

**Чернівецький національний університет
імені Юрія Федьковича**

Схвалено

Вченою радою Чернівецького
національного університету
імені Юрія Федьковича
протокол № _____
від _____

Затверджено

Ректор Чернівецького національного
університету імені Юрія Федьковича
_____ С.В. Мельничук
«__» _____

**Освітня програма
підготовки здобувачів другого (магістерського)
рівня вищої освіти
галузі знань 12 «Інформаційні технології»
спеціальності 125 «Кібербезпека»
спеціалізації «Системи технічного захисту інформації»**

Освітня програма «Кібербезпека» підготовки здобувачів другого (магістерського) рівня вищої освіти – магістра – спеціальності 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» розроблена згідно з вимогами Закону України «Про вищу освіту».

Програма відповідає другому (магістерському) рівню вищої освіти та сьомому кваліфікаційному рівню за Національною рамкою кваліфікації.

Проектна група програми:

Політанський Леонід Францович – д.т.н., професор, професор кафедри радіотехніки та інформаційної безпеки

Кушнір Микола Ярославович – к.ф.-м.н., доцент, доцент кафедри радіотехніки та інформаційної безпеки;

Рождественська Маргарита Григорівна – к.ф.-м.н., доцент, доцент кафедри радіотехніки та інформаційної безпеки.

Гарант освітньої програми:

Політанський Леонід Францович – д.т.н., професор, професор кафедри радіотехніки та інформаційної безпеки

Програму погоджено:

Директор ІФТКН

проф. О.В. Ангельський

Перший проректор

проф. Р.І. Петришин

1. Загальна характеристика освітньої програми

Метою освітньої програми є забезпечення оволодіння студентами другим (магістерським) рівнем вищої освіти, відповідно до сьомого кваліфікаційного рівня Національної рамки кваліфікацій.

Другий (магістерський) рівень вищої освіти передбачає здобуття особою поглиблених теоретичних та практичних знань, умінь, навичок за обраною спеціальністю в рамках запропонованої спеціалізації, загальних засад методології наукової та професійної діяльності, інших компетентностей, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності.

Програмні компетентності

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ 2. Знання та розуміння предметної області та розуміння професії.
	КЗ 3. Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово
	КЗ 4. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки
	КЗ 5. Вміння виявляти, ставити та вирішувати проблеми.
	КЗ 6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
	КЗ 7. Навички міжособистісної взаємодії
	КЗ 8. Прагнення до збереження навколишнього середовища
	КЗ 9. Здатність діяти соціально відповідально та громадянсько свідомо.
	КЗ 10. Здатність вчитися і бути сучасно навченим.
	КЗ 11. Здатність приймати обґрунтовані рішення.
	КЗ 12. Здатність до адаптації та дії в новій ситуації.
	КЗ 13. Дотримання та пропагування здорового способу життя.
	КЗ 14. Здатність бути критичним та самокритичним
Спеціальні компетентності	КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.
	КФ 2. Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС, каналів зв'язку, систем управління процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації.
	КФ 3. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки
	КФ 4. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі

КФ 5	Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем
КФ 6.	Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов
КФ 7.	Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС
КФ 8.	Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки
КФ 9.	Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою
КФ 10.	Здатність здійснювати управління інцидентами інформаційної та кібербезпеки
КФ 11.	Здатність здійснювати управління ризиками інформаційної та кібербезпеки
КФ 12.	Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій
КФ 13.	Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники
КФ 14.	Здатність проводити дослідження у практичній професійній діяльності

2. Перелік навчальних дисциплін освітньої програми

Освітня програма включає наступні розділи:

А. Освітня складова (90 кредитів ECTS)

І. Нормативна частина:

- цикл обов'язкових дисциплін загальної та професійно-наукової підготовки.

ІІ. Варіативна частина:

- цикл дисциплін вибору ВНЗ;

- цикл дисциплін вільного вибору студента.

Б. Практична складова (12 кредитів ECTS)

ІІІ. Практична підготовка.

В. Науково-дослідна складова (12 кредитів ECTS)

ІV. Наукова підготовка.

