ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ:

Ректор

_____ Крисоватий А.І.

«30» травня 2018 р.

ОСВІТНЯ (ОСВІТНЬО-ПРОФЕСІЙНА) ПРОГРАМА

«КІБЕРБЕЗПЕКА»

підготовки здобувачів вищої освіти на другому (магістерському) рівні

за спеціальністю 125 «Кібербезпека»

галузі знань 12 «Інформаційні технології»

Схвалено Вченою Радою ТНЕУ
протокол № 7 від «30» травня 2018 р.
Вчений секретар _____ М.А.Мудрак

Тернопіль – 2018

І. Преамбула

ОПП «Кібербезпека» за спеціальністю 125 «Кібербезпека» для підготовки здобувачів вищої освіти на другому (магістерському) рівні містить обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти; перелік компетентностей випускника; нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання; форми атестації здобувачів вищої освіти; вимоги до наявності системи внутрішнього забезпечення якості вищої освіти.

ІІ. Загальна характеристика

Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня кваліфікація	Магістр з кібербезпеки
Кваліфікація в дипломі	Магістр з кібербезпеки
Опис предметної області	**Об'єкти вивчення:** об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення складових безпеки інформації: безпека інформації, кібербезпека; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту; теоретичні основи, системи та принципи функціонування технології блокчейн; механізми забезпечення безпеки в системах Інтернет речей. **Цілі навчання:** підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області.** Знання: - методів та засобів технічного та криптографічного захисту інформації; - методів та бібліотеки для програмування та обробки

	результатів експериментальних досліджень; - методики, загальних вимог, засобів тестування на проникнення; - методів моніторингу роботи комп'ютерних мереж з метою виявлення зловживань та аномалій; - методів та засобів зворотного проектування, аналізу шкідливого програмне забезпечення; - методів та криміналістичних інструментів, що використовуються для дослідження та аналізу мережевих інцидентів та збереження цифрових доказів. - теорії систем управління інформаційною та/або кібербезпекою; - методів машинного навчання і штучного інтелекту при проектуванні сучасних систем захисту від кібератак; - методів, розробки механізмів забезпечення безпеки в системах Інтернет речей та тестування Інтернет речей - принципів функціонування технології блокчейн; **Методи, методики та технології:** методи дослідницької діяльності та презентації результатів; *м*етоди, методики та технології забезпечення інформаційної та/або кібербезпеки. **Інструменти та обладнання:** системи розробки, забезпечення, моніторингу та контролю інформаційної та/або кібербезпеки; обладнання, необхідне для моніторингу функціонування і підтримки інформаційно-телекомунікаційних систем і мереж.
Академічні права випускників	Здобуття вищої освіти на третьому (освітньо-науковому) рівні
Обсяг освітньої програми магістр	90 кредитів ЄКТС / 1 рік 4 місяці

ІІІ Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Обсяг освітньої програми магістр	90 кредитів ЄКТС / 1 рік 4 місяці

VI. Перелік компетентностей випускника

Інтегральна компетентність	Здатність розв'язувати складні задачі і проблеми у галузі інформаційних технологій, зокрема у сфері кібербезпеки, та/або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог
Загальні компетентності	1. Здатність до абстрактного мислення, аналізу та синтезу. 2. Здатність проведення теоретичних та прикладних досліджень на відповідному рівні. 3. Здатність мотивувати людей та рухатися до спільної мети, працювати в команді співробітників. 4. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності). 5. Здатність удосконалювати свої навички на основі аналізу попереднього досвіду.
Спеціальні (фахові, предметні) компетентності	1. Здатність використовувати сучасні технології програмування при організації наукових досліджень, обробки експериментальних даних та представлення результатів. 2. Здатність проведення досліджень на відповідному рівні, здатність до пошуку, оброблення та аналізу інформації з різних джерел. 3. Здатність проводити тестування на проникнення, розробляти методики та процедури реагування на інциденти, оцінювати етичні та правові наслідки тестування на проникнення. 4. Здатність виконувати моніторинг комп'ютерних мереж з метою виявлення зловживань та аномалій. 5. Здатність виявляти шкідливе програмне забезпечення, проводити аналіз шкідливих програм, розуміти технічні аспекти функціонування шкідливих програм, зменшувати негативні наслідки від впливу шкідливого програмного забезпечення. 6. Здатність збирати та аналізувати докази комп'ютерних злочинів, таких як шахрайство, кібер-шпигунство та інші, розуміти криміналістичні інструменти та методи, що використовуються для дослідження та аналізу мережевих інцидентів та збереження цифрових доказів. 7. Здатність формувати комплекс заходів для управління інформаційною безпекою, здійснювати управління інцидентами кібербезпеки, здійснювати управління ризиками інформаційної та кібербезпеки. 8. Здатність розробляти нові та застосовувати існуючі

