МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ МИКОЛАЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМ. В.О.СУХОМЛИНСЬКОГО»

ЦИКЛОВА КОМІСІЯ ТЕХНІЧНОГО НАПРЯМУ ПІДГОТОВКИ (ВИПУСКОВА)

«ЗАТВЕРДЖУЮ»
Заступник директора
з навчальної роботи
ВСП «Фаховий коледж
МНУ імені В.О.Сухомлинського»
_____ Олена САХАРОВА
«27» серпня 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

освітньо-професійний ступінь — фаховий молодший бакалавр

галузь знань: — 12 Інформаційні технології

спеціальності: — 123 Комп'ютерна інженерія

2024 – 2025 навчальний рік

Розробник: **Божко Надія Валеріївна**, викладач вищої категорії циклової комісії технічно напряму підготовки (випускова)

_____ Надія БОЖКО
(підпис) (прізвище та ініціали)

Програма затверджена на засіданні циклової комісії технічного напряму підготовки.

Протокол № 11 від «26» серпня 2024 року

Голова циклової комісії _____ Ксенія САНАЙКО
(підпис) (прізвище та ініціали)

Програму погоджено навчально-методичною радою коледжу.

Протокол № 8 від «27» серпня 2024 року

Голова навчально-методичної ради _____ Олена САХАРОВА
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-професійний ступінь</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Напрям підготовки 12 «Інформаційні технології»</td><td>Вибіркова</td></tr>
<tr><td rowspan="4">Загальна кількість годин – 90 год.</td><td rowspan="4">Спеціальність 123 «Комп’ютерна інженерія»</td><td>Рік підготовки:</td></tr>
<tr><td>4-й</td></tr>
<tr><td>Семестр</td></tr>
<tr><td>8-й</td></tr>
<tr><td rowspan="8">Тижневих годин для денної форми навчання:
аудиторних – 2
самостійної роботи студента – 1</td><td rowspan="8">Ступінь фаховий молодший бакалавр</td><td>Лекції</td></tr>
<tr><td>16 год.</td></tr>
<tr><td>Лабораторні роботи</td></tr>
<tr><td>24 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>50 год.</td></tr>
<tr><td colspan="2">Вид контролю: іспит</td></tr>
</table>

Мова навчання – українська

Примітка. Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить: для денної форми навчання – 90год.: 40 год. – аудиторні заняття, 50 год. – самостійна робота (44,4%~55,6%)

2. Мета та завдання навчальної дисципліни

2.1. Метою викладання навчальної дисципліни «Захист інформації в комп’ютерних системах» є: формування у студентів знань та навичок, необхідних для забезпечення безпеки інформаційних систем, що включає ознайомлення з основними принципами та методами захисту інформації, розвиток практичних навичок у застосуванні сучасних технологій захисту, таких як криптографія та системи контролю доступу, формування критичного мислення та аналітичних здібностей для оцінки ефективності різних методів захисту, а також підготовку до професійної діяльності у сфері інформаційної безпеки, що охоплює технічні та управлінські аспекти.

2.2 Завдання курсу:

– вивчення основних термінів та концепцій інформаційної безпеки;

– огляд загроз та вразливостей інформаційних систем;

– розгляд законодавчих та етичних аспектів захисту інформації;

– використання криптографічних алгоритмів у широко розповсюджених програмних продуктах;

– проведення перевірки якості криптографічних рішень;
– генерація та розподіл ключів для забезпечення безпеки даних;

Викладення дисципліни обумовлено необхідністю формування у студентів чіткої системи уявлень про цілісний комплекс проблем, пов’язаних з захистом даних що мають бути вирішені в процесі проектуванні та використанні комп’ютерних систем.

Міждисциплінарні зв’язки:

Дисципліна «Захист інформації в комп'ютерних системах» базується на таких предметах, як «Вища математика», «Інформатика», «Комп'ютерні системи та мережі», «Системне програмування», «Теорія інформації», «Основи правознавства» та «Основи економічної теорії». Ці зв’язки забезпечують комплексний підхід до вивчення захисту інформації, інтегруючи знання з різних галузей для формування цілісного розуміння проблематики безпеки інформаційних систем.

