ISO 9001 CERTIFIED
SLC. MS.040. LSO9001. 1693

INTERNATIONAL EUROPEAN UNIVERSITY

SYLLABUS

INTERNATIONAL EUROPEAN UNIVERSITY

EUROPEAN SCHOOL OF BUSINESS

Кібербезпека

2021

SYLLABUS

Дисципліна	
	Кібербезпека
Викладач (-і)	
	Міхно Інеса Сергіївна
Профайл викладача (-ів)	
	https://business.ieu.edu.ua/pro-yemsh/struktura-kafedry-vykladachi/kafedry/kafedra-menedzhmentu#zzz-006
Консультації	
Очні консультації	П’ятниця 14.00 – 15.00
Онлайн консультації	Другий вівторок місяця 15:00-16:00
Контактний телефон	
	+380 93 426 42 45
E-mail	
	inessamikhno@ieu.edu.ua
Сторінка дисципліни	
	https://business.ieu.edu.ua/navchannia/orhanizatsiia-osvitnoho-protsesu/robochi-prohramy/bakalavrat

Форма підсумкового контролю	залік	диференційований залік	екзамен
	☒	☐	☐

SYLLABUS

1 Коротка анотація дисципліни

Дана навчальна дисципліна є напрямок, 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'язаний зі створенням і аудитом комп'ютерних систем, що впливають на безпеку транспортних, енергетичних, медичних та інших комплексів.

2 Передумова вивчення дисципліни

У процесі вивчення дисципліни студенти пізнають теоретичні знання у галузі інформаційної безпеки, набуття практичних навичок застосування сучасних технологій забезпечення інформаційної безпеки

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

5 Кредити ECTS

3 кредити ECTS / 90 академічних годин

6 Структура дисципліни

Назви змістових розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
Змістовий розділ 1. Інформація та інформаційні системи в управлінні: основні поняття, етапи розвитку та класифікація												
Тема 1. Теоретичні та методологічні основи захисту інформації.	**10**	2	1			7	**12**	2				10

6 Структура дисципліни

Назви змістових розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
Тема 2. Структура законодавства в сфері захисту інформації	**11**	2	2			7	**11**		1			10
Тема 3. Законодавче регулювання діяльності у сфері захисту інформації.	**11**	2	2			7	**10**					10
Тема 4. Процедури забезпечення необхідних характеристик та якості засобів захисту інформації.	**12**	4	1			7	**10**					10
Тема 5. Порядок і правила захисту інформації в комп'ютерних системах.	**11**	2	2			7	**10**					10
Тема 6. Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.	**11**	2	2			7	**10**					10
Тема 7. Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.	**11**	2	2			7	**11**		1			10
Тема 8. Стандарти інформаційної та кібернетичної безпеки.	**11**	2	2			7	**12**	2				10
Розрахункова робота	**2**		2			**2**	**4**					4
Разом за змістовим розділом 1	**90**	**16**	**16**			**58**	**90**	**4**	**2**			**84**
Усього разом	**90**	**16**	**16**			**58**	**90**	**4**	**2**			**84**

7 Перелік обов'язкових завдань

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

8 Перелік вибіркових завдань

Провідні світові та національні органи зі стандартизації.
Нормативне регулювання у сфері інформаційної безпеки в ЄС.
Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки.
Стандарти інформаційної та кібернетичної безпеки.
Сімейство стандартів інформаційної та кібернетичної безпеки.
Структура стандарту по кібербезпеці.
Базові блоки стандарту ISO 27032.
Заходи забезпечення кібербезпеки.
Основи обміну інформацією та координації.
Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.
Предмет криптографії.
Криптосистеми та загрози їх безпеки.
Симетричні та асиметричні криптосистеми.
Формування та перевіряння електронного цифрового підпису.
Порядок забезпечення криптографічного захисту інформації.
Управління ризиками.
Модель безпеки з повним перекриттям
Основні принципи побудови концепції ІБ
Основні вимоги міжнародного стандарту ISO 15408.
Методика визначення потенціалу нападу при оцінці стійкості функцій безпеки.

9 Ознаки дисципліни

Термін викладання	Семестр	Міжнародна дисциплінарна інтеграція	Курс (рік навчання)	Цикли: загальної підготовки/ професійної підготовки/ вільного вибору
1 семестр	6 семестр	Так	3 курс	Вільного вибору

10 Система оцінювання та вимоги

У процесі вивчення дисципліни здійснюється поточний та підсумковий контроль знань студентів.
Підсумкова залікова оцінка виставляється відповідно до сумарного рейтингу студента.
За результатами поточного контролю протягом семестру студент може отримати максимально – 100 балів, мінімальна сума балів, що дозволяє студенту бути атестованим з дисципліни – 60 балів.

