МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ЛЬВІВСЬКА ПОЛІТЕХНІКА»

«ЗАТВЕРДЖУЮ»
Ректор
Національного університету
«Львівська політехніка»
_____ /Юрій БОБАЛО/
«27» 12 2023 р.

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

“Системи технічного захисту інформації, автоматизація її обробки”

другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

Розглянуто та затверджено
на засіданні Вченої ради
Університету
від «28» 12 2023 р.
протокол № 7

Львів 2023 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Рівень вищої освіти	Другий (магістерський)
ГАЛУЗЬ ЗНАНЬ	12 Інформаційні технології
СПЕЦІАЛЬНІСТЬ	125 Кібербезпека та захист інформації
Кваліфікація	Магістр з кібербезпеки та захисту інформації

РОЗРОБЛЕНО І СХВАЛЕНО

Науково-методичною комісією спеціальності 125 Кібербезпека та захист інформації
Протокол № 4
від «17» листопада 2023 р.

Голова НМК спеціальності
_____ Валерій ДУДИКЕВИЧ

ПОГОДЖЕНО

Проректор з науково-педагогічної роботи Національного університету «Львівська політехніка»

_____ Олег ДАВИДЧАК
«22» 12 2023 р.

Начальник Навчально-методичного відділу університету

_____ Василь ТОМ'ЮК
«22» 12 2023 р.

РЕКОМЕНДОВАНО

Науково-методичною радою університету
Протокол № 75
від «21» 12 2023 р.

Голова НМР університету
_____ Анатолій ЗАГОРОДНІЙ

Директор ІКТА

_____ Микола МИКИЙЧУК
«21» листопада 2023 р.

ПЕРЕДМОВА

Розроблено відповідно до Стандарту вищої освіти України другого (магістерського) рівня, галузь знань 12 – Інформаційні технології, спеціальність – 125 Кібербезпека та захист інформації, затвердженого та введеного в дію наказом Міністерства освіти та науки України від 18.03.2021р. №332.

Розроблено проектною групою науково-методичної комісії спеціальності 125 «Кібербезпека та захист інформації» Національного університету "Львівська політехніка" у складі:

Хома В.В.	– д.т.н., проф. каф. ЗІ – гарант освітньо-професійної програми
Опірський І.Р.	– д.т.н., проф., завідувач кафедри ЗІ
Журавель І.М.	– д.т.н., проф., завідувач кафедри БІТ
Дудикевич В.Б.	– д.т.н., проф. каф. ЗІ
Гарасимчук О.І.	– к.т.н., доцент кафедри ЗІ
Ясінський А.А.	– директор Alarm Security
Дзіоба Н.І.	– директор ПП Iron Sec
Глущак О.Р.	– провідний інженер Західного регіонального-навчально-наукового центру захисту інформації
Фігурняк В.Р.	– студент КБСТ-21

Гарант освітньо-професійної програми _____ /Володимир ХОМА/

Проект освітньо-професійної програми обговорений та схвалений на засіданні Вченої ради навчально-наукового інституту комп'ютерних технологій, автоматики та метрології

Протокол № _3_ від «_21_» _листопада_ 2023 р.

Голова Вченої ради ІКТА _____ Микола МИКИЙЧУК
(підпис) (прізвище, ініціали)

Затверджено та надано чинності

Наказом ректора Національного університету «Львівська політехніка»

від «_29_» _грудня_ 2023 р. № 676-1-10

Профіль освітньо-професійної програми "Системи технічного захисту інформації, автоматизація її обробки" магістра зі спеціальності 125 "Кібербезпека та захист інформації"

