МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Вченою радою Поліського університету
протокол № 9 від 24 квітня 2024 р.

Голова вченої ради
_____ Олег СКИДАН

Освітньо-професійна програма
вводиться в дію з 01 вересня 2024 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»
(Cybersecurity)

другого (магістерського) рівня вищої освіти
за спеціальністю 125 «Кібербезпека та захист інформації»
галузі знань 12 «Інформаційні технології»
Кваліфікація: магістр з кібербезпеки та захисту інформації

Житомир – 2024

ЛИСТ-ПОГОДЖЕННЯ
освітньо-професійної програми

ВНЕСЕНО:
Кафедра комп'ютерних технологій і моделювання систем
протокол № 16 від 23 квітня 2024 р.

Завідувач кафедри
_____ Ольга НИКОЛЮК

ПРОЄКТНА ГРУПА
Керівник проєктної групи (гарант ОПП)
_____ Катерина МОЛОДЕЦЬКА

Члени проєктної групи
_____ Сергій ВЕРЕТЮК
_____ Андрій ЛАПІН

ПОГОДЖЕНО
Навчально-методична комісія факультету інформаційних технологій, обліку та фінансів
протокол № 5 від "24" 04 2024 р.

Голова навчально-методичної комісії
_____ Ольга НИКОЛЮК

ПОГОДЖЕНО
Вчена рада факультету інформаційних технологій, обліку та фінансів
протокол № 8 від "24" 04 2024 р.

Голова вченої ради факультету
_____ Олександр КОВАЛЬЧУК

ПОГОДЖЕНО
Навчально-науковий центр організації освітнього процесу

Керівник ННЦ організації освітнього процесу
_____ Тетяна УСЮК

ПОГОДЖЕНО
Навчально-науковий центр забезпечення якості освіти

Керівник ННЦ забезпечення якості освіти
_____ Наталія СТЕПАНЕНКО

ПЕРЕДМОВА

Освітньо-професійна програма «Кібербезпека» (Cybersecurity) розроблена на основі Стандарту вищої освіти України другого (магістерського) рівня зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології», затвердженого наказом Міністерства освіти і науки України від 18.03.2021 року № 332 (до введення в дію нового за спеціальністю 125 «Кібербезпека та захист інформації»).

Розроблено проєктною групою у складі:

Прізвище, ім'я та по батькові	**Науковий ступінь, шифр та назва наукової спеціальності**	**Вчене звання (за кафедрою / спеціальністю)**	**Посада та назва підрозділу (за основним місцем роботи)**
Керівник проєктної групи (гарант ОПП)			
МОЛОДЕЦЬКА Катерина Валеріївна	Доктор технічних наук, 21.05.01 – Інформаційна безпека держави	Професор кафедри комп'ютерних технологій і моделювання систем	Керівник навчально-наукового центру інформаційних технологій
Члени проєктної групи			
ВЕРЕТЮК Сергій Михайлович	Кандидат технічних наук, 05.13.06 – Інформаційні технології	–	Старший викладач кафедри комп'ютерних технологій і моделювання систем
ЛАПІН Андрій Валерійович	Кандидат економічних наук, 08.00.03 – управління національним господарством	Доцент кафедри комп'ютерних технологій і моделювання систем	Доцент кафедри комп'ютерних технологій і моделювання систем

Зовнішні стейкхолдери – рецензенти освітньо-професійної програми:

Прізвище, ім'я та по батькові	**Місце роботи, посада, науковий ступінь та вчене звання (за наявності)**
КОРЧЕНКО Олександр Григорович	Національний авіаційний університет, завідувач кафедри безпеки інформаційних технологій, Заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, доктор технічних наук (05.13.21–Системи захисту інформації), професор
ПАРХУЦЬ Любомир Теодорович	Національний університет «Львівська Політехніка», професор кафедри захисту інформації, доктор технічних наук (05.13.21 – Системи захисту інформації), професор, секретар підкомісії НМК (7) НМР МОН України
ГАВРИЛЕНКО Олексій Вадимович	Адміністрація Державної служби спеціального зв'язку та захисту інформації України, начальник управління Департаменту захисту інформації, кандидат технічних наук (за згодою)

