МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

Рівень віщої освіти: другий (магістерський) рівень
(назва рівня вищої освіти)

Ступінь вищої освіти: Магістр

Галузь знань: 12 «Інформаційні технології»
(шифр та назва галузі знань)

Спеціальність: 125 «Кібербезпека»
(код і назва спеціальності)

Кваліфікація: 2149.2 Професіонал із організації інформаційної безпеки.
2310 Викладач університетів та вищих навчальних закладів
(шифр і назва кваліфікації)

Затверджено вченою радою
НУ «Запорізька політехніка»
(протокол № від «__»____2020 р.)
Голова вченої ради
НУ «Запорізька політехніка», проф.
_____ С.Б. Бєліков
« ___ » _____ 2020 р.

Запоріжжя
2020

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»

Рівень вищої освіти: другий (магістерський) рівень
(назва рівня вищої освіти)

Ступінь вищої освіти: Магістр

Галузь знань 12 «Інформаційні технології»
(шифр та назва галузі знань)

Спеціальність 125 «Кібербезпека»
(код і назва спеціальності)

Кваліфікація 2149.2 Професіонал із організації інформаційної безпеки.
2310 Викладач університетів та вищих навчальних закладів
(шифр і назва кваліфікації)

Розробники програми:

1. **Карпуков Л.М.** – д-р техн. наук, професор.
2. **Воскобойник В.О.** – канд. техн. наук, доцент, професор.
3. **Козіна Г. Л.** – канд. фіз-мат. наук, доцент.
4. **Матвейчук О.В. –** бакалавр, студент магістерської групи РТ-819м.

УЗГОДЖЕНО:
Проректор з науково-педагогічної роботи
та питань перспектив розвитку університету
д.т.н., проф.
_____ Піза Д.М.
« ___ » _____ 2020 р.

ВНЕСЕНО
Кафедрою «Захист інформації»
Протокол № 7 від 12 лютого 2020 р.
Завідувач кафедри _____ Карпуков Л.М.

СХВАЛЕНО
Науково-методичною комісією ФРЕТ
Протокол № 6 від 24 лютого 2020 р.
Голова НМК факультету _____ Кабак В.С.

ПРЕДСТАВНИК РОБОТОДАВЦЯ
Начальник бюро інформаційної безпеки АТ «Мотор Січ».
_____ Іголкін М. В.

НАДАНО ЧИННОСТІ ТА ВВЕДЕНО У ДІЮ
Наказ НУ «Запорізька політехніка» №__ від «__» _____ 2020 р.

1 Преамбула

Освітньо-професійна програма (ОПП) «Безпека інформаційних і комунікаційних систем» розроблена на підставі Закону України «Про вищу освіту» №2145-VIII від 05.09.2017 р., листа Міністерства освіти і науки України №1/9-239 від 28.04.2017 р. та наказу МОН України № 1254 від 01.10.2019 р. із змінами та доповненнями.

ОПП розроблена робочою групою (науково-методичною комісією спеціальності 125 Кібербезпека) у складі:

1. **Карпуков Леонід Матвійович** – керівник проектної групи, доктор технічних наук, професор, завідувач кафедри захисту інформації Національного університету «Запорізька політехніка»;
2. **Воскобойник Володимир Олександрович** - член проектної групи, кандидат технічних наук, доцент, професор кафедри захисту інформації Національного університету «Запорізька політехніка».
3. **Козіна Галина Леонідівна** - член проектної групи, кандидат фізико-математичних наук, доцент кафедри захисту інформації Національного університету «Запорізька політехніка».
4. **Матвейчук Олена Валеріївна** – член проектної групи, бакалавр, студентка гр. РТ-819м, яка навчається за програмою магістра Національного університету «Запорізька політехніка».

ОПП є нормативним документом, у якому визначаються термін та зміст навчання, форми державної атестації, встановлюються вимоги до змісту та результатів освітньої діяльності з професійної підготовки магістра за спеціальністю 125 «Кібербезпека».

Освітньо-професійна програма визначає:

- обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти;
- перелік компетентностей випускника;
- нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання;

Ця освітньо-професійна програма розроблена як тимчасовий документ до затвердження відповідного стандарту вищої освіти України за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти.

