МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ІМ.О.С. ПОПОВА

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

Другого рівня вищої освіти

за спеціальністю № 125 Кібербезпека

галузі знань № 12 Інформаційні технології

Кваліфікація: 2149.2 – Професіонал із організації інформаційної безпеки

ЗАТВЕРДЖЕНО
Вченою радою
ОНАЗ ім. О.С. Попова
Голова Вченої ради

_____ / Воробієнко П.П. /

(протокол № 1 від "22" серпня 2017 р.)

Освітня програма вводиться в дію з 1 вересня 2017 р.

Ректор ОНАЗ ім. О.С. Попова

_____ / Воробієнко П. П.

(наказ № 01-05-231а від "23" 08 2017 р.)

Одеса 2017

ПЕРЕДМОВА

Розроблено робочою групою Навчально-наукового інституту Радіо, телебачення та інформаційної безпеки ОНАЗ ім. О.С. Попова у складі:

Керівник – Васіліу 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, доцент кафедри Інформаційної безпеки та передачі даних Одеської національної академії зв'язку ім. О.С. Попова.

Кільдішев Віталій Йосипович – кандидат технічних наук, доцент, доцент кафедри Інформаційної безпеки та передачі даних Одеської національної академії зв'язку ім. О.С. Попова.

Рецензії-відгуки зовнішних стейкголдерів:

1. **Дігол С.О.**, директор ТОВ «Гофер Корпорейшн»

2. **Шкурупій О.В.**, директор ТОВ «ЄВРО Україна ЛТД»

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; Навчально-наукового інституту Радіо, телебачення та інформаційної безпеки.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Другий (магістерський) рівень. 2149.2 – Професіонал із організації інформаційної безпеки
Офіційна назва освітньої програми	Освітньо-професійна програма підготовки магістрів
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 5 місяців.
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. 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 – 8 рівень
Передумови	Особа має право здобувати ступінь магістра за умови наявності в неї ступеня бакалавра.
Мова(и) викладання	Українська
Термін дії освітньої програми	1.07.2022 р.
Інтернет-адреса постійного розміщення опису освітньої програми	https://onat.edu.ua
2 – Мета освітньої програми	
Забезпечити студентам здобуття знань, умінь та розуміння, що відносяться до області технологій, засобів та організації безпеки інформаційних і комунікаційних систем державних та комерційних підприємств.	
3 - Характеристика освітньої програми	
Предметна область	Об'єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології; – 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; – процеси управління інформаційною і кібербезпекою об'єктів, що підлягають захисту. 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%, магістерська робота – 23,3%. Дисципліни вільного вибору студента – 26,7%, з

<table>
<tr><td></td><td>них, що розширюють: загальні компетентності – 30%, професійні – 70%.</td></tr>
<tr><td>Орієнтація освітньої програми</td><td>Освітньо-професійна для магістра. Дослідницька лінія є науково орієнтована, викладацька лінія є практично орієнтована, інші лінії є практично орієнтованими.</td></tr>
<tr><td>Основний фокус освітньої програми та спеціалізації</td><td>Дослідницька лінія програми має спеціалізації в областях: технологій, засобів та організації безпеки інформаційних і комунікаційних систем; технології і засобів захисту та охорони інформаційних ресурсів і баз даних обмеженого доступу.</td></tr>
<tr><td>Особливості програми</td><td>Програма передбачає обов’язкове професійне навчання з метою отримання майбутнім фахівцем кваліфікації фахівця професіонал із організації інформаційної безпеки.
Передбачена практика, з метою забезпечення умов підготовки фахівця в реальному середовищі майбутньої професійної діяльності.
Залучення до викладацької діяльності керівників та професіоналів, які працюють в системі професійної освіти та на виробництві в галузі телекомунікацій, а також представників бізнесу, з метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу.
Реалізація процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін.
Рекомендується реалізація студентської мобільності, академічної співпраці та молодіжних обмінів.
Програма також викладається англійською мовою.</td></tr>
<tr><td colspan="2">4 – Придатність випускників до працевлаштування та подальшого навчання</td></tr>
<tr><td>Придатність до працевлаштування</td><td>Випускник є придатним для працевлаштування в вищих навчальних закладах або наукових організаціях, наукові посади у сфері комунікації, управління та дослідження: державні установи, малі підприємства та інститути, силові структури, ІТ-компанії, посади викладачів у коледжах та інше.</td></tr>
<tr><td>Подальше навчання</td><td>Навчання в аспірантурі</td></tr>
<tr><td colspan="2">5 – Викладання та оцінювання</td></tr>
<tr><td>Викладання та навчання</td><td>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.</td></tr>
<tr><td>Оцінювання</td><td>Модульно-рейтингова система оцінювання. Письмові та усні екзамени, заліки, лабораторні звіти, усні презентації, поточний контроль, захист звіту з практики, есе, публічний захист кваліфікаційної роботи.
*Відповідність підсумкових рейтингових оцінок у балах оцінкам за національною шкалою і шкалою ECTS:
<table>
<tr><td>Оцінка за 100-баловою шкалою</td><td>Оцінка за національною шкалою</td><td>Оцінка за шкалою ЄКТС</td></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>
</table></td></tr>
</table>

