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

ІНФОРМАЦІЙНИЙ ПАКЕТ

Європейська кредитно-трансферна система (ЄКТС)

Галузь знань	**F Інформаційні технології**
Спеціальність	**F5 Кібербезпека та захист інформації**
Освітня програма	**«Кібербезпека та захист інформації»**
Освітній ступінь	**«магістр»**

Київ 2025

3. Освітня програма.

Керівник проєктної групи (гарант освітньої програми) – Хохлачова Ю.Є., кандидат технічних наук, професор, професор кафедри інженерії програмного забезпечення та кібербезпеки.

3.1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем в економіці» зі спеціальності F5 «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
Рівень вищої освіти та назва кваліфікації мовою оригіналу	*Другий (магістерський) рівень вищої освіти* *Кваліфікація – Магістр з кібербезпеки*
Галузь знань	*F Інформаційні технології*
Спеціальність	*F5 Кібербезпека та захист інформації*
Назва освітньої програми	Кібербезпека та захист інформації
Обмеження щодо форм навчання	Обмеження відсутні
Відповідність стандарту вищої освіти МОН України	Відповідає стандарту вищої освіти МОН України (наказ № 332 від 18.03.2021 р.)
Тип диплома та обсяг освітньої програми	Диплом магістра, одиничний. Обсяг освітньо-професійної програми – 90 кредитів ЄКТС. Нормативний строк підготовки 1 рік 4 місяці
Наявність акредитації	Сертифікат про акредитацію спеціальності №9819, дійсний до 01.07.2030 виданий Національним агенством із забезпечення якості вищої освіти.
Цикл, рівень вищої освіти	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL-7 рівень
Передумови вступу на освітню програму	Освітній ступінь бакалавра (6 рівень НРК) або вищий рівень
Мова(и) викладання	Українська
Термін дії освітньої програми	До затвердження нової редакції освітньо-професійної програми

Інтернет-адреса постійного розміщення опису освітньої програми	https://knute.edu.ua/

2-МЕТА ОСВІТНЬОЇ ПРОГРАМИ

Забезпечити здобувачам вищої освіти другого (магістерського) рівня фундаментальну підготовку за спеціальністю F5 «Кібербезпека та захист інформації», що є достатньою для вирішення задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки в галузі економіки.

3-ХАРАКТЕРИСТИКА ОСВІТНЬОЇ ПРОГРАМИ

Предметна область

Об'єкт вивчення:

– 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;

Цілі навчання: Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.

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.

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. 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.

Інструментарій 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.

Орієнтація освітньої програми

Освітньо-професійна, прикладна.

Основний фокус освітньої програми

Спеціальна освіта у галузі знань «Інформаційні технології» спеціальності «Кібербезпека та захист інформації». 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.

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.

Особливості програми

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.

4-ПРИДАТНІСТЬ ВИПУСКНИКІВ ДО ПРАЦЕВЛАШТУВАННЯ ТА ПОДАЛЬШОГО НАВЧАННЯ

Придатність до працевлаштування

Фахівець спроможний виконувати професійні роботи і займати посади, визначені Національним класифікатором України «Класифікатор професій ДК 003:2010»:
2139.2 Фахівець з підтримки інфраструктури кіберзахисту
2139.2 Фахівець з технічного захисту інформації
2139.2 Фахівець з реагування на інциденти кібербезпеки
2139.2 Фахівець з підтримки інфраструктури кіберзахисту
2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки))
2139.2 Фахівець з криптографічного захисту інформації
2139.2 Фахівець з кібердосліджень та розробок систем безпеки
2132.2 Розробник систем захисту інформації
2359.2 Інструктор-методист з інформаційної безпеки
2139.2 Аудитор з інформаційних технологій (з кібербезпеки)

Подальше навчання

Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти.

