**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

# ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

## «КІБЕРБЕЗПЕКА»

**другого (магістерського) рівня вищої освіти**
**за спеціальністю F5 Кібербезпека та захист інформації**
**галузі знань F Інформаційні технології**

**ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ**
**Голова вченої ради**
**_____ Андрій КРИСОВАТИЙ**
**(протокол № 10/1 від " 17 " червня 2026 р.)**

**Освітня програма вводиться в дію з вересня 2026 р.**

**Ректор _____ Оксана ДЕСЯТНЮК**
**(наказ № 438 від " 17 " червня 2026 р.)**

**Тернопіль – 2026**

**ЛИСТ ПОГОДЖЕННЯ**
**освітньо-професійної програми**

**«КІБЕРБЕЗПЕКА»**

**другого (магістерського) рівня вищої освіти**

**за спеціальністю F5 Кібербезпека та захист інформації**

**галузі знань F Інформаційні технології**

| | |
|---|---|
| *Проректор з науково-педагогічної роботи* | *Віктор ОСТРОВЕРХОВ* |
| *Директор центру ліцензування, акредитації, методичної роботи та забезпечення якості освіти* | *Леся БІЛОВУС* |
| *Декан факультету комп'ютерних інформаційних технологій* | *Ігор ЯКИМЕНКО* |
| *Голова ГЗС, завідувач кафедри* | *Василь ЯЦКІВ* |
| *Гарант ОПП* | *Василь ЯЦКІВ* |

# ПЕРЕДМОВА

**Розроблено робочою групою у складі:**

1. Василь ЯЦКІВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки ЗУНУ;
2. Михайло КАСЯНЧУК, доктор технічних наук, професор, професор кафедри кібербезпеки ЗУНУ;
3. Ігор ЯКИМЕНКО, доктор технічних наук, доцент, доцент кафедри кібербезпеки ЗУНУ;
4. Степан ІВАСЬЄВ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки ЗУНУ;
5. Сергій КУЛИНА, доктор філософії з кібербезпеки, доцент кафедри кібербезпеки ЗУНУ;
6. Богдан БАРАННІК, викладач кафедри кібербезпеки, випускник освітньо - професійної програми «Кібербезпека» ЗУНУ;
7. Микола НЕТРЕБЯК, здобувач освіти другого (магістерського) рівня вищої освіти, ОПП Кібербезпека, ЗУНУ;
8. Олена ВОЛОЩУК, к.т.н., доцент, керівник освітнього департаменту Distributed Lab.

**Відгуки та рецензії на освітньо-професійну програму:**

1. Олег ГАРАСИМЧУК, к.т.н., доцент, доцент кафедри захисту інформації Національного університету «Львівська політехніка»;
2. Віктор ЧЕШУН, к.т.н., доцент, доцент кафедри кібербезпеки Хмельницького національного університету;
3. Володимир ДРАПАК, директор комунального підприємства «Тернопільський інформаційно-аналітичний центр» Тернопільської обласної ради;
4. Сергій СТЕПАНЮК, Директор компанії ТОВ «Софт Світ».

# 1. Профіль освітньо-професійної програми «Кібербезпека» зі спеціальності «Кібербезпека та захист інформації»

| 1 – Загальна інформація | |
|---|---|
| **Повна назва вищого навчального закладу та структурного підрозділу** | Західноукраїнський національний університет,<br>факультет комп'ютерних інформаційних технологій,<br>кафедра кібербезпеки |
| **Ступінь вищої освіти та назва кваліфікації мовою оригіналу** | Магістр,<br>магістр з кібербезпеки та захисту інформації |
| **Офіційна назва освітньої програми** | Освітньо-професійна програма «Кібербезпека» |
| **Форма здобуття вищої освіти** | денна, заочна |
| **Тип диплому та обсяг освітньої програми** | Тип диплому – одиничний,<br>диплом магістра, 90 кредитів ЄКТС,<br>термін навчання 1 рік 4 місяці |
| **Наявність акредитації** | Освітня програма акредитована Національним агентством із забезпечення якості вищої освіти №19302, рішення від 05.12.2025 р.<br>Строк дії сертифіката про акредитацію освітньої програми 01.07.2031 р. |
| **Цикл/рівень** | НРК України – 7 рівень |
| **Передумови** | Наявність ступеня вищої освіти «бакалавр», «магістр» (ОКР «спеціаліст») |
| **Мова(и) викладання** | Українська |
| **Термін дії освітньої програми** | Термін не може перевищувати 1 рік 4 місяці |
| **Інтернет-адреса постійного розміщення опису освітньої програми** | https://www.wunu.edu.ua/master_fcit_op/ |
| **2 – Мета освітньої програми** | |
| Підготовка висококваліфікованих, конкурентоспроможних фахівців здатних проводити наукові дослідження в галузі інформаційної безпеки та/або кібербезпеки, які мають теоретичні знання та сформоване критичне мислення достатні для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки; володіють сучасними методами та технологіями тестування на проникнення; методами цифрової криміналістики; вміють безконфліктно та продуктивно працювати в командах щодо розв'язання проблем та прийняття рішень. | |

