**Ф-22.05-04.01/125.00.01/М-2025**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»**

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА**

**«Кібербезпека»**

Другого (магістерського) рівня вищої освіти

галузі знань 12 **«**Інформаційні технології**»**

спеціальності 125 **«**Кібербезпека та захист інформації**»**

Кваліфікація: магістр з кібербезпеки та захисту інформації

ПРОЄКТ

**ЗАТВЕРДЖЕНО**

Вченою радою   
Державного університету «Житомирська політехніка»

Голова Вченої ради

\_\_\_\_\_\_\_\_ Віктор ЄВДОКИМОВ

(протокол від \_\_ \_\_\_\_\_\_\_\_ 202\_ р. № \_)

Освітня програма вводиться в дію з 01 вересня 2025 р.

Ректор

\_\_\_\_\_\_\_\_ Віктор ЄВДОКИМОВ

(наказ від \_\_\_ \_\_\_\_\_ 2025 р. № \_\_\_\_\_

Житомир – 2025

**ПЕРЕДМОВА**

Освітньо-професійну програму «Кібербезпека» розроблено відповідно до Стандарту вищої освіти України за спеціальністю 125 «Кібербезпека та захист інформації» для другого (магістерського) рівня вищої освіти (затверджено і введено в дію наказом Міністерства освіти і науки України № 332 від 18 березня 2021 р.) робочою групою у складі:

1. ВОРОТНІКОВ Володимир, д.т.н., доцент, професор кафедри комп’ютерної інженерії та кібербезпеки – гарант освітньої програми.
2. ЄФІМЕНКО Андрій., к.т.н., доцент, завідувач кафедри комп’ютерної інженерії та кібербезпеки.
3. ЛОБАНЧИКОВА Надія, к.т.н., доцент, доцент кафедри інженерії програмного забезпечення.
4. ШЕЛУХА Олексій, к.т.н., доцент кафедри комп’ютерної інженерії та кібербезпеки.
5. ПІРОГ Олександр, к.т.н. к.т.н., доцент кафедри комп’ютерної інженерії та кібербезпеки.
6. БАЙЛЮК Єлизавета, старший викладач кафедри комп’ютерної інженерії та кібербезпеки.
7. ПОКОТИЛО Олександра, старший викладач кафедри комп’ютерної інженерії та кібербезпеки.
8. КРУЧИНСЬКИЙ Ярослав – представник роботодавця, начальник відділу сервісного обслуговування технічної служби ТОВ «Фрінет».
9. СІНІЦИНА Олександра, здобувачка вищої освіти, 1 курс, група КБм-24-1.
10. ШЕВЧИК Дарина – здобувачка вищої освіти з ОПП, 2 курс, група КБм-23-1.
11. ГОНЧАРОВ Михайло – випускник з ОПП 2023 р.; аналітик з інцидентів. ТОВ «МЕТІНВЕСТ ДІДЖИТАЛ».
12. КУХАРЧУК МАКСИМ – випускник з ОПП 2022 р.; адміністратор системи, ТОВ «ПАРТНЕР».
13. ЛЕЩЕНКО Богдан – випускник з ОПП 2022 р.; адміністратор системи, ТОВ "Сана Комерс Україна".

