МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

Другий (магістерський) рівень вищої освіти

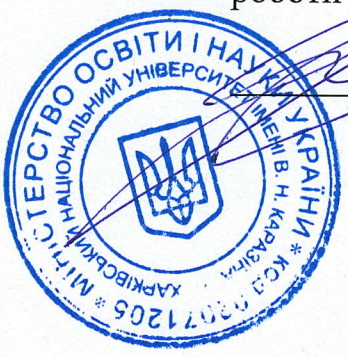
Галузь знань F «Інформаційні технології»

Спеціальність F 5 – Кібербезпека та захист інформації

ЗАТВЕРДЖЕНО
Вченою радою університету
протокол від 26.05.2025 № 14

Введено в дію з _____
наказ від 28.05.2025 № 0114-1/254

Проректор з науково-педагогічної
роботи
Борис САМОРОДОВ
_____



ХАРКІВ–2025

ЛИСТ ПОГОДЖЕННЯ ОПП

Науково-методичною радою університету
протокол від 21.05.2025 № 10
Заст. Голови НМР

_____ **Сергій ЄЛЬЦОВ**

Вчена рада навчально-наукового інституту комп'ютерних наук та штучного інтелекту
протокол від 15.03.2025 № 11
Голова Вченої ради навчально-наукового інституту комп'ютерних наук та штучного інтелекту

_____ **Дмитро УЗЛОВ**

Науково-методична комісія навчально-наукового інституту комп'ютерних наук та штучного інтелекту
протокол від 15.03.2025 № 8
Голова методичної комісії навчально-наукового інституту комп'ютерних наук та штучного інтелекту

_____ **Євген ПОКЛОНСЬКИЙ**

Кафедра кібербезпеки інформаційних систем, мереж і технологій
протокол від 14.03.2025 № 8а
В.о. завідувача кафедри кібербезпеки інформаційних систем, мереж і технологій

_____ **Марина ЄСІНА**

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Прізвище, ім'я, по батькові	Найменування посади	Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно
Керівник робочої групи		
Єсін Віталій Іванович – гарант програми	Професор кафедри кібербезпеки інформаційних систем, мереж і технологій, гарант програми	Доктор технічних наук (05.13.06 – інформаційні технології), професор, професор кафедри кібербезпеки інформаційних систем, мереж і технологій
Члени робочої групи		
Олійников Роман Васильович	Професор кафедри кібербезпеки інформаційних систем, мереж і технологій	Доктор технічних наук (05.13.05 – комп'ютерні системи та компоненти), професор, професор кафедри кібербезпеки інформаційних систем, мереж і технологій
Сватовський Ігор Іванович	Доцент кафедри кібербезпеки інформаційних систем, мереж і технологій	Кандидат технічних наук (20.02.14 – озброєння та військова техніка), старший науковий співробітник.
Мелкозьорова Ольга Михайлівна	Доцент кафедри кібербезпеки інформаційних систем, мереж і технологій	Кандидат технічних наук (05.03.07 – процеси фізико-технічної обробки»), доцент.
Колованова Євгенія Павлівна	Доцент кафедри кібербезпеки інформаційних систем, мереж і технологій	Кандидат технічних наук (05.13.21 – системи захисту інформації)

До проектування освітньої програми долучені:
Представники здобувачів вищої освіти: Логачова Єлізавета Олегівна,
Представники роботодавців: Горбенко Юрій Іванович, Перший заступник головного конструктора ПАТ "Інститут інформаційних технологій", к.т.н.

При розробці проекту Програми враховані вимоги:

1) Освітнього стандарту спеціальності 125 – «Кібербезпека» для другого (магістерського) рівня освіти, що погоджено рішенням Національного агентства із забезпечення якості вищої освіти, протокол від 23.02.2021 р. № 3, та Затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

2) Професійних стандартів у сфері інформаційної безпеки та кібербезпеки, розроблених фахівцями Держспецзв'язку за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»:

- «Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту»;
- «Фахівець з криптографічного захисту інформації»;
- «Фахівець з технічного захисту інформації»;
- «Уповноважений з авторизації безпеки інформації»;
- «Аналітик з оцінки вразливостей»;
- «Фахівець з тестування систем захисту інформації»;
- «Кібероператор».

3) Закону України «Про вищу освіту» від 01.07.2014 р. № 1556-VII зі змінами та доповненнями.
4) Закону України "Про освіту" – https://zakon.rada.gov.ua/laws/show/2145-19#Text.
5) Національного класифікатору України: "Класифікатор професій" ДК 003:2010.
6) Національної рамки кваліфікацій (Додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341 (в редакції постанови Кабінету МіністрівУкраїнивід25 червня 2020 р. №519)) – https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text.
7) Переліку галузей знань і спеціальностей – https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#Text
8) Стандартів і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG 2015). https://www.britishcouncil.org.ua/sites/default/files/standards-and-guidelines_for_qa_in_the_ehea_2015.pdf.

