



Міжнародний європейський університет



КАФЕДРА _____
менеджменту та економіки _____



2021
SYLLABUS
ДОДАТОК 1

Дисципліна

Кібербезпека

Сторінка дисципліни

<https://business.ieu.edu.ua/>

Форма підсумкового контролю

залік

диференційований
залік

екзамен



1 Коротка анотація дисципліни

Дана навчальна дисципліна є напрямком, який пов'язаний з розробкою, реалізацією, впровадженням та управлінням комплексними програмно-технічними системами захисту інформації в установі (компанії, підприємстві). Крім того, цей напрямок також пов'язане зі створенням і аудитом комп'ютерних систем, що впливають на безпеку транспортних, енергетичних, медичних та інших комплексів.

2 Передумова вивчення дисципліни

Предметом вивчення навчальної дисципліни є розвиток безпечного, стабільного і надійного кіберпростору має полягати в тому числі і завдяки «підвищенню цифрової грамотності громадян та культури безпечного поведіння в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту. Велика кількість персональних даних потрапляє до комп'ютерних соцмереж. Важливо розуміти рівні захищеності власних даних, правила використання платіжних систем, наслідки, які можуть спричинити конфіденційні дані, що потрапили у відкритий доступ або у розпорядження кіберзлочинців.

3 Мета та цілі дисципліни

Метою викладання навчальної дисципліни «Кібербезпека» є навчити студента основні концепції безпеки інформації, і дає змогу отримати навички, необхідні для моніторингу, виявлення, аналізу і нейтралізації загроз інформаційної безпеки.

4 Результати навчання

ПРН 1. Знати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства, верховенства права, прав і свобод людини і громадянина в Україні.

ПРН 4. Демонструвати навички виявлення проблем та обґрунтування управлінських рішень.

ПРН 6. Виявляти навички пошуку, збирання та аналізу інформації, розрахунку показників для обґрунтування управлінських рішень.

ПРН 8. Застосовувати методи менеджменту для забезпечення ефективності діяльності організації.

ПРН 11. Демонструвати навички аналізу ситуації та здійснення комунікації у різних сферах діяльності організації.

ПРН 12. Оцінювати правові, соціальні та економічні наслідки функціонування організації в процесі прийняття управлінських рішень.

ПРН 20. Демонструвати навички використання інформаційних, комунікаційних та інноваційних технологій.

5 Кредити ECTS

На вивчення навчальної дисципліни «Кібербезпека» відводиться 90 години 3 кредити ЄКТС.

6 Структура дисципліни

Найменування тем	Вид занять / год		
	Лекції	Семінарські заняття / практичні / лабораторні	Самостійна робота
Тема 1. Теоретичні та методологічні основи захисту інформації.	4	1	6
Тема 2. Структура законодавства в сфері захисту інформації	2	2	6
Тема 3. Законодавче регулювання діяльності у сфері захисту інформації.	2	2	6
Тема 4. Процедури забезпечення необхідних характеристик та якості засобів захисту інформації.	4	1	6
Тема 5. Порядок і правила захисту інформації в комп'ютерних системах.	2	2	6
Тема 6. Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.	4	2	6

Тема 7. Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.	2	2	6
Тема 8. Стандарти інформаційної та кібернетичної безпеки.	4	2	6
Розрахункова робота	-	2	2

7 Перелік обов'язкових завдань

Обов'язкові завдання	Кінцеві терміни підготовки
Теоретичні та методологічні основи захисту інформації.	За розкладом
Структура законодавства в сфері захисту інформації	За розкладом
Законодавче регулювання діяльності у сфері захисту інформації.	За розкладом
Процедури забезпечення необхідних характеристик та якості засобів захисту інформації.	За розкладом
Порядок і правила захисту інформації в комп'ютерних системах	За розкладом
Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.	За розкладом
Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.	За розкладом
Стандарти інформаційної та кібернетичної безпеки.	За розкладом

