

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНИЙ
УНІВЕРСИТЕТ

МІЖДИСЦИПЛІНАРНА
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека автоматизованих, мехатронних і робототехнічних систем»
професійна/наукова

назва ОП

першого (бакалаврського) рівня вищої освіти
назва рівня освіти

за спеціальностями G7 Автоматизація, комп'ютерно-інтегровані технології та
робототехніка
F5 Кібербезпека та захист інформації

код та найменування спеціальності

галузей знань G Інженерія, виробництво та будівництво
F Інформаційні технології

шифр та назва галузі знань

кваліфікація бакалавр з кібербезпеки автоматизованих, мехатронних і
робототехнічних систем
назва кваліфікації

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ ХНАДУ
протокол № від «_» 2025 р.
Голова вченої ради

Віктор БОГОМОЛОВ

підпис

ім'я та прізвище

Освітня програма вводиться в дію
з 01 вересня 2025 р.
наказ № від «_» 2025 р.
Ректор

Віктор БОГОМОЛОВ

підпис

ім'я та прізвище

Харків 2025 р.

ПЕРЕДМОВА

1. Розроблено проектною групою:

Філь Наталія Юріївна,
кандидат технічних наук,
доцент кафедри «Автоматизації
та комп'ютерно-інтегрованих
технологій»

ім'я та прізвище, посада

_____, гарант ОП.
підпис

Гурко Олександр Геннадійович,
доктор технічних наук, професор,
завідувач кафедри «Автоматизації
та комп'ютерно-інтегрованих
технологій»

ім'я та прізвище, посада

підпис

Плехова Ганна Анатоліївна,
доцентка, кандидатка технічних наук,
завідувачка кафедри «Комп'ютерних наук
і інформаційних систем»

ім'я та прізвище, посада

підпис

2. Рекомендовано методичною комісією механічного факультету
Протокол № 5 від « 17 » лютого 2025 р.

3. Схвалено Методичною радою
Протокол № 6 від « 26 » березня 2025 р.

4. Рецензенти:

Тимчук Сергій Олександрович доктор технічних наук, професор кафедри
інформаційних технологій Сумського державного університету

Халімов Геннадій Зайдулович доктор технічних наук, професор,
завідувач кафедри безпеки інформаційних технологій Харківського
національного університету радіоелектроніки

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

1 - Загальна інформація	
Повна назва закладу вищої освіти та кафедри, відповідальної за реалізацію ОП	Харківський національний автомобільно-дорожній університет, кафедра автоматизації і комп'ютерно-інтегрованих технологій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти – бакалавр Кваліфікація - бакалавр з кібербезпеки автоматизованих, мехатронних і робототехнічних систем
Форма здобуття освіти	денна
Офіційна назва освітньої програми	Кібербезпека автоматизованих, мехатронних і робототехнічних систем
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки, 10 місяців
Наявність акредитації	Сертифікат акредитації відсутній
Цикл/рівень	НРК України - 6 рівень, FQ-EHEA - перший цикл, EQF-LLL - 6 рівень
Передумови	Наявність повної загальної середньої освіти або ступеня молодшого бакалавра
Мова(и) викладання	Державна
Термін дії освітньої програми	5 років
Інтернет-адреса постійного розміщення опису освітньої програми	https://www.khadi.kharkov.ua/education/katalog-osvitnikh-program
2 - Мета освітньої програми	
Мета освітньої програми полягає у підготовці кваліфікованих фахівців, здатних розробляти, впроваджувати та використовувати технології забезпечення кібербезпеки автоматизованих, мехатронних і робототехнічних систем, а також розробляти, впроваджувати та експлуатувати ці системи з урахуванням вимог інформаційної безпеки.	

