МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО – НАУКОВА ПРОГРАМА

«Кібербезпека»

третього (освітньо-наукового) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Доктор філософії, Кібербезпека, Кібербезпека

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова вченої ради

_____ / В.В. Семенець /

(протокол № 4 від " 29 " 03 2019 р.)

зі змінами

(протокол № 2 від " 26 " 02 2021 р.)

Освітня програма вводиться в дію з 01.09.2019 р.

Ректор_____ / В.В. Семенець /

(наказ № 178 від " 03 " 04 2019 р.)

зі змінами

(наказ № 77 від " 02 " 03 2021 р.)

Харків 2021 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-наукової програми «Кібербезпека» спеціальності 125 Кібербезпека третього (освітньо-наукового) рівня вищої освіти

УЗГОДЖЕНО

Перший проректор

_____ (підпис) І.В. Рубан

«16» 02 2021 р.

Начальник навчального відділу

_____ (підпис) А.В. Міхнова

«16» 02 2021 р.

В.о. начальника відділу ЛА та ВСЗЯО

_____ (підпис) С.Б. Макашев

«15» 02 2021 р.

Завідувач відділу аспірантури та докторантури

_____ (підпис) В.П. Манаков

«15» 02 2021 р.

Розглянуто на засіданні Вченої Ради факультету КІУ
Протокол № 6 від 08.02.2021 р.
Декан факультету КІУ

_____ О.С. Ляшенко

Розглянуто на засіданні кафедри БІТ
Протокол № 6 від 04.01.2021 р.
Завідувач кафедри БІТ

_____ Г.З. Халімов

Розглянуто на засіданні Вченої Ради факультету ІК
Протокол № 7 від 15.01.2021 р.
Декан факультету ІК

_____ А.В. Снігуров

Розглянуто на засіданні кафедри ІКІ ім. В.В. Поповського
Протокол № 4 від 09.12.2020 р.
Завідувач кафедри ІКІ ім. В.В. Поповського

_____ О.В. Лемешко

Представники роботодавців

Шумов Олександр Іванович,
Приватне акціонерне товариство
«Інститут інформаційних технологій»

_____ (підпис) О.І. Шумов (ІБП)

Мазур Григорій Владиславович,
Товариство з обмеженою відповідальністю
«МНС ГРУП»

_____ (підпис) Г.В. Мазур (ІБП)

Представник ради молодих вчених Наукового товариства молодих учених
Голова ради молодих вчених

_____ (підпис) О.С. Єременко (ІБП)

РОЗРОБЛЕНО

Проєктна група:

керівник проєктної групи:
Халімов Геннадій Зайдулович,
д.т.н., професор, завідувач кафедри БІТ ХНУРЕ _____ Г.З. Халімов
(підпис) (ІБП)

члени проєктної групи:

Сєвєрінов Олександр Васильович,
к.т.н., доцент, доцент кафедри БІТ ХНУРЕ _____ О.В. Сєвєрінов
(підпис) (ІБП)

Олейніков Анатолій Миколайович,
к.т.н., професор, професор кафедри КРіСТЗІ ХНУРЕ _____ А.М. Олейніков
(підпис) (ІБП)

Руженцев Віктор Ігорович,
д.т.н., доцент, професор кафедри БІТ ХНУРЕ _____ В.І. Руженцев
(підпис) (ІБП)