	методи машинного навчання і штучного інтелекту при проектуванні сучасних систем захисту від кібератак. 9. Здатність будувати та тестувати середовища Інтернет речей, використовувати технологію блокчейн та хмарні сервіси.

V. Програмні результати навчання

1. Набувати нові наукові і професійні знання, вдосконалювати навички, прогнозувати розвиток інформаційних систем та технологій.
2. Знати та застосовувати базові концепції і методології проведення досліджень у вибраній сфері діяльності.
3. Вміти приймати організаційно-управлінські рішення в умовах невизначеності.
4. Застосувати знання іноземної мови з метою забезпечення ефективності професійної комунікації.
5. Збирати та обробляти інформацію, необхідну для проведення наукових досліджень; використовувати технології програмування у професійних дослідженнях; логічно побудувати наукове дослідження відповідно до мети та завдання дослідження; науково обґрунтовувати та структурувати отримані наукові положення.
6. Володіти сучасними технологіями програмування для організації наукових досліджень, обробки експериментальних даних та представлення результатів досліджень.
7. Проводити дослідження на відповідному рівні, обробляти та аналізувати отримані експериментальні дані.
8. Здійснювати оцінку можливості проникнення в інформаційні системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності інформаційних систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування.
9. Здійснювати систематичний збір і обробку інформації, яка може бути використана для підвищення захищеності мережі, процесу ухвалення рішення, оцінки програм або вироблення політики безпеки
10. Володіти методиками проведення зворотної розробки програмного забезпечення та апаратних пристроїв.
11. Впроваджувати програмно-апаратні засоби виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки.
12. Використовувати сучасні методики та стандарти проведення технічного аудиту. Здійснювати аналіз ризиків функціонування комп'ютерних систем: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання управління ризиками.

13. Використовувати методи та алгоритми машинного навчання і штучного інтелекту та використовувати їх при проектуванні та дослідженні систем захисту від кібератак.
14. Використовувати основні методи, моделі та алгоритми захисту даних в програмно-апаратних системах Інтернет-речей. Надавати рекомендації щодо побудови та використання апаратних засобів, протоколів при проектуванні системи Інтернет-речей. Знати принципи технології блокчейн та застосовувати її при проектуванні захищених систем Інтернет-речей.

VI Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти за ОПП «Кібербезпека» зі спеціальності 125 «Кібербезпека» здійснюється у формі публічного захисту кваліфікаційної магістерської роботи. Атестація здійснюється відкрито і публічно.
Вимоги до заключної кваліфікаційної роботи	Кваліфікаційна (магістерська) робота є самостійним дослідженням студента і обов'язково перевіряється на плагіат. Закінчена робота оприлюднюється на офіційному сайті ТНЕУ.

VII Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Принципи та процедури забезпечення якості освіти	Визначаються Положенням про внутрішню систему забезпечення якості освіти в ТНЕУ
Моніторинг та періодичний перегляд освітніх програм	Визначається Положенням про організацію освітнього процесу в ТНЕУ
Оцінювання здобувачів вищої освіти	Визначається Положенням про оцінювання в ТНЕУ
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Визначається Положенням про педагогічне і наукове підвищення кваліфікації та стажування педагогічних і науково педагогічних працівників вищих навчальних закладів, затвердженого наказом МОН України № 567 від 24. 01. 2013 року.
Наявність необхідних ресурсів для організації освітнього процесу	Визначається вимогами матеріального забезпечення спеціальності
Наявність інформаційних систем для ефективного	Визначається Положенням про організацію освітнього процесу в ТНЕУ

