МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Львівського національного університету
імені Івана Франка

Голова Вченої ради

_____ В. П. Мельник

протокол № 5774 від «31» 12 2022 р.

Освітня програма вводиться в дію з
01.09.2023 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
“ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ”

Другого (магістерського) рівня вищої освіти

За спеціальністю: 125 Кібербезпека та захист інформації

Галузі знань: 12 Інформаційні технології

Львів 2022

Розроблено робочою групою спеціальності 125 «Кібербезпека та захист інформації» у складі:

1. **Моркун Наталя Володимирівна** (гарант освітньої програми) д-р.тех.наук, професор, професор кафедри кібербезпеки;
2. **Венгерський Петро Сергійович** д-р.фіз.-мат.наук, лоцент, в.о. завідувача кафедри кібербезпеки;
3. **Пелешко Дмитро Дмитрович** д-р.тех.наук, професор, професор кафедри кібербезпеки;
4. **Винокурова Олена Анатоліївна** д-р.тех.наук, професор, професор кафедри кібербезпеки;
5. **Щербина Юрій Миколайович**, професор кафедри дискретного аналізу та інтелектуальних систем, канд.фіз.-мат.н., доцент;
6. **Журавчак Даниїл** - Lead of Department Operational Intelligence EPAM Systems;
7. **Лесик Володимир -** здобувач четвертого року навчання бакалаврату

Рецензії-відгуки стейкхолдерів:
1. Жук Сергій - Управління державного спеціального зв'язку у Львівській області;
2. Євсеєв Сергій - Національний технічний університет «Харківський політехнічний інститут»;
3. Ігор Кантор – ТОВ "TerraSec"

КЕРІВНИК ПРОЕКТНОЇ ГРУПИ

(гарант освітньої програми) _____ Н.А. Моркун

(підпис) (ініціали, прізвище)

УХВАЛЕНО

на засіданні Вченої ради факультету прикладної математики та інформатики

Протокол № 17 від 16 листопада 2022 року

Голова вченої ради _____ І. І. Дияк

(підпис) (ініціали, прізвище)

Декан
факультету прикладної
математики та інформатики _____ І.І.Дияк

(підпис) (ініціали, прізвище)

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ
“ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ ”
ЗА СПЕЦІАЛЬНІСТЮ 125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Львівський національний університет імені Івана Франка, факультет прикладної математики та інформатики, кафедра кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Технології штучного інтелекту в кібербезпеці
Тип диплому та обсяг освітньої програми	Диплом магістра. Одиничний, 90 кредитів ECTS, термін навчання 1 рік 4 місяці
Наявність акредитації	-
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF LLL – 7 рівень,
Передумови	Наявність ОС бакалавра Умови вступу визначаються «Правилами прийому до Львівського національного університету імені Івана Франка».
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступного планового оновлення програми.
Інтернет-адреса постійного розміщення опису освітньої програми	http://cybersecurity.lnu.edu.ua/
2 – Мета освітньої програми	
Підготовка висококваліфікованих та конкурентоспроможних фахівців на ринку праці, які володіють компетентностями необхідними для ефективного розв’язування практичних проблем у сфері захисту інформації; розробці, використанні та впровадженні сучасних технологій штучного інтелекту для забезпечення інформаційної та кібербезпеки. Особлива увага приділена забезпеченню балансу між можливостями штучного інтелекту та соціальними, етичними та правовими аспектами, що виникають при їх практичному застосуванні.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань - 12 «Інформаційні технології». Спеціальність – 125 «Кібербезпека та захист інформації». **Об’єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об’єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології;

	– інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки . **Цілі навчання:** підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, методи та алгоритми машинного навчання, криптографічного та технічного захисту інформації, теорія ризиків, математичної статистики та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** 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. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об’єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна програма підготовки магістра має прикладну орієнтацію, акцентовану на здобуття студентами знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності, а також на розвиток здатності розв’язувати складні задачі і проблеми в галузі захисту інформації з використанням можливостей штучного інтелекту.