Програмні результати навчання (РН):

РН4.	Застосовувати правові норми, норми з охорони праці, безпеки життєдіяльності у професійній діяльності.
РН14.	Використовувати сучасні інтегровані середовища, методи і технології розробки, впровадження, адміністрування комп’ютернихи систем та мереж, баз даних і знань.

Згідно з вимогами освітньо-професійної програми студент оволодіває такими **компетентностями:**

Інтегральна компетентність	Здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій в процесі професійної діяльності або навчання, що вимагає застосування методів і технологій комп’ютерної інженерії та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності, здійснювати контроль інших осіб у визначених ситуаціях
Загальні компетентності	ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
Спеціальні компетентності	СК8. Здатність здійснювати організацію робочих місць з урахуванням вимог охорони праці, їх технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації. СК14. Здатність оцінювати і враховувати економічні, соціальні, технологічні та екологічні чинники, що впливають на сферу професійної діяльності.

Мова навчання – українська**.**

На вивчення навчальної дисципліни відводиться 90 годин / 3 кредити ECTS.

3. Інформаційний обсяг навчальної дисципліни

Кредит 1 Загальні аспекти захисту інформації.

Лекція №1. Вступ. Основні поняття і аналіз загроз інформаційної безпеки.

Визначення інформаційної безпеки. Основні поняття захисту інформації і інформаційної безпеки. Аналіз загроз інформаційної безпеки. Класифікація загроз інформаційній безпеці. Види загроз: технічні, соціальні, природні. Оцінка ризиків та вразливостей. Методи захисту інформації. Приклади реальних інцидентів у сфері інформаційної безпеки. Сучасні тенденції в інформаційній безпеці.

Лекція №2. Основи безпеки даних в комп'ютерних системах. Захист інформації в комп’ютерних системах від випадкових загроз

Основні поняття щодо захисту інформації в автоматизованих системах. Загрози безпеки даних та їх особливості. Дублювання інформації. Підвищення надійності КС. Блокування помилкових операцій. Оптимізація взаємодії користувачів і обслуговуючого персоналу з КС. Мінімізація збитку від аварій і стихійних лих.

Лабораторна робота №1. Аналіз методів і засобів несанкціонованого здобуття інформації .

Лабораторна робота №2. Використання засобів захисту електронних таблиць.

Лекція №3. Аутентифікація та авторизація доступу користувачів комп’ютерної системи.

Поняття ідентифікації, аутентифікації та аудиту. Визначення ідентифікації: процес розпізнавання користувача в системі. Аутентифікація: перевірка, чи є користувач тим, за кого себе видає. Аудит: процес перевірки дій користувачів для забезпечення безпеки системи. Види облікових записів користувачів комп’ютерної системи. Різні типи облікових записів: адміністративні, стандартні, гостьові. Ролі та права доступу, пов'язані з кожним типом облікового запису. Порядок аутентифікації й авторизації у комп’ютерних системах. Процес аутентифікації: введення імені користувача та пароля, біометричні методи. Авторизація: надання прав доступу після успішної аутентифікації. Приклади механізмів аутентифікації: паролі, токени, двофакторна аутентифікація.

Лабораторна робота №3. Використання стандартних засобів захисту та зламу захисту PDF-документів.

Лекція №4. Політики безпеки.

Основні поняття політики безпеки. Визначення політики безпеки: набір вимог, правил, обмежень та рекомендацій, що регламентують інформаційну діяльність в організації. Значення політики безпеки для забезпечення захисту інформації та управління ризиками.

Структура політики безпеки організації. Основні компоненти: мета, обсяг, відповідальність, процедури. Взаємозв'язок між політикою безпеки та іншими політиками організації.

Базова політика безпеки. Основні принципи та правила, що визначають загальний підхід до безпеки інформації. Вимоги до всіх співробітників та користувачів інформаційних систем.

