

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 27.05.2024р № 10

Введено в дію з 2024/2025 н.р.

наказ від 29.05.2024р № 0114-1/178

Проректор з науково-педагогічної роботи

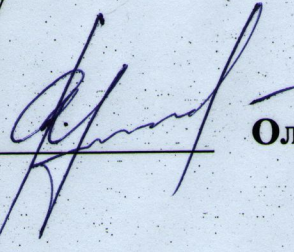
**Олександр ГОЛОВКО**



**ХАРКІВ-2024**

## ЛИСТ ПОГОДЖЕННЯ ОПШ

Науково-методичною радою університету  
протокол від 21.05.2024 № 8  
Голова НМР



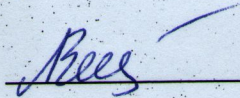
**Олександр ГОЛОВКО**

Вчена рада факультету комп'ютерних наук  
протокол від 14.05.2024 № 10  
Заступник Голови Вченої ради факультету



**Олена ТОЛСТОЛУЗЬКА**

Науково-методична комісія факультету комп'ютерних наук  
протокол від 26.04.2024 № 8  
Голова методичної комісії факультету



**Лариса ВАСИЛЬЄВА**

Кафедра безпеки інформаційних систем і технологій  
протокол від 07.02.2024 № 5  
В.о.завідувача кафедри



**Ольга МЕЛКОЗЬОРОВА**

## ПЕРЕДМОВА

### При розробці проекту ОПШ 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 Міністрів України від 25 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 – гарант програми	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), професор
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)
Горбенко Юрій Іванович	Перший заступник головного конструктора ПАТ “Інститут інформаційних технологій”, м. Харків	Кандидат технічних наук (05.13.21 – системи захисту інформації)
Пеллох Олександр Іванович	Студент 4 курсу	

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

<b>1–Загальна інформація</b>	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій
Офіційна назва програми	Кібербезпека / Cyber Security
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.
Наявність акредитації	Сертифікат про акредитацію спеціальності, виданий Міністерством освіти і науки України 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
Термін дії освітньої програми	з 2024 до 2028 року
Інтернет - адреса постійного розміщення опису освітньої програми	<a href="http://www-csd.univer.kharkov.ua/navchannya/standarti-osviti/osviti-programi/">http://www-csd.univer.kharkov.ua/navchannya/standarti-osviti/osviti-programi/</a>
<b>2– Мета освітньої програми</b>	
Мета програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної безпеки для розв'язання практичних завдань інформаційної безпеки та профілактики кіберзагроз
<b>3 – Характеристика освітньої програми</b>	
Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))	12 – Інформаційні технології 125 – Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітньо-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
<b>4 – Придатність випускників до працевлаштування та подальшого навчання</b>	
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.
<b>5 – Викладання та оцінювання</b>	
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 проводяться 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
<b>6 – Програмні компетентності</b>	
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	<p><b>КЗ 1.</b>Здатність застосовувати знання у практичних ситуаціях.</p> <p><b>КЗ 2.</b>Знання та розуміння предметної області та розуміння професії.</p> <p><b>КЗ 3.</b>Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p><b>КЗ 4.</b>Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p><b>КЗ 5.</b>Здатність до пошуку, оброблення та аналізу інформації.</p> <p><b>КЗ 6.</b> 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;</p> <p><b>КЗ 7.</b> 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</p>

## 7–Програмні результати навчання

Програмні результати  
навчання

**ПРН 1** застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

**ПРН 2** організувати 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 частоті 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-телекомунікаційних системах програмно-

Фахові компетентності

**КФ 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

**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.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

**КФ 6.** Здатність відновлювати штатне функціонування інформаційних, 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 дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

апаратними засобами 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 встановленої 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 рині 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;

