

**Міністерство освіти і науки України
Державний торговельно-економічний університет
Факультет інформаційних технологій**

ІНФОРМАЦІЙНИЙ ПАКЕТ

Європейська кредитно-трансферна система (ЄКТС)

Галузь знань	12«Інформаційні технології»
Спеціальність	125 «Кібербезпека та захист інформації»
Освітня програма	«Безпека систем електронних комунікацій в економіці»
Освітній ступінь	«магістр»

Київ 2023

3. Освітня програма

Керівник проектної групи (гарант освітньої програми) – Савченко Тетяна Віталіївна, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

1. Профіль освітньої програми

**«Безпека систем електронних комунікацій в економіці»
зі спеціальності 125 «Кібербезпека та захист інформації»**

1 – Загальна інформація	
Повна назва ЗВО та структурного підрозділу	Державний торговельно-економічний університет, Факультет інформаційних технологій, Кафедра інженерії програмного забезпечення та кібербезпеки.
Ступінь вищої освіти / фахової передвищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти магістр спеціальність «Кібербезпека та захист інформації»
Офіційна назва освітньої програми	«Безпека систем електронних комунікацій в економіці»
Відповідність стандарту вищої освіти МОН України	Відповідає СВО МОН України
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС
Наявність акредитації	-
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Для здобуття освітнього рівня «магістр» зі спеціальності 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» можуть вступати особи, які здобули освітній рівень «бакалавр». Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти.
Мова(и) викладання	Українська
Термін дії освітньої програми	1 рік 4 місяці
Інтернет-адреса постійного розміщення опису освітньої програми	https://knute.edu.ua

2 – Мета освітньої програми	
<p>Забезпечити здобувачам вищої освіти другого (магістерського) рівня фундаментальну підготовку за спеціальністю 125 «Кібербезпека та захист інформації», що є достатньою для вирішення задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки в галузі економіки.</p>	
3 - Характеристика освітньої програми	
<p>Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))</p>	<p>Об'єкти вивчення:</p> <ul style="list-style-type: none"> – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. <p>Цілі навчання: Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.</p> <p>Теоретичний зміст предметної області: Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки.</p> <p>Методи, методики та технології: Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки.</p>

	<p>Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.</p> <p>Інструменти та обладнання: Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.</p>
Орієнтація освітньої програми	<p>Програма орієнтована на освітньо-професійний та прикладний напрямок підготовки.</p> <p>Акцент програми зроблений на формуванні фахівця, що здатний розв'язувати професійні задачі, пов'язані з системами електронних комунікацій, зокрема в економіці.</p>
Основний фокус освітньої програми	<p>Освітньо-професійний. Програма спрямована на поєднання практики та науки, щодо організації, розробки та експлуатації комплексних складових кіберпростору з метою забезпечення інформаційної безпеки суб'єктів господарювання економіки держави з урахуванням можливих зовнішніх кібервпливів, ймовірних загроз і рівня розвитку технологій захисту систем електронних комунікацій.</p> <p>Ключові слова: технології безпеки безпроводових та мобільних мереж, технології безпеки Web-ресурсів, тестування на проникнення, вразливість системи, система управління інформаційною безпекою суб'єкту господарювання, правове забезпечення інформаційної безпеки в економічних системах, економічна безпека держави.</p>
Особливості програми	<p>Програма передбачає підготовку професіоналів, здатних: моделювати та прогнозувати можливі кібервпливи на суб'єкти господарювання економіки держави та фізичних осіб; проводити аудит систем електронних комунікацій суб'єктів господарювання; застосовувати нормативні документи та стандарти в розробці заходів по захисту систем електронних комунікацій суб'єктів господарювання економіки держави.</p>
<p>4 – Придатність випускників до працевлаштування та подальшого навчання</p>	
Придатність до працевлаштування	<p>Фахівець спроможний виконувати професійні роботи і займати посади, визначені Національним класифікатором України «Класифікатор професій ДК 003:2010», зокрема: 1495 Менеджери (управителі) систем з інформаційної безпеки; 1210.1 Керівник підприємства (установи, організації) (сфера захисту інформації); 2149.2 Професіонал із організації інформаційної безпеки; Професіонал із організації захисту інформації з обмеженим доступом; 3439 Фахівець із організації інформаційної безпеки; Фахівець з</p>

	<p>режиму секретності; Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки; Інспектор з організації захисту секретної інформації.</p> <p>Випускник може обіймати інші посади відповідно до професійних назв робіт, що характеризуються спеціальними (фаховими) компетентностями.</p>
Подальше навчання	<p>Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти.</p> <p>Набуття додаткових кваліфікацій в системі освіти дорослих.</p>
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, самонавчання, навчання через лабораторну практику, проблемні, інтерактивні, проєктні, інформаційно-комп'ютерні, саморозвиваючі, колективні та інтегративні, контекстні технології навчання.
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється на основі: «Положення про організацію освітнього процесу студентів»; «Положення про оцінювання результатів навчання студентів і аспірантів». За 100-бальною шкалою. Письмові екзамени, практична підготовка, презентації, тестування, захист лабораторних робіт, захист індивідуальних проєктів, захист кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (КЗ)	<p>КЗ-1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ-2. Здатність проводити дослідження на відповідному рівні.</p> <p>КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.</p> <p>КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.</p> <p>КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).</p>
Спеціальні (фахові, предметні) компетентності (КФ)	<p>КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.</p> <p>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.</p> <p>КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або</p>

	<p>кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.</p> <p>КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>КФ7. Здатність 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.</p> <p>КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>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.</p> <p>КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.</p> <p><i>КФ11. Здатність аналізувати електронні комунікаційні мережі та протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, зокрема в економіці.</i></p>
7 – Програмні результати навчання	
	<p>РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.</p> <p>РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.</p> <p>РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у</p>

	<p>кіберпросторі.</p> <p>РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.</p> <p>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.</p> <p>РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.</p> <p>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.</p> <p>РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>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.</p> <p>РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.</p> <p>РН16. Приймати обґрунтовані рішення з організаційно-</p>
--	--

	<p>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.</p> <p>PH17. 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.</p> <p>PH18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.</p> <p>PH19. 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.</p> <p>PH20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.</p> <p>PH21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.</p> <p>PH22. 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.</p> <p>PH23. 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.</p> <p><i>PH24. Приймати обґрунтовані рішення та вживати відповідних технічних та організаційних заходів для забезпечення безпеки електронних комунікаційних мереж та послуг з метою гарантування цілісності власних електронних комунікаційних мереж, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до електронних комунікаційних мереж.</i></p>
--	--

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	До реалізації програми залучаються науково-педагогічні працівники з науковими ступенями та/або вченими званнями, а також висококваліфіковані спеціалісти та фахівці-практики.
Матеріально-технічне забезпечення	Використання лабораторій, комп'ютерних та спеціалізованих аудиторій, бібліотеки та інфраструктури ДТЕУ вцілому.
Інформаційне та навчально-методичне забезпечення	Єдиний цифровий простір Університету поєднує всі підрозділи, які направлені на формування індивідуальної траєкторії здобувача вищої освіти. Діюча система дистанційного навчання MOODLE та середовище MS 365 забезпечує самостійну та індивідуальну роботу студентів.
9 – Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність здійснюється відповідно до укладених договорів про академічну мобільність
Міжнародна кредитна мобільність	Міжнародна кредитна мобільність реалізується за рахунок укладання договорів про міжнародну академічну мобільність (Еразмус+), про подвійне дипломування, про тривалі міжнародні проекти, які передбачають навчання студентів, видачу подвійного диплому, тощо.
Навчання іноземних здобувачів вищої освіти	Передбачено, за умови обов'язкового знання української мови на рівні не нижче B1.

