

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

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА  
«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»**

Першого (бакалаврського) рівня вищої освіти  
за спеціальністю 125 Кібербезпека та захист інформації  
галузі знань 12 Інформаційні технології

**ЗАТВЕРДЖЕНО  
ВЧЕНОЮ РАДОЮ**

Голова вченої ради \_\_\_\_\_ М.О. Фролов

(протокол № \_\_\_ від «\_\_\_» \_\_\_\_\_ 2023 р.)

Освітня програма вводиться в дію з 2023/2024 н.р.

В. о. ректора \_\_\_\_\_ М.О. Фролов

(наказ № \_\_\_ від «\_\_\_» \_\_\_\_\_ 2023 р.)

**Запоріжжя  
2023**

## Аркуш погодження

Гарант освітньої програми

О. В. Кудін

Декан математичного факультету

С. І. Гоменюк

Керівник навчально-методичного відділу

Л. О. Нестеренко

Начальник відділу моніторингу якості освіти і ліцензування

М. А. Томченко

Проректор з науково-педагогічної та навчальної роботи

О. І. Гура

## Передмова

Запорізький національний університет. «Кібербезпека»: освітньо-професійна програма.

Освітньо-професійну програму розроблено робочою групою відповідно до стандарту вищої освіти України підготовки бакалавра за спеціальністю 125 Кібербезпека, затвердженого наказом МОН України № 1074 від 04.10.2018

у складі:

№ з/п	Прізвище, ім'я, по батькові	Науковий ступінь, вчене звання
1	Кудін Олексій Володимирович (гарант освітньої програми)	кандидат фізико-математичних наук, доцент по кафедрі програмної інженерії
2	Шило Галина Миколаївна	доктор технічних наук, доцент по кафедрі конструювання та технології виробництва радіоапаратури
3	Чопоров Сергій Вікторович	доктор технічних наук, професор по кафедрі програмної інженерії

Враховано вимоги:

Стандарту вищої освіти України підготовки бакалавра за спеціальністю 125 Кібербезпека, затвердженого наказом МОН України № 1074 від 04.10.2018

РОЗГЛЯНУТО на вченій раді математичного факультету ЗНУ

Протокол № від

Рецензії стейкхолдерів:

1. Чхан Н. В., директорка ФОП «Чхан Наталія Вікторівна» (компанія «DarkLime»), м. Запоріжжя.
2. Кононенко В.Р., технічний директор ТОВ «Комп'ютулс», м. Запоріжжя.
3. Рожок С.В., генеральний директор ТОВ «ЕПАМ СИСТЕМЗ», м Харків.
4. Татієвський Д.М., генеральний директор ТОВ ««АЙТІ ДІМЕНШН», м. Запоріжжя.

•

## I. Профіль освітньої програми

<b>1– Загальна інформація</b>	
Повна назва закладу вищої освіти	Запорізький національний університет
Ступінь вищої освіти	Бакалавр
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньої програми бакалавра 240 кредитів ЄКТС; нормативний термін навчання 3 роки 10 місяців.
Назва кваліфікації	<i>Кваліфікація в дипломі:</i> Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека Освітня програма Кібербезпека  <i>Освітня кваліфікація:</i> бакалавр з кібербезпеки
Наявність акредитації	Неакредитовано.
Цикл / рівень	Національна рамка кваліфікацій України – 6 рівень QF-EHEA – перший цикл вищої освіти EQF-LLL – 6 рівень
Передумови	На базі повної загальної середньої освіти; ступеня «молодший бакалавр» або «фаховий молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»)
Термін дії	До 01.07.2027
Мова викладання	Українська
Інтернет-адреса постійного розміщення освітньої програми	
<b>2 – Мета освітньої програми</b>	
<p>Підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки, а також технології, моделі та методи цифрової економіки.</p> <p>Мета освітньої програми відповідає стратегії розвитку Запорізького національного університету 2023-2028 років щодо формування суспільства майбутнього на засадах концепції сталого розвитку.</p>	
<b>3 – Характеристика освітньої програми</b>	