3 - Характеристика освітньої програми

Предметна область (галузь знань, спеціальність)	<i>Об'єкти:</i> технології та процеси кібербезпеки й автоматизації; методи управління захистом інформаційно-комунікаційних систем та інформаційних ресурсів; технічне, програмне забезпечення та сучасні інформаційні технології для створення безпечних і ефективних автоматизованих систем. <i>Цілі навчання:</i> Підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації, а також здатних до комплексного розв'язання задач розроблення нових і модернізації та експлуатації існуючих автоматизованих, мехатронних і робототехнічних систем. <i>Теоретичний зміст предметної області:</i> • Знання основ законодавства та стандартів у сфері кібербезпеки й автоматизації. • Принципи захисту інформації та автоматизованих систем. • Основи теорії автоматичного керування та систем автоматизації. Поняття та принципи теорії автоматичного керування, систем автоматизації, комп'ютерно-інтегрованих технологій та робототехніки. • Методи виявлення ризиків і забезпечення базового рівня безпеки інформації. • Сучасні інформаційні технології та програмно-технічні засоби для автоматизації й захисту. • Принципи роботи з апаратним і програмним забезпеченням автоматизованих систем. Розподіл дисциплін блока професійної підготовки: а) Кібербезпека та захист інформації (51 ECTS): ОК12, ОК15, ОК16, ОК18, ОК20, ОК23, ОК28, ОК30, ОК31, ОК34, ОК35 Основні дисципліни: «Основи кібербезпеки», «Криптологія, стеганографія та криптоаналіз», «Комплексний захист інформації», «Обробка інцидентів, моніторинг та аудит безпеки».
---	---

	б) Автоматизація, комп'ютерно-інтегровані технології та робототехніка (52 ECTS): ОК14, ОК17, ОК21, ОК22, ОК25, ОК26, ОК29, ОК32, ОК33 Основні дисципліни: «Теорія автоматичного керування», «Робототехніка», «Мехатроніка», «Автоматизовані системи керування технологічними процесами». в) Дисципліни, що забезпечують підготовку за обома напрямками (37 ECTS): ОК10, ОК11, ОК13, ОК19, ОК24, ОК27, ОК36, ОК37 Основні дисципліни: «Алгоритмізація та програмування», «Об'єктно-орієнтоване програмування», «Комп'ютерні мережі», «Управління інформаційною та кібербезпекою». <i>Методи, методики та технології.</i> Методи та технології забезпечення кіберзахисту автоматизованих, мехатронних і роботизованих систем; методики моделювання й налаштування базових систем автоматизації; інформаційні технології та програмні засоби для захисту даних, управління інформаційними ресурсами та автоматизованими об'єктами; використання сучасних технічних засобів автоматизації та розробка прикладного програмного забезпечення безпеки автоматизованих об'єктів. <i>Інструменти та обладнання:</i> • Системи розробки, забезпечення, моніторингу та контролю кібербезпеки автоматизованих, мехатронних і робототехнічних систем. • Сучасні програмно-технічні засоби для моделювання й налаштування базових систем автоматизації. • Програмно-апаратне забезпечення для захисту даних і роботи з автоматизованими об'єктами.
Орієнтація освітньої програми	Освітньо-професійна програма має міждисциплінарний підхід до підготовки фахівців, здатних комплексно розв'язувати задачі зі створення, модернізації, експлуатації та кіберзахисту автоматизованих, мехатронних і робототехнічних систем, використовуючи сучасні програмні й технічні засоби для їх налаштування, безпечного функціонування та захисту від кіберзагроз.

Основний фокус освітньої програми та спеціалізації	Програма спрямована на підготовку фахівців, які набувають навичок забезпечення інформаційної та кібербезпеки відповідно до міжнародних і національних стандартів, світових практик і сучасних технологій, а також оволодівають комп'ютерно-інтегрованими методами для вивчення та впровадження технічного, інформаційного, математичного, програмного й організаційного забезпечення автоматизованих, мехатронних і робототехнічних систем.
Особливості програми	Освітня програма відрізняється тим, що: – надає компетентності на стику кібербезпеки та автоматизації, поєднуючи дві спеціальності вищої освіти; – пропонує на початковому етапі дві освітні траєкторії з вибірконими блоками навчальних компонентів; – забезпечує можливість обрання індивідуальної траєкторії, що поєднує кіберзахист і технології автоматизації; – включає вивчення сучасних підходів до захисту автоматизованих, мехатронних і робототехнічних систем; – застосовує інноваційні технології навчання з використанням актуальних інформаційних інструментів і віртуальних ресурсів, зокрема на платформі Moodle.

