МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
обов'язкового освітнього компонента

ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА КРИПТОВАЛЮТА

галузь знань **12** Інформаційні технології

підготовки бакалавра

спеціальності 125 Кібербезпека та захист інформації

освітньо-професійної програми Кібербезпека та захист інформації

Луцьк – 2024

Силабус навчальної дисципліни «Технології блокчейн та криптовалюта**»** підготовки бакалаврів галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації за освітньою програмою Кібербезпека та захист інформації

Розробник: доцент, кандидат технічних наук Онищук Оксана Олександрівна

Погоджено

Гарант освітньо-професійної програми:  Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 4 від 21.11.2024 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Загальна кількість годин / кредит – 120/4</td><td rowspan="9">Галузь знань
12 «Інформаційні технології»
Спеціальність
125 Кібербезпека та захист інформації
освітньо-професійна програма
Кібербезпека та захист інформації</td><td>Обов’язкова компонента ОП</td></tr>
<tr><td rowspan="8">Змістових модулів – 2, аудиторних 72 год</td><td>Рік підготовки: 4</td></tr>
<tr><td>Семестр: 8-й</td></tr>
<tr><td>Лекції: 30 год.</td></tr>
<tr><td>Консультація: 8 год.</td></tr>
<tr><td>Лабораторні: 42 год.</td></tr>
<tr><td>Самостійна робота: 40 год.</td></tr>
<tr><td>Вид контролю екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить: для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи;

ІІ. Інформація про викладачів

ПІП Онищук Оксана Олександрівна
Науковий ступінь кандидат технічних наук
Вчене звання доцент
Посада доцент кафедри комп’ютерних наук та кібербезпеки

Контактна інформація	(096) 6943585,onyshchuk.oksana@vnu.edu.ua
Дні занять	за розкладом http://94.130.69.82/cgi-bin/timetable.cgi?n=700

III. Опис освітнього компонента

Курс «Технології блокчейн та криптовалюта» є обов'язковим освітнім компонентом освітньо-професійної програми «Кібербезпека та захист інформації» бакалаврського рівня. Дана дисципліна спрямована на підвищення рівня формування у студентів знань та умінь, які дадуть теоретичний і практичний фундамент розуміння принципів функціонування та використання в професійній діяльності проектування систем кібербезпеки та сучасних систем технічного захисту.

IV. Мета і завдання освітнього компонента

Метою навчальної дисципліни є ознайомлення студентів з сутністю, задачами, принципами та сучасними технологіями блокчейну, хмарних обчислень , електронних платежів та криптовалюти.

Завданнями вивчення навчальної дисципліни є формування спеціалізованих концептуальних знань, що включають сучасні наукові здобутки у сфері професійної діяльності та інформаційних технологій і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем технологій блокчейну, , хмарних обчислень, електронних платежів та криптовалюти. Для формування спеціалізованих умінь/навичок розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур: оволодіння етапами технології блокчейну та хмарних обчислень; розуміння головних задач криптовалюти; оволодіння методологічними та законодавчими основами організації, планування, проектування, впровадження, експлуатації та супроводу роботи крипто гаманців; для формування здатності інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах; вивчення основних принципів, засад та методів організаційного та технічного використання електронних гаманців та криптобірж.; оволодіння методами та технологіями електронних платежів.

Для формування здатності розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням електронних підписів та дизруптивних технологій: ChatGPT та валютних ринків .

.

V. Результати навчання та компетентності

Зміст освітньої компоненти направлений на формування наступних компетентностей, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації»:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності

СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
СК 4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
Отримані знання з навчальної дисципліни стануть складовими наступних програмних результатів навчання за спеціальністю 125 «Кібербезпека та захист інформації»:
РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.
РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

VI. Програма навчальної дисципліни

Змістовий модуль 1. Хмарні обчислення. Види блокчейнів.

Тема 1. Характеристика хмарних обчислень.Типи хмарних моделей. Моделі хмарних обчислень. Переваги хмарних обчислень. Недоліки хмарних обчислень.

Тема 2. Використання хеш функції. Дерево Меркла. Спеціальні транзакції. Hard & Soft fork. Обмеження блокчейну. Приватний та публічний блокчейн. Цифровий підпис до блокчейну: підпис транзакцій, підтвердження роботи.

