СХІДНОЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ РАУФА АБЛЯЗОВА



RAUF ABLYAZOV UNIVERSITY EAST EUROPEAN

Кафедра права та інформаційної справи

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНФОРМАЦІЙНА БЕЗПЕКА І ЗАХИСТ ІНФОРМАЦІЇ

Спеціальність	**В13 Бібліотечна, інформаційна та архівна справа**
Освітньо-професійна програма	**Документно-інформаційна діяльність**
Освітній ступінь	**БАКАЛАВР**

1 ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Статус навчальної дисципліни	*обов'язкова*
Мова викладання	українська
Обсяг дисципліни (у кредитах ЄКТС і годинах)	5/150
Передумови вивчення дисципліни:	Інформаційні та комунікаційні технології Документознавство
Анотація навчальної дисципліни:	Дисципліна «Інформаційна безпека і захист інформації» є практикоорієнтованою. Вона формує у здобувачів уявлення про те, що саме потрібно захищати на підприємстві, від чого і якими методами та засобами. У курсі розглядаються об'єкти інформаційної безпеки, джерела небезпек і загрози, режими доступу до інформації та види таємниць, канали витоку. Окремо вивчаються методи й засоби захисту, національна інфраструктура захисту інформації та вимоги стандартів ISO/IEC і української нормативної бази до управління інцидентами ІБ. Студенти опановують модель PDCA, досліджують людський чинник у службі ІБ та планують заходи аудиту інформаційної безпеки підприємства.
Мета і завдання навчальної дисципліни:	Мета і завдання навчальної дисципліни. Метою є формування у студентів системних знань і практичних навичок забезпечення інформаційної безпеки підприємства та установи. Йдеться про здатність аналізувати загрози, застосовувати вимоги стандартів і нормативних документів, описувати процеси управління інцидентами за моделлю PDCA, обґрунтовувати кадрові рішення в службі ІБ і планувати аудит.
Мета орієнтована на формування у студентів таких компетентностей:	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК3. Знання та розуміння предметної області та професійної діяльності. ЗК6. Навички використання інформаційних і комунікативних технологій. ЗК7. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел. ЗК9. Здатність працювати в команді. СК1. Здатність здійснювати відбір, аналіз, оцінку, систематизацію, моніторинг, організацію, зберігання, розповсюдження та надання в користування інформації та знань у будь-яких форматах. СК3. Здатність використовувати сучасні прикладні комп'ютерні технології, програмне забезпечення, мережеві та мобільні технології для вирішення професійних завдань. СК13. Здатність опановувати і використовувати технології електронного урядування та електронного документообігу.

	СК15. Здатність опановувати та застосовувати технології системного аналізу інформаційної діяльності.
Результати навчання:	ПРН5. Узагальнювати, аналізувати і синтезувати інформацію в діяльності, пов'язаній із її пошуком, накопиченням, зберіганням та використанням. ПРН6. Знати, розуміти та застосовувати в практичній діяльності законодавчі та галузеві нормативні документи. ПРН7. Забезпечувати ефективність функціонування документно-комунікаційних систем. ПРН12. Застосовувати сучасні методики і технології автоматизованого опрацювання інформації, формування та використання електронних інформаційних ресурсів та сервісів. ПРН16. Приймати обґрунтовані управлінські та технологічні рішення. ПРН17. Бути відповідальним, забезпечувати ефективну співпрацю в команді.

2 ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Форма організації освітнього процесу	Кількість кредитів	Загальна кількість годин	Семестр вивчення	Обсяги за видами навчальних занять			Самостійна робота (год)	Форма підсумкового контролю (екзамен/залік)
				Лекції (год)	Практичні, семінарські (год)	Лабораторні (год)		
Денна форма навчання	5	150	3	28		28	94	екзамен
Заочна форма навчання	5	150	3	4		2	144	екзамен

3 ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

3.1 Зміст навчальної дисципліни

Тема 1. Безпека, інформаційна безпека, інформаційна війна. Об'єкти інформаційної безпеки

Поняття безпеки як відсутності загрози та можливості надійного захисту. Небезпечний інформаційний вплив. Інформаційна безпека людини, суспільства, держави. Інформаційна війна. Дві площини курсу: захищеність людини й суспільства від шкідливих впливів та захищеність інформаційних ресурсів підприємства. Соціальні й ресурсні об'єкти інформаційної безпеки, їхні джерела загроз і параметри захищеності. Об'єкти забезпечення ІБ на підприємстві: приміщення, технічні й програмні засоби, інформація та носії, співробітники.