	<p><b>ПРН 48</b> виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компонентикриптографічногозахистудлязабезпеченнянеобхідногорівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> <p><b>ПРН49</b> забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p> <p><b>ПРН50</b> забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);</p> <p><b>ПРН51</b> підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;</p> <p><b>ПРН52</b> використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;</p> <p><b>ПРН53</b> вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p> <p><b>ПРН 54</b> усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p>
--	--

**8 – Ресурсне забезпечення реалізації програми**

<b>Специфічні характеристики кадрового забезпечення</b>	Викладання фахових дисциплін забезпечуєпрофесорсько-викладацькийскладкафедри:бдокторів та8кандидатівнаук,якіштатнимиспівробітника миуніверситету.
<b>Специфічні характеристики матеріально-технічного забезпечення</b>	Для навчання використовуються 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.
<b>Специфічні характеристики інформаційного та навчально-методичного забезпечення</b>	Використається навчальний фонд бібліотеки ХНУ, ПЗ дистанційних форм навчання, підручники та навчальні посібники розробки кафедри та провідних світових університетів.

**9 – Академічна мобільність**

<b>Національна кредитна мобільність</b>	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.
---	--

<b>Міжнародна кредитна мобільність</b>	Студенти мають можливість здійснювати навчання в ВНЗ інших країн у відповідності з домовленостями університетів в рамках міжнародних програм співробітництва та академічної мобільності.
<b>Навчання іноземних Здобувачів вищої освіти</b>	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(навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
<b>Обов'язкові компоненти ОП</b>			
OK1.	Іноземна мова	6	Іспит/залік
OK2.	Іноземна мова за фахом	3	Залік
OK3.	Історія України	3	Іспит
OK4.	Філософія	3	Іспит
OK5.	Вища математика, теорія ймовірностей	24	Іспит
OK6.	Дискретна математика	7	Іспит/залік
OK7.	Інформаційні технології	7	Залік
OK8.	Фізика	7	Іспит/залік
OK9.	Безпека життєдіяльності та основи охорони праці	3	Залік
OK10.	Вступ до фаху	3	Іспит
OK11.	Електротехніка та електроніка	5	Іспит
OK12.	Комп'ютерна мережі	4	Іспит
OK13.	Основні теорії передачі інформації	4	Іспит
OK14.	Комп'ютерна графіка	3	Залік
OK15.	Метрологія та вимірювання, комп'ютерна схемотехніка (КР-1)	6	Іспит
OK16.	Мікропроцесори та їх застосування	3	Іспит
OK17.	Операційні системи	4	Залік
OK18.	Оптика та інформатика	3	Залік
OK19.	Основні інформаційної безпеки держави	3	Залік
OK20.	Основні теорії кіл, сигналів та процесів електроніки		Іспит
OK21.	Спеціалізовані мови програмування та проектування електронних елементів і систем	6	Іспит/залік
OK22.	Стеганографія	6	Іспит
OK23.	Теорія чисел, теорія груп, полів, кілець	7	Іспит
OK24.	Теорія інформації кодування (КР-1)	5	Іспит
OK25.	Теорія автоматичного управління	4	Іспит
OK26.	Алгоритмізація та програмування	10	Іспит
OK27.	Крос-платформне програмування	3	Залік
OK28.	Теорія алгоритмів	3	Залік