4 - Придатність випускників до працевлаштування та подальшого навчання

Придатність до працевлаштування	Випускники програми підготовлені до професійної діяльності як фахівці з кіберзахисту автоматизованих, мехатронних і робототехнічних систем, спеціалісти з налаштування комп'ютерних систем та аналітики кібербезпеки. Вони можуть працювати на підприємствах будь-якої форми власності (державні, комерційні, некомерційні) у сферах, пов'язаних із автоматизацією та захистом інформації. Посади, які можуть займати випускники, відповідають Національному класифікатору професій ДК 003:2010, зокрема: 2131.2 аналітик комп'ютерних систем; 2131.2 інженер з автоматизованих систем керування виробництвом; 2131.2 інженер з комп'ютерних систем; 2139.2 інженер із застосування комп'ютерів; 2145.2 інженер з механізації та автоматизації виробничих процесів; 2149.2 інженер з керування й обслуговування систем; 2149.2 інженер із впровадження нової техніки й технології; 2149.2 мехатронік; 2149.2 професіонал із організації захисту інформації з обмеженим доступом; 2149.2 професіонал із організації інформаційної безпеки.
Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня вищої освіти за освітньо-науковою або освітньо-професійною програмою. Набуття додаткових кваліфікацій в системі післядипломної освіти.

5 - Викладання та оцінювання	
Викладання та навчання	Використовується проблемно-орієнтований, професійно-орієнтований, комунікативний, міждисциплінарний підходи до навчання, самонавчання. При викладанні практикується студентоцентроване навчання, самонавчання, застосовуються елементи дистанційної освіти, інтерактивні методи навчання. Основними формами організації навчального процесу є лекції, мультимедійні лекції, практичні заняття, консультації, курсове проектування, самостійна робота з рекомендованою літературою з можливістю консультацій з викладачем, виконання розрахунково-графічних, курсових робіт та проєктів, самостійна робота (використовуються технології дистанційного навчання на платформі Moodle), навчальна та виробнича практика. підготовка кваліфікаційної роботи.
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100- бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F). Поточний контроль знань проводиться в усній формі (опитування за результатами опрацьованого матеріалу) або у письмовій формі та у вигляді тестування. Підсумковий контроль знань у вигляді екзамену/заліку проводиться у письмовій або усній формі, тестового контролю. Оцінювання розрахунково-графічних, курсових робіт (проєктів), здійснюється у вигляді усного захисту. Оцінювання лабораторних робіт, практичних занять та практик – на підставі звітів та усного опитування. Підсумкова атестація здійснюється у формі публічного захисту кваліфікаційної роботи.

6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації, а також проблеми, що характеризуються комплексністю, під час проєктування та налагодження автоматизованих, мехатронних і робототехнічних систем
Загальні компетентності	ЗК1. Здатність застосовувати знання у практичних ситуаціях ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК8. 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 ЗК9. Навички використання інформаційних і комунікаційних технологій. ЗК10. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел. ЗК11. Навички здійснення безпечної діяльності. ЗК12. Здатність працювати в команді.