Тема 2. Джерела небезпек і загрози інформації

Класифікація джерел небезпек ресурсних об'єктів за походженням, способом реалізації та впливом. Конфіденційність, цілісність, доступність як базові властивості інформації. Антропогенні, техногенні та стихійні загрози. Види загроз інформації: викрадення, втрата, блокування, знищення, модифікація, заперечення справжності, нав'язування неправдивої інформації.

Тема 3. Режими доступу до інформації, види таємниць, канали витоку

Режим доступу до інформації. Відкрита інформація та інформація з обмеженим доступом. Таємна й конфіденційна інформація. Державна, службова та комерційна таємниця. Зовнішні та внутрішні канали витоку комерційної таємниці. Зв'язок внутрішніх каналів витоку із задоволеністю працівників.

Тема 4. Методи і засоби захисту інформації

Захист інформації як сукупність організаційно-технічних заходів і правових норм. Методи захисту: організаційні, законодавчі, фізичні, програмно-апаратні. Засоби захисту: технічні, правові, робота з кадрами. Вибір методів і засобів залежно від категорії інформації та ризиків.

Тема 5. Стратегія і тактика захисту інформації в комп'ютерних системах. Національна інфраструктура захисту інформації

Створення системи захисту як процес: етап проектування та етап експлуатації. Контроль і підтримка функціонування системи безпеки, реєстрація звернень до захищеної інформації, статистика та прогнозування. Роль аудиту як замикання циклу. Законодавча, технічна, організаційна, економічна й методологічна компоненти національної інфраструктури захисту інформації. Актуальність нормативної бази.

Тема 6. Стандарти ISO/IEC та українська нормативна база з управління інцидентами ІБ

Міжнародні організації та стандарти у сфері ІБ. Процесний підхід. ISO/IEC 27001, 27002, 27035, 20000: призначення та взаємозв'язок. Події та інциденти ІБ: ознаки розмежування. Вимоги ISO/IEC 27002 до звітування, керування інцидентами, вивчення інцидентів і збору доказів. Вимоги ISO/IEC 27001 (розд. 9.1, Додаток A.16). Етапи процесу реагування за ISO/IEC 27035 і склад групи реагування. Особливості управління IT-інцидентами за ISO/IEC 20000. Вітчизняна база: концепція розвитку телекомунікацій, НД ТЗІ, порядок захисту державних інформаційних ресурсів, Закон «Про захист інформації в інформаційно-телекомунікаційних системах», правила захисту інформації, Кримінальний кодекс, підрозділ реагування Держспецзв'язку. Прийняті в Україні редакції стандартів (ДСТУ ISO/IEC).

Тема 7. Модель PDCA та життєвий цикл процесів управління інцидентами ІБ

Цикл Шухарта–Демінга: походження, зміст фаз Plan–Do–Check–Act. Застосування PDCA до процесів за ISO 9001. Модель PDCA як основа системи управління ІБ. Пріоритезація інцидентів: вплив і терміновість. Нормативні документи з управління інцидентами: перелік подій-інцидентів, порядок оповіщення, усунення наслідків і причин, розслідування, дисциплінарні стягнення, коригувальні та превентивні заходи. Центри управління ІБ. Принципи OECD та їх відповідність фазам PDCA. Збереження статистики інцидентів.

Тема 8. Людський чинник у службі інформаційної безпеки

Працівник як об'єкт захисту й потенційне джерело загрози. Експертні опитування в атестації та адаптації персоналу. Привабливість роботи як інтегральний чинник. Чинники прийнятності та мотиваційні чинники (двофакторна теорія мотивації). Ранжування чинників,

обробка результатів в електронній таблиці, порівняння стовпців, ролей і теоретичної моделі. Кадрові ризики та їх зв'язок із внутрішніми каналами витоку. Обмеження висновків за малою вибіркою.

Тема 9. Аудит інформаційної безпеки підприємства

Поняття аудиту стану ІБ. Внутрішній і зовнішній аудит. Комплексний аудит та перевірка окремих елементів інфраструктури. Цілі аудиту. Етапи: планування, збір свідчень, аналіз і оцінювання, звітування, повторні перевірки. Стандарти як джерело вимог аудиту (ISO/IEC 27001, 27002, ISO 19011). Чотири напрями заходів захисту: організаційні, щодо людей, фізичні, технологічні. Вимоги до організації-аудитора.

Тема 10. Планування аудиту ІБ, методика аналізу результатів і аудиторський звіт

Вибір компанії та області аудиту. Формулювання перевірюваних вимог на підставі стандарту. План заходів аудиту: терміни, підрозділи, види перевірок. Обов'язковий розділ «Робота з кадрами». Методика оцінювання: бал виконання вимоги, вага вимоги, відповідність області, рівень відповідності. Форма аудиторського звіту. План повторних перевірок.

