МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«РАДІОІНЖЕНЕРІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

першого (бакалаврського) рівня вищої освіти,
міждисциплінарна предметна область якої об'єднує
предметні області спеціальності
G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка» галузі знань G «Інженерія, виробництво та будівництво»
та спеціальності F5 «Кібербезпека та захист інформації»
галузі знань F «Інформаційні технології»
Кваліфікація: Бакалавр з радіоінженерії інформаційної безпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова Вченої ради _____ **Ігор РУБАН**

(протокол від " 27 **"** 02 **20** 26 **р. №** 3 **)**

Освітня програма вводиться в дію з 01.09 **20** 26 **р.**

Ректор _____ **Ігор РУБАН**

(наказ від " 04 **"** 03 **20** 26 **р. №** 103**)**

Харків 2026

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Радіоінженерія інформаційної безпеки»,
міждисциплінарна предметна область якої об'єднує предметні області спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка» галузі знань G «Інженерія, виробництво та будівництво» та спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології» першого (бакалаврського) рівня вищої освіти

ПОГОДЖЕНО
Перший проректор

_____ Андрій ЄРОХІН

«_12_» ___02___ 20_26_р.

Начальник відділу ЛА та ВСЗЯО

_____ Ганна ТУГАЙ

«_09_» ___02___ 20_26_р.

Начальник навчального відділу

_____ Аліна МІХНОВА

«_10_» ___02___ 20_26_р.

Розглянуто на засіданні Вченої ради
факультету ІРТМ
(з 03.02.2026 факультету ІРТМ)
Протокол від 31.01.2026 № 2
Декан факультету ІРТМ
(з 04.02.02026 в.о. декана факультету ІРТМ)

_____ Денис ГОРЕЛОВ

Розглянуто на засіданні
кафедри ІРТЗІ
(з 03.02.2026 кафедри ІРТМ)
Протокол від 21.01.2026 № 6
Завідувач кафедри ІРТЗІ
(з 04.02.2026 завідувач кафедри ІРТМ)

_____ Дмитро ГАВВА

Представники роботодавців:

В.О. Директора
Інститут радіофізики та електроніки
ім. О.Я. Усикова НАНА України _____ Юрій ЛОГВІНОВ

директор ТОВ «КРАТОС 1» _____ Іван МЕСТЕЧКІН

Представник студентського самоврядування:
Голова студентського сенату
факультету ІРТЗІ _____ Катерина БУРЦЕВА

РОЗРОБЛЕНО

Робоча група:

ГОРЕЛОВ Денис Юрійович,
кандидат технічних наук, доцент,
декан ІРТЗІ факультету, ХНУРЕ

ГАВВА Дмитро Сергійович,
кандидат технічних наук, доцент,
завідувач кафедри КРіСТЗІ, ХНУРЕ

ЛИКОВ Юрій Володимирович,
кандидат технічних наук, доцент,
старший викладач каф. КРіСТЗІ, ХНУРЕ

ОЛЕЙНІКОВ Анатолій Миколайович,
кандидат технічних наук, професор,
професор кафедри КРіСТЗІ, ХНУРЕ

Проєкт освітньо-професійної програми схвалено на засіданні робочої групи (протокол від 02.01.2026 р. №1), розглянуто та схвалено на засіданні кафедри КРіСТЗІ (протокол від 05.01.2026 р. №5) та винесено на громадське обговорення.

Освітньо-професійна програма «Радіоінженерія інформаційної безпеки», міждисциплінарна предметна область якої об’єднує предметні області спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка» галузі знань G «Інженерія, виробництво та будівництво» та спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології» першого (бакалаврського) рівня вищої освіти допрацьована за результатами громадського обговорення, схвалено на засіданні робочої групи (протокол від 20.01.2026 р. №2), розглянуто та схвалено на засіданні кафедри КРіСТЗІ (протокол від 21.01.2026 р. № 6) та на засіданні вченої ради факультету ІРТЗІ (протокол від 31.01.2026 р. № 2).

ПЕРЕДМОВА

Розроблено робочою групою на основі:

– наказу ХНУРЕ від 09.12.2025 р. № 479 «Про створення робочої групи для формування пакету документів з метою започаткування міждисциплінарної освітньої програми «Радіоінженерія інформаційної безпеки» на першому (бакалаврському) рівні вищої освіти»;

– закону України «Про освіту» від 05.09.2017 № 2145-VIII (із змінами) [Електронний ресурс]. – режим доступу: http://zakon.rada.gov.ua/laws/show/2145-19;

– закону України «Про вищу освіту» від 01.07.2014 № 1556-VII (із змінами) [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18;

– постанови Кабінету Міністрів України від 23.11.2011 № 1341 «Про затвердження Національної рамки кваліфікацій» (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/1341-2011-п

– постанови Кабінету Міністрів України від 29.04.2015 № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/266-2015-п

– національного класифікатора України. Класифікатор професій: ДК 003:2010, затверджений наказом Держспоживстандарту України від 28.07.2010 № 327 (На зміну ДК 003:2005) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/rada/show/va327609-10#Text;

– національного класифікатора України. Класифікація видів економічної діяльності: ДК 009:2010, затверджений наказом Держспоживстандарту України від 11.10.2010 № 457 (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/rada/show/vb457609-10;

– наказу Міністерства освіти і науки України від 19.11.2024 № 1625 «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затверджених постановою Кабінету Міністрів України від 30 серпня 2024 року № 1021» (із змінами) [Електронний ресурс]. – режим доступу: https://ips.ligazakon.net/document/re43178?an=1;

– наказу Міністерства освіти і науки України від 13.06.2024 № 842 «Про внесення змін до деяких стандартів вищої освіти» [Електронний ресурс]. – режим доступу: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/Nakaz-842.vid.13.06.2024.pdf;

– наказу Міністерства освіти і науки України від 15.05.2024 №686 «Про затвердження Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти» [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/z1013-24#Text;

– постанови Кабінету міністрів України від 21.06.2024 № 734 «Про затвердження Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських» [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/734-2024-%D0%BF;

– стандарту вищої освіти для першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека та захист інформації, затвердженого Наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 р. № 1547)) [Електронний ресурс]. – режим доступу: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-bakalavr-1547-vid-29-10-2024.pdf;

– стандарту вищої освіти для першого (бакалаврського) рівня вищої освіти спеціальності 172 Телекомунікації та радіотехніка, затвердженого Наказом Міністерства освіти і науки України від 12.12.2018 р. № 1382 [Електронний ресурс]. – режим доступу: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/12/21/172-telekom.radiotekhn-bakalavr-VO-zatv.stand.01.11.pdf;

– наказу МОНУ від 01.02.2021 № 128 «Про затвердження Вимог до міждисциплінарних освітніх (наукових) програм» [Електронний ресурс]. – режим доступу: https://mon.gov.ua/static-objects/mon/uploads/public/661/690/794/6616907943e7a484181895.pdf.