Набуття додаткових кваліфікацій в системі освіти дорослих.	
5-ВИКЛАДАННЯ ТА ОЦІНЮВАННЯ	
Викладання та навчання	
Збалансоване поєднання аудиторних занять (лекції-дискусії, семінарські заняття, практичні заняття в малих групах, самостійна робота з інформаційними джерелами, консультації викладачів), дистанційного навчання та самостійної роботи на засадах проблемно-орієнтованого, інтерактивного навчання та самонавчання.	
Оцінювання	
Оцінювання результатів навчання студентів здійснюється відповідно до «Положення про оцінювання результатів навчання студентів та аспірантів у ДТЕУ» та передбачає проведення таких контрольних заходів: поточний та підсумковий контролі, атестація. Поточний контроль проводиться на практичному/лабораторному занятті та за результатами виконання завдань самостійної роботи. Передбачає оцінювання теоретичної підготовки студентів під час роботи на семінарських заняттях та набутих практичних навичок під час виконання завдань лабораторних/практичних робіт. Підсумковий контроль – контрольні заходи, що передбачають встановлення відповідності (вимірювання, оцінювання) здобутих особою результатів навчання вимогам освітньої програми у частині відповідного освітнього компонента, що здійснюється в університеті у формі заліку та екзамену. Результати навчання студентів у ДТЕУ оцінюються за 100- баловою шкалою, де: 60-100 балів – результати навчання, що дають студенту право здобути кредити ЄКТС; 0-59 балів – незадовільні результати навчання, що не дають студенту право здобути кредити ЄКТС.	
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-1.	Здатність застосовувати знання у практичних ситуаціях.
КЗ-2.	Здатність проводити дослідження на відповідному рівні.
КЗ-3.	Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4.	Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КЗ-6.	*Здатність діяти соціально відповідально та громадсько свідомо.*
КЗ-7.	*Здатність до адаптації та дії у новій ситуації.*
КЗ-8.	*Здатність до вибору стратегії спілкування, працювати в команді.*
КЗ-9.	*Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.*
Фахові компетентності	
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.
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.
КФ3.	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
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.
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.
КФ6.	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
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.
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.
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.
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.
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.
КФ12.	*Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області.*
КФ13.	*Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки.*
7-ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ	
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.
РН2	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
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.
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології 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.
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.
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.
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.
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.
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.
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.
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.
РН18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму 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.
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.
РН24	*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.*
РН25	*Виконувати обов'язки внутрішнього консультанта/ радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації.*
РН26	*Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу).*
РН27	*Проводити сканування систем безпеки інформаційних ресурсів на вразливості.*
РН28	*Застосовувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності.*
8- РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПРОГРАМИ	
Кадрове забезпечення	
Повністю відповідає Ліцензійним вимогам провадження освітньої діяльності. Реалізацію освітньо-професійної програми «Кібербезпека та захист інформації» здійснюють науково-педагогічні працівники з науковим ступенем та/або вченим званням, які відповідають вимогам чинного законодавства України, мають достатній рівень наукової і професійної кваліфікації. До освітнього процесу також залучаються фахівці-практики і представник професійних об'єднань та іноземні партнери. Всі науково-педагогічні працівники кожні п'ять років проходять стажування / підвищення кваліфікації.	
Матеріально-технічне забезпечення	
Повністю відповідає Ліцензійним вимогам провадження освітньої діяльності. Для зручності здобувачів вищої освіти функціонують корпоративна система дистанційного навчання та автоматизована система управління освітнім процесом «МІА: Освіта». В університеті обладнані сучасні комп'ютерні класи зі спеціалізованим програмним забезпечення, функціонує Навчально-науковий центр бізнес-симуляції та працює Smart-бібліотека. Створенні всі умови для навчання осіб з інвалідністю. Наявна соціально-побутова інфраструктура ДТЕУ.	
Інформаційне та навчально-методичне забезпечення	
Для кожної освітньої програми в університеті розробляється Інформаційний пакет ЄКТС. Кожен студент через особистий кабінет АСУ «МІА: Освіта» може переглянути та сформувати власний індивідуальний план, переглянути навчальний план, здобуті бали за дисциплінами, розклад занять та комунікувати з учасниками освітнього процесу.	

Програми, робочі програми, силабуси дисциплін та критерії оцінювання за освітніми компонентами розміщені на корпоративній платформі дистанційного навчання.
В електронному репозитарію університету розміщено повнотекстовий доступ до наукової та навчальної літератури ДТЕУ, рукописи кваліфікаційних робіт та дисертацій на здобуття наукових ступенів.
Для зручності здобувачів вищої освіти в університеті розроблений Каталог навчальних дисциплін, відповідно якого студенти мають право обирати вибіркові освітні компоненти.

9-АКАДЕМІЧНА МОБІЛЬНІСТЬ

Національна кредитна мобільність

Національна кредитна моблільність здійснюється в межах укладених меморандумів про співпрацю між ДТЕУ та іншими закладами вищої освіти (наукових установах) України відповідно до законодавства.

Міжнародна кредитна мобільність

Університетом укладені договори про співробітництво між ДТЕУ та іноземними закладами вищої освіти, в рамках яких здійснюється партнерський обмін та навчання студентів за Міжнародними програмами і проектами в рамках програми Еразмус+.
Університетом укладені договори про співробітництво між ДТЕУ та іноземними закладами вищої освіти, в рамках яких здійснюється партнерський обмін та навчання студентів за Міжнародними програмами і проєктами в рамках програми Еразмус+.
Організація кредитної мобільності (окрім 1-го курсу) бакалаврів. договор про мобільність між ДТЕУ та Словацьким технологічним університетом (м. Братислава):Erasmus+ Learning Agreement Student Mobility for Studies International Mobility (KA171). Договір про академічну мобільність діє з 2024 по 2027 рік.

Навчання іноземних здобувачів вищої освіти

Здійснюється відповідно до вимог чинного законодавства.