2 ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Форми навчання	Дена, заочна
Освітня кваліфікація	Магістр з кібербезпеки за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем»
Кваліфікація в дипломі	Диплом магістра, одиничний, 90 кредитів ЄКТС 2149.2 Професіонал із організації інформаційної безпеки 2310 Викладач університетів та вищих навчальних закладів НРК України – 8 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Наявність акредитації	Міністерство освіти і науки України: **Сертифікат** про акредитацію спеціальності серія НД № 0888816 від 01.03 2016 р. Термін дії сертифікату по березень 2026 р.
Опис предметної області	***Об'єкт(и) вивчення та/або діяльності:*** сфера забезпечення інформаційної та кібербезпеки. - ***Цілі навчання:*** - підготовка фахівців, здатних розв'язувати складні спеціалізовані задачі і практичні проблеми та реалізовувати інноваційні проекти у сфері забезпечення інформаційної та/або кібербезпеки. - ***Теоретичний зміст предметної області:*** наукові теорії, поняття, закони, принципи виявлення й ідентифікації ризиків та забезпечення інформаційної та/або кібербезпеки. - ***Методи, методики та технології:*** загальнонаукові методи пізнання та дослідницької діяльності, математичні, алгоритмічні, програмно-апаратні методи і технології захисту інформації. - ***Інструменти та обладнання:***сучасне інформаційно-комунікаційне обладнання, інформаційні системи та спеціалізоване програмне забезпечення інформаційної та/або кібербезпеки.
Академічні права	Можливість навчання за кваліфікаційними рівнями: НРК України – 9, рівень FQ-EHEA – третій цикл, EQF-LLL – 8

випускників	рівень за спеціальністю “Кібербезпека”; отримання післядипломної освіти на споріднених та інших спеціальностях; підвищення кваліфікації.
Праце-влаштування випускників	Випускники можуть працювати в державному та приватному секторах України та Європейського Союзу у таких сферах економічної діяльності (за КВЕД ДАК 009:2010): **62** Комп'ютерне програмування, консультування та пов'язана з ними діяльність. **63.1** Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність; веб-портали. **80.2** Обслуговування систем безпеки. А саме: 1) адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.; 2) застосування засобів антивірусного захисту (ESET, McAfee, Zilly, etc.), програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, etc.); 3) створення технічної, проектної та експлуатаційної документації інформаційно-комунікаційних систем (далі – ІКС) та систем захисту інформації (далі – СЗІ); 4) налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; 5) проведення моніторингу несанкціонованої активності в обчислювальних системах; 6) створення, впровадження та експлуатації комплексних систем захисту інформації (далі – КСЗІ), а також СЗІ в складі інформаційно-телекомунікаційних (далі – ІТС) та обчислювальних систем; 7) формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; 8) проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки; 9) підтримка наукових досліджень, педагогічна діяльність і т.п. Магістрам, які здобули освіту за освітньою програмою «Безпека інформаційних і комунікаційних систем» присвоюється кваліфікація (за КВЕД ДК 003:2010): **2149.2** Професіонал із організації інформаційної безпеки; **2310** Викладач університетів та вищих навчальних закладів. Вони можуть обіймати такі посади, як: - керівник служби інформаційної безпеки підприємства; - керівник служби захисту інформації; - керівник аналітичного відділу з забезпечення кібербезпеки;

	- керівник відділу стратегічного планування та прогнозування стану кібербезпеки об'єкту інформаційної діяльності; - керівник інформаційної служби; - керівник служби з інформаційно-аналітичної роботи; - керівник служби з реагування на кіберінцеденти; - інші керівні та профільні місця за фахом в компаніях, підприємствах приватного та державного сектору в сфері забезпечення інформаційної та кібернетичної безпеки ; - викладач університетів та вищих навчальних закладів; - науковий співробітник (кібербезпека, телекомунікації, комп'ютерні мережі, проекти та програми); - професіонал з управління проектами та програмами то що.

3 Обсяг кредитів ЄКТС для здобуття ступеня магістра зі спеціальності 125 Кібербезпека

Цикли підготовки	Кількість кредитів ECTS
Освітньо-професійна програма магістра за циклами:	**90**
Цикл професійної підготовки	**90**
у т. ч.	
базові навчальні дисципліни	67 (74%)
вибіркові навчальні дисципліни	23 (26%)

Примітка: 1 кредит – 30 годин.

Термін навчання: денна форма – один рік 4 місяці; заочна форма – один рік 4 місяці.