OK29.	Об'єктно-орієнтоване програмування (КР-1)	10	Іспит/залік
OK30.	Математичні методи та технології тестування і верифікації програмного забезпечення (КР-1)	4	Іспит
OK31.	Спеціальні методи обробки даних в телекомунікаційних системах	6	Іспит
OK32.	Виробнича практика	5	Залік
OK33.	Переддипломна практика	5	Залік
OK34.	Підготовка бакалаврської роботи	2	ЗАХИСТ
OK35.	Атестаційний екзамен		Іспит
Загальний обсяг обов'язкових дисциплін		180	
<b>Вибіркові компоненти ОІП*</b>			
<b>Вибірковий блок 1</b>			
ВБ1.1.	Захист інформації в інформаційно-комунікаційних системах (КР-2)	13	Іспит/залік
ВБ1.2.	Комплексні системи захисту інформації: проектування, впровадження, супровід (КР-1)	10	Іспит
ВБ1.3.	Компоненти складних комп'ютерних мереж	3	Іспит
ВБ1.4.	Технології блокчейн	3	Іспит
ВБ1.5.	Нормативно-правове забезпечення інформаційної безпеки (КР-1)	3	Іспит
ВБ1.6.	Прикладна криптологія (КР-1)	8	Іспит
ВБ1.7.	Системи технічного захисту інформації	4	Іспит
ВБ1.8.	Управління інформаційною безпекою	4	Іспит
<b>Вибірковий блок 2</b>			
ВБ2.1.	Апаратні засоби захисту інформації та захист програмного забезпечення (КР-2)	13	Іспит/залік
ВБ2.2.	Технології проектування та сертифікації захищених ІС	10	Іспит
ВБ2.3.	Заводо захищені телекомунікаційні технології та системи	3	Іспит
ВБ2.4.	Аналіз застосування криптовалют	3	Іспит
ВБ2.5.	Стандартизація та сертифікація в галузі ІБ (КР-1)	3	Іспит
ВБ2.6.	Криптосистеми та криптопротоколи (КР-1)	8	Іспит
ВБ2.7.	Захист від технічних розвідок	4	Іспит
ВБ2.8.	Системний аналіз процесів та систем захисту інформації	4	Іспит
<b>Вибірковий блок 3 - міжфакультетських дисциплін</b>			
ВБ3.1.	МФ дисципліна за вибором 1	3	Іспит/залік
ВБ3.2.	МФ дисципліна за вибором 2	3	Іспит
ВБ3.3.	МФ дисципліна за вибором 3	3	Іспит
ВБ3.4.	МФ дисципліна за вибором 4	3	Іспит
Загальний обсяг вибіркових дисциплін		60	
<b>ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ</b>		<b>240</b>	



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

### 3. Форма атестації здобувачів вищої освіти

<p><b>Форми атестації здобувачів вищої освіти</b></p>	<p>Атестація осіб, які здобувають ступінь бакалавра з кібербезпеки, проводиться у формі ЄДКІ та захисту кваліфікаційної роботи бакалавра.</p> <p>На ЄДКІ вноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за стандартом вищої освіти за спеціальністю 125 Кібербезпека та захист інформації.</p> <p>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.</p> <p>Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.</p> <p>До атестації допускаються студенти, які виконали всі вимоги програми підготовки.</p> <p>Атестація завершується видачею документу державного зразка про присудження здобувачу вищої освіти ступеня бакалавра із присвоєнням кваліфікації бакалавр кібербезпеки та захисту інформації, кібербезпека.</p> <p>Атестація здійснюється відкрито і публічно.</p>
<p><b>Вимоги до кваліфікаційної роботи бакалавра</b></p>	<p>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.</p> <p>Виконання випускних кваліфікаційних робіт має сприяти:</p> <ul style="list-style-type: none"> <li>- систематизації, закріпленню й розширенню теоретичних і практичних знань зі спеціальності та застосуванню цих знань для вирішення конкретних завдань;</li> <li>- розвитку навичок здійснення самостійної роботи та оволодіння методикою вирішення питань і завдань, поставлених у випускній роботі;</li> <li>- оцінюванню рівня володіння певною сукупністю професійних компетентностей, необхідних для майбутньої професійної діяльності;</li> <li>- дотримання принципів і норм академічної доброчесності та недопущення плагіату.</li> </ul> <p>Зміст кваліфікаційної роботи визначається її темою. Деталізація вимог до кваліфікаційної роботи регламентується внутрішніми документами і положеннями Харківського національного університету імені В.Н. Каразіна.</p>