Спеціалізовані політики безпеки. Політики, що стосуються конкретних аспектів безпеки: доступу, використання мережі, обробки даних. Приклади: політика використання паролів, політика захисту персональних даних.

Процедури безпеки. Опис процедур, які реалізують політики безпеки на практиці. Включення заходів реагування на інциденти, навчання співробітників, моніторинг та аудит.

Лабораторна робота №4. Апаратні засоби захисту інформації в комп'ютерних системах.

Лабораторна робота №5. Аналіз ефективності парольного захисту PDF-документів, архівів у різних форматах, текстових документів та електронних таблиць. Створення стійких паролів.

Кредит 2. Криптографічні методи захисту інформації.

Лекція №5. Криптографічні системи та криптографічні методи захисту. Модулярна арифметика.

Основні терміни та поняття. Визначення криптографії: наука про захист інформації шляхом перетворення даних. Ключові терміни: шифрування, дешифрування, криптографічний алгоритм, ключ. Історія і законодавча база криптографії. Короткий огляд історії розвитку криптографії: від класичних методів до сучасних технологій. Законодавчі аспекти: регулювання використання криптографії в різних країнах. Огляд сучасних криптографічних систем: симетричні та асиметричні. Особливості використання криптографії в інформаційних технологіях. Основи модулярної арифметики: визначення та застосування в криптографії. Приклади використання модулярної арифметики в криптографічних алгоритмах.

Лабораторна робота №6. Класичні техніки шифрування. Шифр Цезаря.

Лекція №6. Класичні методи шифрування.

Огляд класичних методів шифрування: шифр Цезаря, шифр Віженера, шифр заміни. Переваги та недоліки класичних методів. Приклади застосування класичних шифрів у практиці.

Лабораторна робота №7. Класичні шифри та криптоаналіз.

Лекція №7. Симетричні та асиметричні методи шифрування.

Визначення та принципи роботи симетричних алгоритмів (AES, DES). Переваги та недоліки симетричного шифрування.

Визначення та принципи роботи асиметричних алгоритмів (RSA, ECC). Переваги та недоліки асиметричного шифрування. Використання асиметричних методів у сучасних системах безпеки.

Лекція №8. Електронний цифровий підпис (ЕЦП)

Визначення та принципи роботи ЕЦП. Технології, що використовуються для створення та перевірки ЕЦП. Використання ЕЦП в електронному документообігу, фінансових операціях та інших сферах.

Правові аспекти використання електронних підписів.

Лабораторна робота №8. Застосування криптографічних засобів захисту інформації. Генерування і використання електронного цифрового підпису для реалізації захисту файлів користувача.

Кредит 3. Безпека в інформаційних мережах

Лекція №9. Моделі безпеки операційних систем. Захист інформації в мережах.

Визначення моделей безпеки: концептуальні структури, що описують, як забезпечується безпека в операційних системах.

Основні моделі безпеки: модель Біббера, модель Латтера, модель Bell-LaPadula.

Основні загрози для інформації в мережах: несанкціонований доступ, атаки типу «відмова в обслуговуванні» (DoS), шкідливе програмне забезпечення.

Методи захисту інформації в мережах: використання фаєрволів для контролю трафіку, шифрування даних для захисту інформації під час передачі, аутентифікація користувачів для запобігання несанкціонованому доступу.

Роль політик безпеки в управлінні ризиками та забезпеченні безпеки мережевих ресурсів.

Лабораторна робота №9. Використання облікових записів користувачів та груп для захисту від комп'ютерних вірусів на рівні операційної системи за допомогою реалізації політик безпеки з обмеженими правами доступу

Лекція №10. Аудит об'єктів інформаційної безпеки. Аналіз ризиків корпоративних інформаційних систем.

Визначення аудиту інформаційної безпеки: системний процес оцінки стану безпеки інформаційних систем, що включає перевірку політик, процедур, технологій та контролів.

Основні цілі аудиту: виявлення вразливостей, оцінка ефективності заходів безпеки, відповідність нормативним вимогам.

Процес аудиту: планування, виконання, документування результатів, формулювання рекомендацій.

