ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ВІННИЦЬКИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ ІНСТИТУТ

СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Сертифікована на відповідність ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT)

Кафедра економічної кібернетики та інформаційних систем

ЗАТВЕРДЖЕНО
Постанова вченої ради
29.05.2023
протокол № 07, п. 8

ВВЕДЕНО В ДІЮ
Наказ від 29.05.2023 № 70

БЕЗПЕКА ІНТЕГРОВАНИХ ТА РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ/ SECURITY OF INTEGRATED AND DISTRIBUTED INFORMATION SYSTEMS

РОБОЧА ПРОГРАМА

Ступінь вищої освіти	«Магістр» /	«Master»
Галузь знань	12 «Інформаційні технології» /	«Information Technology»
Спеціальність	126 «Інформаційні системи та технології» /	«Information systems and technologies»
Освітня програма	«Інформаційні технології у бізнесі» /	«Information technology in business»

Вінниця 2023

Розробник: Новицький Руслан, кандидат технічних наук, доцент

Гарант освітньої програми «Інформаційні технології у бізнесі» - Вадим Романюк, доктор технічних наук, професор ew

Обговорено та схвалено на засіданні кафедри економічної кібернетики та інформаційних систем від 04.05.2023 р. пр. № 08; на засіданні вченої ради факультету економіки, менеджменту та права від 16.05.2023 р. пр. № 05.

Рецензенти:

Кузьміна Олена, кандидат технічних наук, доцент;
Вапняр Олена, директор ТОВ «Універсальний сервіс»

Редактор: Фатєєва Т.
Комп'ютерна верстка: Тимощук М.

Підп. до друку 01.06.2023. Формат 60х84/16. Папір офсетний
Друк ксероксний. Ум. друк. арк. 0,93.
Обл.-вид. арк. 0,66. Тираж 2. Зам. № 215.

Редакційно-видавничий відділ ВТЕІ ДТЕУ
21000, м. Вінниця, вул. Хмельницьке шосе, 25

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ:

Мета вивчення дисципліни.

Навчання принципам організації та забезпечення безпеки інтегрованих та розподілених інформаційних систем, здобуття поглиблених теоретичних знань, практичних навичок, та умінь у галузі інформаційної безпеки розподілених систем для успішного виконання ними професійних обов'язків за спеціальністю «Інформаційні системи і технології», освітня програма «Інформаційні технології у бізнесі».

Результати вивчення навчальної дисципліни її місце в освітньому процесі.

В результаті вивчення дисципліни студенти повинні вміти застосовувати теоретичний матеріал і володіти практичними навичками з безпеки інтегрованих та розподілених інформаційних систем для успішного розв'язування складних спеціалізованих задач та практичних проблем під час професійної діяльності у галузі інформаційних систем та технологій або у процесі навчання, що передбачає застосування теорій та методів відповідної навчальної дисципліни.

Результатом вивчення навчальної дисципліни «Безпека інтегрованих та розподілених інформаційних систем» для освітньої програми «Інформаційні технології у бізнесі» є формування комплексу компетентностей:

- **інтегральна компетентність:**

Здатність розв'язувати задачі дослідницького та інноваційного характеру у сфері інформаційних систем та технологій.

- **загальні компетентності:**

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК02. Здатність спілкуватися іноземною мовою.

ЗК03. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

ЗК04. Здатність розробляти проекти та управляти ними.

- **фахові (спеціальні) компетентності:**

СК01. Здатність розробляти і застосовувати ІСТ, необхідні для розв'язання стратегічних і поточних задач.

СК03. Здатність проектувати інформаційні системи з урахуванням особливостей їх призначення, неповної/недостатньої інформації та суперечливих вимог.

СК04. Здатність розробляти математичні, інформаційні та комп'ютерні моделі об'єктів і процесів інформатизації.

СК06. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

СК07. Розробляти і реалізовувати інноваційні проекти у сфері ІСТ.

Програмні результати навчання здобувачів з навчальної дисципліни «Безпека інтегрованих та розподілених інформаційних систем» полягають:

ПРН01. Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію.

ПРН03. Приймати ефективні рішення з проблем розвитку інформаційної інфраструктури, створення і застосування ІСТ.

ПРН07. Здійснювати обґрунтований вибір проектних рішень та проектувати сервіс-орієнтовану інформаційну архітектуру підприємства (установи, організації тощо).