**1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ**

|  |  |
| --- | --- |
| **1 – Загальна інформація** | |
| **Повна назва закладу вищої освіти та структурного підрозділу** | Державний університет  «Житомирська політехніка»,  факультет інформаційно-комп’ютерних технологій |
| **Рівень вищої освіти та назва кваліфікації мовою оригіналу** | Другий (магістерський) рівень вищої освіти  Кваліфікація – «магістр з кібербезпеки» |
| **Офіційна назва освітньої програми** | Кібербезпека |
| **Тип диплому та обсяг освітньої програми** | Диплом магістра, одиничний,  90 кредитів ЄКТС,  термін навчання 1 рік 4 місяці |
| **Наявність акредитації** | Сертифікат про акредитацію освітньої програми № 7253, дійсний до 01.07.2029 р. |
| **Цикл /рівень** | НРК України – 8 рівень,  FQ-EHEA – другий цикл,  EQF-LLL – 7 рівень |
| **Передумови** | Наявність освітнього ступеня “Бакалавр”, “Магістр” або освітньо-кваліфікаційного рівня “Спеціаліст” |
| **Мова(и) викладання** | Українська |
| **Термін дії освітньої програми** | Постійно |
| **Інтернет-адреса постійного розміщення опису освітньої програми** | https://ztu.edu.ua |
| **2 – Мета освітньої програми** | |
| Професійна підготовка фахівців з кібербезпеки, набуття ними компетентностей в застосуванні принципів, методів та засобів забезпечення кібербезпеки. | |
| **3 – Характеристика освітньої програми** | |
| **Предметна область**  **(галузь знань, спеціальність, спеціалізація)** | 12 – Інформаційні технології  125 – Кібербезпека та захист інформації |
| **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. |
| **Орієнтація освітньої програми** | Освітньо-професійна |
| **Основний фокус освітньої програми та спеціалізації** | Вища освіта в галузі інформаційних технологій. Програма фокусується на питанням забезпечення кібербезпеки та захисту інформації у сучасних комп’ютерних системах та мережах, зокрема, мережній безпеці, тестуванні на проникнення, реагуванню та розслідуванню інцидентів кібербезпеки, організації SOC.  Ключові слова: кібербезпека, комп’ютерна система, комп’ютерна мережа, інформаційна система, інформаційно-телекомунікаційна система, операційна система, адміністрування систем, прикладне та системне програмування, вразливість, атака, ризик, компрометація, протидія, захист інформації, тестування на проникнення, моніторинг, розслідування інциденту, міжмережне екранування, система виявлення та попередження вторгнень, кібероперації, спеціальні системи забезпечення кібербезпеки. |
| **Особливості**  **програми** | Тісна співпраця з державними та приватними організаціями з метою отримання практичних навичок безпечної експлуатації, адміністрування, забезпе­чення захисту комп’ютерних систем та мереж, навичок розробки захищеного прикладного та системного програмного забезпечення, проходження практичної підготовки з розробки та забезпечення захисту нових і вдосконалення захисту існуючих комп’ютерних та інформаційних систем з подальшим впровадженням науково-практичних розробок у діяльність організацій та установ. |
| **4 – Придатність випускників**  **до працевлаштування та подальшого** навчання | |
| **Придатність до працевлаштування** | Працевлаштування в організаціях та підприємствах будь-якої форми власності на посадах:  І. Згідно ДК 003:2010 (NIST800–181)   1. Розробник систем захисту інформації 2. Адміністратор безпеки мереж і систем 3. Аналітик загроз безпеки 4. Аналітик систем захисту інформації та оцінки вразливостей 5. Аналітик з безпеки інформаційно-телекомунікаційних систем 6. Дізнавач (сфера кібербезпеки та захисту інформації)\* 7. Експерт-криміналіст (сфера кібербезпеки та захисту інформації)\* 8. Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації)\* 9. Слідчий з кіберзлочинів\* 10. Фахівець з криптографічного захисту інформації 11. Фахівець з питань безпеки (інформаційно-комунікаційні технології 12. Фахівець з підтримки інфраструктури кіберзахисту 13. Фахівець з реагування на інциденти кібербезпеки 14. Фахівець з тестування систем захисту інформації 15. Фахівець з технічного захисту інформації 16. Фахівець сфери захисту інформації   \* може потребувати/потребує додаткового навчання/освіти.  ІІ. Згідно ECSF (European Cybersecurity Skills Framework):   1. Chief Information Security Officer (CISO) 2. Cyber Incident Responder 3. Cyber Legal, Policy and Compliance Officer 4. Cyber Threat Intelligence Specialist 5. Cybersecurity Educator 6. Cybersecurity Implementer 7. CybersecurityAuditor 8. Cybersecurity Researcher 9. Cybersecurity Risk Manager 10. Digital Forensics Investigator |
| **Подальше навчання** | Можливість отримання освіти за програма­ми третього (освітньо-наукового) рівня ви­щої освіти.  Можливість набуття додаткових кваліфіка­цій у системі освіти дорослих. |
| **5 – Викладання та оцінювання** | |
