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

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

Перший (бакалаврський) рівень вищої освіти

Галузь знань 12«Інформаційні технології»

Спеціальність 125-Кібербезпека та захист інформації

ЗАТВЕРДЖЕНО
Вченою радою університету
протокол від _____ № _____

Введено в дію з _____
наказ від _____ № _____

Проректор з науково-педагогічної роботи
Олександр ГОЛОВКО
_____

ХАРКІВ–2024

ЛИСТ ПОГОДЖЕННЯ ОПП

Науково-методичною радою університету
протокол від _____ № _____
Голова НМР

_____ **Олександр ГОЛОВКО**

Вчена рада факультету комп'ютерних наук
протокол від _____ № _____
Заступник Голови Вченої ради факультету

_____ **Олена ТОЛСТОЛУЗЬКА**

Методична комісія факультету комп'ютерних наук
протокол від _____ № _____
Голова методичної комісії факультету

_____ **Лариса ВАСИЛЬЄВА**

Кафедра безпеки інформаційних систем і технологій
протокол від _____ № _____
В.о.завідувача кафедри

_____**Ольга МЕЛКОЗЬОРОВА**

ПЕРЕДМОВА

При розробці проекту ОПП враховані вимоги:

- Освітнього стандарту спеціальності 125 – «Кібербезпека та захист інформації» 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.
- Закону України «Про вищу освіту» від 01.07.2014 р. № 1556-VII зі змінами та доповненнями.
- Закону України «Про наукову і науково-технічну діяльність» від 26.11.2015 р. №848-VIII зі змінами та доповненнями.
- Національної рамки кваліфікацій (Додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341 (в редакції постанови Кабінету МіністрівУкраїнивід25 червня 2020 р. №519)).

Розроблено робочою групою у складі:

Прізвище, ім'я, по батькові	**Найменування посади**	**Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно**
Керівник робочої групи		
Сватовський Ігор Іванович	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук, доцент
Члени робочої групи		
Єсін Віталій Іванович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.06 - Інформаційні технології), доцент за кафедрою спец. дисциплін
Кузнецов Олександр Олександрович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.21 – системи захисту інформації), професор за спеціальністю 20.02.12 - військова кібернетика, системи управління та зв'язок
Єсіна Марина Віталіївна	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук (05.13.21 – системи захисту інформації)
Колованова Євгенія Павлівна	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук (05.13.21 – системи захисту інформації)

1. Профіль освітньої програми« Кібербезпека»
зі спеціальності 125 – Кібербезпека та захист інформації

1–Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій
Ступінь вищої освіти та назва освітньої кваліфікації	Перший(бакалаврський)рівень, 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.
Офіційна назва програми	Кібербезпека
Наявність акредитації	2017 рік
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл,EQF-LLL– 6рівень
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
Термін дії освітньої програми	з 2024 до 2028 року
Інтернет - адреса постійного розміщення опису освітньої програми	http://www-csd.univer.kharkov.ua/navchannya/standarti-osviti/osviti-programi/
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))	12 – Інформаційні технології 125 – Кібербезпека та захист інформації
Орієнтація освітньої програми	Фундаментально-професійна.
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 .
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,ставититавирішуватипроблеми запрофесійнимспрямуванням. **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,науковіцінностіідосягненнясуспільстванаосновірозумінняісторії та закономірностей розвитку gПредметної 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

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,щообробляєтьсявінформаційно-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 наосновівпровадженоїсистемиуправлінняінформаційноюта/абокібербезпекою. **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 дестабілізуючинники 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 забезпечуєпрофесорсько-викладацькийскладкафедри:6докторів та8кандидатівнаук,якієштатнимиспівробітника миуніверситету.
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