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1.1. Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Поліський національний університет Кафедра комп'ютерних технологій і моделювання систем
Офіційна назва освітньої програми	Кібербезпека
Ступень вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Назва кваліфікації в дипломі	Ступінь вищої освіти – Магістр Спеціальність – 125 Кібербезпека та захист інформації Магістр з кібербезпеки та захисту інформації
Форма навчання	Денна
Наявність акредитації	Сертифікат про акредитацію ОП № 6749 дійсний до 01.07.2029
Цикл/рівень вищої освіти	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Тип диплома, обсяг та термін навчання	Диплом магістра, одиничний, 90 кредитів ЄКТС, 1 рік 4 місяці
Передумови	Наявність диплому освітнього рівня «бакалавр». Вступники на основі НРК 6 або НРК 7 на підставі складених ЄВІ (2023 або 2024 років) та ЄДКІ (2024 року).
Термін дії освітньої програми	до 31.12.2025
Мова(-и) викладання	Українська
Інтернет-адреса постійного розміщення опису освітньої програми	https://polissiauniver.edu.ua
1.2. Мета освітньої програми	
Підготовка конкурентоспроможних фахівців, затребуваних на загальнодержавному та регіональному ринках праці, здатних розв'язувати складні задачі дослідницького та/або інноваційного характеру на основі застосування сучасних технологій, методів, моделей та засобів забезпечення інформаційної безпеки, кібербезпеки та/або захисту інформації.	

1.3. Характеристика освітньої програми	
Предметна область освітньої програми	**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.
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 напрямами.
Основний фокус освітньої програми	Вища освіта у галузі інформаційних технологій з поглибленою спеціалізованою підготовкою у сфері забезпечення інформаційної та кібербезпеки, зокрема, безпеки інформаційних систем, захисту систем електронних комунікацій (мережі зв'язку, системи передачі даних, мережі Інтернету речей, центри обробки даних); безпеки соціальних інтернет-сервісів; кіберзахисту об'єктів критичної інфраструктури; вдосконаленню, розробленню та провадженню систем управління інформаційною безпекою, в т.ч. із застосуванням методів моделювання безпекових процесів, методів аналізу великих даних, методів захисту інформації та аналізу інцидентів. Ключові слова: кібербезпека, інформаційна безпека, безпека інформаційних систем, захист інформації, системи технічного та криптографічного захисту інформації, адміністрування систем кібербезпеки.

Унікальність освітньої програми	Формування у здобувачів вищої освіти практичних навичок дослідження безпекових процесів із застосуванням методів моделювання для розв'язання складних задач у сфері забезпечення інформаційної та кібербезпеки із фокусуванням уваги на забезпечення безпеки соціальних інтернет-сервісів.
1.4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Робочі місця в державному та приватному секторі у сфері безпеки інформаційних технологій, захисту комп'ютерних систем та мереж, організації захисту інформації, інформаційної та кібербезпеки. Зокрема, здобувачі вищої освіти, які здобули освіту за даною ОПП, можуть займати посади, згідно до Національного класифікатору професій ДК 003:2010 (із змінами), зокрема: – розробник систем захисту інформації; – аналітик загроз безпеки; – фахівець криптографічного захисту інформації; – фахівець реагування на інциденти кібербезпеки; – фахівець підтримки інфраструктури кіберзахисту; – фахівець з технічного захисту інформації; – фахівець з тестування систем захисту інформації.
Академічні права випускників	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
1.5. Викладання та оцінювання	
Викладання та навчання	Лекції, лабораторні роботи, семінари, практичні заняття, самостійна робота, консультації, заліки, іспити, практики, курсова робота (проєкт), підготовка кваліфікаційної роботи магістра.
Оцінювання	Оцінювання академічних успіхів здобувачів здійснюється за 100-бальною шкалою з обов'язковим переведенням оцінок до національної шкали.
1.6. Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

	ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності (ФК)	ФК1. 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. ФК2. 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. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. ФК4. 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. ФК5. 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. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК7. 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. ФК8. 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. ФК9. 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. ФК10. 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. ФК11. Здатність проводити аналіз, дослідження та моделювання процесів забезпечення інформаційної безпеки соціальних інтернет-сервісів. ФК12. Здатність до критичного мислення; керування власними пізнавальними процесами, самокорекції.

1.7. Програмні 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.

РН24. Аналізувати, досліджувати та моделювати процеси забезпечення інформаційної безпеки соціальних інтернет-сервісів.

РН25. Самостійно приймати усвідомлені, неупереджені рішення застосовуючи принципи критичного мислення; розвивати усвідомлення та розуміння власних процесів мислення, використовувати певні стратегії для навчання чи вирішення проблем; активно керувати власними когнітивними процесами у ситуаціях морального вибору; виявляти ознаки маніпулятивного впливу.

1.8. Академічна мобільність

Національна академічна мобільність	На основі двосторонніх договорів між Поліським національним університетом та іншими ЗВО України.
Міжнародна академічна мобільність	Закордонні ЗВО, з якими укладені договори та налагоджена співпраця.

1.9. Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Обсяг освітньо-професійної програми – 90 кредитів ЄКТС;

Мінімум 60% обсягу освітньої програми має бути спрямовано на формування загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених Стандартом вищої освіти.

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 освітньої програми.

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

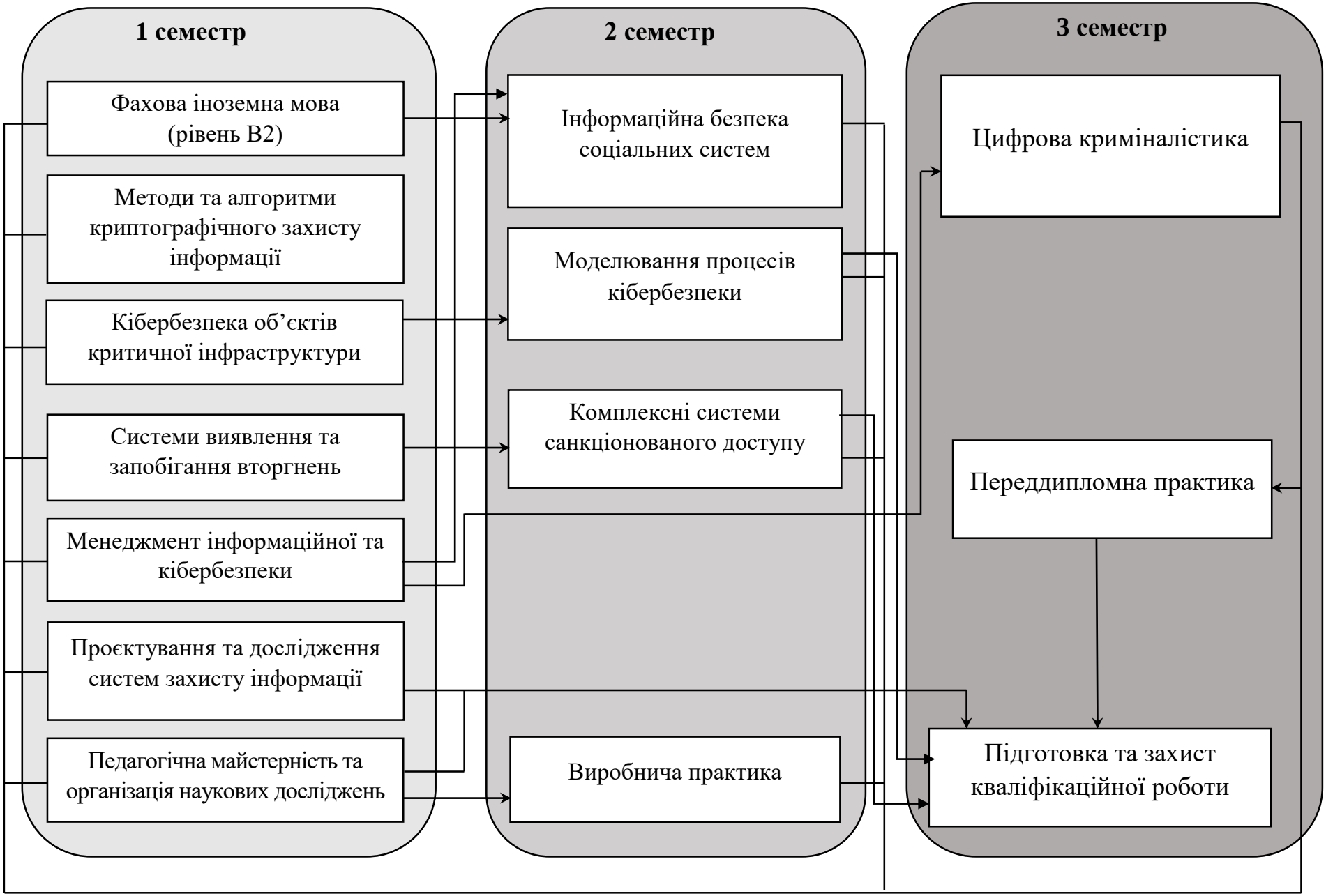
2.1. Перелік компонент освітньо-професійної програми (ОПП)