| **Викладання та**  **навчання** | Викладання здійснюється на засадах студентоцентрованого навчання, самонавчан­ня, проблемно-орієнтованого навчання тощо |
| **Оцінювання** | Оцінювання навчальних досягнень здійс­нюється за 100-бальною (рейтинговою) шкалою ЄКТС.  Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль.  Форми контролю: модульні контрольні роботи за вивченими темами, усне та письмове опитування, компʼютерне тестування, екзамени та заліки (усні, письмові, у формі тестів в тому числі комп’ютерне тестування), презентація індивідуальних завдань, захист звітів (за результатами практики).  Підсумкова атестація – підготовка та публічний захист кваліфікаційної роботи/проекту. |
| **6 – Програмні компетентності** | |
| **Інтегральна компетентність** | Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. |
| **Загальні компетентності (КЗ)** | **КЗ-1**. Здатність застосовувати знання у практичних ситуаціях.  **КЗ-2**. Здатність проводити дослідження на відповідному рівні.  **КЗ-3**. Здатність до абстрактного мислення, аналізу та синтезу.  **КЗ-4**. Здатність оцінювати та забезпечувати якість виконуваних робіт.  **КЗ-5**. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). |
| **Спеціальні (фахові, предметні) компетентності (КФ)** | **КФ-1**. 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.  **КФ-2**. 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.  **КФ-3.** Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.  **КФ-4.** 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.  **КФ-5.** 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.  **КФ-6.** Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформа­ційної безпеки та/або кібербезпеки організації.  **КФ-7**. 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.  **КФ-8**. 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.  **КФ-9**. 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.  **КФ-10**. 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. |
| **7 – Результати навчання** | |
| **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. | |
| **8 – Ресурсне забезпечення реалізації програми** | |
| **Кадрове забезпечення** | У реалізації даної освітньої програми задіяно 5 докторів наук, професорів або доцентів/с.н.с., 6 кандидатів наук, доцентів, 2 кандидати наук/PhD, кожен з яких має виконання не менше 4 пунктів п. 38 Ліцензійних умов провадження освітньої діяльності. Тобто, кадрове забезпечення освітньої програми відповідає ліцензійним вимогам щодо надання освітніх послуг у сфері вищої світи і є достатнім для забезпечення якості освітнього процесу. |
| **Матеріально-технічне забезпечення** | Матеріально-технічне забезпечення відпові­дає ліцензійним вимогам щодо надання освітніх послуг у сфері вищої світи і є достатнім для забезпечення якості освітнього процесу |
| **Інформаційне та навчально-методичне забезпечення** | Інформаційне та навчально-методичне забезпечення освітньої програми «Кібербезпека» з підготовки фахівців зі спеціальності 125 «Кібербезпека та захист інформації» відповідає ліцензійним вимогам, має актуальний змістовий контент, базується на сучасних інформаційно-комунікаційних технологіях та засобах забезпечення кібербезпеки та захисту інформації.  В університеті функціонують Мережна академія Cisco, Центр підтримки академій Cisco, Центр підготовки інструкторів Cisco, ресурси яких доступні для студентів (за умови реєстрації). Також в університеті реалізуються партнерські академічні програми від компаній IBM, Microsoft, Fortinet, AWS, Oracle та ін.  Здобувачам освіти забезпечується доступ до освітніх платформ Udemy, Coursera тощо. |
| **9 – Академічна мобільність** | |
| **Національна кредитна мобільність** | Реалізується в межах спільної діяльності з Національним технічним університетом «КПІ імені Ігоря Сікорського», Хмель­ниць­ким національним універси­тетом, Запорізь­ким національним універси­тетом, Жито­мирським військовим інститутом імені С.П. Корольо­ва, Жито­мирським державним університетом імені Івана Франка, Національним універси­тетом водного господарства та природокористування, Харківським націо­наль­ним університетом радіоелектро­ніки, Харківським національним університетом ім. В. Каразіна, Черкаським державним техноло­гічним університетом, Державним універси­те­том інформаційно-комунікаційних технологій, Національ­ним університетом «Одеська юридична акаде­мія» згідно укладених договорів про співпрацю. |
| **Міжнародна кредитна мобільність** | На основі двосторонніх договорів між Державним університетом «Житомирська політехніка» та зарубіжними закладами вищої освіти. |
| **Навчання іноземних здобувачів вищої освіти** | На навчання приймаються іноземні грома­дяни на умовах контракту, які мають доку­мент про отримання першого (бакалаврського) рівня вищої освіти. |