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	**Національний університет «Львівська політехніка»**, кафедра захисту інформації, Інститут комп'ютерних технологій, автоматики та метрології
Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Назва освітньої програми	Системи технічного захисту інформації, автоматизація її обробки Information Security Systems and Automation of Information Processing
Інтернет-адреса розміщення освітньої програми	https://lpnu.ua/osvita/pro-osvitni-programy/drugyi-riven-vyshchoi-osvity
Обмеження щодо форм навчання	Денна, заочна (дистанційна)
Освітня кваліфікація	Магістр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – Магістр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – Системи технічного захисту інформації, автоматизація її обробки
2 – Мета освітньої програми	
	Надати теоретичні знання та практичні уміння і навички, достатні для успішного виконання професійних обов'язків за спеціальністю 125 «Кібербезпека та захист інформації» та підготувати студентів для подальшого працевлаштування за обраною спеціальністю.
Опис предметної області	**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, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків 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.
Академічні права випускників	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
Обсяг кредитів за Європейською кредитно-трансферною системою	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1,5 роки Диплом магістра, одиничний, 90 кредитів ЄКТС, Мінімум 60% обсягу освітньої програми має бути спрямовано на формування загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених Стандартом вищої освіти. Освітньо-наукова програма магістра обов'язково включає дослідницьку (наукову) компоненту обсягом не менше 30%. Мінімум 15 кредитів ЄКТС має бути призначено для практики. Заклад вищої освіти має право визнати та перезарахувати кредити ЄКТС, отримані за попередньою освітньою програмою підготовки магістра (спеціаліста) за іншою спеціальністю. Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу ОП.
Наявність акредитації	так
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень

Передумови	Наявність ступеня бакалавра
Мова(и) викладання	Українська мова
Основні поняття та їх визначення	У програмі використано основні поняття та їх визначення відповідно до Закону України «Про вищу освіту»
3 - Характеристика освітньої програми	
Орієнтація освітньої програми	Освітньо-професійна програма базується на загальновідомих положеннях та результатах сучасних наукових досліджень з інформаційних технологій, методів управління інформаційною безпекою, безпеки інформаційних та телекомунікаційних систем, систем технічного захисту інформації, автоматизації обробки інформації, правових засад захисту інформації, комп'ютерних мереж, архітектури комп'ютерних систем, теорії та практики криптографічного захисту інформації, адміністрування безпеки комп'ютерних систем та мереж в рамках яких можлива подальша професійна та наукова кар'єра за даними напрямками.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка в області кібербезпеки. ***Ключові слова:*** кібербезпека, безпека інформаційних систем, організація інформаційної безпеки, безпека комп'ютерних мереж, управління інформаційною безпекою, системи технічного захисту інформації, захист інформації, адміністрування систем кібербезпеки.
Особливості програми	
4 – Здатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Робочі місця в державному та приватному у сфері інформаційних технологій, комп'ютерних систем та телекомунікацій, розробка і обслуговування систем інформаційної безпеки, зокрема: спеціаліст по захисту інформації державних та приватних підприємств, професіонал із організації інформаційної безпеки, професіонал із організації захисту інформації з обмеженим доступом, професіонал з режиму секретності, інспектор із організації захисту секретної інформації, менеджер з інформаційної безпеки, професіонал з аудиту мереж передач даних, експерт з безпеки програмного забезпечення; провідний інженер з інформаційної безпеки, професіонал відділу контролю інформаційних ризиків, адміністратор комп'ютерних мереж, професіонал з підтримки інформаційних сервісів, аналітик кібербезпеки.
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	Поєднання лекцій, практичних занять, консультацій, самостійної роботи із розв'язування проблем; виконання проектів, лабораторні роботи, консультації із викладачами, підготовка магістерської кваліфікаційної роботи.
Оцінювання	Екзамени, заліки, лабораторні звіти, усні презентації, поточний контроль, захист курсових проектів (робіт), захист магістерської кваліфікаційної роботи.
6 – Програмні компетентності	

