



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

ПРОЄКТ
від 18 серпня 2022

Освітня програма вводиться в дію

з 01 жовтня 2022 р.

Перший (бакалаврський) рівень вищої освіти

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА

Шифр – 125-0

ID в ЄДЕБО – 50645

Галузь знань

12 Інформаційні технології

Спеціальність

125 Кібербезпека

1 ПЕРЕДМОВА

Освітню програму розроблено на основі стандарту вищої освіти за спеціальністю «125 Кібербезпека» галузі знань «12 Інформаційні технології» для першого (бакалаврського) рівня вищої освіти. Стандарт затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 № 1074.

Група розробників освітньої програми

Члени групи:

Бобок І.І., доктор технічних наук, доцент, доцент кафедри комп'ютеризованих систем та програмних технологій, гарант освітньої програми;
Кобозєва А.А., доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення;
Соколов А.В., кандидат технічних наук, доцент, доцент кафедри кібербезпеки та програмного забезпечення.

Особи, які були додатково залучені до розробки:

Попов Д.С., заступник начальника Управління Держспецзв'язку в Одеській області;
Сокальський С.І., здобувач вищої освіти.

Погодження

Освітню програму розглянуто та схвалено на засіданні кафедри кібербезпеки та програмного забезпечення 21.06.2022, протокол № 13.

Освітню програму розглянуто на засіданні Ради з якості освітньої діяльності Національного університету «Одеська політехніка» 18.08.2022, протокол № 14.

Підписанти

Гарант освітньої програми	Іван БОБОК
Завідувач випускової кафедри	Алла КОБОЗЄВА
Голова Ради з якості освітньої діяльності	Елеонора ЗАБАРНА
Начальник центру із забезпечення якості вищої освіти	Оксана САВЄЛЬЄВА
Перший проректор	Сергій НЕСТЕРЕНКО
Ректор	Геннадій ОБОРСЬКИЙ

Ця освітня програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Національного університету «Одеська політехніка»

2 АНОТАЦІЯ ОСВІТНЬОЇ ПРОГРАМИ

Програма дозволяє оволодіти сучасними методами та засобами кібернетичної та інформаційної безпеки (технічними, програмними, організаційними, законодавчими та іншими), які використовуються сьогодні в інформаційному просторі. Значна увага при підготовці фахівців приділяється програмуванню, опануванням програмними засобами захисту інформації, інформаційно-комунікаційних, комп'ютерних систем, що значно розширює можливості її випускників при працевлаштуванні.

3 ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

3.1 Загальна інформація

Назва освітньої програми: Кібербезпека.

ID освітньої програми в ЄДЕБО: 50645.

Орієнтація освітньої програми: освітньо-професійна.

Рівень вищої освіти: перший (бакалаврський).

Відповідність рамкам кваліфікацій (РК):

Національна РК України (NQF)	– 6 рівень;
Європейська РК для навчання впродовж життя (EQF-LLL)	– 6 рівень;
РК Європейського простору вищої освіти (FQ-EHEA)	– перший цикл.

Галузь знань: 12 Інформаційні технології.

Спеціальність: 125 Кібербезпека.

Наявність акредитації: акредитовано Міністерством освіти і науки України, сертифікат про акредитацію спеціальності серія УД №16013717, строк дії до 01.07.2029.

Ступінь вищої освіти, що присуджується випускнику: Освітній ступінь «Бакалавр».

Освітня кваліфікація, що присвоюється випускнику: Бакалавр з кібербезпеки.

Документи про вищу освіту, що видаються випускнику:

Диплом бакалавра;
Додаток до диплома європейського зразка.

Кваліфікація в дипломі:

ступінь вищої освіти бакалавр,
галузь знань 12 Інформаційні технології,
спеціальність 125 Кібербезпека.

Обсяг програми: 240 кредитів ЄКТС. На базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). На основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати

та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти.

Вимоги щодо попередньої освіти: наявність повної загальної середньої освіти або ступеня фахового молодшого бакалавра або молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста.

Тривалість програми:

Нормативний строк підготовки становить:

- 3 роки 10 місяців – за денною формою здобуття освіти;
- 4 роки 8 місяців – за заочною формою здобуття освіти.

У разі здобуття освіти на базі ступеня фахового молодшого бакалавра або молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста строк підготовки може бути зменшений на 1–2 роки.

