Ф-22.05-04.01/125.00.01/М-2024

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

**ЗАТВЕРДЖЕНО**

Вченою радою Державного університету «Житомирська політехніка»

Голова Вченої ради

_____ Віктор ЄВДОКИМОВ

(протокол від «__» _____ 202_ р. № )

Освітня програма вводиться в дію з __ вересня 202_ р.

Ректор

_____ Віктор ЄВДОКИМОВ

(наказ від «__» _____ 202_ р. № ___)

Житомир – 2024

# 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. БАЙЛЮК Єлизавета, старший викладач кафедри комп'ютерної інженерії та кібербезпеки.
6. ПОКОТИЛО Олександра, старший викладач кафедри комп'ютерної інженерії та кібербезпеки.
7. КРУЧИНСЬКИЙ Ярослав – представник роботодавця, начальник відділу сервісного обслуговування технічної служби ТОВ «Фрінет».
8. ШЕВЧИК Дарина – здобувачка вищої освіти з ОПП, 1 курс, група КБм-23-1.
9. ГОНЧАРОВ Михайло – випускник з ОПП 2023 р., аналітик з інцидентів, ТОВ «МЕТІНВЕСТ ДІДЖИТАЛ».
10. 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<br>Кваліфікація – «магістр з кібербезпеки» |
| **Офіційна назва освітньої програми** | Кібербезпека |
| **Тип диплому та обсяг освітньої програми** | Диплом магістра, одиничний,<br>90 кредитів ЄКТС,<br>термін навчання 1 рік 4 місяці |
| **Наявність акредитації** | Відсутня |
| **Цикл /рівень** | НРК України – 8 рівень,<br>FQ-EHEA – другий цикл,<br>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<br>125 – Кібербезпека та захист інформації |
| **Опис предметної області** | **Об'єкти вивчення:**<br>– 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;<br>– інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології;<br>– інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур;<br>– системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); |

| | |
|---|---|
| | – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси);<br>– програмне та програмно-апаратне забезпечення (засоби) кіберзахисту;<br>– системи управління інформаційною безпекою та/або кібербезпекою;<br>– технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки.<br>**Цілі навчання:**<br>Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.<br>**Теоретичний зміст предметної області**<br>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.<br>**Методи, методики та технології**<br>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.<br>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.<br>**Інструменти та обладнання**.<br>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 систем та мереж, зокрема, мережній безпеці, тестуванні на проникнення, реагуванню та розслідуванню інцидентів кібербезпеки, організації SOC.<br>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:<br>І. Згідно ДК 003:2010 (NIST800–181)<br>1. Розробник систем захисту інформації<br>2. Адміністратор мереж і систем |

| | |
|---|---|
| | 3. Аналітик загроз безпеки<br>4. Аналітик систем захисту інформації та оцінки вразливостей<br>5. Аналітик з безпеки інформаційно-телекомунікаційних систем<br>6. Дізнавач (сфера кібербезпеки та захисту інформації)*<br>7. Експерт-криміналіст (сфера кібербезпеки та захисту інформації)*<br>8. Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації)*<br>9. Слідчий з кіберзлочинів*<br>10. Фахівець з криптографічного захисту інформації<br>11. Фахівець з питань безпеки (інформаційно-комунікаційні технології<br>12. Фахівець з підтримки інфраструктури кіберзахисту<br>13. Фахівець з реагування на інциденти кібербезпеки<br>14. Фахівець з тестування систем захисту інформації<br>15. Фахівець з технічного захисту інформації<br>16. Фахівець сфери захисту інформації<br>* може потребувати/потребує додаткового навчання/освіти.<br>II. Згідно ECSF (European Cybersecurity Skills Framework):<br>1. Chief Information Security Officer (CISO)<br>2. Cyber Incident Responder<br>3. Cyber Legal, Policy and Compliance Officer<br>4. Cyber Threat Intelligence Specialist<br>5. Cybersecurity Educator<br>6. Cybersecurity Implementer<br>7. CybersecurityAuditor<br>8. Cybersecurity Researcher<br>9. Cybersecurity Risk Manager<br>10. Digital Forensics Investigator |
| **Подальше навчання** | Можливість отримання освіти за програмами третього (освітньо-наукового) рівня вищої освіти.<br>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.<br>Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль.<br>Форми контролю: модульні контрольні роботи за вивченими темами, усне та письмове опитування, комп'ютерне тестування, екзамени та заліки (усні, письмові, у формі тестів в тому числі комп'ютерне тестування), презентація індивідуальних завдань, захист звітів (за результатами практики).<br>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.<br>**КЗ-2**. Здатність проводити дослідження на відповідному рівні.<br>**КЗ-3**. Здатність до абстрактного мислення, аналізу та синтезу.<br>**КЗ-4**. Здатність оцінювати та забезпечувати якість виконуваних робіт.<br>**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.<br>**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.<br>**КФ-3.** Здатність досліджувати, розробляти і супроводжувати методи та засоби |

