МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет радіоелектроніки

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»

другого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ
Голова вченої ради
_____ / В.В. Семенець /
(протокол № 2 від 24.02.2020 р.)
зі змінами
протокол № 1 від "28" 01 2021 р.)
Освітня програма вводиться в дію з 1.09 2020 р.
Ректор_____ / В.В. Семенець /
(наказ № 117 від 27.02. 2020 р.)
зі змінами
наказ № 46 від "02" 02 2021 р.)

Харків 2021 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми
«Системи технічного захисту інформації, автоматизація її обробки»
другого рівня вищої освіти
за спеціальністю 125 «Кібербезпека»

УЗГОДЖЕНО
Перший проректор

_____ І.В. Рубан

«26» 01 2021 р.

В.о. начальника відділу ЛА та ВСЗЯО
_____ С.Б. Макашев
«26» 01 2021 р.

Начальник навчального відділу
_____ А.В. Міхнова
«28» 01 2021_ р.

Розглянуто на засіданні Вченої Ради
факультету ІРТЗІ
протокол № 1 від 22.01.2021 р.
декан факультету ІРТЗІ
_____ С.М. Сакало

Розглянутона засіданні кафедри КРіСТЗІ
протокол № 6 від 19.01.2021р.
завідувач кафедри КРіСТЗІ
_____ І.Є. Антіпов

Представник роботодавця

Кравченко Володимир Дмитрович
Виконавчий директор ПрАТ «ІІТ»
_____ В.Д. Кравченко

РОЗРОБЛЕНО

Проектна група:
Керівник проектної групи:
Руженцев Віктор Ігорович, д.т.н., доц.,
проф. кафедри БІТ, ХНУРЕ _____ В.І. Руженцев

члени проектної групи:
Халімов Геннадій Зайдулович, д.т.н., проф.,
зав. каф. БІТ, ХНУРЕ _____ Г.З. Халімов

Олейніков Анатолій Миколайович, к.т.н., проф.,
професор каф. КРіСТЗІ, ХНУРЕ _____ А.М. Олейніков

Снігуров Аркадій Владіславович, к.т.н., доц.,
доц. каф. ІКІ декан факультету ІК, ХНУРЕ _____ А.В. Снігуров

Сєвєрінов Олександр Васильович, к.т.н., доц.,
доц. каф. БІТ, ХНУРЕ _____ О.В. Сєвєрінов

Голова студентського сенату факультету _____ О.О. Гончаренко

ПЕРЕДМОВА

Розроблено проектною групою у складі:

1. Руженцев Віктор Ігорович	– д-р техн. наук, доцент, професор кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Халімов Геннадій Зайдулович	– д-р техн. наук, професор, зав. кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Олейніков Анатолій Миколайович	– канд. техн. наук, професор, професор кафедри Комп'ютерної радіоінженерії та систем технічного захисту інформації Харківського національного університету радіоелектроніки
3. Снігуров Аркадій Владиславович	– канд. техн. наук, доцент, декан факультету Інфокомунікацій, доцент кафедри Інфокомунікаційної інженерії ім.В.В. Поповського Харківського національного університету радіоелектроніки
4. Сєвєрінов Олександр Васильович	– канд. техн. наук, доцент, доцент кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки

1 Профіль освітньої програми «Системи технічного захисту інформації, автоматизація її обробки» за спеціальністю 125 Кібербезпека