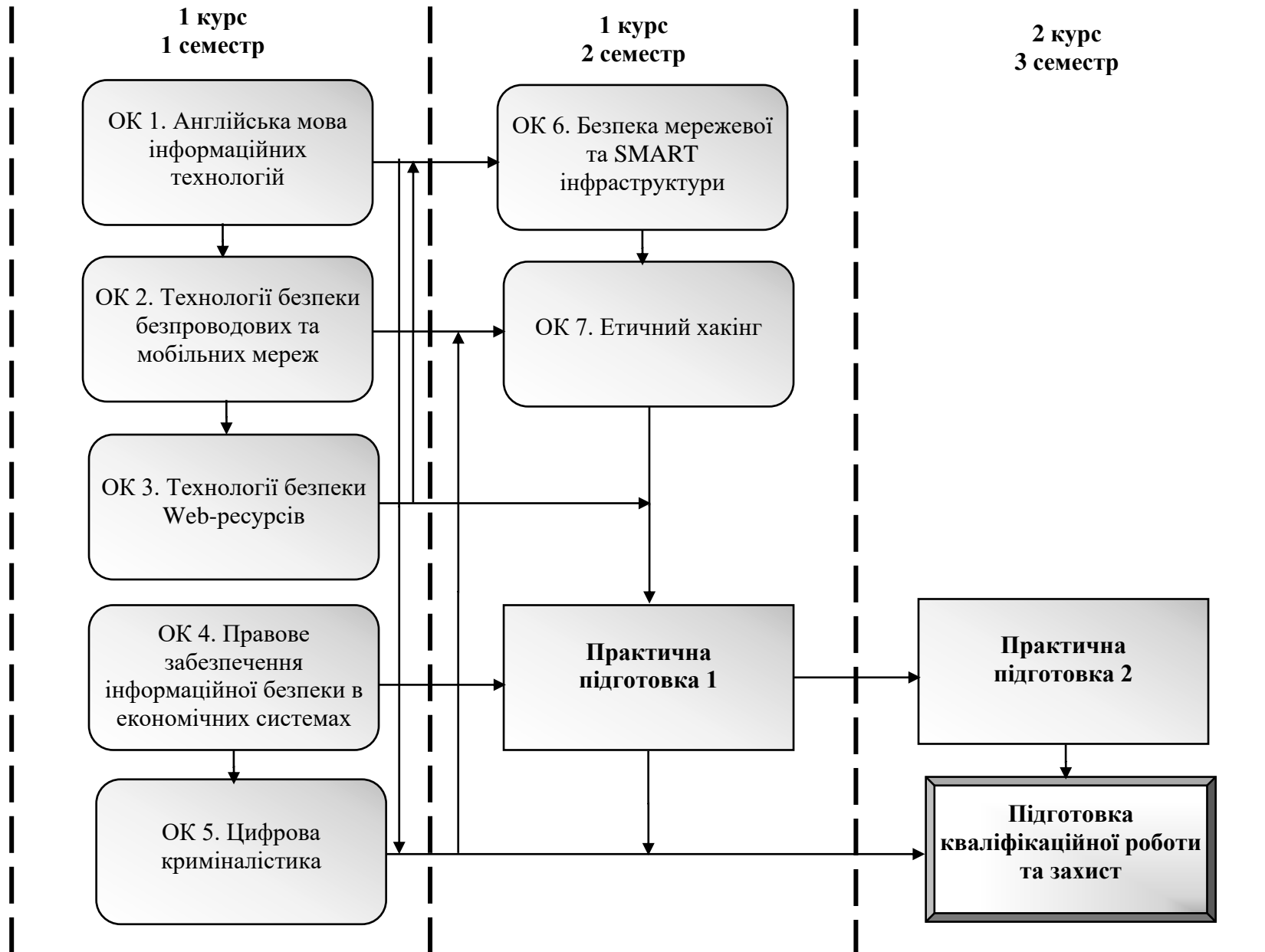
2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційний екзамен, випускна кваліфікаційна робота)	Кількість кредитів
1	2	3
Обов'язкові компоненти ОП		
ОК 1.	Англійська мова інформаційних технологій	6
ОК 2.	Технології безпеки безпроводових та мобільних мереж	6
ОК 3.	Технології безпеки Web-ресурсів	6
ОК 4.	Правове забезпечення інформаційної безпеки в економічних системах	6
ОК 5.	Цифрова криміналістика	6
ОК 6.	Безпека мережевої та SMART інфраструктури	6
ОК 7.	Етичний хакінг	6
Загальний обсяг обов'язкових компонент:		43,5
Вибіркові компоненти ОП		
ВК 1	Адміністрування та захист сховищ даних	6
ВК 2.	Безпека мобільних додатків	6
ВК 3.	Безпека технологій інтернету речей	6
ВК 4.	Безпека життя	
ВК 5.	Біометричні технології аутентифікації в інформаційних системах	6
ВК 6.	Інструментальні засоби бізнес-аналітики	6
ВК 7.	Інтелектуальна власність	6
ВК 8.	Інформаційні технології у системі забезпечення економічної безпеки держави	6
ВК 9	Інформаційні війни	6
ВК 10.	ІТ-право	6
ВК 11.	Комерційна розвідка та внутрішня безпека на підприємстві	6
ВК 12.	Психологія адаптації	6
ВК 13.	Психологія бізнесу	6
ВК 14.	Стохастичні методи в економіці	6
ВК 15.	Технології аналізу даних	6
ВК 16.	Філософія особистості	6
ВК 17.	Функціональне та логічне програмування	6
Загальний обсяг вибірових компонент:		24
Практична підготовка		
	Практична підготовка 1	12
	Практична підготовка 2	3
Атестація		
	Підготовка випускної кваліфікаційної роботи та захист	9
Загальний обсяг освітньої програми		90

Для всіх компонентів освітньої програми формою підсумкового контролю є екзамен.

2.2. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.

Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки передбачати проведення досліджень та/або здійснення інновацій.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4.1. Матриця відповідності програмних компетентностей обов'язковим компонентам освітньої програми

Компоненти Компетентності	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7
КЗ-1.	+	+	+	+	+	+	+
КЗ-2.	+	+	+	+	+		+
КЗ-3.					+	+	+
КЗ-4.			+		+	+	
КЗ-5.	+	+		+	+		+
КФ1.	+	+	+	+	+	+	+
КФ2.	+	+	+	+	+	+	+
КФ3.		+		+	+	+	+
КФ4.		+		+		+	+
КФ5.		+	+			+	+
КФ6.			+				
КФ7.			+		+		
КФ8.						+	
КФ9.		+				+	+
КФ10.	+			+			+
КФ11.		+				+	

4.2. Матриця відповідності програмних компетентностей вибіркоким компонентам освітньої програми

Компоненти Компетентності	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17
КЗ-1.		+	+	+	+	+	+		+	+	+	+	+	+	+	+	+
КЗ-2.		+		+	+	+			+			+	+			+	+
КЗ-3.	+		+		+			+				+	+				+
КЗ-4.					+									+		+	
КЗ-5.		+	+	+	+	+	+		+	+	+	+	+	+			
КФ1.	+	+			+		+	+							+		+
КФ2.		+	+		+	+										+	
КФ3.					+												
КФ4.					+						+						
КФ5.			+		+									+			
КФ6.	+				+			+							+		
КФ7.					+												
КФ8.																+	
КФ9.	+		+			+											
КФ10.											+						
КФ11.			+														

5.1. Матриця забезпечення програмних результатів навчання відповідними обов'язковими компонентами освітньої програми

Компоненти Програмні результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7
PH1	+	+		+			+
PH2	+	+				+	+
PH3			+		+		+
PH4		+	+		+	+	+
PH5	+			+		+	
PH6				+	+	+	
PH7	+		+	+	+	+	
PH8		+				+	+
PH9		+					+
PH10		+	+			+	+
PH11		+	+				+
PH12			+	+	+		
PH13		+				+	+
PH14				+		+	
PH15		+	+				+
PH16			+			+	
PH17	+	+		+	+	+	+
PH18							+
PH19			+				
PH20		+			+	+	+
PH21			+		+	+	
PH22			+	+	+		
PH23	+		+		+	+	
PH24		+				+	

5.2. Матриця забезпечення програмних результатів навчання відповідними вибірковими компонентами освітньої програми

Компоненти Програмні результати навчання	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17
PH01				+	+	+	+		+	+		+	+	+		+	
PH02			+	+	+					+	+				+		+
PH03					+						+			+			
PH04	+	+			+	+		+									+
PH05					+						+				+		
PH06		+			+						+						
PH07		+	+		+		+							+			
PH08					+							+					
PH09			+		+												
PH10			+		+						+						
PH11	+					+		+									
PH12					+										+		
PH13			+														
PH14	+		+														
PH15					+												
PH16					+						+						+
PH17					+												
PH18			+														
PH19					+												
PH20		+			+												
PH21					+												
PH22					+												
PH23		+			+									+		+	+
PH24			+														

4. Інформація про освітні компоненти (дисципліни)

4.1. Назва. АНГЛІЙСЬКА МОВА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Тип. Обов'язкова.

Рік навчання. 2023/2024.

Семестр. I.

Лектор, вчене звання, науковий ступінь, посада. Староста Г.А., старший викладач кафедри сучасних європейських мов; Семідоцька В.А., старший викладач кафедри сучасних європейських мов.

Результати навчання. Дисципліна «Англійська мова інформаційних технологій», як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами фаховими та загальними компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою. Результатами навчання є формування практичних навичок, необхідних для пошуку, систематизації інформації і комунікації англійською мовою у галузі інформаційних технологій.

Обов'язкові попередні навчальні дисципліни. «Іноземна мова за професійним спрямуванням (англійська)».

Зміст. AI (Artificial Intelligence) – predictions, implementation, after-effects AI. (Штучний інтелект) – прогнози, реалізація, наслідки. Принципи використання штучного інтелекту. Штучний інтелект у процесах глобалізації. Вплив штучного інтелекту на формування ринку праці. Людино-машинна взаємодія. Чат бот. Автоматизація задач за допомогою штучного інтелекту. Автоматизація розсилок. Cloudtechnologies. Хмарні Технології. Поняття хмари. Підприємство в хмарі. Суб'єкти хмарних послуг. Кубернетес. IoT (Internetofthings). Інтернет речей. Поняття і визначення Інтернету речей. Типи мереж та їх функції у розповсюдженні і зберіганні інформації. Інтернет речей і технології розумного дому. Персональний цифровий помічник. Роль AzureSecurityCenter в кіберзахисті Інтернету речей. Robotization. Роботизація. Industry 4.0: технології штучного інтелекту, змішаної реальності та автоматизації. Технології провідних виробників продуктів сфери інформаційних технологій у виробництві і наданні послуг. Програмний робот (RoboticProcessAutomation). Автоматизація процесів з використанням програмних роботів (RPA). Віртуальне робоче місце RPA. Чат-боти. Когнітивна автоматизація. Перспективи розвитку і наслідки автоматизації та роботизації у глобальних

процесах. Cybersecurityandpersonaldataprotection. Кібербезпека та захист персональних даних. Поняття кібербезпеки. Кібергігієна. Методи і засоби захисту інформації в комп'ютерних системах. Захист систем електронних комунікацій. Захист інформаційної системи підприємства. Блокчейн і персональний електронний підпис. Роль AzureSecurityCenter в кіберзахисті Інтернету речей. Пошук інформації в науково-метричних базах даних Scopus, WebofScience.

Рекомендовані джерела та інші навчальні ресурси / засоби.