Спеціальні (фахові, предметні) компетентності	Автоматизація, комп'ютерно-інтегровані технології та робототехніка СК1. Здатність застосовувати базові знання математики в обсязі, необхідному для використання математичних методів у галузі автоматизації. СК2. Здатність застосовувати знання загальної фізики, електротехніки та електромеханіки, електроніки і мікропроцесорної техніки в обсязі, необхідному для розуміння процесів в системах автоматизації. СК3. Здатність проектування систем автоматизації з врахуванням вимог відповідних нормативно-правових документів та міжнародних стандартів, включаючи вимоги до кібербезпеки автоматизованих, мехатронних і робототехнічних систем, з використанням базових програмних середовищ для проектування для автоматизованих систем. СК4. Здатність застосовувати знання про основні принципи та методи вимірювання основних технологічних параметрів, необхідних для обслуговування систем автоматизації, з використанням датчиків і простих контролерів, із забезпеченням цілісності, автентичності та захищеності зібраних даних у контексті інформаційної та кібербезпеки. СК5. Здатність аргументувати вибір технічних засобів автоматизації на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи автоматизації і експлуатаційних умов; мати навички налагодження та обслуговування технічних засобів автоматизації і систем керування. СК6. Здатність оцінювати сучасний стан технічного та програмного забезпечення з використанням новітніх комп'ютерних технологій з урахуванням ризиків інформаційної безпеки та кіберзагроз в автоматизованих, мехатронних і робототехнічних системах. СК7. Здатність аналізувати об'єкти автоматизації; вміти вибирати параметри контролю і керування процесами; застосовувати методи теорії автоматичного керування для дослідження та аналізу систем автоматизації, забезпечуючи їхню стійкість до
--	--

	кібератак, несанкціонованого доступу та впливу шкідливого програмного забезпечення. СК8. Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями для вирішення професійних завдань, програмувати та використовувати прикладні та спеціалізовані комп'ютерно-інтегровані середовища для вирішення задач автоматизації, а також для забезпечення кіберзахисту автоматизованих, мехатронних і робототехнічних систем, враховуючи вимоги кібербезпеки, зокрема захисту даних, мережевої безпеки та безпеки програмного забезпечення, а також для забезпечення кіберзахисту автоматизованих, мехатронних і робототехнічних систем. СК9. Здатність застосовувати новітні технології в галузі автоматизації; використовувати комп'ютерно-інтегровані технології для збору даних та із архівування; створення бази даних параметрів процесу та із візуалізація за допомогою засобів людино-машинного інтерфейсу. Кібербезпека та захист інформації СК10. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК11. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації в автоматизованих, мехатронних і робототехнічних системах, зокрема у вбудованих пристроях, промислових контролерах, системах керування виробничими процесами та інтелектуальних кіберфізичних комплексах. СК12. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК13. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК14. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту
--	---

	інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК15. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою в автоматизованих, мехатронних і робототехнічних системах. СК16. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК17. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності, включаючи автоматизовані, мехатронні та робототехнічні системи, промислові мережі, програмно-апаратні комплекси керування та вбудовані системи безпеки. СК18. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 - Програмні результати навчання	
РН01. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН02. Спілкуватись іноземною мовою з метою забезпечення ефективності професійної комунікації. РН03. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. Автоматизація, комп'ютерно-інтегровані технології та робототехніка: РН04. Використовувати основні принципи фізики, електротехніки, електромеханіки, електроніки, схемотехніки, мікропроцесорної техніки для розрахунку параметрів та характеристик типових елементів систем автоматизації, зокрема для забезпечення їх кібербезпеки та захисту від несанкціонованого доступу і зовнішніх загроз в автоматизованих і роботизованих системах. РН05. Знати основні принципи та методи вимірювання основних технологічних параметрів для обґрунтування вибору засобів вимірювань та оцінювання їх метрологічних характеристик, з урахуванням вимог до	

кібербезпеки і захисту інформації в автоматизованих, мехатронних та робототехнічних системах.

РН06. Знати принципи роботи технічних засобів автоматизації та вміти обґрунтувати їх вибір на основі аналізу властивостей, призначення і технічних характеристик з урахуванням вимог до системи автоматизації та експлуатаційних умов; демонструвати навички налагодження технічних засобів автоматизації та вбудованих систем керування.

