125 «КІБЕРБЕЗПЕКА»

ОСВІТНЬО – НАУКОВА ПРОГРАМА

підготовки здобувачів вищої освіти на другому (магістерському) рівні

«МАТЕМАТИЧНІ МЕТОДИ КІБЕРБЕЗПЕКИ»

Обсяг програми *120 кредитів ЄКТС*
Тривалість програми *1 рік 10 місяців*
форма навчання *денна, заочна*

Гарант програми – Лютий Олександр Іванович, кандидат технічних наук, доцент кафедри комп'ютерної математики та інформаційної безпеки КНЕУ
https://kneu.edu.ua/ua/depts9/k_komp_matematyky_ta_informacijnoi_bezpeku/Vikladachi23/Lyutij.O.I/
e-mail: lai1947@ukr.net

Проектна група, яка розробляла та буде здійснювати реалізацію програми:

Джалладова Ірада, д. ф.- м. н., професор, завідувачка кафедри комп'ютерної математики та інформаційної безпеки КНЕУ, https://kneu.edu.ua/ua/depts9/k_komp_matematyky_ta_informacijnoi_bezpeku/Vikladachi23/Dzhalladova I.A./
e-mail: dzhalladovakmib@kneu.edu.ua

Камінський Олег, д.е.н., доцент кафедри комп'ютерної математики та інформаційної безпеки КНЕУ https://kneu.edu.ua/ua/depts9/k_komp_matematyky_ta_informacijnoi_bezpeku/Vikladachi23/Kaminskij.O.E/

e-mail: olkam@kneu.edu.ua

Мета освітньої програми

Підготовка висококваліфікованих фахівців, здатних розробляти, використовувати технології інформаційної безпеки і кібербезпеки, приймати рішення в умовах невизначеності.

Фахівці мають компетенції системного, стратегічного і критичного мислення, знають і вміють застосовувати 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.

Програма спрямована на підготовку фахівців, здатних знати та розуміти концепції, моделі та засоби інформаційної безпеки та/або кібербезпеки; системного аналізу; методи і засоби дослідження, аналізу, створення та забезпечення функціонування систем управління інформаційною безпекою та/або кібербезпекою, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур кібербезпеки; програмні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційнії) та технології; інфраструктуру 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.

Особливості викладання на програмі

Унікальною конкурентною перевагою випускників є збалансоване поєднання широкого спектру знань спеціалізованих розділів математики і сучасних методів системного аналізу, аналітики кібербезпеки, безпеки людини та суспільства зі знаннями інформаційних технологій і систем, здатністю розробляти і використовувати технології інформаційної безпеки і кібербезпеки для розв'язання складних проблем, що виникають в інформаційних, економічних, фінансових, соціальних, політичних, організаційних системах.

Робочі місця магістрів з кібербезпеки у - ІТ-компаніях, банках, фінансових об'єктах, страхових компаніях, аналітичних відділах державних установ, консалтингових фірмах, ІТ-відділах підприємств будь-якої галузі, а саме: керівник служби безпеки банку; керівник служби захисту інформації; керівник аналітичного відділу з забезпечення кібербезпеки; керівник інформаційної служби; керівник служби з інформаційно-аналітичної роботи. Випускники програми здатні виконувати професійну роботу в науково-дослідницьких центрах, державних органах управління, навчальних закладах і організаціях різних форм власності та організаційно-правових форм, організаціях ІТ-індустрії, що розробляють системи, продукти, сервіси інформаційних технологій. Переважна більшість випускників ще до кінця навчання в університеті отримують постійне робоче місце за фахом.

Значення розв’язання наукових і технічних проблем фахівцями спеціальності «Математичні методи кібербезпеки» для держави полягає в розробці нових, і удосконаленні існуючих методів і засобів безпечної обробки інформації, керування складними кіберфізичними системами з урахуванням конфіденційності на всіх етапах проектування, підвищення ефективності і якості технічних, економічних, біологічних, медичних і соціальних систем в умовах цифрового суспільства.