А. Освітня складова (90 кредитів ECTS)

І. Нормативна частина

Цикл “нормативна частина” включає у себе дисципліни загальної підготовки та професійної підготовки.

Тематичний блок І. «Обов'язкові навчальні дисципліни» спрямований на надання студентам оптимальних знань та навичок, необхідних для здійснення майбутніми магістрами професійного наукового пошуку та синтезу виважених обґрунтованих ідей. Дисципліни професійно-наукової підготовки спрямовані на надання студентам, що навчаються в магістратурі,

глибоких доктринальних знань в галузі інформаційних технологій, вироблення необхідних вмінь та навиків самостійної наукової діяльності і продукування нових ідей.

У межах тематичного блоку I «Обов'язкові навчальні дисципліни» вивчаються наступні дисципліни:

№	Назва дисципліни	Кількість кредитів	Кількість годин	Кількість аудиторних годин	Кількість годин на самостійне вивчення	Форма контролю
1	Охорона праці в галузі	4	120	30	90	Екзамен
2	Педагогіка і психологія вищої школи	3	90	30	60	Екзамен
3	Технології комплексного захисту інформації	5,5	165	45	120	Залік
4	Методика викладання дисциплін ТЗІ у вищій школі	5	150	45	105	Екзамен
5	Математичні методи моделювання і оптимізації процесів у ТЗІ	5	150	45	105	Екзамен
6	Теорія захисту інформаційних ресурсів обмеженого доступу	4	120	30	90	Залік
7	Автоматизація обробки інформації з обмеженим доступом	4	120	30	90	Залік
8	Радіомоніторинг і радіо протидія на об'єктах інформаційної діяльності	3	90	30	60	Залік
9	Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	3	90	30	60	Залік
Загалом по блоку I		36,5	1095	315	780	

II. Варіативна частина

Варіативна складова освітньої програми формується з урахуванням сучасного рівня наукових досягнень в галузі та індивідуальних освітніх запитів студентів. Варіативна складова створює передумови для відображення у змісті освітньої програми особливостей вузькопрофільної підготовки в межах обраних дисциплін, а головне — для диференціації та індивідуалізації підготовки магістрів.

Варіативна частина освітньої програми магістра у галузі «Інформаційні технології» за спеціальністю «Кібербезпека» включає в себе 2 цикли:

- цикл дисциплін вибору ВНЗ;
- цикл дисциплін вільного вибору студента.

У межах тематичного блоку II.1. «Цикл дисциплін вибору ВНЗ» вивчаються наступні дисципліни:

№	Назва дисципліни	Кількість кредитів	Кількість годин	Кількість аудиторних годин	Кількість годин на самостійне вивчення	Форма контролю
1	ТЗІ в комп'ютерних системах	5	150	45	105	Екзамен
2	Організація, план-ня та управління виробництвом	3	90	45	45	Екзамен
3	ТЗІ в інформаційно-вимірювальних системах	4,5	135	32	103	Залік
4	ТЗІ в телекомунікаційних системах	5	150	45	105	Залік
5	Інтелектуальна власність	3	90	30	60	Залік
Загалом по блоку II.1		20,5	615	197	418	

Блок II.2 варіативної частини освітньої програми включає в себе 2 навчальні дисципліни, з яких студент обирає для навчання 1 дисципліну.

№	Назва дисципліни	Кількість кредитів	Кількість годин	Кількість аудиторних годин	Кількість годин на самостійне вивчення	Форма контролю
1	Методологічні основи наукових досліджень	3	90	30	60	Залік
	Пристрої і системи телебачення					
Загалом по блоку II.2		3	90	30	60	

Освітня складова завершується державним іспитом, для проведення якого формується Екзаменаційна комісія.

Б. Практична складова (12 кредитів ECTS)

III. Практична підготовка

Цикл практичної підготовки включає в себе асистентську практику магістра на базі Чернівецького національного університету імені Юрія Федьковича, проведення ними семінарських, практичних та лабораторних занять для студентів I-IV курсів спеціальностей "Системи технічного захисту інформації" та "Кібербезпека".

