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 № ____ від «___» _____2022 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
“ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ”

Другого рівня вищої освіти

За спеціальністю: **125 Кібербезпека та захист інформації**

Галузі знань: **12 Інформаційні технології**

Кваліфікація: **Магістр з кібербезпеки**

Освітня програма вводиться в дію з _____2023р.

Ректор _____ В. П. Мельник

наказ № ___ від «___» _____2022 р.

м. Львів, 2022 рік

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.

КЕРІВНИК ПРОЕКТНОЇ ГРУПИ

(гарант освітньої програми) _____ Н.В. Моркун

(підпис) (ініціали, прізвище)

УХВАЛЕНО

на засіданні Вченої ради факультету прикладної математики та інформатики

Протокол №_____ від _____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	Другий (магістерський) Магістр з кібербезпеки
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	Первинна акредитація
Цикл/рівень	НРК – 7 рівень, FQ-EHEA – другий цикл, EQF LLL – 7 рівень,
Передумови	Наявність ступеня бакалавра (або освітньо-кваліфікаційного рівня спеціаліста). Умови вступу визначаються «Правилами прийому до Львівського національного університету імені Івана Франка».
Мова(и) викладання	Українська
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми.
Інтернет-адреса постійного розміщення опису освітньої програми	http://cybersecurity.lnu.edu.ua/
2 – Мета освітньої програми	
Метою навчання та діяльності є: підготовка фахівців, здатних до комплексного розв’язання складних задач і проблем кібербезпеки з використанням загальних методів та інструментів машинного навчання для посилення передових практик кібербезпеки і захисту критичної інфраструктури, виявлення кіберзагроз, шкідливого програмного забезпечення та шахрайства. Особлива увага буде приділена взаємозв'язку галузей (тобто методам штучного інтелекту, що підтримують кібербезпеку та методам кібербезпеки, що забезпечують безпеку штучного інтелекту), а також соціальним, етичним та правовим аспектам, що виникають при їх практичному застосуванні.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань - 12 «Інформаційні технології». Спеціальність – 125 «Кібербезпека». **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 . **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. Інструменти штучного інтелекту, машинного навчання, глибокого навчання та кібербезпеки для виявлення шкідливого програмного забезпечення, шахрайства та вторгнень. 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 з орієнтацією на практичне використання ключових концепцій обробки інцидентів, пошуку кіберзагроз та цифрових розслідувань, а також детальним аналізом реальних кейсів, з великою складовою взаємодії з ІТ-компаніями та представниками роботодавців.
Основний фокус	Основний фокус освітньо-професійної програми зроблений

освітньої програми	на формуванні фахівця, здатного до застосування технологій, методів, інструментів штучного інтелекту та інформаційної безпеки, що використовуються при розробці програмного забезпечення, баз даних та знань, мережевих додатків та Інтернет-сервісів для захисту цифрових активів організації та критичної інфраструктури; використання проактивного машинного навчання для посилення захисту від нових загроз, які традиційні методи не можуть виявити. Ключові слова: інформаційна безпека, кібербезпека, штучний інтелект, кіберзагрози, шахрайства, математичне моделювання, проектування, наукові дослідження.
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, що відбувається сьогодні, ШІ та машинне навчання можуть допомогти автоматизувати процес виявлення загроз і реагувати більш ефективно, ніж звичайні програмні або ручні методи. Випускники ОПП вчаться використовувати методи інтелектуальної автоматизації, штучного інтелекту і машинного навчання 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. Одним з пріоритетів даної ОПП є орієнтація 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	Магістр з кібербезпеки з акцентом на штучний інтелект готує фахівців для роботи на відповідальних посадах у державному та приватному секторах, які займаються аналізом, управлінням, експлуатацією або захистом критично важливих комп'ютерних систем, інформації, мереж, інфраструктур та мереж зв'язку. Випускники освітнього ступеня магістра в галузі штучного інтелекту та кібербезпеки зможуть виконувати професійні ролі в різних секторах, таких як індустрія програмного забезпечення, послуги в галузі ІТ та ІКТ, державне управління, охорона здоров'я, наукові дослідження, навколишнє середовище та територія, культура та культурні цінності, банківська справа та фінанси і інші організації, що використовують складні інформаційні системи. Деякі приклади професійних посад: фахівець зі ШІ, аналітик даних, фахівець із (кібер) безпеки, директор з інформаційної безпеки, фахівець із захисту даних, менеджер із безпеки ІКТ, етичний хакер, фахівець з етики автоматизації, а також інші класичніші посади для випускника в галузі кібербезпеки, такі як аналітик програмного забезпечення, розробник програмного