<p>Предметна область (галузь спеціальність, предметна спеціальність або спеціалізація )</p>	<p>Галузь знань 12 Інформаційні технології          Спеціальність 125 Кібербезпека  <i>Об'єкт вивчення та діяльності:</i>          – 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.  <i>Цілі навчання:</i> підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки  <i>Теоретичний зміст предметної області:</i>          Знання          – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;          – принципів супроводу систем та комплексів 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.  <i>Методи, методики та технології:</i>          Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення кібербезпеки.  <i>Інструменти та обладнання:</i>          – системи розробки, забезпечення, моніторингу та</p>
---	--

	контролю процесів кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Професійна підготовка фахівців у сфері кібербезпеки.
Основний фокус освітньої програми та спеціалізації	Системи та процеси кіберпростору, інформаційні технології захисту інформації, технології розробки та використання програмного забезпечення у сфері кібербезпеки. Ключові слова: кібернетична безпека, інформаційно-телекомунікаційні системи, програмні та апаратні засоби захисту інформації, системи і технології кібербезпеки, математичні методи кібербезпеки, аудит кіберінцидентів, технічний аудит
Особливості програми	Освітньо-професійна програма реалізує комплексний підхід до формування та розвитку компетентностей для здійснення професійної діяльності у сфері кібербезпеки. Програма враховує регіональну специфіку та потреби роботодавців у сфері кібербезпеки та суміжних галузей.
<b>4 – Придатність випускників до працевлаштування та подальшого навчання</b>	
Придатність до працевлаштування	Діяльність як фахівця у сфері кібербезпеки. Випускники можуть працювати за професіями згідно з Національним класифікатором професій ДК 003:2010: 3139 Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки 3121 Фахівець з інформаційних технологій. 2139.2 Аналітик систем захисту інформації та оцінки вразливостей 2139.2 Аналітик загроз безпеки 2132.2 Розробник систем захисту інформації. 2149 Професіонали із організації інформаційної безпеки.
Подальше навчання	Можливість продовження навчання за освітніми програмами другого (магістерського) рівня вищої освіти, а також здобувати додаткові кваліфікації в системі освіти дорослих
<b>5 – Викладання та оцінювання</b>	
Викладання та навчання	Студентоцентроване, інтерактивне, диференційоване, проблемно-орієнтоване навчання. Освітній процес

	<p>підтримано системою електронного забезпечення навчання Moodle.</p> <p>Форми організації освітнього процесу та види навчальних занять: лекції, семінари, лабораторні, практичні заняття, самостійна робота, консультації з викладачами</p>
Оцінювання	<p>Поточний контроль, підсумковий контроль (заліки, екзамени, тести, захист звітів з практики, захист курсових робіт, захист кваліфікаційної роботи бакалавра).</p> <p>Оцінювання навчальних досягнень студентів здійснюється за 100-бальною шкалою</p>
<b>6 – Програмні компетентності</b>	
Інтегральна компетентність (ІК)	<p>Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів комп'ютерних наук, інформаційних технологій і характеризується комплексністю та невизначеністю умов</p>
Загальні компетентності (ЗК)	<p>КЗ 1 Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 2 Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ 3 Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>КЗ 4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5 Здатність до пошуку, оброблення та аналізу інформації.</p> <p>КЗ 6 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;</p> <p>КЗ 7 Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та зако-номірностей 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.</p>
Спеціальні (фахові),	<p>ФК 1 Здатність застосовувати законодавчу та нормативно-</p>

предметні)  
компетентності СК

правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

ФК 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/ або кібербезпеки.

ФК 3 Здатність до використання програмних та програмно- апаратних комплексів засобів захисту інформації в інформаційно- телекомунікаційних (автоматизованих) системах.

ФК 4 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

ФК 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки..