РН07. Вміти аналізувати об'єкти автоматизації (за галузями діяльності) і обґрунтовувати вибір структури, алгоритмів та схем керування ними на основі результатів дослідження їх властивостей, а також з урахуванням вимог кібербезпеки для захисту систем від кіберзагроз, забезпечуючи стійкість і безпеку роботи автоматизованих систем

РН08. Застосовувати базові знання електротехніки і мехатроніки для аналізу систем живлення та систем керування автоматизованого електроприводу, забезпечуючи при цьому належний рівень кібербезпеки для запобігання несанкціонованому доступу та забезпечення захищеності від кіберзагроз.

РН09. Застосовувати методи теорії автоматичного керування для дослідження та створення систем автоматизації, інтегруючи засоби кіберзахисту для забезпечення безпеки та стійкості цих систем.

РН10. Використовувати сучасні комп'ютерно-інтегровані технології для моніторингу та управління технологічними процесами за допомогою засобів людино-машинного інтерфейсу.

РН11. Застосовувати сучасні інформаційні технології та навички розроблення алгоритмів і комп'ютерних програм з використанням сучасних мов та технологій об'єктно-орієнтованого програмування, створювати бази даних та використовувати інтернет-ресурси для розробки систем автоматизації та робототехніки з урахуванням механізмів захисту від кіберзагроз.

РН12. Використовувати телекомунікаційні технології в системах автоматизації, зокрема для забезпечення захищеності каналів зв'язку та захисту від потенційних кіберзагроз у цих системах.

РН13. Знати та застосовувати вимоги нормативних документів і стандартів для конструювання типових схем автоматизації, враховуючи сучасні вимоги до кібербезпеки для захисту інформаційних систем та інфраструктури.

РН14. Враховувати соціальні аспекти та вимоги охорони праці, виробничої санітарії і пожежної безпеки під час формування технічних рішень. Вміти використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

РН15. Знати основи запобігання корупції, суспільної та академічної доброчесності на рівні, необхідному для формування нетерпимості до корупції та проявів недоброчесної поведінки серед здобувачів освіти та вміти

застосовувати їх в професійній діяльності.

Кібербезпека та захист інформації:

РН16. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність у галузі кіберзахисту автоматизованих, мехатронних і робототехнічних систем.

РН17. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення, зокрема у сфері проєктування та впровадження кіберзахисту в автоматизованих системах управління, мехатронних комплексах і робототехнічних системах.

РН18. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН19. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення, а також застосовувати сучасні математичні методи для дослідження та створення систем автоматизації, мехатронних комплексів і роботизованих систем з вбудованими засобами захисту інформації.

РН20. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації, зокрема у сфері автоматизованих, мехатронних і робототехнічних систем.

РН21. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності, у тому числі для забезпечення стійкості до кіберзагроз у автоматизованих, мехатронних та робототехнічних системах.

РН22. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки, з урахуванням особливостей автоматизованих систем управління, мехатронних і робототехнічних комплексів.

РН23. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні

процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

РН24. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації, у тому числі в автоматизованих, мехатронних і робототехнічних системах.

РН25. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН26. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах, а також у системах автоматизованого управління технологічними процесами, мехатронних і робототехнічних системах.

РН27. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН28. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН29. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН30. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

РН31. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

8 - Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Усі науково-педагогічні працівники мають кваліфікацію відповідно освітніх компонент, досвід практичної та науково-педагогічної діяльності, регулярно підвищують свою кваліфікацію через участь у наукових проектах, конференціях, стажування в закладах та підприємствах України.
Матеріально-технічне забезпечення	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою та відповідають вимогам Ліцензійних умов (Постанова Кабінету Міністрів України № 1187 від 30.12.2015 р. «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» у редакції від 24.03.2021 р. № 365). Навчальні аудиторії мають мультимедійне та презентаційне обладнання та устаткування для проведення занять, комп'ютерні класи з підключенням до мережі Інтернет, є можливість здобувачів виходити до Інтернет з власних пристроїв за допомогою Wi-Fi. У наявності соціально-побутова інфраструктура, забезпеченість гуртожитком.
Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт http://www.khadi.kharkov.ua надає інформацію про освітні програми, навчальну, наукову та виховну діяльність, структурні підрозділи, умови вступу та контактні дані. Матеріали навчально-методичного забезпечення освітньої програми доступні у Модульному середовищі. Навчальний процес підтримується сучасною навчально-методичною, науково-технічною та довідковою літературою, яка зберігається у фондах бібліотеки ХНАДУ (http://library.khadi.kharkov.ua) з можливістю вільного доступу через інтернет до електронного каталогу, представлена в електронному архіві ХНАДУ (https://dspace.khadi.kharkov.ua/dspace), а також розміщена на сторінках курсів на освітньому порталі університету (https://dl2022.khadi-kh.com/). Кожен комп'ютер закладу вищої освіти має вільний доступ до ключових наукометричних баз даних, зокрема SCOPUS та Web of Science.