Тема 3. Види криптовалют та механізми консенсусу.

Тема 4. Зберігання та використання криптовалют. Одноосібне управління. Зберігання ключів. Мульти Підписи .Сторонні послуги для використання криптовалют. Платежі. Огляд гаманців.

Змістовий модуль 2. Цифрові криптовалютні біржі.

Тема 5. Цифрові криптовалютні біржі.Термінологія. Стейкінг криптовалюти. Огляд криптобірж.

Тема 6. Цифрові криптовалютні біржі. Огляд криптобірж.

Тема 7. Принципи роботи з ETHEREUM. Обліковий запис Ethereum. Транзакції. Консенсус. Мітки часу. Число nonce. Час блоку. Розгалуження. Генезис. Деномінація ефіру. Віртуальна машина Ethereum. Газ. Виявлення вузлів. Протоколи Whisper та Swarm.

Тема 8. Протоколи електронних платежів . Електронний цифровий підпис. Криптографічні протоколи. Електронні платежі: пластикові картки. Сурогатні платіжні засоби в INTERNET/ Розрахунки пластиковими картками в INTERNET. Електронні гаманці. Цифрові гроші. Електронний цифровий підпис.

VII. Структура освітнього компонента

Змістові модулі і теми	Кількість годин денна форма				
	Усього	Лекції	Лабораторні	Консультації	Самостійна робота
Змістовий модуль 1. Хмарні обчислення. Види блокчейнів.					
Тема 1. Характеристика хмарних обчислень.Типи хмарних моделей. Моделі хмарних обчислень. Переваги хмарних обчислень. Недоліки хмарних обчислень.	15	4	5	1	5
Тема 2. Використання хеш функції. Дерево Меркла. Спеціальні транзакції. Hard & Soft fork. Обмеження блокчейну. Приватний та публічний блокчейн. Цифровий підпис до блокчейну: підпис транзакцій, підтвердження роботи.	15	4	5	1	5
Тема 3. Види криптовалют та механізми консенсусу.	15	4	5	1	5
Тема 4. Зберігання та використання криптовалют. Одноосібне управління. Зберігання ключів. Мульти Підписи .Сторонні послуги для використання криптовалют. Платежі. Огляд гаманців.	15	3	6	1	5
Разом за змістовий модуль 1	60	15	21	4	20
Змістовий модуль 2. Цифрові криптовалютні біржі.					
Тема 5. Цифрові криптовалютні біржі.Термінологія. Стейкінг криптовалюти. Огляд криптобірж.	15	4	5	1	5

Тема 6. Цифрові криптовалютні біржі. Огляд криптобірж.	15	4	5	1	5
Тема 7. Принципи роботи з ETHEREUM. Обліковий запис Ethereum. Транзакції. Консенсус. Мітки часу. Число nonce. Час блоку. Розгалуження. Генезис. Деномінація ефіру. Віртуальна машина Ethereum. Газ. Виявлення вузлів. Протоколи Whisper та Swarm.	15	4	5	1	5
Тема 8. Протоколи електронних платежів . Електронний цифровий підпис. Криптографічні протоколи. Електронні платежі: пластикові картки. Сурогатні платіжні засоби в INTERNET. Розрахунки пластиковими картками в INTERNET. Електронні гаманці. Цифрові гроші. Електронний цифровий підпис.	15	3	6	1	5
Разом за змістовий модуль 2	60	15	21	4	20
ВСЬОГО	120	30	42	8	40

VIII. Завдання для лабораторних робіт

Під час самостійної роботи здобувач освіти опрацьовує додатковий теоретичний матеріал згідно рекомендованих літературних джерел, виконує індивідуальні завдання та переглядає рекомендовані відеоуроки. Питання, опрацьовані здобувачем на самостійній роботі, враховані в модульних контрольних роботах та при складанні іспиту.