– Наказу МОНУ від 07042025 № 537/43943 «Про внесення змін до Вимог до міждисциплінарних освітніх (наукових) програм» [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/z0537-25#Text

Склад робочої групи:

ГОРЕЛОВ Денис Юрійович	кандидат технічних наук, доцент, декан ІРТЗІ факультету, ХНУРЕ.
ГАВВА Дмитро Сергійович	кандидат технічних наук, доцент, завідувач кафедри КРіСТЗІ, факультету ІРТЗІ, ХНУРЕ.
ЛИКОВ Юрій Володимирович	кандидат технічних наук, доцент, старший викладач кафедри КРіСТЗІ, факультету ІРТЗІ, ХНУРЕ
ОЛЕЙНІКОВ Анатолій Миколайович	кандидат технічних наук, професор, професор кафедри КРіСТЗІ, факультету ІРТЗІ, ХНУРЕ

1. Профіль освітньої програми «Радіоінженерія інформаційної безпеки», міждисциплінарна предметна область якої об’єднує предметні області спеціальностей G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка» галузі знань G «Інженерія, виробництво та будівництво» та F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Харківський національний університет радіоелектроніки, Факультет інформаційних радіотехнологій і технічного захисту інформації Кафедра комп’ютерної радіоінженерії та систем технічного захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр з радіоінженерії інформаційної безпеки
Офіційна назва освітньої програми	Радіоінженерія інформаційної безпеки
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців (2 роки 10 місяців)
Наявність акредитації	Підлягає акредитації вперше
Цикл/рівень	НРК України – 6 рівень, QF-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта (або освітньо-кваліфікаційний рівень молодшого спеціаліста / молодшого бакалавра)
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	Посилання на сайт ХНУРЕ
2 – Мета освітньої програми	
Формування та розвиток загальних і професійних компетентностей з впровадження та застосування технологій електроніки, електронних комунікацій, радіотехніки, кібербезпеки та захисту інформації, що сприяють соціальній стійкості та мобільності випускника на ринку праці, а саме, здатність розв'язувати складні спеціалізовані задачі та практичні проблеми розробки, проєктування, виробництва, монтажу, експлуатації, технічного обслуговування, ремонту і модернізації радіотехнічних пристроїв та систем забезпечення інформаційної безпеки, захищеності інформаційного і кіберпросторів держави загалом або окремих суб’єктів їхньої інфраструктури від ризику стороннього кібернетично-технічного впливу	

3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	G Інженерія, виробництво та будівництво G5 Електроніка, електронні комунікації, приладобудування та радіотехніка F Інформаційні технології F5 Кібербезпека та захист інформації ***Об'єкт*:** технічне, програмне, математичне, інформаційне та організаційне забезпечення систем технічного захисту інформації з використанням сучасної мікропроцесорної і комп'ютерної техніки, спеціалізованого прикладного програмного забезпечення, радіоелектронних та інформаційних технологій. ***Цілі навчання*:** підготовка фахівців, здатних до розв'язання складних задач з технічного захисту інформації, а саме, розроблення нових і вдосконалення існуючих пристроїв та систем забезпечення інформаційної безпеки із застосуванням сучасних програмно-технічних комплексів, автоматизованих засобів проєктування та інформаційних технологій; комплексний аналіз об'єктів інформатизації щодо технічних каналів витоку інформації та обґрунтований вибір організаційних і технічних засобів захисту. ***Теоретичний зміст предметної області*:** теорія, моделі та принципи функціонування радіотехнічних пристроїв; принципи, методи та засоби технічного захисту життєво важливих інтересів людини, суспільства, держави під час використання інформаційного простору; сучасне програмно-апаратне забезпечення радіотехнічних та телекомунікаційних систем і мереж для своєчасного виявлення, запобігання і нейтралізації реальних та потенційних загроз на об'єктах інформатизації. ***Методи, методики та технології*:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення для проєктування та моделювання, технічні засоби контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація освітньої програми	Освітньо-професійна програма. Акцент програми зроблений на формуванні фахівця, здатного використовуючи сучасні радіотехнології проєктувати, експлуатувати, модернізувати та масштабувати системи технічного захисту інформації, а також здатного організовувати та підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Основний фокус освітньої програми	Підготовка висококваліфікованих фахівців, які володіють методами аналізу, синтезу, проєктування, налагодження, модернізації, експлуатації та супроводження систем технічного захисту інформації з використанням сучасних комп'ютерно-інтегрованих радіотехнологій і спеціалізованого програмного забезпечення, та мають компетентності, орієнтовані на врахування в професійній діяльності глобальних цілей сталого розвитку.

	Ключові слова: радіотехнології, телекомунікації, електроніка, радіозв'язок, пристрої мікрохвильової техніки, інформаційно-комунікаційні технології та системи, кібербезпека, інформаційна безпека, криптографічний захист інформації, технічний захист інформації, технічні канали витоку інформації, захист інформації від несанкціонованого доступу, захист від технічних розвідок
Особливості програми	Освітня програма передбачає: поглиблену теоретичну та практичну підготовку з використанням сучасної вимірювальної техніки та спеціалізованого обладнання, цифрових та мережних технологій, мікропроцесорів, програмованих логічних контролерів, систем автоматизованого проєктування та комп'ютерного моделювання; апаратно-програмних засобів виявлення / моніторингу технічних каналів витоку інформації; оволодіння вміннями та здатністю до поєднання радіотехнологій та організаційно-технічних принципів захисту інформації разом із формуванням навичок до чіткого розуміння, можливості передбачати та запобігати втратам, оптимізувати ресурси та сприяти їхньої регенерації, зменшувати технологічний вплив на навколишнє середовище.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назва професій згідно з Національним класифікатором України: Класифікатор професій (ДК 003: 2010) **2144 Професіонали в галузі електроніки та телекомунікацій**: ***2144.2 Інженери в галузі електроніки та телекомунікацій***: − інженер електрозв'язку − інженер-електронік − інженер-конструктор (електроніка) **2139 Професіонали в інших галузях обчислень (комп'ютеризації):** ***2139.2 Професіонали в інших галузях обчислень***: − аналітик систем захисту інформації − аналітик систем захисту інформації та оцінки вразливостей – аналітик з безпеки інформаційно-телекомунікаційних систем − фахівець з тестування систем безпеки та захисту інформації − фахівець з оцінки заходів захисту інформації (кібербезпеки) − фахівець з технічного захисту інформації − фахівець сфери захисту інформації – фахівець з питань безпеки (інформаційно-комунікаційні технології) **2149 Професіонали в інших галузях інженерної справи:** ***2149.2 Інженери (інші галузі інженерної справи)***: − інженер-конструктор − інженер-контролер − інженер-лаборант − інженер-технолог − розробник систем (крім комп'ютерів) − професіонал із організації захисту інформації з обмеженим доступом − професіонал із організації інформаційної безпеки

	2359 Інші професіонали в галузі навчання: ***2359.2 Інші професіонали в галузі навчання:*** – інструктор-методист з інформаційної безпеки та кібербезпеки **3114 Технічні фахівці в галузі електроніки та телекомунікацій**: − технік з сигналізації – технік електрозв'язку – технік з радіолокації – технік-конструктор (електроніка) – технік-технолог (електроніка) **3119 Інші технічні фахівці в галузі фізичних наук та техніки** − технік (сфера захисту інформації) **3132 Оператори радіо- та електронно-комунікаційного устаткування**: − фахівець із телекомунікаційної інженерії − оператор радіочастотного контролю − радіоелектронік **3439 Інші технічні фахівці в галузі управління**: − інспектор з організації захисту секретної інформації − фахівець з режиму секретності − фахівець із організації захисту інформації з обмеженим доступом − фахівець із організації інформаційної безпеки **7242 Монтажники електронного устаткування**: − контролер радіоелектронної апаратури та приладів − монтажник інформаційно-комунікаційних мереж − монтажник інформаційно-комунікаційного устаткування − монтажник радіоелектронної апаратури та приладів − регулювальник радіоелектронної апаратури та приладів **7243 Механіки та експлуатаційники електронного устаткування**: − радіомеханік з ремонту радіоелектронного устаткування − радіотехнік **7244 Установники та експлуатаційники телеграфного та телефонного устаткування**: − електромонтер охоронно-пожежної сигналізації − монтажник устаткування зв'язку
Подальше навчання	Випускники мають право продовжити навчання за програмою другого (магістерського) рівня вищої освіти. Також набути додаткові кваліфікації у системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсових робіт, лабораторні роботи, самостійна робота з використанням підручників, навчальних посібників та конспектів лекцій, консультації з викладачами, проєктно-орієнтоване навчання, виробнича практика, проведення наукових досліджень, підготовка кваліфікаційної роботи.
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ЄКТС (A, B, C, D, E, FX, F)