8 Перелік вибірових завдань

Вибіркові завдання	Кінцеві терміни підготовки
1. Складові інформаційної безпеки. 2. Аналіз концепції інформаційної безпеки України. 3. Дозвільна система проведення робіт у галузі технічного захисту інформації. 4. Аналіз пошукових систем для конкурентної розвідки. 5. Забезпечення доступності й цілісності інформації в АС. 6. Порядок забезпечення криптографічного захисту інформації. 7. Циклічна модель інформаційної безпеки. Потенційні загрози безпеки інформації та їх класифікація. 8. Взаємодія суб'єктів системи технічного захисту інформації. 9. Ліцензування господарської діяльності у галузі захисту інформації. 10. Сертифікація продукції в сфері захисту інформації. 11. Модель порушника інформаційної безпеки. 12. Криптосистеми та загрози їх безпеки.	За розкладом

9 Ознаки дисципліни

Термін викладання	Семестр	Міждисциплінарна інтеграція	Курс (рік навчання)	Цикл: загальної підготовки / професійної підготовки / вільного вибору
Один семестр	6 семестр	Так	3-й курс	Цикл вільного вибору

10 Технічне й програмне забезпечення / обладнання

Мобільні пристрої дозволяється використовувати лише під час on-line тестування та підготовки практичних завдань під час заняття.

Списування під час контрольних робіт заборонено (в т.ч. із використанням мобільних девайсів)

11 Система оцінювання та вимоги

Оцінювання окремих видів виконаної студентом навчальної роботи з дисципліни здійснюється в балах відповідно до табл.1. Виконані види навчальної роботи зараховуються студенту, якщо він отримав за них позитивну рейтингову оцінку.

Таблиця 1

Розподіл балів оцінювання успішності студентів з навчальної дисципліни «Кібербезпека»

Розділ I Поточне тестування та самостійна робота									Розділ II Підсумковий контроль	Всього
Змістовий розділ I										
T1	T2	T3	T4	T5	T6	T7	T8	PP		
5	5	5	5	5	10	5	10	10	40	100

*T1, T2, ..., T8 – теми занять

**Розрахункова робота

Поточне оцінювання знань студентів проводиться протягом семестру у наступних формах: усного опитування студентів на практичних заняттях та оцінки рівня їх знань; перевірки правильності розв'язання практичних задач; експрес-опитування (в усній чи письмовій формі).

Загальна оцінка знань студентів за поточним контролем

Результати поточного контролю знань студентів в цілому (за усіма формами робіт) оцінюються в діапазоні від **0** до **60** балів. Студент допускається до підсумкового контролю за умови виконання вимог навчальної програми та у разі, якщо за поточну навчальну діяльність він набрав не менше **36** балів.

Підсумкове оцінювання знань студентів проводиться у формі **заліку**. Максимальна кількість балів, яку можна отримати на заліку складає **40** балів (див. табл. 2).

Під час оцінювання відповіді на окреме питання додатково враховуються допущені недоліки та помилки, якими вважаються: неохайне оформлення роботи (не загальноприйняті скорочення, незрозумілий почерк, використання олівців замість чітких чорнил) (мінус 2 бали); неточності в назвах окремих економічних категорій та понять (мінус 4 бали).

Таблиця 2

Розподіл балів оцінювання при підсумковому контролі з навчальної дисципліни

Оцінка в балах за поточне оцінювання	Оцінка в балах за підсумкове оцінювання	Оцінка за національною шкалою
54-60	36-40	Відмінно
45-53	30-35	Добре
36-44	24-29	Задовільно
менше 36	менше 24	Незадовільно

Критерії оцінювання відповіді на теоретичні питання білету:

1. Повна відповідь на питання, яка оцінюється **«відмінно»**, повинна відповідати таким вимогам:

- розгорнутий, вичерпний виклад змісту даної у питанні проблеми;
- повний перелік необхідних для розкриття змісту питання категорій та законів, що вивчались у навчальному курсі;
- здатність здійснювати порівняльний аналіз різних теорій, концепцій, підходів та самостійно робити логічні висновки й узагальнення;
- уміння користуватись методами наукового аналізу явищ, процесів і характеризувати їхні риси та форми виявлення;
- демонстрація здатності висловлення та аргументування власного ставлення до альтернативних поглядів на дане питання;
- використання актуальних фактичних та статистичних даних, знань дат та історичних періодів, які підтверджують тези відповіді на питання.

2. Відповідь на питання оцінюється **«добре»**, якщо:

- відносно відповіді на найвищий бал не зроблено розкриття хоча б одного з пунктів, вказаних вище (якщо він явно потрібний для вичерпного розкриття питання) або, якщо:
- при розкритті змісту питання в цілому правильно за зазначеними вимогами зроблені окремі помилки під час: використання цифрового матеріалу.

