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

ОСВІТНЬО-НАУКОВА ПРОГРАМА

Кібербезпека (Cyber Security)

третій (освітньо-науковий) рівень вищої освіти
галузі знань 12 Інформаційні технології
спеціальність 125 Кібербезпека та захист інформації

ЗАТВЕРДЖЕНО
Вченою радою
Харківського національного університету
імені В.Н. Каразіна
«____» _____2024 року,
протокол №____
Введено в дію з 2024 р. наказом
від _____ 2024р. № _____
Проректор з науково-педагогічної роботи
_____Олександр ГОЛОВКО

Харків 2024

ЛИСТ ПОГОДЖЕННЯ
освітньо-наукової програми
«Кібербезпека (Cyber Security)»

Освітню програму розглянуто та схвалено:
1. Науково-методичній раді Харківського національного університету імені В.Н. Каразіна протокол №_____ від «_____»_____ 20___р.

Голова науково-методичної ради ,
проректор з науково-педагогічної роботи _____ Олександр ГОЛОВКО

2. Вченій раді факультету комп'ютерних наук:
протокол №____ від «_____»_____ 20___р.
Заступник Голови вченої ради
факультету комп'ютерних наук _____ Олена ТОЛСТОЛУЗЬКА

3. Науково-методичній комісії факультету комп'ютерних наук:
протокол № ____ від «_____»_____ 20___р.
Голова науково-методичної комісії
факультету комп'ютерних наук _____ Лариса ВАСИЛЬЄВА

4. Кафедрі безпеки інформаційних систем і технологій:
протокол №____ від «_____» _____ 20___ р.
В.о. завідувача кафедри безпеки інформаційних систем і технологій,
к.т.н., доцент _____ Ольга МЕЛКОЗЬОРОВА

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Прізвище, ім’я, по батькові	Найменування посади (для сумісників – місце основної роботи, посада)	Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно
Керівник робочої групи - гарант освітньо-наукової програми Горбенко Іван Дмитрович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук, (20.01.09 системи управління (в тому числі зв'язок у Збройних Силах)), професор за кафедрою радіосистем та зв’язку
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
Олійников Роман Васильович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.05 - Комп’ютерні системи і компоненти), доцент
Сватовський Ігор Іванович	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук, доцент
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)
Кандій Сергій Олегович	Аспірант 3 року навчання	
Горбенко Юрій Іванович	Перший заступник головного конструктора ПАТ “Інститут інформаційних технологій”, м. Харків	Кандидат технічних наук (05.13.21 – системи захисту інформації)

При розробці проекту Програми враховані вимоги Національної рамки кваліфікацій України: Ступінь доктора філософії відповідає 8 рівню Національної рамки кваліфікацій, Європейської рамки кваліфікацій для навчання впродовж життя та третьому циклу Рамки кваліфікацій Європейського простору вищої освіти.

Рецензії-відгуки зовнішніх стейкхолдерів на освітньо-наукову програму підготовки докторів філософії з кібербезпеки від наступних організацій:

1. ПАТ «Інститут інформаційних технологій», м. Харків.
2. ТОВ «Трител», м. Київ.
3. ТОВ «Новел Проджектс Енд Солюшинс» м. Дніпро.
4. ТОВ «Новітні комунікаційні технології» м. Харків.

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

1. Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Харківський національний університет імені В.Н. Каразіна факультет комп'ютерних наук
Офіційна назва освітньої програми	Кібербезпека Cyber Security
Ступінь вищої освіти	Третій освітньо-науковий рівень вищої освіти
Кваліфікація, що присвоюється	Доктор філософії з кібербезпеки
Тип диплому та обсяг освітньої програми	Тип диплому - одиничний. Обсяг освітньо-наукової програми становить 4 роки, 1350 годин, 45 кредитів ECTS
Наявність акредитації	Акредитована Національним агентством – сертифікат № 2722 Дата видачі сертифіката про акредитацію освітньої програми - 20.12.2021 Строк дії сертифіката про акредитацію освітньої програми до 01.07.2027 http://start.karazin.ua/programs/8/7/125/31
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – третій цикл, EQF-LLL – 8 рівень
Передумови	Наявність другого освітнього (магістерського) рівня (або освітньо-кваліфікаційний рівень спеціаліста)
Мова викладання	українська
Термін дії освітньої програми	4 роки
Інтернет-адреса постійного розміщення опису освітньої програми	http://start.karazin.ua/programs/8/7/125/31 http://www-csd.univer.kharkov.ua/science/post-graduate/osvitno-naukovi-programi-onp
2. Мета освітньо-наукової програми	
Мета програми	Забезпечити підготовку наукових і науково-педагогічних кадрів у сфері кібербезпеки шляхом здобуття ними компетентностей, достатніх для виконання оригінальних наукових досліджень, результати яких мають наукову новизну, теоретичне та практичне значення, а також їх підтримку в ході підготовки та захисту дисертації
3. Характеристика освітньо-наукової програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	12 – Інформаційні технології, 125 – Кібербезпека та захист інформації