Основний фокус освітньої програми	Спеціальна освіта в галузі 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації. Фокус освітньо-професійної програми націлений на підготовку фахівців у сфері інформаційної та кібербезпеки, здатних застосовувати технології, методи, інструменти штучного інтелекту та інформаційної безпеки, що використовуються для моніторингу та аналізу подій безпеки, виявлення аномалій та прискорення виявлення загроз, з акцентом на етичні та правові аспекти використання штучного інтелекту. Ключові слова: кібербезпека, інформаційна безпека, машинне навчання, нейронні мережі, штучний інтелект, захист персональних даних, захист інформації, захист від несанкціонованого доступу.
Особливості та відмінності	Унікальність ОПП забезпечується поєднанням сильних сторін ШІ і людського інтелекту для вирішення складних задач кібербезпеки. В умовах швидкого розвитку кібератак і стрімкого збільшення кількості пристроїв, ШІ допоможе автоматизувати процес виявлення загроз і реагувати більш ефективно, ніж звичайні програмні або ручні методи. Здобувачі вчаться використовувати методи інтелектуальної автоматизації, штучного інтелекту для виявлення поведінкових аномалій і усунення загроз майже в режимі реального часу. Системи кібербезпеки на основі штучного інтелекту можуть надати найновіші знання про глобальні та галузеві загрози, щоб краще формулювати життєво важливі рішення щодо визначення пріоритетів ризиків, спрямувати реагування на інциденти та виявити атаки шкідливого програмного забезпечення ще до того, як вони стануть помітними. Унікальність даної ОПП орієнтована на підготовку фахівця, здатного вирішувати завдання, які визначаються міжнародними стандартами кібербезпеки, зокрема ISO/IEC 27001 / 27002, ISO/IEC 15408, IEC 62443, ISO/SAE 21434, NIST SP 800-53, NIST CSF, COBIT, CIS Controls, HITRUST Common Security Framework та General Data Protection Regulation (GDPR).
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до Державного класифікатору професій ДК 003:2010 (із змінами і доповненнями) випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 2139.2 Фахівець з кібердосліджень та розробок систем безпеки 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки) 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване, проблемно-орієнтоване навчання, що проводиться у вигляді: лекцій, мультимедійних лекцій, семінарів, практичних занять, лабораторних робіт, консультацій з викладачами, виконанням курсових робіт і проектів та підготовки кваліфікаційної (магістерської) роботи, самостійного навчання з використанням підручників, навчальних посібників, конспектів

	лекцій, методичних рекомендацій, періодичних наукових видань, дистанційних навчальних курсів та мережі Internet. Лекційні заняття мають інтерактивний науково-пізнавальний характер. Практичні проводяться в малих групах, поширеними є розгляд кейс-методів, ситуаційні завдання, ділові ігри, підготовка презентацій з використанням сучасних професійних програмних засобів.
Оцінювання	Оцінювання здійснюється за 100-бальною шкалою ECTS (A, B, C, D, E, FX) та національною шкалою («відмінно», «добре», «задовільно», «незадовільно»); для недиференційованих заліків – за вербальною шкалою («зараховано», «не зараховано»). Поточний контроль – усне та письмове опитування, оцінка роботи в малих групах, тестування, захист індивідуальних завдань. Підсумковий контроль – екзамени та заліки з урахуванням накопичених балів поточного контролю. Атестація – підготовка та захист кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Здатність проводити дослідження на відповідному рівні. ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові) компетентності спеціальності	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно

	встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. *КФ11. Здатність використовувати технології та засоби штучного інтелекту для виявлення вразливостей та захисту інформаційних ресурсів об'єктів інформаційної діяльності та критичної інфраструктури, швидкого аналізу аномалій, загроз та реагування на них.*
7 - Програмні результати навчання	
Програмні результати навчання (ПРН)	РН1. 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 інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі, зокрема з вкиористанням технологій, методів, інструментів штучного інтелекту. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення, та штучного інтелекту. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання

	спеціалізованого програмного забезпечення та методів інтелектуальної автоматизації, штучного інтелекту і машинного навчання для виявлення поведінкових аномалій і усунення загроз. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки та штучного інтелекту. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки, штучного інтелекту і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки та штучного інтелекту. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту,

	розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки та штучного інтелекту з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання, методи та інструменти штучного інтелекту для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. *РН24. Ідентифікувати, виявляти та впроваджувати адаптивні інтелектуальні системи для виявлення вразливостей, розпізнавання аномальних активностей та ефективного реагування на кібератаки; розробляти та вдосконалювати моделі машинного навчання, які сприяють підвищенню рівня кібербезпеки, забезпечуючи надійний захист цифрових систем та даних від потенційних загроз.*
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація програми забезпечується висококваліфікованими науково-педагогічними працівниками, з науковими ступенями та вченими званнями. Всі викладачі що забезпечують освітньо-професійну програму «Технології штучного інтелекту в кібербезпеці» мають великий досвід навчально-методичної, науково-дослідної роботи та підтверджений рівень кваліфікації відповідно до спеціальності згідно ліцензійних умов. Також у викладанні беруть участь працівники ІТ-фірм з практичним досвідом у цьому напрямі, більше 10% викладачів проходять спеціалізовані курси в мережній Академії CISCO та навчальній платформі RangeForce. З метою підвищення фахового рівня усі науково-педагогічні працівники не менше ніж один раз на п'ять років проходять стажування в закладах вищої освіти та ІТ підприємствах Львова.
Матеріально-технічне забезпечення	Використання сучасного програмного забезпечення провідних ІТ компаній у галузі компютерних технологій та інформаційної безпеки а також стандартизованих вітчизняних апаратно-програмних засобів захисту інформації. Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребам. Для проведення практичних і лабораторних робіт, інформаційного пошуку та обробки результатів наявні спеціалізовані лабораторії факультету з необхідним апаратним та програмним забезпеченням та відкритим доступом до Інтернетмережі. Функціонує 8 комп'ютерних класів,

