

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«Ужгородський національний університет»**

ЗАТВЕРДЖЕНО

Вченою радою ДВНЗ

«Ужгородський національний
університет»,

протокол № 6 від 23.05. 2017р.

Голова Вченої ради, ректор

В.І.Смоланка



ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

**Підготовки здобувачів другого (магістерського) рівня
вищої освіти**

ГАЛУЗЬ ЗНАНЬ 12 Інформаційні технології

СПЕЦІАЛЬНІСТЬ 125 Кібербезпека

НАЗВА ОПП Безпека інформаційних і комунікаційних систем

Ужгород 2017 р.

Освітньо професійна програма "Безпека інформаційних і комунікаційних систем" підготовки другого (магістерського) рівня вищої освіти спеціальності 125 "Кібербезпека" розроблена згідно вимог Закону України "Про вищу освіту".

Програма відповідає другому циклу вищої освіти та сьомому кваліфікаційному рівню за Національною рамкою кваліфікацій України.

Укладачі програми:

1. Трефілов Юрій Костянтинович, старший викладач кафедри твердотільної електроніки та інформаційної безпеки
2. Різак Василь Михайлович, доктор фіз.-мат. наук професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки;
3. Січка Михайло Юрійович, кандидат фіз.-мат. наук доцент кафедри твердотільної електроніки та інформаційної безпеки

**1. Профіль освітньої програми зі спеціальності
№ 125 "Кібербезпека" (за спеціалізацією "Безпека інформаційних і
комунікаційних систем ")**

Загальна інформація	
Повна назва вищого навчального закладу	Державний вищий навчальний заклад «Ужгородський національний університет»
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти: магістр. Освітня кваліфікація: магістр з кібербезпеки Професійна кваліфікація : професіонал із організації інформаційної безпеки
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС. Термін навчання 1 рік і 4 місяців.
Наявність акредитації	Акредитаційна комісія України Сертифікат про акредитацію серія НД № 0789904 Термін дії сертифікату до 01.07.2022р.
Цикл/рівень	Національна рамка кваліфікацій України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень.
Передумови	Наявність першого (бакалаврського) рівня вищої освіти. Умови вступу визначаються «Правилами прийому до Ужгородського національного університету»
Мова(и) викладання	Українська
Термін дії освітньої програми	Відповідно до терміну дії сертифікату про акредитацію
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.uzhnu.edu.ua/uk/infocentre/15068
Мета освітньої програми	
Навчання та підготовка професіоналів в області БІКС, які мають базові знання та навички в застосуванні законодавчої бази в галузі інформаційної безпеки, розробці технологій і засобів захисту інформації, застосуванні стандартних і проектуванні нових криптографічних алгоритмів для захисту інформації в комп'ютерних системах і мережах, з метою ефективної боротьби з кіберзлочинністю.	
Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))	12 Інформаційні технології, 125 Кібербезпека, спеціалізація 8.17010201 (Безпека інформаційних і комунікаційних систем). Цикл дисциплін загальної підготовки – 12,5 кредитів ЄКТС, 375 год. З них дисципліни вільного вибору студента – 3,5 кредити ЄКТС, 105 год. Цикл дисциплін професійної підготовки – 77,5 кредитів ЄКТС, 2325 год. З них дисципліни вільного вибору студента – 19 кредитів ЄКТС, 570 год.

Орієнтація освітньої програми	Освітньо-професійна програма орієнтована на поглиблене вивчення дисциплін природничо-наукової підготовки з поглибленим вивченням дисциплін фахової підготовки у тому числі і базових дисциплін суміжних напрямів.
Основний фокус освітньої програми та спеціалізації	Протягом навчання за програмою «Безпека інформаційних і комунікаційних систем» магістр набуває практичних навичок з організації безпеки операційних систем і баз даних, технічного захисту інформації, антивірусного захисту, безпеки Web-сервісів.
Особливості програми	Магістри адаптуються до зростаючих потоків інформації та наслідків науково-технічного прогресу, постійно засвоюють новітні світові науково-технічні досягнення в галузі інформаційної безпеки та захисту інформації, використовують сучасні інформаційні технології, знання фундаментальних законів і понять природничих наук.