	забезпечення, інженер-програміст, менеджер з безпеки, менеджер безпеки бази даних і так далі.
Подальше навчання	Продовження навчання за програмою підготовки доктора філософії на третьому освітньо-науковому рівні вищої освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Студенто-центроване, 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 мережи Internet. Лекційні заняття мають інтерактивний науково-пізнавальний характер. Практичні проводяться в малих групах, поширеними є кейс-метод, ситуаційні завдання, ділові ігри, підготовка презентацій з використанням сучасних професійних програмних засобів.
Оцінювання	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою), шкалою ECTS, національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системами. Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестові завдання в тому числі комп'ютерне тестування, лабораторні звіти, презентації, захист курсових робіт та проектів, звітів з практик, захист кваліфікаційної роботи магістра.
6 – Програмні компетентності	
Інтегральна компетентність	ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної / кібер безпеки 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 методи та засоби штучного інтелекту для захисту інформаційних систем та конфіденційних даних від внутрішніх та зовнішніх загроз, шляхом виявлення потенційних ризиків у програмно-апаратних комплексах, моніторингу, виявлення, розслідування, аналізу та реагування на події безпеки, тим самим зменшуючи ризики в режимі реального часу. КФ12. Здатність плануванти, координувати та здійснювати реалізацію програм інформаційної безпеки, співпрацювати з різними командами для реалізації комплексних програм безпеки, які забезпечують захист від онлайн-загроз, таких як шкідливе програмне забезпечення, фішинг, атаки на відмову в обслуговуванні, інформаційна війна і хакерство. КФ13. Здатність використовувати методи машинного навчання, для відстеження та діагностики подій безпеки, вирішення проблем вразливостей, розробляти потенційні рішення, такі як апаратні та

	програмні засоби, які можуть мінімізувати наслідки порушень. КФ14. Здатність обробляти, аналізувати та зберігати різні типи даних, використовувати аналітику та розвіддані для виявлення та виявлення загроз на ходу, агрегувати дані мережі та додатків, які можуть бути використані в якості еталонів для запобігання майбутнім кібератакам.
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. Впроваджувати та налаштовувати 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. РН25. Ідентифікувати, аналізувати та усувати потенційні вразливості в системах автоматизації та Інтернеті речей, розробляти та впроваджувати ефективні стратегії захисту, а також створювати безпечні архітектури для забезпечення надійності та конфіденційності об'єднаних мереж пристроїв. РН26. Розуміти принципи та методи безпечної розробки програмного забезпечення; виявляти, аналізувати та усувати потенційні вразливості в програмах, розробляти безпечні коди та впроваджувати ефективні практики забезпечення кібербезпеки під час процесу розробки. РН27. Розробляти та впроваджувати ефективні плани заходів для захисту інформації від внутрішніх та зовнішніх загроз, визначати та оцінювати ризики, пов'язані з безпекою даних, та впроваджувати відповідні технічні та організаційні заходи для їх зменшення; ефективно співпрацювати з командами з інформаційної безпеки та керівництвом організацій для забезпечення надійного та стійкого управління інформаційною безпекою на рівні підприємства.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які є штатними співробітниками Львівського національного університету ім. Івана Франка, мають великий досвід навчально-методичної, науково-дослідної роботи та мають підтверджений рівень кваліфікації відповідно до спеціальності згідно ліцензійних умов. Понад 80% науково-педагогічних працівників, задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності 125 «Кібербезпека» мають наукові ступені та вчені звання, також більше 15% у викладанні приймають участь працівники ІТ-фірм з практичним досвідом у цьому напрямі, більше 10% викладачів проходять спеціалізовані курси для отримання сертифікації з курсів.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення за ОПП дозволяє забезпечити освітній процес протягом всього циклу підготовки. Стан приміщень засвідчено санітарно-технічними паспортами, які відповідають діючим нормативним актам. Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає ліцензійним умовам. В університеті в достатній кількості є точки бездротового доступу до мережі Інтернет. Користування Інтернет-мережею безлімітне. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць в гуртожитках відповідає вимогам. Використання сучасного програмного забезпечення провідних компаній у галузі інформаційних технологій та інформаційної безпеки а також стандартизованих вітчизняних апаратно-