1. Профіль освітньої програми «Кібербезпека» зі спеціальності 125 Кібербезпека

1 - Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки. Факультет комп'ютерної інженерії та управління (КІУ) Кафедра Безпеки інформаційних технологій (БІТ). Факультет інфокомунікацій Кафедра інфокомунікаційної інженерії ім. В.В. Поповського (ІКІ)
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Третій (освітньо-науковий) рівень вищої освіти Доктор філософії, Кібербезпека, Кібербезпека
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом доктора філософії, одиничний, 40 кредитів ЄКТС освітньої складової освітньо-наукової програми, термін освітньої складової освітньо-наукової програми – 1 рік термін навчання 4 роки
Наявність акредитації	
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – третій цикл, EQF-LLL – 8 рівень
Передумови	Наявність ступеня магістра або ОКР спеціаліста
Мова(и) викладання	Українська мова, англійська мова
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	https://nure.ua/branch/viddil-aspiranturi-ta-doktoranturi/specialnosti-ta-osvitno-naukovi-programi/125-kiberbezpeka
2 - Мета освітньої програми	
Підготовка висококваліфікованих фахівців, які: володіють методами дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних з організацією, створенням методів і засобів забезпечення захисту інформації при її зберіганні, обробці та передачі з використанням сучасних математичних методів, інформаційних технологій і технічних засобів	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	12 Інформаційні технології, 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-наукова програма акцентована на розвиток здатності розв'язувати проводити наукові дослідження, вирішувати складні задачі і проблеми у галузі професійної діяльності, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог, проведення педагогічної діяльності в ВНЗ за фахом.

Основний фокус освітньої програми та спеціалізації	Формування необхідних дослідницьких навиків для наукової кар'єри та викладання спеціальних дисциплін в галузі інформаційної безпеки та кібербезпеки **Ключові слова:** кібербезпека, інформаційна безпека, криптографічний захист інформації, захист персональних даних, антивірусний захист, технічний захист інформації, захист від несанкціонованого доступу, управління інформаційною безпекою
Особливості програми	Підготовка докторів філософії за програмою відрізняється акцентом у програмах дисциплін на особливостях забезпечення інформаційної безпеки та кібербезпеки у сучасних умовах. Наукова складова освітньо-наукової програми визначається індивідуальним навчальним планом підготовки доктора філософії.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 1226.2 Начальник відділення установи, організації (сфера захисту інформації); 1229.7 (99) Керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної); 2149.2 Професіонал із організації інформаційної безпеки; 2149.2 Професіонал із організації захисту інформації з обмеженим доступом; 2149.1 Наукові співробітники (інформаційна та кібербезпека); 2149.2 Фахівець (сфера захисту інформації); 2310 Викладачі університетів та вищих навчальних закладів; 2310.1 Докторант; 2310.1 Доцент.
Подальше навчання	Здобуття другого наукового ступеня (доктор наук).
5 - Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, наукові та експериментальні дослідження в лабораторіях, самостійна та навчальна робота на основі науково-технічної навчальної літератури та публікацій у фахових періодичних виданнях, консультування із науковим керівником, науково-педагогічною спільнотою, педагогічна практика, проведення наукового дослідження, підготовка та захист дисертаційної роботи.
Оцінювання	Форми семестрового оцінювання освітньої складової: поточний контроль, заліки. Проміжна атестація у вигляді заслуховування на семінарі, обговоренні, засіданні кафедри (кожні півроку). Підсумкова атестація здійснюється у формі публічного захисту дисертаційної роботи.
6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.
Загальні компетентності (ЗК)	ЗК-1. Здатність спілкуватися другою (іноземною) мовою. ЗК-2. Здатність навчатися та самонавчатися. ЗК-3. Здатність до усного та письмового спілкування рідною мовою.