	де встановлено мультимедійну техніку, інтернет, програмне забезпечення, дві навчально-комп'ютерні лабораторії зі спеціалізованим програмним та апаратним забезпеченням (мережеве обладнання Cisco, Ajax та HUAWEI), а також навчальні платформи професійного спрямування RangeForce та CISCO Networking Academy LNU.
Інформаційне та навчально-методичне забезпечення	Офіційний сайт ЛНУ ім. Івана Франка https://lnu.edu.ua /, факультету прикладної математики https://ami.lnu.edu.ua /. Навчально-методичне забезпечення: навчальний план, силабуси навчальних дисциплін, навчальні і робочі плани, використання в освітньому процесі електронних освітніх ресурсів, технологій змішаного або дистанційного навчання, системи електронного навчання Moodle, наукова бібліотека https://www.lnulibrary.lviv.ua / , читальні зали; пакет MS Office 365; корпоративна пошта. Інформаційна система "Dekanat". Доступ до наукометричних баз даних Scopus, Web of Science.
9 – Академічна мобільність	
Національна кредитна мобільність	Індивідуальна академічна мобільність реалізується у рамках міжуніверситетських договорів про встановлення науково-освітянських відносин для задоволення потреб розвитку освіти і науки.
Міжнародна кредит-на мобільність	На основі двосторонніх договорів між Львівським національним університетом ім. Івана Франка та закладами вищої освіти зарубіжних країн. Кафедра кібербезпеки здійснює реалізацію проектів: - ERASMUS-EDU-2023-EMJM-DESIGN 101128245 - Development of Joint Master programme «Artificial Intelligence for Cybersecurity» / AI4CyberSec **Мета проєкту:** Основною ідеєю проекту є розробка та впровадження інноваційної моделі підготовки висококваліфікованих спеціалістів з кібербезпеки на основі дослідження та використання останніх наукових досягнень у галузі штучного інтелекту, інтерактивних та змішаних методів навчання. Технологія MOOC, просування глобальних гуманітарних цінностей та співпраця всіх академічних учасників, громадських організацій та органів влади. Спільна магістерська програма сприятиме не тільки взаємному обміну кращими практиками та досвідом в організації освітнього процесу, а й сприяє знайомству, розумінню та збагаченню культурних цінностей партнерів. - ERASMUS-EDU-2023-CBHE-STRAND-2, ID: 101129022 (: 01.11.2023 – 31.10.2026 - « NEXT – Digital Transformations for Supporting Next-Generation Labour » **Мета проекту** – скоротити існуючий розрив між стрімкими темпами цифрової трансформації та підготовкою фахівців з різних сфер, особливо тих, які не пов'язані з IT. Справа в тому, що наразі вищезазначені спеціалісти недостатньо навчені для ефективної роботи з цифровими технологіями та інструментами, а також для розуміння можливих підводних каменів у їх використанні, включаючи проблеми психічного здоров'я та правові питання. **NEXT** сприятиме процесу набуття цифрових та м'яких навичок майбутніми спеціалістами відповідно до сучасних

	вимог «цифрового» ринку праці в Україні з перспективою поширення результатів проєкту та найкращих практик, розроблених у рамках проєкту.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти можливе, після вивчення курсу української мови .