9 - Академічна мобільність	
Національна кредитна мобільність	Здійснюється порядком реалізації права на академічну мобільність учасників освітнього процесу харківського національного автомобільно-дорожнього університету та передбачає: підвищення кваліфікації викладачів; участь здобувачів і викладачів у міжнародних та всеукраїнських конференціях і семінарах; участь здобувачів у міжнародних та всеукраїнських олімпіадах та конкурсах.
Міжнародна кредитна мобільність	Мобільність студентів організовується на підставі партнерської угоди про співробітництво із зарубіжними університетами про участь у міжнародних освітніх програмах, які дають можливість: одержати додаткові знання у суміжних галузях науки; удосконалювати рівень володіння іноземною мовою.
Навчання іноземних здобувачів вищої освіти	За даною освітньо-професійною програмою можливе навчання іноземних здобувачів вищої освіти.

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонентів ОП

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
Обов'язкові компоненти ОП (216 ECTS)			
Блок загальної підготовки (45 ECTS)			
Компоненти гуманітарної та соціально-економічної підготовки			
OK 01	Іноземна мова (за професійним спрямуванням)	13	екзамен
OK 02	Історія і культура України	3	залік
OK 03	Філософія	3	екзамен
Компоненти природничо-наукової (фундаментальної) підготовки			
OK 04	Основи інформаційних технологій	4	екзамен
OK 05	Українська мова (за професійним спрямуванням)	3	екзамен
OK 06	Фізика	4	екзамен
OK 07	Вища математика	8	екзамен
OK 08	Охорона праці та здоровий спосіб життя	3	екзамен
Блок професійної підготовки (171 ECTS)			
OK 09	Вступ до фаху	3	залік
OK 10	Алгоритмізація та програмування	10	екзамен
OK 11	Основи кібербезпеки	5	екзамен
OK 12	Інформаційна безпека	4	залік
OK 13	Операційні системи та безпека операційних систем	4	залік
OK 14	Теорія інформації та кодування	5	залік
OK 15	Безпека безпроводних, мобільних та хмарних технологій	3	залік
OK 16	Електроніка та мікросхемотехніка	5	екзамен
OK 17	Інтелектуальні системи інформаційної безпеки	4	залік
OK 18	Базові методи аналізу та моделювання в кібербезпеці	4	залік
OK 19	Мехатроніка	7	екзамен
OK 20	Архітектура комп'ютерних систем	3	залік
OK 21	Об'єктно-орієнтоване програмування	5	екзамен
OK 22	Правові основи кібербезпеки і захисту інформації	3	екзамен
OK 23	Теорія автоматичного керування	9	екзамен
OK 24	Автоматизовані системи керування технологічними процесами	5	екзамен
OK 25	Оцінка захищеності інформації в інформаційно-комунікаційних системах	3	залік
OK 26	Числові методи і моделювання на ЕОМ	4	екзамен
OK 27	Робототехніка	8	екзамен
OK 28	Елементи і функціональні вузли інформаційно	4	екзамен