6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі телекомунікацій та радіотехніки, забезпечення інформаційної безпеки і / або кібербезпеки, що характеризується комплексністю та невизначеністю умов
Загальні компетентності (ЗК)	ЗК 1 Здатність до абстрактного мислення, аналізу та синтезу ЗК 2. Здатність вчитися і оволодівати сучасними знаннями ЗК 3. Здатність до пошуку, оброблення та аналізу інформації ЗК 4. Здатність працювати в команді ЗК 5. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням ЗК 6. Здатність спілкуватися державною мовою як усно, так і письмово ЗК 7. Здатність спілкуватися іноземною мовою ЗК 8. 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 ЗК 9. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності ЗК 10. 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 здорового способу життя ЗК 11. Навики здійснення безпечної діяльності ЗК 12. Прагнення до збереження навколишнього середовища
Спеціальні (фахові, предметні) компетентності (ФК)	СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно з встановленою політикою кібербезпеки та захисту інформації СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно з встановленою політикою кібербезпеки й захисту інформації СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо) СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою

	СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності СК 9. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки СК 10. Здатність здійснювати комп’ютерне моделювання пристроїв, систем і процесів з використанням універсальних пакетів прикладних програм СК 11. Здатність проводити інструментальні вимірювання в інформаційно-телекомунікаційних мережах, телекомунікаційних і радіотехнічних системах різного призначення СК 12. Здатність здійснювати монтаж, налагодження, налаштування, регулювання, дослідну перевірку працездатності, випробування та здачу в експлуатацію споруд, засобів і устаткування телекомунікацій, радіотехніки та інформаційної безпеки СК 13. Здатність організовувати і здійснювати заходи з охорони праці та техніки безпеки в процесі експлуатації, технічного обслуговування обладнання інформаційно-комунікаційних мереж, телекомунікаційних, радіотехнічних систем та систем захисту інформації СК 14. Здатність вибирати певні підсистеми для розробки цифрової системи зв'язку, будувати підсистеми принаймі близькі до оптимальних з точки зору якості системи в цілому, обчислювати параметри якості підсистем та системи в цілому; самостійно виконувати розрахунок різноманітних радіотехнічних пристроїв, що є складовими новітніх систем зв’язку; використовувати обчислювальну техніку та сучасні програмні засоби для моделювання та настроювання цих пристроїв СК 15. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах СК 16. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку СК 17. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки СК 18. Здатність здійснювати проєктування на структурному та схемотехнічному рівнях апаратних засобів технічного захисту інформації та засобів зв’язку відповідно до технічного завдання з використанням як стандартних, так і програмних засобів автоматизації проєктування СК 19. Здатність проводити спеціальні дослідження об’єктів інформаційної діяльності згідно з нормативними документами в галузі ТЗІ СК 20. Здатність виявляти та локалізувати джерела небезпечних сигналів на об’єктах інформаційної діяльності

7 – Програмні результати навчання	
Результати навчання (ПР)	РН 1. Вільно спілкуватися державною мовою усно та письмово при виконання професійних обов'язків РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення РН 5. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат РН 6. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчання та професійну діяльність РН 7. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їхню математичну постановку та обирати раціональний метод вирішення РН 8. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для професійної діяльності РН 9 Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки РН 10. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації загалом РН 11. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної та якісної оцінки ризиків РН 12. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності РН 13. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів РН 14. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації

	РН 15. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах РН 16. Виявляти та 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 РН 17. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів в галузі захисту інформації РН 18. Застосовувати засоби автоматизації проєктування і технічної експлуатації пристроїв та систем технічного захисту інформації, інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем у професійній діяльності РН 19. Пояснювати принципи побудови й функціонування апаратно-програмних комплексів та систем технічного захисту інформації та систем зв'язку РН 20. Розуміти та складати проєктну документацію на комплексні системи технічного захисту інформації ПР 21. Вирішувати задачі розробки, впровадження та супроводу систем моніторингу джерел небезпечних сигналів різної фізичної природи РН 22. Аналізувати та виконувати оцінку ефективності проєктування інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем РН 23. Застосовувати фундаментальні і прикладні науки для аналізу процесів, що відбуваються в телекомунікаційних та радіотехнічних системах РН 24. Розуміти основні властивості компонентної бази для забезпечення якості та надійності функціонування телекомунікаційних, радіотехнічних систем і пристроїв РН 25. Контролювати технічний стан інформаційно-комунікаційних мереж, телекомунікаційних і радіотехнічних систем у процесі їх технічної експлуатації з метою виявлення погіршення якості функціонування чи відмов, та його систематична фіксація шляхом документування РН 26. Аналізувати умови приймання радіосигналів, вживати необхідних заходів для зменшення впливу радіозавад шляхом застосування адаптивних пристроїв; виконувати розрахунок адаптивних пристроїв; оцінювати ефективність їх застосування. РН 27. Застосовувати інженерні розрахунки та експериментальні дослідження параметрів НВЧ кіл для аналізу та розробки НВЧ пристроїв та антен для систем різного призначення

	РН 28. Здійснювати стандартні випробування інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем на відповідність вимогам вітчизняних та міжнародних нормативних документів РН 29. Розуміння та дотримання вітчизняних і міжнародних нормативних документів з питань розроблення, впровадження та технічної експлуатації інформаційно-телекомунікаційних мереж, телекомунікаційних і радіотехнічних систем
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями або вченими званнями, які мають значний досвід навчально-методичної, науково-дослідницької роботи та відповідають кваліфікації відповідно до спеціальності згідно з ліцензійними умовами
Матеріально-технічне забезпечення	1. Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. 2. Забезпеченість мультимедійним обладнанням для 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 міжнародними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою (або офіційними мовами країн Європейського Союзу або інших міжнародних союзів) відповідного або спорідненого профілю. 3. Наявність офіційного вебсайту 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 їхній 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 (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти України
Міжнародна кредитна мобільність	На основі двосторонніх договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн
Навчання іноземних здобувачів вищої освіти	На основі договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн

2. Перелік компонентів освітньої програми та їх логічна послідовність

2.1. Перелік компонентів освітньої програми

Таблиця 1 – Перелік компонентів освітньої програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проєкти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ЦИКЛ ЗАГАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни (обов'язкові)			
ОК1.1	Українське фахове мовлення	4	Залік
ОК1.2	Іноземна мова	8	Залік, екзамен
ОК1.3	Філософія	4	Екзамен
ОК 1.4	Основи права	2	Залік
ОК1.5	Безпека життєдіяльності	3	Залік
ОК1.6	Економіка та бізнес	3	Залік
ОК1.7	Академічна доброчесність	2	Залік
	Всього	**26 кредитів ЄКТС**	
Природничо-наукові (фундаментальні) дисципліни			
ОК2.1	Вища математика	12	Екзамен
ОК2.2	Фізика	6	Залік, екзамен
	Всього	**18 кредитів ЄКТС**	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної, практичної підготовки та підсумкова атестація за освітньою програмою (обов'язкові)			
ОК3.1	Програмування. Частина 1	4	Залік
ОК3.2	Програмне забезпечення інженерних розрахунків	2	Залік
ОК3.3	Програмування. Частина 2	4	Екзамен
ОК3.4	Інформаційно-вимірювальні системи	4	Залік
ОК3.5	Основи мережних та мультимедійних технологій. Частина 1	4	Залік
ОК3.6	Основи мережних та мультимедійних технологій. Частина 2	4	Екзамен
ОК3.7	Цифрова обробки сигналів	3	Залік
ОК3.8	Виробнича практика	4,5	Залік
ОК3.9	Основи комп'ютерного моделювання та проєктування	6	Екзамен
ОК3.10	Основи комп'ютерного моделювання та проєктування	1	Курсова робота
ОК3.11	Цифрові системи з радіодоступом	4	Екзамен
ОК3.12	Передатестаційна практика	4,5	Залік
ОК3.13	Кваліфікаційна робота	9	Екзамен
	Всього	**53 кредитів ЄКТС**	
Дисципліни базової (професійної) підготовки за спеціальністю G5 Електроніка, електронні комунікації, приладобудування та радіотехніка (обов'язкові)			
ОК4.1	Елементна база сучасної електроніки	3	Залік
ОК4.2	Теорія кіл	5	Екзамен
ОК4.3	Електродинаміка та випромінюючі системи. Частина 1	4	Залік
ОК4.4	Основи електроніки	4	Залік