Визначення ризику: ймовірність виникнення загрози та її вплив на інформаційні активи.

Основні етапи аналізу ризиків: ідентифікація активів, оцінка загроз, оцінка вразливостей, оцінка ризиків.

Розробка стратегії управління ризиками: визначення заходів для зменшення ризиків до прийнятного рівня.

Лабораторна робота №10. Налаштування рівнів безпеки сучасних браузерів.

Лабораторна робота №11. Встановлення, налаштування та обслуговування програм-антивірусів.

Лабораторна робота №12. Використання програм віддаленого керування.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	денна форма				
	усього	у тому числі			
		лек.	л.р.	пр.р.	с.р.
1	**2**	**3**	**4**	**5**	**6**
Кредит №1. Загальні аспекти захисту інформації.					
Тема №1. Вступ. Основні поняття і аналіз загроз інформаційної безпеки. Основи безпеки даних в комп'ютерних системах. Захист інформації в комп’ютерних системах від випадкових загроз	**10**	2	4	-	4
Тема №2. Аутентифікація та авторизація доступу користувачів комп’ютерної системи	**10**	2	2	-	6
Тема №3. Політики безпеки	**10**	2	4	-	4
Кредит №2. Криптографічні методи захисту інформації.					
Тема №4. Криптографічні системи та криптографічні методи захисту. Модулярна арифметика	**10**	2	2	-	6
Тема №5. Класичні методи шифрування.	**10**	2	2	-	6
Тема №6. Симетричні та асиметричні методи шифрування. Електронний цифровий підпис (ЕЦП)	**10**	2	2	-	6
Кредит №3. Безпека в інформаційних мережах					
Тема №7. Моделі безпеки операційних систем. Захист інформації в мережах	**15**	2	2	-	11
Тема №8. Аудит об’єктів інформаційної безпеки. Аналіз ризиків корпоративних інформаційних систем.	**15**	2	6	-	7
Всього:	**90**	**16**	**24**	**-**	**50**

5. Теми лекційних занять

№	Тема	Год
1	Лекція №1. Вступ. Основні поняття і аналіз загроз інформаційної безпеки. Лекція №2. Основи безпеки даних в комп'ютерних системах. Захист інформації в комп'ютерних системах від випадкових загроз	2
2	Лекція №3. Аутентифікація та авторизація доступу користувачів комп'ютерної системи	2
3	Лекція №4. Політики безпеки	2
4	Лекція №5. Криптографічні системи та криптографічні методи захисту. Модулярна арифметика	2
5	Лекція №6. Класичні методи шифрування	2
6	Лекція №7. Симетричні та асиметричні методи шифрування. Лекція №8. Електронний цифровий підпис (ЕЦП)	2
7	Лекція №9. Моделі безпеки операційних систем. Захист інформації в мережах	2
8	Лекція №10. Аудит об'єктів інформаційної безпеки. Аналіз ризиків корпоративних інформаційних систем.	2
Всього:		**16**

6. Теми лабораторних робіт

№ з/п	Назва теми	Кількість годин
1	Лабораторна робота №1. Аналіз методів і засобів несанкціонованого здобуття інформації	2
2	Лабораторна робота №2. Використання засобів захисту електронних таблиць	2
3	Лабораторна робота №3. Використання стандартних засобів захисту та зламу захисту PDF-документів	2
4	Лабораторна робота №4. Апаратні засоби захисту інформації в комп'ютерних системах	2
5	Лабораторна робота №5. Аналіз ефективності парольного захисту PDF-документів, архівів у різних форматах, текстових документів та електронних таблиць. Створення стійких паролів	2
6	Лабораторна робота №6. Класичні техніки шифрування. Шифр Цезаря	2
7	Лабораторна робота №7. Класичні шифри та криптоаналіз.	2
8	Лабораторна робота №8. Застосування криптографічних засобів захисту інформації. Генерування і використання електронного цифрового підпису для реалізації захисту файлів користувача	2
9	Лабораторна робота №9. Використання облікових записів користувачів та груп для захисту від комп'ютерних вірусів	2

