МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ЗАТВЕРДЖУЮ
В.о. ректора НТУ «ХПІ»
_____ Андрій МАРЧЕНКО
«09» липня 2020 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Кібербезпека»

першого (бакалаврського) рівня вищої освіти
за спеціальністю: **125 Кібербезпека**
галузі знань: **12 Інформаційні технології**
кваліфікація: **Бакалавр з кібербезпеки**

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ НТУ «ХПІ»
Голова Вченої ради
_____ Леонід Товажнянський
Протокол № 11
«03» липня 2020 р.

Харків 2020 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Кібербезпека
Кваліфікація	Бакалавр з кібербезпеки

СХВАЛЕНО
Робоча група
зі спеціальності «Кібербезпека»
Гарант ОП
_____ Олександр РИСОВАНИЙ
«23» червня 2020 р.

РЕКОМЕНДОВАНО
Методичною радою НТУ «ХПІ»
Заступник голови методичної ради
_____ Руслан МИГУЩЕНКО
«23» червня 2020 р.

ПОГОДЖЕНО
Завідувач кафедри обчислювальної
техніки та програмування
_____ Сергій СЕМЕНОВ
«23» червня 2020 р.

ПОГОДЖЕНО
Декан факультету комп'ютерних
та інформаційних технологій
_____ Максим ГЛАВЧЕВ
«23» червня 2020 р.

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ
Наказом в.о. ректора Національного технічного університету «Харківський політехнічний інститут» від «14» липня 2020 р. № 301 ОД

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти (Наказ Міністерства освіти і науки України № 1074 від 04.10.2018).

Розроблено робочою групою зі спеціальності 125 «Кібербезпека» факультету комп'ютерних та інформаційних технологій Національного технічного університету «Харківський політехнічний інститут» у складі:

1. Кандидат технічних наук, професор О.М. Рисований – професор кафедри обчислювальної техніки та програмування (гарант освітньо-професійної програми).

2. Доктор технічних наук, старший науковий співробітник О.В. Коломійцев – професор кафедри обчислювальної техніки та програмування.

3. Кандидат технічних наук Д.О. Лисиця – старший викладач кафедри комп'ютерних і радіоелектронних систем контролю та діагностики.

Рецензії-відгуки на проект освітньо-професійної програми одержано від:

1. Тарас Русланович Кібіткін, директор «Lineup».

2. Михайло Олександрович Можаєв, завідувач сектору комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного інституту судових експертиз ім. Засл. проф. М.С. Бокаріуса.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ
ЗА СПЕЦІАЛЬНІСТЮ 125 «КІБЕРБЕЗПЕКА»

1 – ЗАГАЛЬНА ІНФОРМАЦІЯ	
ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД ТА СТРУКТУРНИЙ ПІДРОЗДІЛ	Національний технічний університет «Харківський політехнічний інститут», факультет «Комп'ютерні та інформаційні технології», кафедра «Обчислювальна техніка та програмування»
СТУПІНЬ ВИЩОЇ ОСВІТИ ТА НАЗВА КВАЛІФІКАЦІЇ МОВОЮ ОРИГІНАЛУ	бакалавр, бакалавр з кібербезпеки
ОФІЦІЙНА НАЗВА ОСВІТНЬОЇ ПРОГРАМИ	освітньо-професійна програма «Кібербезпека»
ТИП ДИПЛОМУ ТА ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
НАЯВНІСТЬ АКРЕДИТАЦІЇ	сертифікат не отриманий
ЦИКЛ/РІВЕНЬ	НРК України - 6 рівень, FQ-EHEA - перший цикл, EQF-LLL - 6 рівень
ПЕРЕДУМОВИ	Наявність документа про повну загальну середню освіту, диплома молодшого спеціаліста (молодшого бакалавра)
МОВИ ВИКЛАДАННЯ	українська, англійська
ТЕРМІН ДІЇ ОСВІТНЬОЇ ПРОГРАМИ	відповідно до терміну дії сертифікату про акредитацію
ПОСИЛАННЯ НА ПОСТІЙНЕ РОЗМІЩЕННЯ ОПИСУ ОСВІТНЬОЇ ПРОГРАМИ	https://www.kpi.kharkov.ua

2 – МЕТА ОСВІТНЬОЇ ПРОГРАМИ
Підготовка бакалаврів, що передбачає здобуття теоретичних знань, умінь, навичок та інших компетентностей, необхідних для виконання професійних обов'язків у складі колективу і можливих первинних посад бакалавра з кібербезпеки в рамках об'єктів професійної діяльності за обраною спеціалізацією, розв'язання технічних та наукових проблем у галузі інформаційних технологій та проведення власного наукового дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