Строк перепідготовки з іншої спеціальності становить 1–2 роки.

Форма здобуття освіти: очна (денна), заочна.

Мова викладання: українська.

Кафедра (спеціальна), яка забезпечує виконання програми: Кафедра кібербезпеки та програмного забезпечення.

Інтернет-адреса постійного розміщення опису освітньої програми:

<https://op.edu.ua/education/programs/bac-125-0>.

Термін дії освітньої програми: 2022–2027 роки.

Сфера застосування освітньої програми:

Програма розповсюджується на здобувачів вищої освіти з нормативним терміном завершення навчання у:

- 2026 році – за денною формою здобуття освіти;
- 2027 році – за заочною формою здобуття освіти.

3.2. Характеристика програми

3.2.1 Опис предметної області

Об'єкти вивчення та діяльності:

об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.

Цілі навчання:

підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.

Теоретичний зміст предметної області:

знання законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів

супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; методів та засобів виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проектування.

Методи, методики та технології:

методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки.

Інструменти та обладнання:

системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

3.2.2 Фокус освітньої програми

Спеціальна освіта, спрямована на підготовку фахівців з кібербезпеки, набуття компетентностей, пов'язаних з захистом складових кіберпростору, спеціалізованими та практичними задачами у галузі забезпечення інформаційної та кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.

Ключові слова: кібербезпека, інформаційна безпека, інформаційна безпека держави.

3.2.3 Особливості та відмінності програми

Характерною особливістю даної програми є надання можливості поглибленого вивчення дисциплін, присвячених безпеці інформаційно-телекомунікаційних систем, програмного забезпечення захисту інформації.

Здобувачі вищої освіти за цією освітньою програмою мають можливість брати участь в програмах міжнародної академічної мобільності (тривалістю 1 або 2 семестри), яка реалізується німецькою, польською, іспанською мовами та вимагає необхідного рівня мовної компетентності.

3.2.4 Додаткові можливості програми

Здобувачі вищої освіти за цією освітньою програмою мають можливість брати участь в програмах міжнародної академічної мобільності (тривалістю 1 або 2 семестри), яка реалізується англійською, німецькою, польською, іспанською мовами.

Здобувачі вищої освіти мають можливість додатково до обсягу освітньої програми пройти курс військової підготовки в обсязі 29 кредитів ЄКТС на кафедрі військової підготовки офіцерів запасу Національного університету «Одеська політехніка».

Здобувачі вищої освіти за цією освітньою програмою мають можливість брати участь в міжнародному проєкті USAID "Кібербезпека критично важливої інфраструктури України".

3.3 Особливості реалізації програми

3.3.1 Підходи до викладання та навчання

Форми і методи навчання і викладання відповідають вимогам студентоцентрованого підходу, принципам академічної свободи та академічної доброчесності.

3.3.2 Система оцінювання

Система оцінювання ґрунтується на принципах ЄКТС та здійснюється за 100-бальною шкалою.

Оцінка за шкалою університету	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	
		Екзамени та диференційовані заліки	Заліки
90–100	A	Відмінно	Зараховано
82–89	B	Добре	
75–81	C		
67–74	D	Задовільно	
60–66	E		
35–59	Fx	Незадовільно	Не зараховано
0–34	F		

Кожний навчальний семестр містить два модульних контролі. Кожний модульний контроль оцінюється у максимально можливі 50 балів.

Якщо підсумковою формою контролю є залік, то підсумкова оцінка формується як накопичувальна за результатами оцінювання всіх навчальних елементів, які заплановані на семестр для виконання здобувачами вищої освіти. Оцінку «зараховано» отримують здобувачі вищої освіти, які виконали всі навчальні елементи не менш, ніж на 60 %.

До екзамену допускаються здобувачі, які виконали всі види навчальних елементів навчальної дисципліни на не менш, ніж 60 %.

Критерії оцінювання кожного навчального елемента визначені в робочій програмі навчальної дисципліни і доводяться до відома здобувачів на першому в семестрі занятті відповідно до Положення про робочу програму навчальної дисципліни.

Оприлюднення змісту навчальної дисципліни та критеріїв оцінювання здійснюється через інформаційні картки дисциплін, які розміщені на офіційному вебсайті Університету.