4 Перелік компетентностей випускника за освітньо-професійної програмою «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека»

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов і вимог.
Загальні компетентності	**ЗК 1**. Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово **ЗК 4**. Здатність до здобування нових знань, накопичення

	наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях **ЗК 5.**Здатність до виявлення, розуміння та аналітичного дослідження проблем за професійним спрямуванням **ЗК 6.** Здатність до сприйняття й спроможність розв'язувати комплексні задачі та практичні проблеми технологій обробки, аналізу, перетворювання й передавання інформації **ЗК 7**. Здатність використовувати методи фундаментальних та загально-професійних наук для розв'язання задач кібербезпеки
Спеціальні (фахові, предметні) компетентності	**СК 1.** Здатність до застосування сучасних інформаційних і технологічних технологій у сфері захисту інформації **СК 2.** Здатність до виявлення вразливостей та забезпечення безпеки дротових і бездротових мереж, розслідування інцидентів інформаційної та/або кібербезпеки та протидії злоякісному програмному забезпеченню. **СК 3.** Здатність до забезпечення безпеки Web- ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження. **СК 4.** Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки. **СК 5.** Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та їх супроводження **СК 6.** Здатність використовувати нормативно-правові, управлінсько-організаційні, математичні, технічні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки. **СК 7.** Здатність організовувати та проводити наукові дослідження, пов'язані із застосуванням математичних та технічних методів для аналізу та дослідження процесів та систем забезпечення інформаційної та кібернетичної безпеки.

Примітка: з метою забезпечення кореляції визначених компетентностей з класифікацією компетентностей НРК використовується матриця відповідності визначених компетентностей та дескрипторів НРК, яка є інформаційним додатком (Таблиця 1 Пояснювальної записки).

5 НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ЗА СПЕЦІАЛЬНІСТЮ 125 «КІБЕРБЕЗПЕКА» ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ», СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Результати навчання	**РН 1.** Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **РН 2**. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності **РН 3.** Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. **РН 4**. Вміти застосовувати спеціалізоване програмне забезпечення, сучасні інформаційні технології у сфері захисту інформації. **РН 5.** Знати методи організації захищеної передачі даних у незахищеному середовищі. **РН 6.** Вміти виявляти загрози проникнення або доступу зловмисників до мереж обробки інформації. **РН 7.** Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів). **РН 8.** Знати методи і способи тестування мережевих ресурсів на наявність вразливостей безпеки **РН 9.** Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки. **РН 10.** Вміти використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності **РН 11.** Вміти застосовувати сучасні методики планування експерименту при побудові математично-статистичних моделей процесів та об’єктів в галузі захисту інформації **РН 12.** Знати особливості побудови математичних моделей при вирішенні задач захисту інформації, вміти їх розробляти та володіти науковими підходами до застосування цих моделей у задачах оптимізації захисту інформації.

6 ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація випускників освітньої програми за спеціальністю 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної магістерської роботи. Кваліфікаційна робота виконується студентом самостійно та є закінченою науково-дослідною роботою, що пов'язана з вирішенням актуальних завдань, зумовлених особливостями підготовки магістрів за зазначеною спеціальністю. Робота має свідчити про те, що її автор володіє сучасними методами наукових досліджень і спроможний самостійно проводити наукові дослідження, що мають теоретичне і практичне значення. Вимоги до змісту, об'єму і структури кваліфікаційної магістерської роботи визначаються методичними вказівками до дипломного проектування магістрів за спеціальністю 125 «Кібербезпека». Теми кваліфікаційних робіт мають бути оприлюднені на офіційному сайті кафедри захисту інформації. Кваліфікаційна робота магістра підлягає обов'язковій перевірці на академічний плагіат та має бути оприлюднена шляхом розміщення її на офіційному сайті вищого навчального закладу або структурного підрозділу до публічного захисту. Атестація здійснюється відкрито і публічно та завершується видачею документу встановленого зразку про присудження йому ступеня магістр з присвоєнням кваліфікації (за КВЕД ДК 003:2010): **2149.2** Професіонал із організації інформаційної безпеки. - **2310** Викладач університетів та вищих навчальних закладів
Вимоги до заключної кваліфі-каційної роботи	Національний університет «Запорізька політехніка» розробляє та затверджує: – положення про Екзаменаційну комісію (ЕК); – порядок перевірки кваліфікаційних дипломних магістерських робіт на плагіат; – нормативи унікальності текстів кваліфікаційних дипломних магістерських робіт. Атестація осіб, які здобувають ступінь магістра, здійснюється ЕК, до складу якої можуть включатися представники роботодавців та їх об'єднань. Атестація здійснюється відкрито і публічно. Дипломна робота магістра допускається до захисту перед ЕК за умови, якщо рівень її унікальності (оригінальності)