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проєкти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОК4.5	Основи електроніки	1	Курсова робота
ОК4.6	Теорія сигналів та передавання інформації. Частина 1	4	Залік
ОК4.7	Схемотехніка	4	Екзамен
ОК4.8	Електродинаміка та випромінюючі системи. Частина 2	4	Екзамен
ОК4.9	Теорія сигналів та передавання інформації. Частина 2	4	Екзамен
ОК4.10	Приймально-передавальні пристрої	4,5	Екзамен
ОК4.11	Пристрої НВЧ та антени	4	Екзамен
	Всього	**41,5 кредити ЄКТС**	
Дисципліни базової (професійної) підготовки за спеціальністю F5 Кібербезпека та захист інформації (обов'язкові)			
ОК5.1	Штучний інтелект в задачах інформаційної безпеки	4	Залік
ОК5.2	OSINT інструменти для ведення розвідки та захисту інформації	4	Залік
ОК5.3	Криптографічний захист інформації	4	Екзамен
ОК5.4	Методи та засоби захисту інформації. Частина 1	5	Екзамен
ОК5.5	Безпека інформаційних та комунікаційних систем	4	Екзамен
ОК5.6	Методи та засоби захисту інформації. Частина 2	5	Екзамен
ОК5.7	Методи та засоби захисту інформації. Частина 2	1	Курсова робота
ОК5.8	Радіопротидія	5	Екзамен
ОК5.9	Організаційне та нормативно-правове забезпечення ТЗІ	4,5	Екзамен
ОК5.10	Технічні засоби охорони об'єктів	4	Екзамен
ОК5.11	Технічні засоби охорони об'єктів	1	Курсова робота
	Всього	**41,5 кредити ЄКТС**	
	РАЗОМ (цикл професійної підготовки)	**136 кредитів ЄКТС**	
	РАЗОМ (цикл загальної (фахової) підготовки та цикл професійної підготовки)	**180 кредитів ЄКТС**	
ЦИКЛ ВИБІРКОВИХ КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ			
Гуманітарні та соціально-економічні дисципліни (вибіркові*)			
ВБ1	Гуманітарна та соціально-економічна дисципліна 1*	3	Залік
ВБ2	Гуманітарна та соціально-економічна дисципліна 2*	3	Залік
	Фізичне виховання (за рахунок вільного часу студентів)		Залік
	Всього	**6 кредитів ЄКТС**	
Дисципліни професійної та практичної підготовки за освітньою програмою (вибіркові)**			
ВБ3	Електроживлення радіоелектронної апаратури	4	Залік
ВБ4	Теорія інформації та кодування	4	Залік
ВБ5	Бази даних	4	Залік
ВБ6	Кібергігієна	3	Залік
ВБ7	Біометричні технології контролю доступу	3	Залік
ВБ8	Технології електронної ідентифікації	4	Залік
ВБ9	Поширення радіохвиль	4	Залік
ВБ10	Системи банківської безпеки	4	Залік
ВБ11	Кріоелектроніка	4	Залік
ВБ12	Розробка багатоплатформенних вебзастосунків	4	Залік
ВБ13	Проєктування пристроїв на мікроконтролерах і ПЛІС. Мікроконтролери	4	Залік

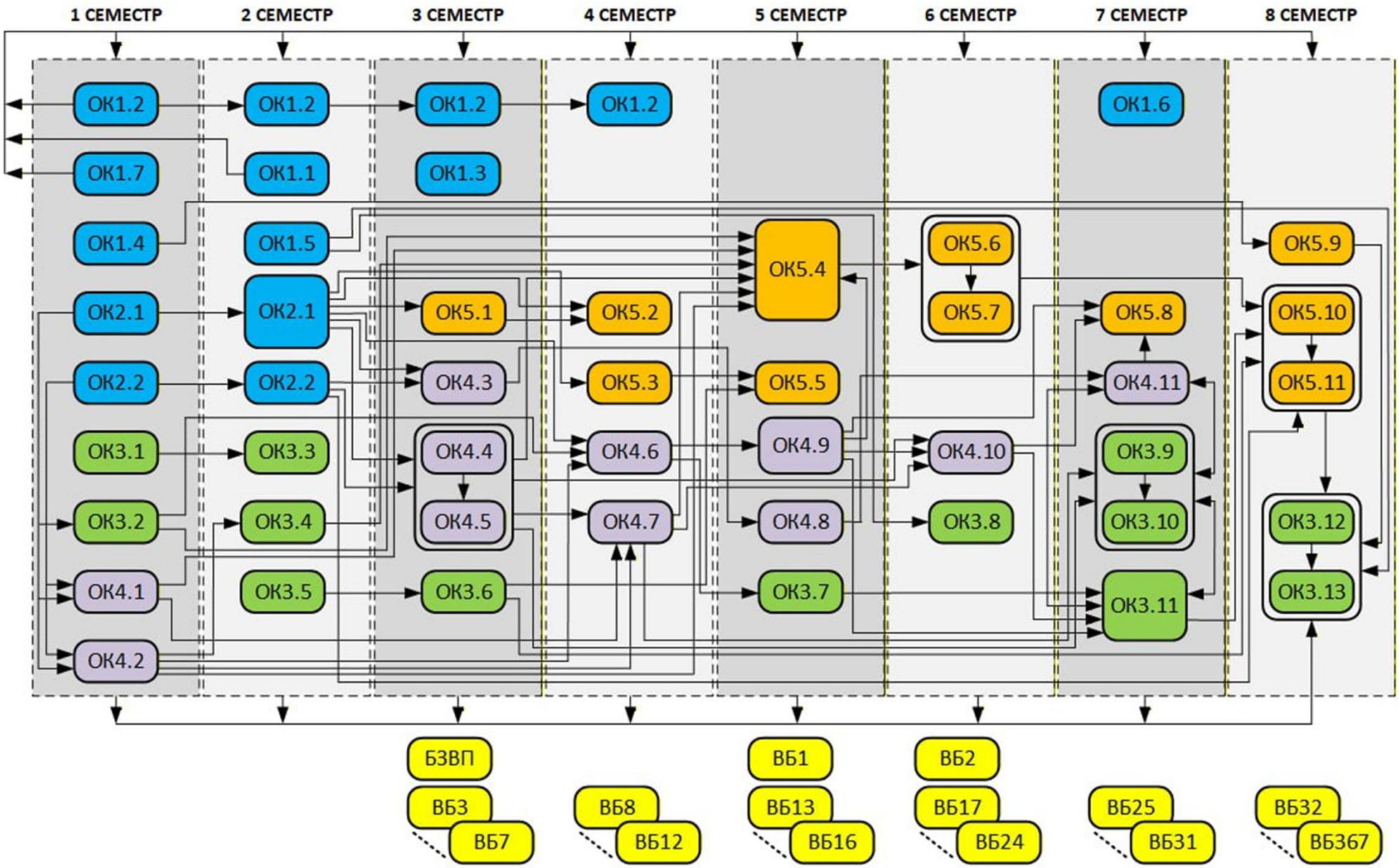
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проєкти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ВБ14	Спеціальні розділи математики для кібербезпеки	4	Залік
ВБ15	Теоретичні основи спеціальних вимірювань	4	Залік
ВБ16	Проєктування користувацьких інтерфейсів інтелектуальних систем	4	Залік
ВБ17	Проєктування пристроїв на мікроконтролерах і ПЛІС. ПЛІС	4	Залік
ВБ18	Радіотехнічні системи	4	Залік
ВБ19	Радіомаскування	4	Залік
ВБ20	Радіомережні технології у вбудованих системах	4	Залік
ВБ21	MEMS-технології	3	Залік
ВБ22	Хмарні платформи та MLOps для інтелектуальних систем	3	Залік
ВБ23	DataOps та інженерія даних для інтелектуальних систем	3	Залік
ВБ24	Основи телебачення та телевізійні системи	3	Залік
ВБ25	Радіомоніторинг	4	Залік
ВБ26	Методи та принципи адаптації в радіоелектронних системах	4	Залік
ВБ27	Електронні системи контролю та керування	4	Залік
ВБ28	Розробка мобільних додатків мікропроцесорних систем	4	Залік
ВБ29	Інформаційні технології пояснення рішень інтелектуальних систем	4	Залік
ВБ30	Радіотехнолгії дистанційного енергозабезпечення	4	Залік
ВБ31	Електромагнітна сумісність РЕЗ	4	Залік
ВБ32	Проєктування систем захисту інформації	4	Залік
ВБ33	Розумні міста та Індустрія 4.0	4	Залік
ВБ34	Паралельні та розподілені обчислення	4	Залік
ВБ35	Наскрізна розробка систем інтелектуального інтернету речей	4	Залік
ВБ36	Радіометричні системи НВЧ діапазону	4	Залік
ВБ37	Завадостійкість РЕЗ	4	Залік
	Всього	**54 кредити ЄКТС**	
Дисципліна обов'язкова для здобувачів вищої освіти чоловічої статі (жіночої статі – добровільно)			
БЗВП	Базова загальновійськова підготовка (теоретична підготовка)	3	залік
	Загальний обсяг вибіркових компонентів	**60 кредитів ЄКТС**	
	ЗАГАЛЬНИЙ ОБСЯГ КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ	**240 кредитів ЄКТС**	