3 – ХАРАКТЕРИСТИКА ОСВІТНЬОЇ ПРОГРАМИ	
ПРЕДМЕТНА ОБЛАСТЬ (ГАЛУЗЬ ЗНАНЬ, СПЕЦІАЛЬНІСТЬ, СПЕЦІАЛІЗАЦІЯ)	**Галузь знань** – 12 «Інформаційні технології» **Спеціальність** – 125 «Кібербезпека» **Об'єкти вивчення:** об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології; технології забезпечення безпеки інформації об'єктів різного рівня (система, об'єкт системи, компонент об'єкта), що пов'язані з

інформаційними, інформаційно-комунікаційними технологіями, що використовуються для забезпечення функціонування цих об'єктів.

Цілі навчання: підготовка фахівців, здатних розробляти і використовувати технології інформаційної безпеки, формування компетенцій, знань та умінь, необхідних для виконання професійних обов'язків у складі колективу і можливих первинних посад фахівця із організації інформаційної безпеки в рамках об'єктів професійної діяльності за обраною спеціалізацією. Проектувати та використовувати цифрові інновації для безпечного програмування з метою нейтралізації негативних і деструктивних тенденцій злому програмного коду; забезпечення теоретичної підготовки для дослідження і виправлення програмного забезпечення, яке знаходиться в експлуатації; створення нової функціональності, використовуючи неявне в експлуатації програмне забезпечення для професійного і системного програмного використання.

Теоретичний зміст предметної області полягає в знанні:

– законодавчої, нормативно-правової бази України та вимог відповідних, в тому числі міжнародних стандартів і практик щодо здійснення професійної діяльності;

– вимог санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки;

– принципів проектування (розробки) систем інформаційної безпеки;

– прав, обов'язків та відповідальності фахівця з інформаційної безпеки;

– щодо функціонування системи управління інформаційною безпекою;

– методів та засобів ідентифікації вразливостей та загроз інформаційній безпеці на об'єктах інформаційної діяльності;

– методів та засобів забезпечення відповідного рівня захищеності інформації;

– методів та засобів оцінки відповідного рівня захищеності інформації;

– аналізу та планування основних економічних показників проектних рішень із забезпечення кібербезпеки.

Теоретичний зміст предметної області пов'язаний з поняттями, концепціями, принципами, методами, програмно-технічними засобами та технологіями дослідження, проектування, виробництва, обслуговування та використання засобів в рамках об'єктів професійної діяльності, що забезпечують набуття відповідних компетенцій.

Методи, методики та технології: загальнонаукові та спеціальні методи і процедури аналізу і прогнозування процесів, які здійснюються в комп'ютерних та інформаційних системах, з метою виявлення різного роду загроз і вразливостей, що можуть привести до втрати або спотворення даних в цих системах, розробка і дослідження апаратних та програмних технологій захисту інформації.

Здобувач вищої освіти має володіти методами фундаментальних та прикладних наук, технологіями виконання

	обчислень, методами автоматизованого проектування програмно-технічних засобів комп'ютерних систем та мереж і їх компонентів, математичного та комп'ютерного моделювання, інформаційними технологіями, професійними прикладними програмами, сучасними мовами програмування. **Інструменти та обладнання:** сучасні комп'ютерні і інформаційні системи та мережі, контрольно-вимірювальні прилади, програмно-технічні засоби захисту даних та системи автоматизації проектування, обладнання, необхідне для моніторингу функціонування і підтримки інформаційних та телекомунікаційних систем і мереж, системи, прилади, апаратура для забезпечення безпеки інформації. Операційні системи, системне та прикладне програмне забезпечення, застосування хмарних обчислень та інтернет речей.
ОРІЄНТАЦІЯ ОСВІТНЬОЇ ПРОГРАМИ	Освітньо-професійна.
ОСНОВНИЙ ФОКУС ОСВІТНЬОЇ ПРОГРАМИ	Загальна освіта професійної діяльності бакалаврів направлена на**:** – програмно-технічні засоби (апаратні, програмовані), системне та прикладне програмне забезпечення комп'ютерів та комп'ютерних систем універсального та спеціального призначення, в тому числі стаціонарних, мобільних, вбудованих, розподілених тощо, локальні, глобальні комп'ютерні мережі інтерфейси та протоколи взаємодії їх компонентів, що направлені на виявлення їх вразливостей і підвищення інформаційної безпеки; – інформаційні процеси, технології, методи, способи та системи автоматизованого та автоматичного проектування; налагодження, виробництва й експлуатації, проектна документація, стандарти, процедури та засоби підтримки керування життєвим циклом вказаних програмно-технічних засобів; – методи та способи опрацювання інформації, математичні моделі обчислювальних процесів, технології виконання обчислень, в тому числі високопродуктивних, паралельних, розподілених, мобільних, веб-базованих та хмарних, енергоефективних, безпечних, автономних, адаптивних, інтелектуальних, розумних тощо, архітектура та організація функціонування відповідних програмно-технічних засобів. **Ключові слова:** інформаційні технології, програмно-технічні засоби, апаратно-програмно-технічні засоби, інформаційна безпека.
ОСОБЛИВОСТІ ОСВІТНЬОЇ ПРОГРАМИ	Здобувач вищої освіти має володіти методами фундаментальних та прикладних наук, технологіями виконання обчислень, методами автоматизованого проектування програмно-технічних засобів захисту даних в комп'ютерних системах та мережах і їх компонентах, математичного та комп'ютерного моделювання, інформаційними технологіями, професійними прикладними програмами, сучасними мовами програмування, методами та технологіями боротьби з небажаною та шкідливою інформацією, методами проектної, організаційної та управлінської діяльності.