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

**2.1. Перелік компонент освітньо-професійної програми**

|  |  |  |  |
| --- | --- | --- | --- |
| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти/ роботи, практики кваліфікаційна робота) | Кількість кредитів | Форма підсумкового контролю |
| 1 | 2 | 3 | 4 |
| **Обов’язкові компоненти ОП** | | | |
| ОК 01 | Англійська мова (за професійним спрямуванням) | 3 | Залік |
| ОК 02 | Методологія наукових досліджень | 3 | Залік |
| ОК 03 | Інтелектуальна власність | 3 | Залік |
| ОК 04 | Філософські проблеми наукового пізнання | 3 | Залік |
| ОК 05 | Педагогіка та психологія | 3 | Залік |
| ОК 06 | Цивільний захист | 3 | Залік |
| ОК 07 | Архітектура, проєктування та безпека веб-орієнто­ваних інформаційних та комп'ютерних систем | 4 | Екзамен |
| ОК 08 | Технології адміністрування та захисту інформаційних систем | 4 | Екзамен |
| ОК 09 | Моніторинг, аудит та управління системами кібербезпеки | 4 | Екзамен |
| ОК 10 | Проектування систем кібербезпеки | 3 | Залік |
| ОК 11 | Хмарна безпека | 3 | Залік |
| ОК 12 | Тестування на проникнення, етичний хакінг та цифрова криміналістика | 3 | Екзамен, курсова робота |
| ОК 13 | Наукова практика | 3 | Диф. залік |
| ОК 14 | Виробнича практика | 6 | Диф. залік |
| ОК 15 | Переддипломна практика | 6 | Диф. залік |
| ОК 16 | Кваліфікаційна робота | 12 | Кваліфікаційна атестація |
| **Загальний обсяг обов’язкових компонент:** | | **66** | |
| **Вибіркові компоненти ОП** | | | |
| ***Вибірковий блок 1*** | | | |
| ВК 1.01 | Дисципліна вільного вибору № 01 | 4 | Залік |
| ***Вибірковий блок 2*** *(обираються навчальні дисципліни загальним обсягом 20 кредитів)* | | | |
| ВК 2.01 | Дисципліна професійної підготовки № 01 | 4 | Залік |
| ВК 2.02 | Дисципліна професійної підготовки № 02 | 4 | Залік |
| ВК 2.03 | Дисципліна професійної підготовки № 03 | 4 | Залік |
| ВК 2.04 | Дисципліна професійної підготовки № 04 | 4 | Залік |
| ВК 2.05 | Дисципліна професійної підготовки № 05 | 4 | Залік |
| **Загальний обсяг вибіркових компонент:** | | **24** | |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** | | **90** | |