	вимірювальних комплексів		
ОК 29	Інформаційно-телекомунікаційні системи, бази даних та їх захист	5	екзамен
ОК 30	Методи оцінки захищеності інформаційних систем	5	залік
ОК 31	Мікропроцесорна техніка	5	екзамен
ОК 32	Бази даних	3	залік
ОК 33	Комплексний захист інформації	4	екзамен
ОК 34	Обробка інцидентів, моніторинг та аудит безпеки	4	екзамен
ОК 35	Основи конструювання та системи автоматизованого проектування	6	екзамен
ОК 36	Промислові логічні контролери	3	залік
ОК 37	Технічні засоби захисту інформації	3	залік
ОК 38	Криптологія, стеганографія та криптоаналіз	6	екзамен
ОК 39	Комп'ютерні мережі	3	екзамен
ОК 40	Управління інформаційною та кібербезпекою	3	залік
	Практична підготовка та атестація (28 ECTS)		
ОК 41	Навчальна практика	4	залік
ОК 42	Навчальна практика	4	залік
ОК 43	Навчальна практика	4	залік
ОК 44	Переддипломна практика	4	залік
ОК 45	Кваліфікаційна робота	12	залік
	Вибіркові дисципліни (24 ECTS)		
	Компоненти гуманітарної та соціально-економічної підготовки		
ВД 01	Вибіркова дисципліна 1	3	залік
ВД 02	Вибіркова дисципліна 2	3	залік
	Компоненти природничо-наукової (фундаментальної) підготовки		
ВД 03	Вибіркова дисципліна 3	3	залік
ВД 04	Вибіркова дисципліна 4	3	залік
	Компоненти професійної підготовки:		
ВД 05	Вибіркова дисципліна 5	4	залік
ВД 06	Вибіркова дисципліна 6	4	залік
ВД 07	Вибіркова дисципліна 7	4	залік
	Дисципліни з окремим статусом		
ОК46	БЗВП	3	залік
	Загальний обсяг вибірових компонентів:	24,00	
	ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	240,00	

*Дозволяється вибір здобувачем із загальноуніверситетського каталогу в тому числі з інших ОП згідно до п. 2.2

2.2 Загально університетський каталог вибіркових дисциплін розміщено на офіційному сайті університету за посиланням:
<https://www.khadi.kharkov.ua/education/katalog-vibirkovikh-disciplin/bakalavr/>

4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників міждисциплінарної освітньої програми «Кіберзахист автоматизованих, мехатронних і робототехнічних систем» здійснюється у формі публічного захисту кваліфікаційної роботи та завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням освітньої кваліфікації «Бакалавр з кібербезпеки та автоматизації і комп'ютерно-інтегрованих технологій».

Атестація здійснюється відкрито і публічно. Кваліфікаційна робота бакалавра підлягає обов'язковій перевірці на академічний плагіат.

Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозиторії закладу вищої освіти.

1. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	OK01	OK02	OK03	OK04	OK05	OK06	OK07	OK08	OK09	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OK37	OK38	OK39	OK40	OK41	OK42	OK43	OK44	OK45	OK46								
3K1						•	•			•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•						
3K2						•	•		•		•	•		•		•			•			•	•	•				•	•						•	•																		
3K3					•																																																	
3K4	•																																																					
3K5									•																																													
3K6		•	•					•															•																															
3K7			•					•	•														•																															
3K8		•	•					•																																														
3K9				•						•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			
3K10			•	•						•			•		•		•	•		•	•				•	•			•	•		•	•	•			•	•	•	•	•					•								
3K11								•			•	•													•																													
3K12										•									•																																			
CK1							•							•				•						•			•																											
CK2						•										•			•									•	•				•																					
CK3																•			•					•	•			•					•			•	•					•												
CK4																•								•				•					•				•																	
CK5																•			•					•			•	•					•			•	•						•											
CK6										•	•												•	•	•		•				•				•																			
CK7																							•	•				•									•																	
CK8				•						•			•				•			•	•					•				•				•				•					•											
CK9										•														•									•				•																	
CK10									•		•	•										•																																
CK11				•					•	•	•	•	•	•	•	•	•	•		•	•			•	•	•			•	•		•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		
CK12						•					•	•	•		•		•								•					•	•						•		•	•	•	•				•								
CK13													•																			•			•	•																		
CK14								•														•													•	•			•	•						•	•							