3.2 Тематика лекцій

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1.	Безпека, інформаційна безпека, інформаційна війна. Об'єкти інформаційної безпеки	2	
2.	Джерела небезпек і загрози інформації	2	
3.	Режими доступу до інформації, види таємниць, канали витоку	4	
4.	Методи і засоби захисту інформації	4	2
5.	Стратегія і тактика захисту інформації в комп'ютерних системах. Національна інфраструктура захисту інформації	4	
6.	Стандарти ISO/IEC та українська нормативна база з управління інцидентами ІБ	2	
7.	Модель PDCA та життєвий цикл процесів управління інцидентами ІБ	4	
8.	Людський чинник у службі інформаційної безпеки	2	
	Аудит інформаційної безпеки підприємства	2	
9.	Планування аудиту ІБ, методика аналізу результатів і аудиторський звіт	2	2
10.	Безпека, інформаційна безпека, інформаційна війна. Об'єкти інформаційної безпеки	2	
	Усього годин	**28**	**2**

3.3 Тематика практичних занять

№ з/п	Назва теми заняття	Обсяг у годинах	
		Денна форма	Заочна форма
1.	Об'єкти інформаційної безпеки підприємства: визначення об'єктів забезпечення ІБ	2	
2.	Класифікація джерел небезпек і загроз інформації для обраного підприємства	2	

№ з/п	Назва теми заняття	Обсяг у годинах	
		Денна форма	Заочна форма
3.	Режими доступу, види таємниць і канали витоку: аналіз внутрішніх та зовнішніх каналів	2	
4.	Методи і засоби захисту інформації: добір заходів для обраного підприємства	2	
5.	Етапи побудови та підтримання захисту. Компоненти національної інфраструктури захисту інформації	2	
6.	**Практична робота № 1.** Аналіз вимог стандартів ISO/IEC та української нормативної бази в частині управління інцидентами ІБ	4	1
7.	**Практична робота № 2.** Модель PDCA опису життєвого циклу процесів управління інцидентами ІБ	4	1
8.	**Практичне заняття.** Людський чинник: інформаційне забезпечення кадрового менеджменту служби ІБ (Розділ 1)	4	
9.	Аудит ІБ: види, цілі, етапи та вимоги до організації-аудитора	2	
10.	**Практичне заняття.** Планування заходів аудиту ІБ (Розділ 2)	4	
	Усього годин	**28**	

Практична робота № 1. Аналіз вимог стандартів ISO/IEC та української нормативної бази в частині управління інцидентами ІБ.

Мета: проаналізувати особливості законодавства України та стандартів ISO/IEC щодо управління інцидентами ІБ, навчитися застосовувати вимоги стандартів і нормативних документів до систем управління інцидентами ІБ.

Завдання: здійснити порівняльний аналіз вимог чотирьох довільно обраних нормативно-правових документів до управління інцидентами ІБ. Посилання на офіційні сайти державних органів і на сайт Верховної Ради України вказати за можливості. До кожного документа обов’язково додати анотацію.

Практична робота № 2. Модель PDCA опису життєвого циклу процесів управління інцидентами ІБ.

Мета: ознайомитися зі сценарієм та описом життєвого циклу управління процесами згідно з моделлю PDCA.

Завдання: 1) ознайомитися з теоретичними даними; 2) самостійно розглянути принципи OECD; 3) скласти таблицю порівняння та відповідності процесів OECD і PDCA; 4) зробити висновки.

Практичне заняття «Людський чинник та планування аудиту інформаційної безпеки підприємства» (комп’ютерна аудиторія, робота в підгрупах по 3–5 осіб, два заняття по 80 хв). Мета: навчитися досліджувати соціально-професійні уподобання працівників служби ІБ і обґрунтовувати кадрові рішення, а також планувати заходи аудиту ІБ та визначати стан захищеності підприємства.

- *Розділ 1.* Експертне опитування в підгрупі (10-бальна оцінка чинників привабливості роботи), заповнення таблиці 1.1, розрахунок середніх значень і різниці Δ, три порівняння (стовпець А проти В; ролі між собою; групи чинників проти теоретичної моделі), висновки та 1–2 кадрові ризики для передачі до Розділу 2.
- *Розділ 2.* Вибір компанії з таблиці описів; формулювання перевірюваних вимог аудиту на підставі стандарту; план заходів аудиту з обов’язковим розділом «Робота з кадрами»; методика аналізу результатів (бал 0–3, вага 1–3, відповідність області у відсотках, рівні відповідності); форма аудиторського звіту; план повторних перевірок.

- Результат: єдиний звіт про виконання, який захищається відповіддю на контрольні запитання.

