**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВЯ'ЗКУ ІМ. О.С. ПОПОВА**

ЗАТВЕРДЖЕНО

Ректор ОНАЗ ім. О.С. Попова
_____ П.П. Воробієнко
"___" _____ 2016 р.
М.П.

# ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

**РІВЕНЬ ВИЩОЇ ОСВІТИ** перший (бакалаврський) рівень
(назва рівня вищої освіти)

**СТУПІНЬ ВИЩОЇ ОСВІТИ** бакалавр
(назва ступеня вищої освіти)

**ГАЛУЗЬ ЗНАНЬ** 12 Інформаційні технології
(шифр та назва галузі знань)

**СПЕЦІАЛЬНІСТЬ** 125 Кібербезпека

Схвалено Вченою Радою
"29" 12 2016 р.
протокол № 5

Одеса – 2016

# ПЕРЕДМОВА

1. Розроблено робочою групою Навчально-наукового інституту Радіо, телебачення та інформаційної безпеки у складі:

**Керівник – Василіу Євген Вікторович**, доктор технічних наук за спеціальністю 05.13.21 – системи захисту інформації, професор, директор Навчально-наукового інституту Радіо, телебачення та інформаційної безпеки, професор кафедри Інформаційної безпеки та передачі даних Одеської національної академії зв'язку ім. О.С. Попова.

**Члени проектної групи:**

**Захарченко Микола Васильович** – доктор технічних наук, професор, завідувач кафедри Інформаційної безпеки та передачі даних Одеської національної академії зв'язку ім. О.С. Попова.

**Корчинський Володимир Вікторович** – доктор технічних наук, доцент, професор кафедри Інформаційної безпеки та передачі даних Одеської національної академії зв'язку ім. О.С. Попова.

**Онацький Олексій Віталійович** – кандидат технічних наук, доцент, доцент кафедри Інформаційної безпеки та передачі даних Одеської національної академії зв'язку ім. О.С. Попова.

# 1. Профіль освітньої програми зі спеціальності
# 125 Кібербезпека

| 1 – Загальна інформація | |
|---|---|
| **Повна назва вищого навчального закладу та структурного підрозділу** | Одеська національна академія зв'язку ім. О.С. Попова.<br>Навчально-науковий інститут Радіо, телебачення та інформаційної безпеки. |
| **Ступінь вищої освіти та назва кваліфікації мовою оригіналу** | Перший (бакалаврський) рівень.<br>Бакалавр з кібербезпеки. |
| **Офіційна назва освітньої програми** | Освітньо-професійна програма підготовки бакалаврів. |
| **Тип диплому та обсяг освітньої програми** | Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців (денна форма), 4 роки 10 місяців (заочна форма) |
| **Наявність акредитації** | Сертифікат акредитації напряму 6.170101 – Безпека інформаційних і комунікаційних систем НД-ІІ № 1679250 від 21.06.2016. Термін дії до 1.07.2021 р.<br>Сертифікат акредитації напряму 6.170102 – Системи технічного захисту інформації НД-ІІ № 1679594 від 21.06.2016. Термін дії до 1.07.2026 р. |
| **Цикл/рівень** | НРК України – 7 рівень |
| **Передумови** | Особа має право здобувати ступінь бакалавра за умови наявності в неї повної загальної середньої освіти. |
| **Мова(и) викладання** | Українська. |
| **Термін дії освітньої програми** | 1.07.2021 р. |
| **Інтернет-адреса постійного розміщення опису освітньої програми** | https://onat.edu.ua |
| **2 – Мета освітньої програми** | |
| Підготовка фахівця за освітнім ступенем бакалавр з кібербезпеки є правом подальшої професійної діяльності у системі державних та комерційних підприємств, пов'язаної з надання послуг щодо захисту інформації на об'єктах інформаційної діяльності | |
| **3 - Характеристика освітньої програми** | |
| **Предметна область** | Об'єкти професійної діяльності випускників:<br>– об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології;<br>– технології забезпечення безпеки інформації об'єктів різного рівня (система, об'єкт системи, компонент об'єкта), що пов'язані з інформаційними, інформаційно-комунікаційними технологіями, що використовуються для забезпечення функціонування цих об'єктів;<br>– процеси управління інформаційною і кібербезпекою об'єктів, що підлягають захисту.<br>Обов'язкові навчальні модулі – 73,3%, з них: дисципліни загальної підготовки – 10 %, професійної підготовки – 56,7%, практична |