Інтегральна компетентність (ІНТ)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (КЗ)	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності спеціальності (КФ)	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.
Фахові компетентності професійного спрямування (ФКС)	**0201:** ***Системи технічного захисту інформації, автоматизація її обробки*** ФКС 1. Уміння організувати моніторинг стану інформаційної системи та аналізувати порушення інформаційної безпеки. ФКС 2. Здатність обґрунтовувати та реалізовувати систему захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності; ФКС 3. Уміння проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ФКС 4. Уміння обробляти отримані результати, аналізувати і осмислювати їх з урахуванням опублікованих матеріалів; **0202:** ***Системи технічного захисту інформації на об'єктах критичної інфраструктури*** ФКС 5. Уміння здійснювати оцінку відповідності системи захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів; ФКС 6. Уміння аналізувати ризики для оцінки реальних загроз порушення захисту та охорони. ФКС 7. Уміння на основі володіння науковою методологією організовувати процес дослідження у галузі інформаційної безпеки та захисту інформації; ФКС 8. Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.
	7 – Програмні результати навчання
Результати навчання (РН)	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. 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. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. 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. 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 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. 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 з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання 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. **0201:** ***Системи технічного захисту інформації, автоматизація її обробки*** РН24. Володіння типовими підходами та методологіями до проектування та модернізації захищених об'єктів інформаційної діяльності відповідно до нормативних вимог чинних стандартів і технічних умов. **0202:** ***Системи технічного захисту інформації на об'єктах критичної інфраструктури*** РН25. Уміння застосовувати знання технічних характеристик, конструкційних особливостей, призначення і правил експлуатації устаткування та обладнання для вирішення технічних задач спеціальності.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Понад 90% науково-педагогічних працівників, задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності 125 «Кібербезпека та захист інформації» мають наукові ступені та вчені звання, з практичним досвідом роботи > 20 %.
Специфічні характеристики матеріально-технічного забезпечення	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. Використання сучасного обладнання провідних компаній у галузі інформаційних технологій та інформаційної безпеки, зокрема

	Xilinx, Altera, а також стандартизованих вітчизняних апаратно-програмних засобів захисту інформації, центр сертифікації ключів, виробництва «Інституту інформаційних технологій» (м.Харків), а також використання сучасних прикладних програм для ефективного вирішення задач з технічного захисту інформації та автоматизації її обробки.
Специфічні характеристики інформаційно-методичного забезпечення	Використання віртуального навчального середовища Національного університету «Львівська політехніка» та авторських розробок науково-педагогічних працівників.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним університетом «Львівська політехніка» та університетами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Національним університетом «Львівська політехніка» та навчальними закладами країн-партнерів
Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови.

2. Розподіл змісту освітньо-професійної програми за групами компонентів та циклами підготовки

	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	2	3	4	5
1.	Цикл загальної підготовки	3/3,5	3/3,5	6/7
2.	Цикл професійної підготовки	57/63	27/30	84/93
Всього за весь термін навчання		60/66,5	30/33,5	90/100

3. Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
Обов'язкові компоненти спеціальності			
1. Цикл загальної підготовки			
СК1.1.	Іноземна мова професійного спрямування	3	диф. залік
Всього за цикл:		**3**	
2. Цикл професійної підготовки			
СК2.1.	Інтернет речей та його безпека	4	екзамен
СК2.2.	Комплексні системи санкціонованого доступу	4	екзамен