	на рівні операційної системи за допомогою реалізації політик безпеки з обмеженими правами доступу	
10	Лабораторна робота №10. Налаштування рівнів безпеки сучасних браузерів	2
11	Лабораторна робота №11. Встановлення, налаштування та обслуговування програм-антивірусів	2
12	Лабораторна робота №12. Використання програм віддаленого керування	2
Всього:		**24**

7. Самостійна робота

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

№ з/п	Назва теми та питання (змістовий модуль)	К-ть годин	Форми контролю
1.	**Тема №1. Основи інформаційної безпеки та захисту даних у комп'ютерних системах** – Що таке інформаційна безпека? Які її основні цілі? – Які основні поняття захисту інформації та інформаційної безпеки? – Як класифікуються загрози інформаційній безпеці? Наведіть приклади технічних, соціальних та природних загроз. – Що таке оцінка ризиків та вразливостей? Які методи використовуються для оцінки ризиків? – Які існують методи захисту інформації? Наведіть приклади їх застосування. – Проаналізуйте реальні інциденти у сфері інформаційної безпеки – Які висновки можна зробити з цих прикладів? – Які сучасні тенденції спостерігаються в інформаційній безпеці? – Які основні поняття захисту інформації в автоматизованих системах? – Які загрози безпеці даних існують? У чому їх особливості? – Що таке дублювання інформації? Як воно допомагає підвищити надійність комп'ютерних систем?	4	Опитування, опрацювання фахових видань відповідно до теми лекції та підготовка реферату.

	– Як блокування помилкових операцій сприяє захисту інформації? – Які заходи можна вжити для оптимізації взаємодії користувачів і обслуговуючого персоналу з комп'ютерними системами? – Як мінімізувати збитки від аварій і стихійних лих у комп'ютерних системах? – Наведіть приклади заходів, які підвищують надійність комп'ютерних систем.		
2.	**Тема №2. Основи контролю доступу в інформаційних системах.** – Що таке ідентифікація, аутентифікація та аудит? Яка роль кожного з цих процесів у забезпеченні безпеки комп'ютерних систем? – Які основні етапи процесу аутентифікації? Які методи аутентифікації існують? – Які типи облікових записів користувачів існують у комп'ютерних системах? Які особливості кожного з них? – Які ролі та права доступу пов'язані з адміністративними, стандартними та гостьовими обліковими записами? – Яким чином відбувається процес авторизації після успішної аутентифікації? – Які приклади механізмів аутентифікації ви знаєте? Які переваги та недоліки кожного з них? – Як біометричні методи аутентифікації відрізняються від традиційних методів, таких як паролі? – Які основні принципи аудиту дій користувачів у комп'ютерних системах? Чому аудит є важливим для безпеки системи?	6	
3.	**Тема №3. Політики безпеки** – Що таке політика безпеки? Які основні елементи вона включає? – Яке значення має політика безпеки для захисту інформації та управління ризиками в організації? – Яка структура політики безпеки організації? Які компоненти є найважливішими? – Які основні принципи базової політики безпеки? Які вимоги вона ставить до співробітників? – Що таке спеціалізовані політики безпеки? Наведіть приклади таких політик та їх значення.	4	

	– Які процедури безпеки реалізують політики безпеки на практиці? Які заходи реагування на інциденти можуть бути включені? – Як політика безпеки взаємодіє з іншими політиками організації? Чому це важливо? – Які основні виклики можуть виникнути при впровадженні політики безпеки в організації?	
4.	**Тема №4. Криптографічні системи та криптографічні методи захисту.** – Що таке криптографія? Які основні терміни та поняття, пов'язані з криптографією, ви знаєте? – Яка історія розвитку криптографії? Які ключові етапи можна виділити в її еволюції? – Які законодавчі аспекти регулюють використання криптографії в різних країнах? – Які основні відмінності між симетричними та асиметричними криптографічними системами? – Які особливості використання криптографії в інформаційних технологіях? – Що таке модулярна арифметика, і як вона застосовується в криптографії? – Наведіть приклади використання модулярної арифметики в криптографічних алгоритмах. – Які основні криптографічні алгоритми ви знаєте? Які їхні переваги та недоліки?	6
5.	**Тема №5. Класичні методи шифрування** – Що таке шифр Цезаря? Який принцип його роботи та які його основні характеристики? – Які переваги та недоліки має шифр Цезаря в контексті криптографії? – Яким чином працює шифр Віженера? Які особливості його використання в порівнянні з шифром Цезаря? – Які переваги та недоліки має шифр Віженера? У яких випадках його доцільно використовувати? – Що таке шифр заміни? Які його основні принципи та методи реалізації? – Які переваги та недоліки мають класичні методи шифрування в сучасному контексті? – Наведіть приклади практичного застосування класичних шифрів у різних сферах.	6

