МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІВЕРСИТЕТ

МІЖДИСЦИПЛІНАРНА ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА АВТОМАТИЗОВАНИХ, МЕХАТРОННИХ І РОБОТОТЕХНІЧНИХ СИСТЕМ»

першого (бакалаврського) рівня вищої освіти
за спеціальностями G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка, F5 Кібербезпека та захист інформації
галузей знань G Інженерія, виробництво та будівництво
F Інформаційні технології
кваліфікація Бакалавр кібербезпеки автоматизованих, мехатронних і робототехнічних систем

ЗАТВЕРДЖЕНО
Вченою радою ХНАДУ
Протокол № 88/26 від «03» липня 2026 р.

Освітня програма вводиться в дію з 1 вересня 2026 р.
Наказ № 92 від «06» липня 2026 р.

Зі змінами на підставі рішення Вченої Ради ХНАДУ
Протокол № 91/26 від «28» серпня 2026 р.
Голова Вченої ради

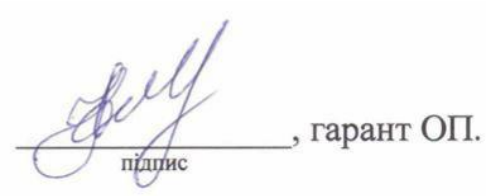
_____ Ілля ДМИТРІЄВ

Харків 2026 р.

1/81.1-01 від 26.03.2021

ПЕРЕДМОВА

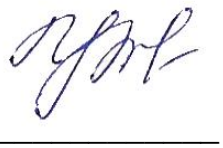
1. Розроблено проектною групою:
Філь Наталія Юріївна,
кандидат технічних наук,
доцент кафедри «Автоматизації
та комп'ютерно-інтегрованих
технологій»
ім'я та прізвище, посада


підпис, гарант ОП.

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


підпис

Крайнюк Олена Володимирівна,
доцент, кандидат технічних наук,
завідувачка кафедри «Кібербезпеки»



ім'я та прізвище, посада

підпис

2. Рекомендовано методичною комісією механічного факультету
Протокол № 7 від « 14 » квітня 2026 р.

3. Схвалено Методичною радою ХНАДУ
Протокол № 8 засідання «27» серпня 2026 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 за цією освітньою програмою	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)	*Об'єкти:* 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. *Цілі навчання:* 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. *Теоретичний зміст предметної області:* • 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): ОК11, ОК12, ОК15, ОК18, ОК16, ОК18, ОК21, ОК25, ОК27, ОК29 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): ОК23, ОК19, ОК26, ОК24, ОК28, ОК33 Основні дисципліни: «Теорія автоматичного керування», «Робототехніка», «Мехатроніка», «Автоматизовані системи керування технологічними процесами», «Мікропроцесорна техніка», «Основи конструювання та системи автоматизованого проєктування». в) Дисципліни, що забезпечують підготовку за обома напрямками (37 ECTS): ОК10, ОК22. Основні дисципліни: «Алгоритмізація та програмування, «Об'єктно-орієнтоване програмування», «Комп'ютерні мережі». *Методи, методики та технології.* 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. *Інструменти та обладнання*: • 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 вибірковими 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-орієнований, 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. Прагнення до збереження навколишнього середовища ЗК13. Здатність працювати в команді.

Спеціальні (фахові, предметні) компетентності	**Автоматизація, комп'ютерно-інтегровані технології та робототехніка** СК1. Здатність застосовувати знання математики, в обсязі, необхідному для використання математичних методів для аналізу і синтезу систем автоматизації. СК2. Здатність застосовувати знання фізики, електротехніки, електроніки і мікропроцесорної техніки, в обсязі, необхідному для розуміння процесів в системах автоматизації та комп'ютерно-інтегрованих технологіях. СК3. Здатність виконувати аналіз об'єктів автоматизації на основі знань про процеси, що в них відбуваються та застосовувати методи теорії автоматичного керування для дослідження, аналізу та синтезу систем автоматичного керування. СК4. Здатність застосовувати методи системного аналізу, математичного моделювання, ідентифікації та числові методи для розроблення математичних моделей окремих елементів та систем автоматизації в цілому, для аналізу якості їх функціонування із використанням новітніх комп'ютерних технологій. СК5. Здатність обґрунтовувати вибір технічних засобів автоматизації на основі розуміння принципів їх роботи аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи автоматизації і експлуатаційних умов; налагоджувати технічні засоби автоматизації та системи керування СК6. Здатність використовувати для вирішення професійних завдань новітні технології у галузі автоматизації та комп'ютерно-інтегрованих технологій, зокрема, проектування багаторівневих систем керування, збору даних та їх архівування для формування бази даних параметрів процесу та їх візуалізації за допомогою засобів людино-машинного інтерфейсу. СК7. Здатність обґрунтовувати вибір технічної структури та вміти розробляти прикладне програмне забезпечення для мікропроцесорних систем керування на базі локальних засобів автоматизації, промислових логічних контролерів та 8 програмованих логічних матриць і сигнальних

