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

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

Перший (бакалаврський) рівень вищої освіти

Галузь знань F«Інформаційні технології»

Спеціальність F5-Кібербезпека та захист інформації

ЗАТВЕРДЖЕНО
Вченою радою університету
протокол від 17.03.2025 № 8

Введено в дію з _____
наказ від 18.03.2025 № 0114-1/142

Проректор з науково-педагогічної роботи
Олександр ГОЛОВКО

ХАРКІВ–2025

ЛИСТ ПОГОДЖЕННЯ ОПП

Науково-методичною радою університету
протокол від 14.03.2025 № 7
Голова НМР

_____ **Олександр ГОЛОВКО**

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**

ПРЕАМБУЛА

Розроблено робочою групою у складі:

Прізвище, ім'я, по батькові	Найменування посади	Науковий ступінь, вчене звання
Керівник робочої групи – гарант ОП		
Лисицька Ірина Вікторівна	Професор кафедри кібербезпеки інформаційних систем, мереж і технологій	Доктор технічних наук, професор
Члени робочої групи		
Єсін Віталій Іванович	Професор кафедри кібербезпеки інформаційних систем, мереж і технологій	Доктор технічних наук, професор
Єсіна Марина Віталіївна	Доцент кафедри кібербезпеки інформаційних систем, мереж і технологій	Кандидат технічних наук, доцент
Сватовський Ігор Іванович	Доцент кафедри кібербезпеки інформаційних систем, мереж і технологій	Кандидат технічних наук, с.н.с.
Колованова Євгенія Павлівна	Доцент кафедри кібербезпеки інформаційних систем, мереж і технологій	Кандидат технічних наук

До проектування освітньої програми долучені:
Представники здобувачів вищої освіти: Барбашин Ілля Станіславович, студент 4 року навчання
Представники роботодавців: Горбенко Юрій Іванович, Перший заступник головного конструктора ПАТ "Інститут інформаційних технологій", к.т.н.

При розробці проекту Програми враховані вимоги:
1) Стандарту вищої освіти спеціальності 125 – «Кібербезпека» для першого (бакалаврського) рівня освіти, що погоджено рішенням Національного агентства із забезпечення якості вищої освіти від 22 травня 2017 р. № 72 та затверджено наказом МОН України № 1074 від 04.10.2018 р.
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 наукову і науково-технічну діяльність» від 26.11.2015 р. №848-VIII зі змінами та доповненнями.
5) Національної рамки кваліфікацій (Додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341 (в редакції постанови Кабінету МіністрівУкраїнивід25 червня 2020 р. №519)).

6) Перелік галузей знань і спеціальностей – https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#Text
7) Стандарти 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« Кібербезпека»
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 / Cyber Security
Ступінь вищої освіти	Перший (бакалаврський) рівень
Кваліфікація, що присвоюється	Бакалавр з кібербезпеки та захисту інформації
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання: денна та заочна форма – 3 роки 10 місяців.
Наявність акредитації	Акредитована, Сертифікат про акредитацію видало Міністерство освіти і науки України, Україна, НД № 2189535 від 18.09.2017
Передумови	Для здобуття освітнього ступеня бакалавра можуть вступати особи, які здобули повну загальну середню освіту, а також особи, які здобули освітній ступінь молодшого бакалавра або освітньо-професійний ступінь фахового молодшого бакалавра
Мова викладання	Українська /Англійська
Термін дії освітньої програми	до 2029 року
Інтернет - адреса постійного розміщення опису освітньої програми	https://csai.karazin.ua/repository/admission-repository/#bachelor
2 – Мета освітньої програми	
Мета програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної безпеки для розв'язання практичних завдань інформаційної безпеки та профілактики кіберзагроз
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))	F – Інформаційні технології F5 – Кібербезпека та захист інформації 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. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології

	інформаційної та/або кібербезпеки. Теоретичний зміст предметної області Знання – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна програма. Акцент програми зроблений на підготовці фахівців, здатних розв'язувати теоретичні та практичні задачі в сфері кібербезпеки та захисту інформації в інформаційно-комунікаційних системах.
Основний фокус освітньої програми та спеціалізації	Об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікації, 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
Особливості програми	Підготовка фахівців, здатних забезпечувати безпеку інформаційно-комунікаційних систем і технологій, криптографічний захист інформації
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Можливість обіймати первинні посади відповідно до Державного класифікатору професій ДК 003:2010: робота в галузі «Інформаційна безпека», фахівець здатний виконувати зазначену професійну роботу - фахівець із організації інформаційної