	НАЗВА ТЕМИ	Кіл-сть годин денна форма
1	Лабораторна робота №1. Середовище розробки та скелет прототипу блокчейну	4
2	Лабораторна робота №2.Транзакції та майнінг блоків в прототипі блокчейну	4
3	Лабораторна робота №3.Взаємодія з прототипом блокчейну засобами Postman	4
4	Лабораторна робота №4.Організація консенсусу в прототипі блокчейну	4
5	Лабораторна робота №5.Транзакції в блокчейні Bitcoin	4
6	Лабораторна робота №6.Смарт-контракти на блокчейні Ethereum	4
7	Лабораторна робота №7. Дизруптивні технології: ChatGPT та валютні	4

	ринки і відносини.	
8	Лабораторна робота №8.Використання цифрових підписів.	4
9	Лабораторна робота №9 Створення та використання електронних гаманців. Використання електронних гаманців.	4
10	Лабораторна робота №10. Процеси використання криптобірж.	4
РАЗОМ		40

IX. Завдання для самостійної роботи

Виконання самостійної роботи студентів можливе у вигляді написання тези чи індивідуального завдання. Здача фінального тесту з вказаного курсу переводиться в бали, виділені для самостійної роботи та заноситься до рейтингу поточного оцінювання студента.

Вимоги до оформлення звітів з самостійної роботи студентів.

Звіт з самостійної роботи студентів оформлюється на аркушах формату А4 (210х297 мм) на одній стороні листа білого паперу у вигляді: титульний аркуш, теоретичні питання, список використаної літератури.

Звіт виконується в електронному варіанті (система Windows, текстовий процесор Word) Вимоги до тексту: заголовок – 16 пт, текст відповіді – 14 пт, вирівняти по ширині, абзаци зі стандартним відступом першого рядка, інтервал міжрядковий – 1,5, поля: ліве – 3 см, праве – 1 см, верхнє, нижнє – 2 см, колонтитули із зазначенням ПІБ, номера сторінки. Об’єм звіту з самостійної роботи по темі складає 4-7 сторінки.

Якість роботи оцінюється з урахуванням правильності відповідей, підбору літератури, проведеного аналізу та відповідність звіту вказаним вимогам щодо оформлення. Захист звітів (рефератів) з самостійної роботи відбувається шляхом опитування на лабораторній роботі або консультації та представлення презентації реферату.

Критерії оцінювання знань та вмінь студента за результати виконання самостійної роботи за національною шкалою

За результати виконання самостійної роботи студенту виставляється оцінка:

в і д м і н н о, якщо студент вміє використовувати основну та додаткову літературу, в письмовій доповіді повністю і якісно розкрив тему, методично обґрунтовано використав теоретичні знання та практичні навички, у висновках дав вірну технічну інтерпретацію, грамотно оформлену роботу подав в установлений термін, доповідь студента чітка, грамотна, супроводжується комп’ютерною презентацією. Студент вірно та обґрунтовано відповів на поставлені питання з наведенням прикладів та аргументуванням своєї власної точки зору. Допускається наявність незначної кількості огріхів та несуттєвих неточностей, які не призвели до помилок у відповіді;

д о б р е, якщо студент вміє використовувати основну та додаткову літературу, в письмовій доповіді повністю і якісно розкрив тему, методично обґрунтовано використав теоретичні знання для виконання завдань, у висновках дав вірну технічну інтерпретацію, допустив несуттєву помилку у відповіді або висновках, допустив незначні відхилення від чинних стандартів при оформленні роботи;

з а д о в і л ь н о, якщо студент в письмовій доповіді розкрив тему, але виконану роботу подав більше двох тижнів після встановленого терміну, допустив помилки у відповіді або висновках, оформлення

роботи, не зовсім відповідає чинним вимогам стандартів, доповідь не супроводжується комп'ютерною презентацією.

н е з а д о в і л ь н о, якщо студент в письмовій доповіді не розкрив тему, не виконав завдання, отримані результати у висновках інтерпретуються невірно, робота оформлена неохайно.

X. Індивідуальні завдання

Індивідуальні завдання з Виконання індивідуального завдання (ІЗ) є важливою частиною дисципліни «Технології блокчейн та криптовалюта» та представляє собою самостійне дослідження студент. Мета виконання ІЗ є закріплення, узагальнення та поглиблення знань, одержаних студентами під час вивчення дисципліни та їх застосування при самостійній роботі, активізація творчих здібностей студентів, розвиток навичок роботи з нормативно-технічною літературою, прийняття самостійних рішень, набуття практичних навичок роботи щодо захисту інформації програмними та криптографічними засобами.