Контрольні запитання до практичних робіт

До практичної роботи № 1:

1. Чим подія ІБ відрізняється від інциденту ІБ?
2. Які міжнародні та національні документи визначають процедури управління інцидентами ІБ?
3. Які етапи управління інцидентами передбачає ISO/IEC 27035?
4. Які цілі має управління інцидентами ІБ?
5. Чим управління IT-інцидентами за ISO/IEC 20000 відрізняється від управління інцидентами ІБ?
6. За яким принципом застосовують міжнародні та національні стандарти з управління інцидентами?
7. Для чого організації потрібні внутрішні нормативні документи з управління інцидентами?

До практичної роботи № 2:

1. Як охарактеризувати цикл Шухарта–Демінга?
2. Яка мета забезпечення ІБ організацій і підприємств?
3. Що таке інцидент ІБ? Наведіть приклади.
4. Охарактеризуйте концепцію PDCA.

До практичного заняття, Розділ 1:

1. Який інтегральний чинник найбільше впливає на професійну діяльність особистості?
2. Із яких компонентів він складається і чим чинники прийнятності відрізняються від мотиваційних?
3. Які засоби захисту інформації розрізняють?
4. У чому полягає робота з кадрами як засіб захисту?
5. Чому працівник є одночасно об’єктом забезпечення ІБ і джерелом загроз?
6. Які внутрішні канали витоку комерційної таємниці пов’язані з людським чинником?
7. Чому важливо порівнювати оцінки за стовпцями А та В, а не лише середню привабливість чинників?
8. Які обмеження має висновок, зроблений за даними опитування чотирьох осіб?

До практичного заняття, Розділ 2:

1. Що являє собою аудит стану ІБ на підприємстві?
2. Які існують два основних види аудиту та чим вони відрізняються?
3. Якими можуть бути цілі аудиту?
4. Яким вимогам має відповідати організація, що здійснює зовнішній аудит?
5. Чим комплексний аудит відрізняється від перевірки окремих елементів інфраструктури?
6. Чому вимоги аудиту мають бути перевірюваними? Наведіть приклад хорошої та поганої вимоги.
7. Як кадровий блок аудиту пов’язаний із внутрішніми каналами витоку інформації?
8. Як розрахувати відповідність області за методикою і чим визначається строк повторної перевірки?

3.4 Самостійна робота студентів (СРС)

№ з/п	Тема СРС	Обсяг у годинах	
		Денна форма	Заочна форма
1.	Безпека, інформаційна безпека, інформаційна війна. Об'єкти інформаційної безпеки	8	14
2.	Джерела небезпек і загрози інформації	8	14
3.	Режими доступу до інформації, види таємниць, канали витоку	10	14
4.	Методи і засоби захисту інформації	10	14
5.	Стратегія і тактика захисту інформації. Національна інфраструктура захисту інформації	10	14
6.	Стандарти ISO/IEC та українська нормативна база з управління інцидентами ІБ	10	15
7.	Модель PDCA та життєвий цикл процесів управління інцидентами ІБ	10	15
8.	Людський чинник у службі інформаційної безпеки	10	15
9.	Аудит інформаційної безпеки підприємства	8	14
10	Планування аудиту ІБ, методика аналізу результатів і аудиторський звіт	10	15
	Усього годин	**94**	**144**

Завдання для самостійної роботи:

- Складіть глосарій основних термінів дисципліни (не менше 25 понять): безпека, інформаційна безпека, інформаційна війна, конфіденційність, цілісність, доступність, режим доступу, комерційна таємниця, канал витоку, подія ІБ, інцидент ІБ, аудит ІБ тощо.
- Складіть порівняльну таблицю «Державна таємниця – службова таємниця – комерційна таємниця» за критеріями: визначення, сфера, суб'єкт-власник, наслідки розголошення.
- Складіть структурно-логічну схему «Методи й засоби захисту інформації» на основі таблиць теоретичної частини.
- Складіть схему етапів процесу реагування на інциденти за ISO/IEC 27035 із зазначенням змісту кожного етапу та складу групи реагування.
- Складіть схему п'яти компонент національної інфраструктури захисту інформації з прикладами для кожної.
- Для обраного підприємства складіть перелік об'єктів забезпечення ІБ і до кожного підберіть по дві актуальні загрози з посиланням на їх класифікацію.
- Складіть таблицю відповідності видів загроз (викрадення, модифікація, блокування тощо) порушуваним властивостям інформації (конфіденційність, цілісність, доступність) з прикладом для кожної.
- Розробіть проєкт переліку подій, що вважаються інцидентами ІБ для установи з 50 працівників, і порядок оповіщення відповідальної особи (формат звіту, контактні особи).
- За описаними в Практичній роботі № 2 прикладами (втрата незашифрованого ноутбука, дії звільненого системного адміністратора) визначте, які саме процедури були відсутні, і запропонуйте внутрішні документи для їх усунення.
- Проаналізуйте за ДСТУ ISO/IEC 27002 заходи, що стосуються роботи з персоналом, і співставте їх із засобом захисту «Робота з кадрами».