* Перелік навчальних вибіркових компонент блоку гуманітарних та соціально-економічних дисциплін доступний за посиланням: https://nure.ua/zagalnij-katalog-vibirkovih-navchalnih-disciplin/vibirkovi-gumanitarni-ta-socialno-ekonomichni-navchalni-disciplini

** Перелік навчальних вибіркових компонент блоку професійної та практичної підготовки за освітньою програмою може бути доповнено у робочому навчальному плані з загального каталогу вибіркових дисциплін Університету (доступний за посиланням: https://nure.ua/zagalnij-katalog-vibirkovih-navchalnih-disciplin/vibirkovi-navchalni-disciplini-ciklu-profesijno-praktichnoi-pidgotovki) – у разі вибору здобувачами вищої освіти

2.2 Структурно-логічна схема освітньої програми

Семестр 1	Іноземна мова ОК1.2	Основи права ОК1.4	Вища математика ОК2.1	Фізика ОК2.2	Академічна доброчесність ОК1.7	Програмування Частина 1 ОК3.1	Програмне забезпечення інженерних розрахунків ОК3.2	Елементна база сучасної електроніки ОК4.1	Теорія кіл ОК4.2
Семестр 2	Українське фахове мовлення ОК1.1	Іноземна мова ОК1.2	Вища математика ОК2.1	Фізика ОК2.2	Безпека життєдіяльності ОК1.5	Програмування Частина 2 ОК3.3	Інформаційно-вимірювальні системи ОК3.4	Основи мережних та мультимедійних технологій. Частина 1 ОК3.5	
Семестр 3	Іноземна мова ОК1.2	Філософія ОК1.3	Основи мережних та мультимедійних технологій. Частина 2 ОК3.6	Електродинаміка та випромінюючі системи Частина 1 ОК4.3	Основи електроніки ОК4.4	Основи електроніки Курсова робота ОК4.5	Штучний інтелект в задачах інформаційної безпеки ОК5.1	Дисципліна за вибором студентів ВБ3-ВБ5	Дисципліна за вибором студентів ВБ6-ВБ7, БЗВП
Семестр 4	Іноземна мова ОК1.2	Теорія сигналів та передавання інформації Частина 1 ОК4.6	Схемотехніка ОК4.7	OSINT інструменти для ведення розвідки та захисту інформації ОК5.2	Криптографічний захист інформації ОК5.3	Дисципліна за вибором студентів ВБ8-ВБ9	Дисципліна за вибором студентів ВБ10	Дисципліна за вибором студентів ВБ11-ВБ12	
Семестр 5	Цифрова обробка сигналів ОК3.7	Електродинаміка та випромінюючі системи Частина 2 ОК4.8	Теорія сигналів та передавання інформації Частина 2 ОК4.9	Методи та засоби захисту інформації. Частина 1 ОК5.4	Безпека інформаційних та комунікаційних систем ОК5.5	Гуманітарна та соціально-економічна дисципліна 1 за вибором студентів ВБ1	Дисципліна за вибором студентів ВБ13-ВБ14	Дисципліна за вибором студентів ВБ15-ВБ16	
Семестр 6	Приймально-передавальні пристрої ОК4.10	Методи та засоби захисту інформації. Частина 2 ОК5.6	Методи та засоби захисту інформації. Частина 2. Курсова робота ОК5.7	Гуманітарна та соціально-економічна дисципліна 1 за вибором студентів ВБ2	Дисципліна за вибором студентів ВБ17-ВБ18	Дисципліна за вибором студентів ВБ19-ВБ20	Дисципліна за вибором студентів ВБ21-ВБ23	Виробнича практика ОК3.8	
Семестр 7	Економіка та бізнес ОК1.6	Основи комп'ютерного моделювання та проєктування ОК3.9	Основи комп'ютерного моделювання та проєктування Курсова робота ОК3.10	Цифрові системи з радіодоступом ОК3.11	Пристрої НВЧ та антени ОК4.11	Радіопротидія ОК5.8	Дисципліна за вибором студентів ВБ25-ВБ267	Дисципліна за вибором студентів ВБ27-ВБ31	
Семестр 8	Організаційне та нормативно-правове забезпечення ТЗІ ОК5.9	Технічні засоби охорони об'єктів ОК5.10	Технічні засоби охорони об'єктів. Курсова робота ОК5.11	Дисципліна за вибором студентів ВБ32-34	Дисципліна за вибором студентів ВБ35-ВБ37	Передатестаційна практика ОК3.12	Кваліфікаційна робота ОК3.13		


1 СЕМЕСТР
2 СЕМЕСТР
3 СЕМЕСТР
4 СЕМЕСТР
5 СЕМЕСТР
6 СЕМЕСТР
7 СЕМЕСТР
8 СЕМЕСТР
ОК1.2
ОК1.7
ОК1.4
ОК2.1
ОК2.2
ОК3.1
ОК3.2
ОК4.1
ОК4.2
ОК1.2
ОК1.1
ОК1.5
ОК2.1
ОК2.2
ОК3.3
ОК3.4
ОК3.5
ОК1.2
ОК1.3
ОК5.1
ОК4.3
ОК4.4
ОК4.5
ОК3.6
ОК1.2
ОК5.2
ОК5.3
ОК4.6
ОК4.7
ОК5.4
ОК5.5
ОК4.9
ОК4.8
ОК3.7
ОК5.6
ОК5.7
ОК4.10
ОК3.8
ОК1.6
ОК5.8
ОК4.11
ОК3.9
ОК3.10
ОК3.11
ОК5.9
ОК5.10
ОК5.11
ОК3.12
ОК3.13
БЗВП
ВБ3
ВБ7
ВБ8
ВБ12
ВБ1
ВБ13
ВБ16
ВБ2
ВБ17
ВБ24
ВБ25
ВБ31
ВБ32
ВБ367

3. Форма атестації здобувачів вищої освіти

Форма атестації здобувачів вищої освіти за освітньою програмою «Радіоінженерія інформаційної безпеки», міждисциплінарна предметна область якої об’єднує предметні області спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка» галузі знань G «Інженерія, виробництво та будівництво» та спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології» першого (бакалаврського) рівня вищої освіти – захист кваліфікаційної роботи з видачою документу встановленого зразка про присудження здобувачеві ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з радіоінженерії інформаційної безпеки.

Форми атестації

Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.

Вимоги до кваліфікаційної роботи

Кваліфікаційна робота має продемонструвати здатність випускника розв’язувати складні задачі і проблеми в сфері електроніки, електронних комунікацій, радіотехніки та захисту інформації на основі досліджень та / або здійснення інновацій за невизначених умов і вимог.

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його підрозділу, або у репозиторії закладу вищої освіти.