	ЗК-4. Здатність знаходити, обробляти та аналізувати інформацію з різних джерел. ЗК-5. Здатність проведення досліджень на відповідному рівні. ЗК-6. Знання і розуміння предметної області та розуміння професії. ЗК-7. Здатність до абстрактного та аналітичного мислення й генерування ідей.
Фахові компетентності спеціальності (ФК)	ФК-1. Можливість отримувати якісну інформацію з кількісних даних для проведення наукових експериментів. ФК-2. Здатність та готовність вирішувати нові проблеми галузі інформаційної та кібербезпеки. ФК-3. Можливість планування та проведення експериментальних та спостережних досліджень, а також аналізу даних та обробки інформації; набуття практичних навичок використання програмних засобів інтелектуального аналізу даних, отриманих за результатами досліджень. ФК-4. Здатність розвивати і реалізовувати нові конкурентоспроможні ідеї інформаційної та кібербезпеки. ФК-5. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної та кібербезпеки. ФК-6. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження засобів і систем інформаційної та кібербезпеки, визнання важливості навчання протягом всього життя. ФК-7. Здатність до пошуку та аналізу науково-технічної, природничо-наукової та загальнонаукової інформації. ФК-8. Здатність здійснювати педагогічну діяльність у вищому навчальному закладі у галузі інформаційної та кібербезпеки.
7 - Програмні результати навчання	
Програмні результати навчання (ПРН)	***Когнітивна сфера (знання з предметної області, уміння та навички)*** ПР-1. На основі знань загальнонаукових методів вміти застосовувати методи емпіричного та теоретичного дослідження. Вивчаючи зміст прогностичної функції філософського знання визначати основні типи та методи прогнозування. ПР-2. Знати основні класи моделей і методів моделювання систем та принципи побудови моделей процесів функціонування засобів і систем інформаційної та кібербезпеки, методи їх формалізації та алгоритмізації. ПР-3. Застосовувати методологію наукової діяльності, організовувати дослідницьку діяльність, структурувати вміст наукових праць та правильно подавати результати досліджень. ПР-4. Уміти проводити планування машинних експериментів, дослідження, обробку та аналіз результатів моделювання засобів і систем інформаційної та кібербезпеки з використанням сучасних програмних і технічних засобів. ПР-5. Знати основні класи сучасних методів аналізу даних, зокрема інтелектуального аналізу, та принципи пошуку неявних закономірностей та практично корисних і доступних інтерпретації знань необхідних для прийняття рішень. ПР-6. Уміти розвивати нові та удосконалювати існуючі засобів і систем інформаційної та кібербезпеки.

	ПР-7. Уміти виконувати дослідження властивостей засобів і систем інформаційної та кібербезпеки та проектувати додаткові компоненти на етапі супроводу. ПР-8. Знати особливості філософсько-світоглядних засад, сучасних тенденцій, напрямків і закономірностей розвитку вітчизняної науки в умовах глобалізації й інтернаціоналізації. ***Ціннісно-мотиваційна сфера*** ПР-9. Виявляти здатність до самонавчання та продовження професійного розвитку. ПР-10. Здатність написати наукову статтю (доповідь) на державній та/або іноземній мові з використанням наукової та навчальної літератури, довідників, словників, документів та іншої науково-технічної інформації, з дотриманням норм авторського права. ПР-11. Ефективно спілкуватися з питань інформаційної та кібербезпеки, включаючи усну та письмову комунікацію українською мовою та принаймні ще однією з поширених європейських мов, зі спеціалістами та суспільством загалом. ПР-12. Здатність виконувати навчальну та методичну роботу зі своєї навчальної дисципліни, керуючись нормативними документами та психолого-педагогічними вимогами до навчального процесу.
8 – Ресурсне забезпечення реалізації	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної, управлінської та інноваційної роботи за фахом. Викладачі та наукові керівники здобувачів є авторами навчальних посібників, монографій та статей, учасниками вітчизняних та міжнародних наукових конференцій.
Матеріально-технічне забезпечення	Навчальний процес відбувається у аудиторіях та лабораторіях, обладнаних сучасними комп'ютерними та технічними засобами, в тому числі мультимедійними, а також спеціалізованим програмним забезпеченням.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. Сайт наукової бібліотеки ХНУРЕ http://lib.nure.ua. Електронний архів відкритого доступу Харківського національного університету радіоелектроніки http://openarchive.nure.ua. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/видавнича/ атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). Сайт ХНУРЕ http://nure.ua. 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання. Наукова бібліотека ХНУРЕ та фонди кафедр БІТ, ІКІ ім. В.В. Поповського, КРіСТЗІ, РТІКС, ПМ, ІМ, філософії, СТ, українознавства, Інф. ХНУРЕ.

9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та університетами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На основі договорів між Харківським національним університетом радіоелектроніки і закладами вищої освіти країн-партнерів.