Перелік компонент освітньо – професійної програми

Код н/д	Компоненти освітньої програми	К-ть кредитів	Семестр	Форма ПК
	Обов’язкові компоненти ОП			
	1.1. Цикл загальної підготовки			
ОКЗ 1.	Методологія наукових досліджень	4	1	Екзамен
ОКЗ 2.	Філософія аналітики	4	1	Екзамен
ОКЗ 3.	Management of Security in the Cyberspace	4	2	Екзамен
ОКЗ 4.	English language: науково-технічний переклад	4	2	Екзамен
ОКЗ 5.	Data Economics and its Security	4	3	Екзамен
	1.2. Цикл професійної підготовки			
ОКП 1.	Безпека WEB-ресурсів	4	1	Екзамен
ОКП 2.	Задачі прикладного системного аналізу	4	1	Екзамен
ОКП 3.	Прийняття рішень в умовах невизначеності	4	1	Екзамен
ОКП 4.	Інтелектуальний аналіз даних	4	2	Екзамен
ОКП 5.	Прикладні задачі стохастичної математики	5	2	Екзамен
ОКП 6.	Security programing	5	2	Екзамен
ОКП 7.	Аудит інформаційних систем	4	3	Екзамен
ОКП 8.	Business Intelligence	5	3	Екзамен
ОКП 9.	Моделі угроз	5	3	Екзамен
	Загальний обсяг обов'язкових компонент:	**60**		
	ІІ. Вибіркові компоненти ОП (студент обирає в кожному семестрі по три дисципліни)			

ВК 1.	Правові та етичні аспекти кібербезпеки (Cyber Security Low)	5	1	Залік
ВК 2.	Human factor in Cyber Security	5	1	Залік
ВК 3.	Кібергігієна	5	1	Залік
ВК 4.	Безпека соціальних медіа	5	1	Залік
ВК 5.	Методи та моделі системної динаміки	5	1	Залік
ВК 6.	Економіка кібербезпеки	5	1	Залік
ВК 7.	Етичне хакерство	5	2	Залік
ВК 8.	Дизайн інфраструктури кібербезпеки	5	2	Залік
ВК 9.	Аналітика даних та виклики на загрози людству	5	2	Залік
ВК 10.	Кібербезпека бізнес-структур	5	2	Залік
ВК 11.	Машинне навчання	5	2	Залік
ВК 12.	Багатовимірний аналіз даних	5	2	Залік
ВК 13.	Цифрова криміналістика	5	3	Залік
ВК 14.	Нейро-нечітки моделі	5	3	Залік
ВК 15.	Безпека даних	5	3	Залік
ВК 16.	Аналіз та безпека біхевіористської економіки	5	3	Залік
ВК 17.	Методологія викладання кібербезпеки	5	3	Залік
ВК 18.	Комп'ютерна дипломатія	5	3	Залік
Разом за циклом		**30**		
Всього		**90**		
	Практична підготовка			
ПП 1	Ситуаційний тренінг	5	3	Звіт
ПП 2	Науково-дослідна та виробнича практика	15	3	Залік
ПП 3	Підготовка та захист кваліфікаційної магістерської роботи	10	3	Захист
	Загальний обсяг практичної підготовки:	**30**		
	Загальний обсяг освітньо-професійної програми	**120**		

Програмні результати навчання

- ✓ Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач кібербезпеки у широких або мультидисциплінарних контекстах.
- ✓ 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 кібербезпеки.
- ✓ Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
- ✓ Провадити дослідницьку та/або інноваційну діяльність в сфері кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
- ✓ Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
- ✓ Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
- ✓ Виконувати аналіз кращих міжнародних практик, зокрема на моделях зрілості Control Objectives for Information and Related Technology (COBIT); виконувати оцінку IT процесів і заходів безпеки в органіації, визначати необхідні послуги ITIL та розробляти плани їх впровадження;
- ✓ Вміти, на основі вимог регуляторів і міжнародних стандартів з захисту інформації в індустрії платіжних карт, зокрема PCI DSS виконувати проектування, реалізацію та експлуатацію захищеної мережі, впроваджувати заходи контролю доступу, забезпечувати захист інформації про власників платіжних карт, розробляти і впроваджувати захищені системи і програми, розробляти і підтримувати політику ІБ;
- ✓ Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
- ✓ 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.

- ✓ 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.
- ✓ 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.
- ✓ Уміти створювати математичні, комп'ютерні моделі забезпечення захищеності інформаційної системи шляхом створення та застосування спеціалізованих програмних засобів;
- ✓ Уміти за допомогою спеціалізованих засобів здійснювати збір, аналіз та обробку інформації для подальшого розслідування інцидентів безпеки та комп’ютерного моделювання.