Орієнтація освітньо- наукової програми	Освітньо-наукова програма ґрунтується на результатах сучасних наукових досліджень у сфері кібербезпеки. Спрямована на актуальні аспекти спеціальності, в рамках якої можлива подальша наукова та викладацька кар'єра.
Основний фокус освітньо-наукової програми та спеціалізації	Загальна освіта в галузі «Інформаційні технології», за спеціальністю 125 – «Кібербезпека та захист інформації». Теоретичний зміст предметної області: моделі і методи забезпечення кібербезпеки. Ключові слова: інформаційні технології, моделі, методи забезпечення кібербезпеки.
Особливості програми	Освітньо-наукова програма вимагає підготовки науковців, здатних формулювати та вирішувати наукові та науково- прикладні завдання за спеціальністю 125 - "Кібербезпека та захист інформації". Наукова складова освітньо-наукової програми визначається індивідуальним навчальним планом підготовки доктора філософії. Здобувач має можливість брати участь у розробці та реалізації державних програм та стандартів у галузі кібербезпеки та захисту інформації України. Завдання програми підготовки містять питання, які актуальні для розробників рішень в сфері інформаційної безпеки України.
4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування випускників на посади, що передбачені штатним розписом за професійним спрямуванням, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (ДК 003:2010):

Код	*Назва класифікаційного угруповання*
2310	Викладачі університетів та вищих навчальних закладів
2131.1	Наукові співробітники (обчислювальні системи)
2132.1	Наукові співробітники (програмування)
2139.1	Наукові співробітники (інші галузі обчислень)
2144.1	Наукові співробітники (електроніка, телекомунікації)
2433.1	Наукові співробітники (інформаційна аналітика)

Подальше навчання	Випускники мають можливість продовжувати в наступному навчання в докторантурі (в строки, встановлені чинним законодавством).
5. Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, самостійна науково-навчальна робота на основі науково-технічної навчальної літератури та публікацій у фахових періодичних виданнях, консультування із науковим керівником, науково-педагогічною спільнотою, проведення наукового дослідження, підготовка та захист дисертаційної роботи.

Оцінювання	Форми семестрового оцінювання: поточний контроль, екзамени, заліки. Підсумкова атестація здійснюється у формі публічного захисту дисертаційної роботи.

6. Програмні компетентності	
Інтегральна	Здатність розв’язувати комплексні проблеми в галузі професійної, у тому числі дослідницько-інноваційної
компетентність	діяльності, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики, які спрямовані на підвищення рівня кібербезпеки, поліпшення експлуатаційних, технічних, економічних та інтегральних показників ефективності інформаційних систем і технологій.
Загальні компетентності (ЗК)	ЗК 1. Здатність до наукового мислення, зокрема володіння загальнонауковими (філософськими) компетентностями, спрямованими на формування системного наукового світогляду, професійної етики та загального культурного кругозору. ЗК 2. Здатність генерувати нові ідеї (креативність). ЗК 3 Здатність спілкуватися іноземною мовою. ЗК 4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК 5. Вміння виявляти, ставити та вирішувати проблеми.
Фахові компетентності спеціальності (ФК)	ФК 1. Здатність використати сучасні досягнення науки і передових технологій. ФК 2. Здатність користуватися нормативною та законодавчою базою в сфері інтелектуальної власності. ФК 3. Здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі інформаційно-комунікаційних технологій. ФК 4. Здатність представляти результати досліджень у вигляді звітів і публікацій на державній та одній з іноземних мов. ФК 5. Здатність до викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційно- комунікаційних технологій. ФК 6. Професійне володіння комп’ютером та інформаційними технологіями. ФК 7. Здатність виконувати роботи з проектування складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем відповідно до сфери їх застосування. ФК 8. Здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних і телекомунікаційних систем. ФК 9. Здатність здійснювати аналіз та синтез криптографічних примітивів. ФК 10. Здатність застосовувати моделі і методи комп’ютерної стеганографії при проектуванні комплексів засобів захисту інформаційних і