| | |
|---|---|
| | інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.<br>**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.<br>**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.<br>**КФ-6.** Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.<br>**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.<br>**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.<br>**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.<br>**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.<br>**РН18.** Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.<br>**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.<br>**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.<br>**РН21.** Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.<br>**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.<br>**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 4 доктори наук, професори, 5 кандидатів наук, доцентів, 2 кандидати наук.<br>Таким чином, 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.<br>В університеті функціонують Мережна академія Cisco, Центр підтримки академій Cisco, Центр підготовки інструкторів Cisco, ресурси яких доступні для студентів (за умови реєстрації). Університет активно співпрацює з організаціями, які надають |

| | |
|---|---|
| | доступ до зовнішніх навчальних платформ, зокрема, активно застосовується онлайнова кібербезпекова платформа RangeForce.com. |
| **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 телекомунікацій, 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

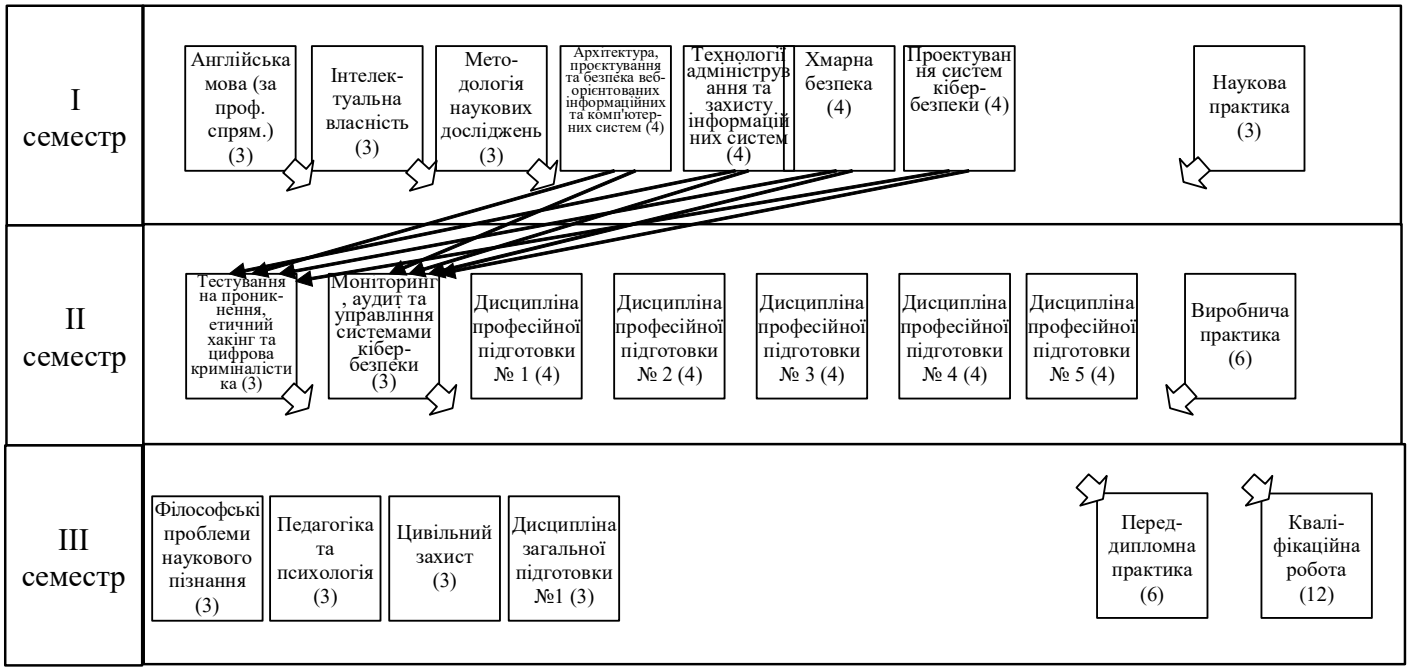
## 2.1. Перелік компонент освітньо-професійної програми