СК2.3.	Комп'ютерні методи аналізу та проектування електронних засобів	4	екзамен
СК2.4.	Гарантоздатність автоматизованих систем	5	екзамен
СК2.5.	Безпека технологій зв'язку	4	диф. залік
СК2.6.	Комплексні системи санкціонованого доступу (КП)	3	диф. залік
СК2.7.	Комп'ютерні методи аналізу та проектування електронних засобів КП	3	диф. залік
СК2.8.	Практика за темою магістерської кваліфікаційної роботи	15	диф. залік
СК2.9.	Виконання магістерської кваліфікаційної роботи	12	диф. залік
СК2.10.	Захист магістерської роботи	3	
Всього за цикл		**57**	
Всього за групу компонентів		**60**	
Вибіркові компоненти освітньо-професійної програми			
Вибіркові блоки компонентів			
1. Цикл загальної підготовки			
Всього:		**3**	
2. Цикл професійної підготовки			
Вибіркові компоненти блоку 0201: Системи технічного захисту інформації та автоматизація її обробки			
ВБ0201.1	Види та засоби технічної розвідки та спеціальні вимірювання	4	екзамен
ВБ0201.2	Методи цифрової обробки сигналів та зображень	4	екзамен
ВБ0201.3	Проектування комплексних систем захисту інформації	4	екзамен
ВБ0201.4	Сучасні методи проектування пристроїв захисту інформації	4	екзамен
ВБ0201.5	Проектування комплексних систем захисту інформації КП	3	диф. залік
ВБ0201.6	Сучасні методи проектування пристроїв захисту інформації КП	3	диф. залік
Вибіркові компоненти блоку 0202: Системи технічного захисту інформації на об'єктах критичної інфраструктури			
ВБ0202.1	Виявлення та ідентифікація сигналів радіозакладних пристроїв	4	екзамен
ВБ0202.2	Теорія захисту інформаційних ресурсів обмеженого доступу	4	екзамен
ВБ0202.3	Тестування комп'ютерних мереж та систем на проникнення	4	екзамен
ВБ0202.4	Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорона державної таємниці	4	екзамен
ВБ0202.5	Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорона державної таємниці КП	3	диф. залік
ВБ202.6.	Тестування комп'ютерних мереж та систем на проникнення КП	3	диф. залік
Всього:		**22**	
Вибіркові компоненти інших освітньо-професійних програми			
Всього:		**5**	
Всього за вибіркові компоненти:		**30**	
Всього зо освітньо-професійну програму:		**90**	

4. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи/проекту	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 у репозитарії філії РСО кафедри захисту інформації. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

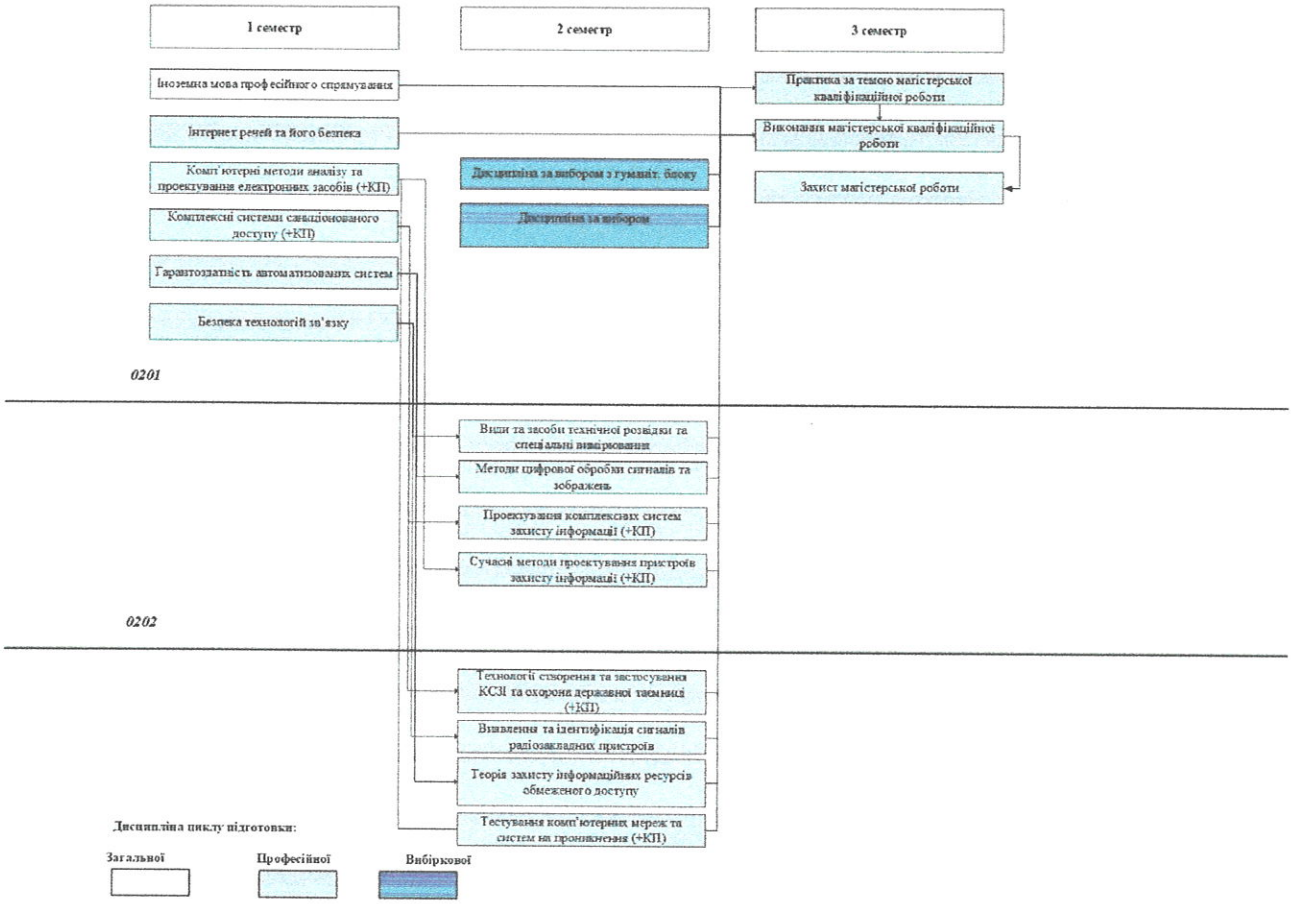
5. Матриця відповідності програмних компетентностей навчальним компонентам