	телекомунікаційних систем.

7 – Програмні результати навчання	
Програмні результати навчання	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 2. Показувати знання основних положень філософських проблем наукового пізнання. Систематизувати методи наукового пізнання, та використовувати їх в дослідженнях. Використовувати знання сутності, принципів, методів, особливостей наукового пізнання для вивчення і розв'язання проблем. ПРН 3. Демонструвати уміння проводити пошук інформації з різних джерел, її обробку та аналіз із залученням сучасних інформаційних технологій ПРН 4. Демонструвати уміння представляти результати досліджень на державній та одній з іноземних мов. ПРН 5. Правильно визначати проблеми інтелектуальної власності та законодавства у цій сфері, шляхи їх подолання, тлумачити та розкривати основні поняття, інститути та категорії інтелектуальної власності. ПРН 6. Використовувати нормативну та законодавчу базу в сфері інтелектуальної власності ПРН 7. Застосовувати знання при проведенні досліджень з кібербезпеки, спираючись на сучасні досягнення світової науки і передові технології. ПРН 8. Показувати знання і розуміння математичних методів моделювання та оптимізації процесів. ПРН 9. Визначати запобіжні дій щодо протидії загальним методам аналізу криптосистем. ПРН 10. Застосовувати знання і розуміння загальних принципів побудови систем захисту, завдань, вихідних даних та факторів, які необхідно враховувати при проектування систем захисту. ПРН 11. Оцінювати поточний стан рівня безпеки. ПРН 12. Планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі кібербезпеки. ПРН 13. Аналізувати фактори ризику та успіху при плануванні та виконанні відповідного проекту складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем. ПРН 14. Оцінювати знання і вміння тих, хто навчається, сприяючи розвитку в них самостійності, творчих здібностей в процесі засвоєння навчальних дисциплін. ПРН 15. Розробляти математичні моделі завдань забезпечення інформаційної безпеки та захисту інформації. ПРН 16. Аргументувати вибір методів і засобів для застосовування побудови захищених інформаційно-телекомунікаційних систем. ПРН 17. Розробляти рекомендації щодо удосконалення системи інформаційної безпеки, застосування якої

	дозволить мінімізувати ризики та формулювати перелік вразливостей. ПРН 18. Упроваджувати в інформаційні і телекомунікаційні системи сучасні методи забезпечення інформаційної безпеки відповідно до вимог вітчизняних та міжнародних стандартів. ПРН 19. Застосовувати знання і розуміння методів аналізу криптосистем та протидії ним. ПРН 20. Застосовувати знання і розуміння математичних методів синтезу та аналізу криптографічних примітивів. ПРН. 21 Пропонувати обґрунтований вибір та застосовування засобів, необхідних для реалізації та компонування криптографічних систем. ПРН 22. Моделювати динамічні процеси, використовуючи методи опису та дослідження складних систем. ПРН 23. Використовувати математичні методи оптимізації з метою одержання найкращих характеристики функціонування засобів та систем. ПРН 24. Аргументувати вибір та застосовування методів і засобів для побудови захищених інформаційно- телекомунікаційних систем.