**4. Матриця відповідності програмних компетентностей компонентам освітньої програми**

		K31	K32	K33	K34	K35	K36	K37	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10	ФК11	ФК12	
OK1.	Іноземна мова			+																	
OK2.	Іноземна мова за фахом	+		+																	
OK3.	Історія України			+			+	+													
OK4.	Філософія	+					+	+													
OK5.	Вища математика	+								+											
OK6.	Теорія ймовірностей	+								+											
OK7.	Дискретна математика								+	+											
OK8.	Інформаційні технології	+			+	+				+											
OK9.	Фізика																				
OK10.	Безпека життєдіяльності та охорони праці	+					+	+	+												
OK11.	Вступ до фаху		+		+				+		+								+		
OK12.	Електротехніка та електроніка	+																			
OK13.	Комп'ютерна мережі					+				+											
OK14.	Основні теорії передачі інформації									+											
OK15.	Комп'ютерна графіка	+				+															
OK16.	Метрологія та вимірювання, комп'ютерна схема техніка	+																			
OK17.	Мікропроцесори та їх застосування				+																
OK18.	Операційні системи	+								+											
OK19.	Оптика інформатика									+											
OK20.	Основи інформаційної безпеки держави	+	+		+				+			+							+	+	+
OK21.	Основи теорії кіл, сигналів та процесів в ЕЛ.									+											
OK22.	Спеціалізовані мови програмування та проектування ЕЕС	+				+															
OK23.	Стеганографія		+		+						+										
OK24.	Теорія чисел, теорія груп, поліів, кілець		+		+													+			
OK25.	Теорія інформації і кодування		+		+					+											
OK26.	Теорія автоматичного управління	+	+		+																
OK27.	Алгоритмізація та програмування																				
OK28.	Крос-платформне програмування	+				+		+													
OK29.	Теорія алгоритмів									+											
OK30.	Об'єктно-орієнтоване програмування	+								+											
OK31.	Математичні методи та технології ТiВПЗ					+			+	+	+	+									
OK32.	Спеціальні методи обробки даних					+			+	+		+					+				
OK33.	Виробнича практика	+			+				+	+							+	+		+	
OK34.	Переддипломна практика				+	+					+					+		+			
OK35.	Підготовка бакалаврської роботи				+						+						+	+			+



ВБ1.1.	Захист інформації в ІКС		+		+						+	+	+	+	+	+			+		+			
ВБ1.2.	Комплексні системи захисту інформації: проектування, впровадження, супровід	+	+		+						+	+	+	+	+	+							+	
ВБ1.3.	Компоненти складних комп'ютерних мереж		+		+						+		+			+					+			
ВБ1.4.	Технології блокчейн		+		+						+	+	+								+			
ВБ1.5.	Нормативно-правове забезпечення ІБ	+	+		+			+				+	+	+	+								+	
ВБ1.6.	Прикладна криптологія		+		+						+	+		+	+						+	+	+	+
ВБ1.7.	Системи технічного захисту інформації	+	+		+						+	+	+			+							+	
ВБ1.8.	Управління інформаційною безпекою	+	+		+			+				+	+		+	+	+					+	+	
ВБ2.1.	Апаратні засоби захисту інформації та захист ПЗ		+		+						+	+	+	+	+								+	
ВБ2.2.	Технології проектування та сертифікації захищених ІС		+		+						+		+	+	+								+	
ВБ2.3.	Завод захищених телекомунікаційні ТІС	+	+		+						+	+	+		+								+	
ВБ2.4.	Аналіз застосування криптовалют		+		+						+			+							+	+		
ВБ2.5.	Стандартизація та сертифікація в галузі ІБ		+		+						+		+		+	+	+				+		+	
ВБ2.6.	Криптосистеми та криптопротоколи	+	+		+						+		+								+		+	
ВБ2.7.	Захист від технічних розвідок	+	+		+							+	+	+	+	+						+		
ВБ2.8.	Системний аналіз процесів та систем ЗІ	+	+		+						+	+	+	+		+	+				+		+	



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

	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	ББ1	ББ2	ББ3	ББ4	ББ5	ББ6	ББ7	ББ8														
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																	+			+																																					