1. Портал навчальних ресурсів Microsoft – URL:

<https://education.microsoft.com/>

2. Портал хмарного сервісу Azure Microsoft –

URL:<https://azure.microsoft.com/en-us/training/>

Заплановані навчальні заходи та методи викладання.

Практичні заняття, самостійна робота. Інтерактивні методи та технології викладання, комп'ютерне тестування.

Методи оцінювання:

– поточний контроль (тестування з граматики, наукова доповідь, фронтальне опитування, тести з читання, завдання для перевірки писемного мовлення, завдання для перевірки усного мовлення, контрольна робота);

– підсумковий контроль (екзамен).

Мова навчання та викладання. Англійська.

4.2. Назва. ТЕХНОЛОГІЇ БЕЗПЕКИ БЕЗПРОВОДОВИХ ТА МОБІЛЬНИХ МЕРЕЖ

Тип. Обов'язкова.

Рік навчання. 2023/2024.

Семестр. I.

Лектор, вчене звання, науковий ступінь, посада. Власенко Л.О., доцент, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Формування у майбутніх спеціалістів умінь та компетенцій для оцінювання та забезпечення необхідного рівня захищеності інформації в безпроводових та мобільних мережах; уміння вирішувати задачі адміністрування безпроводових та мобільних мереж, застосовувати нормативно-правові, організаційні та технічні процедури при роботі безпроводових і мобільних технологій; надання знань з питань безпеки та захисту сучасних безпроводових та мобільних мереж; захист сучасного програмно-апаратного забезпечення безпроводових та мобільних мереж.

Обов'язкові попередні навчальні дисципліни: «Організація комп'ютерних мереж», «Безпека інформаційних систем та мереж».

Зміст. Основи теорії безпроводової передачі. Загрози, атаки та захист безпроводових мереж. Мережеві протоколи та служби. Мережева інфраструктура для безпроводових мереж. Стандарти мереж мобільного зв'язку. Загрози та вразливості мобільних пристроїв. Архітектура безпроводових мережі 4G та 5G. Безпека безпроводових мереж 4G та 5G. Архітектура WiFi-технологій. Загрози та вразливості WiFi-мереж. Моніторинг безпеки безпроводових мереж. Шляхи захисту безпроводових мереж. Мережі ширококутового безпроводового доступу сімейства стандартів IEEE 802.16 (WiMAX). Безпека безпроводових сенсорних мереж WSN. Безпека персональних безпроводових мереж ZigBee. Безпека персональних безпроводових мереж Bluetooth. Безпека безпроводової мережі WiFi. Безпроводова система виявлення вторгнень WIDS. Захист мереж від несанкціонованого доступу з використанням технології VPN.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Бурячок В.Л., Соколов В.Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів: навчальний посібник. Київ: КУБГ, 2019. 164 с.

2. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарев та інші; за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.

3. Безпека інформаційних систем: навч. посіб. / В.І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.

Заплановані навчальні заходи та методи викладання. Вивчення дисципліни проводиться шляхом лекційних (аудиторних) та лабораторних занять (у комп'ютерному класі на ПК), що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.

Методи оцінювання.

- поточний контроль (комп'ютерне тестування, опитування);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.3. Назва. ТЕХНОЛОГІЇ БЕЗПЕКИ WEB-РЕСУРСІВ

Тип. Обов'язкова.

Рік навчання. 2023/2024.

Семестр. I.

Лектор, вчене звання, науковий ступінь, посада. Котенко Н.А., доцент, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результатив навчання. Формування теоретичних знань та практичних навичок з питань захисту веб-застосунків, починаючи з етапів розвідки та пошуку вразливостей, типових вразливостей серверної та клієнтської частини веб-застосунку, а також формування навичок пошуку та виправлення проблем кодування веб-застосунку.

Обов'язкові попередні навчальні дисципліни. «Інформаційні технології у професійній діяльності», «WEB-дизайн та WEB-програмування».

Зміст. Основи конфігурації безпеки Інтернету: протокол передачі гіпертексту; HTTPS (протокол передачі гіпертексту через захищені сокети); протокол SSL (SecureSocketsLayer); симетричне та асиметричне шифрування; використання протоколу простого доступу до об'єктів (SOAP); протокол SMTP (SimpleMailTransferProtocol); протокол поштового відділення (POP3); протокол доступу до Інтернету (IMAP). Огляд технологій веб-автентифікації. Брандмауери веб-додатків. Огляд топ-10 списку OWASP. Розвідка і уразливості веб-додатків: відкриття веб-сторінки/структури програми; збір інформації в веб-застосунках; Сканування вразливостей веб-додатків. Безпека серверної частини веб-додатків: введення в server-side-уразливості, SQL-ін'єкція, автентифікація та авторизація веб-додатків, XXE-ін'єкція, SSRF-підробка запитів на стороні сервера, вразливості бізнес-логіки, та ін. Безпека клієнтської частини веб-додатків: міжсайтові сценарії (XSS), підробка міжсайтових запитів (CSRF), перехресне спільне використання ресурсів (CORS), вразливості на основі DOM, та ін. Інші вразливості клієнтської частини веб-додатків: небезпечна десеріалізація, отруєння веб-кешем, атаки заголовків хостів HTTP, автентифікація OAuth, безпека XML.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. OWASP TopTen. URL: <https://owasp.org/www-project-top-ten/>
2. Professional PenTestingforWebApplications. FrontCover. AndresAndreu. WileyIndiaPvt. Limited, 2016.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання із використанням інноваційних технологій: лекції (тематична, проблемна); лабораторні заняття з використанням сучасних інтерактивних технологій (традиційні, моделювання ситуацій); самостійна робота; консультації.

Методи оцінювання:

– поточний контроль (комп'ютерне тестування, опитування);

– підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.4. Назва. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЕКОНОМІЧНИХ СИСТЕМАХ

Тип. Обов'язкова.

Рік навчання. 2023/2024.

Семестр. I.

Лектор, науковий ступінь, посада. Ситніченко О.М., кандидат юридичних наук, доцент кафедри правового забезпечення безпеки бізнесу.

Результати навчання. Формування у студентів глибоких теоретичних знань в сфері інформаційної безпеки, опанування прийомів і методів захисту інформаційних ресурсів підприємств, установ та організацій, які допоможуть їм створити умови для захисту інформації від несанкціонованого доступу, виявити та притягнути винних осіб до відповідальності за незаконне поширення інформації.

Обов'язкові попередні навчальні дисципліни. «Правознавство», «Інформаційне право».

Зміст. Теоретико-правові засади інформаційної безпеки. Компетенція держави у сфері інформаційної безпеки України. Додержання інформаційних прав і свобод людини як основа інформаційної безпеки. Інформація в житті держави, людини та суспільства. Додержання інформаційних прав і свобод людини як основа інформаційної безпеки. Організаційно-правові основи захисту та обмеження обігу інформації в цілях забезпечення інформаційної безпеки. Організаційне забезпечення захисту інформації підприємства. Інформаційні ресурси підприємства, банку. Організація інформаційно-аналітичної роботи на підприємстві, банку. Правові засади безпеки інформаційної інфраструктури. Кібербезпека. Види юридичної відповідальності за правопорушення в інформаційній сфері.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Бабала Ю.Я, Горбатий І.В, Кіселичник М.Д., Бондарев А.П, Войтусік С.С. Інформаційна безпека: навч. посібник за заг. ред. Ю.Я. Бабала, І.В Горбатий, М.Д. Кіселичник, А.П Бондарев, С.С. Войтусік. – Видавництво «Львівська політехніка» – 2019. – 580 с.
2. Гуз А.М., Мамченко С.М., Ткачук Т.Ю. та ін. Кадрова політика у сфері інформаційної безпеки: навч. посіб. – Київ.: Нац. акад. СБУ, 2017. – 210 с.
3. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. – 446 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання із використанням інноваційних технологій: лекції (оглядові), семінарські/ практичні заняття (тренінг/ презентація/ дискусія/ робота в малих групах/ інше).

Методи оцінювання.

- поточний контроль (опитування, письмові роботи, ситуаційні завдання);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.5. Назва. ЦИФРОВА КРИМІНАЛІСТИКА

Тип. Обов'язкова.

Рік навчання. 2023/2024.

Семестр. I.

Лектор, вчене звання, науковий ступінь, посада. Власенко Л.О., доцент, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Теоретичні основи і сучасні інформаційні технології аналізу та збору криміналістичної цифрової інформації; особливості проведення статистичного аналізу зловмисного програмного забезпечення; принципи роботи програмного забезпечення з відкритим кодом для збору цифрової криміналістичної інформації; сучасний стан і шляхи розвитку цифрової криміналістики.

Обов'язкові попередні навчальні дисципліни. «Основи кібербезпеки», «Безпека операційних систем», «Програмні комплекси захисту інформаційних систем», «Аналіз та оцінка вразливостей інформаційних систем».

Зміст. Введення в цифрову криміналістику. Юридичні аспекти цифрової криміналістики. Розуміння ролі цифрових доказів. Цифрова криміналістика файлових систем. Технічні засоби цифрової криміналістики. Спеціалізоване програмне забезпечення для цифрової криміналістики. Цифрова криміналістика операційних систем: OS WINDOWS. Цифрова криміналістика операційних систем: macOS. Криміналістика мобільних пристроїв. Мережева криміналістика. Онлайн криміналістика: криміналістичне розслідування електронної пошти, вебсайту та соціальних мереж. Хмарна криміналістика.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Шеремет А.П. Криміналістика: навч. пос. для студ. вищ. навч. закл. / А.П. Шеремет. – К.: Центр учбової літератури, 2019. – 472 с.

2. Bill Nelson, Amelia Phillips, Christopher Stuart. Guide to Computer Forensics and Investigations Fifth Edition. Cengage Learning, Boston, 2022. – 690 p.