	СК1.1.	СК2.1.	СК2.2.	СК2.3.	СК2.4.	СК2.5.	СК2.6.	СК2.7.	СК2.8.	СК2.9.	СК2.10.	ВБ0301.1.	ВБ0201.2	ВБ0201.3	ВБ0201.4	ВБ0201.5	ВБ0201.6	ВБ0202.1	ВБ0202.2	ВБ0202.3	ВБ0202.4	ВБ0202.5	ВБ0202.6
ІНТ						•			•														
КЗ1						•									•						•		
КЗ 2										•							•						
КЗ 3	•							•					•		•					•			•
КЗ 4											•							•					
КЗ 5	•						•																
КФ1					•															•		•	•
КФ 2			•		•	•																	
КФ 3			•			•		•						•					•				
КФ 4												•					•				•		
КФ 5															•				•				
КФ 6			•			•										•						•	
КФ 7		•		•									•							•			•
КФ 8					•			•			•					•							
КФ 9		•												•					•				
КФ 10		•							•			•									•		
ФКС1																•			•				
ФКС2											•			•					•				
ФКС3							•						•				•			•		•	•
ФКС4				•						•	•			•									
ФКС5					•			•				•					•				•		
ФКС6															•								
ФКС7							•										•						
ФКС8				•						•					•					•		•	•

6. Матриця відповідності програмних результатів навчання навчальним компонентам

	СК1.1.	СК2.1.	СК2.2.	СК2.3.	СК2.4.	СК2.5.	СК2.6.	СК2.7.	СК2.8.	СК2.9.	СК2.10.	ВБ0301.1.	ВБ0201.2	ВБ0201.3	ВБ0201.4	ВБ0201.5	ВБ0201.6	ВБ0202.1	ВБ0202.2	ВБ0202.3	ВБ0202.4	ВБ0202.5	ВБ0202.6
РН1	•				•			•						•					•				
РН2		•								•		•					•				•		
РН3						•		•			•				•				•				
РН4				•												•						•	
РН5									•				•							•			•
РН6				•												•							
РН7			•		•	•		•						•					•				
РН8		•	•			•				•		•									•		
РН9				•				•			•					•			•				
РН10					•			•						•					•				
РН11			•			•			•				•				•				•		•	•
РН12					•								•					•						
РН13		•								•	•					•				•			•
РН14									•					•				•					
РН15							•						•					•					
РН16			•	•		•			•		•					•				•			•
РН17										•				•				•					
РН18					•					•					•						•		
РН19		•				•						•							•				
РН20						•			•						•			•				•	
РН21													•					•					
РН22									•	•										•			•
РН23									•						•			•				•	
РН24																		•				•	
РН25																•			•		•		