	безпеки, і може займати первинні посади, що передбачені штатним розписом за професійним спрямуванням, такі як: інспектор, спеціаліст державної служби, фахівець підрозділу технічного захисту інформації підприємства.
Подальше навчання	Можливість продовжити навчання за освітньою програмою ступеня магістра.
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 тощо.
Оцінювання	Усні, письмові екзамени та заліки, комп'ютерне і письмове тестування, презентації, захист курсових робіт, матеріалів практики, атестація
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	**КЗ 1**.Здатність застосовувати знання у практичних ситуаціях. **КЗ 2**.Знаннятарозумінняпредметноїобластітарозумінняпрофесії. **КЗ 3**.Здатність професійно спілкуватися державною та іноземною мовами як усно, такі письмово. **КЗ 4**.Вміннявиявляти,ставититавирішуватипроблемизапрофесійнимспрямуванням. **КЗ 5**.Здатність до пошуку, оброблення та аналізу інформації. **КЗ 6**. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні; **КЗ 7**. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку Предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя **КЗ 8**. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності

Фахові компетентності	**КФ 1**. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги ,практики і стандарти з метою здійсненняпрофесійноїдіяльностівгалузіінформаційноїта/абокібербезпеки. **КФ 2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/ або кібербезпеки. **КФ 3**. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **КФ 4**. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. **КФ 5**. Здатністьзабезпечуватизахистінформації,що обробляєтьсявінформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації становленої політики інформаційної та/або кібербезпеки. **КФ 6**. Здатністьвідновлюватиштатнефункціонуванняінформаційних,інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та від мов різних класів та походження. **КФ 7**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації(комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) **КФ 8**. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **КФ 9**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. **КФ 10**. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. **КФ 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних(автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **КФ 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізую чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

7–Програмні результати навчання	
Програмні результати навчання	**ПРН 1** застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; **ПРН 2** організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; **ПРН 3** використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; **ПРН 4** аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; **ПРН 5** адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; **ПРН 6** критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; **ПРН 7** діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; **ПРН 8** готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки; **ПРН 9** впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; **ПРН 10** виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; **ПРН 11** виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; **ПРН 12** розробляти моделі загроз та порушника; **ПРН 13** аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; **ПРН 14** вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційнихсистемахпрограмно-апаратнимизасобами та давати оцінку результативності якості прийнятих рішень;

	ПРН 15 використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій **ПРН 16** реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації(підприємства) відповідно до вимог нормативно-правових документів; **ПРН 17** забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; **ПРН 18** використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; **ПРН 19** застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; **ПРН 20** забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; **ПРН 21** вирішувати задачі забезпечення та супроводу (вт. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих)системах; **ПРН 22** вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та\або кібербезпеки; **ПРН 23** реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних(автоматизованих) системах; **ПРН 24** вирішувати задачі управління доступом до інформаційних ресурсів та процесів інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); **ПРН 25** забезпечувати введення підзвітності системи управління доступом до електронних

	інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; **ПРН 26** впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; **ПРН 27** вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих)системах; **ПРН 28** аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних(автоматизованих) системах в ході проведення випробувань згідно встановлено політики інформаційної та\або кібербезпеки; **ПРН 29** здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; **ПРН 30** здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; **ПРН 31** застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; **ПРН 32** вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; **ПРН 33** вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; **ПРН 34** приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; **ПРН 35** вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або

	кібербезпеки; **ПРН 36** виявляти небезпечні сигнали технічних засобів; **ПРН 37** вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; **ПРН 38** інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; **ПРН 39** проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; **ПРН 40** інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; **ПРН 41** забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; **ПРН 42** впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; **ПРН 43** застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та /або кібербезпеки для розслідування інцидентів; **ПРН 44** вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; **ПРН 45** застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; **ПРН 46** здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; **ПРН 47** вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

	ПРН 48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компонентикриптографічногозахистудлязабезпеченнянеобхідногорівня захищеності інформації в інформаційно-телекомунікаційних системах; **ПРН49** забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; **ПРН50** забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); **ПРН51** підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; **ПРН52** використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; **ПРН53** вирішувати задачі аналізу програмного коду на наявність можливих загроз. **ПРН 54** усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Викладання фахових дисциплін забезпечує професорсько-викладацький склад кафедри: 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 ФКН та 6 науково-виробничих підприємств, з якими укладено відповідні договори.
Специфічні характеристики інформаційного та навчально-методичного забезпечення	Використається навчальний фонд бібліотеки ХНУ, ПЗ дистанційних форм навчання, підручники та навчальні посібники розробки кафедри та провідних світових університетів.
9 – Академічна мобільність	
Національна кредитна мобільність	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	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	Можливим є навчання іноземних студентів за даною програмою з використанням державної, англійської або інших мов викладання.