У межах тематичного блоку III. «Практична підготовка» здійснюється:

№	Вид діяльності	Кількість кредитів	Кількість годин
1	Асистентська практика	12	360
Загалом по блоку III		12	360

В. Науково-дослідна складова (12 кредитів ECTS)

IV. Науково-дослідна підготовка

Цикл науково-дослідної підготовки включає в себе власне роботу магістра над кваліфікаційним проектом (роботою), підготовку виступів на наукових семінарах, участь в роботі з написання наукових статей і тез конференцій, тобто всі можливі види наукової діяльності, в яких магістр реалізовує набуті знання, вміння та навички у практичній науковій роботі.

У межах тематичного блоку IV. «Наукова підготовка» здійснюється:

№	Вид діяльності	Кількість кредитів	Кількість годин
1	Переддипломна практика	12	360
Загалом по блоку IV		12	360

3. Визначення форм державної атестації

Форми атестації здобувачів вищої освіти	<p>Атестація здійснюється екзаменаційною комісією відповідно до вимог стандарту вищої освіти після виконання студентом навчального плану та завершується видачею диплома встановленого зразка.</p> <p>На атестацію вноситься увесь нормативний зміст підготовки фахівця.</p> <p>Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.</p> <p>Атестація здійснюється у формі кваліфікаційного екзамену (освітня складова) та захисту кваліфікаційної роботи/проекту (практична та наукова складова).</p> <p>До атестації допускаються студенти, які виконали всі вимоги освітньої програми та навчального плану.</p> <p>Результати атестації визначаються оцінками за національною шкалою «відмінно», «добре», «задовільно», «незадовільно»</p> <p>Атестація здобувачів вищої освіти ступеня магістра здійснюється екзаменаційною комісією на підставі публічного захисту результатів досліджень у формі дипломного проекту/роботи у ЕК.</p>
Вимоги до кваліфікаційної роботи	<p>Кваліфікаційний проект (кваліфікаційна робота) передбачає розв'язання складного спеціалізованого завдання або практичної проблеми в галузі кібербезпеки, що характеризується комплексністю та невизначеністю умов.</p> <p>Кваліфікаційний проект (кваліфікаційна робота) має бути перевірений на плагіат.</p> <p>Кваліфікаційний проект (кваліфікаційна робота) має бути розміщений на сайті вищого навчального закладу.</p>
Вимоги до кваліфікаційного екзамену	<p>Кваліфікаційний екзамен передбачає оцінювання обов'язкових результатів навчання, визначених освітньою програмою.</p>

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ (загальні)

Освітня складова спрямована на надання студентам оптимальних знань та навичок, необхідних для здійснення ними професійного, наукового пошуку та синтезу виважених обґрунтованих ідей, надання студентам, що навчаються в магістратурі, глибоких знань в галузі інформаційної безпеки.

В результаті навчання в магістратурі очікується набуття таких соціально-особистісних компетентностей:

- здатність до організації власної професійної та науково-дослідницької діяльності;
- здатність до системного критичного мислення; науковий світогляд і творче мислення;

- здатність до навчання впродовж життя; здатність до критики й самокритики; толерантність до різних ідей;
- креативність, здатність до системного мислення; адаптивність і комунікабельність;
- наполегливість у досягненні мети;
- турбота про якість виконуваної роботи.

Також очікується набуття загальнонаукових компетентностей:

- розуміння причинно-наслідкових зв'язків й уміння їх використовувати в професійній і соціальній діяльності;
- аналітичні здібності;
- дослідницькі навички;
- навички управління інформацією;
- здатність виявляти актуальні проблеми;
- здатність здійснювати теоретичний аналіз проблеми; здатність пропонувати та обґрунтовувати гіпотези;
- володіння теоретико-методологічними засадами регулювання відносин інтелектуальної власності;
- розуміння необхідності участі в конкурсах та грантових і стипендіальних програмах;
- знання основ методології, техніки і організації науково-дослідної роботи, підходів до планомірної та ефективної індивідуальної і командної дослідницької діяльності;
- здатність до критичного аналізу та оцінки сучасних наукових досягнень; генерування нових ідей при вирішенні дослідницьких і практичних завдань, в тому числі в міждисциплінарних областях;
- здатність планувати і здійснювати комплексні дослідження на основі цілісного системного наукового світогляду з використанням набутих практичних знань.

5. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ (фахові)

Очікується набуття професійних компетентностей:

науково-дослідницька діяльність:

- готовність використати сучасні досягнення науки і передових технологій;
- здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі інформаційної безпеки;
- готовність представляти результати досліджень у вигляді звітів і публікацій державною та однією з іноземних мов;

науково-педагогічна діяльність:

- здатність до викладання у навчальному закладі предметів, що відносяться до галузі кібербезпеки;

- здатність розробляти методичні матеріали, що використовуються студентами в навчальному процесі;

проектувальна діяльність:

- здатність розуміти і аналізувати напрями розвитку об'єктів інформаційної діяльності, загальної теорії побудови математичних моделей і їх реалізації, теорії і практики керівництва проектами зі створення інформаційних ресурсів обмеженого доступу;

- здатність до організації, розроблення, упровадження та експлуатації систем і комплексів у сфері кібербезпеки;

- здатність здійснювати та детально обгрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки об'єктів інформаційної діяльності;

- здатність розробляти проектну документацію, програми та методики випробувань та організувати тестування та налагодження комплексів, призначених для захисту кіберпростору;

- здатність упроваджувати на об'єктах інформаційної діяльності сучасні методи забезпечення безпеки відповідно до вимог вітчизняних та міжнародних стандартів;

організаційно-управлінська діяльність:

- здатність організувати роботу колективу виконавців, приймати управлінські рішення в умовах різноманіття думок, визначення порядку виконання робіт;

- здатність організувати і виконувати роботи з виготовлення, монтажу, налагодження, випробування та здачі в експлуатацію систем і засобів технічного захисту інформації;

- здатність розробляти проекти методичних і нормативних документів, технічної документації, а також пропозиції та заходи з реалізації розроблених проектів;

- здатність організувати роботу з удосконалення, модернізації, уніфікації систем, засобів і технологій забезпечення безпеки кіберпростору відповідно до нормативно-правових актів і нормативно-методичних документів, що діють в Україні й у світі;

- володіння правовими та науково-організаційними основами проведення ліцензування, атестації та сертифікації об'єктів кіберпростору.

Практична складова, поряд з освітньою, спрямована на отримання студентами, що навчаються в магістратурі, досвіду викладацької діяльності, вміння доносити інформацію до студентів, організувати навчальний процес, залучати студентів до наукової роботи, роботи в лабораторіях, пояснювати на доступному для студентів рівні наукові методи та результати. При цьому очікується набуття магістрами сукупності компетентностей, необхідних для роботи викладачем.

Наукова складова освітньої програми передбачає проведення студентом власного наукового дослідження під керівництвом одного або

двох наукових керівників та оформлення його результатів у вигляді дипломного проекту або дипломної роботи.

Дипломний проект (робота) на здобуття ступеня магістра є самостійним розгорнутим дослідженням, що пропонує розв'язання актуального наукового завдання за спеціальністю «125 - Кібербезпека» (Системи технічного захисту інформації), результати якого становлять оригінальний внесок у суму знань за спеціальністю «125 - Кібербезпека» та оприлюднені у відповідних публікаціях.

Важливою частиною наукової складової освітньої програми магістратури є участь у підготовці наукових статей, виступи на наукових та науково-практичних конференціях, фахових семінарах, круглих столах, симпозиумах.

Тематики дипломних робіт та проектів за спеціальністю «125 - Кібербезпека» (Системи технічного захисту інформації):

1. Застосування хаотичних сигналів у системах кібербезпеки.
2. Дослідження процесів формування та властивостей фрактальних сигналів.
3. Програмно-апаратна реалізація засобів та пристроїв кібербезпеки на основі нелінійної динаміки.
4. Дослідження резонансних явищ у нелінійних параметричних колах.
5. Розробка стеганографічних методів захисту інформації.
6. Підвищення стійкості систем захисту інформації до спеціальних зовнішніх факторів.