4. Матриця відповідності компетентностей компонентам освітньої програми

Таблиця 4.1 – Матриця відповідності загальних компетентностей обов'язковим компонентам освітньої програми

Код	Освітній компонент	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	ЗК10	ЗК11	ЗК12
ОК1.1	Українське фахове мовлення						√						
ОК1.2	Іноземна мова							√					
ОК1.3	Філософія								√		√		
ОК1.4	Основи права								√	√	√		
ОК 1.5	Безпека життєдіяльності								√		√	√	√
ОК1.6	Економіка та бізнес								√		√		
ОК1.7	Академічна доброчесність									√			
ОК2.1	Вища математика	√											
ОК2.2	Фізика				√								
ОК3.1	Програмування. Частина 1		√										
ОК3.2	Програмне забезпечення інженерних розрахунків		√			√							
ОК3.3	Програмування. Частина 2		√										
ОК3.4	Інформаційно-вимірювальні системи				√								
ОК3.5	Основи мережних та мультимедійних технологій. Частина 1					√							
ОК3.6	Основи мережних та мультимедійних технологій. Частина 2					√							
ОК3.7	Цифрова обробки сигналів					√							
ОК3.8	Виробнича практика				√				√			√	√
ОК3.9	Основи комп'ютерного моделювання та проєктування	√											
ОК3.10	Основи комп'ютерного моделювання та проєктування (КР)	√		√		√	√						
ОК3.11	Цифрові системи з радіодоступом		√										
ОК3.12	Передатестаційна практика								√			√	√
ОК3.13	Кваліфікаційна робота	√	√	√		√	√		√				
ОК4.1	Елементна база сучасної електроніки		√			√							
ОК4.2	Теорія кіл		√			√							
ОК4.3	Електродинаміка та випромінюючі системи. Частина 1				√								
ОК4.4	Основи електроніки		√			√							
ОК4.5	Основи електроніки (КР)			√		√	√						
ОК4.6	Теорія сигналів та передавання інформації. Частина 1		√			√							
ОК4.7	Схемотехніка		√		√								
ОК4.8	Електродинаміка та випромінюючі системи. Частина 2				√								
ОК4.9	Теорія сигналів та передавання інформації. Частина 2		√			√							
ОК4.10	Приймально-передавальні пристрої		√										
ОК4.11	Пристрої НВЧ та антени		√		√								
ОК5.1	Штучний інтелект в задачах інформаційної безпеки		√			√							
ОК5.2	OSINT інструменти для ведення розвідки та захисту інформації		√										
ОК5.3	Криптографічний захист інформації	√											

Код	Освітній компонент	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	ЗК10	ЗК11	ЗК12
ОК5.4	Методи та засоби захисту інформації. Частина 1		√		√								
ОК5.5	Безпека інформаційних та комунікаційних систем		√										
ОК5.6	Методи та засоби захисту інформації. Частина 2		√		√								
ОК5.7	Методи та засоби захисту інформації. Частина 2 (КР)			√		√	√						
ОК5.8	Радіопротидія		√		√								
ОК5.9	Організаційне та нормативно-правове забезпечення ТЗІ	√				√							
ОК5.10	Технічні засоби охорони об'єктів		√		√								
ОК5.11	Технічні засоби охорони об'єктів (КР)			√		√	√						

Таблиця 4.2 – Матриця відповідності фахових компетентностей обов’язковим компонентам освітньої програми

Код	Освітній компонент	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14	СК15	СК16	СК17	СК18	СК19	СК20
ОК1.1	Українське фахове мовлення																				
ОК1.2	Іноземна мова																				
ОК1.3	Філософія																				
ОК1.4	Основи права	√																			
ОК 1.5	Безпека життєдіяльності													√							
ОК1.6	Економіка та бізнес			√																	
ОК1.7	Академічна доброчесність																				
ОК2.1	Вища математика										√										
ОК2.2	Фізика										√										
ОК3.1	Програмування. Частина 1										√										
ОК3.2	Програмне забезпечення інженерних розрахунків										√								√		
ОК3.3	Програмування. Частина 2										√										
ОК3.4	Інформаційно-вимірювальні системи									√		√				√		√		√	
ОК3.5	Основи мережних та мультимедійних технологій. Частина 1	√	√		√																
ОК3.6	Основи мережних та мультимедійних технологій. Частина 2	√	√		√																
ОК3.7	Цифрова обробки сигналів											√			√						
ОК3.8	Виробнича практика	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
ОК3.9	Основи комп'ютерного моделювання та проєктування										√								√		
ОК3.10	Основи комп'ютерного моделювання та проєктування (КР)										√								√		
ОК3.11	Цифрові системи з радіодоступом	√													√						
ОК3.12	Передатестаційна практика	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
ОК3.13	Кваліфікаційна робота	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
ОК4.1	Елементна база сучасної електроніки												√		√						

Код	Освітній компонент	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14	СК15	СК16	СК17	СК18	СК19	СК20
ОК4.2	Теорія кіл												√								
ОК4.3	Електродинаміка та випромінюючі системи. Частина 1														√						
ОК4.4	Основи електроніки												√						√		
ОК4.5	Основи електроніки (КР)												√						√		
ОК4.6	Теорія сигналів та передавання інформації. Частина 1														√						
ОК4.7	Схемотехніка												√						√		
ОК4.8	Електродинаміка та випромінюючі системи. Частина 2														√						
ОК4.9	Теорія сигналів та передавання інформації. Частина 2														√						
ОК4.10	Приймально-передавальні пристрої														√				√		
ОК4.11	Пристрої НВЧ та антени												√								
ОК5.1	Штучний інтелект в задачах інформаційної безпеки																√	√			
ОК5.2	OSINT інструменти для ведення розвідки та захисту інформації																√	√			
ОК5.3	Криптографічний захист інформації		√						√												
ОК5.4	Методи та засоби захисту інформації. Частина 1		√							√						√					√
ОК5.5	Безпека інформаційних та комунікаційних систем		√		√	√		√	√									√			
ОК5.6	Методи та засоби захисту інформації. Частина 2		√							√						√					√
ОК5.7	Методи та засоби захисту інформації. Частина 2 (КР)		√							√						√					√
ОК5.8	Радіопротидія						√	√													√
ОК5.9	Організаційне та нормативно-правове забезпечення ТЗІ	√	√	√	√		√	√		√							√	√			
ОК5.10	Технічні засоби охорони об'єктів	√	√				√	√								√					
ОК5.11	Технічні засоби охорони об'єктів (КР)						√	√								√					

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

Таблиця 5.1 – Матриця забезпечення програмних результатів навчання обов'язковими компонентами освітньої програми

Код	Освітній компонент	РН1	РН2	РН3	РН4	РН5	РН6	РН7	РН8	РН9	РН10	РН11	РН12	РН13	РН14	РН15	РН16
ОК1.1	Українське фахове мовлення	√															
ОК1.2	Іноземна мова		√														
ОК1.3	Філософія					√											
ОК1.4	Основи права			√													
ОК 1.5	Безпека життєдіяльності										√						
ОК1.6	Економіка та бізнес				√												
ОК1.7	Академічна доброчесність			√													
ОК2.1	Вища математика							√									
ОК2.2	Фізика							√									
ОК3.1	Програмування. Частина 1							√									
ОК3.2	Програмне забезпечення інженерних розрахунків					√											
ОК3.3	Програмування. Частина 2							√									
ОК3.4	Інформаційно-вимірювальні системи										√				√	√	√
ОК3.5	Основи мережних та мультимедійних технологій. Частина 1								√	√							
ОК3.6	Основи мережних та мультимедійних технологій. Частина 2								√	√							
ОК3.7	Цифрова обробки сигналів																
ОК3.8	Виробнича практика				√												
ОК3.9	Основи комп'ютерного моделювання та проєктування																
ОК3.10	Основи комп'ютерного моделювання та проєктування (КР)				√												
ОК3.11	Цифрові системи з радіодоступом					√					√						
ОК3.12	Передатестаційна практика				√												
ОК3.13	Кваліфікаційна робота				√	√	√	√	√	√	√	√	√	√	√	√	
ОК4.1	Елементна база сучасної електроніки							√									
ОК4.2	Теорія кіл							√									
ОК4.3	Електродинаміка та випромінюючі системи. Частина 1							√									
ОК4.4	Основи електроніки																