управління освітнім процесом	
Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації	Розміщення на сайті ТНЕУ у відкритому доступі
Запобігання та виявлення академічного плагіату	Перевірка на плагіат

VII Перелік нормативних документів, на яких базується стандарт вищої освіти

1. Закон «Про вищу освіту»: за станом на 20.06.2016 р. [Електронний ресурс] // Законодавство України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18 . – Назва з титул. Екрану.
2. Международная стандартная классификация образования (МСКО) 2011 [Електронний ресурс] / Інститут статистики ЮНЕСКО, 2013. – 87 с – Режим доступу: http://www.uis.unesco.org/Education/Documents/isced-2011-ru.pdf. – Назва з титул. екрану.
3. Національний класифікатор України: Класифікатор професій ДК 003:2010. – К. : Видавництво «Соцінформ», 2010. – 746 с.
4. Про затвердження Національної рамки кваліфікацій: Постанова Кабінету Міністрів України від 23 листоп. 2011 р. № 1341 [Електронний ресурс] // Законодавство України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1341-2011-п-. – Назва з титул. екрану.
5. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: Постанова Кабінету Міністрів України від 29 квітня 2015 р. № 266 [Електронний ресурс] // Законодавство України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/266-2015-п . – Назва з титул екрана.
6. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG) [Електронний ресурс]. – К.: ТОВ «ЦС», 2015. – 32 с – Режим доступу: http://ihed.org.ua/images/pdf/standards-and-guidelines_for_qa_in_the_ehea_2015.pdf. – Назва з титул екрану
7. ISCED fields of education and training 2013 (ISCED-F 2013) [Електронний ресурс]. – UNESCO Institute for Statistics, 2014.-21р. – Режим доступу: http://www.uis.unesco.org/Education/Documents/isced-fields-of-education-training-2013.pdf. – Назва з титул. екрану.
8. Розроблення освітніх програм: методичні рекомендації – http://ihed.org.ua/images/biblioteka/rozroblennya_osv_program_2014_tempusoffice.pdf

ПОЯСНЮВАЛЬНА ЗАПИСКА

ОПП «Кібербезпека» за спеціальністю 125 «Кібербезпека» для підготовки здобувачів вищої освіти на другому (магістерському) рівні є нормативним

документом ТНЕУ, в якому визначається сукупність вимог до змісту та результатів освітньої діяльності.

ОПП «Кібербезпека» за спеціальністю 125 «Кібербезпека» для підготовки здобувачів вищої освіти на другому (магістерському) рівні визначає такі вимоги до освітньої програми:

- обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти;
- перелік компетентностей випускника;
- нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання;
- форми атестації здобувачів вищої освіти;
- вимоги до наявності системи внутрішнього забезпечення якості вищої освіти.

Матриця відповідності компетентностей дескрипторам НРК та матриця відповідності результатів навчання та компетентностей представлені в Таблицях 1 і 2.

Таблиця 1

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
1	2	3	4	5
Загальні компетентності				
Здатність до абстрактного мислення, аналізу та синтезу	+	+	+	+
Здатність проведення теоретичних та прикладних досліджень на відповідному рівні.	+	+	+	+
Здатність мотивувати людей та рухатися до спільної мети, працювати в команді співробітників.	+	+	+	+
Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).	+	+	+	+
Здатність удосконалювати свої навички на основі аналізу попереднього досвіду.	+	+	+	+
Спеціальні (фахові, предметні) компетентності				
Здатність використовувати сучасні технології програмування при організації наукових досліджень, обробки експериментальних даних та представлення результатів.	+	+	+	+
Здатність	+	+	+	+

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
1	2	3	4	5
проведення досліджень на відповідному рівні, здатність до пошуку, оброблення та аналізу інформації з різних джерел				
Здатність проводити тестування на проникнення, розробляти методики та процедури реагування на інциденти, оцінювати етичні та правові наслідки тестування на проникнення.	+	+	+	+
Здатність виконувати моніторинг комп'ютерних мереж з метою виявлення зловживань та аномалій.	+	+	+	+
Здатність виявляти шкідливе програмне забезпечення, проводити аналіз шкідливих програм, розуміти технічні аспекти функціонування шкідливих програм, зменшувати негативні наслідки від впливу шкідливого програмного забезпечення.	+	+	+	+
Здатність збирати та аналізувати докази комп'ютерних злочинів, таких як шахрайство, кібер-шпигунство та інші, розуміти криміналістичні	+	+	+	+