	відповідає нормативу, який офіційно затверджений НУ «Запорізька політехніка. Вимоги до заключної кваліфікаційної роботи: Кваліфікаційна дипломна магістерська робота – це навчально-наукова робота студента, яка виконується на завершальному етапі здобуття кваліфікації магістра з кібербезпеки для встановлення відповідності отриманих здобувачами вищої освіти результатів навчання (компетентностей) вимогам стандартів вищої освіти. Вона є кваліфікаційним документом, на підставі якого ЕК визначає рівень теоретичної підготовки випускника, його готовність до самостійної роботи за фахом і приймає рішення щодо присвоєння відповідної кваліфікації та видачу диплома. Дипломна робота магістра є інструментом закріплення та демонстрації сформованих упродовж навчання загальних та спеціальних компетентностей відповідно профілю обраної освітньо-професійної програми. Для оприлюднення та публічного ознайомлення зі змістом кваліфікаційних робіт, запобігання академічного плагіату дипломні роботи мають бути розміщені на офіційному сайті НУ «Запорізька політехніка.
Вимоги до публічного захисту (демонстрації за наявності)	У процесі публічного захисту кандидат на присвоєння магістерського ступеня повинен показати уміння чітко і упевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь студента повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду. Ухвалення екзаменаційною комісією рішення про присудження ступеня магістра з кібербезпеки та видачу диплома магістра за результатами підсумкової атестації студентів оголошуються після оформлення в установленому порядку протоколів засідань екзаменаційної комісії. Після цього студенту видається документ встановленого зразку про присудження йому ступеня магістр з присвоєнням кваліфікації (за КВЕД ДК 003:2010): 2149.2 - Професіонал із організації інформаційної безпеки 2310 викладач університетів та вищих навчальних закладів
Вимоги до кваліфіка-ційного екзамену	Кваліфікаційний екзамен має передбачати оцінювання обов’язкових результатів навчання, визначених стандартами та освітньо-професійною програмою.

7 Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Вимоги визначаються відповідно до Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG), статті 16 Закону України "Про вищу освіту", наказу МОН України № 1254 від 01.10.2019 р. із змінами та доповненнями.

Принципи та процедури забезпечення якості освіти	**Принципи забезпечення якості освіти:** – відповідальність за якість вищої освіти, що надається; – забезпечення якості відповідає різноманітності систем вищої освіти, – закладів вищої освіти, програм і студентів; – забезпечення якості сприяє розвитку культури якості; – забезпечення якості враховує потреби та очікування стейкхолдерів та суспільства. **Процедурами забезпечення якості освіти є:** – розробка стратегії і політики в сфері якості вищої освіти; – розробка механізму формування, затвердження, моніторингу та періодичного перегляду освітньо-професійних програм; – розробка системи оцінювання знань здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярного оприлюднення результатів таких оцінювань на офіційному веб-сайті НУ «Запорізька політехніка», на інформаційних стендах та в будь-який інший спосіб, згідно з розробленими та затвердженими правилами; – організація підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; – формування необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів за освітньо-професійною програмою; – створення та функціонування інформаційних систем для ефективного управління освітнім процесом; – оприлюднення об'єктивної неупередженої інформації просвітньо-професійної програми, ступеня вищої освіти та кваліфікації; – розробка політики що до ефективної системи запобігання та виявлення академічного плагіату у наукових працях здобувачів вищої освіти; – інших процедур та заходів. http://www.zntu.edu.ua/uploads/dept_nm/Polozhennia_pro_za

	bezpechennia_yakosti.pdf http://zntu.edu.ua/uploads/dept_nm/Polozhennia_pro_organizatsiyu_osvitnoho_protsesu.pdf)
Моніторинг та періодичний перегляд освітніх програм	Здійснюються моніторинг і періодичний перегляд програм з метою забезпечення їх відповідності потребам студентів і суспільства. Моніторинг спрямований на безперервне вдосконалення програм. Про будь-які дії, заплановані або вжиті, як результат перегляду, слід інформувати всі зацікавлені сторони. Регулярний моніторинг, перегляд і оновлення освітніх програм мають на меті гарантувати відповідний рівень надання освітніх послуг, а також створює сприятливе й ефективне навчальне середовище для здобувачів вищої освіти. Це передбачає оцінювання: - змісту програми в контексті останніх досліджень у сфері кібербезпеки, гарантуючи відповідність програми сучасним вимогам; - потреб суспільства, що змінюються; - навчального навантаження здобувачів вищої освіти, їх досягнень і результатів завершення освітньо-професійної програми; - ефективності процедур оцінювання студентів; - очікувань, потреб і задоволеності здобувачів вищої освіти змістом та процесом навчання; - навчального середовища відповідності меті і змісту програми; - якості сервісних послуг для здобувачів вищої освіти. Програма переглядається через кожні 5 років, оновлюється у відповідності до змін нормативно-правових актів та наказів МОН України, Законів України з залученням до цього процесу здобувачів вищої освіти, роботодавців та інших стейкхолдерів.
Щорічне оцінювання здобувачів вищої освіти	Оцінювання здобувачів вищої освіти базується на принципах студентоцентрованого навчання та передбачає наступне: – оцінювачі (експерти) ознайомлені з існуючими методами проведення тестування та екзаменування і отримують підтримку для розвитку власних навичок у цій сфері; – критерії та методи оцінювання, а також критерії виставлення оцінок оприлюднюються заздалегідь; – оцінювання здобувачів вищої освіти дозволяє продемонструвати ступінь досягнення ними запланованих результатів навчання; – оцінювання проводиться предметною комісією у складі не менше чотирьох членів комісії; – процедури оцінювання здобувачів вищої освіти повинні враховувати пом’якшувальні обставини;

	– оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених процедур; – наявність офіційної процедури розгляду апеляцій здобувачів вищої освіти.http://www.zntu.edu.ua/uploads/dept_nm/Polozhennia_pro_reytynhovu_systemu.pdf
Підвищення кваліфікації наукових, педагогічних, науково-педагогічних працівників	Система підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників розробляється у відповідності до діючої нормативної бази та будується на наступних принципах: – обов'язковості та періодичності проходження стажування і підвищення кваліфікації; – прозорості процедур організації стажування та підвищення кваліфікації; – моніторингу відповідності змісту програм підвищення кваліфікації – задачам професійного діяльності; – обов'язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; – оприлюднення результатів стажування та підвищення кваліфікації. http://www.zntu.edu.ua/uploads/dept_nm/Polozhennia_pro_pidvyshchennia_kvalifikatsiyi.pdf http://www.zntu.edu.ua/uploads/academic_council/pol_pro_prov_konk_vidbir_vak_npp.pdf
Наявність необхідних ресурсів для організації освітнього процесу	Лекційні, аудиторні приміщення, спеціалізовані лабораторії, мультимедійне обладнання відповідно до вимог навчального процесу. Всі комп'ютери об'єднані у локальну мережу, в якій виділені домени (підмережі) для різних аудиторій і за призначенням: навчальний процес, наука, системно-технічні потреби. Університет має доступ до волоконно-оптичної мережі Уран. Для входу до локальної мережі та мережі Internet, крім того, встановлено Wi-Fi точки доступу. Для проведення інформаційного пошуку та обробка результатів є спеціалізовані комп'ютерні класи кафедри та університету, де є наявне спеціалізоване програмне забезпечення та необмежений відкритий доступ до мережі Інтернет.
Наявність інформаційних систем для ефективного управління освітнім	Навчально-методичні комплекси навчальних дисциплін, програми і бази для їх практичного засвоєння містять: підручники, словники, навчальні посібники, довідкову літературу, фахові періодичні видання тощо. Офіційний веб-сайт http://www.zntu.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти.

процесом	Всі зареєстровані в НУ «Запорізька політехніка» користувачі мають необмежений доступ до мережі Інтернет. Матеріали навчально-методичного забезпечення освітньо-професійної програми викладені на освітньому порталі http://www.zntu.edu.ua/kafedra- zahistu-informaciyi. Бібліотечний фонд наукової бібліотеки НУ «Запорізька політехніка» на 01.09.2019 р. складають паперові видання у обсязі 895285 примірників навчальної та наукової літератури та електронні видання у обсязі 55717 примірників. У НУ «Запорізька політехніка» 8 читальних залів площею 773 м^2 на 454 посадкових місця. Комп'ютерна мережа бібліотеки налічує 2 сервери, 7 сканерів, 7 принтерів, 2 копіювальні апарати, 1 багатофункціональний пристрій та 83 комп'ютера, які об'єднані в єдину інформаційну мережу. Всі ресурси бібліотеки доступні через сайт університету http://zntu.edu.ua/naukova-biblioteka.
Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація про діяльність за спеціальністю 125 "Кібербезпека" публікується на сайті НУ "Запорізька політехніка", включаючи програми для потенційних здобувачів вищої освіти, студентів, випускників, інших стейкхолдерів і громадськості. Надається інформація про освітню діяльність за спеціальністю 125"Кібербезпека", включаючи програми, критерії відбору на навчання; заплановані результати навчання за цими програмами; кваліфікації; процедури навчання, викладання та оцінювання, що використовуються; прохідні бали та навчальні можливості, доступні для студентів то що. http://www.zntu.edu.ua/kafedra- zahistu-informaciyi
Запобігання та виявлення академічного плагіату	Система забезпечення дотримання академічної доброчесності учасниками освітнього процесу, яка сформована в НУ «Запорізька політехніка", базується на таких принципах: – дотримання загально прийнятих принципів моралі; – демонстрація поваги до Конституції і законів України і дотримання їх норм; – повага до всіх учасників освітнього процесу незалежно від їхнього світогляду, соціального стану, релігійної та національної приналежності; – дотримання норм законодавства про авторське право; – посилання на джерела інформації у разі запозичень ідей, тверджень, відомостей; – самостійне виконання індивідуальних завдань. У випадку порушення принципів академічної доброчесності відповідні особи притягуються до відповідальності відповідно до законодавства та діючих у НУ «Запорізька політехніка» положень та норм.