- Підготуйте аналітичну довідку (3–5 сторінок) «Актуальність нормативної бази з ІБ в Україні». Перевірте на порталі законодавства чинні редакції актів, згаданих у навчальних матеріалах, і вкажіть, що змінилося.
- Розробіть проєкт положення про порядок управління інцидентами ІБ для установи за моделлю PDCA (структура, відповідальні, форми звітності).
- Розробіть для обраної установи кадровий блок політики ІБ (перевірка працівників, навчання, ознайомлення з режимом конфіденційності, процедура звільнення) з обґрунтуванням на основі результатів експертного опитування.
- Складіть пам'ятку для працівників «Як діяти при підозрі на інцидент ІБ» (1–2 сторінки), у якій відобразіть вимоги про негайний запис деталей та відмову від самостійних дій.

3.5 Індивідуальні завдання

Однією з форм позааудиторної самостійної роботи студента є виконання індивідуальних завдань (ІЗ). ІЗ оцінюється окремою кількістю балів. Студенти виконують ІЗ у формі контрольної роботи, яка передбачає розв'язання фахових задач із наданням обґрунтованих висновків.

Контрольна робота складається з двох частин:

Частина 1. Загрози, захист інформації та інциденти ІБ

Фахова задача 1. Регіональний архів (35 працівників) переходить на електронний документообіг. Співробітник читального залу виніс на домашній ноутбуці без шифрування оцифровані справи з обмеженим доступом і залишив пристрій у автомобілі. Пристрій викрадено.

Завдання:

- Визначте об'єкти забезпечення ІБ, що постраждали, і порушені властивості інформації (конфіденційність, цілісність, доступність).
- Класифікуйте джерело небезпеки за походженням, способом реалізації та впливом.
- Визначте, чи є подія інцидентом ІБ, і обґрунтуйте віднесення за визначеннями ISO/IEC.
- Опишіть дії установи за етапами процесу реагування ISO/IEC 27035.
- Запропонуйте організаційні, правові та технічні заходи, які мали запобігти інциденту.

Фахова задача 2. Для комунального підприємства з 120 працівниками потрібно описати процес управління інцидентами ІБ за моделлю PDCA.

Завдання:

- Складіть таблицю, у якій для кожної фази Plan, Do, Check, Act зазначено дії, відповідальних, документи та результат.
- Визначте не менше шести типів подій, які підприємство має внести до переліку інцидентів.
- Опишіть порядок присвоєння пріоритету інциденту за впливом і терміновістю.
- Співставте фази PDCA з принципами OECD.
- Складіть форму звіту про інцидент ІБ.

Частина 2. Людський чинник та аудит ІБ

Фахова задача 3. За результатами опитування працівників служби ІБ компанії (адміністратор, молодший спеціаліст, керівник) отримано оцінки чинників привабливості

роботи за 10-бальною шкалою у двох вимірюваннях (А і В). *(Викладач надає вхідні дані кожному студентові.)*

Завдання:

- Розрахуйте середні значення за чинниками та різницю Δ.
- Виконайте порівняння стовпців А і В та порівняння між ролями.
- Співставте результати з двофакторною теорією (чинники прийнятності й мотиваційні чинники).
- Сформулюйте 2 кадрові ризики та вкажіть пов’язані з ними внутрішні канали витоку.
- Запропонуйте заходи роботи з кадрами та оцініть обмеження висновків.

Фахова задача 4. Для обраної установи (з переліку, наданого викладачем) складіть план аудиту ІБ.

Завдання:

- Оберіть область аудиту та сформулюйте не менше шести перевірюваних вимог на основі ISO/IEC 27001/27002.
- Складіть план заходів аудиту із зазначенням термінів, підрозділів і видів перевірок, включно з розділом «Робота з кадрами».
- За наведеними викладачем балами (0–3) і вагами (1–3) розрахуйте відповідність області у відсотках і визначте рівень відповідності.
- Визначте строк повторної перевірки.
- Складіть форму аудиторського звіту.

3.6 Форми поточного, проміжного та підсумкового контролю

Контрольні заходи з перевірки успішності засвоєння навчального матеріалу з дисципліни включають: поточний контроль, виконання ІЗ, проміжний контроль.

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

- заслуховування і публічне обговорення підготовлених виступів, доповідей з тематики занять;
- перевірка виконання практичних завдань на аудиторних заняттях;
- усне опитування або письмовий контроль на аудиторних заняттях;
- перевірка виконання завдань СРС.

Контроль виконання *ІЗ* здійснюється у формі перевірки виконання контрольної роботи.