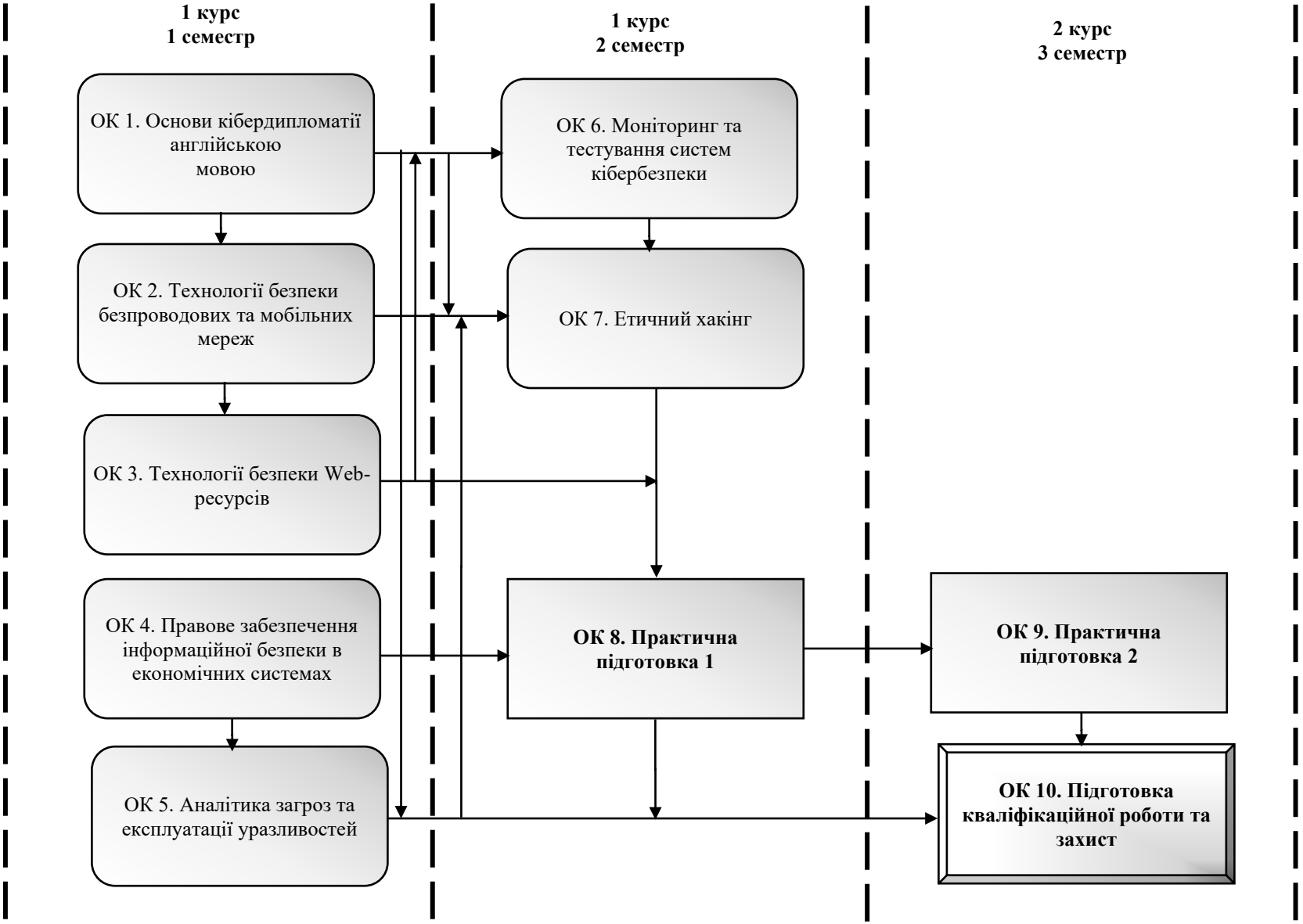
3.2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

3.2.1 ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ

Код	Освітні компоненти програми	Кредити ЄКТС	Форма контролю
Обов'язкові компоненти			
ОК 1.	Основи кібердипломатії англійською мовою	6	Екзамен
ОК 2.	Технології безпеки безпроводових та мобільних мереж	6	Екзамен
ОК 3.	Технології безпеки Web-ресурсів	6	Екзамен
ОК 4.	Правове забезпечення інформаційної безпеки в економічних системах	6	Екзамен
ОК 5.	Аналітика загроз та експлуатації уразливостей	6	Екзамен
ОК 6.	Моніторинг та тестування систем кібербезпеки	6	Екзамен
ОК 7.	Етичний хакінг	6	Екзамен
ОК 8.	Практична підготовка 1	12	Залік
ОК 9.	Практична підготовка 2	3	Залік
ОК 10.	Підготовка кваліфікаційної роботи та захист	9	Захист
Загальний обсяг обов'язкових компонент		**66**	
Вибіркові компоненти			
ВК 1.	Освітній компонент 1	6	Екзамен
ВК 2.	Освітній компонент 2	6	Екзамен
ВК 3.	Освітній компонент 3	6	Екзамен
ВК 4.	Освітній компонент 4	6	Екзамен
Загальний обсяг вибіркових компонент		**24**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90,0**	

Здобувачі вищої освіти обирають вибіркові навчальні дисципліни через особистий кабінет порталу «МІА: Освіта». Опис навчальних дисциплін та їх пререквізити представлені в Каталозі навчальних дисциплін ДТЕУ

3.2.2. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОП



3.3.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 і 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.