	http://www.zntu.edu.ua/uploads/dept_nm/Polozhennia_pro_perevirku_na_plahiat.pdf»
Національна кредитна мобільність	На підставі договорів про співробітництво між НУ «Запорізька політехніка" та вітчизняними вищими навчальними закладами (науковими установами) України.
Міжнародна кредитна мобільність	На підставі міжнародних договорів про співробітництво в галузі освіти та науки, міжнародних програм та проектів, договорів про співробітництво між НУ «Запорізька політехніка" та іноземними вищими навчальними закладами (науковими установами) на основі індивідуальних запрошень та інших механізмів. http://zntu.edu.ua/akademichna-mobilnist

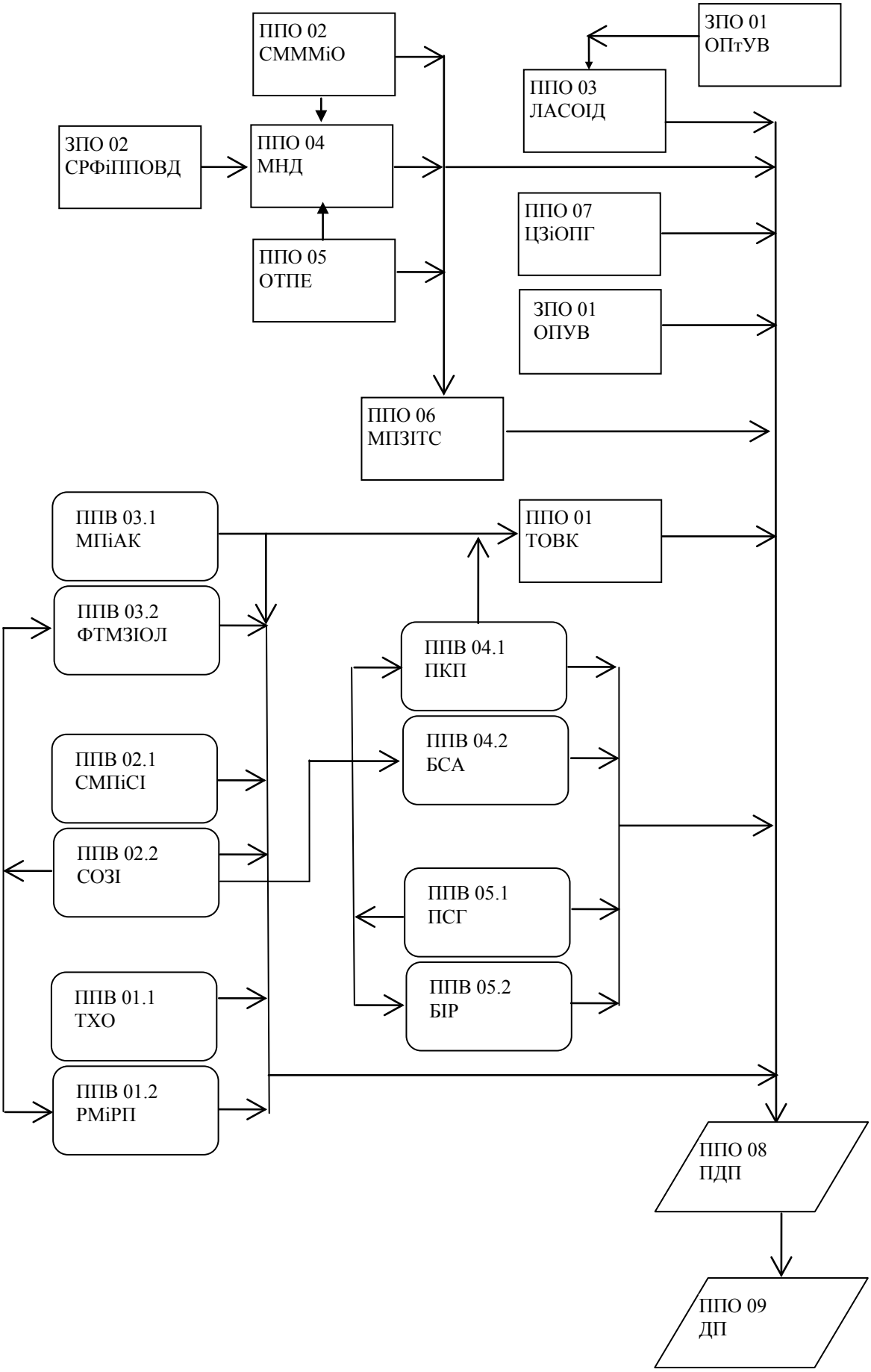
8 Перелік компонент ОПП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
Загальна підготовка			
ЗПО 01	*Організація, планування та управління виробництвом*	3	залік
ЗПО 02	*Спеціальні розділи філософії та психолого-педагогічні основи викладацької діяльності.*	3	залік
	Всього	**6**	
Професійна підготовка			
ППО 01	*Технологія організації відкритих ключів*	6	екзамен, курсовий проект
ППО 02	*Сучасні методи математичного моделювання та оптимізації*	4,5	залік
ППО 03	*Ліцензування, атестація, сертифікація у сфері безпеки об'єктів інформаційної діяльності*	4	залік
ППО 04	*Методологія наукових досліджень*	4	залік
ППО 05	*Основи теорії планування експерименту*	4	залік
ППО 06	*Моделювання процесів захисту інформації в технічних системах*	6	екзамен, курсовий проект