**2.2. Структурно-логічна схема освітньо-професійної програми**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти/ роботи, практики кваліфікаційна робота) | Кількість кредитів | Загальний обсяг год. | Форма підсумкового контролю |
| 1 | 2 | 3 | 4 | 5 |
| **І курс, І семестр** | | | | |
| ОК 01 | Англійська мова (за професійним спрямуванням) | 3 | 90 | Залік |
| ОК 02 | Методологія наукових досліджень | 3 | 90 | Залік |
| ОК 03 | Інтелектуальна власність | 3 | 90 | Залік |
| ОК 07 | Архітектура, проєктування та безпека веб-орієнто­ваних інформаційних та комп'ютерних систем | 4 | 120 | Екзамен |
| ОК 08 | Технології адміністрування та захисту інформаційних систем | 4 | 120 | Екзамен |
| ОК 09 | Моніторинг, аудит та управління системами кібербезпеки | 4 | 120 | Екзамен |
| ОК 10 | Проектування систем кібербезпеки | 3 | 90 | Залік |
| ОК 11 | Хмарна безпека | 3 | 90 | Залік |
|  | **Разом** | **27** | **810** |  |
| **І курс, ІІ семестр** | | | | |
| ВК 1.01 | Дисципліна вільного вибору №01 | 4 | 120 | Залік |
| ВК 2.01 | Дисципліна професійної підготовки №01 | 4 | 120 | Залік |
| ВК 2.02 | Дисципліна професійної підготовки №02 | 4 | 120 | Залік |
| ВК 2.03 | Дисципліна професійної підготовки №03 | 4 | 120 | Залік |
| ВК 2.04 | Дисципліна професійної підготовки №04 | 4 | 120 | Залік |
| ВК 2.04 | Дисципліна професійної підготовки №05 | 4 | 120 | Залік |
| ОК 13 | Наукова практика | 3 | 90 | Диф. залік |
| ОК 14 | Виробнича практика | 6 | 180 | Диф. залік |
|  | **Разом** | **33** | **990** |  |
| **ІІ курс, І семестр** | | | | |
| ОК 04 | Філософські проблеми наукового пізнання | 3 | 90 | Залік |
| ОК 05 | Педагогіка та психологія | 3 | 90 | Залік |
| ОК 06 | Цивільний захист | 3 | 90 | Залік |
| ОК 12 | Тестування на проникнення, етичний хакінг та цифрова криміналістика | 3 | 90 | Екзамен, Курсова робота |
| ОК 15 | Переддипломна практика | 6 | 180 | Диф. залік |
| ОК 16 | Кваліфікаційна робота | 12 | 360 | Кваліфікаційна атестація |
|  | **Разом** | **30** | **900** |  |
| **Загальний обсяг:** | | **90** | **2700** |  |

**СТРУКТУРНО-ЛОГІЧНА СХЕМА**



**3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ**

Поточна атестація студентів здійснюється у формі екзаменів, заліків, диференційованих заліків, захисту курсових робіт та проектів.

Атестація випускників освітньо-професійної програми «Кібербезпека» за спеціальністю 125 «Кібербезпека та захист інформації» проводиться у формі публічного захисту кваліфікаційного проекту/роботи та завершується видачою документу встановленого зразка про присудження йому освітнього ступеня «магістр» з присвоєнням кваліфікації: магістр з кібербезпеки та захисту інформації. У кваліфікаційному проекті/роботі не допускається порушень академічної доброчесності, зокрема, наявність академічного плагіату, результатів фабрикації та фальсифікації.

Атестація здійснюється відкрито і публічно.

Кваліфікаційний проект/робота оприлюднюється у репозитарії закладу вищої освіти.

**4. ВІДПОВІДНІСТЬ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ**

**4.1. Матриця відповідності програмних компетентностей обов’язковим компонентам освітньо-професійної програми**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Загальні компетентності (К3)** | | | | | **Спеціальні (фахові, предметні) компетентності (КФ)** | | | | | | | | | |
|  | **КЗ-1** | **КЗ-2** | **КЗ-3** | **КЗ-4** | **КЗ-5** | **КФ-1** | **КФ-2** | **КФ-3** | **КФ-4** | **КФ-5** | **КФ-6** | **КФ-7** | **КФ-8** | **КФ-9** | **КФ-10** |
| **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** | + | + | + | + | + | + |  | + | + | + |  | + | + | + | + |
| **ОК 14** | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **ОК 15** | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **ОК 16** | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |

**5. ЗАБЕЗПЕЧЕНІСТЬ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ**

**5.1. Матриця забезпечення програмних результатів навчання відповідними обов’язковими компонентами освітньо-професійної програми**

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