8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	100% науково-педагогічних працівників, які задіяні для викладання навчальних дисциплін, передбачених освітньо- науковою програмою, є штатними співробітниками Харківського національного університету імені В. Н. Каразіна. Вони мають наукові ступені і вчені звання та підтверджений рівень наукової і професійної активності, визначений Ліцензійними умовами провадження освітньої діяльності.
Матеріально-технічне забезпечення	Для забезпечення навчального процесу використовується спеціалізований комп’ютерний клас, навчальна лабораторія, навчально-науковий центр сертифікації ключів електронного цифрового підпису кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна. Реалізація результатів досліджень здійснюється в науково-виробничих підприємствах, з якими укладено відповідні договори.
Інформаційне та навчально-методичне забезпечення	Забезпеченість бібліотеки Харківського національного університету імені В. Н. Каразіна вітчизняними та закордонними фаховими періодичними виданнями відповідного профілю, в тому числі в електронному вигляді. Наявність доступу до баз даних провідних закордонних наукових видань, міжнародних наукометричних баз через власну локальну мережу. Вхід до мережі можливий як зі стаціонарних комп’ютерів, так і шляхом використання технології WiFi з приміщень

	університету. Наявність електронного ресурсу університету, який містить навчально- методичні матеріали з дисциплін навчального плану.

9. Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх угод про академічну мобільність для навчання та проведення досліджень між Харківським національним університетом імені В. Н. Каразіна та закладами вищої освіти України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом ім. В.Н.Каразіна та закладами вищої освіти зарубіжних країн-партнерів. План роботи підрозділу, що координує діяльність з інтернаціоналізації. https://www.univer.kharkov.ua/docs/work/umc-polozhennya.pdf Посилання на сайт університету щодо інформації про інтернаціоналізацію https://www.univer.kharkov.ua/ua/general/structure/international_relations_department/about
Навчання іноземних здобувачів вищої освіти	На основі угод між Харківським національним університетом імені В. Н. Каразіна та закладами вищої освіти іноземних країн.

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

а. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові компоненти ОП			
ОК 1	Філософські засади та методологія наукових досліджень	5	залік
ОК 2	Іноземна мові для аспірантів	10	екзамен, залік
ОК 3	Реєстрація прав інтелектуальної власності	3	залік
ОК 4	Підготовка наукових Публікацій та презентація результатів досліджень	4	залік
ОК 5	Математичні методи в кібербезпеці	6	екзамен
ОК 6	Практика	5	залік
Загальний обсяг обов'язкових компонент:		**33**	
2. Вибіркові компоненти ОП			
Вибірковий блок 1			
ВБ 1.1	Методи синтезу та аналізу захищених телекомунікацій	6	залік
ВБ 1.2	Математичні методи синтезу та аналізу криптографічних примітивів	6	екзамен
Вибірковий блок 2			
ВБ 2.1	Методи побудови телекомунікаційних протоколів фізичного та канальних рівнів	6	залік
ВБ 2.2	Моделі і методи комп'ютерної стеганографії	6	екзамен
Вибірковий блок 3			
ВБ 3.1	Методи та системи пост-квантової криптології	6	залік
ВБ 3.2	Математичні методи та технології тестування і верифікації програмного забезпечення	6	екзамен
Загальний обсяг обов'язкових компонент:		**12**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**45**	

b. Структурно-логічна схема ОНП

Рік навчання	1-й		2-й		3-й		4-й	
Семестр	1	2	3	4	5	6	7	8
ОК 1.								
ОК 2.								
ОК 3.								
ОК 4.								
ОК 5.								
ОК 6.								
ВБ 1.1.								
ВБ 1.2.								
ВБ 2.1.								
ВБ 2.2.								
ВБ 3.1.								
ВБ 3.2.								
					Проведення наукового дослідження. Педагогічна практика		Обробка та оформлення результатів дослідження	

3. Форма атестації здобувачів вищої освіти

Атестація випускників третього (освітньо-наукового) рівня вищої освіти освітньої програми спеціальності 125 Кібербезпека та захист інформації проводиться у формі публічного захисту дисертаційної роботи. До захисту дисертації допускаються здобувачі, які виконали всі вимоги навчального плану. Захист дисертаційної роботи відбувається з метою з'ясування рівня підготовленості здобувачів для виконання професійних завдань, передбачених стандартом вищої освіти. Присудження ступеня «доктор філософії» з кібербезпеки та захисту інформації здійснюється відповідно з діючим законодавством України.

Дисертації осіб, які здобувають ступінь доктора філософії, а також відгуки опонентів оприлюднюються на офіційному веб-сайті Харківського національного університету ім. В.Н. Каразіна відповідно до законодавства.