Здобувачі зобов'язані дотримуватись принципів академічної доброчесності при виконанні модульних контрольних робіт, поточних контрольних завдань, індивідуальних завдань з дисципліни (дотримання встановленого deadline, коректна поведінка, під час лекції здійснювати телефонні дзвінки забороняється, заборонено використання будь-яких підручників, посібників, конспектів лекцій, шпаргалок під час проходження модульних контролів, тощо).

3.3.3 Ресурсне забезпечення реалізації програми

Кадрове забезпечення

Освітню програму забезпечують: докторів наук – 3, кандидатів наук – 6. Відсоток НПП, залучених до викладання навчальних дисциплін за ОП, які мають відповідні наукові ступені, становить 83%.

Матеріально-технічне та програмне забезпечення

Освітній процес відбувається в аудиторіях та лабораторіях, обладнаних аудіовізуальною апаратурою і необхідними технічними засобами. Зокрема, в навчальному процесі використовується:

Комп'ютери (30 шт.); Спеціалізована система захисту інформації Лоза-2; Система контролю та управління доступом (Контроллер для СКУД Redtech BDN-XFH12, зчитувач для СКУД Redtech BDN128-MF, ідентифікатори для СКУД – пластикові картки, блок живлення для СКУД12B\1A SEVEN PS-769W); Адаптер блокування запису на носії інформації Mobile Forensic Universal Bridge; Програмне забезпечення (CredentialsFileView, DataProtectionDecryptor, PasswordFox, Cisco Packet Tracer); Мережеве обладнання (комутатор Cisco SG350-10 (2 шт.); маршрутизатор Cisco RV340-K9 (1 шт.); міжмережевий екран Cisco ASA 5506 (1 шт.)); Кіберполігон Rangeforce.

Інформаційно-методичне забезпечення

Здобувачі освіти мають доступ до книжкового фонду науково-технічної бібліотеки, електронної бібліотеки, електронного каталогу, читальних залів з безкоштовною зоною Wi-Fi, баз даних SCOPUS та Web of Science з комп'ютерів локальної мережі університету. Система дистанційного навчання і консультування забезпечується завдяки платформам й інструментам Google які мають розширений корпоративний функціонал, продуктам Microsoft. Доступ до всіх бібліотечних баз надається користувачам внутрішньої мережі університету.

Важливою складовою інформаційно-методичного забезпечення, притаманного цій ОП, є періодичне наукове фахове видання - журнал "Інформатика та математичні методи в моделюванні" (Національний університет "Одеська політехніка"), одним з наукових напрямків якого є кібербезпека. Результати, що публікуються в журналі, зокрема здобувачами ОПП "Кібербезпека", включаються до відповідних дисциплін навчального плану ОП.

3.3.4 Академічна мобільність

Загальна інформація

Академічна мобільність в університеті заохочується та визнається згідно із процедурами ЄКТС.

Академічна мобільність регламентується Постановою КМУ № 579 «Про затвердження Положення про порядок реалізації права на академічну мобільність» від 12 серпня 2015 року та Положенням університету про порядок реалізації права на академічну мобільність <https://op.edu.ua/document/2501>.

Міжнародна академічна мобільність

Міжнародна академічна мобільність реалізується здобувачами вищої освіти за освітньою програмою у партнерських вищих навчальних закладах та наукових установах поза межами України.

Внутрішня академічна мобільність

Внутрішня академічна мобільність реалізується здобувачами вищої освіти за освітньою програмою у партнерських вищих навчальних закладах та наукових установах в межах України.

3.3.5 Навчання іноземних здобувачів вищої освіти

Іноземні здобувачі вищої освіти та особи без громадянства навчаються на загальних умовах з обов'язковим вивченням в межах освітньої програми дисципліни «Українська мова як іноземна» в обсязі 6–12 кредитів ЄКТС.

3.4 Академічні та професійні права випускників

3.4.1 Академічні права випускників

Здобуття освіти на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти (системі освіти дорослих), підвищення кваліфікації.

3.4.2 Працевлаштування випускників

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.

3.5 Перелік компетентностей випускника

Інтегральна компетентність:

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.

Загальні компетентності:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професії.

ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності:

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-комунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної безпеки та/або кібербезпеки.

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної безпеки та/або кібербезпеки.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки та/або кібербезпеки.

3.6 Програмні результати навчання

ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які

характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

ПРН12. Розробляти моделі загроз та порушника.

ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах організації, підприємства відповідно до вимог нормативно-правових документів.

ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

ПРН21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.

ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН25. Забезпечувати ведення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.

ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

ПРН33. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків.

ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної та/або кібербезпеки.

ПРН36. Виявляти небезпечні сигнали технічних засобів.

ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність

захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.

ПРН44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

ПРН45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

4 ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТІВ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

4.1 Розподіл кредитів ЄКТС між освітніми компонентами

№ з/п	Групи освітніх компонентів	Кількість кредитів ЄКТС / %		
		Обов'язкова частина	Вибіркова частина	Всього за весь термін навчання
1	Навчальні дисципліни загальної підготовки	36 / 15%	12 / 5%	48 / 20%
2	Навчальні дисципліни професійної підготовки	120 / 50%	49.5 / 20.6%	169.5 / 70.6%
3	Курсові проекти	3 / 1.25%	Немає	3 / 1.25%
4	Практична підготовка	9 / 3.75%	Немає	9 / 3.75%
5	Атестація	10.5 / 4.4%	Немає	10.5 / 4.4%
Всього за весь термін навчання		178.5 / 74.4%	61.5 / 25.6%	240 / 100%

4.2 Обов'язкова частина

4.2.1 Освітні компоненти

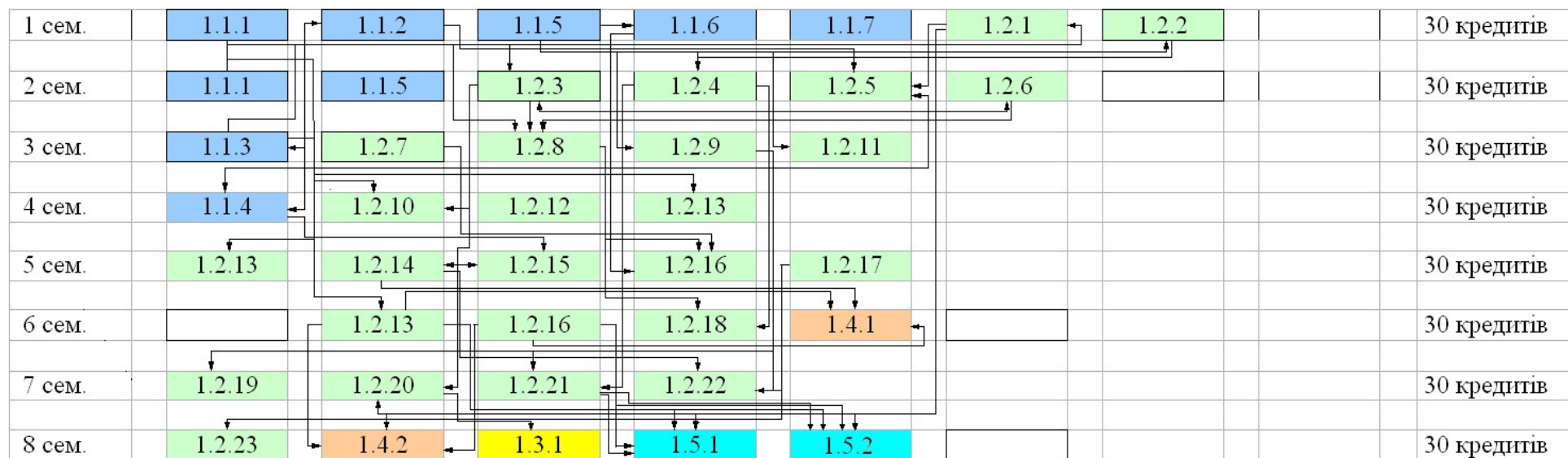
№ з/п	Освітні компоненти	Індивідуальне завдання	Форма контролю	Кількість кредитів ЄКТС
1	2	3	4	5
1 Навчальні дисципліни загальної підготовки				
1.1.1	Іноземна мова ¹		Залік, екзамен	6.0
1.1.2	Історія України та української культури	РР	Залік	3.0
1.1.3	Українська мова (за професійним спрямуванням) ¹		Залік	3.0
1.1.4	Філософія	РР	Залік	3.0
1.1.5	Вища математика	РГР, РГР	Екзамен, екзамен	12.0
1.1.6	Фізика		Екзамен	6.0
1.1.7	Фізичне виховання		Залік	3.0
1.1.8	Іноземна мова ²		Залік	3.0
1.1.9	Українська мова як іноземна ²		Залік, Екзамен	6.0
Всього за групою				36.0
2. Навчальні дисципліни професійної підготовки				
1.2.1	Нормативно-правове та організаційне забезпечення захисту інформації	КР	Екзамен	6.0
1.2.2	Дискретна математика		Залік	3.0
1.2.3	Програмування	КР	Екзамен	6.0
1.2.4	Спеціальні розділи математики		Залік	4.5
1.2.5	Інформаційна безпека держави	КР	Екзамен	6.0