3.4. 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	ОК 8	ОК 9	ОК 10
КЗ-1.	+	+	+	+	+	+	+	+	+	+
КЗ-2.		+	+	+	+		+			+
КЗ-3.	+				+	+	+			+
КЗ-4.			+		+	+		+	+	
КЗ-5.	+	+		+	+		+			
КЗ-6.	+			+	+		+			
КЗ-7.	+			+	+			+	+	
КЗ-8.	+			+				+	+	
КЗ-9.	+							+	+	+
КФ1.		+	+	+	+	+	+	+	+	+
КФ2.	+	+	+	+	+	+	+	+	+	+
КФ3.		+		+	+	+	+	+	+	+
КФ4.	+	+		+		+	+	+	+	+
КФ5.	+	+	+			+	+	+	+	+
КФ6.			+					+	+	+
КФ7.			+		+			+	+	+
КФ8.						+		+	+	+
КФ9.		+				+	+	+	+	+
КФ10.	+			+			+	+	+	+
КФ11.		+			+	+		+	+	+
КФ12.	+	+	+	+	+	+	+	+	+	+
КФ13.		+	+		+	+	+	+	+	+

3.5.МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ОБОВ'ЯЗКОВИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Компоненти / Програмні результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10
РН1	+	+		+			+	+	+	+
РН2	+	+				+	+	+	+	+
РН3	+				+		+	+	+	+
РН4		+	+		+	+	+	+	+	+
РН5	+			+		+		+	+	+
РН6			+	+	+	+		+	+	+
РН7	+		+	+	+	+		+	+	+
РН8		+				+	+	+	+	+
РН9		+					+	+	+	+
РН10		+	+			+	+	+	+	+
РН11		+	+				+	+	+	+
РН12			+	+	+			+	+	+
РН13		+				+	+	+	+	+
РН14				+		+		+	+	+
РН15	+	+	+				+	+	+	+
РН16	+		+			+		+	+	+
РН17	+	+		+	+	+	+	+	+	+
РН18	+						+	+	+	+
РН19			+					+	+	+
РН20		+			+	+	+	+	+	+
РН21					+	+		+	+	+
РН22			+	+	+			+	+	+
РН23			+		+	+		+	+	+
РН24		+				+		+	+	+
РН25	+	+	+	+	+	+	+	+	+	+
РН26	+			+				+	+	+
РН27		+	+		+	+	+	+	+	+
РН28		+	+		+	+	+	+	+	+

Додаток

СПИСОК РЕКОМЕНДОВАНИХ ВИБІРКОВИХ КОМПОНЕНТІВ

Код	Освітні компоненти	Кредити ЄКТС
ВК 1.	UI/UX дизайн англійською мовою	**6**
ВК 2.	Адміністрування та захист сховищ даних	**6**
ВК 3.	Безпека мобільних додатків	**6**
ВК 4.	Безпека технологій інтернету речей	**6**
ВК 5.	Інформаційні технології у системі забезпечення економічної безпеки держави	**6**
ВК 6.	Правове регулювання безпеки підприємницької діяльності	**6**

4. Інформація про освітні компоненти (дисципліни).

4.1. Назва. ОСНОВИ КІБЕРДИПЛОМАТІЇ АНГЛІЙСЬКОЮ МОВОЮ
Тип. Обов'язкова.
Рік навчання. 2025/2026.
Семестр. І.
Лектор, вчене звання, науковий ступінь, посада. Гайдук О.В., старший викладач кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання. Формування комплексних знань з основ кібердипломатії; усвідомлення ролі та місця кібердипломатії в системі забезпечення національної безпеки; орієнтація в основних міжнародно-правових нормах, що регулюють кіберпростір; розуміння особливостей реалізації кібердипломатії провідними державами світу; практичні навички аналізу ризиків та загроз у сфері міжнародної кібербезпеки; оцінювання перспектив та можливих сценаріїв розвитку кібердипломатії; застосування набутих знань для прийняття обґрунтованих рішень у сфері кібердипломатії.
Обов'язкові попередні навчальні дисципліни. «Соціотехнічна кібербезпека», «Організація комп'ютерних мереж», «Безпека інформаційних систем та мереж».
Зміст. Вступ до кібердипломатії. Кібербезпека як складова національної безпеки. Міжнародне право та норми поведінки держав у кіберпросторі. Інституційна структура кібердипломатії та її економічно-фінансове наповнення. Нормативно-правова база з кібердипломатії провідних держав. Використання інформаційно-комунікаційних технологій у публічній дипломатії. Кіберзагрози та моделі кіберконфліктів. Міжнародне співробітництво у сфері кібербезпеки. Кіберзлочинність та кібертероризм. Кібершпигунство та кіберрозвідка. Економічні аспекти кібердипломатії. Кібербезпека критичної інфраструктури. Кібердіалог як інструмент кібердипломатії. Перспективи розвитку кібердипломатії.
Рекомендовані джерела та інші навчальні ресурси / засоби.
1. Cyberdiplomacy: Managing Security and Governance Online. Shaun Riordan. – Polity, 2019. – 160 p.
2. Internet Diplomacy. Shaping the Global Politics of Cyberspace. Meryem Marzouki, Andrea Calderaro. – Rowman & Littlefield Publishers, 2023. – 280 p.
3. Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century. Edited By Evan H.Potter. – McGill-Queen's University Press, 2022. – 216 p.
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. Англійська.

4.2. Назва. ТЕХНОЛОГІЇ БЕЗПЕКИ БЕЗПРОВОДОВИХ ТА МОБІЛЬНИХ МЕРЕЖ.

Тип. Обов'язкова.

Рік навчання. 2025/2026.

Семестр. І.