Захист дисертаційної роботи відбувається з метою з'ясування рівня підготовленості здобувачів для виконання професійних завдань, передбачених стандартом вищої освіти.

Наукова складова освітньо-наукової програми передбачає проведення власного наукового дослідження під керівництвом одного або двох наукових керівників та оформлення його результатів у вигляді дисертації. Наукова складова освітньо-наукової програми містить перелік видів наукової роботи аспіранта та форми контролю (звітування), що містяться в таблиці:

Рік підготовки	**Зміст наукової роботи аспіранта (вид роботи)**	**Форма звітності, форма контролю**
1 рік	Аналіз джерел , пов'язаних з тематикою дисертаційної роботи	Виступи на НТК чи МНТК(звіт щодо НДР) та статей(статті) щодо стану досліджень та постановки задач досліджень за тематикою дисертаційної роботи. Наявність опублікованих доповідей(тез) на НТК чи МНТК, матеріалу у звітах щодо НДР та статей (статті). Заслуховування на семінарах та (чи) засіданнях кафедри
2 рік	Проведення наукового дослідження	Виступи на НТК та МНТК, звіти щодо НДР, що виконуються, наявність статей щодо отриманих наукових та науково - практичних результатів, патенти на винахід. Наявність опублікованих доповідей (тез) на НТК чи МНТК, наявність матеріалу у звітах щодо НДР та статтях (статті). Заслуховування на семінарах та (чи) засіданнях кафедри. Посилання та опубліковані результати
3 рік	Проведення наукового експерименту	Програмна чи програмно -апаратна модель її обґрунтування та опис, виступи на НТК чи МНТК, звіт щодо НДР та опубліковані статті(стаття) щодо результатів експерименту, макети досліджень. Наявність опублікованих доповідей (тез) на НТК чи МНТК, наявність матеріалу у звітах щодо НДР та статтях (статті) необхідного рівня публікації. Заслуховування на семінарах та (чи) засіданнях

		кафедри.
4 рік	Впровадження результатів наукових досліджень (патентів), програмного чи / та програмно -апаратного забезпечення. Оформлення та захист дисертаційної роботи.	Методика наукового експерименту, програмного чи / та програмно -апаратне забезпечення, рекламні матеріали та презентації. Посилання на опубліковані результати в інших робота, статтях та доповідях. Акти на реалізації, рецензії на результати практичного значень та застосувань, акти організацій на результати НДР та ДКР, що отримані здобувачем Захист дисертаційної роботи

Дисертація на здобуття наукового ступеня доктора філософії за освітньо-науковою програмою повинна мати обсяг основного тексту не менше як шість авторських аркушів та не більше як дев’ять авторських аркушів, оформлених відповідно до вимог, установлених МОН за поданням Національного агентства.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ВБ 1.1	ВБ 1.2	ВБ 2.1	ВБ 2.2
ЗК 1	.		.	.		.				
ЗК 2	.			.						
ЗК 3		.		.						
ЗК 4			.	.	.					
ЗК 5				.		.	.	.	.	.
ФК 1			.	.	.		.	.	.	.
ФК 2				.	.	.				
ФК 3				.						
ФК 4		.	.	.		.				
ФК 5						.	.		.	
ФК 6					.			.		.
ФК 7							.	.	.	.
ФК 8							.	.	.	.
ФК 9								.		
ФК 10										.

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ВБ 1.1	ВБ 1.2	ВБ 2.1	ВБ 2.2
ПРН 1		.				.				
ПРН 2	.					.				
ПРН 3			.	.		.				
ПРН 4	.	.		.						
ПРН 5			.			.				
ПРН 6			.							
ПРН 7			.	.	.					.
ПРН 8					.	.				
ПРН 9							.	.	.	.
ПРН 10					.		.		.	
ПРН 11					.		.		.	.
ПРН 12			.	.	.					
ПРН 13				.	.		.			
ПРН 14	.	.	.	.	.		.	.	.	.
ПРН 15					.					
ПРН 16							.		.	
ПРН 17								.		.
ПРН 18			.				.		.	
ПРН 19								.		.
ПРН 20								.		.
ПРН 21			.			.	.		.	
ПРН 22					.					
ПРН 23					.					
ПРН 24						.	.		.	