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

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК1.	Іноземна мова за фахом	12	Екзамен
ОК2.	Історія України: цивілізаційний вимір	3	Екзамен
ОК3.	Дискретна математика	8	Екзамен
ОК4.	Фізика	8	Екзамен
ОК5.	Вища математика	17	Екзамен
ОК6.	Філософія	3	Екзамен
ОК7.	Теорія ймовірності	5	Екзамен
ОК8.	Вступ до фаху	5	Екзамен
ОК9.	Алгоритмізація та програмування	12	Екзамен
ОК10.	Об'єктно-орієнтоване програмування	10	Екзамен
ОК11.	Безпека життєдіяльності та основи охорони праці	4	Залік
ОК12.	Математичні методи та технології тестування і верифікації програмного забезпечення	4	Екзамен
ОК13.	Крос-платформне програмування	4	Залік
ОК14.	Теорія чисел, теорія груп, полів, кілець	7	Екзамен
ОК15.	Операційні системи	4	Залік
ОК16.	Теорія інформації і кодування	4	Екзамен
ОК17.	Системи технічного захисту інформації	4	Екзамен
ОК18.	Прикладна криптологія	8	Екзамен
ОК19.	Комп'ютерні мережі	4	Залік
ОК20.	Основи теорії передачі інформації	4	Екзамен
ОК21.	Основи управління критичними цифровими системами	4	Екзамен
ОК22.	Захист інформації в інформаційно-комунікаційних системах	13	Екзамен
ОК23.	Стеганографія	4	Екзамен
ОК24.	Компоненти складних комп'ютерних мереж	5	Екзамен

ОК25.	Комплексні системи захисту інформації: проектування, впровадження, супровід	8	Екзамен
ОК26.	Управління інформаційною безпекою	3	Екзамен
ОК27.	Виробнича практика	5	Залік
ОК28.	Преддипломна практика	5	Залік
ОК29.	Підготовка та захист кваліфікаційної роботи бакалавра	3	Екзамен
Загальний обсяг обов'язкових дисциплін		180	
Вибіркові компоненти ОП*			
Загальної підготовки			
МФ1	Теоретична підготовка БЗВП/ Домедична допомога та ментальне здоров'я*	3	Залік
МФ2	МФ дисципліна за вибором 2	3	Залік
МФ3	МФ дисципліна за вибором 3	3	Залік
МФ4	МФ дисципліна за вибором 4	3	Залік
Фахової підготовки			
ВБ2.1.	Інформаційні технології	3	Залік
ВБ3.1.	Теорія алгоритмів	3	Залік
ВБ3.2.	Електротехніка та електроніка	3	Залік
ВБ3.3.	Комп'ютерна графіка	3	Залік
ВБ4.1.	Основи теорії кіл, сигнали та процеси в електроніці	3	Залік
ВБ5.1.	Метрологія та вимірювання, комп'ютерна схемотехніка	6	Залік
ВБ5.2.	Мікропроцесори та їх застосування	3	Залік
ВБ6.1.	Курсова робота – Методи та засоби забезпечення криптографічного захисту систем обробки та зберігання даних.	3	Залік
ВБ7.1.	Технології блокчейн	3	Залік
ВБ7.2.	Курсова робота - Проєктування, дослідження та супровід систем захисту інформації	3	Залік
ВБ7.3.	Спеціалізовані мови програмування та проектування електроних елементів і систем	6	Залік
ВБ8.1.	Командна робота	3	Залік
ВБ8.2.	Спеціальні методи обробки даних в телекомунікаційних системах	3	Залік
ВБ8.3.	Курсова робота – Методи та засоби захисту інформації в мережах інформаційно-комунікаційних систем	3	Залік
Загальний обсяг вибіркових дисциплін		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

* - Дисципліна є обов'язковою для її включення до індивідуальних навчальних планів здобувачів вищої освіти, для яких це передбачено законодавством.