	– Які основні методи криптоаналізу використовуються для зламу класичних шифрів?	
6.	**Тема №6. Симетричні та асиметричні методи шифрування. ЕЦП.** – Що таке симетричне шифрування? Які основні принципи роботи симетричних алгоритмів, таких як AES та DES? – Які переваги та недоліки симетричного шифрування? У яких випадках його доцільно використовувати? – Що таке асиметричне шифрування? Які основні принципи роботи асиметричних алгоритмів, таких як RSA та ECC? – Які переваги та недоліки асиметричного шифрування? Чому асиметричні методи важливі для сучасних систем безпеки? – Як симетричні та асиметричні методи шифрування взаємодіють у сучасних криптографічних системах? – Які приклади використання асиметричних методів у сучасних системах безпеки ви знаєте? – Які основні фактори слід враховувати при виборі між симетричними та асиметричними методами шифрування? – Які сучасні тенденції в розвитку симетричних та асиметричних алгоритмів шифрування? – Що таке електронний цифровий підпис (ЕЦП) і які його основні функції? – Які технології використовуються для створення та перевірки ЕЦП? Які етапи цього процесу? – Які переваги надає використання ЕЦП в електронному документообігу? – У яких сферах, окрім електронного документообігу, застосовується ЕЦП? Наведіть приклади. – Які правові аспекти регулюють використання електронних підписів в Україні? – Як ЕЦП прирівнюється до власноручного підпису або печатки з правового погляду? – Які основні види електронних підписів існують, і в чому їхні відмінності? – Які виклики та ризики пов'язані з	6

	використанням електронних цифрових підписів?		
7.	**Тема №7. Моделі безпеки операційних систем. Захист інформації в мережах** – Що таке моделі безпеки в контексті операційних систем? Яка їхня роль у забезпеченні безпеки? – Які основні моделі безпеки ви знаєте? Опишіть модель Біббера, модель Латтера та модель Bell-LaPadula. – Які основні загрози для інформації в мережах існують? Як вони можуть вплинути на безпеку систем? – Що таке атака типу «відмова в обслуговуванні» (DoS) і які її наслідки? – Які методи захисту інформації в мережах ви знаєте? Як фаєрволи, шифрування даних та аутентифікація користувачів допомагають у захисті? – Яка роль політик безпеки в управлінні ризиками та забезпеченні безпеки мережевих ресурсів? – Як моделі безпеки можуть бути адаптовані для захисту інформації в сучасних мережах? – Які виклики стоять перед організаціями при впровадженні моделей безпеки в операційних системах?	7	
8.	**Тема №8. Аудит об'єктів інформаційної безпеки. Аналіз ризиків корпоративних інформаційних систем** – Що таке аудит інформаційної безпеки? Які основні цілі та завдання аудиту? – Які основні етапи процесу аудиту інформаційної безпеки? Опишіть кожен з них. – Що таке ризик в контексті інформаційної безпеки? Як визначається ймовірність виникнення загрози та її вплив на інформаційні активи? – Які основні етапи аналізу ризиків корпоративних інформаційних систем? Опишіть кожен з них. – Яким чином розробляється стратегія управління ризиками? Які заходи можуть бути застосовані для зменшення ризиків до прийнятного рівня? – Які нормативні вимоги та стандарти	11	