ІЗ повинно бути результатом самостійних досліджень студента, які: сприяють розвитку ініціативності студентів у їх виробничій і дослідницькій діяльності; поглиблюють, систематизують та закріплюють теоретичні знання та практичні навички, отримані під час навчання; перевіряють вміння студента самостійно освоїти та використовувати сучасні інформаційні технології; розвивають у студента навички ведення самостійного науково практичного пошуку, оволодіння методикою дослідження й експериментування в ході вирішення проблем і питань, поставлених до виконання; сприяють набуттю вміння аналізувати отримані результати досліджень, формулювати висновки та положення.

За всі відомості, що викладені в ІЗ, порядок використання в ході підготовки фактичного матеріалу та іншої інформації, пропозиції, технології, обґрунтованість і вірогідність висновків та положень, що захищаються, несе відповідальність безпосередньо автор.

Викладач надає студенту допомогу у виборі теми роботи, проводить консультації з проблемних питань, що виникають у процесі виконання, надає допомогу в пошуку методичної та технічної документації, науково-технічної літератури.

XI. Методи навчання

В ході вивчення дисципліни використовуються наступні методи навчання: мультимедійні презентації, аналіз інформації з відкритих джерел, комп'ютерне моделювання, статистичний аналіз. Основними видами занять, які проводяться під керівництвом викладача, є лекції, лабораторні роботи та самостійна робота. На лекціях розглядаються загальні теоретичні положення дисципліни. Під час проведення лекцій використовуються мультимедійні засоби для інтерактивної демонстрації прикладів та графічного матеріали. До кожної лекції студентам додається презентація основних положень. При виконанні лабораторних робіт зміцнюються знання, отримані на лекціях, набуваються первинні навички з проведення розрахунків міцності захисту, створення моделі загроз та моделі порушника, комп'ютерного моделювання загроз за допомогою різного програмного забезпечення, реалізації моделей контролю доступу до інформації з обмеженим доступом. При самостійній роботі студенти набувають навички самостійного освоєння матеріалу, який не використаний в навчальному процесі.На лекційних заняттях: розповідь, пояснення, демонстрація, бесіда, дискусія. На лабораторних роботах: пояснення, дослідження, розв`язування ситуаційних задач, виконання індивідуального варіанту завдання. Самостійна робота студента: реферати, повідомлення, науково-пошукові, дослідницькі проекти, виконання онлайн курсів. За джерелами знань використовуються такі методи навчання: словесні – розповідь, пояснення, лекція, інструктаж; наочні – демонстрація,

ілюстрація; практичні – лабораторна робота, практична робота, вправи. За характером логіки пізнання використовуються такі методи: аналітичний, синтетичний, аналітико-синтетичний, індуктивний, дедуктивний. За рівнем самостійної розумової діяльності використовуються методи: проблемний, частково пошуковий, дослідницький.

XII. Методи контролю

Контрольні заходи включають поточний та підсумковий модульний контроль. Поточний контроль здійснюється під час проведення лабораторних занять для перевірки рівня підготовки студента до виконання конкретного завдання. Форма проведення поточного контролю: усне опитування, вирішення ситуаційних задач, тестовий контроль. Оцінюється вхідний, проміжний, кінцевий рівень знань студента. Підсумковий контроль проводиться у вигляді комп'ютерних тестів та/або виконання практичних завдань.

XIII. Політика оцінювання

Політика оцінювання та організація контрольних заходів здійснюється згідно з Положенням про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки http://surl.li/lnfyv .

Оцінювання навчальних досягнень з Комп'ютерних мереж здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань, самостійне опрацювання теоретичного матеріалу) та підсумковий модульний контроль (письмові модульні контрольні роботи). Максимальна кількість балів, яку може накопичити здобувач під час поточного оцінювання за семестр – 40 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за модульні контрольні роботи (МКР). Максимальна кількість балів, яку може накопичити здобувач під час модульного контролю за семестр, складає 60 балів. Модульні контрольні роботи складаються з тестів по темах. Упродовж семестру, після завершення відповідних тем (модулів), проводяться М1, М2 модульні контрольні роботи у тестовій формі.

Якщо за результатами семестру накопичено не менше 75 балів і здобувач погоджується із цим результатом, то оцінка за семестр може виставлятися без складання іспиту. В іншому разі студент складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається.