Рецензії-відгуки зовнішніх стейкголдерів):
1. Мичуда Л., заступник директора з науково-педагогічної роботи Інституту комп'ютерних технологій Національного університету «Львівська Політехніка»
2. Халімов Г.З., завідувач кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
3. Кравченко В., виконавчий директор АТ «ІІТ»
4. Ісірова К., Senior Security & Compliance Auditor, 1GLOBAL
5. Вілігура В., технічний директор ТОВ «ДЕВБРАЗЕР»

1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем» зі спеціальності F5 – Кібербезпека та захист інформації

1–Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет імені В. Н. Каразіна, Навчально-науковий інститут комп'ютерних наук та штучного інтелекту, кафедра кібербезпеки інформаційних систем, мереж і технологій
Офіційна назва програми	Кібербезпека та захист інформації / Cyber Security and Information Protection
Ступінь вищої освіти	Другий (магістерський) рівень
Кваліфікація, що присвоюється	Магістр кібербезпеки та захисту інформації, безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання: денна форма – 1 роки 4 місяці.
Наявність акредитації	Акредитована, Сертифікат про акредитацію спеціальності, виданий Міністерством освіти і науки України «НД № 2189569 від 18.09.2017»
Передумови	Для здобуття освітнього рівня магістра можуть вступати особи, що здобули освітній рівень бакалавра. Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти.
Мова викладання	Українська, англійська
Термін дії освітньої програми	до 2027 року
Інтернет-адреса постійного розміщення опису освітньої програми	https://csai.karazin.ua/repository/admission-repository/#bachelor
2 - Мета освітньої програми	
Мета програми	Узагальнює зміст навчання, встановлює вимоги до змісту та рівня освітньої та професійної підготовки фахівця другого (магістерського) рівня вищої освіти за спеціальністю F5 – Кібербезпека та захист інформації.
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності)**)**	F – Інформаційні технології; F5 – Кібербезпека та захист інформації. **Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних

	систем і технологій, інших бізнес-операційних процесів на об’єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у

	кіберпросторі. **Інструменти та обладнання.** Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна програма. Акцент програми зроблений на підготовці фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.
Основний фокус освітньої програми та спеціалізації	Загальна освіта другого (магістерського) рівня в галузі знань F «Інформаційні технології», за спеціальністю F5 – Кібербезпека та захист інформації. **Ключові слова:** інформаційні технології, безпека інформаційно-комунікаційних систем і технологій, інформаційна безпека, кібербезпека, політики інформаційної безпеки, захист інформації.
Особливості програми	Освітньо-професійна програма передбачає підготовку фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки, ґрунтуючись на сучасних технологіях, математичних методах проектування та оптимізації інформаційно-комунікаційних систем, методах оцінювання захищеності інформації в інформаційно-комунікаційних системах, методах та засобах криптографічного захисту інформації, законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності.
4 – Придатність випускників до працевлаштуваннята подальшого навчання	
Придатність до працевлаштування	Об'єкти професійної діяльності випускників: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або

	кібербезпекою об’єктів, що підлягають захисту. Можливість обіймати посади відповідно до Державного класифікатору професій ДК 003:2010: інженер з безпеки інформаційних і телекомунікаційних систем, молодший науковий співробітник, науковий співробітник науково-дослідного підрозділу (установи)
Подальше навчання	Можливість навчатися за програмою третього (освітньо-наукового) рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Вивчення компонент освітньої (професійної) програми передбачається у формі проведення навчальних занять, організації самостійної роботи здобувачів вищої освіти, практичної підготовки та контрольних заходів. Навчальні заняття проводиться у виді: лекційних курсів, зокрема мультимедійних, семінарських, практичних, індивідуальних, лабораторних занять, консультацій із науково-педагогічними співробітниками тощо.
Оцінювання	За 100 бальною та 4 (2)-ох рівневою національною шкалою. Форми семестрового оцінювання: поточний контроль, екзамени, заліки. Підсумкова атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	**КЗ 1**. Готовність використати сучасні досягнення науки і передових технологій. (визначено університетом) **КЗ 2**.Здатність застосовувати знання у практичних ситуаціях; знання та розуміння предметної області та розуміння професії. **КЗ 3**. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності), здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **КЗ 4**. Здатність проводити дослідження на відповідному рівні. Вміння виявляти, ставити та вирішувати науково-технічні завдання за професійним спрямуванням; здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі інформаційно-комунікаційних технологій.