Лектор, вчене звання, науковий ступінь, посада. Шестак Я.І., PhD, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки, директор ІОЦ - ГЦІТ ДТЕУ

Результати навчання. Формування теоретичних знань та практичних навичок необхідних для ефективного використання інформаційних технологій в інформаційних системах і мережах а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, протиправним діям щодо знищення, модифікації, копіювання і блокування інформації. Вміння інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. Здатність застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. Вміння досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/ або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури

Обов'язкові попередні навчальні дисципліни. «Основи кібербезпеки», «Соціотехнічна кібербезпека», «Організація комп′ютерних мереж».

Зміст. Основи теорії безпроводової передачі. Загрози, атаки та захист безпроводових мереж. Мережеві протоколи та служби безпроводових мереж. Стандарти мереж мобільного зв'язку. Загрози та вразливості мобільних пристроїв. Архітектура безпроводових мереж 4G та 5G. Загрози та вразливості стандартів 3G, 4G, 5G. Архітектура WiFi-технологій. Загрози та вразливості WiFi-мереж. Моніторинг безпеки безпроводових мереж. Шляхи захисту безпроводових мереж. Мережі широкосмугового бездпроводового 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. 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. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.

3. Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання із використанням інноваційних технологій: лекції (тематична; проблемна); лабораторні заняття.

Методи оцінювання.

– поточний контроль (тестування; усне та письмове опитування; виконання практичних та лабораторних завдань, курсова робота);
– підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.3. Назва. ТЕХНОЛОГІЇ БЕЗПЕКИ WEB-РЕСУРСІВ

Тип. Обов’язкова.

Рік навчання. 2025/2026.

Семестр. І.

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

Результати навчання. Формування теоретичних знань та практичних навичок з питань захисту вебзастосунків, починаючи з етапів розвідки та пошуку вразливостей, типових вразливостей серверної та клієнтської частини вебзастосунку, а також формування навичок пошуку та виправлення проблем кодування вебзастосунку.

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 (Secure Sockets Layer); симетричне та асиметричне шифрування; використання протоколу простого доступу до об’єктів (SOAP); протокол SMTP (Simple Mail Transfer Protocol); протокол поштового відділення (POP3); протокол доступу до Інтернету (IMAP). Огляд технологій вебавтентифікації. Брандмауери вебдодатків. Огляд топ-10 списку OWASP. Розвідка і уразливості веб-додатків: відкриття веб-сторінки/структури програми; збір інформації в вебзастосунках; Сканування вразливостей веб-додатків. Безпека серверної частини вебдодатків: введення в server-side-уразливості, SQL-ін'єкція, автентифікація та авторизація вебдодатків, 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

вебкешем, атаки заголовків хостів HTTP, автентифікація OAuth, безпека XML.

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. – 218с.
2. Anoop Singhal, Theodore Winograd, Karen Scarfone. Guide to secure web services. National Institute of Standards and Technology Special Publication 800-95, 2007. - 128 Pages
3. Andrew Homan. Web Application Security Exploitation and Countermeasures for Modern Web Applications. United States of America, 2020. – 331 Pages. ISBN: 978-1-492-08796-0

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. 2025/2026.

Семестр. І.

Лектор, вчене звання, науковий ступінь, посада. Ситніченко О.М., доцент, 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. Остроухов В.В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. Інформаційна безпека: підруч. [за загал. ред. В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська.]. — Видавництво Ліра-К, 2021. – 412 с.

2. Бабала Ю.Я, Горбатий І.В, Кіселичник М.Д., Бондарєв А.П, Войтусік С.С. Інформаційна безпека: навч.посібник [за заг.ред. Ю.Я.Бабала , І.В Горбатий, М.Д. Кіселичник, А.П Бондарєв, С.С. Войтусік].–Видавництво Львівська політехніка -2019.- 580 с.

3. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник [за заг.ред. А.М. Гребенюк, Л.В. Рибальченко].Видавництво– Дніпро: Дніпроп. держ. Ун-т внутріш. справ, 2020. – 144 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання із використанням інноваційних технологій: лекції (оглядова); семінарські, практичні заняття.

Методи оцінювання.

– поточний контроль (тестування, опитування, контрольна робота);

– підсумковий контроль (екзамен).

Мова навчання та викладання. Українська.

4.5. Назва. АНАЛІТИКА ЗАГРОЗ ТА ЕКСПЛУАТАЦІЇ УРАЗЛИВОСТЕЙ.

Тип. Обов’язкова.

Рік навчання. 2025/2026.

Семестр. І.

Лектор, вчене звання, науковий ступінь, посада. Хохлачова Ю.Є., професор, кандидат технічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. 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.

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.

Обов'язкові попередні навчальні дисципліни. «Безпека інформаційних систем і мереж», «Архітектура комп'ютера», «Організація комп′ютерних мереж».