	процесорів. СК8. Здатність проектування систем автоматизації з врахуванням вимог відповідних нормативно-правових документів та міжнародних стандартів. СК9. Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями для вирішення професійних завдань, програмувати та використовувати прикладні та спеціалізовані комп'ютерноінтегровані середовища для вирішення задач автоматизації. СК10. Здатність враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії і пожежної безпеки під час формування технічних рішень. СК11. Врахування комерційного та економічного контексту при проектуванні систем автоматизації. **Кібербезпека та захист інформації** СК12. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК13. 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. СК14. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК15. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК16. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК17. Здатність здійснювати професійну діяльність на основі впровадженої системи управління

	інформаційною та кібербезпекою в автоматизованих, мехатронних і робототехнічних системах. СК18. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК19. 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. СК20. 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. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких проявів недоброчесності **Автоматизація, комп'ютерно-інтегровані технології та робототехніка:** ПР04. Знати лінійну та векторну алгебру, диференціальне та інтегральне числення, функції багатьох змінних, функціональні ряди, диференціальні рівняння для функції однієї та багатьох змінних, операційне числення, теорію функції комплексної змінної, теорію ймовірностей та математичну статистику, теорію випадкових процесів в обсязі, необхідному для користування математичним апаратом та методами у галузі автоматизації. ПР05. Знати фізику, електротехніку, електроніку та схемотехніку, мікропроцесорну техніку на рівні, необхідному для розв'язання типових задач і проблем автоматизації. ПР06. Вміти застосовувати сучасні інформаційні технології та мати навички розробляти алгоритми та комп'ютерні програми з використанням мов високого рівня та технологій об'єктно-орієнтованого програмування, створювати бази даних та використовувати інтернет-ресурси. ПР07. Розуміти суть процесів, що відбуваються в об'єктах автоматизації (за галузями діяльності) та вміти проводити аналіз об'єктів автоматизації і обґрунтовувати вибір структури, алгоритмів та схем керування ними на	

основі результатів дослідження їх властивостей.

ПР08. Вміти застосовувати методи теорії автоматичного керування для дослідження, аналізу та синтезу систем автоматичного керування.

ПР09. Вміти застосовувати методи системного аналізу, моделювання, ідентифікації та числові методи для розроблення математичних та імітаційних моделей окремих елементів та систем автоматизації в цілому, для аналізу якості їх функціонування із використанням новітніх комп'ютерних технологій.

ПР10. Вміти застосовувати знання про основні принципи та методи вимірювання фізичних величин і основних технологічних параметрів для обґрунтування вибору засобів вимірювань та оцінювання їх метрологічних характеристик.

ПР11. Знати принципи роботи технічних засобів автоматизації та вміти обґрунтувати їх вибір на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи автоматизації та експлуатаційних умов; мати навички налагодження технічних засобів автоматизації та систем керування.

ПР12. Вміти проектувати багаторівневі системи керування і збору даних для формування бази параметрів процесу та їх візуалізації за допомогою засобів людино-машинного інтерфейсу, використовуючи новітні комп'ютерноінтегровані технології.

ПР13. Вміти обґрунтовувати вибір структури та розробляти прикладне програмне забезпечення для мікропроцесорних систем управління на базі локальних засобів автоматизації, промислових логічних контролерів та програмованих логічних матриць і сигнальних процесорів.

ПР14. Вміти виконувати роботи з проектування систем автоматизації, знати зміст і правила оформлення проектних матеріалів, склад проектної документації та послідовність виконання проектних робіт з врахуванням вимог відповідних нормативно-правових документів та міжнародних стандартів.

ПР15. Вміти використовувати різноманітне спеціалізоване програмне забезпечення для розв'язування типових інженерних задач у галузі автоматизації, зокрема, математичного моделювання, автоматизованого проектування, керування базами даних, методів комп'ютерної графіки.

ПР16. Вміти враховувати соціальні, екологічні, етичні, економічні аспекти, 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.