	КЗ 5. Здатність до абстрактного мислення, аналізу та синтезу. Здатність до пошуку, оброблення та аналізу інформації; готовність представляти результати досліджень у вигляді звітів і публікацій на державній та одній з іноземних мов; здатність користуватися нормативною та законодавчою базою в сфері інтелектуальної власності. **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. (визначено університетом) **КЗ 7**. Розуміти глобальні проблеми сучасності; володіти здатністю 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. (визначено університетом) **КЗ 8.** Здатність оцінювати та забезпечувати якість виконуваних робіт. Здатність до викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційно-комунікаційних технологій; здатність розробляти методичні матеріали, що використовуються в навчальному процесі. **КЗ 9.** Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. (визначено університетом)
Фахові компетентності	**КФ 1**. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, атакож технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. Здатність розуміти і аналізувати напрями розвитку розподілених інформаційно-комунікаційних систем і мереж, загальної теорії побудови математичних моделей і їх реалізації,теорії і практики керівництва проектами зі створення захищених розподілених інформаційних ресурсів.

	КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. Здатність виконувати роботи з проектування складних комплексів засобів кібербезпеки і управління безпекою інформаційних і комунікаційних систем відповідно до сфери їх застосування. **КФ 3**. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. Здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення кібербезпеки. **КФ 4**. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. **КФ 5.** Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ 6.** Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ 7.** Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. **КФ 8**. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також

	здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ 9**. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. **КФ 10**. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. **КФ 11**. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність. (визначено університетом) **КФ 12**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. (визначено університетом)
7 – Програмні результати навчання	
Програмні результати навчання	**ПРН 1.** Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **ПРН 2.** Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. **ПРН3**. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. **ПРН 4**. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. **ПРН 5**. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому

	числі на міжгалузевому та міждисциплінарному рівні, зокрема наоснові розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. **ПРН 6**. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. **ПРН 7**. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **ПРН 8.** Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. **ПРН 9.** Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. **ПРН 10**. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. **ПРН 11**. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/абокібербезпеки організації. **ПРН 12**. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснюватипроцедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. **ПРН 13**. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. **ПРН 14.** Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій,

	бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому. **ПРН 15.** Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. **ПРН 16.** Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. **ПРН 17.** Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. **ПРН 18.** Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. **ПРН 19.** Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. **ПРН 20.** Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. **ПРН 21.** Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. **ПРН 22.** Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. **ПРН 23.** Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури

	та іншої доступної інформації. **ПРН 24.** Використовувати математичні методи оптимізації з метою одержання найкращих характеристик функціонування засобів та систем. (визначено університетом)
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Викладання фахових дисциплін забезпечує професорсько-викладацький склад кафедри, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов: 4 доктори та 9 кандидатів наук (PhD), які є штатними співробітниками університету.
Специфічні характеристики матеріально-технічного забезпечення	Для навчання використаються 8 комп'ютерних класів та навчальна лабораторія факультету комп'ютерних наук, навчально-науковий центр сертифікації ключів ЕЦП, виробнича та переддипломна практика здійснюється на базі навчально-наукового інституту комп'ютерних наук та штучного інтелекту та 3-ох науково-виробничих підприємствах.
Специфічні характеристики інформаційного та навчально-методичного забезпечення	Використається навчальний фонд бібліотеки Харківського національного університету імені В. Н. Каразіна, підручники та навчальні посібники розробки кафедри та провідних світових університетів. Забезпеченість бібліотеки Харківського національного університету імені В. Н. Каразіна вітчизняними та закордонними фаховими періодичними виданнями відповідного профілю, в тому числі в електронному вигляді. Наявність доступу до баз даних провідних закордонних наукових видань, міжнародних наукометричних баз через власну локальну мережу. Вхід до мережі можливий як зі стаціонарних комп'ютерів, так і шляхом використання технології WiFi з приміщень університету. Наявність електронного ресурсу університету, який містить навчально-методичні матеріали з дисциплін навчального плану.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх угод про академічну мобільність для навчання та проведення досліджень між Харківським національним університетом імені В. Н. Каразіна та закладами вищої освіти України. Студенти мають можливість здійснювати перехід до інших ВНЗ та/або спеціальностей (згідно до положень Закону про освіту та відповідних рішень ВНЗ) з урахуванням накопиченого обсягу кредитів навчання.