Зміст. Національна база даних уразливостей (National Vulnerability Database). Протоколи докумен-тування, відстеження та спільного використання інформації про інциденти. Банк даних загроз безпеки інформації. Калькулятор CVSS v2.0. База даних уразливостей від відкритих джерел (Open Sourced Vulnerability Database). Сучасні бази даних атак та їх використання в системах виявлення вторгнень. База даних інцидентів веб-хакерства. Бази даних атак, сформовані при проведенні конкурсів з кібербезпеки. База даних уразливостей IBM X-Force. База даних записів уразливостей US-CERT. Бази даних уразливостей в VND. База даних уразливостей SecurityFocus. Бази шаблонів атак KDD-99. Бази шаблонів атак CAPEC.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник. К.: НАУ, 2023 312 с.
2. М.М. Браіловський, Н.С. Вишневська, В.Д. Козюра, Ю.В. Пепа, В.О. Хорошко, Ю.Є. Хохлачова. Комп'ютерні технології: навчальний посібник. К.: ФОП Ямчинський О.В., 2023. 200 с.
3. Браіловський М.М., Зибін С.В., Кобозєва А.А., Хорошко В.О., Хохлачова Ю.Є. Аналіз кіберзахищеності інформаційних систем Київ: ФОП Ямчинський О.В. 2021. 360 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання із використанням інноваційних технологій: лекції (оглядова); семінарські, практичні заняття.

Методи оцінювання.

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

Мова навчання та викладання. Українська.

4.6. Назва. МОНІТОРИНГ ТА ТЕСТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ.

Тип. Обов'язкова.

Рік навчання. 2025/2026.

Семестр. II.

Лектор, вчене звання, науковий ступінь, посада. Хохлачова Ю.Є., професоркандидат технічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки.

Результати навчання. 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. Вміння виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області. Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки. 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. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

Обов'язкові попередні навчальні дисципліни. «Архітектура комп'ютера», «Безпека інформаційних систем і мереж», «Організація комп′ютерних мереж».

Зміст. Предмет дисципліни, її цілі. Основні терміни та визначення. Організація захисту інформації в системі. Поняття моніторингу. Характеристики та види подій при моніторингу. Види моніторингу та основні питання. Сучасні методи та технології моніторингу. Прогнозування (передбачення). Загальні питання. Підходи та методи моніторингу. Методи тестування криптографічних програмних систем. Основні принципи процесу тестування. Методика забезпечення якості програмного забезпечення

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Хохлачова Ю.Є. Моніторинг та тестування систем кібербезпеки: лабораторний практикум / Ю.Є. Хохлачова, В.М. Кінзерявий, В.В. Погорелов та ін. К.: НАУ, 2022. 56 с.
2. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. К.: ЦП «Компринт», 2021. 296 с.
3. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник. К.: НАУ, 2023. 312 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання із використанням інноваційних технологій: лекції (оглядова); семінарські, практичні заняття.

Методи оцінювання.

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

Мова навчання та викладання. Українська.

4.7. Назва. ЕТИЧНИЙ ХАКІНГ.
Тип. Обов'язкова.
Рік навчання. 2025/2026.
Семестр. ІІ.
Лектор, вчене звання, науковий ступінь, посада. Чубаєвський В.І., проофесор, доктор економічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання. 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. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. Виконувати обов'язки внутрішнього консультанта/ радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації. Проводити сканування систем безпеки інформаційних ресурсів на вразливості. Застосовувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності.
Обов'язкові попередні навчальні дисципліни. «Безпека інформаційних систем і мереж», «Організація комп′ютерних мереж».
Зміст. Введення в етичний хакінг. Хакерські атаки і фази хакінгу. Збір інформації і попереднє вивчення об'єкта атаки. Сканування мережі. Збір інформації за допомогою сервісів прикладного рівня. Засоби проникнення на об'єкт атаки. Засоби закріплення та поширення на об'єкті атаки. Мережеві аналізатори. Методи виявлення вразливостей. Виконання тесту на проникнення, пентестінг. Інструменти етичного хакінгу.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. – NY.: Press.Inc, 2014, – 478 с.
2. Ярошенко А.А.ХАКІНГ на прикладах. Вразливості, взлом, захист. Посібник. К.: Наука і техніка, 2021. – 320с.
3. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А. П. Бондарєв 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.
Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання із використанням інноваційних технологій: лекції (оглядова); семінарські, практичні заняття.

Методи оцінювання.
– поточний контроль (тестування, опитування, контрольна робота);
– підсумковий контроль (екзамен).
Мова навчання та викладання. Українська.

4.8. Назва. UI/UX ДИЗАЙН АНГЛІЙСЬКОЮ МОВОЮ

Тип. За вибором.
Рік навчання. 2025/2026, 2026/2027.
Семестр. II -III.
Лектор, вчене звання, науковий ступінь, посада. Котенко Н. О., доцент, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання. Чітке розуміння того як влаштований дизайн-процес. Ґрунтовні знання у сфері UI/UX дизайну. Практичні навички використання інструментів Figma для побудови вайрфреймів, макетів та прототипів програмних продуктів відповідно до поставленого завдання чи сформульованої проблеми. Здатність здійснювати тестування інтерфейсів.
Обов'язкові попередні навчальні дисципліни: «Англійська мова інформаційних технологій», «Інформатика».
Зміст. Що таке дизайн, та як він працює. Як влаштований дизайн процес. Методи та процеси. Які підходи існують. Які підходи і коли краще використовувати. Дослідження потреб бізнесу. Інструменти дизайнера. Як змінювався софт. Принципи роботи з Figma. Основи інтерфейсу. Організація макетів. Елементи сайту. Стилі, сітки та автолейаути. Візуальний дизайн: шрифти та типографіка. Збір даних від замовника. Аналіз конкурентів. Опитування. Інформаційна архітектура. Дизайн система та UI kit. iOs, Android. Особливості та гайдлайни. Веб аналітика. Тестування інтерфейсів.
Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Hill A. Complete figma tutorial for ui/ux: the comprehensive beginners to expert guide for learning and mastering FIGMA for UI/UX with pictures and illustrations. Independently Published, 2022.
2. Nielsen norman group: UX training, consulting, & research. Nielsen Norman Group. URL: https://www.nngroup.com/ (date of access: 23.02.2024).
3. Staiano F. Designing and Prototyping Interfaces with Figma: Learn essential UX/UI design principles by creating interactive prototypes for mobile, tablet, and desktop. Packt Publishing, 2022. 382 p.