3. Відповідь на питання оцінюється **«задовільно»**, якщо:

- відносно відповіді на найвищий бал не зроблено розкриття чотирьох чи більше пунктів, зазначених у вимогах до нього (якщо вони явно потрібні для вичерпного розкриття питання);
- одночасно присутні чотири чи більше типів недоліків, які окремо характеризують критерій оцінки питання;
- висновки, зроблені під час відповіді, не відповідають правильним чи загально визначеним при відсутності доказів супротивного аргументами, зазначеними у відповіді;
- характер відповіді дає підставу стверджувати, що особа, яка складає іспит, не зовсім правильно зрозуміла зміст питання чи не знає правильної відповіді і тому не відповіла на нього по суті, допустивши грубі помилки у змісті відповіді.

З урахуванням вищевикладеного результати заліку оцінюються в діапазоні від **0** до **40** балів для студентів. При цьому, якщо відповіді студента на екзамені оцінені менше ніж на 30%, він отримує незадовільну оцінку за результатами заліку та незадовільну загальну підсумкову оцінку. Загальна підсумкова оцінка з дисципліни складається з суми балів за

результати поточного контролю знань та за виконання завдань, що виносяться на залік.

Загальна підсумкова оцінка не може перевищувати **100 балів**.

Загальна підсумкова оцінка в балах, за національною шкалою та за шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента (див. табл. 3).

Таблиця 3

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проєкту (роботи), практики	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
66-73	D	задовільно	
60-65	E		
30-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-29	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

12 Політика дисципліни

Політика навчальної дисципліни визначається системою вимог, які викладач пред'являє до студента при вивченні дисципліни та ґрунтується на засадах академічної доброчесності. Вимогою для студентів є активна участь, виконання необхідного мінімуму навчальної роботи.

13 Політика щодо пропусків занять

Під час зайнять є неприпустимим пропусків без поважної причини, запізень. При наявності пропущених більше 50% зайнять студент не буде допущений до підсумкового контролю знань. Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

14 Політика щодо виконання завдань пізніше встановленого терміну

При виконанні завдання пізніше терміну здачі на тиждень при наявності поважної причини, підсумковий бал за завдання знижується на 10% від отриманої оцінки. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання

модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

15 Політика дотримання академічної доброчесності

Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%.

Списування під час контрольних робіт та екзаменів заборонені.

Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування.

Учасники освітнього процесу керуються принципами академічної доброчесності в Міжнародному європейському університеті згідно з Кодексом академічної доброчесності науково-педагогічних, наукових, педагогічних працівників та здобувачів вищої освіти Міжнародного європейського університету – <https://ieu.edu.ua/pro-mieu/publicna-informatsiia>

16 Рекомендовані джерела інформації

1. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
2. Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432 с.
3. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. - 364 с.
4. Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.
5. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
6. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
7. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 с.
8. 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. /В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко/ –К.:ДУТ, 2015. – 345 с.
9. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.

- 10.Постанова Кабінету Міністрів України від 18.05.2011 року №517 Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню.
- 11.Постанова Кабінету Міністрів України від 25.05.2011 року №543 Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню.
- 12.Бекірова Е. Правова природа інституту ліцензування певних видів господарської діяльності // Підприємництво, господарство і право. – 2007, №10, С. 95-97.
- 13.Господарський кодекс України: Коментар. – Х.: "Одіссей", 2004. – 848 с.
- 14.Верховна Рада України. Законодавство України // [Електронний ресурс]. – Режим доступу: <http://zakon.rada.gov.ua/laws/>
- 15.Державна служба спеціального зв'язку та захисту інформації // [Електронний ресурс]. – Режим доступу: <http://www.dsszzi.gov.ua/dsszzi/control/uk/index>.
- 16.CERT-UA // [Електронний ресурс]. – Режим доступу: <http://cert.gov.ua>

17 Поради з успішного навчання на курсі

Відповідальність – це усвідомлення того, що для досягнення успіху ви самі маєте визначити свої пріоритети, розподілити час і ресурси.

Шукайте оптимальний розв'язок завдання.

Будьте вимогливими до себе.