Код компоненти	Компоненти освітньо-професійної програми	Кількість кредитів ЄКТС	Форма підсумкового контролю
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
Цикл загальної підготовки			
ОК1	Педагогічна майстерність та організація наукових досліджень	4,0	Залік
ОК2	Фахова іноземна мова	5,0	Екзамен
Всього за цикл:		*9,0*	
Цикл професійної підготовки			
ОК3	Методи та алгоритми криптографічного захисту інформації	4,0	Екзамен
ОК4	Кібербезпека об'єктів критичної інфраструктури	4,0	Екзамен
ОК5	Інформаційна безпека соціальних систем	4,0	Екзамен
ОК6	Комплексні системи санкціонованого доступу	4,0	Екзамен
ОК7	Системи виявлення та запобігання вторгнень	4,0	Залік
ОК8	Менеджмент інформаційної та кібербезпеки	4,0	Залік
ОК9	Проєктування та дослідження систем захисту інформації	5,0	Екзамен
ОК10	Моделювання процесів кібербезпеки	5,0	Екзамен, курсова робота
ОК11	Цифрова криміналістика	4,0	Залік
ОК12	Виробнича практика	9,0	Захист звіту
ОК13	Переддипломна практика	6,0	Захист звіту
ОК14	Підготовка та захист кваліфікаційної роботи	4,0	Захист
Всього за цикл:		*57,0*	
Загальний обсяг обов'язкових компонент		**66,0**	
ВИБІРКОВІ КОМПОНЕНТИ			
ВК1	Вибіркова дисципліна	4,0	Залік
ВК2	Вибіркова дисципліна	4,0	Залік
ВК3	Вибіркова дисципліна	4,0	Залік
ВК4	Вибіркова дисципліна	4,0	Залік
ВК5	Вибіркова дисципліна	4,0	Залік
ВК6	Вибіркова дисципліна	4,0	Залік
Загальний обсяг вибіркових компонент		**24,0**	
Загальний обсяг ОПП		**90,0**	

2.2. Структурно-логічна схема послідовності вивчення компонент освітньо-професійної програми