Заплановані навчальні заходи та методи навчання. Поєднання традиційних та нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); практичні заняття (традиційні); самостійна робота (з використанням елементів програмування).

Методи оцінювання:

- поточний контроль (комп'ютерне тестування, опитування);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.6. Назва. БЕЗПЕКА МЕРЕЖЕВОЇ ТА SMART ІНФРАСТРУКТУРИ

Тип. Обов'язкова.

Рік навчання. 2023/2024.

Семестр. II.

Лектора, вчене звання, науковий ступень, посада. Власенко Л.О., доцент, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Освоєння принципів побудови безпеки комп'ютерних мереж для їх використання в сучасних інформаційних системах; дослідження різних механізмів захисту мереж даних, від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів; засвоєння основ розробки та програмування пристроїв, які працюють з використанням смарт-технологій та технологій «Інтернету речей»; отримання теоретичних знань та практичних вмінь в сфері впровадження, безпечної експлуатації та супроводження SMART інфраструктури.

Обов'язкові попередні навчальні дисципліни. «Основи кібербезпеки»; «Безпека операційних систем»; «Безпека інформаційних систем та мереж»; «Організація комп'ютерних мереж».

Зміст. Причини захисту мереж. Вектори мережеских атак. Найпоширеніші вектори втрати даних: електронна пошта/соціальні мережі; нешифровані пристрої; пристрої хмарного зберігання; знімні носії, паролі, тощо. Політичні аспекти безпеки мережі. Захист мережескої інфраструктури: маршрутизаторів, комутаторів, серверів, кінцевих точок та інших пристроїв. Три області безпеки маршрутизатора. Налаштування безпечного адміністративного доступу. Безпечний локальний та віддалений доступ. Налаштування SSH. Фільтрація трафіку та пом'якшення мережеских атак на мережу.

Мережеві системи запобігання вторгненням для захисту мережі. Безпека кінцевих точок. Загрози безпеки 2-го рівня моделі OSI. Віртуальні приватні мережі (VPN) для створення наскрізних приватних мережевих з'єднань. Тестування безпеки мережі. Введення в SMART безпеку. Безпека SMART інфраструктури. Апаратні засоби та технології SMART інфраструктури. Ризики цифрової безпеки для соціально-економічної діяльності SMART інфраструктури. Стан і головні небезпеки цифровізації на шляху розбудови SMART інфраструктури в містах України. Необхідність безпеки Інтернету речей у SMART інфраструктурі. Безпека обладнання та заходи щодо зменшення загроз пристроям IoT. Атаки на комунікаційному рівні IoT. Атаки рівня додатків IoT. Оцінка вразливості та тестування на проникнення систем IoT.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. Підручник. / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.: КУБГ, 2019. – 218 с.
2. MarkCiampa, Ph.D. CompTIA® Security+ GuidetoNetworkSecurityFundamentals, FifthEdition. CengageLearningCustomer&SalesSupport, 2015. – 724 p.
3. Mike, Chapple, Gibson, Darril, Stewart, JamesMichael. (ISC)² CISSP certifiedinformationsystemssecurityprofessional: officialstudyguide. PublishedsimultaneouslyinCanada, 2018. - 1107 p.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні) з використанням мультимедійних засобів та демонстрацією відеороликів; практичні роботи (традиційні, тренінгові завдання, комп'ютерне тестування).

Методи оцінювання:

- поточний контроль (опитування, тестування);
- підсумковий контроль (письмовий екзамен).

Мова навчання та викладання. Українська.

4.7. Назва. ЕТИЧНИЙ ХАКІНГ

Тип. Обов'язкова.

Рік навчання. 2023/2024.

Семестр. II.

Лектор, вчене звання, науковий ступінь, посада. Зверев В.П., с.н.с., кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання.Набуття теоретичних знань і практичних навичок, необхідних професіоналу із захисту інформації у сфері технологій збору інформації про комп'ютерні системи, проведення аудиту і пентестингу інформаційних систем, планування та здійснення атаки на захисні механізми операційних систем і додатків; роботі із засобами виявлення вразливостей та виконання аналізу захищеності інформаційних систем.

Обов'язкові попередні навчальні дисципліни: «Технології безпеки безпроводових та мобільних мереж», «Цифрова криміналістика», «Правове забезпечення інформаційної безпеки в економічних системах».

Зміст.Хакінг: концепція, види і стадії. Складові етичного хакінгу. Основні терміни і поняття хакінгу. Сертифікація хакінгу. Фази хакінгу (ланцюг кібервбивства): підготовка, проникнення, поширення та закріплення в системі, досягнення цілей атаки, замітання слідів. Таргетовані та АТР –атаки. Техніки і інструменти DoS/DDoS атак. Атаки на Web-додатки. Проект OWASP. Методологія, інструмент та способи збирання інформації. Збір інформації без явного підключення до об'єкта атаки (footprinting). Аналіз публічно доступних ресурсів про об'єкт атаки. Інструментарій Google: GoogleHackingDatabase (GHDB). Збір інформації реєстраційного характеру. Методика збору інформації OSINT. Алгоритми та способи сканування мережі. Ідентифікація вузлів мережі. Ідентифікація відкритих портів. Інструменти сканування. Ідентифікація сервісів та додатків. Ідентифікація операційних систем. Визначення топології мережі. Отримання інформації з бази серверів DNS. Прийоми скритого сканування і ухиляння від систем виявлення вторгнень IDS. Шпигунське програмне забезпечення. Способи зараження систем. Способи обходу антивірусного захисту. Руткіти, їх різновиди, принципи роботи, методи виявлення. Атаки на механізми реєстрації подій: чищення журналів реєстрації, спотворення результатів аудиту. Управління скомпрометованими системами (використання троянів і «бекдорів»). Сховані та відкриті канали взаємодії. Способи приховування слідів. Інструменти та техніки підбору облікових даних і паролів користувачів. Методи аудиту парольного захисту. Аналіз захищеності інформаційних систем. Пошук і експлуатація вразливостей системи. Сканери безпеки: NessusSecurityScanner і LANguardNetworkSecurityScanner. Аудит безпеки інформаційних систем. Стандарт і концепція виконання тесту на проникнення. Типи, техніки та фази пентесту. Підготовка до пентесту: договір про проведення робіт, дозвіл на тестування. Сбір даних. Моделювання загроз. Аналіз і експлуатація вразливостей.

Перевірка стійкості систем до атак. Атестація системи. Підготовка звіту. Інструменти етичного хакінгу.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Weidman G. PenetrationTesting: A Hands-OnIntroductiontoHacking. – NY.: Press.Inc, 2014. – 478 p.
2. JonErickson, Hacking: TheArtOfExploitation, 2nd Edition. – SanFrancisco, 2008. – 475 p.
3. Інформаційна безпека: навчальний посібник. / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А. П. Бондарев та інші; за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. – Львів : Видавництво «Львівська політехніка», 2019. – 580 с.

Заплановані навчальні заходи та методи викладання. Вивчення дисципліни проводиться шляхом лекційних (аудиторних) та лабораторних занять (у комп'ютерному класі на ПК), що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.

Методи оцінювання.

- поточний контроль (комп'ютерне тестування, опитування);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.8. Назва. АДМІНІСТРУВАННЯ ТА ЗАХИСТ СХОВИЩ ДАНИХ.

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Рзаєва С.Л., доцент, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Формування теоретичних знань та практичних навичок необхідних для аналізу ефективності обраної системи захисту сховищ даних, обґрунтування вибору технічних і програмних засобів для ефективного адміністрування та захисту сховищ даних; забезпечення надійності функціонування сховищ даних, з врахуванням факторів помилки користувачів.

Обов'язкові попередні навчальні дисципліни: «Хмарні та GRID-технології», «Технології проектування інформаційних систем».

Зміст. Поняття бази даних, сховища даних, системи баз даних. Характеристика та класифікація OLTP – систем, OLAP – систем. Загальна характеристика сховищ даних (DataWarehouse). Типи сховищ даних – систем: MOLAP (Multidimensional), ROLAP (Relational), HOLAP (Hybrid). Характеристика багатовимірної моделі даних.

Програмні засоби сховища даних: засоби інтеграції неоднорідних баз даних, засоби управління даними сховища, засоби аналізу даних (DataMining), засоби візуалізації результатів обробки. Створення вітрин даних (DataMart). Засоби захисту сховищ даних (DataWarehouse). Загальна характеристика NoSQLTP – систем, OLAP – систем. систем управління даними. Засоби захисту NoSQLTP – систем, OLAP – систем. систем управління даними. Загальна характеристика NewSQLTP – систем, OLAP – систем. систем управління даними. Засоби захисту NewSQLTP – систем, OLAP – систем. систем управління даними. Загальна характеристика хмарних систем управління даними. Засоби захисту хмарних систем управління даними. Захист озер даних.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Демиденко М.А. Введення в сучасні бази даних :навч. посіб. / М.А. Демиденко. – Д. : НТУ «Дніпровська політехніка, 2020. – 38 с.
2. Пасічник В.В. Сховища даних: підручник. / В.В. Пасічник, Н.Б.Шаховська– Л. : Магнолія, 2021. – 496 с.
3. MattHowTheModernDataWarehouseinAzure: BuildingwithSpeedandAgilityonMicrosoft’sCloudPlatform. – Apress; 1st ed. edition (June 16, 2020), 304p.

Заплановані навчальні заходи та методи викладання. Вивчення дисципліни проводиться шляхом лекційних (аудиторних) та лабораторних занять (у комп’ютерному класі на ПК), що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.

Методи оцінювання.