4 – ПРИДАТНІСТЬ ВИПУСКНИКІВ ДО ПРАЦЕВЛАШТУВАННЯ ТА ПОДАЛЬШОГО НАВЧАННЯ	
ПРИДАТНІСТЬ ДО ПРАЦЕВЛАШТУВАННЯ	Випускники можуть працювати за такими професіями (згідно з Національним класифікатором професій ДК 003:2010): 3439 Фахівець із організації інформаційної безпеки. Назви професій згідно International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
ПОДАЛЬШЕ НАВЧАННЯ	Можливе подальше продовження освіти за другим (магістерським) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – ВИКЛАДАННЯ ТА ОЦІНЮВАННЯ	
ВИКЛАДАННЯ ТА НАВЧАННЯ	Студентоцентроване навчання, що проводиться у формі лекцій, практичних та лабораторних занять, семінарів, консультацій з викладачами, самостійного навчання за індивідуальними завданнями, виконання курсових проектів та робіт, переддипломна практика, підготовка кваліфікаційної роботи з використанням розроблених підручників, посібників, конспектів лекцій, методичних рекомендацій, періодичних наукових видань та мережі Internet.
ОЦІНЮВАННЯ	Поточний та підсумковий контроль знань (опитування, контрольні та індивідуальні завдання, тестування тощо), заліки та екзамени (усні та письмові), захист навчальних та реальних проектів з презентацією, публічний захист кваліфікаційної роботи.
6 – ПРОГРАМНІ КОМПЕТЕНТНОСТІ	
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.
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. 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. КЗ 7. 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) КОМПЕТЕНТНОСТІ	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 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. КФ 13. Здатність проводити обробку сигналів, зображень та даних. КФ 14. Здатність проектувати, обробляти і застосовувати бази даних. КФ 15. Прагнення до збереження навколишнього середовища.
7 – ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ	
ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ ЗА СПЕЦІАЛЬНІСТЮ	РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній

діяльності, оцінювати їхню ефективність;
РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
РН 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;
РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки;
РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки;
РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
РН 12 – розробляти моделі загроз та порушника;
РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
РН 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;
РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
РН 20 – забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-

телекомунікаційних системах;
РН 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;
РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки;
РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
РН 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);
РН 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;
РН 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;
РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
РН 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;
РН 29 – 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;
РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
РН 33 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків;
РН 34 – приймати участь у розробці та впровадженні стратегії

інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
РН 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;
РН 36 – виявляти небезпечні сигнали технічних засобів;
РН 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;
РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;
РН 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;
РН 45 – застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
РН 49 – забезпечувати належне функціонування системи

	моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні; РН 55 – знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж; РН 56 – вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності; РН 57 – вміти розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем, розраховувати, експлуатувати типове для спеціальності обладнання; РН 58 – мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах; РН 59 – знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті; РН 60 – знати основи проектування клієнт-серверних застосунків; РН 61 – знати критерії, методи та алгоритми прийняття рішень, основні концепції і методи штучного інтелекту; базові знання принципів та методів захисту інформації, знання способів забезпечення безпеки інформаційних систем; РН 62 – вміти будувати та використовувати математичні та комп'ютерні моделі в галузі інформаційних технологій; РН 63 – вміти проводити обробку сигналів, зображень та даних; РН 64 – вміти забезпечувати захист сигналів, зображень та даних; РН 65 – демонструвати та пропагувати здоровий спосіб життя.
8 – РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПРОГРАМИ	
КАДРОВЕ ЗАБЕЗПЕЧЕННЯ	Відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187 (зі змінами, внесеними згідно з Постановою КМ № 347 від 10.05.2018).
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ	Відповідає технологічним вимогам щодо матеріально-технічного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету

	міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187 (зі змінами, внесеними згідно з Постановою КМ № 347 від 10.05.2018). Проведення лабораторних занять, виконання курсових та дипломних проєктів здійснюється у комп'ютерних лабораторіях відомих IT-компаній – NIX Solution, EPAM, GlobalLogic, які оснащені сучасним технічним і програмним забезпеченням.
ІНФОРМАЦІЙНЕ ТА НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ	Відповідає технологічним вимогам щодо навчально-методичного та інформаційного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187 (зі змінами, внесеними згідно з Постановою КМ № 347 від 10.05.2018).
9 – АКАДЕМІЧНА МОБІЛЬНІСТЬ	
НАЦІОНАЛЬНА КРЕДИТНА МОБІЛЬНІСТЬ	На основі двосторонніх договорів між Національним технічним університетом «Харківський політехнічний інститут» та вищими навчальними закладами України.
МІЖНАРОДНА КРЕДИТНА МОБІЛЬНІСТЬ	На основі двосторонніх договорів між Національним технічним університетом «Харківський політехнічний інститут» та навчальними закладами вищої освіти зарубіжних країн-партнерів.
НАВЧАННЯ ІНОЗЕМНИХ ЗДОБУВАЧІВ ОСВІТИ	На основі договорів між Національним технічним університетом «Харківський політехнічний інститут» та закладами вищої освіти іноземних країн.

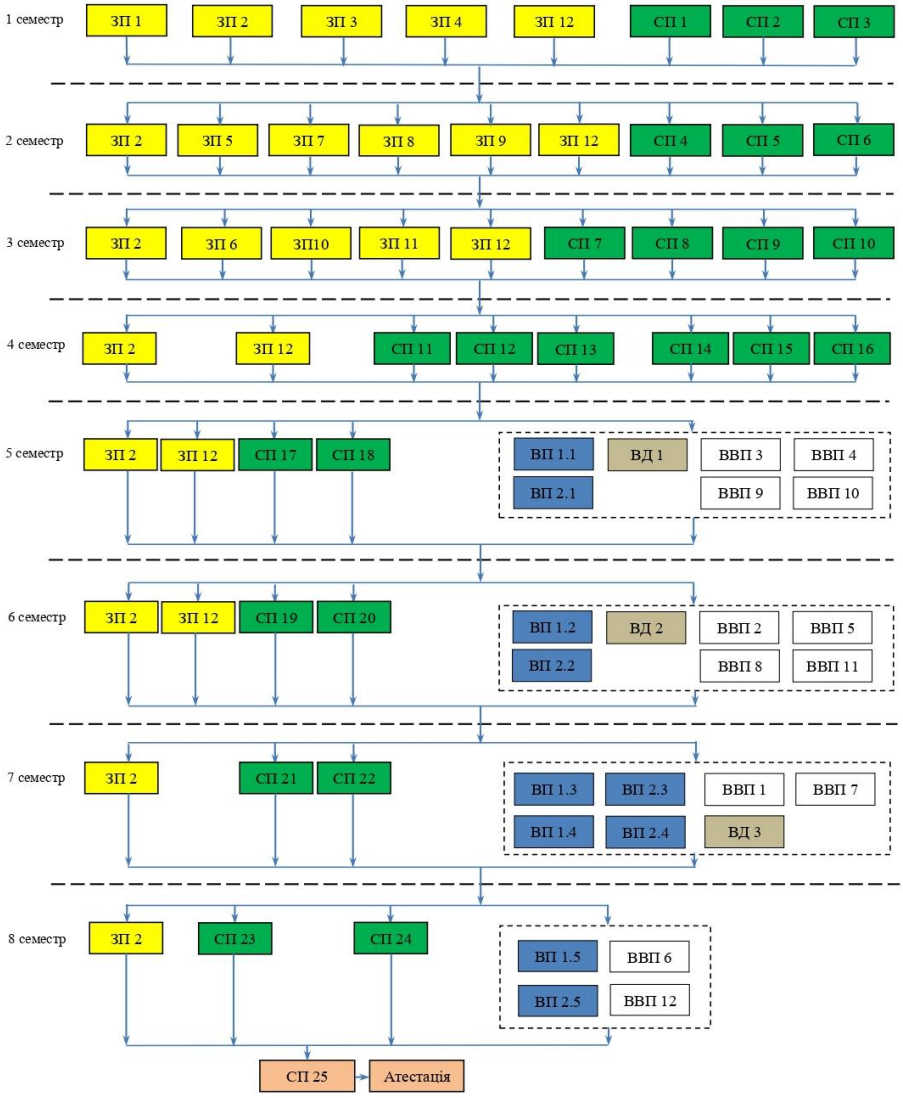
2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