Кодн/д	Компоненти освітньої програми(навчальнідисципліни,курсові проекти (роботи), практики, кваліфікаційнаробота)	Кількість кредитів	Формапідсумковогоконтролю
1	2	3	4
Обов'язковікомпонентиОП			
ОК1.	Іноземнамова	6	Іспит/залік
ОК2.	Іноземнамовазафахом	3	Залік
ОК3.	ІсторіяУкраїни	3	Іспит
ОК4.	Філософія	3	Іспит
ОК5.	Вищаматематика,теоріяймовірностей	24	Іспит
ОК6.	Дискретнаматематика	7	Іспит/залік
ОК7.	Інформаційнітехнології	7	Залік
ОК8.	Фізика	7	Іспит/залік
ОК9.	Безпека життєдіяльності та основи охоронипраці	3	Залік
ОК10.	Вступдофаху	3	Іспит
ОК11.	Електротехнікатаелектроніка	5	Іспит
ОК12.	Комп'ютернімережі	4	Іспит
ОК13.	Основитеоріїпередачіінформації	4	Іспит
ОК14.	Комп'ютернаграфіка	3	Залік
ОК15.	Метрологіятавимірювання,комп'ютернасхемотехніка(КР-1)	6	Іспит
ОК16.	Мікропроцесоритаїхзастосування	3	Іспит
ОК17.	Операційнісистеми	4	Залік
ОК18.	Оптоінформатика	3	Залік
ОК19.	Основиінформаційноїбезпекидержави	3	Залік
ОК20.	Основитеоріїкіл,сигналитапроцесивелектроніці		Іспит
ОК21.	Спеціалізовані мови програмування та проектування електронних елементів і систем	6	Іспит/залік
ОК22.	Стеганографія	6	Іспит
ОК23.	Теоріячисел,теоріягруп,полів,кілець	7	Іспит
ОК24.	Теоріяінформаціїікодування(КР-1)	5	Іспит
ОК25.	Теоріяавтоматичногоуправління	4	Іспит
ОК26.	Алгоритмізаціятапрограмування	10	Іспит
ОК27.	Крос-платформнепрограмування	3	Залік
ОК28.	Теоріяалгоритмів	3	Залік

ОК29.	Об’єктно-орієнтованепрограмування(КР-1)	10	Іспит/залік
ОК30.	Математичніметодитатехнологіїтестуванняіверифікаціїпрограмногозабезпечення(КР-1)	4	Іспит
ОК31.	Спеціальні методи обробки даних в телекомунікаційнихсистемах	6	Іспит
ОК32.	Виробничапрактика	5	Залік
ОК33.	Переддипломнапрактика	5	Залік
ОК34.	Підготовкабакалаврськоїроботи	2	ЗАХИСТ
ОК35.	Атестаційнийекзамен		Іспит
Загальнийобсягобов’язковихдисциплін		180	
ВибірковікомпонентиОП*			
Вибірковийблок1			
ВБ1.1.	Захист інформації в інформаційно-комунікаційнихсистемах(КР-2)	13	Іспит/залік
ВБ1.2.	Комплекснісистемизахистуінформації:проектування, впровадження, супровід (КР-1)	10	Іспит
ВБ1.3.	Компоненти складних комп’ютернихмереж	3	Іспит
ВБ1.4.	Технологіїблокчейн	3	Іспит
ВБ1.5.	Нормативно-правове забезпеченняінформаційноїбезпеки(КР-1)	3	Іспит
ВБ1.6.	Прикладнакриптологія(КР-1)	8	Іспит
ВБ1.7.	Системитехнічногозахистуінформації	4	Іспит
ВБ1.8.	Управлінняінформаційноюбезпекою	4	Іспит
Вибірковийблок2			
ВБ2.1.	Апаратнізасобизахистуінформаціїтазахистпрограмногозабезпечення(КР-2)	13	Іспит/залік
ВБ2.2.	Технологіїпроектуваннятасертифікації захищених ІС	10	Іспит
ВБ2.3.	Завадозахищені телекомунікаційні	3	Іспит
	технологіїтасистеми		
ВБ2.4.	Аналізтазастосуваннякриптовалют	3	Іспит
ВБ2.5.	СтандартизаціятасертифікаціявгалузіІБ (КР-1)	3	Іспит
ВБ2.6.	Криптосистемита криптопротоколи(КР-1)	8	Іспит
ВБ2.7.	Захиствідтехнічнихрозвідок	4	Іспит
ВБ2.8.	Системнийаналізпроцесівтасистемзахистуінформації	4	Іспит
Вибірковийблок3-міжфакультетськихдисциплін			
ВБ3.1.	МФдисципліназавибором1	3	Іспит/залік
ВБ3.2.	МФдисципліназавибором2	3	Іспит
ВБ3.3.	МФдисципліназавибором3	3	Іспит
ВБ3.4.	МФдисципліназавибором4	3	Іспит
Загальнийобсягвибірковихдисциплін		60	
ЗАГАЛЬНИЙОБСЯГОСВІТНЬОЇПРОГРАМИ		240	

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.								
ОК30.								
ОК31.								
ОК32.								
ОК33.								
ОК34.								
ОК35.								
ВБ1.1.								
ВБ1.2.								
ВБ1.3.								
ВБ1.4.								
ВБ1.5.								
ВБ1.6.								
ВБ1.7.								
ВБ1.8.								
ВБ2.1.								
ВБ2.2.								
ВБ2.3.								