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
1	2	3	4	5
інструменти та методи, що використовуються для дослідження та аналізу мережевих інцидентів та збереження цифрових доказів.				
Здатність формувати комплекс заходів для управління інформаційною безпекою, здійснювати управління інцидентами кібербезпеки, здійснювати управління ризиками інформаційної та кібербезпеки.	+	+	+	+
Здатність розробляти нові та застосовувати існуючі методи машинного навчання і штучного інтелекту при проектуванні сучасних систем захисту від кібератак.	+	+	+	+
Здатність будувати та тестувати середовища Інтернет речей, використовувати технологію блокчейн та хмарні сервіси.	+	+	+	+

Таблиця 2

Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Програмні результати навчання	Компетентності														
	Інтегральна компетентність	Загальні компетентності					Спеціальні (фахові) компетентності								
		1	2	3	4	5	1	2	3	4	5	6	7	8	9
Набувати нові наукові і професійні знання, вдосконалювати навички, прогнозувати розвиток інформаційних систем та технологій.	+	+													
Знати та застосовувати базові концепції і методології проведення досліджень у вибраній сфері діяльності.	+		+												
Вміти приймати організаційно-управлінські рішення в умовах невизначеності.	+			+											
Застосувати знання іноземної мови з метою забезпечення ефективності професійної комунікації.	+				+					+					
Збирати та обробляти інформацію, необхідну для проведення наукових досліджень; використовувати технології програмування у професійних дослідженнях; логічно побудувати наукове	+					+				+					+

Програмні результати навчання	Компетентності														
	Інтегральна компетентність	Загальні компетентності					Спеціальні (фахові) компетентності								
		1	2	3	4	5	1	2	3	4	5	6	7	8	9
дослідження відповідно до мети та завдання дослідження; науково обґрунтовувати та структурувати отримані наукові положення.															
Володіти сучасними технологіями програмування для організації наукових досліджень, обробки експериментальних даних та представлення результатів досліджень.	+					+	+	+	+	+	+	+	+	+	+
Проводити дослідження на відповідному рівні, обробляти та аналізувати отримані експериментальні дані.	+							+			+				
Здійснювати оцінку можливості проникнення в інформаційні системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності інформаційних систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування.	+								+			+			

Програмні результати навчання	Компетентності														
	Інтегральна компетентність	Загальні компетентності					Спеціальні (фахові) компетентності								
		1	2	3	4	5	1	2	3	4	5	6	7	8	9
Здійснювати систематичний збір і обробку інформації, яка може бути використана для підвищення захищеності мережі, процесу ухвалення рішення, оцінки програм або вироблення політики безпеки	+									+			+		
Володіти методиками проведення зворотної розробки програмного забезпечення та апаратних пристроїв.	+										+			+	
Впроваджувати програмно-апаратні засоби виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки.	+										+				+
Використовувати сучасні методики та стандарти проведення технічного аудиту. Здійснювати аналіз ризиків функціонування комп’ютерних	+												+		

Програмні результати навчання	Компетентності														
	Інтегральна компетентність	Загальні компетентності					Спеціальні (фахові) компетентності								
		1	2	3	4	5	1	2	3	4	5	6	7	8	9
систем: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання управління ризиками.															
Використовувати методи та алгоритми машинного навчання і штучного інтелекту та використовувати їх при проектуванні та дослідженні систем захисту від кібератак.	+													+	
Використовувати основні методи, моделі та алгоритми захисту даних в програмно-апаратних системах Інтернет-речей. Надавати рекомендації щодо побудови та використання апаратних засобів, протоколів при проектуванні системи Інтернет-речей. Знати принципи технології блокчейн та застосовувати її при проектуванні захищених систем Інтернет-речей.	+														+