ПРН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.

ПРН11. Розв’язувати задачі цифрової трансформації у нових або невідомих середовищах на основі спеціалізованих концептуальних знань, що включають сучасні наукові здобутки у сфері інформаційних технологій, досліджень та інтеграції знань з різних галузей.

Міждисциплінарні зв'язки: програма упорядкована відповідно до анотації освітньо-професійної програми підготовки магістрів, базується на вивченні таких нормативних дисциплін, як «Кібербезпека», «Проектування інформаційних систем».

Критерії оцінювання результатів навчання

Критерієм успішного проходження здобувачем освіти підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни. Мінімальний пороговий рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати його в мінімальну позитивну оцінку використовуваної числової (рейтингової) шкали.

Рівні компетентності	За шкалою ДТЕУ	Критерії оцінювання
1	2	3
Високий (дослідницький)	90-100	Має обґрунтовані та всебічні знання з дисципліни, вміє узагальнювати та систематизувати набуті знання; самостійно знаходить джерела інформації та працює з ними; проводить власні дослідження, може використовувати набуті знання та вміння при розв'язанні задач.
Достатній (частково-пошуковий)	82-89	Володіє навчальним матеріалом, вміє зіставляти та узагальнювати, виявляє творчий інтерес до предмету, виконує завдання з повним поясненням та обґрунтуванням, але допускає незначні помилки; може усвідомити нові для нього факти, ідеї.
	75-81	Володіє визначеним програмою навчальним матеріалом; розв'язує завдання, передбачені програмою, з частковим поясненням.
Елементарний (репродуктивний)	69-74	Володіє навчальним матеріалом на репродуктивному рівні; може самостійно розв'язати та пояснити розв'язання завдання.
	60-68	Ознайомлений з навчальним матеріалом, відтворює його на репродуктивному рівні; виконує елементарні завдання за зразком або відомим алгоритмом.
Низький (фрагментарний)	35-59	Ознайомлений та відтворює навчальний матеріал на рівні окремих фактів та фрагментів матеріалу; під керівництвом викладача виконує елементарні завдання.
	1-34	Ознайомлений з навчальним матеріалом на рівні розпізнавання та відтворення окремих фактів.

Здобувачі вищої освіти, які повністю виконали програму дисципліни та набрали достатню кількість балів, отримують підсумкову оцінку без опитування чи виконання екзаменаційного завдання (згідно з Положенням Про оцінювання результатів навчання здобувачів вищої освіти №12 від 07.02.2022).

У разі, якщо здобувач вищої освіти бажає поліпшити свою оцінку, або не набрав 75 балів, він складає екзамен з усієї програми навчальної дисципліни у вигляді письмового опитування знань згідно завдань встановленого зразка.

Результат виконання екзаменаційних завдань оцінюється з урахуванням результатів у співвідношенні 80:20, де 80 – максимальна оцінка за виконання екзаменаційного завдання, 20 – результат поточної успішності відповідно до шкали переводу поточної роботи для врахування її при підсумковій оцінці.

Здобувач вищої освіти, який не погоджується з оцінкою, отриманою під час підсумкового (семестрового) контролю, має право звернутися із проханням переглянути оцінку, одержану на екзамені (згідно Положення про апеляцію результатів підсумкового контролю знань студентів №32 від 07.02.2022).

Обсяг дисципліни в кредитах та його розподіл (тематичний план)

Назва теми	Кількість годин				Форми контролю
	Усього годин / редитів	з них			
		лекції	лабораторні заняття	самостійна робота студентів	
Тема 1. Предмет та завдання дисципліни. Поняття інтегрованої та розподіленої інформаційних систем	14	2		12	ДН
Тема 2. Архітектура та складові частини систем захисту інформації. Об'єкти захисту розподілених інформаційних систем	18	2	4	12	ДН, РІЗ, ОЗІЗ,
Тема 3. Основні джерела небезпек для розподілених інформаційних систем. Міжнародні та корпоративні стандарти захисту розподілених інформаційних систем	18	2	4	12	ДН, РІЗ, ОЗІЗ,
Тема 4. Методи та засоби інформаційної безпеки в розподілених інформаційних системах	18	2	4	12	ДН, РІЗ, ОЗІЗ,
Тема 5. Криптографічні методи захисту інформації. Сучасні симетричні криптосистеми	18	2	4	12	ДН, РІЗ, ОЗІЗ,
Тема 6. Криптографічні методи захисту інформації. Асиметричні криптосистеми	18	2	4	12	ДН, РІЗ, ОЗІЗ, Т
Тема 7. Аутентифікація та ідентифікація об'єктів та суб'єктів розподіленої інформаційної системи. Електронний цифровий підпис	20	2	4	14	ДН, РІЗ, ОЗІЗ,
Тема 8. Мережа та безпека інформації. Вплив типу та архітектури мережі на безпеку інформації. Огляд безпеки протоколів обміну даними	18	2	4	12	ДН, РІЗ, ОЗІЗ,
Тема 9. Безпека каналів передачі даних. Віртуальні мережі. Мережеві екрани	18	2	4	12	ДН, РІЗ, ОЗІЗ,
Тема 10. Безпека комерційних операцій в Internet. Основи технології блокчейн	20	2	4	14	ДН, РІЗ, ОЗІЗ, Т
Разом	**180**	**20**	**36**	**124**	
Підсумковий контроль – екзамен					

Умовні позначення: Т – тестування, ДН – використання системи дистанційного навчання, РІЗ – розв’язання індивідуальної практичної задачі в електронному вигляді, ОЗІЗ – оформлення звіту та захист індивідуального завдання

ІІ. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТ ДИСЦИПЛІНИ (теми програми).

Тема 1. **Предмет та завдання дисципліни. Поняття інтегрованої та розподіленої інформаційних систем**

Предмет та завдання дисципліни. Поняття централізованого та розподіленого інформаційних ресурсів. Проблеми створення розподілених інформаційних ресурсів. Розподілені бази даних. Розподілений реєстр.

Тема 2. **Архітектура та складові частини систем захисту інформації. Об'єкти захисту розподілених інформаційних систем**

Архітектура мережі Інтернет. Загрози безпеці в інформаційних системах. Основні підходи до захисту інформації в інтегрованих і розподілених інформаційних системах. Об’єкти захисту.

Тема 3. **Основні джерела небезпек для розподілених інформаційних систем. Міжнародні та корпоративні стандарти захисту розподілених інформаційних систем**

Класифікація основних джерел небезпеки та видів загроз. Порівняльний аналіз стандартів інформаційної безпеки. Міжнародні стандарти серії ISO. Системи управління інформаційною безпекою. Принципи побудови збалансованої системи інформаційної безпеки.

Тема 4. **Методи та засоби інформаційної безпеки в розподілених інформаційних системах**

Класифікація методів і засобів інформаційної безпеки в інтегрованих та розподілених інформаційних системах. Їх переваги та недоліки. Апаратно-програмні засоби захисту.

Тема 5. **Криптографічні методи захисту інформації. Сучасні симетричні криптосистеми**

Характеристика алгоритмів шифрування. Принципи криптографічного захисту інформації. Основні вимоги до криптографічних систем захисту. Сучасні криптосистеми та їх особливості. Стандарти шифрування даних DES, IDEA. Блочні та потокові шифри.

Тема 6. **Криптографічні методи захисту інформації. Асиметричні криптосистеми**

Концепція криптосистем з відкритим ключем. Криптосистема шифрування даних RSA. Схема шифрування Поліга-Хеллмана. Схема шифрування Ель Гамаля. Комбінований метод шифрування.

Тема 7. **Аутентифікація та ідентифікація об'єктів та суб'єктів розподіленої інформаційної системи. Електронний цифровий підпис**

Системи автентифікації електронних даних. Ідентифікація та перевірка справжності. Типові схеми ідентифікації та автентифікації користувача. Електронний цифровий підпис (ЕЦП). Хеш-функції. Алгоритми ЕЦП.

Тема 8. **Мережа та безпека інформації. Вплив типу та архітектури мережі на безпеку інформації. Огляд безпеки протоколів обміну даними**

Безпека інформації в мережах: поняття, важливість, основні принципи Види мереж та огляд їх впливу на безпеку інформації. Архітектурні рішення для покращення безпеки мережі. Огляд основних протоколів обміну даними: TCP/IP, HTTP, SMTP, FTP і їх вразливості щодо безпеки.

Тема 9. **Безпека каналів передачі даних. Віртуальні мережі. Мережеві екрани**

Безпека каналів передачі даних: загальні поняття та основні принципи. Захист безпровідних мереж. Віртуальні приватні мережі (VPN). Використання мережевих екранів (firewalls) для захисту мережі: типи, функції, правила налаштування. Веб-проксі-сервери: фільтрація веб-трафіку, захист від вразливостей веб-додатків. Планування та реалізація безпеки мережі: аналіз загроз, розробка стратегій, впровадження та тестування заходів безпеки.

Тема 10. **Безпека комерційних операцій в Internet. Основи технології блокчейн**

Захист фінансових транзакцій в електронній комерції: електронні платежі, безпека банківських операцій, мобільні платежі. Захист особистих даних та конфіденційності в електронній комерції. Огляд технології блокчейн: поняття та принципи роботи. Безпека та захист в блокчейн-системах. Найпоширеніші блокчейни.

Структура навчальної дисципліни

Результати навчання	Навчальна діяльність	Робочий час студента, год
1	*2*	*3*
Знати: Основні характеристики і принципи функціонування інтегрованих та розподілених інформаційних систем **Вміти:** Використовувати технології та інструменти для забезпечення безпеки інтегрованих та розподілених інформаційних систем.	**Тема 1. Предмет та завдання дисципліни. Поняття інтегрованої та розподіленої інформаційних систем** **Лекція № 1** План лекції 1. Предмет та завдання дисципліни. Поняття централізованого та розподіленого інформаційних ресурсів. 2. Проблеми створення розподілених інформаційних ресурсів. 3. Розподілені бази даних. Розподілений реєстр. **Рекомендовані джерела:** Основна: 1-4. Додаткова: 6. Інтернет-ресурси: 13-17.	2
	Самостійна робота студентів. 1. Огляд методів і стратегій захисту інтегрованих та розподілених інформаційних систем. 2. Загрози та ризики, пов'язані з використанням інтегрованих та розподілених інформаційних систем.	12
Знати: 1. Концепції архітектури систем захисту інформації. 2. Різні типи об'єктів захисту в розподілених ІС. **Вміти:** 1. Визначати вимоги безпеки для різних типів об'єктів захисту. 2. Аналізувати та ідентифікувати вразливості й розробляти стратегії та рішення для захисту об'єктів захисту розподілених ІС.	**Тема 2. Архітектура та складові частини систем захисту інформації. Об'єкти захисту розподілених інформаційних систем** **Лекція № 2** План лекції 1. Архітектура мережі Інтернет. 2. Загрози безпеці в інформаційних системах. 3. Основні підходи до захисту інформації в інтегрованих і розподілених інформаційних системах. **Рекомендовані джерела:** Основна: 1-4. Додаткова: 7, 8. Інтернет-ресурси: 13, 14, 19.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	12
	Лабораторне заняття № 1. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2

	Лабораторне заняття № 2. Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2
Знати: 1. Основні джерела небезпек, що можуть впливати на розподілені інформаційні системи. 2. Основні принципи та вимоги, що містяться в міжнародних та корпоративних стандартах безпеки **Вміти:** 1. Визначати різні типи загроз для розподілених ІС. 2. Аналізувати та застосовувати відповідні стандарти безпеки для розподілених ІС залежно від їх потреб та характеристик.	**Тема 3. Основні джерела небезпек для розподілених інформаційних систем. Міжнародні та корпоративні стандарти захисту розподілених інформаційних систем** **Лекція № 3** План лекції 1. Класифікація основних джерел небезпеки та видів загроз. 2. Міжнародні стандарти серії ISO. 3. Системи управління інформаційною безпекою. 4. Принципи побудови збалансованої системи інформаційної безпеки **Рекомендовані джерела:** Основна: 1-4. Додаткова: 6, 7. Інтернет-ресурси: 9, 13-17.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	12
	Лабораторне заняття № 3. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2
	Лабораторне заняття № 4. Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2
Знати: 1. Основні методи захисту інформації в розподілених ІС. 2. Різні засоби захисту та актуальні технології й практики інформаційної безпеки. **Вміти:** 1. Вибирати і застосовувати відповідні методи та засоби захисту в залежності від потреб та вимог розподіленої ІС. 2. Використову-	**Тема 4. Методи та засоби інформаційної безпеки в розподілених інформаційних системах** **Лекція № 4** План лекції 1. Класифікація методів і засобів інформаційної безпеки в інтегрованих та розподілених інформаційних системах. 2. Апаратно-програмні засоби захисту **Рекомендовані джерела:** Основна: 1-4. Додаткова: 6, 7.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	12
	Лабораторне заняття № 5. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2

вати інструменти та платформ для реалізації методів та засобів захисту	**Лабораторне заняття № 6.** Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2
Знати: 1. Принципи криптографії та її роль у захисті інформації. 2. Основні поняття про симетричні криптосистеми і їхні принципи роботи. **Вміти:** 1. Вибирати і застосовувати відповідні симетричні криптосистеми залежно від вимог безпеки	**Тема 5. Криптографічні методи захисту інформації. Сучасні симетричні криптосистеми** **Лекція № 5** План лекції 1. Характеристика алгоритмів шифрування. 2. Принципи криптографічного захисту інформації. 3. Сучасні криптосистеми та їх особливості. **Рекомендовані джерела:** Основна: 1-5. Додаткова: 7. Інтернет-ресурси: 14, 18, 19.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	12
	Лабораторне заняття № 7. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2
	Лабораторне заняття № 8. Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2
Знати: 1. Основні поняття асиметричної криптографії. 2. Основні алгоритми асиметричного шифрування. **Вміти:** 1. Створювати та керувати ключами асиметричних криптосистем. 2. Застосовувати асиметричну криптографію та аналізувати її ефективність.	**Тема 6. Криптографічні методи захисту інформації. Асиметричні криптосистеми** **Лекція № 6** План лекції 1. Концепція криптосистем з відкритим ключем. 2. Криптосистема шифрування даних RSA. 3. Схема шифрування Поліга-Хеллмана. 4. Схема шифрування Ель Гамаля. **Рекомендовані джерела:** Основна: 1-5. Додаткова: 7. Інтернет-ресурси: 14, 18, 19.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	12
	Лабораторне заняття № 9. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2
	Лабораторне заняття № 10. Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2

Знати: 1. Основні методи та протоколи аутентифікації. 2. Основні алгоритми ЕЦП та їх використання. **Вміти:** 1. Вибирати та застосовувати відповідні методи аутентифікації залежно від потреб і вимог безпеки системи. 2. Генерувати та перевіряти електронні цифрові підписи	**Тема 7. Аутентифікація та ідентифікація об'єктів та суб'єктів розподіленої інформаційної системи. Електронний цифровий підпис** **Лекція № 7.** План лекції 1. Системи автентифікації електронних даних. 2. Типові схеми ідентифікації та автентифікації користувача. 3. Електронний цифровий підпис (ЕЦП). **Рекомендовані джерела:** Основна: 1-5. Додаткова: 6, 7. Інтернет-ресурси: 11-19.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	14
	Лабораторне заняття № 11. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2
	Лабораторне заняття № 12. Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2
Знати: 1. Основні типи загроз та вразливостей, які пов'язані з різними типами мереж і архітектурою. 2. Основні мережеві протоколи та їх безпеку. **Вміти:** 1. Оцінювати ризики та застосовувати відповідні заходи безпеки для різних типів мереж. 2. Аналізувати та використовувати інструменти для моніторингу та виявлення загроз у мережевому середовищі.	**Тема 8. Мережа та безпека інформації. Вплив типу та архітектури мережі на безпеку інформації. Огляд безпеки протоколів обміну даними** **Лекція № 8.** План лекції 1. Види мереж та огляд їх впливу на безпеку інформації. 2. Архітектурні рішення для покращення безпеки мережі. 3. Основні протоколи обміну даними та їх безпека. **Рекомендовані джерела:** Основна: 1-5. Додаткова: 6-8. Інтернет-ресурси: 9.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	12
	Лабораторне заняття № 13. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2
	Лабораторне заняття № 14. Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2