ФК 6 Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

ФК 7 Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно- правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

ФК 8 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

ФК 9 Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою

ФК 10 Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

ФК 11 Здатність виконувати моніторинг процесів функціонування інформаційних інформаційно-телекомунікаційних (автоматизованих) систем згідно

	<p>встановленої політики інформаційної та/ або кібербезпеки.</p> <p>ФК 12 Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки</p>
<p>Спеціальні компетентності, визначені закладом вищої освіти у межах спеціальності та освітньо-професійної програми</p>	<p>СК 1 Здатність розробляти та застосовувати математичні моделі, аналізувати статистичні дані розробляти прогностичні моделі для виявлення та дослідження загроз у комп'ютерних системах.</p> <p>СК 2 Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в області кібербезпеки, що характеризуються комплексністю та невизначеністю умов, які потребують застосування математичних теорій та методів.</p> <p>СК 3 Здатність до проектування та реалізації методів захисту інформації у мобільних пристроях.</p> <p>СК 4 Здатність до проектування та реалізації вебзастосунків з урахуванням вимог кібербезпеки.</p>
<b>7 – Програмні результати навчання</b>	
<p>ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації</p> <p>ПРН 2 Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність</p> <p>ПРН 3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності</p> <p>ПРН 4 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</p> <p>ПРН 5 Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат</p> <p>ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності</p> <p>ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;</p>	

- ПРН 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
- ПРН 9 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки
- ПРН 10 Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем
- ПРН 11 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах
- ПРН 12 Розробляти моделі загроз та порушника
- ПРН 13 Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних
- ПРН 14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
- ПРН 15 Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
- ПРН 16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів
- ПРН 17 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
- ПРН 18 Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
- ПРН 19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах
- ПРН 20 Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах
- ПРН 21 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
- ПРН 22 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-

телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки

ПРН 23 Реалізувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах

ПРН 24 Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових)

ПРН 25 Забезпечувати введення 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

ПРН 26 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем

ПРН 27 Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах

ПРН 28 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

ПРН 29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно-телекомунікаційних системах, ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів

ПРН 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем

ПРН 31 Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем

ПРН 32 Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки

ПРН 33 Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

ПРН 34 Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та\або кібербезпеки відповідно до цілей і завдань організації

ПРН 35 Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до

інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки;

ПРН 36 Виявляти небезпечні сигнали технічних засобів

ПРН 37 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;

ПРН 38 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації

ПРН 39 Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах

ПРН 40 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН 41 Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур

ПРН 42 Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки

ПРН 43 Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

ПРН 44 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

ПРН 45 Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

ПРН 46 Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах

ПРН 47 Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації

ПРН 48 Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах

ПРН 49 Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно- телекомунікаційних системах;

ПРН 50 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)

ПРН 51 Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах

ПРН 52 Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах

ПРН 53 Вирішувати задачі аналізу програмного коду на наявність можливих загроз

ПРН 54 Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні

### **8 – Ресурсне забезпечення реалізації програми**

<b>Кадрове забезпечення</b>	Освітньо-професійна програма реалізується та забезпечується висококваліфікованими викладачами, які мають навчально-методичної та наукової роботи, а також досвід практичної діяльності в сфері ІТ
<b>Матеріально-технічне забезпечення</b>	Забезпеченість освітньої програми навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає її потребам. Наявна необхідна соціально-побутова інфраструктура, кількість місць в гуртожитках відповідає вимогам. Зокрема для проведення лабораторних занять, інформаційного пошуку та обробки результатів наявні спеціалізовані комп'ютерні класи університету з необхідним програмним забезпеченням та необмеженим відкритим доступом до Інтернет-мережі, спеціалізовані навчальні аудиторії, обладнані інтерактивними дошками, спеціалізованим аудіовізуальним обладнанням
<b>Інформаційне та навчально-методичне забезпечення</b>	Офіційний веб-сайт Запорізького національного університету ( <a href="https://www.znu.edu.ua/">https://www.znu.edu.ua/</a> ), містить інформацію про освітні програми, навчальну, наукову, виховну, видавничу, атестаційну (науково-педагогічних кадрів) діяльність, структурні підрозділи, правила прийому, контакти. Фонд наукової бібліотеки: вітчизняні та закордонні фахові періодичні видання відповідного або спорідненого профілю, науково-методичні розробки, в тому числі в електронному