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет радіоелектроніки Факультет Інформаційних радіотехнологій та технічного захисту інформації Кафедра комп'ютерної радіоінженерії та систем технічного захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки
Офіційна назва освітньої програми	Системи технічного захисту інформації, автоматизація її обробки
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання, 1 рік 4 місяці
Наявність акредитації	Сертифікат про акредитацію спеціальності МОН України НД №2190672 від 02.10.2017 року Строк дії сертифіката до 01.07.2025 року
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра (або освітньо-кваліфікаційний рівень спеціаліста)
Мова(и) викладання	Українська мова
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розміщення опису освітньої програми	https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/magistr-125-kiberbezpeka/osvitnja-programa-sistemi-tehnichnogo-zahistu-informacii-avtomatizacija-ii-obrobki
2 – Мета освітньої програми	
Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками використовувати і впроваджувати технології інформаційної та/або кібербезпеки; набуття компетентностей у використанні методів дослідження і проектування систем та комплексів забезпечення інформаційної та кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність,)	12 Інформаційні технології, 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна програма Акцентована на розвиток здатності розв'язувати складні задачі і проблеми у галузі професійної діяльності, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта другого (магістерського) рівня в галузі інформаційної та кібербезпеки за спеціальністю Кібербезпека Ключові слова: кібербезпека, інформаційна безпека, технічний захист інформації, захист від несанкціонованого доступу
Особливості про-	Програма передбачає вивчення:

грами	- законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – методів та засобів оцінювання захищеності інформації; – методів та засобів технічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; автоматизованих систем проектування. Підготовка висококваліфікованих фахівців на високому методичному та професійному рівні.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 2149.2 Професіонал із організації захисту інформації з обмеженим доступом 2149.2 Професіонал із організації інформаційної безпеки
Подальше навчання	Можливість навчання за програмою третього (освітньо-наукового) рівня вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсової роботи, лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, консультації з викладачами, науково-дослідна практика, підготовка атестаційної роботи.
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F)
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	ЗК-1 Здатність застосовувати знання у практичних ситуаціях. ЗК-2 Здатність спілкуватися державною та іноземною мовою. ЗК-3 Навички використання інформаційних і телекомунікаційних технологій. ЗК-4 Здатність проведення досліджень на відповідному рівні. ЗК-5 Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК-6 Вміння виявляти, ставити та вирішувати проблеми. ЗК-7 Здатність приймати обґрунтовані рішення.
Фахові компетентності спеціальності (ФК)	ФК-1 Здатність застосовувати відповідні математичні, наукові і технічні методи, а також комп'ютерне програмне забезпечення для вирішення завдань в сфері інформаційної та кібербезпеки; ФК-2 Здатність продемонструвати практичні навички в сфері інформаційної та кібербезпеки; ФК-3 Здатність продемонструвати знання і розуміння наукових фактів,

	концепцій, теорій, принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки; ФК-4 Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному/кібернетичному простору та інформаційним ресурсам. ФК-5 Здатність продемонструвати розуміння проблем інформаційної та кібербезпеки; ФК-6 Здатність продемонструвати розуміння питань використання технічної літератури та інших джерел інформації ФК-7 Здатність виявляти і описувати ефективність рішень в сфері інформаційної та кібербезпеки на основі використання аналітичних методів і методів моделювання; ФК-8 Здатність продемонструвати знання і розуміння математичних принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки; ФК-9 Здатність розробляти плани і проекти для забезпечення досягнення поставленої певної мети з урахуванням всіх аспектів вирішуваної проблеми ФК-10 Здатність продемонструвати розуміння вимог до діяльності в сфері інформаційної та кібербезпеки; ФК-11 Здатність застосовувати системний підхід до вирішення проблем інформаційної та кібербезпеки.
7 – Програмні результати навчання	
ПРН - 1	Знання і розуміння сучасних методів ведення науково-дослідних робіт, організації та планування експерименту, фізико-математичних методів, що застосовуються в інженерній і дослідницькій практиці, на рівні, необхідному для досягнення інших результатів освітньої програми
ПРН - 2	Здатність аналізувати складні інженерні продукти, процеси і системи відповідно до спеціалізації; обирати і застосовувати придатні типові аналітичні, розрахункові та експериментальні методи; правильно інтерпретувати результати таких досліджень
ПРН - 3	Здатність виявляти, формулювати і вирішувати завдання в сфері інформаційної та кібербезпеки відповідно до спеціалізації; обирати і застосовувати адекватні аналітичні, розрахункові та експериментальні методи
ПРН - 4	Здатність розробляти і проектувати, відповідно до спеціалізації, складні вироби, процеси і системи, які задовольняють встановлені вимоги
ПРН - 5	Здатність виявляти, формулювати і вирішувати незнайомі складні задачі в умовах технічної невизначеності, обирати і застосовувати найбільш прийнятні і відповідні методи з відомих аналітичних, обчислювальних й експериментальних, або нових і новаторських
ПРН - 6	Здатність здійснювати пошук літератури, консультуватися і критично використовувати наукові бази даних та інші відповідні джерела інформації, здійснювати моделювання та аналіз з метою детального вивчення і дослідження питань інформаційної та кібербезпеки відповідно до спеціалізацій
ПРН - 7	Розуміння застосовуваних методик та методів аналізу, проектування і дослідження, а також обмежень їх використання
ПРН - 8	Практичні навички вирішення складних завдань, реалізації складних інженерних проектів і проведення досліджень в сфері інформаційної та кібербезпеки