| | |
|---|---|
| | підготовка – 16,7%, вивчення іноземної мови – 6,7%, дипломне проектування – 23,3%. Дисципліни вільного вибору студента – 26,7%, з них, що розширюють: загальні компетентності – 30%, професійні – 70%. |
| **Орієнтація освітньої програми** | Освітньо-професійна для бакалавра. Професійно-орієнтовані дисципліни забезпечують базові знання з усіх аспектів захисту інформації. |
| **Основний фокус освітньої програми та спеціалізації** | Загальна освіта зі спеціальності кібербезпеки. Акцент робиться на формуванні та розвитку професійних компетентностей щодо захисту інформації на об'єктах інформаційної діяльності; вивченні теоретичних та методичних положень, організаційних та практичних інструментів зі спеціальності кібербезпеки; методики та технології забезпечення безпеки інформації. |
| **Особливості програми** | Програма передбачає обов'язкове професійне навчання з метою отримання майбутнім фахівцем кваліфікації фахівця захисту інформації в інформаційних і комунікаційних системах.<br>Передбачена практика, з метою забезпечення умов підготовки фахівця в реальному середовищі майбутньої професійної діяльності.<br>Залучення до викладацької діяльності керівників та професіоналів, які працюють в системі професійної освіти та на виробництві в галузі захисту інформації, а також представників бізнесу, з метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу.<br>Реалізація процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін.<br>Рекомендується реалізація студентської мобільності, академічної співпраці та молодіжних обмінів. |
| **4 – Придатність випускників до працевлаштування та подальшого навчання** | |
| **Придатність до працевлаштування** | Випускник є придатним для працевлаштування на підприємствах, в організаціях та установах на яких обробляєтеся інформація з обмеженим доступом, що займаються розробкою та супроводом програмного забезпечення захисту інформації.<br>Посада: фахівець із організації інформаційної безпеки, код КП 3439. |
| **Подальше навчання** | Можливість навчатися за програмою другого циклу за цією ж галуззю знань або суміжною (що узгоджується з отриманим дипломом бакалавра).<br>Отримання другої вищої освіти (за наявності диплому бакалавра) за цією ж галуззю знань або суміжною (що узгоджується з отриманим дипломом бакалавра). |
| **5 – Викладання та оцінювання** | |
| **Викладання та навчання** | Використовується студенто-центроване та проблемно-орієнтоване навчання, навчання через практичну підготовку та самонавчання. Система методів навчання базується на принципах цілеспрямованості, бінарності – активної безпосередньої участі викладача і студента. Основними підходами при викладанні та навчанні є студенто-центризм, системність, технологічність, дискретність. Основні види занять: лекції, практичні заняття, лабораторна практика, самостійна робота, групові та індивідуальні консультації, розробка фахових проектів або робот. |