	<p>вигляді (<a href="http://library.znu.edu.ua/">http://library.znu.edu.ua/</a>). міжнародних наукометричних баз Web of Science, Scopus.</p> <p>Освітній процес підтримано системою електронного забезпечення навчання Moodle (<a href="https://moodle.znu.edu.ua/">https://moodle.znu.edu.ua/</a>)</p>
<b>9 – Академічна мобільність</b>	
<b>Національна кредитна мобільність</b>	На основі двосторонніх договорів про співпрацю і партнерські відносини між ЗНУ та закладами вищої освіти України, що здійснюють підготовку за освітньою програмою «Кібербезпека»
<b>Міжнародна кредитна мобільність</b>	На основі двосторонніх договорів про співпрацю і партнерські відносини між ЗНУ та іноземними закладами вищої освіти
<b>Навчання іноземних здобувачів вищої освіти</b>	Можливе навчання (на загальних умовах або за індивідуальним планом) іноземних студентів за умови додаткової мовної підготовки, якщо рівень володіння українською мовою є недостатнім

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

### 2.1. Перелік компонент освітньо-професійної програми «Кібербезпека»

Код навч. дисц.	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (робота), види практики, кваліфікаційна робота тощо)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
<b>I. ОBOB'ЯЗКОВІ ДИСЦИПЛІНИ</b>			
<b>1.1. Цикл загальної підготовки</b>			
ЗП 1	Історія України	3	екзамен
ЗП 2	Українська мова професійного спрямування	3	екзамен
ЗП 3	Фізичне виховання	3	залік
ЗП 4	Іноземна мова	3	залік
	Іноземна мова	5	екзамен
ЗП 5	Вступ до спеціальності	4	залік
ЗП 6	Історія науки та техніки	3	залік
ЗП 7	Нормативно-правове забезпечення інформаційної безпеки	3	екзамен
ЗП 8	Права і свободи людини та громадянина в Україні	3	залік
<b>1.2. Цикл професійної підготовки спеціальності</b>			
ППС 1	Лінійна алгебра та аналітична геометрія	3	екзамен
ППС 2	Математичний аналіз	4	залік
	Математичний аналіз	4	екзамен
ППС 3	Дискретні структури	6	залік
ППС 4	Основи криптографії	4	залік
ППС 5	Програмування	6	залік
	Програмування	4	екзамен
	Програмування	5	екзамен
ППС 6	Фізика	5	екзамен
ППС 7	Цифрова схемотехніка	3	залік
ППС 8	Комп'ютерні мережі та їх безпека	4	екзамен
ППС 9	Операційні системи та їх безпека	5	екзамен
ППС 10	Проектування та впровадження комплексних систем захисту інформації	6	залік
	Курсова робота з дисципліни "Проектування та впровадження комплексних систем захисту інформації"	1	залік
ППС 11	Теорія інформації та кодування даних	4	екзамен
ППС 12	Основи криптоаналізу	4	екзамен
ППС 13	Ідентифікація об'єктів та користувачів	4	екзамен
ППС 14	Системи технічного захисту інформації	4	екзамен
ППС 15	Управління інформаційною та кібербезпекою	3	залік