Співвідношення між національними та ECTS оцінками і рейтингом студента:
https://ieu.edu.ua/docs/pol-mark-esb.pdf

11 Умови допуску до підсумкового контролю

Мінімальна кількість балів, яку повинен набрати здобувач освіти за поточну навчальну діяльність за семестр для допуску до підсумкового контролю – 36 балів. Оцінка за дисципліну визначається як сума підсумкового балу за поточну діяльність та балу за підсумковий контроль і виражається за багатобальною шкалою.

11 Умови допуску до підсумкового контролю

Оцінка з дисципліни, яка завершується заліком, визначається як сума балів за поточну навчальну діяльність (не менше 36), бали за індивідуальну самостійну роботу здобувача освіти (не більше 6) та балів за залік (не менше 24).
Загальний бал з дисципліни становить 100. Сумарна оцінка за вивчення дисципліни виставляється за національною та європейською шкалою.
Підсумковий контроль у формі заліку проводиться після завершення вивчення усіх тем дисципліни і складається здобувачами освіти у період залікової сесії.
https://ieu.edu.ua/docs/050.pdf

12 Політика дисципліни

Для продуктивної навчально-пізнавальної діяльності студентів при вивченні дисципліни здійснюються актуальні лекції та семінари у вигляді презентацій, кейсів, робота в групах, семінарів-дискусій. На заняттях та під час перебування в університеті студент повинен поважно ставитися до викладачів, співробітників та інших студентів, відвідувати заняття згідно з розкладом, приходити вчасно і не залишати аудиторії без дозволу викладача. Необхідно виконувати всі академічні завдання і роботи у визначені терміни.
Викладач, у свою чергу повинен постійно підвищувати свій професійний рівень, педагогічну майстерність, загальну культуру, забезпечувати умови для засвоєння студентами навчальних програм на рівні обов'язкових вимог щодо змісту, рівня та обсягу освіти, сприяти всебічному професійному розвитку студентів. Обов'язково дотримуватися навчально-тематичного плану, не спізнюватися на заняття, не допускати жодних проявів корупції, дискримінації, булінгу, цькування та утиску прав здобувачів освіти.

13 Політика щодо пропусків занять та виконання завдань пізніше встановленого терміну

Студент, який з поважних причин, підтверджених документально, не підлягав поточному контролю має право пройти поточний контроль у двотижневий термін після повернення до навчання.
Студент, що був відсутній на заняттях без поважних причин, не брав участі у заходах поточного контролю, не ліквідував академічну заборгованість, не допускається до підсумкового семестрового контролю знань з цієї дисципліни, а в день складання екзамену в екзаменаційній відомості науково-педагогічним працівником виставляється оцінка «недопущений». Повторне складання екзамену з дисципліни призначається за умови виконання всіх видів навчальної, самостійної (індивідуальної) роботи, передбачених робочою навчальною програмою дисципліни, і проводиться згідно із затвердженим директоратом графіком ліквідації академічної заборгованості.
https://ieu.edu.ua/docs/050.pdf

14 Політика дотримання академічної доброчесності

Учасники освітнього процесу керуються принципами академічної доброчесності
https://ieu.edu.ua/docs/011.pdf

15 Рекомендовані джерела інформації

Основна (базова):
Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.
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.
Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 с.
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.
Допоміжна:
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.
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.
Бекірова Е. Правова природа інституту ліцензування певних видів господарської діяльності // Підприємництво, господарство і право. – 2007, №10, С. 95-97.
Господарський кодекс України:Коментар. – Х.:"Одіссей", 2004.– 848с.
Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432 с.
Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. - 364 с.
Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.
Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.
Інформаційні ресурси:
Верховна Рада України. Законодавство України // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/
Державна служба спеціального зв'язку та захисту інформації // [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.
CERT-UA // [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/

16 Поради з успішного навчання на курсі

Якщо Ви бажаєте успішно засвоїти цей предмет, необхідно бути:
- наполегливим, уважним і допитливим;
- креативним і життєрадісним, відкритим для спілкування та дискусій;
- готовим отримувати інформацію і знання з предмету не лише на лекціях, а й у позааудиторний час.
До зустрічі!