| 3 - Характеристика освітньої програми | |
|---|---|
| **Предметна область** | **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);<br>– 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><br>**Цілі навчання:**<br>підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.<br><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><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. |

| | |
|---|---|
| | **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** | Враховуючи збільшення кібератак на підприємства та організації ОПП орієнтується на поглиблене вивчення систем моніторингу та управління інформаційною безпекою та також сучасних методів та технологій тестування на проникнення. |
| **Основний фокус освітньої програми** | Підготовка фахівців для проведення досліджень та науково-технічних розробок у галузі інформаційної безпеки та\або кібербезпеки.<br>Ключові слова: інформаційна безпека, кібербезпека, цифрова криміналістика, тестування безпеки, аналіз шкідливого програмного забезпечення, блокчейн, безпека Інтернет речей. |
| **Особливості програми** | Освітня програма «Кібербезпека» спрямована на формування у здобувачів знань і практичних навичок захисту інформаційних систем від сучасних кіберзагроз. Її відмінністю є поєднання теоретичної підготовки з практично орієнтованими дисциплінами:<br>– моніторинг та управління інформаційною безпекою – вивчення принципів організації систем захисту, управління інцидентами та застосування міжнародних стандартів (ISO, NIST);<br>– Аналіз шкідливого програмного забезпечення – дослідження зразків шкідливого коду, технік зворотного інжинірингу та розробка заходів протидії;<br>– тестування комп'ютерних систем на проникнення – оволодіння інструментами та методиками пентесту для виявлення й усунення вразливостей;<br>– дослідження і проєктування систем захисту інформації – моделювання загроз, архітектурний дизайн засобів захисту, оцінка ефективності та стійкості рішень;<br>– цифрова криміналістика – освоєння методів збору, зберігання та аналізу цифрових доказів із дотриманням вимог.<br>Програма орієнтована на підготовку висококваліфікованих фахівців, здатних працювати у сферах захисту критичної інфраструктури, розслідування кіберінцидентів та розробки сучасних систем інформаційної безпеки. |
| **4 – Придатність випускників до працевлаштування та подальшого навчання** | |
| **Придатність до працевлаштування** | Згідно з Національним класифікатором професій ДК 003:2010 (зі змінами) випускники можуть обіймати такі первинні посади, як:<br>- 2139.2 Аналітик загроз безпеки;<br>- 2139.2 Фахівець з кібердосліджень та розробок систем;<br>- 2139.2 Фахівець з криптографічного захисту інформації; |

| | |
|---|---|
| | - 2139.2 Фахівець з реагування на інциденти кібербезпеки;<br>- 2139.2 Фахівець з тестування систем захисту інформації;<br>- 2139.2 Фахівець сфери захисту інформації. |
| **Подальше навчання** | Можливість здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти.<br>Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти. |
| **5 – Викладання та оцінювання** | |
| **Викладання та навчання** | Основні підходи: студенто-центроване навчання, самонавчання, проблемно-орієнтоване навчання, інтерактивне навчання, навчання через практику.<br>Методи та технології: загальнонаукові, математично-статистичні, інформаційно-комунікаційні технології, методи науково-дослідницької діяльності та презентації результатів.<br>Викладання проводиться у формі: лекції, лабораторних занять, самостійного навчання на основі підручників і конспектів, консультації з викладачами, підготовки кваліфікаційної роботи. |
| **Оцінювання** | Оцінювання рівня засвоєння освітньо-професійної програми здійснюється за допомогою поточного опитування, модульного контролю, тести, заліки, екзамени, індивідуальні завдання, звіт про проходження переддипломної практики, кваліфікаційна робота тощо. |
| **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). |
| **Фахові компетентності спеціальності (КФ)** | КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.<br>КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. |