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

2.1.Перелік компонент ОП

Код н/д	Компоненти освітньої програми	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
1. Загальнонаукові (філософські) дисципліни (обов'язкові)			
ОК 1.1	Філософія та методологія сучасної науки, проблеми формування критичного мислення	3	залік
ОК 1.2	Психолого-педагогічні основи науково-педагогічної діяльності	2	залік
2. Дисципліни, що формують універсальні навички дослідника (обов'язкові)			
ОК 2.1	Математичне моделювання процесів та систем	6	залік
ОК 2.2	Особливості сучасної української мови	3	залік
ОК 2.3	Сучасні методи аналізу даних	6	залік
3. *Дисципліни, що формують мовні компетентності (обов'язкові)*			
ОК 3.1	Іноземна мова як мова наукової комунікації	6	залік
Загальний обсяг *дисциплін загальної підготовки*:		26	
4. Дисципліни зі спеціальності (обов'язкові)			
ОК 4.1	Методологія наукових досліджень	4	залік
Загальний обсяг *дисциплін зі спеціальності (обов'язкових)*:		4	
Загальний обсяг обов'язкових компонент:		**30**	
Вибіркові компоненти ОП			
1. Дисципліни зі спеціальності (вибіркові)			
ВБ 1.1	Методи побудови криптосистем стійких до квантових обчислень	5	залік
ВБ 1.2	Методи побудови криптосистем на групах	5	залік
ВБ 2.1	Захист інформації у провідних та мобільних системах зв'язку	5	залік
ВБ 2.2	Фізичні поля об'єктів технічного захисту інформації	5	залік
ВБ 3.1	Перспективні технології та методи забезпечення кібербезпеки в інфокомунікаційних системах	10	залік
ВБ 4.1	Сучасні методи захисту інформації на фізичному рівні інформаційно-комунікаційних систем	10	залік
Загальний обсяг вибіркових компонент:		**10**	
ВСЬОГО ОСВІТНЯ СКЛАДОВА		**40**	
ПП	**Педагогічна практика**	**2**	
Проведення наукового дослідження		**138**	
Обробка та оформлення результатів дослідження		**60**	
ВСЬОГО ПІДГОТОВКА ДОКТОРА ФІЛОСОФІЇ		**240**	

2.2. Структурно-логічна схема ОП

1 семестр	2 семестр
ОК 1.1. ОК 2.1. ОК 3.1. ОК 4.1. ВБ 1.1., ВБ 2.1., ВБ 3.1., ВБ 4.1	ОК 1.2. ОК 2.2. ОК 3.1. ВБ 1.2., ВБ 2.2., ВБ 3.1., ВБ 4.1

3. Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти ступеня доктора філософії спеціальності 125 Кібербезпека проводиться два рази на рік протягом навчання (піврічна проміжна та щорічна). Метою проміжних звітів є контроль за виконанням індивідуального плану аспіранта за всіма складовими, передбаченими навчальним планом.

Підсумковий контроль за дисциплінами навчального плану підготовки аспірантів здійснюється профільними кафедрами.

Під час атестації аспіранта враховується виконання освітньої і наукової компонент освітньо-наукової програми 125 Кібербезпека.

Аспіранти, що успішно пройшли щорічну атестацію, переводяться на наступний рік навчання. Аспіранти, які не пройшли атестацію, підлягають відрахуванню.

Стан готовності дисертації здобувача вищої освіти ступеня доктора філософії до захисту визначається науковим керівником (або консенсусним рішенням двох керівників).

Обов’язковою умовою допуску до захисту є успішне виконання аспірантом його індивідуального навчального плану.

Підсумкова атестація здобувачів вищої освіти ступеня доктора філософії спеціальності 125 Кібербезпека здійснюється спеціалізованою вченою радою, постійно діючою або утвореною для проведення разового захисту, на підставі публічного захисту наукових досягнень у формі дисертації.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1.1	ОК 1.2	ОК 2.1	ОК 2.2	ОК 2.3	ОК 3.1	ОК 4.1	ПП	ВБ 1.1	ВБ 1.2	ВБ 2.1	ВБ 2.2	ВБ 3.1	ВБ 4.1
ЗК-1						+								
ЗК-2		+					+	+						
ЗК-3	+	+		+			+							
ЗК-4			+		+		+		+	+	+	+	+	+
ЗК-5			+		+		+							
ЗК-6		+					+	+	+	+	+	+	+	+
ЗК-7	+		+		+		+							
ФК-1					+		+							
ФК-2	+								+	+	+	+	+	+
ФК-3					+		+							
ФК-4							+		+	+	+	+	+	+
ФК-5							+		+	+	+	+	+	+
ФК-6	+						+		+	+	+	+	+	+
ФК-7				+		+	+							
ФК-8		+						+						