*Проміжний контрол*ь проводиться у формі усного і письмового опитування за матеріалами тем змістових модулів курсу.

Формою *підсумкового контролю* з навчальної дисципліни «Інформаційна безпека і захист інформації» є *екзамен*.

При проведенні *підсумкового контролю* у формі електронного тестування використовується набір тестових завдань, які містяться в бібліотеці електронних курсів системи дистанційного навчання Moodle.

Перелік питань до підсумкового контролю (екзамен)

1. Дайте визначення безпеки та поясніть, які два питання потрібно з’ясувати, оцінюючи безпеку.
2. Що таке інформаційна безпека людини, суспільства, держави?
3. У чому суть інформаційної війни?
4. Які існують соціальні та ресурсні об’єкти інформаційної безпеки?
5. Що належить до об’єктів забезпечення ІБ на підприємстві?
6. Назвіть три базові властивості інформації та поясніть кожну.
7. За якими ознаками класифікують джерела небезпек ресурсних об’єктів?

8. Чим антропогенні загрози відрізняються від техногенних і стихійних?
9. Назвіть основні види загроз інформації.
10. Що таке режим доступу до інформації?
11. Чим таємна інформація відрізняється від конфіденційної?
12. Які існують види таємниць?
13. Що розуміють під комерційною таємницею?
14. Які джерела загроз для комерційної таємниці вважають зовнішніми, а які внутрішніми?
15. Що таке захист інформації?
16. Назвіть методи захисту інформації.
17. Які засоби захисту інформації розрізняють?
18. Що таке подія ІБ і що таке інцидент ІБ?
19. Які стандарти серій ISO/IEC стосуються управління інцидентами ІБ?
20. Назвіть етапи процесу реагування на інциденти за ISO/IEC 27035.
21. Що означає абревіатура PDCA і що робиться на кожній фазі циклу?
22. Хто запропонував цикл PDCA і хто його популяризував?
23. Які основні цілі аудиту ІБ?
24. Які існують види аудиту ІБ?
25. Які етапи включає типовий аудит ІБ?
26. Порівняйте інформаційну безпеку як захищеність людини й суспільства та як захищеність ресурсів підприємства.
27. Поясніть, чому працівник є одночасно об’єктом захисту та джерелом загрози.
28. Проаналізуйте, як різні види загроз (блокування, модифікація, перехоплення) пов’язані з порушенням конфіденційності, цілісності чи доступності.
29. Порівняйте державну, службову та комерційну таємницю за змістом і наслідками розголошення.
30. Проаналізуйте внутрішні канали витоку, пов’язані з людським чинником.
31. Порівняйте організаційні та програмно-апаратні методи захисту, наведіть приклади.
32. Розкрийте зміст етапів проектування та експлуатації системи захисту інформації.
33. Проаналізуйте компоненти національної інфраструктури захисту інформації та роль кожної.
34. Проаналізуйте вимоги Додатка A.16 ISO/IEC 27001 до управління інцидентами.
35. Проаналізуйте рекомендації ISO/IEC 27002 щодо збору й збереження доказів.
36. Поясніть склад і завдання групи реагування на інциденти за ISO/IEC 27035.
37. Порівняйте управління IT-інцидентами (ISO/IEC 20000) та інцидентами ІБ.
38. Проаналізуйте обов’язки щодо повідомлення про інциденти, що встановлені українським законодавством.
39. Поясніть, як визначають пріоритет інциденту за впливом і терміновістю.
40. Розкрийте, чому відсутність зафіксованих інцидентів не доводить належної роботи системи управління ІБ.
41. Проаналізуйте на прикладі втрати незашифрованого ноутбука, які процедури мали бути в компанії.
42. Проаналізуйте, чому недостатньо регістрації дій системного адміністратора для притягнення до відповідальності і що ще необхідно.
43. Поясніть відмінність між чинниками прийнятності та мотиваційними чинниками.
44. Розкрийте зв’язок між результатами кадрового опитування та ризиками витоку інформації.
45. Порівняйте комплексний аудит з перевіркою окремих елементів інфраструктури.
46. Розкрийте вимоги до організації, що проводить зовнішній аудит.
47. Проаналізуйте, чому вимоги аудиту мають бути перевірюваними, і наведіть приклади хорошої та поганої вимог.
48. Поясніть, як розраховується відповідність області за методикою оцінювання аудиту.
49. Поясніть, як рівень відповідності визначає строк повторної перевірки.