Код	Освітній компонент	РН1	РН2	РН3	РН4	РН5	РН6	РН7	РН8	РН9	РН10	РН11	РН12	РН13	РН14	РН15	РН16
ОК4.5	Основи електроніки (КР)				√												
ОК4.6	Теорія сигналів та передавання інформації. Частина 1						√										
ОК4.7	Схемотехніка																
ОК4.8	Електродинаміка та випромінюючі системи. Частина 2						√	√									
ОК4.9	Теорія сигналів та передавання інформації. Частина 2																
ОК4.10	Приймально-передавальні пристрої																
ОК4.11	Пристрої НВЧ та антени																
ОК5.1	Штучний інтелект в задачах інформаційної безпеки					√						√				√	
ОК5.2	OSINT інструменти для ведення розвідки та захисту інформації					√							√			√	
ОК5.3	Криптографічний захист інформації						√							√			
ОК5.4	Методи та засоби захисту інформації. Частина 1					√	√	√	√						√	√	
ОК5.5	Безпека інформаційних та комунікаційних систем								√	√	√		√				
ОК5.6	Методи та засоби захисту інформації. Частина 2					√	√	√	√						√	√	
ОК5.7	Методи та засоби захисту інформації. Частина 2 (КР)				√												
ОК5.8	Радіопротидія					√											√
ОК5.9	Організаційне та нормативно-правове забезпечення ТЗІ								√	√	√	√	√				
ОК5.10	Технічні засоби охорони об'єктів					√					√				√	√	
ОК5.11	Технічні засоби охорони об'єктів (КР)				√												

Продовження таблиці 5.1

Код	Освітній компонент	РН17	РН18	РН19	РН20	РН21	РН22	РН23	РН24	РН25	РН26	РН27	РН28	РН29
ОК1.1	Українське фахове мовлення													
ОК1.2	Іноземна мова													√
ОК1.3	Філософія													
ОК1.4	Основи права													
ОК 1.5	Безпека життєдіяльності									√				
ОК1.6	Економіка та бізнес													
ОК1.7	Академічна доброчесність													
ОК2.1	Вища математика							√						
ОК2.2	Фізика							√						
ОК3.1	Програмування. Частина 1													
ОК3.2	Програмне забезпечення інженерних розрахунків		√									√		
ОК3.3	Програмування. Частина 2													
ОК3.4	Інформаційно-вимірювальні системи	√				√				√			√	
ОК3.5	Основи мережних та мультимедійних технологій. Частина 1						√			√			√	√
ОК3.6	Основи мережних та мультимедійних технологій. Частина 2						√			√			√	√
ОК3.7	Цифрова обробки сигналів			√										
ОК3.8	Виробнича практика													
ОК3.9	Основи комп'ютерного моделювання та проєктування		√				√					√		√
ОК3.10	Основи комп'ютерного моделювання та проєктування (КР)		√				√					√		√
ОК3.11	Цифрові системи з радіодоступом			√						√				√
ОК3.12	Передатестаційна практика													
ОК3.13	Кваліфікаційна робота	√	√	√	√	√	√	√	√	√	√	√	√	√
ОК4.1	Елементна база сучасної електроніки							√	√					
ОК4.2	Теорія кіл							√						
ОК4.3	Електродинаміка та випромінюючі системи. Частина 1							√						
ОК4.4	Основи електроніки							√	√					
ОК4.5	Основи електроніки (КР)							√						
ОК4.6	Теорія сигналів та передавання інформації. Частина 1	√						√						
ОК4.7	Схемотехніка			√		√		√	√					

Код	Освітній компонент	РН17	РН18	РН19	РН20	РН21	РН22	РН23	РН24	РН25	РН26	РН27	РН28	РН29
ОК4.8	Електродинаміка та випромінюючі системи. Частина 2													
ОК4.9	Теорія сигналів та передавання інформації. Частина 2	√												
ОК4.10	Приймально-передавальні пристрої			√		√					√			
ОК4.11	Пристрої НВЧ та антени			√		√						√	√	
ОК5.1	Штучний інтелект в задачах інформаційної безпеки													
ОК5.2	OSINT інструменти для ведення розвідки та захисту інформації													
ОК5.3	Криптографічний захист інформації													
ОК5.4	Методи та засоби захисту інформації. Частина 1	√												
ОК5.5	Безпека інформаційних та комунікаційних систем													
ОК5.6	Методи та засоби захисту інформації. Частина 2	√												
ОК5.7	Методи та засоби захисту інформації. Частина 2 (КР)													
ОК5.8	Радіопротидія			√		√				√	√			
ОК5.9	Організаційне та нормативно-правове забезпечення ТЗІ													
ОК5.10	Технічні засоби охорони об'єктів			√									√	
ОК5.11	Технічні засоби охорони об'єктів (КР)				√									

6. Матриця відповідності компетентностей дескрипторам НРК

	Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
Загальні компетентності					
ЗК1	ЗК 1 Здатність до абстрактного мислення, аналізу та синтезу		√		√
ЗК2	Здатність вчитися і оволодівати сучасними знаннями		√		√
ЗК3	Здатність до пошуку, оброблення та аналізу інформації		√		
ЗК4	Здатність працювати в команді		√	√	√
ЗК5	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням	√	√	√	√
ЗК6	Здатність спілкуватися державною мовою як усно, так і письмово	√	√	√	
ЗК7	Здатність спілкуватися іноземною мовою	√	√	√	
ЗК8	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	√	√	√	√
ЗК9	Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності	√	√		√
ЗК10	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 здорового способу життя	√	√		√
ЗК11	Навики здійснення безпечної діяльності	√	√		√
ЗК12	Прагнення до збереження навколишнього середовища	√	√		√
Спеціальні (фахові, предметні) компетентності					
СК1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності	√	√		√
СК2	Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації	√	√		√
СК3	Здатність забезпечувати неперервність бізнес-процесів згідно з встановленою політикою кібербезпеки та захисту інформації	√	√	√	√
СК4	Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно з встановленою політикою кібербезпеки й захисту інформації	√	√		√
СК5	Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження	√	√		√

	Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
СК6	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо)	√	√		√
СК7	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою	√	√		√
СК8	Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності	√	√		√
СК9	Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки	√	√		√
СК10	Здатність здійснювати комп’ютерне моделювання пристроїв, систем і процесів з використанням універсальних пакетів прикладних програм	√	√		√
СК11	Здатність проводити інструментальні вимірювання в інформаційно-телекомунікаційних мережах, телекомунікаційних і радіотехнічних системах різного призначення		√		√
СК12	Здатність здійснювати монтаж, налагодження, налаштування, регулювання, дослідну перевірку працездатності, випробування та здачу в експлуатацію споруд, засобів і устаткування телекомунікацій, радіотехніки та інформаційної безпеки	√	√		√
СК13	Здатність організовувати і здійснювати заходи з охорони праці та техніки безпеки в процесі експлуатації, технічного обслуговування обладнання інформаційно-комунікаційних мереж, телекомунікаційних, радіотехнічних систем та систем захисту інформації	√	√	√	√
СК14	Здатність вибирати певні підсистеми для розробки цифрової системи зв'язку, будувати підсистеми принаймі близькі до оптимальних з точки зору якості системи в цілому, обчислювати параметри якості підсистем та системи в цілому; самостійно виконувати розрахунок різноманітних радіотехнічних пристроїв, що є складовими новітніх систем зв’язку; використовувати обчислювальну техніку та сучасні програмні засоби для моделювання та настроювання цих пристроїв.	√	√		√
СК15	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах	√	√		√
СК16	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку	√	√		√
СК17	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	√	√		√

	Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
СК18	Здатність здійснювати проєктування на структурному та схемотехнічному рівнях апаратних засобів технічного захисту інформації та засобів зв'язку відповідно до технічного завдання з використанням як стандартних, так і програмних засобів автоматизації проєктування	√	√		√
СК19	Здатність проводити спеціальні дослідження об'єктів інформаційної діяльності згідно з нормативними документами в галузі ТЗІ	√	√		√
СК20	Здатність виявляти та локалізувати джерела небезпечних сигналів на об'єктах інформаційної діяльності		√		√

7 Матриця відповідності результатів навчання та інтегральної / загальних компетентностей

Програмні результати навчання	Інтегральна компетентність	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	ЗК10	ЗК11	ЗК12
РН 1. Вільно спілкуватися державною мовою усно та письмово при виконання професійних обов'язків	√						√						
РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації	√							√					
РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності	√								√	√	√		
РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення	√	√		√	√	√	√		√		√	√	√
РН 5. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат	√		√		√	√			√		√		
РН 6. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчання та професійну діяльність	√	√	√		√	√							
РН 7. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їхню математичну постановку та обирати раціональний метод вирішення	√	√	√		√	√							
РН 8. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для професійної діяльності	√		√		√	√							
РН 9 Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки	√	√	√			√							
РН 10. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації загалом	√	√	√		√	√			√		√	√	√
РН 11. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної та якісної оцінки ризиків	√	√	√			√							
РН 12. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності	√	√	√			√							

Програмні результати навчання	Інтегральна компетентність	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	ЗК10	ЗК11	ЗК12
РН 13. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів	√	√											
РН 14. Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації	√		√		√								
РН 15. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах	√		√		√	√							
РН 16. Виявляти та 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	√		√		√								
РН 17. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів в галузі захисту інформації	√		√		√	√							
РН 18. Застосовувати засоби автоматизації проєктування і технічної експлуатації пристроїв та систем технічного захисту інформації, інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем у професійній діяльності	√	√	√	√		√	√						
РН 19. Пояснювати принципи побудови й функціонування апаратно-програмних комплексів та систем технічного захисту інформації та систем зв'язку	√		√		√	√							
РН 20. Розуміти та складати проєктну документацію на комплексні системи технічного захисту інформації	√			√		√	√						
РН 21. Вирішувати задачі розробки, впровадження та супроводу систем моніторингу джерел небезпечних сигналів різної фізичної природи	√		√		√								
РН 22. Аналізувати та виконувати оцінку ефективності проєктування інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем	√	√		√		√	√						

Програмні результати навчання	Інтегральна компетентність	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	ЗК10	ЗК11	ЗК12
РН 23. Застосовувати фундаментальні і прикладні науки для аналізу процесів, що відбуваються в телекомунікаційних та радіотехнічних системах	√	√	√	√	√	√	√						
РН 24. Розуміти основні властивості компонентної бази для забезпечення якості та надійності функціонування телекомунікаційних, радіотехнічних систем і пристроїв	√		√		√	√							
РН 25. Контролювати технічний стан інформаційно-комунікаційних мереж, телекомунікаційних і радіотехнічних систем у процесі їх технічної експлуатації з метою виявлення погіршення якості функціонування чи відмов, та його систематична фіксація шляхом документування	√		√		√	√			√		√	√	√
РН 26. Аналізувати умови приймання радіосигналів, вживати необхідних заходів для зменшення впливу радіозавад шляхом застосування адаптивних пристроїв; виконувати розрахунок адаптивних пристроїв; оцінювати ефективність їх застосування.	√		√		√								
РН 27. Застосовувати інженерні розрахунки та експериментальні дослідження параметрів НВЧ кіл для аналізу та розробки НВЧ пристроїв та антен для систем різного призначення	√	√	√	√		√	√						
РН 28. Здійснювати стандартні випробування інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем на відповідність вимогам вітчизняних та міжнародних нормативних документів	√		√		√	√							
РН 29. Розуміння та дотримання вітчизняних і міжнародних нормативних документів з питань розроблення, впровадження та технічної експлуатації інформаційно-телекомунікаційних мереж, телекомунікаційних і радіотехнічних систем	√	√	√	√		√	√	√					

8 Матриця відповідності результатів навчання та спеціальних (фахових, предметних) компетентностей

Програмні результати навчання	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14	СК15	СК16	СК17	СК18	СК19	СК20
РН 1. Вільно спілкуватися державною мовою усно та письмово при виконання професійних обов'язків																				
РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації																				
РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності	√																			
РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення		√	√			√	√		√	√		√			√			√		√
РН 5. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат	√	√				√	√		√	√				√	√	√	√	√		√
РН 6. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчання та професійну діяльність		√						√	√					√	√					√
РН 7. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їхню математичну постановку та обирати раціональний метод вирішення		√							√	√		√		√	√					√
РН 8. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для професійної діяльності	√	√	√	√	√	√	√	√	√						√	√	√			√
РН 9 Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки	√	√	√	√	√	√	√	√								√	√			

Програмні результати навчання	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14	СК15	СК16	СК17	СК18	СК19	СК20
РН 10. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації загалом	√	√	√	√	√	√	√	√	√		√		√	√	√	√	√		√	
РН 11. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної та якісної оцінки ризиків	√	√	√	√		√	√		√							√	√			
РН 12. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності	√	√	√	√	√	√	√	√	√							√	√			
РН 13. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів		√						√												
РН 14. Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації	√	√				√	√		√		√				√		√		√	√
РН 15. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах	√	√				√	√		√		√				√	√	√		√	√

Програмні результати навчання	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14	СК15	СК16	СК17	СК18	СК19	СК20
РН 16. Виявляти та 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						√	√		√		√				√		√		√	√
РН 17. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів в галузі захисту інформації		√							√		√			√	√		√		√	√
РН 18. Застосовувати засоби автоматизації проєктування і технічної експлуатації пристроїв та систем технічного захисту інформації, інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем у професійній діяльності										√								√		
РН 19. Пояснювати принципи побудови й функціонування апаратно-програмних комплексів та систем технічного захисту інформації та систем зв'язку	√	√				√	√				√	√		√	√			√		√
РН 20. Розуміти та складати проєктну документацію на комплексні системи технічного захисту інформації						√	√								√					
РН 21. Вирішувати задачі розробки, впровадження та супроводу систем моніторингу джерел небезпечних сигналів різної фізичної природи						√	√		√		√	√		√	√		√	√	√	√
РН 22. Аналізувати та виконувати оцінку ефективності проєктування інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем	√	√		√						√								√		
РН 23. Застосовувати фундаментальні і прикладні науки для аналізу процесів, що відбуваються в телекомунікаційних та радіотехнічних системах										√		√	√	√				√		
РН 24. Розуміти основні властивості компонентної бази для забезпечення якості та надійності функціонування телекомунікаційних, радіотехнічних систем і пристроїв												√		√				√		

Програмні результати навчання	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14	СК15	СК16	СК17	СК18	СК19	СК20
РН 25. Контролювати технічний стан інформаційно-комунікаційних мереж, телекомунікаційних і радіотехнічних систем у процесі їх технічної експлуатації з метою виявлення погіршення якості функціонування чи відмов, та його систематична фіксація шляхом документування	√	√		√		√	√		√		√		√	√	√		√		√	√
РН 26. Аналізувати умови приймання радіосигналів, вживати необхідних заходів для зменшення впливу радіозавад шляхом застосування адаптивних пристроїв; виконувати розрахунок адаптивних пристроїв; оцінювати ефективність їх застосування.						√	√							√				√		√
РН 27. Застосовувати інженерні розрахунки та експериментальні дослідження параметрів НВЧ кіл для аналізу та розробки НВЧ пристроїв та антен для систем різного призначення										√		√						√		
РН 28. Здійснювати стандартні випробування інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем на відповідність вимогам вітчизняних та міжнародних нормативних документів	√	√		√		√	√		√		√	√			√		√		√	
РН 29. Розуміння та дотримання вітчизняних і міжнародних нормативних документів з питань розроблення, впровадження та технічної експлуатації інформаційно-телекомунікаційних мереж, телекомунікаційних і радіотехнічних систем	√	√		√						√				√				√		