	OK01	OK02	OK03	OK04	OK05	OK06	OK07	OK08	OK09	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OK37	OK38	OK39	OK40	OK41	OK42	OK43	OK44	OK45	OK46		
CK15											•											•																										
CK16														•																																		
CK17																			•					•				•																				
CK18												•	•		•		•	•							•				•	•				•	•									•				

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

	OK01	OK02	OK03	OK04	OK05	OK06	OK07	OK08	OK09	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OK37	OK38	OK39	OK40	OK41	OK42	OK43	OK44	OK45	OK46			
ПРН1					•																																												
ПРН2	•																																																
ПРН3		•	•																			•																		•						•			
ПРН4				•		•			•							•				•								•					•																
ПРН5				•		•	•													•													•																
ПРН6																•				•									•	•			•			•	•				•								
ПРН7																	•						•	•					•	•					•	•													
ПРН8																•				•				•	•					•													•						
ПРН9																			•				•	•																		•							
ПРН10										•											•				•				•							•	•												
ПРН11				•					•	•			•							•	•				•				•				•				•	•					•						
ПРН12															•																•							•											
ПРН13																						•												•					•										
ПРН14								•																																									
ПРН15		•	•																																														•
ПРН16									•	•	•										•																			•	•		•						
ПРН17											•													•													•						•	•					

	OK01	OK02	OK03	OK04	OK05	OK06	OK07	OK08	OK09	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OK37	OK38	OK39	OK40	OK41	OK42	OK43	OK44	OK45	OK46	
ПРН18									•		•										•																			•	•						
ПРН19						•	•			•				•				•					•			•								•							•	•					
ПРН20											•	•										•													•				•								
ПРН21										•	•		•		•		•	•		•	•				•	•				•			•	•									•				
ПРН22												•			•		•	•			•					•	•			•			•	•			•										
ПРН23													•							•																		•									
ПРН24													•										•			•									•							•	•				
ПРН25																	•	•							•						•			•													
ПРН26																	•							•						•				•								•	•				
ПРН27																										•					•			•						•							
ПРН28														•				•																				•					•	•			
ПРН29														•							•		•																•	•							
ПРН30											•														•																		•	•			
ПРН31																																•			•												

2. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ТА КОМПЕТЕНТНОСТЕЙ

	ПРН1	ПРН2	ПРН3	ПРН4	ПРН5	ПРН6	ПРН7	ПРН8	ПРН9	ПРН10	ПРН11	ПРН12	ПРН13	ПРН14	ПРН15	ПРН16	ПРН17	ПРН18	ПРН19	ПРН20	ПРН21	ПРН22	ПРН23	ПРН24	ПРН25	ПРН26	ПРН27	ПРН28	ПРН29	ПРН30	ПРН31		
3K1				•	•						•								•	•		•											
3K2																		•	•														
3K3																•	•									•							
3K4		•																															
3K5	•																																
3K6																	•								•								
3K7																•										•				•			
3K8			•												•												•						
3K9																				•									•				
3K10																												•			•		
3K11																•	•																
3K12														•	•		•																
CK1				•						•			•																				
CK2											•										•				•								
CK3																						•						•	•		•		
CK4																								•		•	•						
CK5																										•		•			•	•	
CK6																							•							•	•		
CK7																								•	•	•		•					
CK8											•	•											•										
CK9													•								•									•			
CK10						•	•		•																								
CK11												•											•							•			
CK12							•		•	•														•									
CK13																						•				•						•	
CK14															•							•		•									
CK15																					•			•				•		•			
CK16																								•	•							•	
CK17																						•		•		•			•				
CK18																												•	•	•			

Гарант освітньо-професійної програми
к.т.н., доцент, доцент кафедри
«Автоматизації та комп'ютерно-
інтегрованих технологій»

Н. Ю. Філь

Структурно-логічна схема міждисциплінарної освітньо-професійної програми