**Придатність
випускників до працевлаштування та подальшого навчання**

Придатність до працевлаштування	<p style="text-align: center;">Професіонал здатний виконувати професійну роботу і може займати первинні посади:</p> <ul style="list-style-type: none"> – Інженер з комп'ютерних систем – Інженер з програмного забезпечення комп'ютерів – Інженер-дослідник з комп'ютеризованих систем та автоматики – Інженер-програміст – Інженер із застосування комп'ютерів – Інженер електрозв'язку – Інженер засобів радіо та телебачення – Інженер лінійних споруд електрозв'язку та абонентських пристроїв – Інженер мережі стільникового зв'язку – Інженер-електронік – Інженер інформаційно-телекомунікаційних систем – Інженер інформаційно-телекомунікаційних технологій – Професіонал із організації захисту інформації з обмеженим доступом
--	--

	<ul style="list-style-type: none"> - Професіонал із організації інформаційної безпеки - Асистент
Подальше навчання	<p>Випускник з дипломом магістра може продовжити навчання в аспірантурі для отримання наукового ступеня доктора філософії.</p> <p>Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти.</p>
Викладання та оцінювання	
Викладання та навчання	Студентсько-центроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуально-творчий підхід, навчання через виробничу та педагогічну практики.
Оцінювання	<p>Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної навчальної діяльності, спрямованої на опанування навчального навантаження з освітньої програми: поточний, модульний, підсумковий контроль, комплексний кваліфікаційний екзамен;</p> <p>Усні та письмові екзамени, заліки, презентації, проектна робота диференційований залік з педагогічної практики, переддипломної практики, курсова робота.</p>
Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	<ul style="list-style-type: none"> - Здатність до професійного спілкування іноземною мовою; (ЗК1) - Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях; (ЗК2) - Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням;(ЗК3)

Фахові компетентності (ФК)	<ul style="list-style-type: none"> - Здатність до застосування сучасних інформаційних технологій і технологій безпеки у сфері захисту інформації;(ФК1) - Здатність до виявлення уразливостей та забезпечення безпеки проводових і бездротових мереж, розслідування інцидентів інформаційної та кібербезпеки та протидії злочинному програмному забезпеченню; (ФК2) - Здатність до забезпечення безпеки Web ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження; (ФК3) - Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки; (ФК4) - Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації; (ФК5)
Програмні результати навчання	
Загальні результати навчання	<ul style="list-style-type: none"> - вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації; (ПРН 1) - вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; (ПРН 2) - вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки; (ПРН 3)
Фахові результати навчання	<ul style="list-style-type: none"> - вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації; (ПРН 4) - знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки безпроводових і мобільних мереж; (ПРН 5) - знати методи і способи розробки та тестування програмного забезпечення з виявлення і

	<p>усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів); (ПРН 6)</p> <ul style="list-style-type: none"> - вміти проводити семантичний аналіз файлів;(ПРН 7) - вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою; (ПРН 8) - вміти відновлювати пошкоджену інформацію;(ПРН 9) - вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ; (ПРН 10) - знати існуючі уразливості Web ресурсів (sql ін'єкції, брутфорс, xss й т.д) та способи боротьби з ними на етапі розробки та в процесі експлуатації, знати шаблони проектування безпечних Web додатків; (ПРН 11) - знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки, вміти знаходити шляхи для їх усунення;(ПРН 12) - вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки. (ПРН 13) - знати уразливості й методи їх застосування в різних телекомунікаційних технологіях, знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж; (ПРН 14)
Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Склад проектної групи освітньої програми, професорсько-викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на першому (бакалаврському) рівні вищої освіти.

Матеріально-технічне забезпечення	<p>Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребам. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць в гуртожитку відповідає вимогам. Для проведення практичних і лабораторних робіт, інформаційного пошуку та обробки результатів наявні спеціалізовані комп'ютерні класи факультету з необхідним програмним забезпеченням та необмежено відкритим доступом до Інтернет-мережі.</p>
Інформаційне та навчально- методичне забезпечення	<p>-офіційний веб-сайт http://www.uzhnu.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти;</p> <ul style="list-style-type: none"> - необмежений доступ до мережі Інтернет; - наукова бібліотека, читальні зали; - навчальні і робочі плани; - графіки навчального процесу; - навчально-методичні комплекси дисциплін; - дидактичні матеріали для самостійної та індивідуальної роботи студентів з дисциплін, програми практик; - методичні вказівки щодо виконання кваліфікаційних робіт.
Академічна мобільність	
Національна кредитна мобільність	<p>Підвищення кваліфікації (стажування) науково-педагогічних працівників у вітчизняних закладах вищої освіти на основі двосторонніх договорів між Ужгородським національним університетом та університетами України.</p>
Міжнародна кредитна мобільність	<p>Угода щодо семестрового академічного обміну між Поморською Академією у м. Слупськ (Польща) та Ужгородським національним університетом.</p>
Навчання іноземних здобувачів вищої освіти	<p>Можливе навчання іноземних громадян. Навчання іноземних студентів проводиться на загальних умовах або за індивідуальним графіком.</p>