50. Співставте принципи OECD та фази циклу PDCA.
51. Розробіть перелік об’єктів забезпечення ІБ і матрицю загроз для бібліотеки або архіву середнього розміру.
52. Спрогнозуйте наслідки витоку комерційної таємниці через незадоволеного працівника і запропонуйте комплекс запобіжних заходів.
53. Складіть комплекс організаційних, правових і технічних заходів захисту конфіденційної інформації для установи з електронним документообігом.
54. Оцініть, наскільки повно національна інфраструктура захисту інформації забезпечує потреби підприємства, і запропонуйте шляхи вдосконалення.
55. Розробіть проєкт переліку подій-інцидентів і порядок оповіщення для обраної установи.
56. Розробіть проєкт процедури розслідування інциденту ІБ зі збором і збереженням доказів.
57. Розробіть опис життєвого циклу процесу управління інцидентами за моделлю PDCA для підприємства з розподіленою мережею філій.
58. Оцініть, які ризики виникають у разі відсутності нормативно визначеного переліку інцидентів та їх документування.
59. Запропонуйте комплекс робіт з кадрами за результатами експертного опитування працівників служби ІБ і обґрунтуйте його.
60. Оцініть достовірність висновків, зроблених за малою вибіркою опитування, і запропонуйте способи її підвищення.
61. Розробіть план аудиту ІБ для обраного підприємства з розділом «Робота з кадрами».
62. Розробіть форму аудиторського звіту та план повторних перевірок за наведеними результатами оцінювання.
63. Оцініть доцільність залучення зовнішнього аудитора для підприємства заданого розміру та профілю.
64. Спрогнозуйте результати аудиту кадрової області, якщо не налагоджено блокування облікових записів звільнених працівників і навчання з ІБ, і запропонуйте заходи.
65. Розробіть комплексну програму підвищення рівня ІБ установи на 12 місяців із критеріями результативності за циклом PDCA.

3.7 Методика навчання

Лекції (проблемні лекції, лекції-демонстрації з використанням мультимедійного обладнання).

Семінарські заняття (доповіді, виступи, публічне обговорення питань тем курсу, виконання завдань, розв’язання фахових задач (кейс-метод), рольові ігри у форматі «клієнт – юрист-консультант»).

Самостійне навчання: виконання завдань самостійної роботи; індивідуальних завдань; робота з навчальною літературою, правовими джерелами.

4 КРИТЕРІЇ І ПОРЯДОК ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Кожний вид поточної навчальної роботи студента оцінюються за 5-бальною шкалою.

Критерії оцінювання роботи студентів на семінарських, практичних заняттях, виконання завдань СРС:

Оцінка	Критерії оцінювання навчальних досягнень
5 балів	Оцінюється робота студента, який у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко та всебічно розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов’язкову та додаткову літературу, вільно послуговується науковою термінологією, розв’язує задачі стандартним або

	оригінальним способом, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки. Може аргументовано обрати раціональний спосіб виконання завдання й оцінити результати власної практичної діяльності; виконує завдання, не передбачені навчальною програмою; вільно використовує знання для розв'язання поставлених перед ним завдань.
4 бали	Оцінюється робота студента, який достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову літературу, розв'язує задачі стандартним способом, послуговується науковою термінологією. Але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки. За зразком самостійно виконує практичні завдання, передбачені програмою; має стійкі навички виконання завдання.
3 бали	Оцінюється робота студента, який відтворює значну частину навчального матеріалу, висвітлює його основний зміст, виявляє елементарні знання окремих положень, записує основні формули, рівняння, закони. Не здатний до глибокого, всебічного аналізу, обґрунтування та аргументації, не користується необхідною літературою, допускає істотні неточності та помилки. Планує та виконує частину завдання за допомогою викладача.
2 бали	Оцінюється робота студента, який не володіє навчальним матеріалом у достатньому обсязі, проте фрагментарно, поверхово (без аргументації та обґрунтування) викладає окремі питання навчальної дисципліни, не розкриває зміст теоретичних питань і практичних завдань. Виконує лише елементи завдання, потребує постійної допомоги викладача.
1 бал	Оцінюється робота студента, який не в змозі викласти зміст більшості питань теми та курсу, володіє навчальним матеріалом на рівні розпізнавання явищ, допускає істотні помилки, відповідає на запитання, що потребують однослівної відповіді. Виконує лише елементи завдання, потребує постійної допомоги викладача.
0 балів	Оцінюється робота студента, який не володіє навчальним матеріалом та не в змозі його висвітлити, не розуміє змісту теоретичних питань та практичних завдань.

Критерії оцінювання виконання індивідуальних завдань (ІЗ)

для дисциплін, вивчення яких завершується екзаменом	
10 балів	Оцінюється робота студента, який у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко та всебічно розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу, вільно послуговується науковою термінологією, розв'язує задачі стандартним або оригінальним способом, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки. Може аргументовано обрати раціональний спосіб виконання завдання й оцінити результати власної практичної діяльності; виконує завдання, не передбачені навчальною програмою; вільно використовує знання для розв'язання поставлених перед ним завдань.
8-9 балів	Оцінюється робота студента, який достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову літературу, розв'язує задачі стандартним способом, послуговується науковою термінологією. Але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки. За зразком самостійно виконує практичні завдання, передбачені програмою; має стійкі навички виконання завдання.

