


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

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

протокол № 1 від « 25 » січня 2021 р.

Освітня програма вводиться в дію з 18.02.2021 р.

Ректор  Віль БАКІРОВ
(наказ № 410 / 164 від « 18 » лютого 2021 р.)



**ОСВІТНЬО-НАУКОВА ПРОГРАМА
«Кібербезпека»**

Третього (освітньо-наукового) рівня вищої освіти

за спеціальністю № 125 «Кібербезпека»

галузі знань № 12 «Інформаційні технології»

Кваліфікація: доктор філософії з кібербезпеки

Харків

2021

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної (освітньо-наукової) програми

Вчена рада факультету комп'ютерних наук:
протокол № 7 від «19» січня 2021 р.

Голова Вченої ради факультету _____



Валентин ЛАЗУРИК

Методична комісія факультету комп'ютерних наук:
протокол № 4 від «18» січня 2021 р.

Голова методичної комісії факультету _____



Анатолій БЕРДНІКОВ

Кафедра безпеки інформаційних систем і технологій:
протокол № 5 від «15» січня 2021 р.

Завідувач кафедри _____



Сергій РАССОМАХІН

ПЕРЕДМОВА

При розробці проекту Програми враховані вимоги:

- 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.
- Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах), затвердженого Постановою Кабінету Міністрів від 23.03.2016 р. № 261.
- 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 (для сумісників – місце основної роботи, посада)	Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно
<i>Керівник робочої групи</i>		
Горбенко Іван Дмитрович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук, (20.01.09 системи управління (в том числі зв'язок у Збройних Силах)), професор за кафедрою радіосистем та зв'язку
<i>Члени робочої групи</i>		
Рассомахін Сергій Геннадійович	Завідувач кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.06 - Інформаційні технології), доцент за кафедрою автоматизованих систем управління
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
Колованова Євгенія Павлівна	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук (05.13.21 – системи захисту інформації)

Рецензії 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»

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 кваліфікації мовою оригіналу	Третій освітньо-науковий рівень вищої освіти, доктор філософії з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом доктора філософії, одиничний, 40 кредитів ЄКТС, термін навчання 4 роки
Наявність акредитації	
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – третій цикл, EQF-LLL – 8 рівень
Передумови	Наявність ступеня магістра
Мова викладання	українська
Термін дії освітньої програми	4 роки
Інтернет-адреса постійного розміщення опису освітньої програми	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 спеціальність, спеціалізація)	12 – Інформаційні технології, 125 – Кібербезпека
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». 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. Наукова складова освітньо-наукової програми визначається індивідуальним навчальним планом підготовки доктора філософії.														
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): <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;"><i>Код</i></th> <th style="text-align: center;"><i>Назва класифікаційного угруповання</i></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">2310</td> <td>Викладачі університетів та вищих навчальних закладів</td> </tr> <tr> <td style="text-align: center;">2131.1</td> <td>Наукові співробітники (обчислювальні системи)</td> </tr> <tr> <td style="text-align: center;">2132.1</td> <td>Наукові співробітники (програмування)</td> </tr> <tr> <td style="text-align: center;">2139.1</td> <td>Наукові співробітники (інші галузі обчислень)</td> </tr> <tr> <td style="text-align: center;">2144.1</td> <td>Наукові співробітники (електроніка, телекомунікації)</td> </tr> <tr> <td style="text-align: center;">2433.1</td> <td>Наукові співробітники (інформаційна аналітика)</td> </tr> </tbody> </table>	<i>Код</i>	<i>Назва класифікаційного угруповання</i>	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)
<i>Код</i>	<i>Назва класифікаційного угруповання</i>														
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 компетентність	Здатність розв'язувати комплексні проблеми в галузі професійної, у тому числі дослідницько-інноваційної 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)	<p>ЗК 1. Здатність до наукового мислення, зокрема володіння загальнонауковими (філософськими) компетентностями, спрямованими на формування системного наукового світогляду, професійної етики та загального культурного кругозору.</p> <p>ЗК 2. Здатність генерувати нові ідеї (креативність).</p> <p>ЗК 3 Здатність спілкуватися іноземною мовою.</p> <p>ЗК 4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.</p> <p>ЗК 5. Вміння виявляти, ставити та вирішувати проблеми.</p>
Фахові компетентності спеціальності (ФК)	<p>ФК 1. Здатність використати сучасні досягнення науки і передових технологій.</p> <p>ФК 2. Здатність користуватися нормативною та законодавчою базою в сфері інтелектуальної власності.</p> <p>ФК 3. Здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі інформаційно-комунікаційних технологій.</p> <p>Ф 4. Здатність представляти результати досліджень у вигляді звітів і публікацій на державній та одній з іноземних мов.</p> <p>ФК 5. Здатність до викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційно-комунікаційних технологій.</p> <p>ФК 6. Професійне володіння комп'ютером та інформаційними технологіями.</p> <p>ФК 7. Здатність виконувати роботи з проектування складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем відповідно до сфери їх застосування.</p> <p>ФК 8. Здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних і телекомунікаційних систем.</p> <p>ФК 9. Здатність здійснювати аналіз та синтез криптографічних примітивів.</p> <p>ФК 10. Здатність застосовувати моделі і методи комп'ютерної стеганографії при проектуванні комплексів засобів захисту інформаційних і телекомунікаційних систем.</p>
7 – Програмні результати навчання	
Програмні результати навчання	<p>ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.</p> <p>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.</p> <p>ПРН 3. Демонструвати вміння проводити пошук інформації з різних джерел, її обробку та аналіз із залученням сучасних</p>

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 дії 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 застосування 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 застосування засобів, необхідних для реалізації та компонування криптографічних систем.

ПРН 22. Моделювати динамічні процеси, використовуючи

	<p>методи опису та дослідження складних систем.</p> <p>ПРН 23. Використовувати математичні методи оптимізації з метою одержання найкращих характеристики функціонування засобів та систем.</p> <p>ПРН 24. Аргументувати вибір та застосування методів і засобів для побудови захищених інформаційно-телекомунікаційних систем.</p>
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 угод між Харківським національним університетом імені В. Н. Каразіна та навчальними закладами країн-партнерів.
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

2.1. 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 мова 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
Загальний обсяг обов'язкових компонент:		28	
2. Вибіркові компоненти ОП			
<i>Вибірковий блок 1</i>			
ВБ 1.1	Методи синтезу та аналізу захищених телекомунікацій	6	залік
В.Б 1.2	Математичні методи синтезу та аналізу криптографічних примітивів	6	екзамен
<i>Вибірковий блок 2</i>			
ВБ 2.1	Методи побудови телекомунікаційних протоколів фізичного та каналних рівнів	6	залік
ВБ 2.2	Моделі і методи комп'ютерної стеганографії	6	екзамен
Загальний обсяг обов'язкових компонент:		12	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		40	

2.2. Структурно-логічна схема ОНП

Рік навчання	1-й		2-й		3-й		4-й	
	1	2	3	4	5	6	7	8
Семестр								
ОК 1.								
ОК 2.								
ОК 3.								
ОК 4.								
ОК 5.								
ВБ 1.1.								
ВБ 1.2.								
ВБ 2.1.								
ВБ 2.2.								
					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» 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 здійснюється відповідно з діючим законодавством України.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	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	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			•	•	•				•

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ВБ 1.1	ВБ 1.2	ВБ 2.1	ВБ 2.2
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						•		•	