	регулюють процес аудиту інформаційної безпеки? Наведіть приклади.,,, – Які інструменти та методики використовуються для проведення аудиту інформаційної безпеки? Наведіть приклади. – Які основні виклики та складнощі можуть виникати при проведенні аудиту інформаційної безпеки? Як їх можна подолати?		
	Разом	**50**	

8. Форми роботи та критерії оцінювання

Рейтинговий контроль знань студентів здійснюється за 100-бальною шкалою:

Шкала оцінювання: національна та ECTS

ОЦІНКА ЄКТС	СУМА БАЛІВ	ОЦІНКА ЗА НАЦІОНАЛЬНОЮ ШКАЛОЮ	
		екзамен	залік
A	90-100	5 (відмінно)	5/відм./зараховано
B	80-89	4 (добре)	4/добре/ зараховано
C	65-79		
D	55-64	3 (задовільно)	3/задов./ зараховано
E	50-54		
FX	35-49	2 (незадовільно)	Не зараховано
F*	1-34	2 (незадовільно)	Не зараховано

Форми поточного та підсумкового контролю.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

–Методи усного контролю: індивідуальне опитування, фронтальне опитування, співбесіда, іспит.

–Комп'ютерного контролю: програми - емулятори.

–Методи самоконтролю: уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

–систематичність відвідування занять;

–своєчасність виконання навчальних і індивідуальних завдань;

–повний обсяг їх виконання;

–якість виконання навчальних і індивідуальних завдань;

–самостійність виконання;

–творчий підхід у виконанні завдань;

–ініціативність у навчальній діяльності;

–виконання тестових завдань.

Усі форми контролю включено до 100-бальної шкали оцінювання.

Оцінювання результатів поточної роботи (завдань, що виконуються на лабораторних заняттях, результати самостійної роботи студентів) проводиться за такими критеріями:

Лабораторні роботи (у % від кількості балів, виділених на завдання із заокругленням до цілого числа):

0% - завдання не виконано;

40% - завдання виконано частково та містить суттєві помилки методичного та розрахункового характеру;

60% - завдання виконано повністю, але містить суттєві помилки у розрахунках або методиці;

80% - завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (розмірності, висновки, оформлення тощо);

100% - завдання виконано правильно, вчасно і без зауважень.

Критерії оцінювання відповідей на лабораторних заняттях:

Студенту виставляється **відмінно**, якщо студент здатний самостійно здійснювати основні види навчальної діяльності. Знання студента є глибокими, міцними, узагальненими; студент вміє застосовувати знання творчо, його навчальна діяльність позначена вмінням самостійно оцінювати різноманітні життєві ситуації, явища, факти, виявляти і відстоювати особисту позицію.

Студенту виставляється **добре**, якщо студент знає істотні ознаки понять, явищ, закономірностей, зв'язків між ними, а також самостійно застосовує знання в нестандартних ситуаціях, володіє розумовими операціями, вміє робити висновки, виправляти допущені помилки. Відповідь повна, правильна, логічна, обґрунтована. Якщо студент знає ознаки понять, явищ, закономірностей, зв'язків між ними на середньому рівні, а також самостійно застосовує знання в стандартних ситуаціях, володіє розумовими операціями, вміє робити висновки, виправляти допущені помилки. Відповідь повна, правильна, логічна, обґрунтована.

Студенту виставляється **задовільно**, якщо відповідь студента при відтворенні навчального матеріалу елементарна, зумовлюється початковими уявленнями про предмет вивчення. Студент відтворює основний навчальний матеріал.

Відповідний **розподіл балів, які отримують студенти** за 3 кредитами.

Оцінювання 3 кредитів = 150 – 300 балів

Поточне тестування та самостійна робота								Накопичувальні бали/Сума
Кредит1			Кредит2			Кредит3		150 –300
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	
30	30	40	30	30	40	50	50	

9. Засоби діагностики

Засобами діагностики та методами демонстрування результатів навчання є: завдання до практичних занять, завдання для самостійної роботи (реферати, творчі завдання, термінологічний словник), контрольні роботи, поточне опитування, тестування, перевірка лекційних зошитів.