2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1 Обов'язкові компоненти ОП			
1.1 Цикл загальної підготовки			
ОК 1.1.1	Охорона праці в галузі	3	Іспит
ОК 1.1.2.	Дидактика вищої школи	3	Залік
ОК 1.1.3.	Основи наукових досліджень та організація науки	3	Іспит
1.2. Цикл професійної підготовки			
ОК 1.2.1.	Методи моделювання та оптимізації процесів	8	Іспит, залік
ОК 1.2.2.	Теорія розподілених інформаційних ресурсів, захист баз даних та знань	6	Іспит
ОК 1.2.3.	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	4,5	Залік
ОК 1.2.4.	Технології створення та застосування систем захисту інформаційно-комунікаційних систем	4	Залік
ОК 1.2.5.	Методи побудови та аналізу криптосистем	6	Іспит
ОК 1.2.6.	Педагогічна практика у ВНЗ (2 тижні)	3	Залік
ОК 1.2.7.	Науково-дослідна практика (2 тижні)	3	Залік
ОК 1.2.8.	Переддипломна практика (3тижні)	4,5	Залік
ОК 1.2.9.	Виконання магістерської роботи	16,5	
ОК 1.2.10.	Атестація	3	

Загальний обсяг обов'язкових компонент:		67,5 кредитів	
2.Вибіркові компоненти ОП			
2.1. Цикл загальної підготовки			
ВБ 2.1.1.	Виявлення та попередження правопорушень, вчинених із використанням інформаційних технологій / Технології запобігання злочинності в інформаційно - комунікаційних системах.	3,5	Залік
2.2. Дисципліни професійної її підготовки			
ВБ 2.2.1.	Технологія організації інфраструктури відкритих ключів/Безпека передачі даних у інформаційно-комунікаційних мережах	3,5	Залік
ВБ 2.2.2	Бездротові інформаційно-комунікаційні системи та їх проектування/Мережі зв'язку нового покоління	5,5	Іспит
ВБ 2.2.3	Технології стиску інформаційних потоків/Мультиплексування	4,5	Іспит
ВБ 2.2.4	Автоматизоване проектування технічних засобів захисту інформації/Технології проектування систем технічного захисту інформації	5,5	Залік
Загальний обсяг вибірових компонент		22,5 кредити	
Загальний обсяг освітньої програми		90 кредит	

2.2 Структурно-логічна схема ОП

Семестр	Номер дисципліни згідно навчального плану
1	1.1.1., 1.1.3., 1.2.1.,1.2.5., 2.1.1., 2.2.2., 2.2.4.
2	1.1.2., 1.2.1., 1.2.2., 1.2.3., 1.2.4., 2.2.1., 2.2.3.
3	1.2.7., 1.2.8., 1.2.9.
4	1.2.9., 1.2.10.

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності №125 «Кібербезпека», спеціалізація 8.17010201 «Безпека інформаційних і комунікаційних систем», проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документа встановленого зразка про присудження ступеня магістра із присвоєнням кваліфікації: Магістр з кібербезпеки за спеціалізацією професіонал із організації інформаційної безпеки.

Захист кваліфікаційної (магістерської) роботи відбувається як публічна презентація.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1.1.1.	ОК 1.1.2.	ОК 1.1.3.	ОК 1.2.1.	ОК 1.2.2.	ОК 1.2.3.	ОК 1.2.4.	ОК 1.2.5.	ОК 1.2.6.	ОК 1.2.7.	ОК 1.2.8.	ОК 1.2.9.	ОК 1.2.10.	ВБ 2.1.1.	ВБ 2.2.1.	ВБ 2.2.2.	ВБ 2.2.3.	ВБ 2.2.4.
ЗК 1			+															
ЗК 2	+	+								+								
ЗК 2								+	+	+	+			+				
ФК 1					+		+							+		+	+	+
ФК 2				+	+		+							+	+			+
ФК 3						+	+								+			
ФК 4								+							+		+	
ФК 5					+	+								+			+	

4. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ОК 1.1.1.	ОК 1.1.2.	ОК 1.1.3.	ОК 1.2.1.	ОК 1.2.2.	ОК 1.2.3.	ОК 1.2.4.	ОК 1.2.5.	ОК 1.2.6.	ОК 1.2.7.	ОК 1.2.8.	ОК 1.2.9.	ОК 1.2.10.	ВБ 2.1.1.	ВБ 2.2.1.	ВБ 2.2.2.	ВБ 2.2.3.	ВБ 2.2.4.
ПРН 1	+	+	+															
ПРН 2		+	+						+	+	+							
ПРН 3							+			+	+							
ПРН 4						+								+			+	
ПРН 5							+									+		+
ПРН 6						+									+			+
ПРН 7					+										+		+	
ПРН 8					+										+			+
ПРН 9																	+	
ПРН 10				+													+	+
ПРН 11							+									+		+
ПРН 12				+										+				
ПРН 13								+										
ПРН 14					+	+								+				