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

	ОК 1.1	ОК 1.2	ОК 2.1	ОК 2.2	ОК 2.3	ОК 3.1	ОК 4.1	ПП	ВБ 1.1	ВБ 1.2	ВБ 2.1	ВБ 2.2	ВБ 3.1	ВБ 4.1
ПР-1	+						+							
ПР-2			+											
ПР-3							+							
ПР-4			+		+		+							
ПР-5					+									
ПР-6							+		+	+	+	+	+	+
ПР-7							+		+	+	+	+	+	+
ПР-8	+													
ПР-9		+					+	+						
ПР-10				+		+								
ПР-11	+			+		+			+	+	+	+	+	+
ПР-12		+						+						

6. Матриця відповідності визначених стандартом компетентностей дескрипторам НРК

Класифікація компетентностей за НРК	**Знання** **Зн1** Концептуальні та методологічні знання в галузі чи на межі галузей знань або професійної діяльності.	**Уміння** **Ум1** Спеціалізовані уміння/навички і методи, необхідні для розв'язання значущих проблем у сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики. **Ум2** Започаткування, планування, реалізація та коригування послідовного процесу ґрунтовного наукового дослідження з дотриманням належної академічної доброчесності. **Ум3** Критичний аналіз, оцінка і синтез нових та комплексних ідей.	**Комунікація** **К1** Вільне спілкування з питань, що стосуються сфери наукових та експертних знань, з колегами, широкою науковою спільнотою, суспільством у цілому. **К2** Використання академічної української та іноземної мови у професійній діяльності та дослідженнях.	**Автономія та відповідальність** **АВ1** Демонстрація значної авторитетності, інноваційність, високий ступінь самостійності, академічна та професійна доброчесність, постійна відданість розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності. **АВ2** Здатність до безперервного саморозвитку та самовдосконалення.
Загальні компетенції				
ЗК-1	**Зн1**	**Ум1**	**К1**	**АВ1**
ЗК-2	**Зн1**	**Ум1, Ум3**	**К1, К2**	**АВ1, АВ2**
ЗК-3	**Зн1**	**Ум1**	**К2**	**АВ1**
ЗК-4	**Зн1**	**Ум1, Ум2**	**К1, К2**	**АВ1, АВ2**
ЗК-5	**Зн1**	**Ум1, Ум2**	**К1, К2**	**АВ1**
ЗК-6	**Зн1**	**Ум1, Ум2**	**К1, К2**	**АВ1**
ЗК-7	**Зн1**	**Ум1, Ум2, Ум3**	**К1, К2**	**АВ1, АВ2**
Фахові компетенції				
ФК-1	**Зн1**	**Ум1**	**К1**	**АВ1**
ФК-2	**Зн1**	**Ум1, Ум2, Ум3**	**К1, К2**	**АВ1, АВ2**
ФК-3	**Зн1**	**Ум1, Ум2, Ум3**	**К1, К2**	**АВ1, АВ2**
ФК-4	**Зн1**	**Ум1, Ум2, Ум3**	**К1, К2**	**АВ1, АВ2**
ФК-5	**Зн1**	**Ум1, Ум2**	**К1, К2**	**АВ1, АВ2**
ФК-6	**Зн1**	**Ум1, Ум2**	**К1, К2**	**АВ1, АВ2**
ФК-7	**Зн1**	**Ум1, Ум2**	**К1, К2**	**АВ1**
ФК-8	**Зн1**	**Ум1, Ум2**	**К1, К2**	**АВ1, АВ2**

7. Наукова та педагогічна компоненти ОНП

Наукова складова освітньо-наукової програми передбачає проведення аспірантами власного наукового дослідження під керівництвом наукових керівників (одного або двох) та оформлення їх результатів у вигляді дисертації.