| | |
|---|---|
| | КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.<br>КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.<br>КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.<br>КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.<br>КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.<br>КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.<br>КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.<br>КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.<br>КФ11. Здатність використовувати програмно-апаратні засоби та інструменти аналізу артефактів, відновлення даних, а також шифрування та захищеного зберігання інформації в інформаційних системах та мережах. |
| **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.<br>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.<br>РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.<br>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.<br>РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.<br>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.<br>РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.<br>РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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><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.<br>РН24. Впроваджувати повний цикл аналізу артефактів; проводити відновлення видалених / пошкоджених файлів та інших даних з цифрових носіїв та / або систем. |
| **8 – Ресурсне забезпечення реалізації програми** | |
| **Кадрове забезпечення** | Всі науково-педагогічні працівники, залучені до реалізації освітньо-професійної програми мають науковий ступінь і/або вчене звання та підтверджений рівень наукової і професійної активності, що відповідає вимогам ліцензійних умов. До освітнього процесу можуть залучатися фахівці з іноземних країн. |
| **Матеріально-технічне забезпечення** | Освітній процес здійснюється в спеціально обладнаних аудиторіях і лабораторіях, які відповідають санітарно-технічним нормам і оснащених сучасним спеціалізованим обладнанням (сервер, маршрутизатори, керовані комутатори, міжмережні екрани, генератор віброакустичного зашумлення, генератори завад, пристрій |

| | |
|---|---|
| | захисту від електромагнітних завад), мультимедійною, комп'ютерною технікою та спеціалізованим програмним забезпеченням, з можливістю постійного доступу до мережі Internet та внутрішньої мережі ЗУНУ. |
| **Інформаційне та навчально-методичне забезпечення** | Онлайн-бібліотека (https://library.wunu.edu.ua/?lang=uk), робочі програми дисциплін, методичні рекомендації та вказівки до вивчення дисциплін, проходження практики і написання випускної кваліфікаційної роботи.<br>Офіційний веб-сайт https://www.wunu.edu.ua/ містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти, тощо. |
| **9 – Академічна мобільність** | |
| **Національна кредитна мобільність** | Відповідно до угод ЗУНУ. |
| **Міжнародна кредитна мобільність** | Відповідно до угод ЗУНУ та угод про міжнародну академічну мобільність (Еразмус+ К1) |
| **Навчання іноземних здобувачів вищої освіти** | Відповідно до нормативно-правових документів. |