для дисциплін, вивчення яких завершується екзаменом	
7 балів	Оцінюється робота студента, який відтворює значну частину навчального матеріалу, висвітлює його основний зміст, виявляє елементарні знання окремих положень, записує основні формули, рівняння, закони. Не здатний до глибокого, всебічного аналізу, обґрунтування та аргументації, не користується необхідною літературою, допускає істотні неточності та помилки. Планує та виконує частину завдання за допомогою викладача.
6 балів	Оцінюється робота студента, який не володіє навчальним матеріалом у достатньому обсязі, проте фрагментарно, поверхово (без аргументації та обґрунтування) викладає окремі питання навчальної дисципліни, не розкриває зміст теоретичних питань і практичних завдань. Виконує лише елементи завдання, потребує постійної допомоги викладача.
5 балів	Оцінюється робота студента, який не в змозі викласти зміст більшості питань теми та курсу, володіє навчальним матеріалом на рівні розпізнавання явищ, допускає істотні помилки, відповідає на запитання, що потребують однослівної відповіді. Виконує лише елементи завдання, потребує постійної допомоги викладача.
< 5 балів	Оцінюється робота студента, який не володіє навчальним матеріалом та не в змозі його висвітлити, не розуміє змісту теоретичних питань та практичних завдань.

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

Підсумкова оцінка виставляється на підставі суми накопичених балів студентом, отриманих у ході поточного, рубіжного контролів, виконання ІЗ, складання заліку та екзамену (підсумковий контроль).

Схема розподілу балів:

Екзамен	50 балів (поточний, рубіжний контроль)	10 балів (контроль виконання індивідуальних завдань)	40 балів (підсумковий контроль)

Мінімальний пороговий рівень з кожного виду контролю:

Екзамен	30 балів (поточний, рубіжний контроль)	5 балів (контроль виконання індивідуальних завдань)	25 балів (підсумковий контроль)

Підсумкова 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	
75-81	C		
64-74	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

5 ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засобами оцінювання та методами демонстрування результатів навчання з вивчення навчальної дисципліни «Інформаційна безпека і захист інформації» є:

- тести;
- індивідуальні завдання;
- усні, письмові відповіді при проведенні контрольних заходів (рубіжний контроль);
- доповіді і виступи на заняттях;
- проведення опитування на заняттях;
- звіти з виконання завдань СРС;
- звіти з виконання практичних завдань;
- презентації результатів виконаних завдань та досліджень.

6 ІНСТРУМЕНТИ, ОБЛАДНАННЯ, ПРОГРАМНЕ І МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Електронні ресурси: конспект лекцій, електронна бібліотека навчальної літератури, презентації окремих тем, банк тестів, методичні вказівки до вивчення дисципліни для студентів.

7 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Управління інформаційною безпекою : навч. посібник / О. М. Богданов та ін. Київ : КПІ ім. Ігоря Сікорського, 2020. URL: https://ela.kpi.ua/bitstreams/78ac6951-65ee-4a76-8acf-ba0554c5de4c/download.

2. Основи кібербезпеки : навч. посібник / А. М. Гребенюк, Л. В. Рибальченко. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. URL: https://dspace.ddpu.edu.ua/bitstreams/54f48bb1-bb45-4a1d-942b-9f7b9f4fe2ee/download.

4. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с. URL: https://er.dduvs.edu.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

5. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний К. ,2018. URL: https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf.

6. Костюк Ю. В., Складанний П.М. Захист інформації в комп'ютерних системах та мережах. Частина І: підручник /Ю.В. Костюк, П.М. Складанний. Київ : Київський столичний університет імені Бориса Грінченка, 2026. 401 с. URL: https://elibrary.kubg.edu.ua/id/eprint/56332/1/ZIKSM_part_1_2026_FITM.pdf.

7. ДСТУ ISO/IEC 27035-1:2024. Інформаційна безпека, кібербезпека та захист конфіденційності. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес (ISO/IEC 27035-1:2023, IDT). [Чинний від 2024-06-01]. Київ : ДП «УкрНДНЦ», 2024. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=112378.

8. ДСТУ ISO/IEC 27035-2:2024. Інформаційна безпека, кібербезпека та захист конфіденційності. Керування інцидентами інформаційної безпеки. Частина 2. Рекомендації щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2023, IDT). [Чинний від 2024-06-01]. Київ : ДП «УкрНДНЦ», 2024. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=112379.