	програмних засобів захисту інформації.
Інформаційне та навчально-методичне забезпечення	Використання навчальних класів університету та спеціалізованих лабораторій комп'ютерних фірм для виконання лабораторних та практичних завдань та авторські розробки професорсько-викладацького складу. Інформаційні та навчально-методичні матеріали розміщені на сайті кафедри кібербезпеки (http://cybersecurity.lnu.edu.ua/) та освітньому порталі університету. Наукові, методичні та фахові періодичні видання представлені у науковій бібліотеці університету (https://www.lnulibrary.lviv.ua/). Для проведення методичної роботи при кафедрі функціонує навчально-методичний кабінет з навчальною літературою, комп'ютерами, оргтехнікою та відповідними меблями. На офіційному веб-сайті університету (https://lnu.edu.ua/) розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня / освітньо-наукова / видавнича /атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація).
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 кредитна 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-2021-VIRT-EXCH-NDICI № 101083883: «Development of the Model and Common Information Space of Virtual Exchange Programs / MOVEx» - «Розробка моделі та Єдиного Інформаційного Простору Програм Віртуальних Обмінів» (1.12.2022 – 30.11.2025). MOVEs - це 3-річний проект, спрямований на організацію ефективної Програми віртуальних обмінів як платформи для професійної та міжкультурної взаємодії, обміну досвідом, забезпечення якісних освітніх послуг та створення умов для розвитку навичок співпраці та комунікації молоді, а також розширення доступу до міжнародного навчання для кожного студента, незалежно від його обставин, походження чи здібностей, особливо в умовах обмеженої мобільності студентів та обмежених фінансів. Програма віртуальних обмінів є не лише короткостроковим рішенням проблеми, з якою стикаються сьогодні вищі навчальні заклади України, але й частиною комплексного плану, спрямованого на просування інтернаціоналізації для кожного вищого навчального закладу та кожного студента. Для організації активної взаємодії між підрозділами, що беруть участь у залученні та навчанні студентів в рамках проектів академічної мобільності, буде розроблена модель віртуальних національних та міжнародних програм академічних обмінів, яка складається з взаємопов'язаних