Міжнародна кредитна мобільність	На основі двосторонніх угод між Харківським національним університетом імені В. Н. Каразіна та навчальними закладами країн-партнерів. Студенти мають можливість здійснювати навчання в ВНЗ інших країн у відповідності з домовленостями університетів в рамках міжнародних програм співробітництва та академічної мобільності.
Навчання іноземних здобувачів вищої освіти	На основі угод між Харківським національним університетом імені В. Н. Каразіна та закладами вищої освіти іноземних країн. Можливим є навчання іноземних студентів за даною програмою у відповідності з домовленостями університетів в рамках міжнародних програм співробітництва та академічної мобільності.

2. Перелік компонент освітньо-професійної /наукової програми та їх логічна послідовність

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційнаробота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Глобальні проблеми сучасності	3	Залік
ОК 2.	Криптографічні методи в кібербезпеці	5	Екзамен
ОК 3.	Теорія розподілених інформаційних ресурсів, захист баз даних	6	Екзамен
ОК 4.	Курсова робота - Методи та засоби забезпечення безпеки в системах обробки та зберігання даних	3	Залік
ОК 5.	Методологія і організація наукових досліджень	3	Залік
ОК 6.	Стандартизація в сфері кібербезпеки	3	Екзамен
ОК 7.	Безпека бездротових мереж	7	Екзамен
ОК 8.	Науково-дослідна практика	10	Залік
ОК 9.	Переддипломна практика	10	Залік
ОК 10.	Виконання кваліфікаційної роботи магістра	10	Екзамен
Загальний обсяг обов'язкових дисциплін		60	
Вибіркові компоненти ОП*			
Загальної підготовки			
ВБ 2.4.	Вибіркова 1	3	Залік
Фахової підготовки			
ВБ 1.1.	Вибіркова 2	3	Залік
ВБ 1.2.	Вибіркова 3	6	Залік
ВБ 1.3.	Вибіркова 4	6	Залік
ВБ 2.1.	Вибіркова 5	6	Залік
ВБ 2.2.	Вибіркова 6	3	Залік
ВБ 2.3.	Вибіркова 7	3	Залік
Загальний обсяг вибіркових дисциплін		30	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ		90	

2.2 Структурно-логічна схема ОП

Рік навчання	**1-й**		**2-й**	
Семестр	1	2	3	
ОК 1.				
ОК 2.				
ОК 3.				
ОК 4.				
ОК 5.				
ОК 6.				
ОК 7.				
ОК 8.				
ОК 9.				
ОК 10.				
ВБ 1.1.				
ВБ 1.2.				
ВБ 1.3.				
ВБ 2.1.				
ВБ 2.2.				
ВБ 2.3.				
ВБ 2.4.				

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищоїосвіти	Атестація здійснюється екзаменаційною комісією відповідно до вимог цього стандарту після виконання студентом навчального плану. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даною програмою Термін проведення атестації визначається навчальним планом таграфіком освітнього процесу. Атестація здійснюється у формі публічного захисту кваліфікаційної магістерської роботи. До атестації допускаються студенти, які виконали всі вимоги програми.

Вимоги до кваліфікаційної роботи/проекту	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозиторії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КЗ 9	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
ОК 1.	+		+			+	+	+													
ОК 2.	+			+				+		+	+	+							+	+	
ОК 3.	+	+	+	+	+	+		+	+	+	+		+		+				+		+
ОК 4.	+			+	+			+	+					+	+				+	+	
ОК 5.												+			+	+					+
ОК 6.	+	+						+					+			+	+	+	+		+
ОК 7.	+	+		+	+			+	+	+	+		+	+	+				+	+	
ОК 8.	+	+	+	+	+					+	+	+		+		+	+			+	
ОК 9.	+	+	+	+	+					+	+	+		+		+	+			+	
ОК 10.	+	+	+	+	+			+	+	+	+	+		+		+	+			+	

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10
ПРН 1	+		+	+		+	+	+	+	+
ПРН 2		+		+			+	+	+	+
ПРН 3		+		+			+	+	+	+
ПРН 4		+		+			+	+	+	+
ПРН 5		+	+	+	+		+	+	+	+
ПРН 6					+		+	+	+	+
ПРН 7			+	+		+	+	+	+	+
ПРН 8					+	+	+	+	+	+
ПРН 9		+		+			+	+	+	+
ПРН 10				+			+	+	+	+
ПРН 11				+					+	+
ПРН 12			+					+	+	
ПРН 13					+	+				
ПРН 14										+
ПРН 15			+	+		+				
ПРН 16			+		+				+	+
ПРН 17			+					+	+	
ПРН 18			+	+				+	+	+
ПРН 19								+	+	+
ПРН 20						+		+	+	+
ПРН 21		+						+	+	+
ПРН 22	+			+				+	+	+
ПРН 23	+				+			+	+	+
ПРН 24		+		+			+	+	+	+