Поломки техніки. Витік з технічних каналів передачі даних.

Контроль персоналу. Найбільш складні напрями в роботі з персоналом. Використання формалізованих методів при підборі та розстановці кадрів.

Норми документування та передачі комерційної таємниці. Вимоги щодо захисту зберігання електронних документів.

Тема 7. ЗАПОБІГАННЯ ПРОСОЧУВАННЮ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ.

Організаційні заходи щодо запобігання просочування інформації: Робота з кадрами. Пропускний режим. Обмеження допуску. Контроль діловодства. Інструктаж. Групи безпеки.

Правові способи запобігання просочування інформації. Законодавство про охорону комерційної таємниці. Правила укладання договорів і угод.

Технічні способи запобігання просочування інформації. Типи програмних засобів захисту персонального комп'ютера.

Тема 8. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ПІДПРИЄМСТВА.

Поняття комп'ютерної системи підприємства. Складові комп'ютерної системи підприємства.

Основні загрози інформації в КС підприємства. Класифікація загроз за результатом їх впливу на інформацію. Об'єкти захисту. Джерела зовнішніх загроз. Джерела внутрішніх загроз.

Змістовий модуль 2.

Тема 9. ЗАХИСТ ІНФОРМАЦІЇ ПІД ЧАС ВИКОРИСТАННЯ ЗАСОБІВ КОПІЮВАЛЬНО-РОЗМНОЖУВАЛЬНОЇ ТЕХНІКИ

Основні положення. Класи засобів КРТ.

Вимоги до захисту інформації та організація технічного захисту інформації. Рекомендації із захисту інформації, що обробляється засобами КРТ класу Б. Класифікатор засобів копіювально-розмножувальної техніки.

ТЕМА 10. РОЛЬ ПЕРСОНАЛУ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА.

Планування персоналу. Методи убезпечення (охорони) інтелектуальної й кадрової складової інформаційної безпеки. Мотиваційна модель поведінки персоналу по А.Маслоу. Врахування особливостей політичної, соціальної та демографічної ситуацій при плануванні роботи з персоналом. Принципи планування персоналу. Методи планування чисельності персоналу.

Методи та принципи відбору персоналу. Етапи формування трудового колективу. Джерела залучення персоналу.

Принципи підбору і розстановка кадрів.

Поняття психологічної сумісності. Фактори формування психологічної сумісності колективу.

Групи організаційних заходів при підборі персоналу, що одержує доступ до конфіденційної інформації. Основні особисті якості, які повинен мати потенційний працівник, пов’язаний з конфіденційною інформацією. Особисті якості, які не сприяють збереженню секретів. Методи підвищення ефективності дій персоналу щодо забезпечення ІБ.

ТЕМА 11. ЗАХОДИ ІЗ ФОРМУВАННЯ ПОЛІТИКИ БЕЗПЕКИ ПІДПРИЄМСТВА

Основні завдання забезпечення внутрішньооб'єктного режиму. Організація внутрішньооб'єктного режиму і охорони приміщень.

Фізичний захист. Складові фізичного захисту об’єктів.

Організація режиму секретності в установах і на підприємствах. Основний елемент організації режиму секретності.

ТЕМА 12. КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Поняття комплексної системи захисту інформації. Основні компоненти комплексної системи захисту інформації.

Основні особливості сучасного підприємства. Основні підходи до створення комплексної системи захисту інформації. Основні вимоги до комплексної системи захисту інформації.

Найпоширеніші види носіїв конфіденційної інформації. Об’єкти захисту.

Тема 13. УПРАВЛІННЯ КОМПЛЕКСНОЮ СИСТЕМОЮ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Поняття та класифікаційні ознаки надзвичайних ситуацій.

Технологія ухвалення рішення в умовах надзвичайної ситуації. Завдання системи управління НС. Режими системи управління НС.

Інформаційна підтримка прийнятих рішень.

Тема 14. ПІДРОЗДІЛ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Мета створення підрозділу захисту інформації (ПЗІ). Правова основа для створення і діяльності ПЗІ.

Основні завдання підрозділу захисту інформації.

Особливості взаємодії підрозділу захисту інформації з іншими підрозділами підприємства та зовнішніми організаціями.

Штатний розклад та структура підрозділу захисту інформації. Порядок визначення штату

ПЗІ.

Тема 15. АУДИТ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Поняття аудиту стану інформаційної безпеки на підприємстві. Аудит, види аудиту.Етапи проведення аудиту. Аналіз інформації, отриманої в результаті аудиту. Звіт (висновок) як заключний результат аналізу та узагальнення даних, отриманих в процесі аудиту, та додаткові рекомендації.