	компонентів: організаційна структура, цифрова підтримка, комунікація та взаємодія. - ERASMUS-EDU-2022-CBHE № 101082928: «Students'Personalised Learning Model, Based on the Virtual Learning Environment of Intellectual Tutoring "Learning with No Limits" / SMART-PL» - «Персоналізована модель навчання студентів на основі віртуального навчального середовища інтелектуального тьюторства "Навчання без обмежень"» (1.01.2023 – 31.12.2025). SMART-PL - це 3-річний проект, орієнтований на впровадження моделі персоналізованого навчання, що базується на віртуальному навчальному середовищі інтелектуального тьюторства "Навчання без обмежень". Інтелектуальне тьюторство - це комплекс засобів навчання: SMART-платформа для віртуального персоналізованого навчання та формувального оцінювання учнів; коворкінг-центр з обладнанням для організації гібридного навчання, що підвищує ефективність освітнього процесу та надає більше можливостей як вчителям, так і учням. "Навчання без обмежень" означає, що вітаються всі студенти - незалежно від віку, особистості, соціально-економічного статусу чи освітніх потреб, незалежно від можливості бути присутнім в аудиторії чи ні. Основоположним принципом проекту є персоніфікований підхід, спрямований на формування висококваліфікованого конкурентоспроможного фахівця, здатного до інноваційної діяльності та володіє навичками безперервного професійного розвитку. Персоналізований підхід характеризується інноваційними методами навчання, покликаними заохочувати співпрацю між студентами та викладачами, підкреслюючи центральну роль студентів у контролі свого навчання. - EU ERASMUS+ «University teachers' certification centres: innovative approach to promotion teaching excellence» (Центри сертифікації викладачів: інноваційні підходи до досконалості викладання - UTTERLY, 619227-EPP-1-2020-1-UA-EPPKA2-CBHE-JP). Терміни виконання -01.01.2021-31.12.2022 рр. Проект передбачає розробку та впровадження нової програми досконалості викладання, включаючи описи навчальних на основі кращих європейських практик та освітніх інновацій для забезпечення досконалості викладання та підвищення якості атестації викладачів університету.
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
Обов'язкові компоненти освітньої програми			
Цикл загальної підготовки			
ОК1	Іноземна мова за професійним спрямуванням	6	екзамен
ОК2	Соціальні, етичні та правові аспекти штучного інтелекту та кібербезпеки	3	екзамен
Цикл професійної підготовки			
ОК3	Проектування систем інформаційної безпеки та/або кібербезпеки	6	екзамен
ОК4	Машинне навчання та адаптивний інтелект для кібербезпеки	5	екзамен
ОК5	Інтелектуальні системи аналізу та захисту даних	6	екзамен
ОК6	Безпека систем автоматизації та Інтернету речей	4	екзамен
ОК7	Безпечна розробка та тестування програмного забезпечення	5	екзамен
ОК8	Управління інформаційною безпекою	3	екзамен
ОК9	Курсова робота	3	кр
ОК10	Науковий семінар	3	залік
ОК11	Практика науково-дослідна	3	диф. залік
ОК12	Виробнича (переддипломна) практика	6	диф. залік
ОК13	Кваліфікаційна (магістерська) робота	9	захист
Загальний обсяг обов'язкових компонент		**62**	
Вибіркові компоненти освітньої програми			
ВК1	Моделі машинного навчання для виявлення аномалій та шахрайства	5	залік
ВК2	Аналітика великих даних для кібербезпеки та розвідки загроз (Big Data Analytics for Cybersecurity & Threat Intelligence)	5	залік
ВК3	Практичне застосування методів машинного навчання та інтелектуального аналізу даних	5	залік
ВК4	Криптографія та безпечний комунікаційний зв'язок	5	залік
ВК5	Мережева безпека та виявлення вторгнень	5	залік
ВК6	Технології аналізу кібератак	5	залік
ВК7	Хмарна безпека та віртуалізація	5	залік
ВК8	Технологія Blockchain для кібербезпеки	5	залік
ВК9	Аналіз шкідливого програмного забезпечення та розвідка загроз	5	залік
ВК10	Технології віртуальної реальності	3	залік
ВК11	Системна інтеграція технологій безпеки	3	залік
ВК12	Технології моделювання систем безпеки	3	залік
ВК13	Конфіденційність та етика в ШІ для кібербезпеки	3	залік

Код н/д	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
ВК14	Управління проєктами забезпечення інформаційної безпеки	3	залік
ВК15	Управління ризиками кібербезпеки	3	залік
ВК16	Операції з безпеки та реагування на інциденти	3	залік
ВК17	Цифрова криміналістика та розслідування інцидентів	3	залік
ВК18	Законодавство та політика у сфері кібербезпеки	3	залік
Загальний обсяг вибіркових компонент		**28**	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» проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачою документу встановленого зразка про присудження йому ступеня вищої освіти магістр зі спеціальності 125 «Кібербезпека» за ОПП „Технології штучного інтелекту в кібербезпеці».

Атестація здійснюється у формі публічного захисту випускної кваліфікаційної роботи.

Випускна кваліфікаційна робота має продемонструвати здатність випускника розв’язувати складні завдання і проблеми в галузі автоматизації на основі досліджень та/або здійснення інновацій за наявності невизначених умов і вимог. Кваліфікаційна робота здобувача підлягає обов’язковій перевірці на академічний плагіат та повинна бути розміщена на сайті Львівського національного університету ім. Івана Франка.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Таблиця 4.1

	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
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 1	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 2	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 3	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 4	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 5	+	+	+	+	+	+	+	+	+	+	+	+	+
СК 1			+		+		+		+	+	+	+	+
СК 2			+					+	+	+	+	+	+
СК 3			+		+			+	+	+	+	+	+
СК 4	+		+					+	+	+	+	+	+
СК 5			+					+	+	+	+	+	+
СК 6			+						+	+	+	+	+
СК 7	+		+					+	+	+	+	+	+
СК 8			+			+	+	+	+	+	+	+	+
СК 9						+		+	+	+	+	+	+
СК 10	+							+	+	+	+	+	+
СК 11				+	+				+	+	+	+	+
СК 12				+	+				+	+	+	+	+
СК 13				+	+				+	+	+	+	+
СК 14				+	+	+	+		+	+	+	+	+