МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ Д.В. Дмитришин

протокол № ____ від "____"_____ 20__ р.

Освітня програма вводиться в дію з _____20__ р.

Проректор, голова комісії з реорганізації

_____ С.А.Нестеренко

наказ № ___ від "____"_____ 20__ р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Другий (магістерський) рівень вищої освіти
(назва рівня вищої освіти)

МАГІСТР
(назва ступеня, що присвоюється)

ГАЛУЗЬ ЗНАНЬ 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
(шифр та назва галузі знань)

СПЕЦІАЛЬНІСТЬ 125 КІБЕРБЕЗПЕКА
(код та найменування спеціальності)

О Д Е С А - 2 0 2 1

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Спеціалізація	
Рівень вищої освіти	другий (магістерський)
Ступінь	Магістр
Професійна кваліфікація	КП 1210.1 - Керівник підприємства (установи, організації) (сфера захисту інформації) КП 1226.2 - Керівник структурного підрозділу (сфера захисту інформації) КП 1226.2 - Начальник відділення (сфера захисту інформації) КП 1495 - Менеджер (управитель) систем з інформаційної безпеки КП 2149.2 - Професіонал із організації захисту інформації з обмеженим доступом КП 2149.2 - Професіонал із організації інформаційної безпеки КП 2149.2 - Розробник систем (крім комп'ютерів) КП 2149.2 - Фахівець (сфера захисту інформації) КП 2149.2 - Інженер з керування й обслуговування систем КП 2132.2 - Програміст прикладний КП 2131.2 - Адміністратор доступу КП 2131.2 - Адміністратор доступу (груповий) КП 3439 Інспектор з організації захисту секретної інформації КП 3439 Фахівець з режиму секретності КП 3439 Фахівець із організації захисту інформації з обмеженим доступом КП 3439 Фахівець із організації інформаційної безпеки

РОЗРОБЛЕНО
Робочою групою освітньо-професійної програми
Гарант освітньо-професійної програми
_____ Лебедєва О.Ю.
"____" _____ 20__ р.

ПОГОДЖЕНО
Проректор з науково-педагогічної та
виховної роботи
_____ С.А. Нестеренко
"____" _____ 20__ р.

ПОГОДЖЕНО
Проректор з науково-педагогічної роботи
та інформаційних технологій
_____ Ю.М.Свінарьов
"____" _______ 20__ р.

ПОГОДЖЕНО
Начальник центру із забезпечення
якості вищої освіти
_____ О.С.Савєльєва
"____" _____ 20__ р.

І - Преамбула

Освітньо-професійна програма зі спеціальності 125 «Кібербезпека» розроблена робочою групою за другим (магістерським) рівнем навчально-наукового інституту інформаційної безпеки, радіоелектроніки та телекомунікацій на основі стандарту вищої освіти, затвердженого наказом Міністерства освіти і науки України № 332 від 18.03.2021 року.

ВНЕСЕНО
Кафедрою кібербезпеки та програмного забезпечення
(назва структурного підрозділу закладу вищої освіти)

В розробці освітньо-професійної програми брали участь: здобувач вищої освіти за другим (магістерським) рівнем зі спеціальності 125 «Кібербезпека» Вайтовецька Марія (2020 р. вступу), здобувач вищої освіти за третім (освітньо-науковим) рівнем зі спеціальності 125 «Кібербезпека» Батієне Лаїрі Ератостенес Мухамін.

Рецензії-відгуки зовнішніх стейкхолдерів:

Назва організації, підприємства тощо	**Посада, наукова ступінь та вчене звання,**	**ПІБ**	**Підпис**	**Дата**
Департамент кіберполіції Національної поліції України	**Начальник сектору управління протидії кіберзлочинам в Одеській області, підполковник поліції**	**Тіщенко Євген Іванович**		
Національна академія внутрішніх справ	**Головний науковий співробітник науково-дослідної лабораторії з проблем криміналістичного забезпечення та судової експертології, доктор технічних наук, професор**	**Рибальський Олег Володимирович**		

1. ВСТУП

Відповідно до ст. 1 "Основні терміни та їх визначення" Закону України "Про вищу освіту": **освітня (освітньо-професійна, освітньо-наукова) програма** – єдиний комплекс освітніх компонентів (навчальних дисциплін, індивідуальних завдань, практик, контрольних заходів тощо), спрямованих на досягнення передбачених такою програмою результатів навчання, що дає право на отримання визначеної освітньої або освітньої та професійної (професійних) кваліфікації (кваліфікацій).