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ППО 07	*Цивільний захист і охорона праці в галузі*	3	залік
ППО 08	*Переддипломна практика*	6	залік
ППО 09	*Дипломування*	21,5	
ППО 09	*Дипломування*	1	
ППО 09	*Дипломування*	1,5	
	Всього	**61**	
	Загальний обсяг нормативних компонент	**67**	
	ВИБІРКОВІ КОМПОНЕНТИ		
ППВ 01.1	*Технології хмарних обчислень в задачах захисту інформації*	5	екзамен
ППВ 01.2	*Радіомоніторинг і радіопротидія на об'єктах інформаційної діяльності*		
ППВ 02.1	*Сучасні методи перетворення та стиснення інформації*	4	залік
ППВ 02.2	*Сучасне обладнання захисту інформації*		
ППВ 03.1	*Методи побудови і аналізу криптосистем*	4,5	залік
ППВ 03.2	*Фізико-технічні методи захисту інформації в волоконно-оптичних лініях передачі*		
ППВ 04.1	*Програмування криптоперетворень*	4,5	екзамен
ППВ 04.2	*Біометричні системи аутентифікації*		
ППВ 05.1	*Прикладна стеганографія*	5	екзамен
ППВ 05.2	*Безпека інтернет-ресурсів*		
	Загальний обсяг вибіркових компонент	**23**	
	Загальний обсяг освітньої програми	**90**	

Позначення та скорочення, які наведені в таблиці:
ЗПО дисципліна циклу загальної підготовки обов'язкова;
ППО дисципліна циклу професійної підготовки обов'язкова;
ППВ - дисципліна циклу професійної підготовки вибіркова.

9 Структурно-логічна схема ОПП



10 Перелік нормативних документів, на яких базується освітньо-професійна програма

Освітньо-професійна програма розроблена як тимчасовий документ до затвердження відповідного стандарту вищої освіти України за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти.

Освітня діяльність НУ «Запорізька політехніка» ґрунтується на концептуальних засадах Національної Доктрини розвитку освіти, Державній Національній програмі «Освіта» («Україна XXI століття»), Законі України «Про освіту», Законі України «Про вищу освіту», наказах Міністерства освіти і науки, листа Міністерства освіти і науки України №1/9-239 від 28.04.2017 р., наказу МОН України № 1254 від 01.10.2019 р. із змінами та доповненнями, Статуті НУ «Запорізька політехніка», Правилах розпорядку університету та інших нормативно-правових актах.

Бібліографічний список

1. Закон України № 1556-18 «Про вищу освіту» №2145-VIII від 05.09.2017 р.
2. НаціональнийкласифікаторУкраїни: «Класифікатор професій «ДК 003:2010 – К. : Видавництво «Соцінформ», 2010. – 746с.
3. Національний класифікатор України: «Класифікація видів економічної діяльності» ДК 009:2010 - К. : Видавництво «Соцінформ», 2010.
4. Міжнародна стандартна класифікація освіти (ISCED – 97: International Standard ClassificationofEducation/UNESCO, Paris).
5. Структури кваліфікацій для Європейського простору вищої освіти (TheframeworkofqualificationsfortheEuropeanHigherEducationArea).
6. Структури ключових компетенцій, які розглядаються як необхідні для всіх у суспільстві, заснованому на знаннях (KeyCompetencesforLifelonglearning: A EuropeanReference Framework – IMPLEMENTATION OF «EDUCATION AND TRAINING 2010», Workprogramme, WorkingGroupB «KeyCompetences», 2004.
7. Наказу МОН України № 1254 від 01.10.2019 р. із змінами та доповненнями
8. Національна рамка кваліфікацій –http://zakon4.rada.gov.ua/laws/show/1341-2011-п.