- поточний контроль (комп’ютерне тестування,опитування);
- підсумковий контроль(екзамен).

Мова навчання та викладання.Українська.

4.9. Назва. БЕЗПЕКА МОБІЛЬНИХ ДОДАТКІВ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. ЖироваТ.О., кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання.Формування теоретичних знань та практичних навичок з таких питань: основні загрози для мобільного ПЗ; захистінформації в мобільних ОС; безпека AppleiOS; безпека GoogleAndroid; тестування безпеки мобільних додатків.

Обов'язкові попередні навчальні дисципліни. «Інформаційні технології в професійній діяльності», «WEB-дизайн та WEB-програмування», «Основи кібербезпеки».

Зміст. Вступ. Історія розвитку мобільних додатків та їх класифікація. Захист інформації в мобільних ОС. Загальні принципи безпеки і конфіденційності даних мобільних пристроїв. Безпека Apple iOS. Підвищення захисту Apple iOS. Безпека Google Android. Техніки обходу захисту користувацьких даних та підвищення захисту Android. Тестування безпеки мобільних додатків. Інструменти тестування безпеки мобільних додатків. Автоматизація тестування безпеки мобільних додатків.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Шматко О.В. Аналіз методів і технологій розробки мобільних додатків для платформи Android: навч. посіб. / О.В. Шматко, А.О. Поляков, В.М. Федорченко. – Харків: НТУ «ХПІ», 2018. – 284 с.

2. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. Підручник. / В.Л. Бурячок, А.О.Аносов, В.В.Семко, В.Ю.Со-колов, П.М.Складанний. – К.: КУБГ, 2019. – 218 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання із використанням інноваційних технологій: лекції (тематична, проблемна); лабораторні заняття з використанням сучасних інтерактивних технологій (традиційні, моделювання ситуацій); самостійна робота; консультації.

Методи оцінювання:

– поточний контроль (комп'ютерне тестування, опитування);

– підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.10. Назва. БЕЗПЕКА ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Власенко Л.О., доцент, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Формування теоретичних знань та практичних навичок з таких питань: загальноновизнані технології та стандарти для забезпечення безпеки IoT, безпека обладнання IoT, безпека хмарних технологій в IoT, безпека в цифровому світі на основі IoT.

Обов'язкові попередні навчальні дисципліни. «Інформаційні технології у професійній діяльності», «Основи кібербезпеки».

Зміст. Вступ. Вступ. Цифрова трансформація бізнесу. Загально визнані технології та стандарти для забезпечення безпеки IoT. Апаратна частина «Інтернету Речей». Безпека обладнання IoT. Застосування автоматизації в IoT. Застосування BigData для підтримки пристроїв IoT. Застосування AI та ML, базового програмування для підтримки пристроїв IoT. Застосування хмарних технологій в IoT. Безпека в цифровому світі на основі IoT. Принципи безпечного підключення «Інтернету Речей» до мережі. Приклади безпечного підключення пристроїв Інтернету речей.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Hanes D. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. 1st ed. Cisco Press, 2017. 576 p.
2. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. Підручник. / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.: КУБГ, 2019. – 218 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання із використанням інноваційних технологій: лекції (тематична, проблемна); лабораторні заняття з використанням сучасних інтерактивних технологій (традиційні, моделювання ситуацій); самостійна робота; консультації.

Методи оцінювання:

- поточний контроль ((комп'ютерне тестування, опитування);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.11. Назва. БЕЗПЕКА ЖИТТЯ.

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II - III.

Лектор, вчене звання, науковий ступінь, посада. Расулов Р.А., доц., канд. техн. наук, доцент кафедри дизайну та інжинірингу.

Результати навчання.

Знати кодекс професійної етики, розуміти соціальну значимість та культурні аспекти інженерії програмного забезпечення і дотримуватись їх в професійній діяльності.

Обов'язкові попередні навчальні дисципліни.

«Правознавство», «Філософія».

Зміст.

Оцінка небезпек. Ризики. Ризики під час надзвичайних ситуацій. Організаційні заходи збереження життя персоналу і споживачів та їх рятування. Основи рятування і збереження життя людини у

невідкладному стані (домедична допомога). Нормативно-правове та організаційне забезпечення безпеки життя працівників. Державний нагляд і громадський контроль за безпекою праці в Україні. Світовий досвід та міжнародне співробітництво у сфері безпеки праці. Директиви ЄС і конвенції МОП, впровадження їх в Україні. Ризик-орієнтовне управління професійною безпекою. Стратегія діяльності керівника підприємства. Оцінка ризику виробничих травм. Профілактика виробничого травматизму. Чинники виробничого середовища, їх вплив на працюючих, нормування та нормалізація. Виробнича безпека працюючих. Електробезпека: правила та відповідальність. Забезпечення відповідності робочого місця нормативним вимогам та його комплексна оцінка. Ризики пов'язані з пожежами. Пожежна безпека будівель та споруд. Пожежна безпека та профілактика: обов'язки та відповідальність керівника підприємства, установ та організацій.

Рекомендовані джерела та інші навчальні ресурси/засоби:

1. Безпека життя діяльності : навч. посіб. / О.І. Запорожець – К., Центр навчальної літератури, 2019. – 448 с.
2. Основи охорони праці. : навч. посіб. / О. Запорожець, О. Протоєрейський, Г. Франчук, І. Боровик - К. : Центр навч. л-ри, 2021. — 264 с.
3. Охорона праці. : навч. посіб. / В. Грибан, О. Негодченко - К. : Центр навч. л-ри, 2021.– 280 с,
Заплановані навчальні заходи та методи навчання.
– поточний контроль (тестування, усне / письмове опитування);
– підсумковий контроль (екзамен).

Методи оцінювання.

Тестування; захист індивідуальних завдань, презентація та оцінка результатів самостійної та науково дослідної роботи, письмовий іспит.

Мова навчання та викладання. Українська.

4.12. Назва. БІОМЕТРИЧНІ ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Франчук Т.М., кандидат економічних наук, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Вивчення основних положень сучасних біометричних технологій, опанування методів та методологістворення біометричних систем автентифікації, що дозволяють підвищити надійність функціонування складних інформаційних систем.

Обов'язкові попередні навчальні дисципліни: «Методи і засоби захисту інформації в комп'ютерних системах», «Безпека інформаційних систем та мереж».

Зміст. Біометрія, біометричні технології: основні поняття та визначення. Правові засади застосування біометричних технологій в захисті інформації. Біометричні системи захисту, взаємодія з іншими системами. Програмні засоби біометричних технологій. Методи автентифікації біометричних систем. Сучасні види біометричних технологій, позитивні і негативні сторони застосування кожної з них. Області застосування біометричних систем. Застосування біометричних технологій для захисту сучасних систем передачі даних. Основні напрямки розвитку біометричних технологій.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Царьов Р.Ю. Біометричні технології: навч. посіб. / Р.Ю. Царьов, Т.М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова. – 2019. – 140 с.
2. Корченко О. Методологія розроблення нейромережових засобів інформаційної безпеки Інтернет-орієнтованих інформаційних систем: навч. посіб. / О. Корченко, І. Терейковський, А. Білощицький. – К.: ТОВ «Наш Формат». – 2019. – 249 с.
3. Тарнавський Ю.А. Технології захисту інформації: підручник. – К.: КПІ ім. Ігоря Сікорського. – 2020. – 162 с.

Заплановані навчальні заходи та методи викладання. Вивчення дисципліни проводиться шляхом лекційних (аудиторних) та лабораторних занять (в комп'ютерному класі на ПК), що забезпечують закріплення теоретичних знань, опанування біометричних технологій автентифікації.

Методи оцінювання:

- поточний контроль (комп'ютерне тестування, опитування, перевірка самостійної роботи);
- підсумковий контроль (екзамен).

Мова навчання та викладання: Українська.

4.13. Назва. ІНСТРУМЕНТАЛЬНІ ЗАСОБИ БІЗНЕС-АНАЛІТИКИ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Роскладка А.А., проф., доктор економічних наук, завідувач кафедри цифрової економіки та системного аналізу.

Результати навчання. Знання основних алгоритмічних елементів мови R, типів даних, процедур імпорту та експорту даних у середовищі RStudio, технологій роботи із великими та розподіленими даними, графіки і візуалізації даних в R, описової статистики даних. Практичні вміння проводити регресійний, дисперсійний, факторний, кластерний бізнес-аналіз з використанням інструментарію мови R.

Обов'язкові попередні навчальні дисципліни. «Вища математика», «Комп'ютерна дискретна математика», «Теорія чисел», «Інформаційні технології в професійній діяльності».

Зміст. Основні поняття аналітики. Аналітичні дані. Види аналітики. Основні компоненти середовища R. Графічний інтерфейс RStudio. Проектування аналітичних веб-додатків за допомогою пакету Shiny. Створення набору бізнес-даних. Типи даних R і принципи роботи з ними. Методи роботи з пропущеними даними. Імпорт даних з мережі Інтернету. Основи управління даними в R. Описова аналітика. Розвідувальна аналітика. Вибір форми візуалізації даних. Індуктивна аналітика. Прогностична аналітика. Дисперсійний аналіз. Кореляційний аналіз. Факторний аналіз. Діагностика моделі даних.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Майборода Р. Є., Сугакова О. В. Аналіз даних за допомогою пакета R: навчальний посібник. – К.: ВПЦ «Київський університет», 2015. – 65 с.
2. Kabacoff R. R inAction. Dataanalysisandgraphicswith R. – Manning: Shelterisland, 2015. – 608 p.
3. Matloff N. ProbabilityandStatisticsforDataScience: Math + R + Data. – London: Chapman&Hall, 2019. – 376 p.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематична, проблемна); лабораторні заняття (традиційні, робота в малих групах).