Код н/д	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1	**Обов'язкові освітні компоненти**		
1.1	**Загальна підготовка**		
ЗП 1	Історія та культура України	2	екзамен
ЗП 2	Іноземна мова	16	залік, екзамен
ЗП 3	Фізика	6	екзамен
ЗП 4-6	Вища математика	12	залік, екзамен
ЗП 7	Українська мова	2	екзамен
ЗП 8	Філософія	3	екзамен
ЗП 9-10	Дискретна математика	7	залік, екзамен
ЗП 11	Теорія ймовірності	4	екзамен
ЗП 12	Фізичне виховання	12	залік
1.2	**Спеціальна (фахова) підготовка**		
СП 1	Алгебра програмування	3	екзамен
СП 2	Основи кібербезпеки	4	екзамен
СП 3	Програмування	6	екзамен
СП 4	Основи безпечного програмування	5	екзамен

1	2	3	4
СП 5	Архітектура операційних систем	3	залік
СП 6	Алгоритми захисту даних	5	екзамен
СП 7	Основи електротехніки та електроніки	3	екзамен
СП 8	Організація та проектування баз даних	4	залік
СП 9	Теорія інформації та кодування	5	екзамен
СП 10-11	Об’єктно-орієнтоване програмування	8	залік, екзамен
СП 12	Схемотехнічні пристрої захисту інформації	5	екзамен
СП 13	Обробка сигналів та даних	5	екзамен
СП 14	Розробка та застосування баз даних	3	екзамен
СП 15	Управління інформаційною безпекою	4	екзамен
СП 16	Безпека інформації в інформаційних та комп'ютерних мережах	5	екзамен
СП 17	Веб-програмування	5	екзамен
СП 18	Архітектура обчислювальних систем	4	екзамен
СП 19	Захист інформації в комп'ютерних мережах	5	екзамен
СП 20	Тестування безпеки комп’ютерних систем	5	екзамен
СП 21	Комплексні системи захисту	5	екзамен
СП 22	Ризик-орієнтований аналіз в IT-технології	4	екзамен
СП 23	Аналіз та синтез захищених комп'ютерних систем	4	екзамен
СП 24	Комп'ютерна стеганографія	4	екзамен
СП 25	**Практика**	6	залік
	Атестація	6	
	Загальний обсяг обов’язкових освітніх компонент	**180**	
2	**Вибіркові освітні компоненти**		
2.1	**Профільна підготовка**		
2.1.1	**Профільований пакет дисциплін 01 «Безпека мережевих ресурсів та систем»**		
ВП 1.1	Антивірусний захист	5	екзамен
ВП 1.2	Безпека веб-ресурсів	5	екзамен
ВП 1.3	Системи та засоби криптоаналізу	5	екзамен
ВП 1.4	Інтелектуальні системи інформаційної безпеки	5	екзамен
ВП 1.5	Інтелектуальний аналіз даних	4	екзамен
2.1.2	**Профільований пакет дисциплін 02 «Інженерія захищених систем та даних»**		
ВП 2.1	Основи безпеки програм та даних	5	екзамен
ВП 2.2	Моделювання стеганографічних даних	5	екзамен
ВП 2.3	Паралельні та хмарні обчислювальні системи	5	екзамен
ВП 2.4	Системи штучного інтелекту	5	екзамен
ВП 2.5	Machine learning	4	екзамен
2.2	**Дисципліни вільного вибору студента профільної підготовки згідно переліку**		
ВВП1	Захищені вбудовані системи	5	екзамен
ВВП2	Green computing	3	екзамен
ВВП3	Прикладна криптологія	5	екзамен
ВВП4-5	Блокчейн і децентралізовані системи	7	екзамен
ВВП6	Проектування мобільних застосунків	4	екзамен