10 Пояснювальна записка

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК та матриця відповідності визначених Стандартом результатів навчання та компетентностей представлені в Таблиці 1 та Таблиці 2.

Таблиця 1 -Матриця відповідності визначених компетентностей дескрипторам НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
ЗК 1. Здатність застосовувати знання у практичних ситуаціях.	+	+	+	+
ЗК 2. Знання та розуміння предметної області та розуміння професії.	+	+	+	+
ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово	+	+	+	+
ЗК 4. Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях	+	+	+	+
ЗК 5.Здатність до виявлення, розуміння та аналітичного дослідження проблем за професійним спрямуванням	+	+		+
ЗК 6. Здатність до сприйняття й спроможність розв'язувати комплексні задачі та практичні проблеми технологій обробки, аналізу, перетворювання й передавання інформації	+	+	+	+
ЗК. 7. Здатність використовувати методи фундаментальних та загально-професійних наук для розв'язання задач кібербезпеки	+	+	+	+
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
СК 1. Здатність до застосування сучасних інформаційних і технологічних технологій у сфері захисту інформації	+	+		
СК 2. Здатність до виявлення	+	+		+

вразливостей та забезпечення безпеки дротових і бездротових мереж, розслідування інцидентів інформаційної та/або кібербезпеки та протидії злоякісному програмному забезпеченню				
СК 3. Здатність до забезпечення безпеки Web- ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження	+	+	+	+
СК 4. Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки	+	+		+
СК 5. Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та їх супроводження	+	+	+	+
СК 6. Здатність використовувати нормативно-правові, управлінсько-організаційні, математичні, технічні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки	+	+	+	+
СК 7. Здатність організовувати та проводити наукові дослідження, пов’язані із застосуванням математичних та технічних методів для аналізу та дослідження процесів та систем забезпечення інформаційної та кібернетичної безпеки.	+	+	+	+

Таблиця 2-Матриця відповідності визначених ОПП результатів навчання та компетентностей

Програмні результати навчання	**Компетенції**														
	Інтегральна	**Загальні**							**Спеціальні (фахові)**						
		ЗК 1	**ЗК 2**	**ЗК 3**	**ЗК 4**	**ЗК 5**	**ЗК 6**	**ЗК 7**	**СК 1**	**СК 2**	**СК 3**	**СК 4**	**СК 5**	**СК 6**	**СК 7**
РН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.	+	+	+	+					+						
РН 2. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності	+				+	+	+			+		+			+
РН 3. Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки	+			+	+	+		+					+		+
РН 4. Вміти застосовувати спеціалізоване	+					+	+	+	+		+	+	+		

програмне забезпечення, сучасні інформаційні технології у сфері захисту інформації.															
РН 5. Знати методи організації захищеної передачі даних у незахищеному середовищі	+							+	+	+				+	
РН 6. Вміти виявляти загрози проникнення або доступу зловмисників до мереж обробки інформації	+	+					+		+	+	+	+	+		
РН 7. Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів)	+	+						+	+	+	+	+	+		
РН 8. Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки	+		+				+	+		+	+		+		

РН 9. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки	+						+	+				+	+		+
РН 10. Вміти використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності	+		+	+					+					+	
РН 11. Вміти застосовувати сучасні методики планування експерименту при побудові математично-статистичних моделей процесів та об’єктів в галузі захисту інформації	+				+							+			+

РН 12. Знати особливості побудови математичних моделей при вирішенні задач захисту інформації, вміти їх розробляти та володіти науковими підходами до застосування цих моделей у задачах оптимізації захисту інформації	+	+	+		+			+	+			+			+

Керівник проектної групи,
завідувач кафедри ЗІ
д.т.н., проф. Л.М. Карпуков

Члени проектної групи:
к.т.н., доц., проф. кафедри ЗІ В.О. Воскобойник

канд. фіз-мат. наук, доцент кафедри ЗІ Г.Л. Козіна

бакалавр, ст. магістерської групи РТ-819м О.В. Матвейчук