Педагогічна складова забезпечує підготовку здобувачів до можливої подальшої викладацької діяльності в ЗВО.

7.1. Наукова компонента ОНП

Наукова складова освітньо-наукової програми оформляється у вигляді індивідуального плану наукової роботи аспіранта і є невід'ємною частиною навчального плану аспірантури.

Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання актуального наукового завдання за спеціальністю 125 Кібербезпека, результати якого характеризуються науковою новизною та практичною цінністю.

Невід'ємною частиною наукової складової освітньо-наукової програми аспірантури є підготовка та публікація наукових статей, виступи на наукових конференціях, наукових фахових семінарах, круглих столах, симпозіумах.

Науково-дослідна тематика дисертаційних робіт пов'язана з науковою проблематикою кафедр БІТ та ІКІ ХНУРЕ та спрямована на формування компетенцій проведення наукових досліджень у галузі інформаційної та кібербезпеки.

Основні напрямки досліджень:

- теоретичні, методологічні, технічні, технологічні та організаційні основи створення комплексних систем захисту інформації (КСЗІ), зокрема інформації, що зберігається, оброблюється і передається в комп'ютерних системах і мережах;
- дослідження та розробка методичних основ, та концептуальних положень процесного підходу до захисту інформації;
- організація, архітектура, методологія проектування, технологія функціонування КСЗІ;
- технічні канали витоку інформації та їх моделі, нові технології та засоби захисту інформації від витоку технічними каналами;
- дослідження та обґрунтування вимог, проектування, створення методів блокового симетричного шифрування, гешування та направленого шифрування інформації, дослідження ефективності та криптографічної стійкості;
- криптографічні протоколи та способи вибору систем криптозахисту, адекватних прийнятій політиці безпеки інформації;
- методологія криптографічного аналізу та побудови оцінок криптографічної стійкості шифросистем, методи викриття механізмів

криптоперетворень, зокрема дешифрування;

- методи побудови криптографічних систем на основі обчислень над функціональними полями проективних різноманіть та оцінка їх стійкості;

- математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем і криптографічних протоколів;

- математичні та обчислювальні методи розрахунку надійності криптосистем, прогнозування оцінок криптографічної стійкості, вирішення задач криптографічного аналізу та синтезу шифросистем і криптографічних протоколів;

− методи забезпечення інформаційної безпеки в інфокомунікаційних системах;

- моделі та методи оцінки ризиків інформаційної безпеки;

− моделі та методи забезпечення інформаційної та мережної безпеки, розробка систем оцінки ризиків, пошуку вразливостей та виявлення атак в мережах;

− інформаційна безпека інфокомунікаційних і хмарних технологій;

− розслідування інцидентів порушень інформаційної безпеки, розробка пропозицій щодо мінімізації ризиків і загроз;

− аналіз інформаційної безпеки і прогнозування стану елементів мережі і сегмента мережі в цілому;

- методи та засоби автентифікації користувачів мережі.

7.2. Педагогічна практика

Педагогічна практика є невід'ємною складовою програми підготовки здобувачів і призначена для набуття компетентностей щодо здійснення освітнього процесу, навчання, розвитку і професійної підготовки студентів до певного виду професійно-орієнтованої діяльності.

Метою практики є формування та розвиток професійно-педагогічних компетентностей, знань, навичок та умінь викладача вищої школи з питань організації і форм здійснення освітнього процесу в сучасних умовах.

Педагогічна практика полягає в участі аспіранта у забезпеченні освітнього процесу кафедри та реалізується у вивченні досвіду викладацької діяльності провідних викладачів, роботі з вивчення дисциплін, проведенні занять, що відповідають науково-дослідній роботі здобувача та навчальним планам підготовки студентів першого та другого освітнього рівня вищої освіти, забезпеченні виробничої, професійної та науково-дослідної практик студентів, участі в розробці навчально-методичного забезпечення викладання дисциплін кафедр за спеціальністю 125 Кібербезпека.