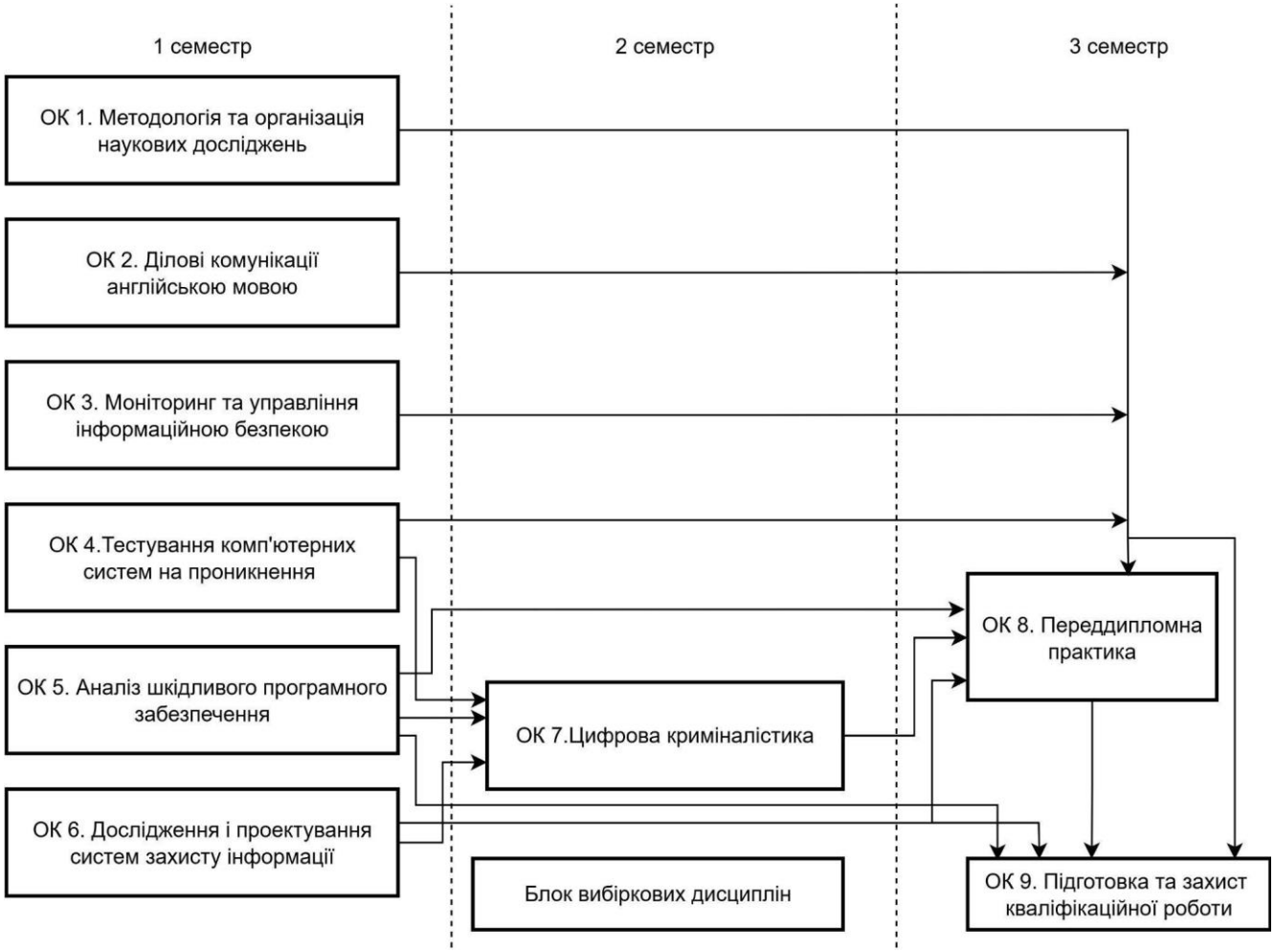
## 2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

### 2.1. Перелік компонентів ОП

| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів ЄКТС | Форма підсумкового контролю |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **Обов'язкові компоненти освітньої програми** | | | |
| **Цикл загальної підготовки** | | | |
| ОК 1 | Методологія наукових досліджень | 5 | залік |
| ОК 2 | Ділові комунікації англійською мовою | 5 | залік |
| **Цикл професійної підготовки** | | | |
| ОК 3 | Моніторинг та управління інформаційною безпекою | 5 | екзамен |
| ОК 4 | Цифрова криміналістика | 5 | екзамен |

| | | | |
|---|---|---|---|
| ОК 5 | Аналіз шкідливого програмного забезпечення | 5 | екзамен |
| ОК 6 | Дослідження і проектування систем захисту інформації | 5 | екзамен |
| ОК 7 | Тестування комп’ютерних систем на проникнення | 5 | екзамен |
| ОК 8 | Переддипломна практика | 15 | залік |
| ОК 9 | Підготовка та захист кваліфікаційної роботи | 15 | захист |
| **Загальний обсяг обов’язкових компонентів**: | | 65 | |
| **Загальний обсяг вибіркових компонентів:** | | 25 | |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** | | 90 | |

2.2. Структурно-логічна схема освітньо-професійної програми «Кібербезпека»



## 3. Форма атестації здобувачів вищої освіти

| | |
|---|---|
| **Форми 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.<br>Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.<br>Кваліфікаційна робота має бути розміщена у репозитарії ЗУНУ. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства. |