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. Англійська.

4.9. Назва. АДМІНІСТРУВАННЯ ТА ЗАХИСТ СХОВИЩ ДАНИХ
Тип. За вибором.
Рік навчання. 2025/2026, 2026/2027.
Семестр. II -III.
Лектора, вчені звання, наукові ступені, посади. Лахно В.А., професор, доктор технічних наук; Десятко А.М., доцент, доктор філософії (PhD), в.о. завідувача кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами інших галузей знань/видів економічної діяльності). Розробляти і координувати процеси, етапи та ітерації життєвого циклу програмного забезпечення на основі застосування сучасних моделей, методів та технологій розроблення програмного забезпечення та забезпечувати якість програмного забезпечення. Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення. Аналізувати, оцінювати і застосовувати на системному рівні сучасні програмні та апаратні платформи для розв'язання складних задач інженерії програмного забезпечення. Розробляти і модифікувати архітектуру програмного забезпечення для реалізації вимог замовника.
Обов'язкові попередні навчальні дисципліни. «Технології розробки та тестування програмного забезпечення», «Об'єктно-орієнтоване програмування», «Алгоритми та структури даних», «Архітектура та проектування програмного забезпечення», «Бази даних».
Зміст. Введення в сховища даних. Поєктування архітектури сховищ даних.
Методи логічного проектування сховищ даних. Фізичне моделювання сховищ даних. Метод багатовимірного моделювання. Завантаження та очищення даних. Організація доступу до сховищ даних. Фізична організація даних та механізми доступу. Безпека доступу до сховищ даних.
Методи інтелектуального аналізу даних.
Рекомендовані джерела та інші навчальні ресурси/засоби.
1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99
2. Державний стандарт України ДСТУ 3396.0–96. Захист інформації. Технічний захист інформації. Основні положення.
3. Державний стандарт України ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни та визначення.
Методи оцінювання:
- поточний контроль (опитування, тестування, індивідуальний проєкт);
- підсумковий контроль (письмовий екзамен).

Мова навчання та викладання. Українська.

4.10. Назва. БЕЗПЕКА МОБІЛЬНИХ ДОДАТКІВ.
Тип. За вибором.
Рік навчання. 2025/2026, 2026/2027.
Семестр. II -III.
Лектор, вчене звання, науковийступень, посада. Яремич В.Р., асистент кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик при розробці мобільних додатків. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них під час організації безпеки мобільних додатків.
Обов'язкові попередні навчальні дисципліни. «Безпека інформаційних систем і мереж», «Правове забезпечення інформаційної безпеки держави», «Криптографічні методи захисту інформації», «Організація комп′ютерних мереж».
Зміст. 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.
3. Gupta B. B. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives (Security, Privacy, and Trust in Mobile Communications) Auerbach Publications; 1st edition (September 30, 2020) 694 pages
Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання із використанням інноваційних технологій: лекції (тематична; проблемна); лабораторні заняття.

Методи оцінювання.
– поточний контроль (тестування, усне та письмове опитування);
– підсумковий контроль (екзамен).
Мова навчання та викладання. Українська.

4.11. Назва. БЕЗПЕКА ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ.
Тип. За вибором.
Рік навчання. 2025/2026, 2026/2027.
Семестр. II -III.
Лектор, вчене звання, науковийступень, посада. Москаленко В.В., асистент кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання. Вміння проводити аналіз загроз на рівні застосунків в екосистемі Інтернету речей (IoT). Виявляти вразливості веб-інтерфейсів та мобільних додатків для керування IoT-пристроями. Оцінювати ризики, пов'язані з хмарними сервісами IoT. Характеризувати атаки на прикладному рівні: міжсайтовий скриптинг (XSS), SQL-ін'єкції, атаки на автентифікацію та авторизацію. Розуміти моделі загроз безпеки в мережі IoT: STRIDE, DREAD, PASTA. Вміння організовувати процес створення та аналізу моделей загроз. Вміння застосовувати моделі загроз у контексті IoT. Розуміти та використовувати методи зменшення ризиків на рівні застосунків: безпечне програмування, регулярні оновлення, шифрування даних.
Обов'язкові попередні навчальні дисципліни. «Безпека інформаційних систем і мереж», «Правове забезпечення інформаційної безпеки держави», «Організація комп'ютерних мереж».
Зміст. Основні поняття та стандарти Інтернету речей (IoT). Основні загрози інтернету речей. Архітектура IoT. Загрози на прилади IoT. Протоколи та принципи передачі даних в IoT. Загрози рівня застосунків моделі загроз безпеки в мережі IoT. Загрози рівня підтримки моделі загроз безпеки в мережі IoT. Загрози рівня мережі моделі загроз безпеки в мережі IoT. Загрози рівня сприйняття моделі загроз безпеки в мережі IoT. Технологія Blockchain для безпеки IoT. Основи організації процесу та засоби автоматизації тестування програмного забезпечення інтернету речей.
Рекомендовані джерела та інші навчальні ресурси/засоби.
1. Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 1. Основи і технології / За ред. В. С. Харченка. - Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. -547 с.
2. Жураковський, Б. Ю. Технології інтернету речей. Навчальний посібник [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Інформаційне забезпечення робототехнічних систем» за спеціальністю 126 «Інформаційні системи та технології» / Б. Ю. Жураковський, І. О. Зенів ; КПІ ім. Ігоря Сікорського. –

Електронні текстові дані (1 файл: 5,1 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 271 с.
3. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том І. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018. -344 с.
Заплановані навчальні заходи та методи викладання. Поєднання традиційних та нетрадиційних методів викладання із використанням інноваційних технологій: лекції (тематична; проблемна); лабораторні заняття.
Методи оцінювання.
– поточний контроль (тестування, усне та письмове опитування);
– підсумковий контроль (екзамен).
Мова навчання та викладання. Українська.

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

Тип. За вибором.
Рік навчання. 2025/2026, 2026/2027.
Семестр. II -III.
Лектор, вчене звання, науковий ступінь, посада. Токар В. В., доктор економічних наук, професор, 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. «Алгоритмізація та програмування», «Об'єктно-орієнтоване програмування», «Основи баз даних та СУБД», «Технології розробки та тестування програмного забезпечення», «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. Токар В.В. Інноваційно-інвестиційна діяльність промислових підприємств та економічна безпека України: навч.посіб. - Київ: ТОВ "ПанТот", 2020. - 305 с. ISBN 978-966-1531-33-7/

2. Мельникова О.П. Економічна інформатика: навч.посіб. - Київ: Центр навчальної літератури, 2019 - 424 с.

3. Хорошко О.В., Криворучко О.В., Браіловський М.М. та ін. Захист систем електронних комунікацій: навч.посіб. - Київ: Київський національний торговельно-економічний університет, 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.

4.12. Назва. ПРАВОВЕ РЕГУЛЮВАННЯ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

Тип. За вибором.

Рік навчання. 2025/2026, 2026/2027.

Семестр. II -III.

Лектор, вчене звання, науковий ступінь, посада. Мельниченко Р.В., канд. юрид. наук, завідувач кафедри правового забезпечення безпеки бізнесу, адвокат.

Результати навчання. Опанування студентами таких знань та навичок: вміння аналізувати основні проблеми правового регулювання безпеки підприємницької діяльності; засвоєння і уміння використання правових засад забезпечення безпеки підприємницької діяльності; освоєння законодавчих засад правового регулювання охоронної діяльності; інформаційної-аналітичної роботи приватних підприємств; навички розробки нормативно-правових документів підприємств; уміння використовувати міжнародні норми права щодо забезпечення безпеки підприємницької діяльності на зовнішньоекономічному ринку.

Обов'язкові попередні навчальні дисципліни. «Кримінальне право», «Адміністративне право і процес».

Зміст. Основи правового захисту підприємницької діяльності в Україні. Правове регулювання охоронної діяльності. Правове регулювання захисту інформації та інформаційних відносин у діяльності комерційних підприємств, банків. Правове регулювання інформаційно-аналітичної роботи комерційних підприємств, банків. Нормативно-правові документи підприємств, банків з питань безпеки їх діяльності. Правовий статус працівника приватних охоронних організацій. Міжнародні норми права щодо забезпечення безпеки підприємницької діяльності на зовнішньоекономічному ринку.

Рекомендовані джерела та інші навчальні ресурси/засоби.

1. Організаційно-правові засади безпеки підприємницької діяльності (в таблицях і схемах) : навчальний посібник / Крегул Ю.І., Банк Р.О. – К. : Київ. нац. торг.-екон. ун-т, 2020. – 216 с.
2. Правове забезпечення безпеки суб'єктів господарської діяльності в Україні : навчальний посібник / В. В. Сергієнко, А. С. Пешкова. – Харків : ХНЕУ ім. С. Кузнеця, 2021. – 140 с.
3. Правове забезпечення охоронної діяльності та безпеки: хрестоматія / укладачі: Чайковський В.А., Кузнецов В.В., Сийплокі М.В. ; за заг. ред. В.В. Гелетея. К. :. 2020. – 573 с.

Заплановані навчальні заходи та методи викладання. Поєднання традиційних і нетрадиційних методів викладання із використанням інноваційних технологій: лекції (оглядові / тематичні); семінарські / практичні заняття.

Методи оцінювання.
– поточний контроль (тестування, усне / письмове опитування, вирішення юридичних задач, тощо);
– підсумковий контроль (екзамен).
Мова навчання та викладання. Українська.

ЗМІСТ