Освітня програма повинна містити: перелік освітніх компонентів; їх логічну послідовність; вимоги до рівня освіти осіб, які можуть розпочати навчання за цією програмою; кількість кредитів ЄКТС, необхідних для виконання цієї програми, а також очікувані програмні результати навчання (компетентності), якими повинен оволодіти здобувач вищої освіти.

Освітня програма використовується під час:

– розроблення навчального плану, робочих програм навчальних дисциплін і програм практик;

– розроблення засобів оцінювання (ідентифікація компетентностей та вимірювання результатів навчання) якості вищої освіти;

– внутрішнього і зовнішнього контролю якості підготовки здобувачів;

– атестації здобувачів;

– акредитації освітньої програми, інспектування освітньої діяльності за спеціальністю (спеціалізації за наявності);

– визначення змісту навчання в системі перепідготовки та підвищення кваліфікації;

– професійної орієнтації здобувачів спеціальності.

Освітня програма враховує вимоги Закону України "Про вищу освіту", Національної рамки кваліфікацій, затвердженої постановою Кабінету Міністрів України від 23 листопада 2011 р. № 1341 (у редакції від 25.06.2019) і встановлює: обсяг та термін навчання магістрів; загальні компетентності; спеціальні компетентності; програмні результати навчання; перелік та обсяг освітніх компонентів для опанування компетентностей освітньої програми.

Користувачі освітньої програми:

- здобувачі вищої освіти, які навчаються в Державному університеті «Одеська політехніка»;
- науково-педагогічні працівники, які здійснюють підготовку магістрів зі спеціальності 125 «Кібербезпека»;
- екзаменаційна комісія спеціальності 125 «Кібербезпека»;
- приймальна комісія Державного університету «Одеська політехніка».

Освітня програма поширюється на випускову кафедру кібербезпеки та програмного забезпечення для підготовки здобувачів 125 «Кібербезпека»: Навчально-наукового інституту інформаційної безпеки, радіоелектроніки та телекомунікацій (ІІБРТ), Українсько-німецького Навчально-наукового інституту (УНІ)*, Українсько-іспанського навчально-наукового інституту (УІІ)*, Українсько-польського навчально-наукового інституту (УПІ)*.

2. НОРМАТИВНІ ПОСИЛАННЯ

Освітня програма розроблена на основі таких нормативних документів та рекомендацій:

2.1 Закон України «Про вищу освіту».http://zakon.rada.gov.ua/laws/show/1556-18

2.2 Закон України «Про освіту». https://zakon.rada.gov.ua/laws/show/2145-19

2.3 Національна рамка кваліфікацій. Додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341 (у редакції від 02.07.2020 р.).http://zakon.rada.gov.ua/laws/show/1341-2011-п

2.4 Постанова Кабінету Міністрів України від 26.04.2015 № 266 "Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти" (редакція від 11.02.2017 р.). https://zakon.rada.gov.ua/laws/show/z1460-15

2.5 Постанова КМУ № 579 “Про затвердження Положення про порядок реалізації права на академічну мобільність” від 12 серпня 2015 року.

2.6 Національний класифікатор України: "Класифікатор професій" ДК 003:2010", затверджений наказом Держспоживстандарту від 28.07.2010 р. (редакція від 01.03.2015 р.). https://zakon.rada.gov.ua/rada/show/va327609-10/ed20150301

2.7 Положення про організацію освітнього процесу в ОНПУ. Введено в дію наказом ректора від 03 жовтня 2019 р. № 34. https://opu.ua/document/2492

2.8 Наказ Міністерства освіти і науки України від «01» червня 2016 р. № 600 (у редакції наказу Міністерства освіти і науки України від 01.10.2019 р. № 1254) «Про внесення змін до методичних рекомендацій щодо розроблення стандартів вищої освіти».http://edu-mns.org.ua/img/news/8635/NakMON_1254_19.pdf.

2.9 A Tuning Guide to Formulating Degree Programme Profiles Including Programme Competences and Programme Learning Outcomes. -Bilbao, Groningen and The Hague, 2010.

2.10 A TUNING-AHELO conceptual framework of expected/desired learning outcomes in engineering. OECD Education Working Papers, No. 60, OECD Publishing 2011. Режим доступу: http://dx.doi.org/10.1787/5kghtchn8mbn-en.

2.11 Процедура з розроблення освітніх програм.Введено в дію наказом ректора від 6 березня 2020 р. № 23. https://opu.ua/document/3355

2.12 Положення про порядок організації вивчення вибіркових освітніх компонентів. Введено в дію наказом ректора від 6 березня 2020 р. № 24. https://opu.ua/document/3354

2.13 Положення про систему внутрішнього забезпечення якості вищої освіти та освітньої діяльності Одеського національного політехнічного університету. Введено в дію наказом ректора від 31 жовтня 2019 р. № 54. https://opu.ua/document/2545

2.14 Положення про порядок реалізації права на академічну мобільність (нова редакція). Введено в дію наказом ректора від 3 жовтня 2019 № 37. https://opu.ua/document/2501

2.15 Наказ Міністерства праці та соціальної політики України «Про затвердження Випуску 1 "Професії працівників, що є загальними для всіх видів економічної діяльності" Довідника кваліфікаційних характеристик професій працівників» від 29.12.2004 N 336https://zakon.rada.gov.ua/rada/show

2.16. Стандарт вищої освіи за спеціальністю 125- Кібербезпека для другого (магістерського) рівня вищої освіти https://mon.gov.ua/ua/osvita/visha-osvita/naukovo-metodichna-rada-ministerstva-osviti-i-nauki-ukrayini/zatverdzheni-standarti-vishoyi-osviti

3. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ МАГІСТРА

Рівень вищої освіти	Другий (магістерський) рівень
Ступінь, що присвоюється	Магістр
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека
Назва спеціалізації	
Наявність акредитації	Міністерство освіти і науки України, сертифікат акредитації спеціальності 125 - Кібербезпека серія НД, № 1695134, дійсний до 1 липня 2022 р.
Документ про вищу освіту, що видається випускникам	Диплом магістра; Додаток до диплома магістра європейського зразка.
Передумови	Наявність ступеня бакалавра або магістра.
Обсяг кредитів ЄКТС, необхідний для здобуття освіти	90 кредитів ЄКТС, нормативний строк підготовки за денною та заочною формами здобуття освіти – 1 рік 4 місяців.
Термін дії освітньої програми	2021 – 2025 рр.
Цикл/рівень	FQ-EHEA – другий цикл, QF-LLL – сьомий рівень, НРК – сьомий рівень
Обмеження щодо форм навчання	Обмеження відсутні
Кваліфікація освітня	Магістр з кібербезпеки
Кваліфікація, що присвоюється випускникам	Ступінь вищої освіти – Магістр Спеціальність – 125 Кібербезпека Освітня програма – Кібербезпека
Мова (и) викладання	Українська
Інтернет-адреса постійного розміщення опису освітньої програми	https://opu.ua/education/programs/mag-125-0

А	**Мета освітньої програми**
	Програма призначена для розвитку професійних, творчих здібностей, приумноження інтелектуального потенціалу студентів щодо оволодіння методологією наукової діяльності та забезпечення студентам фундаментальної підготовки у вигляді поглиблених теоретичних і практичних знань, умінь та навичок, оволодіння

	сучасними підходами, зокрема математичними, розв'язання задач в галузі кібербезпеки, забезпечення у студентів можливості відповісти на сучасні виклики в галузі кібербезпеки шляхів використання набутих компетентностей для отримання очікуваних результатів.
В	**Характеристика програми**
Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні іматематичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.

	Інструменти та обладнання. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Фокус програми: Загальна / спеціальна	Загальна. Кібербезпека. Програма спрямована на захист складових кіберпростору з метою зменшення небажаних наслідків від максимально можливого кількості загроз і впливів, зокрема соціо-технічних систем, шляхом використання сучасних інформаційних технологій та унікальних найсучасніших математичних підходів. *Ключові слова*: кібербезпека, стеганографія та стеганоаналіз, обмежений доступ, сучасні криптосистеми, хмарні технології, комп'ютерні мережі, соціо-технічні системи, математичне моделювання
Орієнтація програми	Освітньо-професійна
Особливості та відмінності	Характерною особливістю даної програми є її орієнтованість на сучасні інформаційні технології та унікальні в галузі кібербезпеки математичні підходи, їх застосування для розв'язку задач кібербезпеки, зокрема для захисту соціо-технічних систем.
С	**Придатність до працевлаштування та подальшого навчання**
Придатність до працевлаштування	Працевлаштування на підприємствах та установах будь якої організаційно-правової форми. КП 1210.1 - Керівник підприємства (установи, організації) (сфера захисту інформації) КП 1226.2 - Керівник структурного підрозділу (сфера захисту інформації) КП 1226.2 - Начальник відділення (сфера захисту інформації) КП 1495 - Менеджер (управитель) систем з інформаційної безпеки КП 2149.2 - Професіонал із організації захисту інформації з обмеженим доступом КП 2149.2 - Професіонал із організації інформаційної безпеки КП 2149.2 - Розробник систем (крім комп'ютерів) КП 2149.2 - Фахівець (сфера захисту інформації) КП 2149.2 - Інженер з керування й обслуговування систем КП 2132.2 - Програміст прикладний КП 2131.2 - Адміністратор доступу КП 2131.2 - Адміністратор доступу (груповий) КП 3439 Інспектор з організації захисту секретної інформації КП 3439 Фахівець з режиму секретності КП 3439 Фахівець із організації захисту інформації з обмеженим доступом КП 3439 Фахівець із організації інформаційної безпеки
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти.

	Набуття додаткових кваліфікацій в системі освіти дорослих.
D	**Стиль та методика навчання**
Підходи до викладання та навчання	Проблемно-орієнтоване навчання, навчання на основі сучасних досліджень. Викладання та навчання проводиться у вигляді: лекцій, мультимедійних лекцій, практичних занять, лабораторних робіт, самостійної роботи, участь у міждисциплінарних проектах та тренінгах, консультацій із науково-педагогічними співробітниками, підготовки магістерської роботи тощо.
Система оцінювання	Екзамени, заліки, модульний та поточний контроль, захист звіту з практики, захист курсових робіт, захист випускної роботи (проекту) магістра.
E	**Програмні компетентності**
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності	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. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимогитехнічного 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. 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. 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.

	КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. 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. 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. 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. 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.
F	**Програмні результати навчання**
	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання

	спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

	РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
G	**Ресурсне забезпечення реалізації програми**
Специфічні характеристики кадрового забезпечення	100 % професорсько-викладацького складу, задіяного до викладання циклу дисциплін професійної підготовки, мають відповідні наукові ступені до дисциплін, які викладають
Специфічні характеристики матеріально-технічного забезпечення	Використання сучасного обладнання, зокрема https://opu.ua/about/reports#11
Специфічні характеристики інформаційно-методичного забезпеченн	Використання віртуального навчального середовища Державного університету «Одеська політехніка» та авторських розробок професорсько-викладацького складу. https://library.opu.ua https://el.opu.ua
H	**Основні компоненти освітньої програми**
	Перелік компонент освітньо-професійної програми наведено в розділі 4.
I	Академічна мобільність регламентується Постановою КМУ № 579 "Про затвердження Положення про порядок реалізації права на академічну мобільність" від 12 серпня 2015 року та Положенням про порядок реалізації права на академічну мобільність (нова редакція). (Введено в дію наказом ректора від 3 жовтня 2019 № 37). https://opu.ua/document/2501
Національна кредитна мобільність	На основі двосторонніх договорів між ОНПУ (зараз Державним університетом «Одеська політехніка») та технічними університетами України.
Міжнародна	У рамках програми ЄС Еразмус+ на основі спільних договорів між

кредитна мобільність	ОНПУ (зараз Державним університетом «Одеська політехніка») та університетами партнерами
Навчання іноземних здобувачів вищої освіти	На загальних умовах та засвоєнні дисципліни «Українська мова як іноземна»

4 РОЗПОДІЛ ЗМІСТУ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА ГРУПАМИ ОСВІТНІХ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
		Обов'язкові компоненти ОП (обов'язкова частина за НП)	Вибіркові компоненти ОП (вибіркова частина за НП)	Всього за весь термін навчання
1	**Навчальні дисципліни загальної підготовки**	9/10	6/7	15/17
2	**Навчальні дисципліни професійної підготовки**	27/30	18/20	45/50
3	**Курсові проекти**	Немає	Немає	-/-
4	**Практична підготовка**	15/16.5	Немає	15/16.5
5	**Атестація**	15/16.5	Немає	15/16.5
6	**Всього за весь термін навчання:**	66/73	24/27	90/100

Перелік компонентів освітньо-професійної програми та їх логічна послідовність

4.1 Перелік компонентів ОПП

Шифр ОК	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумк. контролю
1	2	3	4
1 Обов'язкові компоненти ОПП/ОНП			
1.1Навчальні дисципліни загальної підготовки			
О301	Професійна іноземна мова	3	З
О302	Професійне навчання та професійна кар'єра	3 в 1 сем	З
О303	Організація винахідницької діяльності в ІТ-галузі	3	З
1.2Навчальні дисципліни професійної підготовки			
ОП01	Сучасні КСЗІ та їх особливості	4.5	І
ОП02	Бізнес-процеси в кібербезпеці	4.5	І
ОП03	Проблеми кібербезпеки та сучасні підходи до їх вирішення	7.5	І
ОП04	Захист соціо-технічних систем	3	З
ОП05	Сучасні методи захисту комп'ютерних мереж	4.5	І
ОП06	Прикладна загальна теорія систем безпеки	3	З
1.3 Практична підготовка			
ПП01	Переддипломна практика	15	З
1.5 Атестація			
А01	Кваліфікаційна робота	15	І
Загальний обсяг обов'язкових компонентів:		66	
2 Вибіркові компоненти ОПП/ОНП*			
2.1Навчальні дисципліни загальної підготовки			
В301	Українська мова як іноземна*	4.5	З

Шифр ОК	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумк. контролю
В302	Інтелектуальна власність та авторське право	3	З
В303	Професійна педагогіка	3	З
В304	Екологічна безпека	3	З
В305	Організаційна психологія	3	З
В306	Патентознавство	3	З
В307	Кадровий менеджмент	3	З
2.2Навчальні дисципліни професійної підготовки			
ВП01	Інтелектуальні методи підтримки прийняття рішень та їх застосування в інформаційній безпеці	4.5	І
ВП02	Технології безпеки мобільних мереж	4.5	І
ВП03	Обробка інформації з обмеженим доступом	4.5	І
ВП04	Програмні методи організації прихованого каналу зв’язку	4.5	І
ВП05	Моделі та методи аналізу об'єктів інформатизаціїї	4.5	І
ВП06	Розподілені системи та їх захист	4.5	І
ВП07	Захист інформації в мобільних пристроях	4.5	І
ВП08	Безпечні інформаційні системи та блокчейн-технології	4.5	І
ВП09	Кібербезпека сучасних інформаційних технологій	4.5	І
ВП10	Методологія agile розробки інформаційних систем	4.5	І
ВП11	Проектування систем штучного інтелекту	4.5	І
ВП12	Професійна іноземна мова 2	4.5	І
ВП13	Стеганографія та стеганоаналіз	4.5	І
	Дисципліна $1^{(2)}$	4.5	І
Загальний обсяг вибіркових компонент:		24	
В308	Військова підготовка**	29	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

Примітка:

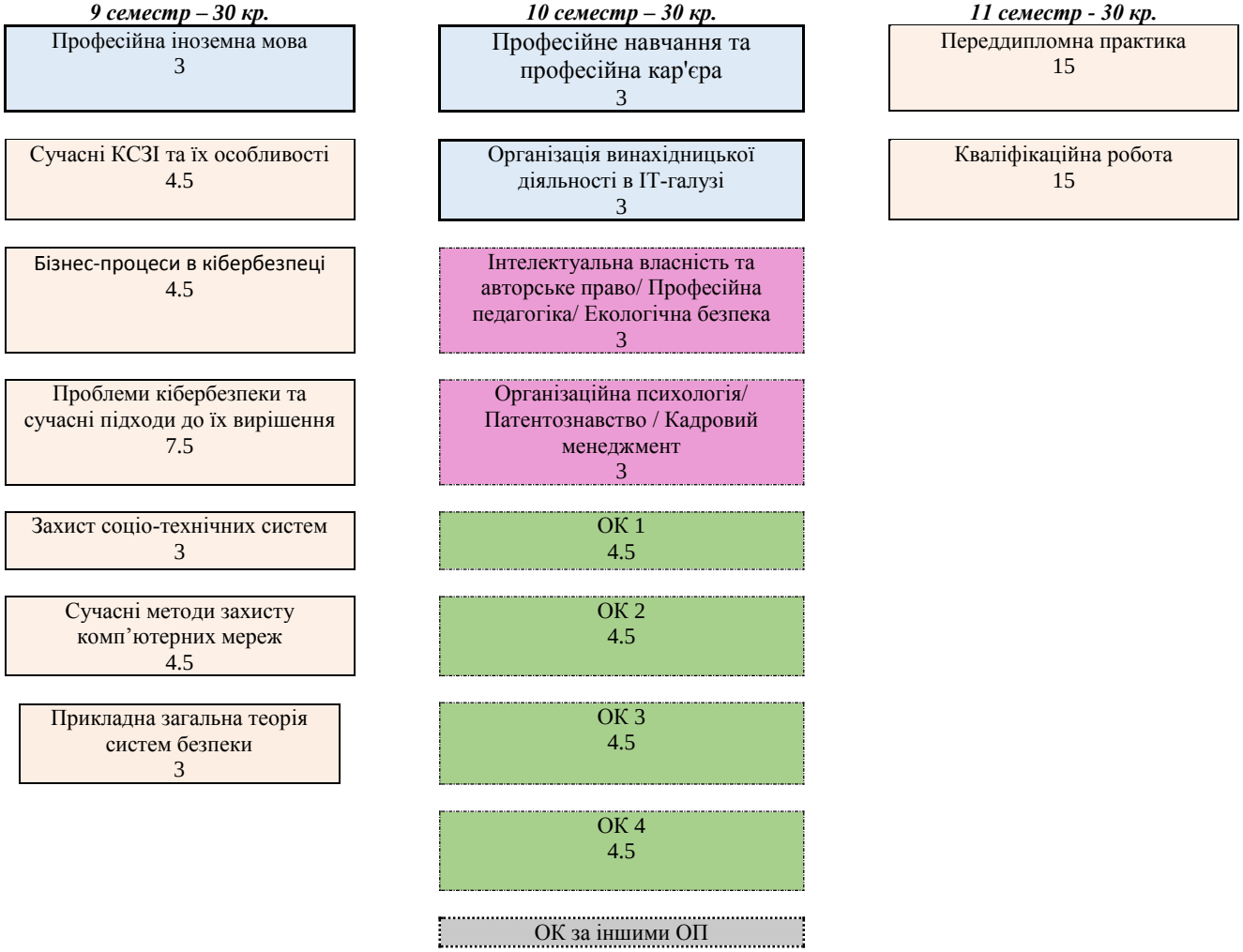
* Згідно із Законом України “Про вищу освіту” здобувачі вищої освіти мають право на: вибір навчальних дисциплін у межах, передбачених відповідною освітньою програмою та навчальним планом, в обсязі, що становить не менш як 25 відсотків загальної кількості кредитів ЄКТС, передбачених для даного рівня вищої освіти. При цьому здобувачі певного рівня вищої освіти мають право вибирати навчальні дисципліни, що пропонуються для інших рівнів вищої освіти, за погодженням з керівником відповідного факультету чи підрозділу.

** Послідовність вивчення дисципліни, графік навчального процесу, форми проведення навчальних занять та їх обсяг, форми та засоби поточного і підсумкового контролю встановлюються відповідною програмою військової підготовки.

Дисципліна $1^{(2)}$ - в другому семестрі здобувачі можуть обирати дисципліну обсягом 4.5 кредити ЄКТС з інших діючих навчальних планів.

4.2 Структурно-логічна схема ОП

Структурно-логічна схема ОПП магістра. Короткий опис логічної послідовності вивчення компонент освітньої програми:



Умовні позначення:

ОБОВ'ЯЗКОВА ЧАСТИНА **ВИБІРКОВА ЧАСТИНА**

ОК загальної підготовки	ОК професійної підготовки	ОК загальної підготовки	ОК професійної підготовки	ОК за іншими ОП

кр – кількість кредитів

5.1. Матриця співвідношення програмних компетентностей до освітніх компонент

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
Дисципліни загальної підготовки															
О301	+														
О302				+											+
О303		+	+		+										
Дисципліни професійної підготовки															
ОП01							+	+	+		+				
ОП02								+		+				+	
ОП03						+							+		
ОП04						+									
ОП05												+			+
ОП06						+					+				
Практична підготовка															
ПП01	+	+	+	+		+		+							+
Атестація															
А01	+	+	+	+		+		+							+

5.2. Матриця відповідності визначених Стандартом 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
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	+		+	+		+	+	+			+	+	+	+	

5.3 Матриця співвідношення програмних результатів навчання до освітніх компонент

Програмні результати навчання	Шифри освітніх компонент ОПП										
	О301	О302	О303	ОП01	ОП02	ОП03	ОП04	ОП05	ОП06	ПП01	А01
РН1	+		+							+	+
РН2			+	+		+	+		+	+	+
РН3						+			+	+	+
РН4				+		+	+		+	+	+
РН5				+						+	+
РН6				+		+		+	+	+	+
РН7			+	+						+	+
РН8					+			+			
РН9				+							
РН10					+						
РН11									+		
РН12				+				+			
РН13						+				+	+
РН14				+							
РН15		+								+	+
РН16				+							
РН17		+								+	+
РН18		+	+								
РН19					+		+			+	+
РН20				+					+	+	+
РН21						+	+			+	+
РН22						+				+	+
РН23				+					+	+	+

6. Форма атестації

Атестація випускників спеціальності 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної роботи та завершується видачею документів встановленого зразка про присудження йому відповідного освітнього ступеня магістра та присвоєнням кваліфікації: магістр з кібербезпеки. Атестація здійснюється відкрито і публічно.

Форма 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. Регламент обсягу (40-60 сторінок пояснювальної записки) та структура роботи у відповідності до затвердженого Положення щодо оформлення кваліфікаційних робіт здобувачів вищої освіти (магістр). Перевірка на плагіат. Оприлюднення кваліфікаційної роботи у репозитарії Державного університету «Одеська політехніка». Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

7 Система внутрішнього забезпечення якості вищої освіти Державним університетом «Одеська політехніка» складається з таких процедур і заходів, передбачених законом «Про вищу освіту»:

1) визначення принципів та процедур забезпечення якості вищої освіти;
2) здійснення моніторингу та періодичного перегляду освітніх програм;
3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних працівників ОНПУ та регулярне оприлюднення результатів такого оцінювання на офіційному веб-сайті університету;
4) забезпечення підвищення кваліфікації науково-педагогічних працівників;
5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, в тому числі самостійної роботи здобувачів вищої освіти;
6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
7) забезпечення публічності інформації про освітні програми;
8) забезпечення дотримання академічної доброчесності працівниками закладу вищої освіти та здобувачами вищої освіти, у тому числі створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату;
9) інших процедур і заходів.

Положення про систему внутрішнього забезпечення якості вищої освіти та освітньої діяльності Державного університету «Одеська політехніка» затверджено Вченою радою Одеського національного політехнічного університету, протокол від 29.10.2019 р. № 3 та введено в дію наказом ректора від 31.10.2019 р. № 54.