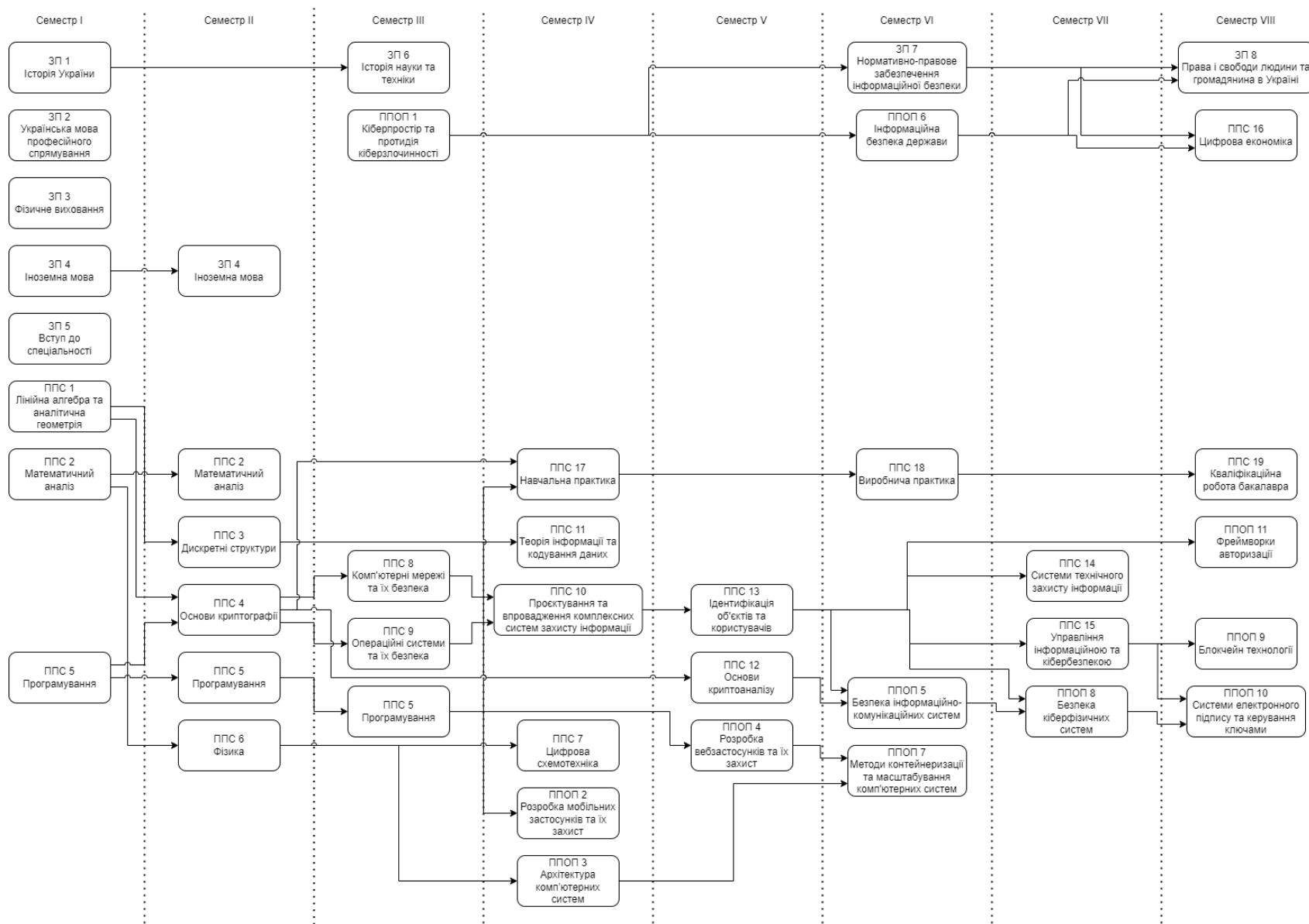
ППС 16	Цифрова економіка	3	екзамен
ППС 17	Навчальна практика	3	залік
ППС 18	Виробнича практика	6	залік
ППС 19	Кваліфікаційна робота бакалавра	9	екзамен
<b>1.3. Цикл професійної підготовки освітньої програми</b>			
ППОП 1	Кіберпростір та протидія кіберзлочинності	5	екзамен
ППОП 2	Розробка мобільних застосунків та їх захист	5	екзамен
ППОП 3	Архітектура комп'ютерних систем	7	екзамен
ППОП 4	Розробка вебзастосунків та їх захист	5	екзамен
	Курсова робота з дисципліни "Розробка вебзастосунків та їх захист"	1	залік
ППОП 5	Безпека інформаційно-комунікаційних систем	4	залік
ППОП 6	Інформаційна безпека держави	3	екзамен
ППОП 7	Методи контейнеризації та масштабування комп'ютерних систем	3	залік
ППОП 8	Безпека кіберфізичних систем	5	екзамен
ППОП 9	Блокчейн технології	4	екзамен
ППОП 10	Системи електронного підпису та керування ключами	4	залік
ППОП 11	Фреймворки авторизації	4	залік
<b>Загальний обсяг обов'язкових компонентів:</b>		<b>180</b>	
<b>II. ВИБІРКОВІ ДИСЦИПЛІНИ</b>			
<b>2.1. Блок дисциплін вільного вибору студента в межах Університету</b>			
ВСУ 1	Вибіркова дисципліна № 1	3	залік
ВСУ 2	Вибіркова дисципліна № 2	3	залік
ВСУ 3	Вибіркова дисципліна № 3	3	залік
ВСУ 4	Вибіркова дисципліна № 4	3	залік
ВСУ 5	Вибіркова дисципліна № 5	3	залік
ВСУ 6	Вибіркова дисципліна № 6	3	залік
ВСУ 7	Вибіркова дисципліна, що забезпечує рухову активність, фізичну підготовку	3	залік
ВСУ 8	Вибіркова дисципліна, що забезпечує формування компетентності з української і зарубіжної культури	3	залік
ВСУ 9	Вибіркова дисципліна, що забезпечує формування компетентності з медичної допомоги, безпеки життєдіяльності, охорони праці, цивільного захисту	3	залік
ВСУ 10	Вибіркова дисципліна, що забезпечує формування компетентності з філософії, соціально-політичних наук	3	залік
<b>2.2. Блок дисциплін вільного вибору студента в межах спеціальності*</b>			
ВСС 1	Вибіркова дисципліна № 1	5	залік
ВСС 2	Вибіркова дисципліна № 2	5	залік