ПР17. Вміти використовувати у виробничій і соціальній діяльності фундаментальні поняття і категорії державотворення для обґрунтування власних світоглядних позицій та політичних переконань з урахуванням процесів соціально-політичної історії України, правових засад та етичних норм.

Кібербезпека та захист інформації:

ПР18. 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.

ПР19. 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.

ПР20. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

ПР21. 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.

ПР22. 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.

ПР23. 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.

ПР24. 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.

ПР25. 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.

ПР26. 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.

ПР27. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

ПР28. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах, а також у системах автоматизованого управління технологічними процесами, мехатронних і робототехнічних системах.

ПР29. 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.

ПР30. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.

ПР31. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

ПР32. 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.

ПР33. 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.

ПР34 Розуміти і реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності вільного демократичного суспільства, верховенства права, прав і свобод людини і громадянина в Україні.

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 (180 **ECTS**)			
	Блок загальної підготовки (44 ECTS)		
Компоненти гуманітарної та соціально-економічної підготовки			
ОК 01	Українська мова (за професійним спрямуванням)	3	екзамен
ОК 02	Іноземна мова (за професійним спрямуванням)	11	екзамен
ОК 03	Основи національного спротиву	5	залік
ОК 04	Історія і культура України	3	залік
ОК 05	Філософія	3	екзамен
Компоненти природничо-наукової (фундаментальної) підготовки			
ОК 06	Основи інформаційних технологій	4	екзамен
ОК 07	Фізика	4	залік
ОК 08	Вища математика	8	екзамен
ОК 09	Охорона праці та здоровий спосіб життя	3	екзамен
	Блок професійної підготовки (108 ECTS)		
ОК 10	Алгоритмізація та програмування	7	екзамен
ОК 11	Основи кібербезпеки	6	екзамен
ОК 12	Вступ до фаху	3	залік
ОК13	Інформаційна безпека	4	залік
удалить	Операційні системи та безпека операційних систем		залік
ОК 14	Теорія інформації та кодування	4	залік
ОК 15	Базові методи аналізу та моделювання в кібербезпеці	3	екзамен
ОК 16	Безпека безпровідних, мобільних та хмарних технологій	3	залік
ОК 17	Електроніка та мікросхемотехніка	5	екзамен
ОК 18	Правові основи кібербезпеки і захисту інформації	3	залік
ОК 19	Мехатроніка	7	екзамен
ОК 20	Архітектура комп'ютерних систем та захист операційних систем	6	екзамен
ОК 21	Об'єктно-орієнтоване програмування	5	екзамен
ОК 22	Теорія автоматичного керування	8	екзамен
ОК 23	Автоматизовані системи керування технологічними процесами	5	екзамен
ОК 24	Комплексний захист інформації	3	екзамен

ОК 25	Методи оцінки захищеності інформаційних та комунікаційних системах	3	залік
ОК 26	Робототехніка	8	екзамен
ОК 27	Мережеві інформаційно-телекомунікаційні системи, бази даних та їх захист	3	екзамен
ОК 28	Мікропроцесорна техніка	5	екзамен
ОК 29	Обробка інцидентів, моніторинг та аудит безпеки	4	екзамен
ОК 30	Основи конструювання та системи автоматизованого проєктування	5	екзамен
ОК 31	Програмовані логічні контролери	3	екзамен
ОК 32	Криптологія, стеганографія та криптоаналіз	5	екзамен
	Практична підготовка та атестація (28 ECTS)		
ОК 33	Навчальна практика	4	залік
ОК 34	Навчальна практика	4	залік
ОК 35	Виробнича (технологічна) практика	4	залік
ОК 36	Переддипломна практика	4	залік
ОК 37	Кваліфікаційна робота	12	залік
	Вибіркові дисципліни (60 ECTS)		
	Компоненти гуманітарної та соціально-економічної підготовки		
ВД 01	Психологія	3	залік
ВД 02	Правознавство	3	залік
ВД 03	Політологія	3	залік
ВД 04	Економічна теорія	3	залік
	Компоненти природничо-наукової (фундаментальної) підготовки		
ВД 05	Вступ до ймовірнісно-статистичного аналізу	3	залік
ВД 06	Математичні методи в техніці і технологіях	3	залік
ВД 07	Основи наукових досліджень та інженерна творчість	3	залік
ВД 08	Сучасні інформаційні технології	3	залік
	Компоненти професійної підготовки:		
ВД 09	Кібербезпека IoT-систем та смарт-пристроїв	4	залік
ВД 10	Геоінформаційні системи	4	залік
ВД 11	Кібербезпека промислових систем	4	залік
ВД 12	Основи CALS-технологій	4	залік
ВД 13	Автоматизовані системи управління експериментом	4	залік
ВД 14	Гнучке автоматизоване виробництво і робото-технічні комплекси	4	залік
ВД 15	Технічні засоби захисту інформації	4	залік
ВД 16	Безпека штучного інтелекту в кіберфізичних системах	4	залік
ВД 17	Методи та системи штучного інтелекту	4	залік

