125 «КІБЕРБЕЗПЕКА»
ОСВІТНЬО – НАУКОВА ПРОГРАМА
підготовки здобувачів вищої освіти на першому (бакалаврському) рівні
«КІБЕРБЕЗПЕКИ»

Гарант програми – Бєгун Анатолій Володимирович, кандидат економічних наук, професор кафедри системного аналізу та кібербезпеки КНЕУ
https://kneu.edu.ua/ua/depts9/k_komp_matematyky_ta_informacijnoi_bezpeku/Vikladachi23/Begun.A.V/
e-mail: anatolii.biehun@kneu.ua

Галузь знань 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека»
Обсяг програми 240 кредитів ЄКТС
Тривалість програми 3 роки та 10 місяців
Форма навчання очна (денна), заочна

Освітньо-професійна програма «Кібербезпека» спрямована на підготовку висококваліфікованих фахівців, здатних розробляти, використовувати технології кібербезпеки та захисту інформації, приймати рішення в умовах невизначеності.

Здобувачі отримають 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.

Особливості освітньо-професійної програми

Особливістю програми є підготовка фахівців з кібербезпеки, які добре розуміються на методології і технології, розробки та експлуатації комплексних систем захисту інформації, джерелах та засобах впливу загроз на об’єкти інформаційної безпеки держави, обчислювальних засобах інформаційних систем. Отримавши диплом з цієї спеціальності, випускники стануть гарними фахівцями по боротьбі з кіберзлочинністю. Кіберзлочинність (хакери, хактивісти, комерційний шпіонаж, інформаційний тероризм, інформаційна війна тощо) сьогодні – це багатомільярдна індустрія. Отже, фахівець із захисту персонального та корпоративного кіберпростору знайде гідне місце на ринку праці.

Унікальною конкурентною перевагою випускників є збалансоване поєднання широкого спектру знань спеціалізованих розділів математики і сучасних методів програмування, аналітики кібербезпеки, безпеки людини та суспільства зі знаннями інформаційних технологій і систем, здатністю розробляти і використовувати комплексні системи захисту інформації.

№ п.п.	Назва навчальної дисципліни	Кількість кредитів ЄКТС
	Обов'язкові компоненти ОП	
	1.1. Цикл загальної підготовки	
1.1	Іноземна мова	10
1.2	Українознавство	4
1.3	Алгебра та геометрія	4
1.4	Дискретна математика	9
1.5	Операційні системи	4
1.6	Філософія	4
1.7	Вступ до спеціальності	5
1.8	Архітектура обчислювальних систем	4
1.9	Програмування та алгоритмічні мови (Python)	5
1.10	Організація баз та сховищ даних	5
1.11	Теорія ймовірностей і математична статистика	4
1.12	Інтелектуальний аналіз даних	4
1.13	Теорія інформаційних систем	4
1.14	Математичний аналіз	10
1.15	Комп'ютерна математика	4
	1.2. Цикл професійної підготовки	
1.16	Фізика 1	4
1.17	Фізика 2	4
1.18	Комп'ютерні мережі	4
1.19	Диференціальні рівняння	4
1.20	Економіка захисту інформації	5
1.21	Теорія інформації і кодування	4
1.22	Основи теорії кіл, сигнали і процеси в електроніці	5
1.23	Спеціальні розділи математики	4
1.24	Інформаційно-комунікаційні системи	4
1.25	Прикладна криптологія	5
1.26	Управління інформаційною безпекою	4
1.27	Комп'ютерна стеганографія	4
1.28	Захист інформації в ІКС	4
1.29	Цифрова обробка сигналів і зображень	4
1.30	Комплексні системи захисту інформації: проектування, впровадження, супровід	10
1.31	Кібербезпека	5
1.32	Нормативне правове забезпечення захисту інформації	4

	ІІ. Вибіркові компоненти ОП (студент обирає в кожному семестрі по три дисципліни)	
2.1	Бізнес-інформатика	4
2.2	Основи кібербезпеки	4
2.3	Основи криптографії	4
2.4	Бібліографічні дослідження	4
2.5	Електроніка	4
2.6	Технології і безпека хмарних обчислень	4
2.7	Фахова іноземна мова	4
2.8	Безпека комунікацій і мереж	4
2.9	Основи метрології та вимірювання	4
2.10	Web технології	4
2.11	Еконофізика	4
2.12	Фахова іноземна мова	4
2.13	Управління конфліктами в кіберпросторі	4
2.14	Теорія ігор	4
2.15	Фахова іноземна мова	4
2.16	Економічна безпека	4
2.17	Статистика в кіберпросторі	4
2.18	Системне програмування	4
2.19	Інформаційна культура	4
2.20	Управління персоналом та кадрова безпека	4
2.21	Фахова іноземна мова	4
2.22	Безпека і конфіденційність	4
2.23	Цифрова економіка	4
2.24	Теорія ризику в кіберпросторі	4
2.25	Бізнес-розвідка	4
2.26	Data Science	4
2.27	Фахова іноземна мова	4
2.28	Системи моніторингу	4
2.29	Бихейвірістська економіка в кіберпросторі	4
2.30	Мова ділових комунікацій та робота в команді	4
2.31	Кібербезпека бізнесу	4
2.32	Інформаційна безпека держави	4
	Загальний обсяг освітньо-професійної програми	**240**

Працевлаштування та конкурентні переваги випускників програми

Робочі місця бакалаврів з кібербезпеки у органах державної безпеки, ІТ-компаніях, банках, фінансових об’єктах, страхових компаніях, аналітичних відділах державних установ, консалтингових фірмах, ІТ-відділах підприємств будь-якої галузі. Переважна більшість випускників ще до кінця навчання в університеті отримують постійне робоче місце за фахом. Цьому сприяють постійна

профорієнтаційна робота в інституті, на кафедрі, проведення навчальної практики та регулярних зустрічей з потенційними роботодавцями.

Бакалавр з кібербезпеки може працювати:

- керівник підприємства (установи, організації) (сфера захисту інформації)
- керівники проектів та програм
- головний фахівець з програмного забезпечення
- головний фахівець з електронного устаткування
- менеджер (управитель) систем з інформаційної безпеки
- аналітик операційного та прикладного програмного забезпечення
- аналітик комп'ютерних систем
- аналітик з питань фінансово-економічної безпеки
- експерт технічний з промислової безпеки
- професіонал з фінансово-економічної безпеки
- судовий експерт

Програмні результати навчання

Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач кібербезпеки у широких або мульти дисциплінарних 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, 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; досліджувати, розробляти та впроваджувати методи і заходи протидії кібер інцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кібер інцидентів в цілому;

здатність володіти основними методами шифрування інформації з різним рівнем криптостійкості, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.