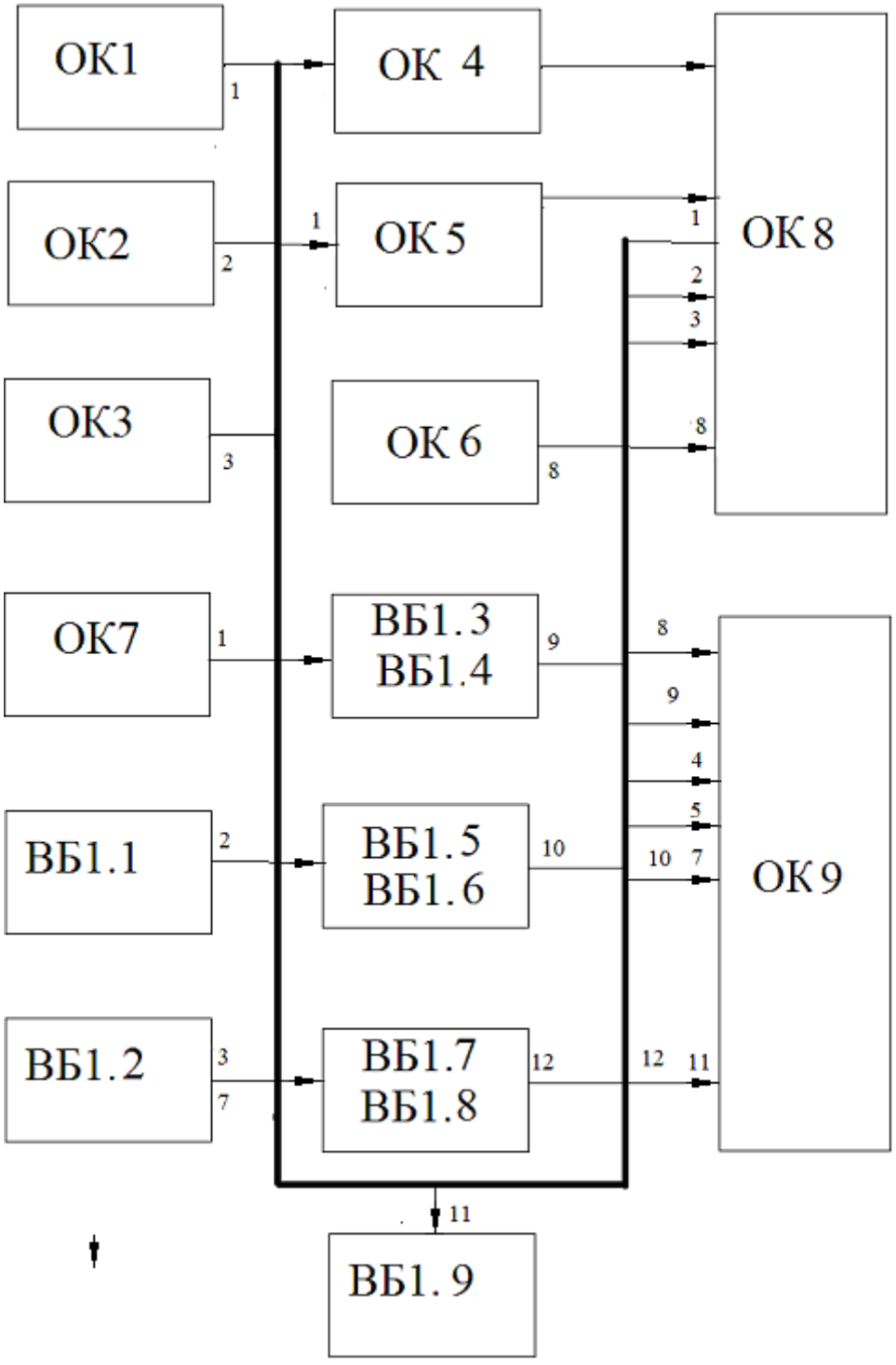
ПРН - 9	Розуміння технічних наслідків діяльності в сфері інформаційної та кібербезпеки
ПРН - 10	Здатність продемонструвати мовні компетентності, достатні для представлення та обговорення своїх наукових результатів іноземною мовою (англійською або іншою, відповідно до специфіки спеціальності) в усній та письмовій формах, а також для повного розуміння іншомовних наукових текстів
ПРН - 11	Знати та уміти застосовувати засоби сучасних інформаційних технологій для вирішення задач в сфері інформаційної та кібербезпеки
ПРН - 12	Орієнтуватися в патентній інформації і документації, досліджувати і правильно формувати ознаки новизни в об'єктах
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов.
Матеріально-технічне забезпечення	1.Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. 2. Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях. 3. Наявність соціально-побутової інфраструктури. 4. Забезпеченість здобувачів вищої освіти гуртожитком. 5. Забезпеченість комп'ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням, необхідними для виконання навчальних планів.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 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). 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти 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 (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн.