1	2	3	4
ВВП7	Формальні мови, граматики і автомати	5	екзамен
ВВП8	Реверсне програмування	3	екзамен
ВВП9	Програмні засоби захисту інформації	5	екзамен
ВВП10	Проектування серверних застосунків	3	екзамен
ВВП11	Управління IT-проектами	4	екзамен
ВВП12	Основи обчислювального інтелекту	4	екзамен
2.3	**Дисципліни вільного вибору студента із загальноуніверситетського каталогу дисциплін**		
ВД 1	Дисципліна 1	4	залік
ВД 2	Дисципліна 2	4	залік
ВД 3	Дисципліна 3	4	залік
	Загальний обсяг вибіркових освітніх компонент	**60**	
Загальний обсяг		**240**	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ



4. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Цикл загальної підготовки	64 / 26,7	- / -	64 / 26,7
2	Цикл спеціальної (фахової) підготовки	116 / 48,3	- / -	116 / 48,3
3	Вибіркові освітні компоненти	- / -	60 / 25	60 / 25
Всього за весь термін навчання		180 / 75	60 / 25	240 / 100

5. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ	Публічний захист (демонстрація) кваліфікаційної роботи.
ВИМОГИ ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ (ЗА НАЯВНОСТІ)	Кваліфікаційна робота – це самостійно виконана проектно-дослідна робота студента, яка передбачає авторське бачення проблеми, можливості її дослідження та розв'язання. Робота свідчить про вміння автора проводити емпіричне дослідження, розробляти відповідні системи (засоби), обґрунтовувати проектні рішення, опрацьовувати та аналізувати отримані результати, формулювати аргументовані висновки. Виконання випускних кваліфікаційних робіт має сприяти: – систематизації, закріпленню й розширенню теоретичних і практичних знань зі спеціальності та застосуванню цих знань для вирішення конкретних завдань; – розвитку навичок здійснення самостійної роботи й оволодіння методикою вирішення питань і проблем, поставлених у випускній роботі; – оцінюванню рівня володіння певною сукупністю професійних компетентностей, необхідних для майбутньої професійної діяльності.
ВИМОГИ ДО ПУБЛІЧНОГО ЗАХИСТУ (ДЕМОНСТРАЦІЇ) (ЗА НАЯВНОСТІ)	Виступ складається із трьох смислових частин: вступу, основної частини та висновків кваліфікаційної роботи. У вступі висвітлюється актуальність досліджуваної проблеми, об'єкт, предмет, гіпотези та завдання дослідження і розроблення. Основна частина розкриває суть, методологію і особливості організації та проведення дослідження та розроблення проекту. У висновках наводяться головні результати дослідження та розроблення, визначається теоретичне і практичне значення отриманих результатів та можливі перспективи подальших досліджень і розробок. Оцінки кваліфікаційної роботи виносяться членами екзаменаційної

	комісії на її закритому засіданні. Комісія бере до уваги зміст роботи, обґрунтованість висновків, зміст доповіді, рівень презентації проекту і відповідей на запитання, відгуки на роботу, рівень теоретичної та практичної підготовки студента. Оцінки кваліфікаційної роботи оголошуються в той же день після закінчення захисту всієї групи та оформлення протоколу засідання комісії. За результатами підсумкової атестації студентів екзаменаційна комісія ухвалює рішення про присвоєння кваліфікації зі спеціальності та видачі диплома бакалавра.

6. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ПРИНЦИПИ ТА ПРОЦЕДУРИ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ	Принципи: – відповідність європейським і національним стандартам якості вищої освіти; – автономія закладу вищої освіти, який відповідає за забезпечення якості освітньої діяльності та якості вищої освіти; – системний підхід, який передбачає управління якістю на всіх рівнях освітнього процесу; – здійснення моніторингу якості освіти; – залучення студентів, роботодавців та інших зацікавлених сторін до процесу забезпечення якості; – відкритість інформації на всіх етапах забезпечення якості. Процедури: – удосконалення планування освітньої діяльності; – затвердження, моніторинг і періодичний перегляд освітніх програм; – підвищення якості підготовки контингенту здобувачів вищої освіти; – посилення кадрового потенціалу університету; – забезпечення наявності необхідних ресурсів для організації освітнього процесу та підтримки здобувачів вищої освіти; – розвиток інформаційних систем з метою підвищення ефективності управління освітнім процесом; – забезпечення публічності інформації про діяльність університету; – створення ефективної системи запобігання та виявлення академічного плагіату в наукових працях викладачів та здобувачів вищої освіти.
МОНІТОРИНГ ТА ПЕРІОДИЧНИЙ ПЕРЕГЛЯД ПРОГРАМ	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, гарантуючи відповідність програми сучасним вимогам; потреб суспільства, що змінюються; навчального навантаження здобувачів вищої освіти, їх досягнень і результатів завершення освітньої 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. Програми регулярно переглядають і оновлюють після завершення повного циклу підготовки до початку нового навчального року.
ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ	Оцінювання результатів навчання студентів здійснюється під час проведення контрольних заходів. Контрольні заходи передбачають поточний і семестровий контроль. Завданням поточного контролю є перевірка розуміння і засвоєння певного матеріалу, вироблених навичок проведення розрахункових робіт, умінь самостійно опрацьовувати тексти, публічно чи письмово представляти певний матеріал тощо. Формами поточного контролю є: виконання індивідуальних завдань; виконання тестових завдань; виконання контрольних робіт, які виконуються в аудиторії або під час самостійної роботи; написання і захист рефератів; захист лабораторних робіт. Підсумковий контроль проводиться з метою оцінки результатів навчання на відповідному освітньому рівні або на окремих його завершальних етапах. Підсумковий контроль включає семестровий контроль (екзамен, диференційований залік) та атестацію студента. Семестровий контроль проводиться у формі семестрового екзамену або заліку з конкретної навчальної дисципліни в обсязі навчального матеріалу, визначеного навчальною програмою, і в терміни, встановлені навчальним планом. Для здійснення контролю успішності студентів на рівні ректорату проводяться моніторингові контрольні роботи. Навчальні дисципліни, з яких заплановано проведення моніторингових контрольних робіт, терміни проведення контрольних заходів визначаються графіком навчального процесу. Оцінювання результатів навчання студентів університету проводиться методами, що відповідають специфіці конкретної навчальної дисципліни. Моніторинг успішності студента здійснюється за допомогою 100-бальної системи оцінювання з обов’язковим переведенням оцінок до національної шкали та шкали ECTS.
ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ НАУКОВО-ПЕДАГОГІЧНИХ, ПЕДАГОГІЧНИХ ТА НАУКОВИХ 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 професійної діяльності; обов’язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; оприлюднення результатів стажування та підвищення кваліфікації.

НАЯВНІСТЬ НЕОБХІДНИХ РЕСУРСІВ ДЛЯ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ	Наявне кадрове, матеріально-технічне, навчально-методичне та інформаційне забезпечення зі спеціальності відповідає вимогам діючих Ліцензійних умов провадження освітньої діяльності закладів освіти та забезпечує реалізацію державних вимог до фахівця з вищою освітою.
НАЯВНІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ЕФЕКТИВНОГО УПРАВЛІННЯ ОСВІТНІМ ПРОЦЕСОМ	З метою управління освітніми процесами розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну систему управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної компанії, планування та організацію навчального процесу; доступ до навчальних ресурсів; облік та аналіз успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; моніторинг дотримання стандартів якості. Для управління якістю освітньої діяльності в Університеті створена інформаційна система АСУ НП.
ПУБЛІЧНІСТЬ ІНФОРМАЦІЇ ПРО ОСВІТНІ ПРОГРАМИ, СТУПЕНІ ВИЩОЇ ОСВІТИ ТА КВАЛІФІКАЦІЇ	Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації розміщена на сайті НТУ «ХПІ» у відкритому доступі.
ДОТРИМАННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ ПРАЦІВНИКАМИ УНІВЕРСИТЕТУ ТА ЗДОБУВАЧАМИ ВИЩОЇ ОСВІТИ	В університеті працівниками та здобувачами вищої освіти здійснюється дотримання академічної доброчесності. Система забезпечення дотримання академічної доброчесності учасниками освітнього процесу базується на таких принципах: дотримання загальноприйнятих принципів моралі; демонстрація поваги до Конституції і законів України і дотримання їхніх 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.
СИСТЕМА ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ АКАДЕМІЧНОГО ПЛАГІАТУ	Здійснюється перевірка на плагіат згідно з вимогами нормативних документів Університету.

7. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

	ЗП 1	ЗП 2	ЗП 3	ЗП 4-6	ЗП 7	ЗП 8	ЗП 9-10	ЗП 11	ЗП 12	СП 1	СП 2	СП 3	СП 4	СП 5	СП 6	СП 7	СП 8	СП 9	СП 10-11	СП 12	СП 13	СП 14	СП 15	СП 16	СП 17	СП 18	СП 19	СП 20	СП 21	СП 22	СП 23	СП 24	СП 25	Атестація	ВП 1.1	ВП 1.2	ВП 1.3	ВП 1.4	ВП 1.5	ВП 2.1	ВП 2.2	ВП 2.3	ВП 2.4	ВП 2.5	ВВП 1	ВВП 2	ВВП 3	ВВП 4-5	ВВП 6	ВВП 7	ВВП 8	ВВП 9	ВВП 10	ВВП 11	ВВП 12
КЗ 1			X				X	X																																	X															
КЗ 2											X																																												
КЗ 3		X			X																											X																								
КЗ 4																														X			X																							
КЗ 5			X	X	X		X	X																																	X														
КЗ 6	X					X																																																		
КЗ 7	X					X			X																																															
КФ1																																X																							X	
КФ2										X		X	X	X	X			X	X						X					X			X		X		X	X	X		X		X	X	X			X				X	
КФ3										X		X	X	X						X				X		X	X																	X			X			X	X			X
КФ4																													X																										
КФ5														X	X		X	X				X		X			X					X		X	X			X														
КФ6																																		X																				
КФ7																	X						X					X				X																				
КФ8																							X																															X	
КФ9																							X									X																					X	
КФ10												X	X							X													X	X																			
КФ11																								X				X						X																		
КФ12																									X			X			X				X																		
КФ13																X		X	X		X																																		
КФ14																			X			X																																
КФ15																																																								

8. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

	ЗП 1	ЗП 2	ЗП 3	ЗП 4-6	ЗП 7	ЗП 8	ЗП 9-10	ЗП 11	ЗП 12	СП 1	СП 2	СП 3	СП 4	СП 5	СП 6	СП 7	СП 8	СП 9	СП 10-11	СП 12	СП 13	СП 14	СП 15	СП 16	СП 17	СП 18	СП 19	СП 20	СП 21	СП 22	СП 23	СП 24	СП 25	Атестація	ВП 1.1	ВП 1.2	ВП 1.3	ВП 1.4	ВП 1.5	ВП 2.1	ВП 2.2	ВП 2.3	ВП 2.4	ВП 2.5	ВВП 1	ВВП 2	ВВП 3	ВВП 4-5	ВВП 6	ВВП 7	ВВП 8	ВВП 9	ВВП 10	ВВП 11	ВВП 12
РН 1		X			X							X	X																																									
РН 2							X	X				X	X						X											X		X													X										
РН 3	X				X		X	X				X	X	X	X		X		X													X							X							X									
РН 4				X				X		X		X	X																X		X																								X
РН 5						X					X						X		X		X																								X						X				
РН 6			X	X		X					X				X																																							
РН 7																																	X																					
РН 8																											X						X																					
РН 9																											X		X				X																					
РН 10																								X		X					X																						
РН 11																																										X											
РН 12																																							X					X									
РН 13																																X																					
РН 14														X						X						X							X																				
РН 15							X											X		X																																		
РН 16																										X			X																								
РН 17																								X	X																												
РН 18																				X							X																										
РН 19																								X																													
РН 20																																	X																					
РН 21																								X																													
РН 22														X																X																							
РН 23																											X	X						X	X	X																	
РН 24																																																					
РН 25																																																					
РН 26																																																					
РН 27															X			X				X		X																													
РН 28																												X					X																				
РН 29																																																					
РН 30																																			X																			
РН 31																																					X										X						
РН 32																																		X																		
РН 33																																																				X	
РН 34																																																			X	
РН 35																							X		X				X				X																			
РН 36																																							X					X									X
РН 37																X																																				
РН 38																							X																													X
РН 39																				X																																
РН 40																					X																															
РН 41																							X																													
РН 42																																																					
РН 43																							X																													
РН 44																																																				
РН 45																							X																													
РН 46																																			X																	
РН 47																									X																											
РН 48																																			X																	
РН 49																																			X																	
РН 50																																			X																	
РН 51																																			X																	
РН 52																																				X																
РН 53												X	X													X																										
РН 54	X					X																																														
РН 55										X	X																																								
РН 56																										X									X																
РН 57																																										X			X				X				
РН 58			X							X												X									X														X							
РН 59						X														X																											X					
РН 60																			X																																X		
РН 61																																							X				X	X								
РН 62							X										X		X		X											X										X	X						X			
РН 63																X		X	X		X															X																
РН 64																					X															X				X											
РН 65									X																																										