1.2.6	Операційні системи та системне програмування		Залік	4.5
1.2.7	Схемотехніка та архітектура комп'ютерів	РГР	Екзамен	4.5
1.2.8	Спеціальні розділи програмування	КР	Екзамен	6.0
1.2.9	Математичне моделювання в кібербезпеці		Екзамен	4.5
1.2.10	Комп'ютерна вірусологія та антивірусне програмне забезпечення	КР	Екзамен	4.5
1.2.11	Теорія ймовірності та математична статистика	РГР	Залік	4.5
1.2.12	Бази даних та їх захист	РГР	Екзамен	6.0
1.2.13	Інформаційно-телекомунікаційні системи та їх захист		Екзамен, залік, екзамен	12.0
1.2.14	Комплексні системи захисту інформації	РГР	Екзамен	4.5
1.2.15	Системний аналіз в кібербезпеці		Залік	3.0
1.2.16	Програмно-технічні засоби захисту інформації		Екзамен, екзамен	9.0
1.2.17	Управління ризиками		Екзамен	3.0
1.2.18	Основи криптографії		Екзамен	4.5
1.2.19	Методи оцінки захищеності інформаційних систем	РГР	Екзамен	6.0
1.2.20	Управління доступом		Екзамен	4.5
1.2.21	Основи стеганографії		Екзамен	4.5
1.2.22	Управління кібербезпекою	РГР	Екзамен	6.0
1.2.23	Управління та обробка інцидентів кібербезпеки		Екзамен	3.0
Всього за групою				120.0
3 Курсові проекти				
1.3.1	Управління доступом		Захист	3.0
Всього за групою				3.0
4 Практична підготовка				
1.4.1	Виробнича практика		Диф.залік	4.5
1.4.2	Переддипломна практика		Диф.залік	4.5
Всього за групою				9.0
5 Атестація				
1.5.1	Єдиний державний кваліфікаційний іспит			1.5
1.5.2	Кваліфікаційна робота			9.0
Всього за групою				10.5
Загальний обсяг обов'язкових освітніх компонентів				178.5

¹ Не вивчається іноземними студентами

² Вивчається тільки іноземними студентами

4.2.2 Структурно-логічна схема ОП



4.2.3 Матриця відповідності програмних результатів навчання програмним компетентностям

Програмні результати навчання	Загальні компетентності							Спеціальні компетентності											
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12
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											+								
ПРН 26											+								
ПРН 27												+							
ПРН 28														+					+
ПРН 29														+					+
ПРН 30																			+
ПРН 31												+							
ПРН 32													+						
ПРН 33																+			
ПРН 34																+			
ПРН 35														+					
ПРН 36																	+		
ПРН 37																	+		
ПРН 38																	+		
ПРН 39																			+
ПРН 40																	+		
ПРН 41															+				

[illegible]

4.2.4 Матриця забезпечення програмних результатів навчання відповідними освітніми компонентами ОП

Програмні результати навчання	Шифри освітніх компонент ОПП																																				
	1.1.1	1.1.2	1.1.3	1.1.4	1.1.5	1.1.6	1.1.7	1.2.1	1.2.2	1.2.3	1.2.4	1.2.5	1.2.6	1.2.7	1.2.8	1.2.9	1.2.10	1.2.11	1.2.12	1.2.13	1.2.14	1.2.15	1.2.16	1.2.17	1.2.18	1.2.19	1.2.20	1.2.21	1.2.22	1.2.23	1.3.1	1.4.1	1.4.2	1.5.1	1.5.2		
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																												+					+				
ПРН 26																												+					+				
ПРН 27																					+																
ПРН 28																						+				+	+					+	+	+	+	+	
ПРН 29																						+					+	+				+	+	+	+	+	
ПРН 30																										+	+	+				+	+	+	+	+	
ПРН 31																						+															
ПРН 32																									+						+						
ПРН 33																								+								+		+	+	+	
ПРН 34												+																		+							
ПРН 35																					+												+	+	+	+	
ПРН 36																							+										+				
ПРН 37																							+										+				
ПРН 38																							+														
ПРН 39								+																			+				+	+					
ПРН 40																							+														
ПРН 41																															+		+				
ПРН 42																															+						
ПРН 43																															+						

[illegible]

4.3 Вибіркова частина

Обсяг вибірових освітніх компонентів за весь строк навчання за освітньою програмою становить не менше 25 % від загального обсягу кредитів ЄКТС.