ВСС 3	Вибіркова дисципліна № 3	5	залік
ВСС 4	Вибіркова дисципліна № 4	5	залік
ВСС 5	Вибіркова дисципліна № 5	5	залік
ВСС 6	Вибіркова дисципліна № 6	5	залік
<b>Загальний обсяг вибірових компонентів:</b>		<b>60</b>	
<b>Загальний обсяг освітньої програми</b>		<b>240</b>	

**\*Перелік дисциплін вільного вибору студента в межах спеціальності**

Шифр	Назва дисципліни
ВСС 1	Правове забезпечення інформаційної безпеки
	Інтелектуальна власність систем безпеки
	Методи та технології інформаційних війн
ВСС 2	Документообіг з обмеженим доступом
	Системи електронної комерції
	Реагування на кіберінциденти
ВСС 3	Децентралізовані системи
	Промислове шпигунство
	Проектування та розробка вебдодатків
ВСС 4	Програмування розподілених систем
	Блокчейн технології захисту інформації
	Засоби JavaScript для захисту інформації
ВСС 5	Методи кібербезпеки у робототехніці
	Програмування високонавантажених систем
	Методи виявлення порушників у мережі
ВСС 6	Методи кібербезпеки у програмуванні мобільних пристроїв
	Основи наукових досліджень
	Нейромережеві методи у кібербезпеці

## 2.2 Структурно-логічна схема освітньо-професійної програми “Інформаційні системи та технології”



### **III. Форма атестації здобувачів вищої освіти**

Атестація здобувачів вищої освіти освітнього рівня «бакалавр» спеціальності 125 Кібербезпека здійснюється у формі єдиного держаного кваліфікаційного іспиту. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.