Таблиця 1

# Матриця відповідності компетентностей / результатів навчання дескрипторам НРК

| **Класифікація компетентностей (результатів навчання) за НРК** | **Знання**<br>**Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань | **Уміння/Навички Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур<br>**Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах<br>**Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності | **Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються | **Відповідальність і автономія АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів<br>**АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів<br>**АВ3** Здатність продовжувати навчання з високим ступенем автономії |
|---|---|---|---|---|
| **Загальні компетентності** | | | | |
| КЗ1 | Зн1, | Ум1, Ум3 | К1 | АВ1, АВ2 |
| КЗ2 | Зн1, | Ум1, Ум2, Ум3 | | АВ2, АВ3 |
| КЗ3 | Зн1 | Ум2, Ум3 | | АВ1 |
| КЗ4 | Зн1 | Ум3 | | АВ1, АВ2 |
| КЗ5 | Зн1 | Ум2 | К1 | АВ1 |
| **Спеціальні (фахові) компетентності** | | | | |
| КФ1 | Зн1 | Ум2 | | АВ2 |
| КФ2 | Зн1, | Ум2 | | АВ2 |
| КФ3 | Зн1 | Ум1, Ум2, Ум3 | К1 | АВ1, АВ2 |
| КФ4 | Зн1, | Ум1, Ум2 | К1 | АВ1, АВ2 |
| КФ5 | Зн1, | Ум1, Ум2 | К1 | АВ1, АВ2 |
| КФ6 | Зн1 | Ум1, Ум2 | К1 | АВ1 |
| КФ7 | Зн1 | Ум1, Ум2 | К1 | АВ1 |
| КФ8 | Зн1 | Ум1, Ум2 | К1 | АВ1 |
| КФ9 | Зн1 | Ум1, Ум2 | К1 | АВ1 |
| КФ10 | Зн1 | Ум1, Ум2, Ум3 | К1 | АВ1, АВ2 |
| КФ11 | Зн1 | Ум2 | К1 | АВ1 |

Таблиця 2

Матриця відповідності результатів навчання та компетентностей

| **Програмні результати навчання** | **Компетентності** | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Інтегральна компетентність** | | | | | | | | | | | | | | |
| | **Загальні компетентності** | | | | | **Спеціальні (фахові) компетентності** | | | | | | | | | |
| | КЗ1 | КЗ2 | КЗ3 | КЗ4 | КЗ5 | КФ1 | КФ2 | КФ3 | КФ4 | КФ5 | КФ6 | КФ7 | КФ8 | КФ9 | КФ10 | КФ11 |
| 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 | + | | + | + | | + | + | + | | | + | + | + | + | | |
| РН24 | + | | + | + | | | | | | | | | | | | + |

## 4. Матриця відповідності програмних компетентностей компонентам освітньої програми

| | ОК 1 | ОК 2 | ОК 3 | ОК 4 | ОК 5 | ОК6 | ОК 7 | ОК 8 | ОК 9 |
|---|---|---|---|---|---|---|---|---|---|
| **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** | | | + | | | | | + | + |
| **КФ10** | + | + | | | | | | + | + |
| **КФ11** | | | | | | | + | + | + |

## 5. Матриця забезпечення програмних результатів навчання (РН) відповідними компонентами освітньої програми

| РН / ОК | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 |
|---|---|---|---|---|---|---|---|---|---|
| РН1 | + | + | | | | | | + | + |
| РН2 | + | | | | + | + | | + | + |
| РН3 | + | | | | | + | | + | + |
| РН4 | | | | | | + | | + | + |
| РН5 | + | | | | | + | | + | + |
| РН6 | | | | + | + | | | + | + |
| РН7 | | | + | | | + | | + | + |
| РН8 | | | + | | | + | | + | + |
| РН9 | | | + | | | | | + | + |
| РН10 | | | | + | + | | | + | + |
| РН11 | | | + | + | | | | + | + |
| РН12 | | | | | + | | + | + | + |
| РН13 | | | | + | | + | | + | + |
| РН14 | | | + | | | | | + | + |
| РН15 | + | + | | | | | + | + | + |
| РН16 | | | + | | | | | + | + |
| РН17 | + | + | | | | | | + | + |
| РН18 | | | + | + | | | | + | + |
| РН19 | | | | | | + | + | + | + |
| РН20 | | | + | | | + | | + | + |
| РН21 | | | | | | + | | + | + |
| РН22 | + | | | + | | + | | + | + |
| РН23 | + | | + | + | | | | + | + |
| РН24 | | | | | | | + | + | + |