Здобувачі вищої освіти можуть обирати освітні компоненти для формування власної індивідуальної траєкторії навчання з каталогів вибірових освітніх компонентів або з навчальних планів інших діючих освітніх програм. Вибір освітніх компонентів здобувачами здійснюється відповідно до «Порядку формування індивідуальної освітньої траєкторії здобувачами вищої освіти» в Одеській політехніці.

5 АТЕСТАЦІЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форма атестації: Єдиний державний кваліфікаційний іспит.

Вимоги до єдиного державного кваліфікаційного іспиту:

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

6 СИСТЕМА ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Система внутрішнього забезпечення якості вищої освіти функціонує в Університеті відповідно до Закону України «Про вищу освіту», Закону України «Про освіту», «Стандартів і рекомендацій щодо забезпечення якості в Європейському просторі вищої освіти» Європейської асоціації із забезпечення якості вищої освіти, національного стандарту «Системи управління якістю» ДСТУ ISO 9001:2015 та професійних стандартів.

1. Принципи і процедури забезпечення якості вищої освіти встановлені в «Політиці Університету в сфері якості» (<https://op.edu.ua/document/10107>) та Положенні про систему внутрішнього забезпечення якості (<https://op.edu.ua/document/8818>), Положенні про центр із забезпечення якості вищої освіти (<https://op.edu.ua/document/8852>), Положенні про Раду з якості освітньої діяльності в Національному університеті «Одеська політехніка» (<https://op.edu.ua/document/8817>).

2. Моніторинг та періодичний перегляд освітніх програм здійснюється відповідно до Процедури з розроблення освітніх програм (<https://op.edu.ua/document/3355>).

3. Результати щорічного оцінювання здобувачів вищої освіти та НПП відповідно до «Положення про щорічне оцінювання науково-педагогічних і педагогічних працівників Одеської політехніки» (<https://op.edu.ua/document/7233>), «Процедури організації моніторингу оцінювання здобувачів вищої освіти та аналізу освітньої діяльності» (<https://op.edu.ua/document/2536>) оприлюднено за посиланням: <https://op.edu.ua/about/reports>.

4. Підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників відбувається у відповідності до Порядку підвищення кваліфікації педагогічних і науково-педагогічних працівників (<https://op.edu.ua/document/2518>).

5. НПП забезпечується можливість підвищити кваліфікацію та пройти стажування в Центрі дистанційної освіти або в Центрі педагогічної майстерності Університету <https://op.edu.ua/quality/pedagogic-master>.

6. Організація освітнього процесу відбувається у відповідності до Положення про організацію освітнього процесу в Національному університеті «Одеська політехніка»

(<https://op.edu.ua/document/9419>); процедури вибору дисциплін визначено в Положенні про порядок організації вивчення вибіркових освітніх компонентів (<https://op.edu.ua/document/3354>), самостійна робота здобувачів забезпечується відповідно до Положення про робочу програму навчальної дисципліни (<https://op.edu.ua/document/2549>) та унормовується відповідно до Положення про самостійну роботу здобувачів вищої освіти (<https://op.edu.ua/document/2294>).

7. Ефективне управління освітнім процесом забезпечується за допомогою широко розвиненої інформаційної системи Університету (<https://is.op.edu.ua>).

8. ОП розміщені в «Каталозі освітніх програм» (<https://op.edu.ua/education/programs>). Доступна інформація про всі ОП, ступені вищої освіти та кваліфікації.

9. Перевірка на академічний плагіат відбувається у відповідності до «Порядку перевірки навчальних, кваліфікаційних, навчально-методичних та наукових робіт на унікальність та наявність академічного плагіату» (<https://op.edu.ua/document/2754>).

10. Для осіб з особливими потребами створено групи психологічно-педагогічного супроводу інклюзивного навчання (<https://op.edu.ua/document/2542>).

11. В Університеті діє Антикорупційна програма запобігання та виявлення корупції (<https://op.edu.ua/document/8518>).