XIV. Політика викладача щодо здобувача

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих морально-етичних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття без поважних причин; користування мобільним телефоном або іншими мобільними пристроями під час заняття не з навчальною метою, зокрема розмови, переписка, ігри та інші розваги; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу. У випадку запровадження дистанційної форми навчання, що може бути пов'язано із карантином, надзвичайними ситуаціями,

воєнним станом і т. ін., заняття проводитимуться в режимі відео конференції Zoom та / або з використанням платформи Moodle https://moodle-cs.vnu.edu.ua/. Матеріал пропущених занять здобувач опрацьовує самостійно, звітує про виконання викладачу в індивідуальному порядку. Пропущені заняття не звільняють студента від своєчасного виконання модульних контрольних робіт разом із групою.

Перезарахування окремих змістових модулів, модульних контрольних заходів в межах освітнього компонента регламентується Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або формальній освіті у Волинському національному університеті імені Лесі Українки https://bit.ly/3Bdq6qP .

XV. Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності https://bit.ly/3BFUETR .

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

XVI. Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, виконують всі завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати питання викладачу.

Перескладання модульних контрольних робіт заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

XVII. Підсумковий контроль

Якщо за результатами семестру накопичено не менше 75 балів і здобувач погоджується із цим результатом, то оцінка за семестр може виставлятися без складання іспиту. В іншому разі студент складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається. Екзамен проходить шляхом складання тесту. Оцінка за семестр у випадку складання іспиту є сумою балів поточного контролю та балів, отриманих під час іспиту.

Шкала оцінювання

Оцінка в балах	Лінгвістична оцінка	Оцінка за шкалою ECTS	
		оцінка	пояснення
90–100	Відмінно	A	інне виконання
82–89	Дуже добре	B	е середнього рівня
75–81	Добре	C	ном хороша робота
67–74	Задовільно	D	гано
60–66	Достатньо	E	нання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	хідне перескладання

XVIII. Рекомендована література та інтернет-ресурси

Основна

1. Конституція України. Режим доступу: https://zakon.rada.gov.ua/go/254к/96-вр
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах», від 05.07.1994 № 81/94-ВР (Зі змінами, внесеними згідно із Законом № 1089-IX від 16.12.2020. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
3. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
4. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
5. ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
6. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
7. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.
8. Інформаційні технології. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:1995): ДСТУ 3918–1999. – [Чинний від 2000–01– 01]. – К.: Держстандарт України, 2000. – 50 с. – (Національний стандарт України).
9. ISO/IEC 27002:2022 (en). Information security, cybersecurity and privacy protection – Information security controls// Online Browsing Platform (OBP). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en
10. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
11. НД ТЗІ 2.5-004-99: Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
12. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
13. НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000, № 53.
14. Закон України «Про інформацію» № 2657-ХИ від 02.10.1992. - ВВР, 1992, № 48, ст. 650.Система управління якістю відповідає ДСТУ ISO 9001:2015

15. Закон України «Про державну таємницю» № 3855-XII від 21.01.1994, ВВР, 1994, № 16, ст. 93 (остання редакція № 1519-IV від 19.02.2004). 16. Закон України «Про електронні документи і електронний документообіг», № 851-IV від 22.05.2003, ВВР, 2003, № 36, ст. 275 (зі змінами, внесеними згідно із Законом № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст. 349).
17. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
18. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
19. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
20. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
21. . НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.
22. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.
23. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). Затверджені наказом ДСТЗІ від 09.06.1995 № 25.

ДОДАТКОВА ЛІТЕРАТУРА

1. Chocolatey:https://docs.chocolatey.org/en-us/choco/setup#nonadministrative-install
2. Ganache: https://www.trufflesuite.com/ganache
3. Фреймворк Truffle: https://www.trufflesuite.com/truffle
4. Kovan testnet: https://gitter.im/kovan-testnet/faucet
5. Сервіс Infura: https://infura.io/
6. Сервіс Kovan: https://kovan.etherscan.io/
7. VisualStudioCode:https://code.visualstudio.com/download
8. Geth:https://geth.ethereum.org/downloads/ Node.js: https://nodejs.org/uk/
9. https://github.com/dvf/blockchain
10. Learn Blockchains by Building One https://medium.com/@vanflymen/learn-blockchains-by-building-one117428612f46 12.
11. https://medium.com/tixlorg/guide-get-a-btc-testnet-wallet-withtokens-and-transfer-them-to-the-tixl-testnet-807f1a6ef8b2