ВБ2.4.								
ВБ2.5.								
ВБ2.6.								
ВБ2.7.								
ВБ2.8.								
ВБ3.1.								
ВБ3.2.								
ВБ3.3.								
ВБ3.4.								

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.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК1	ФК10	ФК11	ФК12
ОК1.	Іноземнамова			+																	
ОК2.	Іноземнамовазафахом	+		+																	
ОК3.	ІсторіяУкраїни			+			+	+													
ОК4.	Філософія	+					+	+													
ОК5.	Вища математика	+								+											
ОК6.	Теорія ймовірностей	+								+											
ОК7.	Дискретнаматематика								+	+											
ОК8.	Інформаційнітехнології	+			+	+				+											
ОК9.	Фізика																				
ОК10.	Безпекажиттєдіяльностітаосновиохоронипраці	+					+	+	+												
ОК11.	Вступдофаху		+		+				+		+								+		
ОК12.	Електротехніка таелектроніка	+																			
ОК13.	Комп'ютернімережі					+				+											
ОК14.	Основитеоріїпередачіінформації									+											
ОК15.	Комп’ютернаграфіка	+				+															
ОК16.	Метрологіятавимірювання, комп'ютернасхемотехніка	+																			
ОК17.	Мікропроцесоритаїхзастосування				+																
ОК18.	Операційнісистеми	+								+											
ОК19.	Оптоінформатика									+											
ОК20.	Основи інформаційноїбезпекидержави	+	+		+				+			+							+	+	+
ОК21.	Основи теорії кіл,сигналитапроцесивЕл.									+											
ОК22.	Спеціалізованімови програмування тапроектуванняЕЕС	+				+															
ОК23.	Стеганографія		+		+						+										
ОК24.	Теоріячисел,теоріягруп,полів,кілець		+		+													+			
ОК25.	Теорія інформації ікодування		+		+					+											
ОК26.	Теоріяавтоматичногоуправління	+	+		+																
ОК27.	Алгоритмізація тапрограмування																				
ОК28.	Крос-платформнепрограмування	+				+		+													
ОК29.	Теоріяалгоритмів									+											
ОК30.	Об’єктно-орієнтованепрограмування	+								+											
ОК31.	Математичніметодитатехнології ТіВПЗ					+				+	+	+	+								
ОК32.	Спеціальні методиобробкиданих					+				+	+		+				+				
ОК33.	Виробничапрактика	+			+					+	+						+	+		+	
ОК34.	Переддипломнапрактика				+	+					+					+		+			
ОК35.	Підготовка бакалаврської роботи				+						+						+	+			+

ВБ1.1.	ЗахистінформаціївІКС		+		+					+	+	+	+	+	+			+		+	
ВБ1.2.	Комплексні системи захисту інформації: проектування, впровадження, супровід	+	+		+					+	+	+	+	+	+						+
ВБ1.3.	Компоненти складнихкомп’ютернихмереж		+		+					+		+			+				+		
ВБ1.4.	Технологіїблокчейн		+		+					+	+	+						+			
ВБ1.5.	Нормативно-правовезабезпечення ІБ	+	+		+				+			+	+	+	+					+	
ВБ1.6.	Прикладнакриптологія		+		+						+	+		+	+			+	+	+	+
ВБ1.7.	Системи технічногозахистуінформації	+	+		+						+	+	+			+					+
ВБ1.8.	Управління інформаційноюбезпекою	+	+		+				+			+	+		+	+	+			+	+
ВБ2.1.	АпаратнізасобизахистуінформаціїтазахистПЗ		+		+					+	+	+	+		+					+	
ВБ2.2.	Технологіїпроектування тасертифікаціїзахищенихІС		+		+					+		+	+		+						+
ВБ2.3.	Завадозахищенітелекомунікаційні ТіС	+	+		+					+	+	+		+						+	
ВБ2.4.	Аналізтазастосуваннякриптовалют		+		+					+			+					+	+		
ВБ2.5.	СтандартизаціятасертифікаціявгалузіІБ		+		+					+		+		+	+	+		+			+
ВБ2.6.	Криптосистеми такриптопротоколи	+	+		+					+		+						+		+	
ВБ2.7.	Захист від технічнихрозвідок	+	+		+						+	+	+	+	+				+		
ВБ2.8.	Системний аналізпроцесівтасистемЗІ	+	+		+					+	+	+	+		+	+		+		+	+

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	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ВБ1	ВБ2	ВБ3	ВБ4	ВБ5	ВБ6	ВБ7	ВБ8
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						+	+					+																+				+									+		