Методи оцінювання.

- поточний контроль (перевірка індивідуальних завдань, тестування);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.14. Назва. ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Дараганова Н.В., професор, докторюридичних наук, професор кафедри адміністративного, фінансового та інформаційного права; Гуржій А.В., доцент, кандидат юридичних наук, доцент кафедри адміністративного, фінансового та інформаційного права.

Результати навчання. Ознайомлення з нормами міжнародного та національного законодавства в сфері інтелектуальної власності; опанування правових механізмів реєстрації, реалізації та захисту права інтелектуальної власності. Формування навичок здійснювати професійну діяльність, також практично застосовувати нормативні та правові акти. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (демократичного) суспільства, верховенства права, прав і свобод людини і громадянина в Україні. Здатність асоціювати себе як члена громадянського суспільства, розуміти і вміти користуватися власними правами і свободами, виявляти повагу до прав і свобод інших осіб.

Обов'язкові попередні навчальні дисципліни. «Правознавство».

Зміст. Поняття інтелектуальної власності, об'єкти та суб'єкти інтелектуальної власності. Поняття, принципи та джерела авторського права; об'єкти та суб'єкти авторського права; особисті немайнові та майнові права на твори літератури, мистецтва і науки; колективне управління авторськими правами; відповідальність за порушення авторських прав. Правова охорона суміжних прав. Поняття та умови правової охорони винаходів, корисних моделей, промислових зразків. Правова охорона нетрадиційних результатів інтелектуальної власності. Правова охорона засобів індивідуалізації суб'єктів господарського обороту, товарів, робіт і послуг. Поняття та правовий захист комерційних (фірмових) найменувань; торговельної марки та географічних значень. Захист від недобросовісної конкуренції. Відповідальність за порушення прав інтелектуальної власності.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Право інтелектуальної власності: підручник / за заг.ред. О.І.Харитонов. – К.: Юрінком Інтер, 2019. – 540 с.
2. Інтелектуальна власність: навч. посібн. / за ред. О.В. Нестерцової-Собакар. – К.: Дніпро, 2018. – 140 с.
3. Право інтелектуальної власності: підручник. / О.І. Харитонов, Є.О. Харитонов, Т.С. Ківалова, В.С. Дмитришин, О.О. Кулініч, Л.Д. Романадзе та ін. за заг. ред. О.І. Харитонової, 2018. – К.: Юрінком Інтер. – 367 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання із використанням інноваційних технологій: лекції (оглядові, тематичні, проблемні), практичні заняття (презентація, дискусія, комунікативний метод, метод кейс-стаді, індивідуальні завдання тощо).

Методи оцінювання:

- поточний контроль (тестування, усне / письмове опитування, вирішення юридичних задач тощо);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.15. Назва. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Токар В.В., професор, доктор економічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. У результаті вивчення дисципліни студенти повинні знати: зміст основних понять курсу: «безпека», «економічна безпека», «економічна безпека держави» тощо; базові принципи та концепції забезпечення економічної безпеки держави з використанням інформаційних технологій; основні методи оцінювання та аналізу загроз економічній безпеці на мікро-, макро- та глобальному рівнях; основні методи та прийоми розрахунку порогових значень індикаторів економічної безпеки держави; принципи формування та стратегії забезпечення економічної безпеки із застосуванням інформаційних технологій на національному, регіональному та глобальному рівнях; методичні підходи до аналізу та оцінювання рівня економічної безпеки на мікро-, макро- та глобальному рівнях; повинні вміти: здійснювати пошук та обробку інформації стосовно загроз економічній безпеці на мікро-, макро- та глобальному рівнях; застосовувати математичні методи для аналізу і обробки даних з метою оцінювання рівня економічної безпеки держави; проводити аналіз економічної безпеки держави за окремими складовими; використовувати існуючі програмні рішення для спрощення розрахунків.

Обов'язкові попередні навчальні дисципліни. «Інформаційні технології в професійній діяльності», «Об'єктно-орієнтоване програмування», «WEB-дизайн та WEB-програмування».

Зміст. Співвідношення понять ризик і загроза. Класифікація загроз.

Генезис поняття безпека. Поняття економічна безпека. Ієрархія поняття економічна безпека. Складові економічної безпеки. Поняття економічна безпека держави. Компоненти економічної безпеки держави. Макроекономічна безпека держави. Зовнішньоекономічна безпека держави. Науково-технологічна безпека держави. Енергетична безпека держави. Соціальна безпека держави. Демографічна безпека держави. Продовольча безпека держави. Виробнича безпека держави. Сутність фінансової безпеки. Складові фінансової безпеки. Рівні фінансової безпеки. Поняття глобальної фінансової безпеки. Ухилення від оподаткування в глобальному вимірі. Глобальний тіньовий фінансовий сектор. Офшорні схеми. Схеми фінансування відмивання брудних коштів та фінансування тероризму. Поняття індикатора економічної безпеки держави. Класифікація показників економічної безпеки держави. Порогові значення. Інтегральний показник економічної безпеки держави. Експертні методи оцінювання рівня економічної безпеки держави. Кореляційно-регресійний аналіз в оцінці економічної безпеки держави. Індикативний метод оцінювання економічної безпеки держави. Система забезпечення економічної безпеки. Сутність системи забезпечення економічної безпеки держави. Структура системи забезпечення економічної безпеки держави. Суб'єкти забезпечення економічної безпеки держави. Методи мінімізації та нейтралізації загроз економічній безпеці держави. Поняття економічної безпеки України. Оцінювання рівня забезпечення складових економічної безпеки України.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Остапов С.Е. Технології захисту інформації: навч. посібник. / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Чернівці. – Видавничий дім «Родовід», 2014. – 471с.
2. Пількевич І.А. Захист інформації в автоматизованих системах управління: навч. посібник. / І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
3. Хорошко О. В. Захист систем електронних комунікацій: навч. посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браїловський та ін. – Київ: КНТЕУ, 2019. – 164 с.

Заплановані навчальні заходи та методи викладання. Вивчення дисципліни проводиться шляхом лекційних (аудиторних) та лабораторних занять (у комп'ютерному класі на ПК), що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.

Методи оцінювання:

- поточний контроль (тестування, наукова доповідь, перевірка

конспекту, опитування, контрольна робота);
– підсумковий контроль (екзамен).

Мова навчання та викладання. Українська, англійська.

4.16. НАЗВА. ІНФОРМАЦІЙНІ ВІЙНИ.

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вченезвання, науковийступінь, посада. Гамова І. В., доц., канд. екон. наук, доц. каф. журналістики та реклами.

Результативнавчання. Формування у студентів спеціальних теоретичних знань та практичних навичок щодо методики, технології та організації інформаційної політики держави, проблем протидії інформаційним загрозам.

Обов'язкові попередні навчальні дисципліни. «Основиреклами», «Основи зв'язків із громадськістю», «Масові комунікації».

Зміст.

Інформаційний суверенітет та інформаційна безпека України. Інформаційні війни у сучасному світі. Інформаційні війни в політичних кампаніях. Інформаційна асиметрія та формування інформаційного простору. Інструмент впливу в інформаційному просторі. Методи боротьби в інформаційному просторі. Інструменти протидії в інформаційному просторі. Методи реструктуризації інформаційного простору. Спіндоктор. Засоби інформаційного впливу на людину. Образ ворога в інформаційній війні.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Гороховський О. М. Фактчек як тренд розслідувань: можливості та перспективи: практичний посібник / О. М. Гороховський. – Дніпро: ЛІРА, 2017. – 133 с.

2. Золотухін Д. Ю. #Біла книга спеціальних інформаційних операцій проти України 2014 – 2018. Підручник / Д. Ю. Золотухін. – К., 2018. – 384 с.

3. Гамова І.В. Інформаційні війни: підручник. / І.В. Гамова. – Київ: Держ. торг. – екон. ун-т, 2022. – 184 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання із використанням інноваційних технологій: лекції (оглядова / тематична); практичні заняття (презентація / метод кейс-стаді).

Методи оцінювання:

- поточний контроль (тестування, усне / письмове опитування, перевірка підготовленого есе / презентації / розрахунково-графічної роботи / задачі / ситуаційні завдання);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.17. Назва. ІТ-ПРАВО

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Тімашов В.О., доцент, доктор юридичних наук, професор кафедри адміністративного, фінансового та інформаційного права.

Результати навчання. Формування професійних знань і навичок застосування правових норм, що регулюють відносини між учасниками ІТ-сфери.

Обов'язкові попередні навчальні дисципліни. «Правознавство».

Зміст. Поняття ІТ-права, сфера його дії та структура. Юридичні особливості відкриття ІТ-бізнесу в Україні. Відкриття ІТ-компаній в Україні. Цілі та обмеження міжнародного структурування ІТ-бізнесу. Законодавче регулювання електронної комерції в Україні. Юридична відповідальність за використання недостовірної інформації в мережі Інтернет. Порядок реєстрації авторського права на комп'ютерну програму. Авторські права на створення комп'ютерного коду та програмного забезпечення. Договірні правовідносини у сфері ІТ-Права. Правове регулювання стартапу в Україні. Конфіденційність та способи захисту комерційної таємниці за DNA договором. Забезпечення права на приватність при використанні інформаційних технологій. Правові проблеми регулювання відносин у соціальних мережах. Міжнародне законодавство у сфері охорони інтелектуальної власності.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Основи ІТ-права: навчальний посібник / Т.В. Бачинський, Р.І. Радейко, О.І. Харитонова та ін.; за заг. ред. Т.В. Бачинського. 2-ге вид., допов. і перероб. – К.: Юрінком Інтер, 2019. – 208 с.
2. Бачинський Т. Основи ІТ-права. Навчальний посібник. – Львів: Априорі, 2018. – 36 с.
3. Кульчій О.О. Інформаційне право: навч.-метод. посіб. / О.О. Кульчій. – Полтава: ВНЗ Укоопспілки «ПУЕТ», 2018. – 193 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання із використанням

інноваційних технологій: лекції (оглядова); семінарські та практичні заняття (тренінг / презентація / дискусія / моделювання ситуацій / робота в малих групах / інше); самостійна робота.