Методи викладання, навчання:

Проблемні лекції.

Практичні заняття: публічне обговорення питань тем курсу, виконання практичних завдань, експрес-опитування.

Виконання індивідуальних навчально-дослідних завдань (ІНДЗ): практичні завдання, електронна презентація на обрану тему наукової доповіді.

Форми контролю успішності навчання:

Контрольні заходи з перевірки успішності засвоєння навчального матеріалу з дисципліни включають: поточний контроль, виконання індивідуальних навчально-дослідних занять (ІНДЗ), підсумковий контроль.

Поточний контроль має на меті перевірку виконання завдань як аудиторної, так і самостійної роботи студентів та може проводитися в таких формах:

- перевірка підготовлених виступів, доповідей з тематики лекційних занять;
- усне опитування або письмовий експрес-контроль на аудиторних заняттях;
- перевірка виконання завдань СРС.

Контроль виконання *ІНДЗ* здійснюється у формі перевірки практичних завдань, наукової доповіді на обрану тему з електронною презентацією.

Формою *підсумкового контролю* з навчальної дисципліни є *залік*.

Семестровий залік – вид підсумкового контролю засвоєння студентами теоретичного та практичного матеріалу з навчальної дисципліни за семестр, що проводиться в період екзаменаційної сесії.

Форма проведення семестрового заліку – електронне тестування. При проведенні *підсумкового контролю* у формі електронного тестування використовується набір тестових завдань, які містяться в бібліотеці електронних курсів системи дистанційного навчання СУРА для перевірки знань студентів.

Рекомендована література:

1. Бабак В. П. Теоретичні основи захисту інформації: підручник. Київ: НАУ, 2008. 752 с.
2. Бегун. В.І. Інформаційна безпека: навч. посіб. К.: КНЕУ, 2008. 280с.
3. Бондарчук Ю.В., Марущак А.І. Безпека бізнесу: організаційно-правові основи: наук.-практ. посіб. К.: Видавничий дім «Скіф», КНТ, 2013. 372 с.
4. Васильченко М.І., Гришко В.В. Комунікативний менеджмент: навч.посіб. Полтава: ПолтНТУ, 2018. 208 с.
5. Гуцалюк М.В. Організація захисту інформації : навч.посіб. К.: Альтерпрес, 2011. 308 с.
6. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом: навч.посіб. Національний авіаційний університет; МОН. К.: НАУ, 2006. 108 с.
7. Зубок М.І. Інформаційна безпека: навч. посіб. К.: КНТЕУ, 2005. 133с.
8. Зубок М.І. Правове регулювання безпеки підприємницької діяльності: навч. посіб. К.: КНТЕУ, 2005. 141с.
9. Зубок М.І., Зубок Р.М. Безпека підприємницької діяльності. Нормативно-правові документи комерційного підприємництва, банку. К.: Істина, 2004. 144с.
10. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека: навч.посіб. Харків: Вид-во ХНЕУ, 2007. 352 с.
11. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч.посіб. К.:

Кондор, 2008. 383 с.
12. Крегул Ю.І., Зубок М.І. Правове регулювання безпеки підприємницької діяльності: навч. посіб. К.: КНТЕУ, 2013. 216с.
13. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення: підручник. К. : НАУ, 2011. 640 с.

Електронні ресурси:

14. Ахрамович В.М., Чегренец В.М. Інформаційна безпека. Практикум. К.:ДУТ, 2017. 396 с. URL: http://www.dut.edu.ua/uploads/l_1667_57891789.pdf.
15. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посіб. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с. URL: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf.
16. Живко З. Б. Сучасні методи забезпечення надійності персоналу: навч. посіб. у схемах і таблицях. Львів: ЛьвДУВС, 2019. 128 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/2774/3/%D0%B6%D0%B8%D0%B2%D0%BA%D0%BE%D0%9F%D0%95%D0%A0%D0%A1%D0%9E%D0%9D%D0%90%D0%9B_20-01-2020.pdf.
17. Зубок М.І. Інформаційна безпека в підприємницькій діяльності: підручник. К.: ГНОЗІС, 2015. 216 с. URL: http://www.dut.edu.ua/uploads/l_1472_54063755.pdf.
18. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y.
19. Кавун С. В., Пилипенко А. А., Ріпка Д. О. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навч. посіб. Х. : Вид. ХНЕУ, 2013. 364 с. URL: http://repository.hneu.edu.ua/bitstream/123456789/6818/1/Економічна%20та%20інформаційна%20безпека%20підприємств%20у%20системі%20консолідованої%20інформації%20%20навчальний%20посібник.pdf.
20. Комплексні системи захисту інформації: навч.посіб. / Яремчук Ю. Є., Павловський П. В., Катаєв В.С., Сінюгін В.В. URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/index.html.
21. Небава М. І., Міронова Ю.В. Економічна безпека підприємства : навч.посіб. Вінниця : ВНТУ, 2017. 73 с. URL: http://www.dut.edu.ua/uploads/l_1852_74531568.pdf.
22. Низенко Е. І., Каленяк В. П. Забезпечення інформаційної безпеки підприємництва: навч. посіб. К. : МАУП, 2006. 134 с. URL: https://maup.com.ua/assets/files/lib/book/p09_27.pdf.
23. Управління інформаційною безпекою: конспект лекцій : для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: Носок С. О., Фаль О. М., Ткач В. М. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с. URL: https://ela.kpi.ua/handle/123456789/43377.

Система оцінювання результатів навчання:

Згідно з діючою в університеті системою комплексної діагностики знань студентів, з метою стимулювання планомірної та систематичної навчальної роботи, оцінка знань студентів здійснюється за 100-бальною системою.

Підсумкова оцінка (залік) виставляється на підставі суми накопичених балів студентом, отриманих у ході поточного контролю, виконання індивідуального завдання.

Схема розподілу балів:

70 балів (поточний контроль)	30 балів (контроль виконання індивідуального завдання)

Мінімальний пороговий рівень з кожного виду контролю:

45 балів (поточний контроль)	15 балів (контроль виконання індивідуального завдання)

Накопичування балів з навчальної дисципліни під час *поточного* контролю відбувається під час оцінювання таких видів робіт:

1) участь у дискусіях, доповіді (презентації), виступи на практичних заняттях;
2) виконання практичних індивідуальних завдань;
3) усне опитування;
4) електронне тестування;
5) виконання завдань самостійної роботи.

Загальна семестрова оцінка за 100-бальною шкалою переводиться у національну шкалу відповідно до таблиці

Сума балів за всі види навчальної діяльності	Шкала ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проєкту (роботи)	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Критерії і порядок оцінювання навчальних досягнень здобувачів під час усіх видів контролю здійснюється відповідно до затверджено в університеті «Положення про критерії та порядок оцінювання навчальних досягнень з навчальних дисциплін здобувачів вищої освіти» (URL : https://www.suem.edu.ua/normatyvni-dokumeny).

Політика курсу:

Політика дотримання академічної доброчесності

Викладання навчальної дисципліни ґрунтується на засадах академічної доброчесності. Порушеннями академічної доброчесності вважаються: академічний плагіат, фабрикація, фальсифікація, списування.

За порушення академічної доброчесності студенти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання (контрольна робота, іспит тощо); повторне проходження відповідного освітнього компонента освітньої програми.

Комунікаційна політика

Студенти повинні мати активовану університетську пошту.

Обов'язком студента є перегляд новин на Телеграм-каналі.

Протягом тижнів самостійної роботи обов'язком студента є робота з дистанційним курсом «Управління інформаційною безпекою підприємства».

Політика щодо пропусків занять

Студенти мають відвідувати лекційні й практичні заняття. Відсутність студента на занятті може бути виправдана поважною причиною. Поважними причинами відсутності вважаються: хвороба, участь у Всеукраїнській студентській олімпіаді, Всеукраїнському конкурсі студентських наукових робіт чи будь-якому іншому заході, який можна віднести до заходів, що сприяють розвитку студентів і поліпшенню іміджу університету (факультету).

Політика щодо виконання навчальних завдань пізніше встановленого терміну

Студенти мають виконувати всі навчальні завдання у встановлені терміни. Студент, який не виконав ту чи іншу кількість навчальних завдань вчасно й хоче надолужити прогаяне, може звернутися по допомогу до викладача.

Політика щодо оскарження оцінювання

Якщо студент не згоден з оцінюванням його знань він може оскаржити виставлену викладачем оцінку у встановленому порядку.

Бонуси

Студенти, які регулярно відвідували лекції (мають не більше двох пропусків без поважних причин) та мають написаний конспект лекцій отримують додатково 2 бали до результатів оцінювання до підсумкової оцінки.