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ІХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент освітньої програми

Код н/д	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
1.Обов'язкові компоненти освітньої програми			
1.1.Цикл загальної підготовки			
ОК1	Іноземна мова за професійним спрямуванням	6	залік,екзамени
ОК2	Соціальні, етичні та правові аспекти штучного інтелекту та кібербезпеки	3	екзамен
1.2. Цикл професійної та практичної підготовки			
ОК3	Безпека систем автоматизації та Інтернету речей	3	екзамен
ОК4	Безпечна розробка та тестування програмного забезпечення	4	екзамен
ОК5	Виробнича практика	9	диф. залік
ОК6	Виробнича (переддипломна) практика	6	диф. залік
ОК7	Кваліфікаційна (магістерська) робота	9	захист в ЕК
Освітньо-професійна програма "Технології штучного інтелекту в кібербезпеці"			
ОК8	Методи штучного інтелекту для кібербезпеки	5	екзамен
ОК9	Управління проєктами забезпечення інформаційної безпеки	3	екзамен
ОК10	Курсова робота	3	диф. залік
ОК11	Науковий семінар	3	залік
ОК12	Машинне навчання та адаптивний інтелект	6	екзамен
ОК13	Інтелектуальні системи аналізу та захисту даних	6	екзамен
Загальний обсяг обов'язкових компонент		**66**	
2. Вибіркові навчальні дисципліни			
2.1.1 Цикл загальної підготовки			
ВД 1	Дисципліни вільного вибору	3	залік
2.1.2. Цикл професійної та практичної підготовки			
ВД 2	Моделі машинного навчання для виявлення аномалій та шахрайства Інтелектуальний аналіз даних для кібербезпеки Практичне застосування методів машинного навчання та інтелектуального аналізу даних	4	залік
ВД 3	Криптографія та безпечний комунікаційний зв'язок Мережева безпека та виявлення вторгнень Технології аналізу кібератак	4,5	залік
ВД 4	Хмарна безпека та віртуалізація Технологія Blockchain для кібербезпеки Аналіз шкідливого програмного забезпечення та розвідка загроз	3,5	залік
ВД 5	Технології віртуальної реальності Системна інтеграція технологій безпеки	3	залік

Код н/д	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
	Технології моделювання систем безпеки		
ВД 6	Конфіденційність та етика в ШІ для кібербезпеки	3	залік
	Етичне тестування на злом і проникнення		
	Управлінні ризиками кібербезпеки		
ВД 7	Операції з безпеки та реагування на інциденти	3	залік
	Цифрова криміналістика та розслідування інцидентів		
	Законодавство та політика у сфері кібербезпеки		
Загальний обсяг вибіркових компонент		**24**	залік
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

* - можливість вибору дисциплін з інших освітніх програм, за умови співпадіння кредитів.

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВІЩОЇ ОСВІТИ

Атестація випускників освітньо-професійної програми „Технології штучного інтелекту в кібербезпеці» спеціальності 125 «Кібербезпека та захист інформації» проводиться у формі захисту кваліфікаційної роботи та завершується видачою документу встановленого зразка про присудження йому ступеня вищої освіти **Магістр з кібербезпеки та захисту інформації**.