Методи оцінювання:

- поточний контроль (тестування, усне / письмове опитування, перевірка підготовленого есе / тощо);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.18. Назва. КОМЕРЦІЙНА РОЗВІДКА ТА ВНУТРІШНЯ БЕЗПЕКА НА ПІДПРИЄМСТВІ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада.Корягіна А.М., доцент, кандидат юридичних наук, доцент кафедри правового забезпечення безпеки бізнесу.

Результати навчання.Формування у студентів знань з основ комерційної розвідки та детективної діяльності розвідувального та контррозвідувального забезпечення підприємницької діяльності.

Обов'язкові попередні навчальні дисципліни. «Правознавство».

Зміст. Комерційна розвідка як елемент інформаційного забезпечення підприємницької діяльності. Об'єкти та джерела комерційної розвідки. Інформаційно-пошукова робота. Розвідувальні операції. Розвідувальне забезпечення комерційних операцій. Розвідувальне забезпечення конкурентної боротьби. Розвідувальне забезпечення фінансово-господарської діяльності підприємства, банку. Основи детективної діяльності. Закінчення таблиці. Забезпечення внутрішньої безпеки підприємства. Внутрішні загрози діяльності підприємства. Організація внутрішньої безпеки на підприємстві. Робота сил безпеки підприємства з його персоналом.

Рекомендовані джерела та інші навчальні ресурси /засоби.

1. Конкурентна розвідка: навчальний посібник. Копотун І. М., Падалка А. М., Кузьмічова-Кисленко Є. В. та ін. Ірпінь: Університет ДФС України, 2020. 188 с. (Серія «На допомогу студенту УДФСУ», т. 74).
2. Про охоронну діяльність: Закон України від 22.03.2012 // Відомості Верховної Ради України. 2012. № 30. Ст.260 (із змінами і допов.).
3. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 // Відомості Верховної Ради України. 1992. N 22. Ст.303. (із змінами і допов.).

Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання із використанням інноваційних технологій: Лекції (оглядові / тематичні), семінарські / практичні, кейс-стаді, самостійна робота, консультації.

Методи оцінювання:

- поточний (опитування, письмові роботи, ситуаційні завдання);
- підсумковий (екзамен).

Мова навчання та викладання. Українська.

4.19. Назва. ПСИХОЛОГІЯ АДАПТАЦІЇ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Корольчук М.С., професор, доктор психологічних наук, професор кафедри психології.

Результати навчання. Формування системи знань щодо використання адаптивних можливостей особистості для забезпечення збереження працездатності і здоров'я та ефективної і безпечної діяльності фахівців.

Обов'язкові попередні навчальні дисципліни. «Психологія».

Зміст. Теоретичні та методологічні засади психології адаптації. Види, типи, динаміка, критерії та межі адаптивних можливостей фахівців. Біологічна адаптація. Рівні соціально-психологічної адаптації. Захисні механізми та адаптивні стратегії особистості. Зміст професійної адаптації. Проблема адаптації фахівця до екстремальних умов діяльності. Психологічне забезпечення оптимізації адаптивних можливостей особистості. Особливості адаптації студентів та психологічні методи її оптимізації до умов професійно-освітньої діяльності.

Рекомендовані джерела та інші навчальні ресурси / засоби.

1. Корольчук М.С. Психологія діяльності: Підручник для студ. вищих навчальних закладів. – К.: Ельга, Ніка-Центр, 2012. – 400 с.
2. Психологія праці в звичайних та екстремальних умовах: навч. посіб. / М.С. Корольчук, В.М. Корольчук, С.М. Миронець, Г. М.Ржевський та ін. – К.: КНТЕУ, 2015. – 652 с.
3. Практична психологія. Навчальний посібник для студентів ВНЗ / Корольчук М.С., Корольчук В.М., Ржевський Г.М., Миронець С.М., Осьодло В.І., Зазимко О.В. – К. : КНТЕУ, 2014. – 728 с.

Заплановані навчальні заходи та методи викладання.

Поєднання традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (оглядові, тематичні,

проблемні, лекції-конференції, лекції-дискусії); практичні заняття (тренінги, презентації, дискусії, робота в малих групах, моделювання ситуацій, кейс-стаді).

Методи оцінювання.

- поточний контроль (тестування, усне / письмове опитування, тощо);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.20. Назва. ПСИХОЛОГІЯ БІЗНЕСУ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Овдієнко І.М., кандидат психологічних наук, доценткафедри психології, Євченко І.М., кандидат психологічних наук, доценткафедри психології.

Результати навчання. Знати основні напрями досліджень та завдання психології бізнесу, розуміти її міждисциплінарний характер, її структуру та зв'язок з іншими науками; володіти основні поняттями психології бізнесу, методами та підходами до проведення соціально-психологічних досліджень в сфері бізнесу.

Обов'язкові попередні навчальні дисципліни. «Психологія», «Психологія управління», «Філософія».

Зміст. Основні поняття, методологія, методи, завдання та принципи психології бізнесу. Психологічні джерела, чинники, механізми та закономірності розвитку бізнесу як системи, а також психологічні фактори появи кризових явищ в економічних відносинах. Психологічні передумови формування ділової активності. Процес формування підприємницької мотивації; професійно-важливі психологічні і психофізіологічні якості бізнесмена; соціально-психологічні чинники успішності ведення бізнесу. Основні напрями та підходи в оцінці професійних і ділових якостей бізнесмена; основи підбору та заохочення персоналу. Основні морально-етичні проблеми представників сучасного бізнесу. Роль та значення комунікативних процесів в діяльності підприємця; психологічне значення ділового спілкування в досягненні успіху, психологія прийняття рішення в складній ситуації.

Рекомендовані джерела та інші навчальні ресурси / засоби.

1. Гура Т., Романовський О., Книш А. Психологія лідерства в бізнесі: Навчальний посібник / Т. Гура, О. Романовський, А. Книш. –Харків : «Друкарня Мадрид», 2017. –100 с.

2. Гусєва О. Ю., Легомінова С. В., Воскобоева О. В., Ромашенко О. С., Хлевицька Т. Б. Психологія підприємництва та бізнесу: Навчальний посібник. –К.: Держ. ун-т телекомунікацій, 2019. –257с.

3. Мілютіна К. Л., Трофімов А. Ю. Психологія сучасного бізнесу: Навчальний посібник. –К.: Видавництво Ліра-К, 2020. –168 с.

Заплановані навчальні заходи та методи викладання.

Поєднання традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (оглядові, тематичні, проблемні, лекції-конференції, лекції-дискусії); практичні заняття (тренінги, презентації, дискусії, робота в малих групах, моделювання ситуацій).

Методи оцінювання:

– поточний контроль (тестування усне / письмове опитування; перевірка підготовленого есе / огляду / звіту / презентації / ситуаційні завдання тощо);

– підсумковий контроль (письмовий екзамен).

Мова навчання та викладання. Українська.

4.21. Назва. СТОХАСТИЧНІ МЕТОДИ В ЕКОНОМІЦІ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Гамалій В.Ф., проф., д-р фіз.-мат. наук, професор кафедри цифрової економіки та системного аналізу.

Результати навчання. Здобуття теоретичних знань і набуття практичних навичок кількісного аналізу та стохастичного математичного моделювання економічних процесів.

Обов'язкові попередні навчальні дисципліни. «Вища математика», «Теорія чисел», «Економічна теорія».

Зміст. Вступ до теорії випадкових процесів. Імовірнісні економічні моделі з використанням однорідних ланцюгів Маркова. Постановка стохастичних задач оптимального планування. Імовірнісні моделі найпростіших економічних систем. Аналітичний метод дослідження стохастичних економічних моделей. Методи економіко-математичного аналізу прикладних стохастичних моделей економіки.

Рекомендовані джерела та інші навчальні ресурси / засоби.

1. Лукяненко І.Г., Семко Р.Б. Динамічні стохастичні моделі загальної рівноваги: теорія побудови та практика використання у фінансових дослідженнях: І.Г. Лукяненко, Р.Б. Семко. Навчальний посібник.– К.:НУ «Києво-Могилянська академія», 2015.– 248с.

2. Козак Ю.Г. Математичні методи та моделі для магістрів з економіки. Практичне застосування. Навч. посіб./Ю.Г.Козак, В.М.Мацкул. – К.: Центр учбової літератури, 2017.–254 с.

3. Шамровський О.Д. Системний аналіз: математичні методи та застосування. Навчальний посібник / О.Д. Шамровський. – Львів: Магнолія 2006.– 2021. – 275 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і не традиційних методів викладання з використанням інноваційних технологій: лекції (тематична, проблемна); практичні заняття.

Методи оцінювання:

- поточний контроль (тестування; усне та письмове опитування);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.20. Назва. ТЕХНОЛОГІЇ АНАЛІЗУ ДАНИХ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Роскладка А. А., професор, доктор економічних наук, завідувач кафедри цифрової економіки та системного аналізу.

