МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи
_____
Каріна ПЕМАШКАЛЮ

ТЕХНОЛОГІЇ УПРАВЛІННЯ БЕЗПЕКОЮ БІЗНЕС-ПРОЦЕСІВ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***другий (магістерський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЄЄВ*

Харків
2021

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2021 р.

Розробники:
Мілов О.В., д.т.н., проф. кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Інструменти презентації вже існуючих та постійно обновлюваних знань мають широке представлення на сучасному ринку ІТ-інструментів, так як забезпечують більш наочне та переконливе відображення процесів сучасності, допомагають розширити аудиторію зацікавлених та виявити специфічні вимоги до представленого матеріалу.

Предметом вивчення дисципліни є базові визначення та поняття інженерії знань і нейроінформатикі, основні завдання та методи інженерії знань та методи представлення й обробки знань. Об'єктами вивчення виступають знання як суб'єктивна категорія, взаємозв'язок з поняттями даних і інформації, методи формалізації знань, в тому числі, нечітких, методи вирішення завдань в системах, заснованих на знаннях, методи придбання знань, архітектура експертних систем, як одного з типів інтелектуальних інформаційних систем та інструментальні засоби для розробки баз знань.

Мета навчальної дисципліни "Технології управління безпекою бізнес-процесів" – сформувати системне базове уявлення, первинні знання, вміння і навички студентів з основ технології управління безпекою бізнес-процесів, як одним з напрямків побудови систем безпеки, дати уявлення про моделі бізнес-процесів та методах моделювання на засадах процесного підходу.

Результатами вивчення дисципліни є надбання вміння і навичок з орієнтації в різних методах представлення знань, переходах від одного методу до іншого, формалізації знань експертів із застосуванням різних методів представлення знань, розроблення продукційної бази знань для вирішення задач з вибору варіантів в предметній області, що слабо формалізована та програмування на мові Пролог.

Характеристика навчальної дисципліни

Курс	**1 М**
Семестр	**1**
Кількість кредитів ECTS	**3**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Дипломний проект бакалавра	Передові методики програмування
Бази даних та знань	Безпека Інтернет-речей

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.	РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

	РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або

	кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.	РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

	РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Програма навчальної дисципліни

Змістовий модуль 1. Введення в управління безпекою бізнес-процесів

Тема 1. Функціональний і процесний підходи до управління безпекою бізнес-процесами
Тема 2. Теоретичні основи управління бізнес-процесами
Тема 3. Бізнес-процес і його компоненти
Тема 4. Еталонні і референтні моделі
Тема 5. Методології опису діяльності

Змістовий модуль 2. Інструментарій управління безпекою бізнес-процесів

Тема 6. Інструментальні системи для моделювання бізнесу
Тема 7. Методики опису різних предметних областей
Тема 8. Методи аналізу процесів
Тема 9. Контролінг і моніторинг процесів
Тема 10. Процесна трансформація та процесна організація

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції (теми 1-10), презентації (теми 1-10), лабораторні роботи (теми 1, 3, 5, 7, 9).

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту поставити залік, – 60 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- обробляти дані представляти результати за допомогою технологій робочого столу;
- вміння аналізувати та використовувати стан кібербезпеки в сучасних світових умовах;
- вміння зберігати отримані дані;
- знання основ організації та використання сучасних операційних систем та мереж;
- знання у використанні алгоритмів;
- знати класифікацію мов програмування;
- використовувати технології розробки програмного забезпечення;
- знання щодо структур даних, файлових структур та структур баз даних;
- вміння використовувати знання щодо штучного інтелекту;
- вміння застосовувати теорію розрахунків.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та

обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: максимальна кількість балів становить 24 (робота на лекціях – 10, експрес-опитування – 14).

Лабораторні заняття: максимальна кількість балів становить 76 (виконання лабораторних робіт – 5, захист лабораторних робіт – 35, контрольні роботи – 36), а мінімальна – 50.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями та контрольних робіт за лабораторними роботами дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням отриманих балів у продовж семестру.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Проблемна лекція	Проблемна лекція "Функціональний і процесний підходи до управління безпекою бізнес-процесами"	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №1.* Опис роботи системи, побудованої за концепцією «Удосконалення процесів»	Виконання лабораторної роботи	3
			Захист лабораторної роботи № 1	7

	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Проблемна лекція	Лекція "Теоретичні основи управління бізнес-процесами"	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Проблемна лекція	Лекція "Бізнес-процес і його компоненти"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2. Опис роботи системи, побудованої за концепцією «Формалізація процесів»	Виконання лабораторної роботи	3
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Проблемна лекція	Лекція "Еталонні і референтні моделі"	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Проблемна лекція	Лекція "Методології опису діяльності"	Робота на лекції	1
			Експрес-опитування	7
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт.		

		Виконання лабораторних завдань		
Тема 6	***Аудиторна робота***			
	Проблемна лекція	Лекція "Інструментальні системи для моделювання бізнесу"	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Проблемна лекція	Лекція "Методики опису різних предметних областей"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3. Організація управління наскрізними процесами і групами процесів	Виконання лабораторної роботи	3
			Захист лабораторної роботи № 3	7
			Контрольна робота 1	18
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Проблемна лекція	Лекція "Методи аналізу процесів"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №4 Побудова системи процесів організації на основі аналізу ланцюжків створення цінності	Виконання лабораторної роботи	3
			Захист лабораторної роботи № 4	7
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 9	***Аудиторна робота***			
	Проблемна лекція	Лекція " Контролінг і моніторинг процесів "	Робота на лекції	1
			Експрес-опитування	7
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 10	***Аудиторна робота***			
	Проблемна лекція	Лекція "Процесна трансформація та процесна організація"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5 Аналіз топології процесу управління безпекою	Захист лабораторної роботи № 5	7
			Контрольна робота 2	18
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Рекомендована література

Основна

1. Аудит інформаційної безпеки: підручник / В. А. Ромака, А. Е. Лагун, Ю. Р. Гарасим та ін. ; Держ. служба України з надзвич. ситуацій, Львів. держ. ун-т безпеки життєдіяльності, НАН України, Ін-т приклад. проблем механіки і математики ім. Я. С. Підстригача. — Львів: Сполом, 2015. — 363 с. : іл. — Бібліогр.: с. 280—281 (37 назв). — ISBN 978-966-919-123-6
2. Абдалла А. Кібербезпека та інформаційні технології / Абдалла А., Альошин Г. В., Вдовиченко І. Н. та ін. – Х.; ТОВ “ДІСА ПЛЮС”, 2020. -380 с.

Додаткова

3. Kostina O. M. Diagnostics and management of business processes in the context of enterprise crisis management / Electronic scientific edition “Ekonomika i suspilstvo”.2019. № 10 – С. 287-297.
4. Md Imtiaz Mostafiz, Murali Sambasivan, See Kwong Goh, (2019) "Impacts of dynamic managerial capability and international opportunity identification on firm performance", Multinational Business Review, 13. Prodius O.I., Naida E.D. Business process reingineering as a modern management concept // Electronic scientific edition "Ekonomika ta suspilstvo" 2019.

Інформаційні ресурси.

5. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Технології управління безпекою бізнес-процесів" https://pns.hneu.edu.ua/course/view.php?id=8052.