	Загальний обсяг вибіркових компонентів:	**60,00**	
	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

	ОК01	ОК02	ОК03	ОК04	ОК05	ОК06	ОК07	ОК08	ОК09	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37
ЗК1	•	•				•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК2		•				•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•					•
ЗК3	•	•			•							•						•	•				•			•										•
ЗК4		•				•		•		•					•														•			•				•
ЗК5	•	•				•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК6																			•	•			•			•				•	•						•
ЗК7				•	•							•						•																			•
ЗК8	•			•	•				•																												•
ЗК9		•				•				•	•		•			•				•	•						•						•	•	•		•
ЗК10		•				•	•	•		•	•		•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ЗК11									•																												•
ЗК12									•																					•					•		•
ЗК13		•								•		•																					•				•
СК1						•	•	•							•							•											•			•	•
СК2							•										•		•								•					•			•	•
СК3																						•	•			•								•		•	•
СК4								•							•							•												•		•	•
СК5																	•		•				•			•		•		•	•			•	•	•	•
СК6												•							•			•	•			•				•					•	•	•
СК7																			•		•	•				•		•			•			•		•	•
СК8																														•					•	•	•
СК9										•		•					•		•	•	•					•		•		•	•		•		•	•
СК10									•			•											•							•					•	•	•
СК11												•						•				•	•							•	•				•	•	•
СК12											•		•					•																	•	•	•
СК13										•	•	•	•	•	•	•			•	•	•		•		•	•	•					•	•	•	•	•	•

CK14	CK15	CK16	CK17	CK18	CK19	CK20	
•	•	•	•	•	•	•	
•	•	•	•	•	•	•	
•	•	•	•	•	•	•	
		•					
•							
•				•		•	
•	•		•			•	
					•		
•	•	•	•			•	
•						•	
•						•	
•	•	•	•			•	
•			•				
			•				
•			•			•	
			•		•		
•	•	•					
				•		•	
•		•				•	
•						•	
•						•	
			•				
							•

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

	ОК01	ОК02	ОК03	ОК04	ОК05	ОК06	ОК07	ОК08	ОК09	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37
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	ПРН32	ПРН33	ПРН34
ОК01								
ОК02								
ОК03								•
ОК04								
ОК05								
ОК06								
ОК07								
ОК08								
ОК09								
ОК10								
ОК11								
ОК12	•							
ОК13	•							
ОК14								
ОК15								
ОК16								
ОК17								
ОК18								
ОК19								
ОК20								
ОК21								
ОК22			•					
ОК23		•						
ОК24		•	•	•	•	•	•	
ОК25	•							
ОК26						•		
ОК27						•		
ОК28							•	
ОК29	•	•	•		•		•	
ОК30								
ОК31		•						
ОК32				•	•			
ОК33								
ОК34								
ОК35								
ОК36	•							
ОК37	•	•	•	•	•	•	•	

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	ППР21	ПРН22	ПРН23	ПРН24	ПРН25	ПРН26	ПРН27	ПРН28	ПРН29	ПРН30	ПРН31	ПРН32	ПРН33	ПРН34
ЗК1						•		•	•	•	•	•												•		•							•	
ЗК2				•	•		•				•			•						•	•													
ЗК3	•																																	
ЗК4		•																																
ЗК5						•									•					•			•											
ЗК6																	•																	•
ЗК7			•																															
ЗК8																•	•																	
ЗК9						•				•					•								•		•	•								
ЗК10						•		•											•							•	•						•	
ЗК11																•								•				•						
ЗК12																•																		
ЗК13																		•											•					
СК1				•				•	•												•													
СК2					•		•																											
СК3							•	•																										
СК4								•	•						•																			
СК5										•	•																							
СК6						•				•		•			•																			
СК7						•				•			•																					
СК8														•																				
СК9						•				•					•																			
СК10																•																		
СК11																•																		
СК12														•								•												
СК13																							•		•	•								
СК14																								•	•								•	
СК15																										•	•	•						
СК16																									•	•		•	•					
СК17																							•			•			•					
СК18																														•	•			
СК19																																•	•	
СК20																											•						•	

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