Результати навчання. Знання основних розділів науки про дані. Знання процедур передобробки даних: консолідація, трансформація, очищення, збагачення даних; проектування структури сховищ даних та *OLAP*-систем; моделей та методів інтелектуального аналізу даних: асоціації, кластеризації, класифікації, регресії, прогнозування, візуалізації даних; сучасних програмних засобів аналізу даних. Практичні вміння проводити аналіз даних для виявлення знань, будувати та досліджувати системи інтелектуального аналізу даних при вирішенні прикладних задач з використанням сучасних аналітичних платформ *Tableau* та *Microsoft PowerBI*.

Обов'язкові попередні навчальні дисципліни. «Комп'ютерна дискретна математика», «Вища математика», «Теорія чисел».

Зміст. Наука про дані (*DataScience*). Консолідація даних. Трансформація даних. Пошук асоціативних правил (*RulesMining*). Кластерний аналіз даних. Візуальний аналіз даних (*VisualMining*). Аналіз текстової інформації (*TextMining*). Аналіз даних мережі Інтернет (*WebMining*). Аналіз даних у реальному часі (*RealTimeDataMining*). Програмні аналітичні платформи.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Гладун А.Я. Datamining: пошук знань в даних. Посібник. / А.Я. Гладун, Ю. В. Рогушина.– Київ: АДЕФ-Україна, 2016. – 451 с.
2. Олійник А.О. Інтелектуальний аналіз даних: навч. посібн. / А.О.Олійник, С.О. Субботін, О.О. Олійник. – Запоріжжя: ЗНТУ, 2012. – 278 с.
3. Cuesta H., Kumar S. Practical Data Analysis. Birmingham: Packt Publishing Ltd, 2016. – 316 p.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематична, проблемна); лабораторні заняття (традиційні, робота в малих групах).

Методи оцінювання:

- поточний контроль (перевірка індивідуальних завдань, тестування);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.22. Назва. ФІЛОСОФІЯ ОСОБИСТОСТІ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Морозов А.Ю., професор, доктор філософських наук, професор кафедри філософії, соціології та політології.

Результати навчання. Формування філософської самосвідомості особистості спеціаліста психолога, здатності теоретичного дослідження та узагальнення історичних, соціокультурних, ідеологічних та аксіологічних засад формування та розвитку особистості.

Обов'язкові попередні навчальні дисципліни. «Філософія», «Психологія».

Зміст. Проблема людини в античній філософії. Розуміння особистості в філософських пошуках християнського Середньовіччя. Інтерпретації феномену людини у модерній і постмодерній парадигмах мислення. Екзистенціальні виміри особистості. Містичний досвід особистості, пікові переживання та значення інтуїції в духовному житті. Свідомість, несвідоме, мозок: проблеми генезису та розвитку. Смысл і цінності у бутті людини. Гуманізм і транс-гуманізм: проблеми гендеру та клонування.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Бауман З. Актуальність Голокосту. Посібник. – К., Логос, 2018. – 316 с.

2. Франкл В. Людина в пошуках справжнього сенсу. Посібник. – К., Основи, 2017. – 360 с.

3. Морозов А.Ю. Зло: метафізичні і богословські виміри. Посібник. – К., КНТЕУ, 2018. – 256 с.

Заплановані навчальні заходи та методи викладання. Заходи: відвідування Українського національного музею образотворчого мистецтва. Загальні методи: спів падіння логічного та історичного, метод тотожності-протилежностей. Проведення лекцій, семінарських занять з використанням мультимедійних технологій.

Методи оцінювання:

- поточний контроль (комп'ютерне тестування, опитування); модульний (комп'ютерне тестування, контрольна робота);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.22. Назва. ФУНКЦІОНАЛЬНЕ ТА ЛОГІЧНЕ ПРОГРАМУВАННЯ

Тип. Вибіркова.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Савченко Т. В., доцент, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Формування здатності до алгоритмічного та логічного мислення; мотивовано обирати мови програмування та технології розробки для розв'язання завдань створення і супроводження програмного забезпечення; теоретичних знань та практичних навичок, необхідних для засвоєння основ функціонального та логічного програмування та розв'язання складних і неформалізованих задач, що зустрічаються в реальних економічних, організаційних і виробничих системах, а також задач штучного інтелекту з використанням мов Lisp та Prolog.

Обов'язкові попередні навчальні дисципліни. «Алгоритми та структури даних», «Бази даних», «Технології розробки та тестування програмного забезпечення», «Експертні системи».

Зміст. Домінуючі парадигми програмування. Концепція функціонального програмування. Загальне уявлення про функціональне програмування та його застосування. Елементарний LISP. Конструювання списків. Числові функції. Керуючі структури. Поняття рекурсії. Функціонал. Концепція логічного програмування.

Області застосування мови Prolog. Особливості мови VisualProlog. Факти та правила у VisualProlog. Поняття аргументів та предикатів. Призначення запитів у Prolog. Застосування мов програмування високого рівня для побудови експертних систем.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Заяць В. М. Логічне і функціональне програмування. Системний підхід: підруч. для студентів базового напрямку підготовки «Комп'ютерні науки», «Комп'ютерна інженерія» та «Програмна інженерія» / В. М. Заяць, М. М. Заяць ; Нац. ун-т водного госп-ва та природокористування. – 2-ге вид, випр. та допов. – Рівне : НУВГП, 2020. – 421 с.

2. Месюра В. І. Функціональне та логічне програмування: посіб. / В. І. Месюра, Н. В. Лисак, О. І. Суприган ; Вінниц. нац. техн. ун-т. – Вінниця : ВНТУ, 2021. – 105 с.

3. Бадаєв Ю. І. Функціональне програмування : навч. посіб. для студ. вищ. навч. закл. / Ю.І. Бадаєв та ін. ; Нац. техн. ун-т України «Київ. політехн. ін-т». – К. : НТУУ «КПІ», 2019. – 135 с.

Заплановані навчальні заходи та методи викладання.

Лекції, лабораторні заняття, самостійна робота.

Методи оцінювання:

- поточний контроль (опитування, тестування);
- підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.22. Назва. ФУНКЦІОНАЛЬНЕ ТА ЛОГІЧНЕ ПРОГРАМУВАННЯ

Тип. За вибором.

Рік навчання. 2023/2024, 2024/2025.

Семестр. II-III.

Лектор, вчене звання, науковий ступінь, посада. Савченко Т.В., доцент, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Формування здатності до алгоритмічного та логічного мислення; мотивовано обирати мови програмування та технології розробки для розв'язання завдань створення і супроводження програмного забезпечення; теоретичних знань та практичних навичок, необхідних для засвоєння основ функціонального та логічного програмування та розв'язання складних і неформалізованих задач, що зустрічаються в реальних економічних, організаційних і виробничих системах, а також задач штучного інтелекту з використанням мов Lisp та Prolog.

Обов'язкові попередні навчальні дисципліни. «Об'єктно-орієнтоване програмування», «Бази даних», «Експертні системи».

Зміст. Домінуючі парадигми програмування. Концепція функціонального програмування. Загальне уявлення про функціональне програмування та його застосування. Елементарний LISP. Конструювання списків. Числові функції. Керуючі структури. Поняття рекурсії. Функціонал. Концепція логічного програмування. Области застосування мови Prolog. Особливості мови VisualProlog. Факти та правила у VisualProlog. Поняття аргументів та предикатів. Призначення запитів у Prolog. Застосування мов програмування високого рівня для побудови експертних систем.

Рекомендовані джерела та інші навчальні ресурси/засоби.

4. Заяць В.М. Логічне і функціональне програмування. Системний підхід: підруч. / В.М. Заяць, М.М. Заяць. – Рівне: НУВГП, 2018. – 421 с.

5. Месюра В. І. Функціональне та логічне програмування: посіб. / В. І. Месюра, Н. В. Лисак, О. І. Суприган– Вінниця : ВНТУ, 2011. – 105 с.

6. Бадаєв Ю. І. Функціональне програмування : навч. посіб. / Ю.І. Бадаєв та ін. – К. : НТУУ «КПІ», 2012. – 135 с.

Заплановані навчальні заходи та методи викладання.

Лекції, лабораторні заняття, самостійна робота.

Методи оцінювання:

– поточний контроль (опитування, тестування);

– підсумковий контроль (екзамен).
Мова навчання та викладання. Українська.

ЗМІСТ

ВСТУП
1. Загальна інформація про університет
1.1. Назва та адреса.....
1.2. Опис закладу (тип і статус).....
1.3. Керівництво університету.....
1.4. Академічний календар
1.5. Перелік запропонованих освітніх програм.....
1.6. Вимоги щодо прийому, у тому числі мовна політика та процедури реєстрації.....
1.7. Механізми для визнання кредитної мобільності студентів та попереднього навчання (неформального та інформального)
1.8. Політика розподілу кредитів ЄКТС (інституційна кредитна рамка).....
1.9. Механізми академічного управління
2. Загальна інформація для студентів
2.1. Відділ обліку студентів
2.2. Умови проживання
2.3. Харчування.....
2.4. Вартість проживання.....
2.5. Фінансова підтримка для студентів
2.5.1. Стипендіальне забезпечення студентів.....
2.5.2. Пільгова оплата за проживання у гуртожитках
2.5.3. Фінансове забезпечення студентів з числа дітей-сиріт та дітей, позбавлених батьківського піклування
2.6. Медичні послуги
2.7. Страхування
2.8. Умови для студентів з обмеженими можливостями та особливими потребами.....
2.9. Навчальне обладнання
2.10. Організація мобільності студентів за освітніми програмами
2.11. Заклади вищої освіти – партнери університету
2.12. Програми англійською мовою викладання
2.13. Мовні курси.....
2.14. Можливості для практичної підготовки
2.15. Дуальна форма освіти.....
2.16. Умови для занять спортом і відпочинку
2.17. Студентські організації
3. Освітня програма
4. Інформація про освітні компоненти (дисципліни)