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	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій шифрування даних, виявлення вразливостей в програмному забезпеченні та апаратних засобах. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, наявністю спеціалізованих лабораторій. Кафедра кібербезпеки виконує: - проект Erasmus + Internet of Things: Emerging Curriculum for Industry and Human Applications ALIOT (reference number 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP). Інтернет речей: нова навчальна програма для потреб промисловості та суспільства; – науково-дослідні проекти, що фінансуються за кошти державного бюджету, на тему: 1) Методи захисту від комп’ютерних атак на основі нейронних

	мереж і штучних імунних систем; 2) Теоретичні основи та апаратні засоби підвищення продуктивності роботи безпровідних сенсорних мереж.
Академічні права випускників	Здобуття вищої освіти на третьому (освітньо-науковому) рівні

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

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

IV Перелік компетентностей випускника

Інтегральна компетентність	Здатність використовувати поглиблені теоретичні та фундаментальні знання в галузі інформаційних технологій для ефективного розв'язування складних спеціалізованих завдань та практичних проблем під час професійної діяльності, зокрема у сфері кібербезпеки.
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 використовувати знання методів, моделей та принципів для моделюванні захисту інформаційних систем. 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. Нормативний зміст підготовки здобувачів вищої освіти

Програмні результати навчання

1. Застосувати знання іноземної мови з метою забезпечення ефективності професійної комунікації.

2. 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.

3. Володіти сучасними технологіями програмування для організації наукових досліджень, обробки експериментальних даних та представлення результатів досліджень.

4. Володіти методиками опису і моделювання процесів в кіберпросторі, засобами моделювання процесів, моделями і алгоритмами прогнозування складних процесів в умовах проектування нових захищених інформаційних систем за допомогою спеціалізованих пакетів програм.

5. 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.

6. Здійснювати систематичний збір і обробку інформації, яка може бути використана для підвищення захищеності мережі, процесу ухвалення рішення, оцінки програм або вироблення політики безпеки.

7. Володіти методиками проведення зворотної розробки програмного забезпечення та апаратних пристроїв.

8. 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.

9. 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.

10. Використовувати методи та алгоритми машинного навчання і штучного інтелекту та використовувати їх при проектуванні та дослідженні систем захисту від кібератак.

11. 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 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

У ВНЗ повинна функціонувати система забезпечення вищим навчальним закладом якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;

9) інших процедур і заходів.

Система забезпечення вищим навчальним закладом якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням ВНЗ оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним агентством із

забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

VIII 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.

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 ом 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
використовувати знання методів, моделей та принципів для моделюванні захисту інформаційних систем.				
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	+	+	+	+

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
криміналістичні 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
1. Застосувати знання іноземної мови з метою забезпечення ефективності професійної комунікації.	+	+													
2. 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.	+		+												
3. Володіти сучасними технологіями програмування для організації наукових досліджень, обробки експериментальних даних та представлення результатів досліджень.	+			+											
4. Володіти методиками опису і моделювання процесів в кіберпросторі, засобами моделювання процесів, моделями і алгоритмами прогнозування складних процесів в умовах проектування нових захищених інформаційних систем за допомогою спеціалізованих пакетів програм.	+				+					+					
5. Здійснювати оцінку можливості проникнення в інформаційні системи та	+					+				+					+

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
мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності інформаційних систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування.															
6. Здійснювати систематичний збір і обробку інформації, яка може бути використана для підвищення захищеності мережі, процесу ухвалення рішення, оцінки програм або вироблення політики безпеки.	+					+	+	+	+	+	+	+	+	+	+
7. Володіти методиками проведення зворотної розробки програмного забезпечення та апаратних пристроїв.	+							+			+				
8. 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.	+								+			+			
9. 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	+									+			+		

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
управління ризиками.															
10. Використовувати методи та алгоритми машинного навчання і штучного інтелекту та використовувати їх при проектуванні та дослідженні систем захисту від кібератак.	+										+			+	
11. 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.	+										+				+