2 Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (робота), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
	Обов'язкові компоненти ОП		
ОК 1.	Математичні методи моделювання та оптимізації процесів	5	іспит
ОК 2.	Комплекси захисту і охорони об'єктів інформаційної діяльності	6	іспит
ОК 3.	Захист від технічних розвідок	5	іспит
ОК 4	Спеціальні дослідження в галузі ТЗІ	5	залік
ОК 5	Обробка сигналів у системах ТЗІ	6	іспит
ОК 6	Автоматизація обробки інформації з обмеженим доступом	6	залік
ОК 7	Основи наукових досліджень, організація науки та авторське право	5	залік
ОК 8	Передатестаційна практика	15	залік
ОК 9	Кваліфікаційна робота	15	Захист кваліфікаційної роботи
	Вибіркові компоненти ОП		
	Вибірковий блок 1		
ВБ 1.1	Радіомоніторінг	5	іспит
ВБ 1.2	Виявлення радіосигналів	5	іспит
ВБ 1.3	Спецрозділи фізики	5	залік
ВБ 1.4	Електродинаміка в СТЗІ	5	залік
ВБ 1.5	Проектування цифрових систем ТЗІ	5	іспит
ВБ 1.6	Моделювання цифрових СТЗІ	5	іспит
ВБ 1.7	Спец. мікропроцесори систем ТЗІ	5	іспит
ВБ 1.8	Мікроконтролери в СТЗІ	5	іспит
ВБ 1.9	Іноземна мова за професійним спрямуванням	3	залік
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

2.2 Структурно-логічна схема ОПП



3 Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 Кібербезпека проводиться у формі захисту кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: Магістр, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки.

Атестація здійснюється відкрито і публічно.

4 Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9
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	*								*					*	*			
ФК-9			*				*		*									
ФК-10		*	*			*			*		*							
ФК-11		*				*			*									

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9
ПРН - 1	*			*			*							*	*			
ПРН - 2		*	*	*	*				*	*	*							
ПРН - 3		*		*	*		*	*	*									
ПРН - 4		*	*			*								*	*			
ПРН - 5	*	*	*	*					*			*	*					
ПРН - 6	*	*			*				*			*	*			*	*	
ПРН - 7			*	*			*		*									
ПРН - 8		*	*	*			*	*	*									
ПРН - 9		*	*	*		*			*	*	*			*	*			
ПРН-10		*			*		*		*					*	*	*	*	*
ПРН-11		*	*	*		*											*	
ПРН-12								*	*									