Форма підсумкового контролю успішності навчання: іспит.

Підсумкове оцінювання у 8-му семестрі здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Іспит оцінюється у 40 балів за розподілом: 20 балів – комплексний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з побудови інформаційних мереж та управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для побудови захищених інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем.

Бали за виконання тесту та бали за виконання практичного завдання додаються.

Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

10. Методи навчання

1.Методи організації та здійснення навчально-пізнавальної діяльності:

1) словесні: метод пояснення, метод розповіді, метод лекції, метод бесіди (вступної бесіди, бесіди-повідомлення, бесіди-повторення, контрольної бесіди, репродуктивної бесіди, евристичної бесіди, катехізисної бесіди);

2) наочні методи навчання: метод ілюстрування, метод демонстрування, самостійне спостереження;

3) практичні методи навчання: вправи, практичні роботи, дослідні роботи.

2. Методи стимулювання навчальної діяльності студентів: метод навчальної дискусії, метод забезпечення успіху в навчанні, метод пізнавальних ігор, метод створення ситуації інтересу в процесі викладання навчального матеріалу, метод створення ситуації новизни навчального матеріалу.
3. Методи стимулювання обов'язку і відповідальності в навчанні.

11. Список рекомендованої літератури:

Базова

1. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. К.: МОУ, 2009. 456 с.
2. Богуш В.М., Юдін О.К. Основи інформаційної безпеки держави. К.: "МК-Прес", 2005. 432 с.
3. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. К. : ДУТ - КНУ, 2016. 178 с.
5. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.
6. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. К: ДУТ, 2015. 345 с.
7. Вербіцький О. В. Вступ до криптології. Львів: ВНТЛ, 1998. 248 с.
8. ДСТУ 2462--94. Сертифікація. Основні поняття. Терміни та визначення.- К.: Держстандарт України, 1994. - 24 с.
9. ДСТУ 2874--94. Системи обробки інформації. Бази даних. Терміни та визначення.
10. ДСТУ 2938--94. Системи оброблення інформації. Основні поняття. Терміни та визначення.
11. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
12. Комп'ютерні мережі: навч. посіб. для технічних спец. вищих навч. закл. Кн. 2. - Львів: Магнолія 2006, 2014. - 327 с.
13. Пономаренко В.С. Основи захисту інформації. Навчальний посібник Харків: Вид. ХДЕУ, 2003. 176 с.

Допоміжна література

1. International Standard ISO 7498-2: 1989 Information processing systems. Open Systems Interconnection. - Basic Reference Model. - Part 2: Security Architecture. First edition. 15.02.1989.
2. International Standard ISO/IEC 17799. Information technology - Code of practice for information security management. First edition 2000-12-01.
3. Panoc C. Lekkas. Network Processors. The McGraw-Hill Companies, 2003.
4. Scott Mueller. Upgrading and Repairing Networks, Third Edition. Que, 2002.
5. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи. К.:

Видавничий дім "СофтПрес", 2005. 316 с.
6. ДСТУ 2226--93. Автоматизовані системи. Терміни та визначення.

Інформаційні ресурси

1. An improved algorithm for CIOQ switches. Yossi Azar, Ybssi Richter. http://portal.acm.org
2. Andreas D. Bovopoulos and Micha Zeiger. Shared-Memory Fabrics Meet 10-Gbit Backplane Demands. TeraChip, Inc. http://www.commsdesign.com
3. Evolution: 20 years of switching fabric. Ori Aruj, Dune Networks http://www.commsdesign.com
4. History of LAN Switching. http://www.myipaddressinfo.com
5. http://bezopasnost.biz.
6. http://dstszi.gov.ua.
7. http://it.ridne.net
8. Institute of Electrical and Electronics Engineers) http://www.ieee.org
9. Matching Output Queueing with a Combined Input Output Queued Switch http://www-rcf.usc.edu
10. On-chip Global Interconnects for Networking ASICs http://www.lsi.com