2.2 Структурно-логічна схема ОП

Рік навчання	1-й		2-й		3-й		4-й	
Семестр	1	2	3	4	5	6	7	8
ОК1.								
ОК2.								
ОК3.								
ОК4.								
ОК5.								
ОК6.								
ОК7.								
ОК8.								
ОК9.								
ОК10.								
ОК11.								
ОК12.								
ОК13.								
ОК14.								
ОК15.								
ОК16.								
ОК17.								
ОК18.								
ОК19.								
ОК20.								
ОК21.								
ОК22.								
ОК23.								
ОК24.								
ОК25.								
ОК26.								
ОК27.								
ОК28.								
ОК29.								
МФ1								
МФ2								
МФ3								
МФ4								
ВБ2.1.								
ВБ3.1.								
ВБ3.2.								
ВБ3.3.								
ВБ4.1.								
ВБ5.1.								
ВБ5.2.								
ВБ6.1.								
ВБ7.1.								
ВБ7.2.								
ВБ7.3.								
ВБ8.1.								
ВБ8.2.								
ВБ8.3.								

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація осіб, які здобувають ступінь бакалавра з кібербезпеки, проводиться у формі ЄДКІ та захисту кваліфікаційної роботи бакалавра. На ЄДКІ виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за стандартом вищої освіти за спеціальністю 125 Кібербезпека та захист інформації. Захист кваліфікаційної роботи бакалавра проводиться та оцінюється атестаційною комісією, до складу якої можуть входити представники роботодавців та їх об'єднань, відповідно до положення про атестаційну комісію, затвердженого вченою радою Харківського національного університету імені В.Н. Каразіна. Термін проведення атестації визначається навчальним планом та графіком освітнього процесу. До атестації допускаються студенти, які виконали всі вимоги програми підготовки. Атестація завершується видачею документу державного зразка про присудження здобувачу вищої освіти ступеня бакалавра із присвоєнням кваліфікації бакалавр кібербезпеки та захисту інформації, кібербезпека. Атестація здійснюється відкрито і публічно.
Вимоги до кваліфікаційної роботи бакалавра	Кваліфікаційна робота - це самостійно виконана проектно-дослідна робота студента, яка передбачає авторське бачення задачі, можливості її дослідження та розв’язання. Робота свідчить про вміння автора проводити емпіричне дослідження, розробляти відповідні системи (засоби), обґрунтовувати проектні рішення, опрацьовувати та аналізувати отримані результати, формулювати аргументовані висновки. Виконання випускних кваліфікаційних робіт має сприяти: - систематизації, закріпленню й розширенню теоретичних і практичних знань зі спеціальності та застосуванню цих знань для вирішення конкретних завдань; - розвитку навичок здійснення самостійної роботи та оволодіння методикою вирішення питань і завдань, поставлених у випускній роботі; - оцінюванню рівня володіння певною сукупністю професійних компетентностей, необхідних для майбутньої професійної діяльності; - дотримання принципів і норм академічної доброчесності та недопущення плагіату. Зміст кваліфікаційної роботи визначається її темою. Деталізація вимог до кваліфікаційної роботи регламентується внутрішніми документами і положеннями Харківського національного університету імені В.Н. Каразіна. Роботи розміщуються в репозитарії університету.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК1	ФК10	ФК11	ФК12
ОК1.			+		+		+	+													
ОК2.	+		+																		
ОК3.			+			+	+	+													
ОК4.	+					+	+	+													
ОК5.	+									+											
ОК6.	+									+											
ОК7.									+	+											
ОК8.	+			+	+					+											
ОК9.																					
ОК10.	+					+	+		+												
ОК11.		+		+				+	+		+								+		
ОК12.	+																				
ОК13.					+					+											
ОК14.										+											
ОК15.	+				+																
ОК16.	+																				
ОК17.				+																	
ОК18.	+									+											
ОК19.										+											
ОК20.	+	+		+					+			+							+	+	+
ОК21.										+											
ОК22.	+				+																
ОК23.		+		+							+										
ОК24.		+		+														+			
ОК25.		+		+						+											
ОК26.	+	+		+																	
ОК27.																					
ОК28.	+				+		+														
ОК29.										+											

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29
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	+								+														+						
ПРН35															+						+								
ПРН36														+									+			+			
ПРН37										+								+											
ПРН38						+	+																	+					
ПРН39												+				+				+									
ПРН40						+	+			+	+																		
ПРН41																												+	
ПРН42			+												+				+						+				
ПРН43	+							+			+																		
ПРН44				+											+		+						+						
ПРН45																			+										
ПРН46																					+						+		
ПРН47												+					+												
ПРН48									+																				
ПРН49													+			+													+
ПРН50																								+					
ПРН51																				+									
ПРН52											+		+					+											
ПРН53																+			+										
ПРН54	+					+	+					+																+	