Логічно-структурна схема освітньо-професійної програми “Системи технічного захисту інформації, автоматизація її обробки” магістра зі спеціальності 125 “Кібербезпека та захист інформації”



ВИТЯГ
з протоколу №04
засідання кафедри «Захисту інформації»
від 16.11.2023 р.

Присутні: 60 членів кафедри
Відсутні: 8 членів кафедри

СЛУХАЛИ:

Інформацію завідувача кафедри захисту інформації Опірського Івана Романовича щодо необхідності внесення змін до ОПП магістрів «Системи технічного захисту інформації та автоматизація її обробки», «Управління інформаційною безпекою» та «Адміністрування систем кібербезпеки».

ВИСТУПИЛИ:

Гарант ОПП «Адміністрування систем кібербезпеки» проф. Опірський І.Р. надав інформацію щодо необхідності включення дисципліни «Іноземна мова професійного спрямування» відповідно до вимог стандарту «Кібербезпека та захист інформації» відзначених після проходження акредитації. Також за рекомендацією стейкхолдерів та згідно з проведеними нарадами зі студентами винесено пропозицію уточнити назву дисципліни «Міжнародні стандарти із кібербезпеки» на назву «Міжнародні практики з дослідження вразливостей Web-додатків». Також проф. Опірський І.Р. надав пропозиції щодо включення додаткових курсових проєктів у вибірковий блок 0402. "Адміністративний менеджмент у сфері кібербезпеки" з відповідної дисципліни.

З підтримкою змін виступила гарант ОПП магістрів «Управління інформаційною безпекою» професор Микитин Галина Василівна, яка наголосила за доцільність внесення змін у відповідне ОПП з метою аналогічного уточнення назви дисципліни з «Міжнародні стандарти із кібербезпеки» на «Міжнародні практики з дослідження вразливостей Web-додатків». Згідно з проведеними опитуваннями та популяризацією блоку 0302. «Управління інформаційною безпекою» запропоновано додати курсові проєкти з дисциплін «Адміністрування в інформаційних системах» та «Технології створення та застосування КСЗІ з обмеженим доступом» як результат самотійної роботи студентів з вивичення критично важливих для блоку дисциплін.

Також з підтримкою змін виступив гарант ОПП магістрів «Системи технічного

захисту інформації та автоматизація її обробки» проф. Хома В.В., який наголосив на важливості продовження вивчення іноземної мови і запропонував у межах існуючих кредитів додати курсові проєкти у блок 0202. "Системи технічного захисту інформації на об'єктах критичної інфраструктури" з дисциплін «Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорона державної таємниці» та «Тестування комп'ютерних мереж та систем на проникнення» як необхідні складові успішного опанування навичок і застосування їх під час вивчення відповідних дисциплін.

УХВАЛИЛИ:

Затвердити зазначені зміни в освітньо-професійних програмах кафедри захисту інформації «Системи технічного захисту інформації та автоматизація її обробки», «Управління інформаційною безпекою» та «Адміністрування систем кібербезпеки». Розробити нові ОПП згідно наданих рекомендацій та пропозицій гарантів освітніх програм для 2024 року вступу.

Завідувач кафедри ЗІ,
д.т.н., професор Іван ОПІРСЬКИЙ

Секретар кафедри ЗІ,
к.т.н., доцент Ярослав СОВИН