Знати: 1. Про загрози, пов'язані з каналами передачі даних, та способи їх запобігання 2. Протоколи та механізми безпеки, що використовуються в безпекових каналах передачі даних 3. Технології шифрування, які застосовуються у безпекових каналах передачі даних. **Вміти:** 1. Налаштовувати віртуальні мережі та мережеві екрани для забезпечення конфіденційності та захисту даних	**Тема 9. Безпека каналів передачі даних. Віртуальні мережі. Мережеві екрани** **Лекція № 9.** План лекції 1. Безпека каналів передачі даних 2. Захист безпровідних мереж. Віртуальні приватні мережі (VPN). 3. Мережеві екрани для захисту мережі. Веб-проксі-сервери. 4. Планування та реалізація безпеки мережі. **Рекомендовані джерела:** Основна: 1-5. Додаткова: 7, 8. Інтернет-ресурси: 9, 14.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	12
	Лабораторне заняття № 15. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2
	Лабораторне заняття № 16. Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2
Знати: 1. Про загрози, пов'язані з електронною комерцією, та способи їх запобігання. 2. Основні поняття технології блокчейн і її застосування в контексті безпеки комерційних операцій. **Вміти:** 1. Оцінювати ризики та вибирати відповідні механізми захисту для комерційних операцій в Інтернеті.	**Тема 10. Безпека комерційних операцій в Internet. Основи технології блокчейн** **Лекція № 10.** План лекції 1. Захист фінансових транзакцій в електронній комерції. 2. Захист особистих даних та конфіденційності в електронній комерції. 3. Технології блокчейн. **Рекомендовані джерела:** Основна: 1-5. Додаткова: 6-8. Інтернет-ресурси: 10, 12-14.	2
	Самостійна робота студентів. Вивчення та доповнення матеріалу лекції. Підготовка до виконання завдань лабораторної роботи та оформлення звіту.	14
	Лабораторне заняття № 17. Питання / завдання до заняття 1. Опрацювати теоретичні відомості. 2. Дати відповіді на контрольні запитання.	2
	Лабораторне заняття № 18. Питання / завдання до заняття 1. Виконати завдання до лабораторного заняття. 2. Оформити звіт та захистити викладачу.	2
ВСЬОГО:		**180/6**

ІІІ. РЕКОМЕНДОВАНІ ДЖЕРЕЛА

Основні:

1. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
2. Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0.
4. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
5. Євсеєв С.П. Кібербезпека: Криптографія з Python: навчальний посібник. – Львів “Новий світ-2000”, 2021. – 120 с.

Додаткові:

6. Економічна безпека підприємства [Текст] : навч. посіб. / Т.М. Іванюта, А.О. Заїчковський. – Київ : Центр учбової літератури, 2017. – 256 с. – 978-611-01-0978-9.
7. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем [Електронний ресурс] : підручник / М. В. Грайворонський, О. М. Новіков. – Електронні текстові дані (1 файл: 8,54 Мбайт). – Київ : Видавнича група BHV, 2009. – 698 с.
8. Кулаков, Ю. О. Комп’ютерні мережі [Електронний ресурс] : навчальний посібник для здобувачів ступеня магістра за освітньою програмою «Комп’ютерні системи та мережі» спеціальності 123 Комп’ютерна інженерія / Кулаков Ю. О. ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 18,3 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 247 с. – Назва з екрана.

Інтернет-ресурси:

9. ISO [Електронний ресурс] // Офіційний сайт ISO. – Режим доступу: http://www.iso.org/iso/home.htm.
10. Nakamoto S.. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. URL: https://bitcoin.org/bitcoin.pdf (дата звернення 01.11.2019).
11. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. №851-IV. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T030851.html
12. Про електронний цифровий підпис: Закон України від 22 травня 2003 р. №851-IV. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T030852.html

13. Про захист інформації в автоматизованих системах. Закон України від 05.07.94р. / *Відомості Верховної Ради України.* 1994.

14. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 31.05.2005 №2594-IV-ВР. / База даних «Законодавство України. URL: http://zakon4.rada.gov.ua/laws/show/80/94

15. Про національну програму інформатизації: Закон України від 04.02.1998 №74/98 – ВР. / *Відомості Верховної Ради України*. 1998. №27-28. Ст. 181.

16. Про основні засади розвитку інформаційного суспільства в Україні 2007-2015 роки: Закон України від 09 січня 2007. / *Відомості Верховної Ради України*. 2007. № 12. – Ст. 102.

17. Про основи національної безпеки України: Закон України від 19 червня 2003 р. / *Голос України*. 2003. №134.

18. Про порядок здійснення криптографічного захисту інформації в Україні: Указ президента України від 22 травня 1998 р. №505/98. URL: http://www.uapravo.net/akty/ministerstvo-main/akt9pprs7f.htm

19. Про положення про технічний захист інформації в Україні: Указ президента України від 27 вересня 1999 р. №1229. / База даних «Законодавство України. URL: http://zakon4.rada.gov.ua/laws/show/1229/99