<table>
<tr><td>Оцінювання</td><td colspan="2">Модульно-рейтингова система оцінювання. Відповідність підсумкових рейтингових оцінок у балах оцінкам за національною шкалою і шкалою ECTS:
<table>
<tr><th>Оцінка за 100-баловою шкалою</th><th>Оцінка за національною шкалою</th><th>Оцінка за шкалою ЄКТС</th></tr>
<tr><td>90 – 100</td><td>відмінно</td><td>A</td></tr>
<tr><td>82 – 89</td><td rowspan="2">добре</td><td>B</td></tr>
<tr><td>74 – 81</td><td>C</td></tr>
<tr><td>64 – 73</td><td rowspan="2">задовільно</td><td>D</td></tr>
<tr><td>60 – 63</td><td>E</td></tr>
<tr><td>35 – 59</td><td rowspan="2">незадовільно</td><td>FX</td></tr>
<tr><td>0 – 34</td><td>F</td></tr>
</table>
Види контролю: вхідний, поточний, рубіжний, семестровий, державна атестація (бакалаврська кваліфікаційна робота).</td></tr>
<tr><td colspan="3">6 – Програмні компетентності</td></tr>
<tr><td>Інтегральна компетентність</td><td colspan="2">Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки, що характеризується комплексністю та неповною визначеністю умов.</td></tr>
<tr><td rowspan="12">Загальні компетентності (ЗК)</td><td>ЗК 1</td><td>Здатність працювати в команді.</td></tr>
<tr><td>ЗК 2</td><td>Здатність приймати обґрунтовані рішення.</td></tr>
<tr><td>ЗК 3</td><td>Вміння виявляти, ставити та вирішувати проблеми.</td></tr>
<tr><td>ЗК 4</td><td>Застосування базових знань на практиці.</td></tr>
<tr><td>ЗК 5</td><td>Здатність працювати в команді фахівців з різних підрозділів.</td></tr>
<tr><td>ЗК 6</td><td>Уміння працювати в міжнародному контексті.</td></tr>
<tr><td>ЗК 7</td><td>Здатність адаптуватися до нових ситуацій.</td></tr>
<tr><td>ЗК 8</td><td>Здатність бути критичним та самокритичним.</td></tr>
<tr><td>ЗК 9</td><td>Здатність до пошуку, оброблення та аналізу інформації з різних джерел.</td></tr>
<tr><td>ЗК 10</td><td>Здатність до самонавчання.</td></tr>
<tr><td>ЗК 11</td><td>Елементарні навички роботи з ПК.</td></tr>
<tr><td>ЗК 12</td><td>Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово.</td></tr>
<tr><td rowspan="7">Фахові компетентності спеціальності (ФК)</td><td>ФК 1</td><td>Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.</td></tr>
<tr><td>ФК 2</td><td>Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС, каналів зв'язку, систем управління процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації.</td></tr>
<tr><td>ФК 3</td><td>Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки.</td></tr>
<tr><td>ФК 4</td><td>Здатність здійснювати протидію несанкціонованому проникненню в інформаційно-телекомунікаційних системи і мережі.</td></tr>
<tr><td>ФК 5</td><td>Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об’єктів і систем.</td></tr>
<tr><td>ФК 6</td><td>Здатність відновлювати нормальне функціонування ІТС і мереж після здійснення кібернападів, збоїв та відмов.</td></tr>
</table>

| | | |
|---|---|---|
| **Фахові компетентності спеціальності (ФК)** | **ФК 7** | Здатність виконувати дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС. |
| | **ФК 8** | Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки. |
| | **ФК 9** | Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою. |
| | **ФК 10** | Здатність здійснювати управління інцидентами інформаційної та кібербезпеки. |
| | **ФК 11** | Здатність здійснювати управління ризиками інформаційної та кібербезпеки. |
| | **ФК 12** | Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій. |
| | **ФК 13** | Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники. |
| | **ФК 14** | Здатність проводити дослідження у практичній професійній діяльності. |

| **7 – Програмні результати навчання** | |
|---|---|
| | **Знання та розуміння:** |
| **ПРН 1** | Базові знання фундаментальних наук, в обсязі, необхідному для освоєння загально-професійних дисциплін. |
| **ПРН 2** | Знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації. |
| **ПРН 3** | Базові знання функціонування ІТ систем та мереж і їхніх компонентів. |
| **ПРН 4** | Базові знання законодавчої та нормативно-правової бази, а також вимог відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності. |
| **ПРН 5** | Базові знання з проектування (розробки) систем, технологій і засобів інформаційної безпеки. |
| **ПРН 6** | Базові знання з оцінювання стану інформаційної безпеки об'єктів і систем. |
| **ПРН 7** | Базові знання сучасних технічних і програмно-апаратних засобів захисту обробки інформації в ІТС. |
| **ПРН 8** | Базові знання методів протидії несанкціонованому проникненню в інформаційно-телекомунікаційних системи і мережі. |
| **ПРН 9** | Базові знання в галузі сучасних інформаційних технологій. |
| **ПРН 10** | Базові знання з проектування комплексної системи захисту інформації ІТС. |
| **ПРН 11** | Базові знання з криптографіческих методів захисту інформації. |
| **ПРН 12** | Базові знання з організаційного забезпечення технічного захисту інформації на об'єктах інформаційної діяльності. |
| | **Застосування знань та розумінь:** |
| **ПРН 13** | Здатність удосконалювати і розвивати свій інтелектуальний і загальнокультурний рівень, самостійно навчатись новим методам дослідження, до змін наукового і науково-виробничого профілю в своїй професійній діяльності. |
| **ПРН 14** | Вибирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів ІБ щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки. |
| **ПРН 15** | Проектувати та реалізувати комплексну систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації. |