<table>
<tr><td></td><td colspan="3">
<table>
<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 (магістерська кваліфікаційна робота).
</td></tr>
<tr><td colspan="4">6 – Програмні компетентності</td></tr>
<tr><td>Інтегральна компетентність</td><td colspan="3">Здатність до успішного засвоєння складніших програм в рамках спеціалізації для наукових дослідників та розробників, проектантів, експертів, викладачів, наукових менеджерів у бізнесових структурах, наукових робітників та викладачів для вищих навчальних закладів в області технологій, засобів та організації безпеки інформаційних і комунікаційних систем.</td></tr>
<tr><td rowspan="14">Загальні компетентності (ЗК)</td><td>ЗК 1</td><td colspan="2">Здатність гнучкого способу мислення та застосовувати знання у практичних ситуаціях.</td></tr>
<tr><td>ЗК 2</td><td colspan="2">Знання та розуміння предметної області та розуміння професії.</td></tr>
<tr><td>ЗК 3</td><td colspan="2">Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово</td></tr>
<tr><td>ЗК 4</td><td colspan="2">Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки</td></tr>
<tr><td>ЗК 5</td><td colspan="2">Вміння виявляти, ставити та вирішувати наукові та практичні проблеми.</td></tr>
<tr><td>ЗК 6</td><td colspan="2">Здатність до пошуку, оброблення та аналізу інформації з різних джерел.</td></tr>
<tr><td>ЗК 7</td><td colspan="2">Навички міжособистісної взаємодії.</td></tr>
<tr><td>ЗК 8</td><td colspan="2">Прагнення до збереження навколишнього середовища</td></tr>
<tr><td>ЗК 9</td><td colspan="2">Здатність до пошуку, оброблення та аналізу інформації з різних джерел.</td></tr>
<tr><td>ЗК 10</td><td colspan="2">Здатність діяти соціально відповідально та громадянсько свідомо</td></tr>
<tr><td>ЗК 11</td><td colspan="2">Здатність вчитися і бути сучасно навченим</td></tr>
<tr><td>ЗК 12</td><td colspan="2">Здатність приймати обґрунтовані рішення</td></tr>
<tr><td>ЗК 13</td><td colspan="2">Дотримання здорового способу життя</td></tr>
<tr><td>ЗК 14</td><td colspan="2">Здатність бути критичним та самокритичним</td></tr>
<tr><td rowspan="5">Спеціальні компетентності</td><td>ФК 1</td><td colspan="2">Здатність вибирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки.</td></tr>
<tr><td>ФК 2</td><td colspan="2">Здатність формулювати, аналізувати та синтезувати рішення наукових задач і проблем на абстрактному рівні шляхом декомпозиції їх на складові, які можна дослідити окремо в їх більш та менш важливих аспектах.</td></tr>
<tr><td>ФК 3</td><td colspan="2">Здатність будувати та оцінювати на основі сучасних принципів, способів та методів теорії захищених систем моделі загроз, порушника, політики безпеки, досліджувати їх для отримання нових висновків та поглибленого розуміння.</td></tr>
<tr><td>ФК 4</td><td colspan="2">Здатність розробляти і впроваджувати комп’ютерні програми та використовувати існуючі.</td></tr>
<tr><td>ФК 5</td><td colspan="2">Здатність комунікувати з колегами з інформаційної безпеки щодо наукових досягнень, як на загальному рівні, так і на</td></tr>
</table>

Фахові компетентності спеціальності (ФК)		рівні спеціалістів, здатність робити усні та письмові звіти, обговорювати наукові теми рідною та англійською мовами.
	ФК 6	Здатність формулювати (роблячи презентації або представляючи звіти) нові гіпотези та наукові задачі в області інформаційної безпеки. Вибирати належні напрями і відповідні методи для їх розв'язання, беручи до уваги наявні ресурси.
	ФК 7	Здатність розробляти та впровадити комплексну систему захисту інформації, що протидіє багатьом різним за природою загрозам (кібератаки з боку інсайдерів та хакерів, злам програм, віруси, перехоплення трафіку, помилки тощо).
	ФК 8	Здатність сприймати ново здобуті знання в області технологій та засобів кібербезпеки та інтегрувати їх із уже наявними. Здатність зорієнтуватися на рівні спеціаліста в певній вузькій області знань кібербезпеки, яка лежить поза межами обраної спеціалізації.
	ФК 9	Здатність ефективно використовувати на практиці різні теорії в області комунікації.
	ФК 10	Здатність розуміти шляхи практичного використання комунікаційних навичок, ефективно застосовуючи комунікаційні концепції.
	ФК 11	Розуміння факторів, які мають позитивний чи негативний вплив на комунікацію та здатність визначити та врахувати ці фактори в конкретних комунікаційних ситуаціях.
	ФК 12	Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж.
	ФК 13	Здатність аналізувати шляхи якими викладацькі навички використовуються на практиці, ефективно застосовуючи основні педагогічні концепції.
	ФК 14	Здатність бути наставником молодших колег у вдосконаленні викладацької майстерності.
	ФК 15	Здатність аналізувати та формулювати висновки (діагноз) для різних типів складних управлінських задач у наукових установах.
	ФК 16	Здатність ефективно використовувати на практиці різні теорії в управлінні наукою та в області ділового адміністрування.
	ФК 17	Здатність виконувати літературний пошук джерел, які мають відношення до цих теорій, здатність їх критично оцінювати, базуючись на фахових у цих областях статтях.
7 – Програмні результати навчання		
	Знання та розуміння:	
ПРН 1	Базові знання діючих державних та міжнародних стандартів, що пред'являються до інформаційної безпеки інформаційно-комунікаційних систем.	
ПРН 2	Вміння готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки інформаційно-комунікаційних систем	
ПРН 3	Розуміння відповідних розділів статистичного аналізу для синтезу існуючих та нових принципів побудови систем інформаційної безпеки інфокомунікацій.	
ПРН 4	Розуміння комп'ютерних технологій для моделювання процесів на основі сучасних принципів, способів та методів теорії захищених систем моделей загроз, моделей порушника, моделей політики безпеки з метою досліджування їх для отримання нових висновків та поглибленого аналізу;	
ПРН 5	Знання вимоги до математичних моделей проектованого об'єкта.	

ПРН 6	Знання основ проектних процедури та принципів проектування складних технічних систем, принципів побудови систем автоматизованого проектування;
ПРН 7	Знання методів створення систем моніторингу безпеки в інфокомунікаційних системах та мережах;
ПРН 8	Знання основи проведення аудиту безпеки інформаційних і комунікаційних систем
ПРН 9	Розуміння основних методів захисту інформації, що зберігається та передається в електронних платіжних системах;
ПРН 10	Знання методів автентифікації, зокрема електронний цифровий підпис.
ПРН 11	знання протоколів використання електронних грошей;
ПРН 12	Розуміння методів створення атак на сучасні системи захисту інформації;
ПРН 13	Розуміння методів розробки криптоситем стійких до різноманітних видів атак
ПРН 14	Розуміння основних принципів і загальних правил ліцензування, атестації та сертифікації в галузі ТЗІ.
ПРН 15	Розуміння головних аспектів використання шумоподібних сигналів для захисту конфіденційної інформації.
	Застосування знань та розумінь:
ПРН 16	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 17	Володіти достатніми науковими навичками в технологіях, засобах та організаційних заходах інформаційної безпеки інформаційно-комунікаційних систем та мереж (ІКСМ) для того, щоб успішно проводити наукові дослідження під наглядом наукового наставника, при цьому:
ПРН 18	Використовувати знання сутності, принципів, методів, особливостей наукового пізнання для вивчення і розв’язання проблем забезпечення інформаційної безпеки та захисту інформації, розвивати творче, діалектичне мислення та наукове передбачення роз витку процесів та явищ у галузі інформаційної безпеки та захисту інформації;
ПРН 19	Здатність брати участь в наукових розробках методів захисту інформації для ІКСМ та її компонентів.
ПРН 20	Здатність планувати та проводити експериментальні дослідження з метою визначення оцінки ефективності функціонування об’єктів ІКСМ з урахуванням ризиків, моделей порушника та загроз, моделі і політики безпеки, а також враховуючи сучасні принципи, способи та методи теорії захищених систем.
ПРН 21	Здійснювати на основі системного підходу та знань теорії інформаційної безпеки оптимальні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій.
ПРН 22	Здійснювати перевірку об’єктів інформаційної діяльності (ОІД) і технічних засобів.
ПРН 23	Здійснювати оцінку захищеності ОІД по технічних каналах витоку інформації, виявляти закладні пристрої та засоби схованого відеоспостереження
ПРН 24	Здійснювати документальне оформлення протоколів спецдослідження або перевірки захищеності виділеного приміщення різної категорії.
ПРН 25	Здійснювати розроблення методик аналізу, синтезу, оптимізації та прогнозування якості процесів захисту інформації з обмеженим доступом на об’єктах інформаційної діяльності.
ПРН 26	Здатність застосовувати шумоподібні сигнали для захисту інформації та оцінювати рівень завадозахищеності систем зв’язку.
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) 2. Договор о сотрудничестве с Казахским национальным техническим университетом им. К.И. Сатпаева (12.09.2016) 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/наукової 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. ОБОВ'ЯЗКОВІ ДИСЦИПЛІНИ			
1.1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1.1.1. Цикл гуманітарної підготовки (180 годин/6 кредитів)			
ОК 1.	Охорона праці в галузі	3	Залік
ОК 2.	Цивільний захист	3	Залік
1.1.2 Цикл фундаментальної підготовки (330 годин/11 кредитів)			
ОК 3.	Математичні методи моделювання та оптимізації процесів	4	Залік
ОК 4.	Моделювання та організація наукових досліджень	3	Залік
ОК 5.	Система менеджменту інформаційної безпеки	4	Залік
1.2 Цикл професійної підготовки (840 годин/28 кредитів)			
ОК 6.	Ліцензування, атестація та сертифікація в галузі ТЗІ	4	Іспит
ОК 7.	Спеціальні вимірювання в галузі ТЗІ	4	Іспит
ОК 8.	Комплексні системи безпеки	4	Іспит
ОК 9.	Інформаційна безпека в мережі Інтернет	4	Іспит
ОК 10.	Захист інформації в радіомережах	4	Іспит
ОК 11.	Методи побудови в криптографічних системах	4	Іспит
ОК 12.	Моніторинг та аудит інформаційно-комунікаційних систем	4	Іспит
Загальний обсяг обов'язкових компонент:		**45**	
2. ВИБІРКОВІ ДИСЦИПЛІНИ			
2.1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ ЗАКЛАДУ			
2.1.1. Дисципліни гуманітарної підготовки (120 годин/4 кредитів)			
ВБ 1.1.	Технічна іноземна мова	4	
2.1.2. Цикл фундаментальної підготовки (360 годин/12 кредитів)			
ВБ 1.2.	Системи оптичного та електричного зв'язку	4	Іспит
ВБ 1.3.	Перспективні напрямки захисту інформації	4	Залік
ВБ 1.4.	Сучасна теорія та техніка інформаційної безпеки	4	Залік
2.2 ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ (240 годин/8 кредитів)			
ВБ 1.5.	Теоретична криптологія	4	Іспит
ВБ 1.6.	Методи оцінки інформаційної захищеності	4	Залік
Загальний обсяг вибіркових компонент:		**24**	
3 ПРАКТИЧНА ПІДГОТОВКА, ПІДСУМКОВА АТЕСТАЦІЯ (630 годин/21 кредит)			
ВБ 1.7.	Переддипломна практика	6	
ВБ 1.8.	Підготовка наукових праць та атестаційної роботи	9	
ВБ 1.9.	Захист магістерської роботи	6	
Загальний обсяг практичної підготовки, підсумкової атестації		**21**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

2.2 Структурно-логічна схема ОП

Структурно-логічна схема підготовки фахівця освітньо-кваліфікаційного рівня магістр за спеціальністю 125 Кібербезпека

5 курс		**6 курс**	
5.1	5.2	6.1	6.2
І. Обов'язкові дисципліни			
1.1. Цикл гуманітарної підготовки			
Охорона праці в галузі	Цивільний захист		
1.2. Цикл фундаментальної підготовки			
Математичні методи моделювання та оптимізації процесів	Моделювання та організація наукових досліджень	Система менеджменту інформаційної безпеки	
1.3. Цикл професійної підготовки			
Ліцензування, атестація та сертифікація в галузі ТЗІ	Спеціальні вимірювання в галузі ТЗІ	Комплексні системи безпеки	
Інформаційна безпека в мережі Інтернет	Захист інформації в радіомережах		
Методи побудови в криптографічних системах	Моніторинг та аудит інформаційно-комунікаційних систем		
ІІ. Вибіркові дисципліни			
2.1. Дисципліни гуманітарної підготовки			
Технічна іноземна мова			
2.2. Цикл фундаментальної підготовки			
Сучасна теорія та техніка інформаційної безпеки	Системи оптичного та електричного зв'язку	Перспективні напрямки захисту інформації	
2.3. Цикл професійної підготовки			
Теоретична криптологія	Методи оцінки інформаційної захищеності		
ІІІ. Практична підготовка			
		Переддипломна практика	
		Підготовка наукових праць та атестаційної роботи	
		Захист магістерської 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 магістра із присвоєнням кваліфікації – 2149.2 – Професіонал із організації інформаційної безпеки.

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	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9
ЗК1	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК 2	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК 3									•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК 4			•		•	•		•	•	•							•		•		
ЗК 5			•	•	•			•	•	•	•		•	•	•	•	•	•	•		
ЗК 6			•	•		•	•	•	•	•	•		•	•	•	•	•	•		•	•
ЗК 7	•	•	•		•														•		
ЗК 8			•																•		
ЗК 9	•	•	•	•	•	•				•	•	•	•		•		•	•	•		
ЗК 10	•	•	•		•	•															
ЗК 11	•	•	•	•	•	•	•		•		•		•			•					
ЗК 12	•	•	•	•	•	•		•			•	•									
ЗК 13	•	•	•		•																
ЗК 14	•	•	•	•	•																
ЗК 15			•	•	•																
ФК 1	•	•	•				•	•	•	•	•	•	•		•		•		•	•	
ФК 2	•	•	•				•	•	•	•	•	•	•		•		•		•	•	
ФК 3	•	•	•				•	•	•	•		•	•		•		•	•	•	•	
ФК 4	•	•	•					•	•				•							•	
ФК 5	•	•	•					•		•			•							•	
ФК 6	•	•	•				•		•	•			•		•					•	
ФК 7	•	•	•				•	•			•		•		•		•			•	
ФК 8	•	•	•				•			•	•	•	•			•	•				
ФК 9	•	•	•						•	•			•	•					•		
ФК 10	•	•	•										•	•						•	
ФК 11	•	•	•							•			•								
ФК 12	•	•	•							•	•		•								•
ФК13	•	•	•										•							•	•
ФК 14	•	•	•																		
ФК 15	•	•	•					•				•	•		•						•
ФК 16	•	•	•									•	•		•				•		
ФК 17	•	•	•				•	•		•		•	•		•	•	•	•	•	•	•

5. Матриця забезпечення програмних результатів навчання (ПРН) 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	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6
ПРН1	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•
ПРН 2		•			•	•	•	•	•	•	•	•	•	•	•			
ПРН3			•		•	•		•	•	•	•	•	•	•	•		•	
ПРН4			•	•	•			•	•	•		•	•			•		
ПРН5	•	•	•	•	•	•	•			•		•	•			•		
ПРН6	•	•				•	•	•				•	•			•		
ПРН7					•	•			•			•	•			•		
ПРН8					•	•						•	•		•	•		
ПРН9									•		•	•	•		•	•	•	
ПРН10									•			•	•		•	•	•	
ПРН11									•			•	•			•	•	
ПРН12			•						•		•		•			•		•
ПРН13									•	•	•		•			•		•
ПРН14			•	•		•						•	•			•		•
ПРН15										•			•		•	•		•
ПРН16			•						•			•	•		•	•		
ПРН17			•	•						•			•			•		
ПРН18			•						•				•			•	•	
ПРН19							•						•	•			•	
ПРН20			•			•		•		•	•	•	•	•			•	•
ПРН21								•				•	•		•			•
ПРН22							•	•					•		•			•
ПРН23					•	•	•	•					•		•			•
ПРН24			•	•	•		•	•				•	•					
ПРН25			•	•						•		•	•		•			•
ПРН26			•	•						•			•		•	•		•

Додаток

Рецензії-відгуки зовнішних стейкголдерів

РЕЦЕНЗІЯ – ВІДГУК

на освітньо-професійну програму підготовки магістрів
за спеціальністю 125 – Кібербезпека
Одеської національної академії зв'язку ім. О.С. Попова

Освітньо-професійна програма підготовки магістрів за спеціальністю 125 – кібербезпека Одеської національної академії зв'язку ім. О.С. Попова у цілому відповідає вимогам до професійної діяльності фахівців з інформаційної та кібербезпеки ступеня магістр. Перелік компетентностей випускника містить одну інтегральну, 14 загальних та 17 фахових компетентностей, які охоплюють предметну область фахівців як безпосередньо з кібербезпеки, так і з технічного захисту інформації та управління інформаційною безпекою. Це, на мій погляд, підвищує конкурентоспроможність випускників – фахівців з інформаційної та кібербезпеки на вітчизняному та міжнародному ринку праці.

Результати навчання в цілому корелюють з переліком компетентностей. Доречним є те, що до навчального плану включено такі дисципліни, як: «Комплексні системи безпеки», «Інформаційна безпека в мережі Інтернет», «Моніторинг та аудит інформаційно-комунікаційних систем», «Методи оцінки інформаційної захищеності», «Система менеджменту інформаційної безпеки», «Ліцензування, атестація та сертифікація в галузі ТЗІ», які надають випускнику – магістру необхідних компетентностей для фахової та науково-дослідної роботи в галузі кібербезпеки, технічного захисту інформації, управління інформаційною безпекою тощо.

Даною освітньо-професійною програмою підготовки магістрів передбачено достатньо кредитів на переддипломну практику та підготовку наукових праць, що є необхідною умовою підготовки висококваліфікованого фахівця в галузі захисту інформації.

У цілому є підстави вважати, що освітньо-професійна програма підготовки магістрів за спеціальністю 125 – кібербезпека Одеської національної академії зв'язку ім. О.С. Попова є актуальною та цілком відповідає сучасним вимогам до професійної діяльності фахівців з інформаційної та кібербезпеки ступеня магістр.

Директор ТОВ «Гофер Корпорейшн» С.О. Дігол

РЕЦЕНЗІЯ – ВІДГУК

на освітньо-професійну програму підготовки магістрів
за спеціальністю 125 – Кібербезпека
Одеської національної академії зв'язку ім. О.С. Попова

Професіонал з інформаційної безпеки - одна з ключових і затребуваних професій сучасної України. Актуальність підготовки таких кадрів зумовлена статистикою загроз і ризиків останнього часу. При цьому потенційні кадри повинні отримувати знання і вміння на підставі оптимальних навчальних програм.

Було розглянуто освітньо-професійну програма підготовки магістрів за спеціальністю 125 – кібербезпека Одеської національної академії зв'язку ім. О.С. Попова. Програма відповідає вимогам до професійної діяльності та компетенціям фахівців з кібербезпеки ступеня магістр. Перелік компетенцій випускника охоплює предметну область фахівців як безпосередньо з кібербезпеки, так і з технічного захисту інформації та управління інформаційною безпекою. Комплексний підхід в підготовці дозволяє формувати компетенції оптимально і з високою ефективністю. В свою чергу, це підвищує конкурентоспроможність випускників – фахівців з інформаційної та кібербезпеки на вітчизняному та міжнародному ринку праці.

До навчального плану включено ланку дисциплін, які надають випускнику – магістру необхідних компетентностей для фахової та науково-дослідної роботи в галузі кібербезпеки, технічного захисту інформації, управління інформаційною безпекою, аудиту, менеджменту інформаційної безпеки тощо.

На основі розглянутого прийнято рішення вважати освітньо-професійну програму підготовки магістрів за спеціальністю 125 – кібербезпека Одеської національної академії зв'язку ім. О.С. Попова актуальною та такою, яка відповідає сучасним вимогам до професійної діяльності фахівців з кібербезпеки та інформаційної ступеня магістр.

Директор ТОВ «ЄВРО Україна ЛТД» О.В. Шкурупій