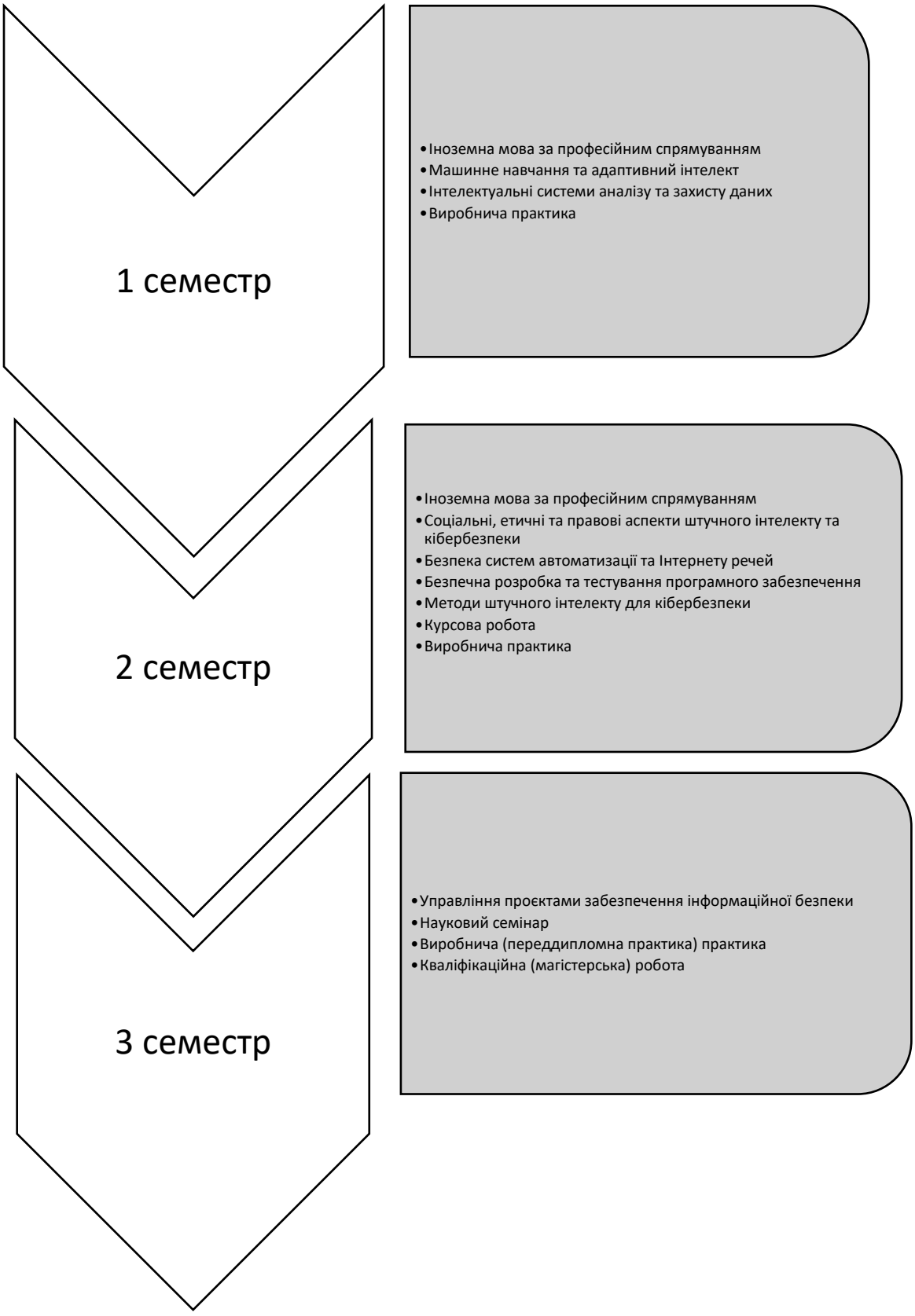
Кваліфікаційна робота має розв’язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Кваліфікаційна робота має бути розміщена на офіційному сайті (у репозиторії) Львівського національного університету ім. Івана Франка.

Атестація здійснюється відкрито і публічно.

Структурно-логічна схема освітньої програми



4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Таблиця 4.1 Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	**ОК 2**	**ОК3**	**ОК 4**	**ОК 5**	**ОК 6**	**ОК 7**	**ОК 8**	**ОК 9**	**ОК 10**	**ОК 11**	**ОК 12**	**ОК 13**
ЗК 1	+	+		+	+	+	+	+	+	+			+
ЗК 2	+	+	+	+	+	+	+	+		+	+	+	+
ЗК 3	+	+			+	+	+	+	+	+		+	+
ЗК 4	+				+	+	+	+	+	+	+	+	+
ЗК 5	+	+		+	+	+			+				
КФ 1		+		+	+	+	+	+		+	+	+	+
КФ 2		+	+		+	+	+		+	+	+		+
КФ 3					+		+	+		+	+	+	+
КФ 4	+		+		+		+						
КФ 5			+		+		+	+					
КФ 6			+	+				+					
КФ 7	+	+		+	+			+		+			
КФ 8					+					+			+
КФ 9		+	+		+								
КФ 10	+	+			+	+	+		+		+		
КФ 11						+	+	+				+	+

Таблиця 4.2 Матриця забезпечення програмних результатів навчання (РН) відповідними програмних компонентами освітньої програми

	ОК 1	**ОК 2**	**ОК 3**	**ОК 4**	**ОК 5**	**ОК 6**	**ОК 7**	**ОК 8**	**ОК 9**	**ОК 10**	**ОК 11**	**ОК 12**	**ОК 13**
РН 1	+				+	+	+			+	+		
РН 2		+	+				+		+	+	+		
РН 3					+	+	+			+	+		
РН 4				+	+	+	+	+		+		+	+
РН 5						+	+		+		+		
РН 6			+		+				+				
РН 7	+	+		+	+				+		+		
РН 8			+	+					+				
РН 9			+						+				
РН 10			+			+			+				
РН 11			+	+	+				+				
РН 12				+					+			+	+
РН 13					+			+					
РН 14					+				+				
РН 15	+	+					+				+		
РН 16		+	+					+					
РН 17	+	+			+	+	+			+	+		
РН 18		+							+				
РН 19		+		+		+	+			+		+	+
РН 20	+	+					+	+					
РН 21			+				+	+					
РН 22							+	+		+	+		
РН 23			+	+			+					+	+
РН 24						+	+	+		+		+	+