Код компо-ненти	Назва компоненти освітньої програми	Кількість кредитів ЄКТС	Загаль-ний обсяг годин	Форма підсумкового контролю
1 семестр				
ОК1	Педагогічна майстерність та організація наукових досліджень	4,0	120	Залік
ОК2	Фахова іноземна мова	5,0	150	Екзамен
ОК3	Методи та алгоритми криптографічного захисту інформації	4,0	120	Екзамен
ОК4	Кібербезпека об’єктів критичної інфраструктури	4,0	120	Екзамен
ОК7	Системи виявлення та запобігання вторгнень	4,0	120	Залік
ОК8	Менеджмент інформаційної та кібербезпеки	4,0	120	Залік
ОК9	Проєктування та дослідження систем захисту інформації	5,0	150	Екзамен
	Всього	***30,0***	***900***	
2 семестр				
ОК10	Моделювання процесів кібербезпеки	4,0	140	Екзамен
		1,0	30	Курсова робота
ОК5	Інформаційна безпека соціальних систем	4,0	120	Екзамен
ОК6	Комплексні системи санкціонованого доступу	4,0	120	Екзамен
ВК1	Вибіркова дисципліна	4,0	120	Залік
ВК2	Вибіркова дисципліна	4,0	120	Залік
ОК12	Виробнича практика	9,0	270	Захист звіту
	Всього	***30,0***	***900***	
3 семестр				
ОК11	Цифрова криміналістика	4,0	120	Залік
ВК3	Вибіркова дисципліна	4,0	120	Залік
ВК4	Вибіркова дисципліна	4,0	120	Залік
ВК5	Вибіркова дисципліна	4,0	120	Залік
ВК6	Вибіркова дисципліна	4,0	120	Залік
ОК13	Переддипломна практика	6,0	180	Захист звіту
ОК14	Підготовка та захист кваліфікаційної роботи	4,0	120	Захист
	Всього	***30,0***	***900***	
ЗАГАЛЬНИЙ ОБСЯГ ОПП		**90,0**	**2700**	

2.3. Структурно-логічна схема освітньо-професійної програми



3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форма атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	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 (або у репозиторії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Принципи та процедури забезпечення якості вищої освіти	***Принципи забезпечення якості вищої освіти:*** – відповідність національним та європейським стандартам якості вищої освіти; – автономність Університету, як відповідального за забезпечення якості освітньої діяльності та якості вищої освіти; – системність та процесний підхід до управління якістю освітнього процесу; – комплексність в управлінні процесом контролю якості освітньої діяльності та якості вищої освіти; – системність у здійсненні моніторингових процедур з якості; – безперервність підвищення якості вищої освіти. ***Процедури забезпечення якості вищої освіти:*** – здійснення моніторингу та періодичного перегляду освітньої програми; – щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті Університету, на інформаційних стендах та в будь-який інший спосіб; – забезпечення підвищення кваліфікації педагогічних і науково-педагогічних працівників; – забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів вищої освіти, за освітньою програмою;

	– забезпечення наявності інформаційних систем для ефективного управління освітнім процесом; – забезпечення публічності інформації про освітню програму, ступінь вищої освіти та кваліфікацію; – забезпечення дотримання академічної доброчесності працівниками та здобувачами вищої освіти, у тому числі створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату; – інші процедури та заходи.
Моніторинг та періодичний перегляд освітньої програми	Освітня програма має відповідати вимогам Стандарту вищої освіти. Періодичний перегляд освітньої програми здійснюється за критеріями, які формулюються у результаті зворотного зв'язку із науково-педагогічними працівниками, здобувачами вищої освіти, випускниками, роботодавцями, а також внаслідок прогнозування розвитку галузі, потреб суспільства
Щорічне оцінювання здобувачів вищої освіти	Система оцінювання здобувачів вищої освіти включає здійснення таких контрольних заходів: вхідного, поточного, модульного (рубіжного), підсумкового та відстроченого контролю.
Щорічне оцінювання науково-педагогічних працівників	Оцінювання науково-педагогічних працівників проводиться на підставі ключових показників, визначених з урахуванням їх посадових обов'язків (виконання навчальної, методичної, наукової, організаційної роботи та інших трудових обов'язків).
Підвищення кваліфікації педагогічних і науково-педагогічних працівників	Педагогічні і науково-педагогічні працівники підвищують кваліфікацію та проходять стажування в Україні або за кордоном не рідше одного разу на п'ять років. В Університеті реалізуються власні програми підвищення кваліфікації (семінари, тренінги, вебінари, «круглі столи» тощо). Працівникам, які пройшли стажування або підвищення кваліфікації, видається відповідний документ.
Наявність необхідних ресурсів для організації освітнього процесу	Ресурсами для організації освітнього процесу за освітньою програмою є: – стандарт вищої освіти; – індивідуальний навчальний план; – робочі програми навчальних дисциплін; – програми навчальної, виробничої та інших видів практик; – інші ресурси (підручники і навчальні посібники; інструктивно-методичні матеріали до семінарських, практичних і лабораторних занять; завдання для самостійної роботи тощо).

	Відповідно до Ліцензійних умов провадження освітньої діяльності дотримуються вимоги до кадрового, матеріально-технічного та інформаційного забезпечення освітньої діяльності.
Наявність інформаційних систем для ефективного управління освітнім процесом	Ефективному управлінню освітньою діяльністю сприяють: – Єдина державна електронна база з питань освіти; – пакет «Деканат», який включає модуль «Навчальний план», модуль «Навчальний процес» і модуль «Розклад»; – система дистанційного навчання на платформі Moodle для організації самостійної роботи здобувачів вищої освіти; – електронний архів; – кампусна комп'ютерна мережа, яка складається з 2 корпоративних мереж, що включають 7 локальних мереж і 36 точок бездротового доступу до мережі Інтернет; – інші інформаційні системи.
Забезпечення публічності інформації про освітню програму, ступінь вищої освіти та кваліфікацію	Публічність інформації про освітню програму, ступінь вищої освіти та кваліфікацію забезпечується шляхом: – оприлюднення інформації на офіційному веб-сайті Університету; – розміщення інформації на інформаційних стендах; – в інший спосіб відповідно до чинного законодавства.
Забезпечення дотримання академічної доброчесності	Процедури та заходи забезпечення дотримання академічної доброчесності: – використання Положення про академічну доброчесність, запобігання та виявлення плагіату в Університеті; – проведення комплексу відповідних профілактичних заходів в Університеті; – здійснення контролю за дотриманням академічної доброчесності працівниками та здобувачами вищої освіти, у тому числі шляхом перевірки на плагіат, із використанням відповідної програми, кваліфікаційних робіт, дисертацій та авторефератів, монографій, підручників і посібників, рукописів статей і тез доповідей, курсових робіт (проєктів) тощо; – у разі виявлення академічного плагіату автори несуть відповідальність відповідно до чинного законодавства.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ

Компоненти / Компетентності	Освітні компоненти													
	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14
ЗК1											+	+	+	+
ЗК2	+												+	+
ЗК3	+										+		+	+
ЗК4	+													+
ЗК5	+	+												
ФК1			+	+			+		+	+		+	+	+
ФК2		+		+			+	+		+		+	+	+
ФК3			+	+		+			+			+	+	+
ФК4					+			+				+	+	+
ФК5								+				+	+	+
ФК6						+	+					+	+	+
ФК7										+	+	+	+	+
ФК8			+						+			+		+
ФК9								+				+		+
ФК10	+											+		+
ФК11					+					+				
ФК12	+				+					+				+

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ ОСВІТНІМИ КОМПОНЕНТАМИ

Компоненти / Програмні результати навч.	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14
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	+				+					+				+