| | |
|---|---|
| **ПРН 16** | Використовувати інструментальні засоби оцінки наявних вразливостей. |
| **ПРН 17** | Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах. |
| **ПРН 18** | Вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень. |
| **ПРН 19** | Здійснювати оцінку захищеності ІТ систем та мереж. |
| **ПРН 20** | Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей. |
| **ПРН 21** | Здійснювати організацію робіт з технічного захисту інформації на об'єктах інформаційної діяльності. |
| **ПРН 22** | Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем. |
| **ПРН 23** | Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації |
| **ПРН 24** | Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки |
| **ПРН 25** | Застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки |

| **8 – Ресурсне забезпечення реалізації програми** | |
|---|---|
| **Кадрове забезпечення** | Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. В процесі організації навчального процесу залучаються професіонали з досвідом дослідницької/управлінської/інноваційної/творчої роботи та/або роботи за фахом. |
| **Матеріально-технічне забезпечення** | Матеріально-технічне забезпечення дозволяє повністю забезпечити освітній процес протягом всього циклу підготовки за освітньою програмою. Стан приміщень засвідчено санітарно-технічними паспортами, що відповідають існуючим нормативним актам. |
| **Інформаційне та навчально-методичне забезпечення** | Програма повністю забезпечена комплексом методичної літератури, розробленої викладачами кафедр академій: підручниками, навчальними посібниками та методичними вказівками як друкованими, так і в електронному вигляді, наявність яких представлена у електронної бібліотеки академії – https://onat.edu.ua/biblioteka/ |
| **9 – Академічна мобільність** | |
| **Національна кредитна мобільність** | Передбачає можливість національної кредитної мобільності за деякими навчальними модулями, що забезпечують набуття загальних компетентностей. |
| **Міжнародна кредитна мобільність** | 1. Agreement of co-operation Between University of Bielsko-Biala, Poland and Odessa National Academy of Telecommunications n.a. O.S. Popov (29.03.2017)<br>2. Договор о сотрудничестве с Казахским национальным техническим университетом им. К.И. Сатпаева (12.09.2016)<br>3. Договор о сотрудничестве с учреждением образования «Белорусская государственная академия связи» (23.10.2015) |
| **Навчання іноземних здобувачів вищої освіти** | Основні навчальні модулі програми забезпечені комплексом методичної літератури для іноземних студентів російською та англійською мовою/мовами. |

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

### 2.1 Перелік компонент ОП

| 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 1 | Історія України, української культури | 5 | Залік |
| ОК 2 | Українська мова (за професійним спрямуванням) | 3 | Залік |
| ОК 3 | Філософія | 3 | Екзамен |
| ОК 4 | Іноземна мова | 5 | Екзамен |
| ОК 5 | Вища математика | 20 | Екзамен |
| ОК 6 | Фізика | 11 | Екзамен |
| ОК 7 | Інформаційні технології | 5 | Екзамен |
| ОК 8 | Теорія ймовірностей і мат. статистика | 3 | Екзамен |
| ОК 9 | Дискретна математика | 3 | Залік |
| ОК 10 | Технології програмування | 12 | Екзамен |
| ОК 11 | Основи теорія кіл, сигналів та процесів в електроніці | 4 | Екзамен |
| ОК 12 | Операційні системи | 4 | Залік |
| ОК 13 | Електроніка | 4 | Залік |
| ОК 14 | Архітектура комп'ютерних систем | 3 | Екзамен |
| ОК 15 | Інформаційно-комунікаційні системи | 9 | Екзамен |
| ОК 16 | Теорія інформації та кодування | 6 | Екзамен |
| ОК 17 | Прикладна криптологія | 9 | Екзамен |
| ОК 18 | Нормативно-правове забезпечення інформаційної безпеки | 3 | Залік |
| ОК 19 | Системи технічного захисту інформації | 4 | Екзамен |
| ОК 20 | Захист інформації в інформаційно-комунікаційних системах | 11 | Екзамен |
| ОК 21 | Комплексні системи захисту інформації. Проектування, впровадження, супровід | 10 | Екзамен |
| ОК 22 | Управління інформаційною безпекою | 3 | Залік |
| ОК 23 | Екологія | 3 | Залік |
| ОК 24 | Автоматизовані системи моніторингу надзвичайних ситуацій та безпека життєдіяльності | 3 | Залік |
| ОК 25 | Ознайомлювальна практика | 4 | Залік |
| ОК 26 | Технологічна практика | 4 | Залік |
| ОК 27 | Експлуатаційна практика | 5 | Залік |
| ОК 28 | Виробнича практика | 5 | Залік |
| ОК 29 | Підготовка та захист атестаційної роботи | 8 | Захист роб. |
| **Загальний обсяг обов'язкових компонент:** | | **172** | |
| **Вибіркові компоненти ОП** | | | |
| ВБ 1.1 | Економіка | 3 | Екзамен |
| ВБ 1.2 | Соціологія, політологія | 3 | Залік |
| ВБ 1.3 | Іноземна мова (за професійним спрямуванням) | 5 | залік |
| ВБ 1.4 | Технічна графіка | 3 | Залік |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| ВБ 1.5 | Створення та обробка баз даних | 4 | Екзамен |
| ВБ 1.6 | Основи інформаційної безпеки держави | 3 | Залік |
| ВБ 1.7 | Цифрова обробка сигналів | 3 | Залік |
| ВБ 1.8 | Організаційне забезпечення технічного захисту інформації | 4 | Залік |
| ВБ 1.9 | Технічні засоби охорони об’єктів | 6 | Екзамен |
| ВБ 1.10 | Методи та засоби захисту інформації | 5 | Екзамен |
| ВБ 1.11 | Метрологія та вимірювання | 3 | Залік |
| ВБ 1.12 | Програмування механізмів інформаційної безпеки | 4 | Екзамен |
| ВБ 1.13 | Кібербезпека інфокомунікацій | 4 | Залік |
| ВБ 1.14 | Основи комп’ютерної стеганографії | 4 | Екзамен |
| ВБ 1.15 | Системи банківської безпеки | 5 | Екзамен |
| ВБ 1.16 | Аудит інформаційної безпеки | 3 | Залік |
| ВБ 1.17 | Компонентна база засобів технічного захисту інформації | 3 | Залік |
| ВБ 1.18 | Безпека технологій електронного документообігу | 3 | Екзамен |
| **Загальний обсяг вибіркових компонент:** | | **68** | |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** | | **240** | |

## 2.2 Структурно-логічна схема ОП

Структурно-логічна схема підготовки фахівця рівня бакалавр за спеціальністю 125 Кібербезпека

| **І курс** | | **ІІ курс** | | **ІІІ курс** | | **IV курс** | |
|---|---|---|---|---|---|---|---|
| **1.1** | **1.2** | **2.1** | **2.2** | **3.1** | **3.2** | **4.1** | **4.2** |
| **І. Обов’язкові дисципліни** | | | | | | | |
| **1.1. Цикл гуманітарної підготовки** | | | | | | | |
| Іноземна мова | | Українська мова (за проф. спрям.) | | Соціологія та політологія | | | |
| Філософія | | | | | | | |
| Історія України, української культури | | | | | | | |
| | | | | | | | |
| **1.2. Цикл фундаментальної підготовки** | | | | | | | |
| Інформаційні технології | | Дискретна математика | Теорія ймовірності і мат. стат. | | | | |
| Вища математика | | | | | | | |
| Фізика | | | | | | | |
| **1.3. Цикл професійної підготовки** | | | | | | | |
| | Технології програмування | | | Нормативно-правове забезпечення інформаційної безпеки | Системи технічного захисту інформації | Прикладна криптологія | |
| | Основи теорії кіл, сигналів та процесів в електроніці | Електроніка | Операційні системи | | Автоматизовані системи моніторингу надзвичайних ситуацій та безпека життєдіяльн. | Комплексні системи захисту інформації: Проектування, впровадження, супровід | |

| 1.1 | 1.2 | 2.1 | 2.2 | 3.1 | 3.2 | 4.1 | 4.2 |
|---|---|---|---|---|---|---|---|
| | | Архітектура комп'ютерних систем | | Інформаційно-комунікаційні системи | | Управління інформаційної безпекою | |
| | | | Теорія інформації та кодування | | | | |
| | | | | Захист інформації в інформаційно-комунікаційних системах | | | |
| | | | | | | | |
| **ІІ. Вибіркові дисципліни** | | | | | | | |
| **2.1. Дисципліни гуманітарної підготовки** | | | | | | | |
| | | Іноземна мова (за проф. спрямуванням) | | | | | Екологія |
| | | | Економіка | | | | |
| **2.2. Цикл фундаментальної підготовки** | | | | | | | |
| Технічна графіка | Компонент. база засобів технічного захисту інформації | Метрологія та вимірювання | Кібербезпека інфоком. | Створення та обробка баз даних | Програмування механізмів інформаційної безпеки | Аудит інформаційної безпеки | |
| | | | | | | | |
| | | | | Безпека технологій електрон. документо-обігу | | | |
| **2.3. Цикл професійної підготовки** | | | | | | | |
| | Основи інформаційної безпеки держави | | | Цифрова обробка сигналів | Організаційне забезпечення технічного захисту інформації | Методи та засоби захисту інформації | Технічні засоби охорони об'єктів |
| | | | | | | Основи комп'ютерної стегано-графії | |
| | | | | | | Системи банківської безпеки | |
| **ІІІ. Практична підготовка** | | | | | | | |
| | Ознайом-лювальна практика | | Технологічна практика | | Експлуатаційна практика | | Виробнича практика, науково-дослідна робота та виконання випускної роботи |

## 3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 Кібербезпека проводиться у формі захисту кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації – бакалавр з кібербезпеки.

Атестація здійснюється відкрито і публічно.

## 4. Матриця відповідності програмних компетентностей компонентам освітньої програми

| | 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 | ОК 17 | ОК 18 | ОК 19 | ОК 20 | ОК 21 | ОК 22 | ОК 23 | ОК 24 | ОК 25 | ОК 26 | ОК 27 | ОК 28 | ОК 29 | ВБ 1.1 | ВБ 1.2 | ВБ 1.3 | ВБ 1.4 | ВБ 1.5 | ВБ 1.6 | ВБ 1.7 | ВБ 1.8 | ВБ 1.9 | ВБ 1.10 | ВБ 1.11 | ВБ 1.12 | ВБ 1.13 | ВБ 1.14 | ВБ 1.15 | ВБ 1.16 | ВБ 1.17 | ВБ 1.18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ЗК 1** | • | • | | • | | • | • | | | • | • | • | • | • | • | • | • | | • | • | • | • | | • | • | • | • | • | | • | • | | | • | | | • | | | | | | | | | |
| **ЗК 2** | • | • | • | | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | | • | • | • | • | • | • | | • | • | • | • | • | • | • |
| **ЗК 3** | • | • | • | | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | | • | • | • | • | • | • | | • | • | • | • | • | • | • |
| **ЗК 4** | | | | | | | | | | | | | | | | | | | | | | | | • | • | • | • | | | | | | • | | | • | • | • | • | • | • | • | • | • | • | • |
| **ЗК 5** | • | • | | • | | • | • | | | • | • | • | • | • | • | • | • | | • | • | • | • | | • | • | • | • | • | | • | • | | | • | | | • | | | | | | | | | |
| **ЗК 6** | | | | • | | | • | | | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | | | • | | | | | | • | | | • | • | | • | • | | • |
| **ЗК 7** | | | | • | | | • | | | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | | | | • | | | • | • | • | | • | • | • | • | • | • | • |
| **ЗК 8** | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • |
| **ЗК 9** | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • |
| **ЗК 10** | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • |
| **ЗК 11** | | | | | | | • | • | | • | • | • | • | • | • | • | • | • | • | • | • | • | | • | • | • | • | • | | | | • | • | | | | | | | | | • | | | | | • |
| **ЗК 12** | • | • | | • | | | | | | | | | | | | | | | | | | | | | | | | | | | | • | | | | | | | | | | | | | | | |
| **ФК 1** | | | | | | | | | | | | | | • | • | | | • | • | • | • | • | • | • | | • | • | • | • | | | | | | • | | • | | | | | | | • | | |
| **ФК 2** | | | | | | | • | | | • | | • | | • | | • | | | | • | • | • | | | | • | • | • | • | | | | | • | | | | | | | | • | | | • | | • |
| **ФК 3** | | | | | | | | | | | | | | • | • | | • | | | • | • | • | | | | | • | • | • | | | | | | • | | | | • | • | | • | • | | • | | | • |
| **ФК 4** | | | | | | | | | | | | | | | | | • | | • | • | • | • | | | | • | • | • | • | | | | | | | | • | | • | | | • | • | | • | • | | • |
| **ФК 5** | | | | | | | | | | | | | | | | | • | | • | • | • | • | | | | • | • | • | • | | | | | | | | • | • | • | | | • | | | • | | | |
| **ФК 6** | | | | | | | | | | | | | | | | | • | | • | • | • | • | | | | • | • | • | • | | | | | | | | • | | | | | • | | | • | | | |
| **ФК 7** | | | | | | | | | | | | | | | • | | • | | • | • | • | • | | | | • | • | • | • | | | | | | | | | • | • | | | • | | | • | | | |
| **ФК 8** | | | | | | | | | | | | | | | • | | • | • | • | • | • | • | | | | • | • | • | • | | | | | | | | | • | • | | | | | | • | | | |
| **ФК 9** | | | | | | | • | | | | | • | | • | • | | • | • | • | • | • | • | | | | • | • | • | • | | | | | | | | • | • | | | • | | | • | | | |
| **ФК 10** | | | | | | | • | | | | | • | | • | • | | • | • | • | • | • | • | | | | • | • | • | • | | | | | | | | | | | | | • | | | • | | | |
| **ФК 11** | | | | | | | • | | | | | • | | • | • | | • | • | • | • | • | • | | | | • | • | • | • | | | | | | | | | | | | | • | | | • | | | |
| **ФК 12** | | | | | | | • | | | | | • | | • | • | | • | • | • | • | • | • | | • | | • | • | • | • | | | | | | | | | | | | | • | | | • | | | • |
| **ФК 13** | | | | | | | • | | | | | • | | • | • | | • | • | • | • | • | • | | • | | • | • | • | • | | | | | | | | | • | • | | | • | | | • | | | • |
| **ФК 14** | | | | • | | | • | | | • | | | | • | • | • | • | • | • | • | • | • | | | | • | • | • | • | | | | | | | | | • | • | | • | • | | • | • | | |

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

| | 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 | ОК 17 | ОК 18 | ОК 19 | ОК 20 | ОК 21 | ОК 22 | ОК 23 | ОК 24 | ОК 25 | ОК 26 | ОК 27 | ОК 28 | ОК 29 | ВБ 1.1 | ВБ 1.2 | ВБ 1.3 | ВБ 1.4 | ВБ 1.5 | ВБ 1.6 | ВБ 1.7 | | ВБ 1.8 | ВБ 1.9 | ВБ 1.10 | ВБ 1.11 | ВБ 1.12 | ВБ 1.13 | ВБ 1.14 | ВБ 1.15 | ВБ 1.16 | ВБ 1.17 | ВБ 1.18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПРН 1** | • | • | • | • | • | • | | • | • | • | • | | | | | | | | | | | | • | | | | | | • | • | | • | • | | | | | | | | | • | | | | | | |
| **ПРН 2** | | • | | • | | | | | | | | | | | | | | | | | | | | | | | | | | | • | | | | | | | | | | | | | | | | | |
| **ПРН 3** | | | | | | | • | | | • | | • | | • | • | | | | | • | • | • | | | • | • | • | • | • | | | | | | | | | | | | | | • | | | | | |
| **ПРН 4** | | | | | | | | | | | | | | | | | | • | | | • | • | | • | • | • | • | • | • | | | | | | • | | | • | | | | | | • | | | | | |
| **ПРН 5** | | | | | | | | | | | | | | • | • | | • | | • | • | • | • | | • | | | | • | • | | | | | | | | | | • | • | | | | • | • | | | | | • |
| **ПРН 6** | | | | | | | | | | | | | | | | | | | • | • | • | • | | | • | • | • | • | • | | | | | | | | | • | | | | • | • | | | • | • | | • |
| **ПРН 7** | | | | | | | | | | | | | | • | • | | | | • | • | | | | | • | • | • | • | • | | | | | | | | | | • | • | | • | • | | • | | • | |
| **ПРН 8** | | | | | | | | | | | | | | | | | • | | • | • | • | • | | | | • | • | • | • | | | | | | | | | • | | • | | | • | | • | • | | • |
| **ПРН 9** | | | | | | | • | | | • | • | • | • | • | | • | | | | | | | | | | • | • | • | • | | | | | • | | • | | | | | | | | | | | |
| **ПРН 10** | | | | | | | | | | | | | | | • | | | • | • | • | • | | | | | | | • | • | | | | | | | | | • | • | • | | | | | | | | |
| **ПРН 11** | | | | | | | | | | | | | | | | • | • | | | • | | | | | | | | • | • | | | | | | | | | | | | • | | • | • | | | | |
| **ПРН 12** | | | | | | | | | | | | | | | | | | • | | • | • | • | | | | • | • | • | • | | | | | | | | | • | | | | | • | | | • | | • |
| **ПРН 13** | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | | • | • | • | • | • | • | • | • | • | • | • |
| **ПРН 14** | | | | | | | | | | | | | | | • | | | • | | • | • | • | | | | | | • | • | | | • | | | • | | | | | | | | | | | | • |
| **ПРН 15** | | | | | | | | | | | | | | • | • | | | • | • | • | • | • | | | | | | • | • | | | | | | • | | | | • | • | • | | | • | | • | • | | |
| **ПРН 16** | | | | | | | | | | | | | | | | | | | • | • | • | • | | | | | | • | • | | | | | | | | | | | | • | | | • | | | • | | |
| **ПРН 17** | | | | | | | | | | | | | | | • | • | | | | • | • | • | | | | | | • | • | | | | | | | | | | | • | • | | | • | | | | | |
| **ПРН 18** | | | | | | | | | | | | | | • | • | | | | • | • | • | • | | | | | | • | • | | | | | | | | | | | | | | | | | | | | |
| **ПРН 19** | | | | | | | | | | | | | | | • | | | | • | • | • | • | | | | | | | • | | | | | | | | | | | • | | | • | | | • | • | | |
| **ПРН 20** | | | | | | | | | | | | | | | • | | | | • | • | • | • | | | | | | | • | | | | | | | | | | | • | | | • | | | • | • | | |
| **ПРН 21** | | | | | | | | | | | | | | | | | | • | | • | • | • | | | | • | • | • | • | | | | | | | | | | • | | | | | • | | | • | | • |
| **ПРН 22** | | | | | | | | | | | | | | | • | | | • | | • | • | • | | | | • | • | • | • | | | | | | • | | | | • | | | | | • | | • | • | | • |
| **ПРН 23** | | | | | | | • | | | | | | | • | • | | | | | • | • | • | | | | | | • | • | | | | | | | | | | • | | | | | • | | • | | | |
| **ПРН 24** | | | | | | | • | | | | | | | • | • | | | | | • | • | • | | | | | | • | • | | | | | | | | | | • | | | | | • | | • | | | |
| **ПРН 25** | | | | | | | | | | | | | | | | | | | | | | • | | | | | • | • | • | | | | | | | | | | • | | | | | • | | • | • | | |