| 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** | | | |
| ОК1 | Англійська мова (за професійним спрямуванням) | 3 | Залік |
| ОК2 | Інтелектуальна власність | 3 | Залік |
| ОК3 | Методологія наукових досліджень | 3 | Залік |
| ОК4 | Філософські проблеми наукового пізнання | 3 | Залік |
| ОК5 | Педагогіка та психологія | 3 | Залік |
| ОК6 | Цивільний захист | 3 | Залік |
| ОК7 | Архітектура, проєктування та безпека веб-орієн-тованих інформаційних та комп'ютерних систем | 4 | Екзамен |
| ОК8 | Технології адміністрування та захисту інформаційних систем | 4 | Екзамен |
| ОК9 | Хмарна безпека | 4 | Екзамен |
| ОК10 | Проектування систем кібербезпеки | 4 | Залік |
| ОК11 | Тестування на проникнення, етичний хакінг та цифрова криміналістика | 3 | Екзамен |
| ОК12 | Моніторинг, аудит та управління системами кібербезпеки | 3 | Екзамен, курсовий проєкт |
| ОК13 | Наукова практика | 3 | Диф. залік |
| ОК14 | Виробнича практика | 6 | Диф. залік |
| ОК15 | Переддипломна практика | 6 | Диф. залік |
| ОК16 | Кваліфікаційна робота | 12 | Кваліфікаційна атестація |
| **Загальний обсяг обов'язкових компонент:** | | **67** | |
| **Вибіркові компоненти ОП** | | | |
| ***Вибірковий блок 1*** *(вибіркові освітні компоненти університету, перелік освітніх компонент блоку затверджуються наказом ректора щорічно, студенти обирають 1 навчальну дисципліну загальним обсягом 3 кредити)* | | | |
| ВК1.1 | Дисципліна загальної підготовки №1 | 3 | Залік |
| ***Вибірковий блок 2*** *(обираються навчальні дисципліни загальним обсягом 20 кредитів)* | | | |
| ВК2.1 | Дисципліна професійної підготовки № 1 | 4 | Залік |
| ВК2.2 | Дисципліна професійної підготовки № 2 | 4 | Залік |
| ВК2.3 | Дисципліна професійної підготовки № 3 | 4 | Залік |
| ВК2.4 | Дисципліна професійної підготовки № 4 | 4 | Залік |
| ВК2.5 | Дисципліна професійної підготовки № 5 | 4 | Залік |
| **Загальний обсяг вибіркових компонент:** | | **23** | |
| **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** | | | | |
| ОК1 | Англійська мова (за професійним спрямуванням) | 3 | 90 | Залік |
| ОК2 | Інтелектуальна власність | 3 | 90 | Залік |
| ОК3 | Методологія наукових досліджень | 3 | 90 | Залік |
| ОК7 | Архітектура, проєктування та безпека веб-орієнтованих інформаційних та комп'ютерних систем | 4 | 120 | Екзамен |
| ОК8 | Технології адміністрування та захисту інформаційних систем | 4 | 120 | Екзамен |
| ОК9 | Хмарна безпека | 4 | 120 | Екзамен |
| ОК10 | Проектування систем кібербезпеки | 4 | 120 | Екзамен |
| ОК13 | Наукова практика | 3 | 90 | Диф. залік |
| | **Разом** | **28** | **840** | |
| **І курс, ІІ семестр** | | | | |
| ОК11 | Тестування на проникнення, етичний хакінг та цифрова криміналістика | 3 | 90 | Екзамен |
| ОК12 | Моніторинг, аудит та управління системами кібербезпеки | 3 | 90 | Екзамен, курсовий проєкт |
| ВК2.1 | Дисципліна професійної підготовки №1 | 4 | 120 | Залік |
| ВК2.2 | Дисципліна професійної підготовки №2 | 4 | 120 | Залік |
| ВК2.3 | Дисципліна професійної підготовки №3 | 4 | 120 | Залік |
| ВК2.4 | Дисципліна професійної підготовки №4 | 4 | 120 | Залік |
| ВК2.4 | Дисципліна професійної підготовки №5 | 4 | 120 | Залік |
| ОК14 | Виробнича практика | 6 | 180 | Диф. залік |
| | **Разом** | **32** | **960** | |
| **ІІ курс, І семестр** | | | | |
| ОК4 | Філософські проблеми наукового пізнання | 3 | 90 | Залік |
| ОК5 | Педагогіка та психологія | 3 | 90 | Залік |
| ОК6 | Цивільний захист | 3 | 90 | Залік |
| ВК1.1. | Дисципліна загальної підготовки №1 | 3 | 90 | Залік |
| ОК15 | Переддипломна практика | 6 | 180 | Диф. залік |
| ОК16 | Кваліфікаційна робота | 12 | 360 | Кваліфікаційна атестація |
| | **Разом** | **30** | **900** | |
| | **Загальний обсяг:** | **90** | **2700** | |

## СТРУКТУРНО-ЛОГІЧНА СХЕМА




Вихідна стрілка, яка розміщена в правому чи лівому нижньому кутку, показує, що ОК забезпечує решту ОК поточного і наступних семестрів;
Вхідна стрілка, яка розміщена у правому чи лівому верхньому кутку, показує, що ОК забезпечується ОК попередніх та поточного семестрів.

## 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. 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 (КЗ)** | | | | | **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** | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |