

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Чернівецький національний університет імені Юрія Федьковича

Відокремлений структурний підрозділ «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича»



“ЗАТВЕРДЖЕНО”

Вченою радою Чернівецького національного університету імені Юрія Федьковича
Голова Вченої ради

(підпис)

Руслан БІЛОСКУРСЬКИЙ
(ім'я та прізвище)

Протокол № 4 від “30” 03 2026 року

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

Рівень освіти

фахова передвища

за спеціальністю

F5 Кібербезпека та захист інформації

галузі знань

F Інформаційні технології

кваліфікація

фаховий молодший бакалавр

із кібербезпеки та захисту інформації



СХВАЛЕНО на засіданні Педагогічної ради Відокремленого структурного підрозділу «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича»

Голова Педагогічної ради Олександр СОБЧУК /

Протокол № 7 від “17” березня 2026 року

Освітньо-професійна програма вводиться в дію з 31.03 2026р.

Ректор

Руслан БІЛОСКУРСЬКИЙ /

(Наказ № 114 від “31” 03 2026р.)



Чернівці, 2026

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

РІВЕНЬ ОСВІТИ	<u>фахова передвища</u>
ГАЛУЗЬ ЗНАНЬ	<u>F Інформаційні технології</u>
СПЕЦІАЛЬНІСТЬ	<u>F5 Кібербезпека та захист інформації</u>
КВАЛІФІКАЦІЯ	<u>фаховий молодший бакалавр</u> <u>із кібербезпеки та захисту інформації</u>

РОЗРОБЛЕНО робочою (проектною) групою

Керівник групи

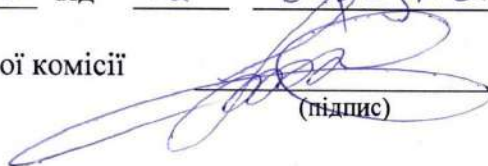

(підпис)

Олександр ГРЕСЬ
(ім'я та прізвище)

ПОГОДЖЕНО цикловою комісією комп'ютерної інженерії

Протокол № 9 від "12" березня 2026 року

Голова циклової комісії


(підпис)

Олександр ТАЩУК
(ім'я та прізвище)

СХВАЛЕНО методичною радою ВСП «Фаховий коледж ЧНУ»

Протокол № 5 від "16" березня 2026 року

Голова методичної ради

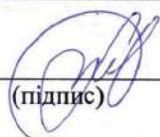

(підпис)

Ольга БІЛОКРИЛА
(ім'я та прізвище)

СХВАЛЕНО комісією з питань освітньої діяльності Вченої ради ЧНУ

Протокол № 7 від "25" березня 2026 року

Голова комісії


(підпис)

Ольга МАРТИНЮК
(ім'я та прізвище)

ПЕРЕДМОВА

Освітньо-професійна програма «**Кібербезпека та захист інформації**» для підготовки здобувачів фахової передвищої освіти за спеціальністю **F5 Кібербезпека та захист інформації** розроблена відповідно до абзацу 1 пункту 5 наказу Міністерства освіти і науки України «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти», затвердженого Постановою Кабінету Міністрів України від 30.08.2024 №1021 (<https://zakon.rada.gov.ua/laws/show/1021-2024>) та з врахуванням «Методичних рекомендацій розроблення освітньо-професійної програми та навчального плану підготовки здобувачів фахової передвищої освіти», розроблених Державною установою «Науково-методичний центр вищої та фахової передвищої освіти», 2022, УДК 377(072+073).

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ (ДУ «НМЦ ВИЩОЇ та ФПО», 2022)

РОЗРОБЛЕНО робочою (проектною) групою у складі:

Гресь Олександр Володимирович, керівник робочої (проектної) групи, викладач (за суміщенням), спеціаліст вищої категорії, кандидат технічних наук, доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича;

Рожественська Маргарита Григорівна, викладач (за суміщенням), спеціаліст вищої категорії, кандидат фізико-математичних наук, доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича;

Косован Григорій Васильович, викладач (за суміщенням), спеціаліст вищої категорії, кандидат технічних наук, асистент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича;

Ташук Роман Юрійович, викладач, спеціаліст вищої категорії, доктор філософії (спеціальність 104 Фізика та астрономія), магістрант ОПП «Кібербезпека» спеціальності F5 Кібербезпека та захист інформації Чернівецького національного університету імені Юрія Федьковича.

1. Опис освітньо-професійної програми «Кібербезпека та захист інформації» спеціальності F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології

1 – Загальна інформація	
Повна назва ЗВО та структурного підрозділу	Чернівецький національний університет імені Юрія Федьковича; Відокремлений структурний підрозділ «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича»
Освітньо-професійний ступінь	Фаховий молодший бакалавр
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Форми здобуття освіти	Інституційна (очна)
Освітня кваліфікація	Фаховий молодший бакалавр із кібербезпеки та захисту інформації
Професійна кваліфікація	–
Кваліфікація у дипломі	Освітньо-професійний ступінь – фаховий молодший бакалавр; Спеціальність – F5 Кібербезпека та захист інформації; Освітньо-професійна програма – «Кібербезпека та захист інформації»
Рівень кваліфікації згідно з Національною рамкою кваліфікації	5 рівень Національної рамки кваліфікацій
Офіційна назва освітньо-професійної програми	Кібербезпека та захист інформації
Обсяг кредитів ЄКТС, необхідний для здобуття ступеня фахового молодшого бакалавра	Обсяг освітньо-професійної програми фахового молодшого бакалавра на базі повної загальної середньої освіти або диплому кваліфікованого робітника становить 180 кредитів ЄКТС (2 роки та 10 місяців) та 240 кредитів ЄКТС на основі базової середньої освіти (3 роки та 10 місяців) На основі базової середньої освіти здобувачі фахової передвищої освіти зобов'язані одночасно виконати освітню програму профільної середньої освіти, тривалість здобуття якої становить два роки. Освітня програма профільної середньої освіти професійного спрямування, що відповідає галузі знань F Інформаційні технології зі спеціальності F5 Кібербезпека та захист інформації, інтегрується з освітньо-професійною програмою фахового молодшого бакалавра.
Наявність акредитації	Акредитація освітньо-професійної програми запланована на 2030-2031 навчальний рік
Термін дії освітньої програми	До введення в дію нової освітньо-професійної програми або прийняття рішення Вченою радою Чернівецького національного університету імені Юрія Федьковича про закриття чи призупинення діючої освітньо-професійної програми.
Вимоги до осіб, які можуть розпочати навчання за програмою	Наявність базової середньої освіти або повної загальної (профільної) середньої освіти. Умови вступу визначаються Правилами прийому до ВСП «Фаховий коледж ЧНУ» відповідного року.
Мова(и) викладання	Українська
Інтернет-адреса постійного розміщення освітньо-професійної програми	https://college.chnu.edu.ua/osvitni-prohramy/kiberbezpeka-ta-zakhyst-informatsii/

2 – Мета освітньої програми	
<p>Формування особистісних компетенцій фахівця, здатного розв'язувати типові та спеціалізовані професійні завдання з інформаційної безпеки та/або кібербезпеки, підвищувати ефективність захисту існуючих інформаційних і телекомунікаційних систем, обслуговувати системи захисту та безпеки в процесі професійної діяльності або навчання.</p>	
3 - Характеристика освітньої програми	
Предметна область	<p><i>Галузь знань:</i> F «Інформаційні технології» <i>Спеціальність:</i> F5 Кібербезпека та захист інформації <i>Об'єкти вивчення та діяльності:</i> Системи технічного захисту інформації, інформаційно-комунікаційні та комп'ютерні системи і мережі, системи кібербезпеки, об'єкти інформаційної інфраструктури, системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації, процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. <i>Цілі навчання:</i> Підготовка фахівців, здатних розв'язувати типові задачі, пов'язані з використанням інформаційно-комунікаційних технологій, сучасних методів і моделей кібербезпеки, розробкою та використанням програмних та програмно-апаратних засобів захисту інформації для забезпечення кібербезпеки, формування та розвиток Soft Skills шляхом заохочення до всебічного використання індивідуальної освітньої траєкторії. <i>Методи, методики та технології:</i> Технології забезпечення безпеки в інформаційно-комунікаційних системах та мережах, засоби виявлення, управління та ідентифікації ризиків, засоби технічного та криптографічного захисту інформації. Інструменти та обладнання: системи розробки, забезпечення, моніторингу та контролю процесів кібербезпеки інформаційно-комунікаційних системах, сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. <i>Теоретичний зміст предметної області:</i> Законодавча, нормативно-правова база України та вимоги відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципи супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделі та принципи управління доступом до інформаційних ресурсів; теорії, методи та засоби забезпечення захисту інформації з обмеженим доступом.</p>
Орієнтація освітньої програми	<p>Освітньо-професійна, базується на загальнонаукових та практичних результатах в кібербезпеці і має прикладну орієнтацію напрямку інтеграції програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.</p>

Основний фокус освітньої програми та спеціалізації	<p>Загальна вища освіта в галузі інформаційних технологій з поглибленим вивченням теоретичних основ інформатики, та здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої обґрунтованості, технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.</p>
Особливості програми	<p>Освітньо-професійна програма зі спеціальності «Кібербезпека та захист інформації» передбачає вивчення теоретичних основ і сучасних технологій забезпечення кібербезпеки, захисту інформації, проєктування, впровадження, експлуатації та адміністрування захищених комп'ютерних систем, мереж і інформаційно-комунікаційних інфраструктур.</p> <p>Особливістю програми є підготовка фахівців, здатних реалізовувати повний життєвий цикл систем інформаційної та кібербезпеки: від аналізу загроз і ризиків, формування політик безпеки та проєктування архітектури захисту — до впровадження, моніторингу, супроводу та реагування на кіберінциденти. Програма орієнтована на опанування методів криптографічного та технічного захисту інформації, безпеки мереж і операційних систем, захисту програмного забезпечення, управління доступом, виявлення та запобігання кібератакам відповідно до національних і міжнародних стандартів у сфері кібербезпеки.</p>
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	<p>Фаховий молодший бакалавр з захисту та безпеки інформаційних систем (коди та назви класифікаційного угруповання професійних назв робіт згідно з Національним класифікатором України «Класифікатор професій ДК 003:2010» (затверджено і надано чинності наказом Держспоживстандарту України від 28.07.2010 №327 (зі змінами)):</p> <ul style="list-style-type: none"> - 3119 - технік (сфера захисту інформації); - 3121 - фахівець з інформаційних технологій. - 3439 - фахівець із організації інформаційної безпеки; - 3439 - фахівець із організації захисту інформації з обмеженим доступом - 4113 – кібероператор.
Подальше навчання	<p>Можливе продовження навчання за початковим рівнем (короткий цикл) та/або першим (бакалаврським) рівнем вищої освіти та набуття додаткових кваліфікацій в системі освіти дорослих, в тому числі післядипломної освіти.</p>
5 – Викладання та оцінювання	
Викладання та навчання	<p>Організація освітнього процесу здійснюється на основі студентоорієнтованого навчання, що передбачає заохочення здобувачів фахової передвищої освіти до ролі автономних і відповідальних суб'єктів освітнього процесу та створення освітнього середовища, орієнтованого на задоволення їх потреб та інтересів.</p> <p><i>Освітній процес здійснюється за такими формами:</i></p> <ul style="list-style-type: none"> • навчальні заняття; • самостійна робота, яка включає виконання індивідуальних завдань; • практична підготовка; • тематичні факультативи;

	<ul style="list-style-type: none"> • проблемні групи; • тематичні гуртки; • контрольні заходи, які включають атестацію здобувачів освіти. <p><i>Основні види навчальних занять:</i></p> <ul style="list-style-type: none"> • лекції; • лабораторні, практичні, семінарські; • тренінги, майстер-класи, круглі столи, конференції, залучення студентів до участі в проєктних роботах, конкурсах, олімпіадах, застосування інноваційних технологій дистанційного навчання, самостійне навчання на основі підручників та конспектів, консультацій з викладачами. <p><i>Дослідницька та інноваційна діяльність:</i></p> <p>Дослідницька діяльність може здійснюватися в межах виконання лабораторних та практичних робіт, написання рефератів, курсового та дипломного проєктування, участь в проблемних групах та гуртках, студентських конференціях, олімпіадах, конкурсах, хакатонах.</p> <p>Процес дослідницької діяльності включає: вибір теми, постановку мети і завдань дослідження, планування дослідження та вибір методів; пошук інформації, проведення дослідів, опитувань, створення графіків і діаграм; формулювання висновків, представлення результатів, аналіз своєї діяльності та самооцінка.</p> <p>Інноваційна діяльність здобувачів визначається як процес, що пов'язаний з одержанням, відтворенням і реалізацією новизни у сфері кібербезпеки та захисту інформації (пошук інноваційних ідей; розробка інноваційних продуктів в предметній діяльності та в системі викладання; заохочення творчих особистостей; позитивне сприйняття креативних ідей, нагромадження інноваційного потенціалу та розвиток інноваційної культури; формування іміджу закладу, який постійно впроваджує інновації, підтримує дух новаторства)</p> <p><i>Студентоцентризм</i></p> <p>Передбачає впровадження особистісно-орієнтованої технології навчання, для забезпечення всебічного розвитку особистості здобувача фахової передвищої освіти, враховуючи його індивідуальні особливості, здібності, інтереси, потреб, можливості, індивідуального профілю компетенцій.</p>
Оцінювання	<p>Усні та письмові екзамени; заліки; проведення модульних контрольних робіт; індивідуальне усне опитування; індивідуальне письмове опитування (самостійна робота, тестування); презентація результатів самостійної роботи (реферати, опитування); захист комплексних практичних індивідуальних завдань; захист курсових робіт; захист звітів про проходження практики. Атестація у формі кваліфікаційного іспиту.</p> <p>Оцінювання результатів навчання здобувачів фахової передвищої освіти проводиться за 100-бальною шкалою.</p>
6 – Програмні компетентності випускника	
Інтегральна компетентність	<p>Здатність вирішувати типові спеціалізовані задачі в галузі кібербезпеки, що вимагає застосування положень і методів відповідних наук та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях.</p>

Загальні компетентності	ЗК.01	Здатність застосовувати знання у практичних ситуаціях.
	ЗК.02	Знання та розуміння предметної області та розуміння професійної діяльності.
	ЗК.03	Здатність спілкуватися державною та іноземною мовами як усно, так і письмово.
	ЗК.04	Здатність вчитися та оволодівати сучасними знаннями.
	ЗК.05	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.06	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.
	ЗК.07	Здатність працювати в команді.
	ЗК.08	Здатність виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
	ЗК.09	Здатність використовувати інформаційні і комунікаційні технології.
	ЗК.10	Здатність діяти на основі етичних міркувань (мотивів), застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
	ЗК.11	Здатність діяти соціально відповідально та свідомо. Виявляти готовність до національного спротиву та захисту Батьківщини, усвідомлення суспільної значущості військової служби та повага до неї.
	ЗК.12	Здатність раціонально та ефективно організовувати працю на робочому місці.
Спеціальні (фахові, предметні) компетентності	СК.01	Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
	СК.02	Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
	СК.03	Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки.
	СК.04	Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
	СК.05	Здатність до розробки та використання програмних та програмно-апаратних засобів.
	СК.06	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
	СК.07	Здатність застосовувати методи та засоби криптографічного захисту інформації.

	СК.08	Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
	СК.09	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 вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
	СК.11	Здатність застосовувати теоретичні знання та практичні навички з організації та функціонування сучасних операційних систем, уміння створювати та використовувати безпечне програмне забезпечення для керування обчислювальними ресурсами в багатокористувацьких операційних системах.
	СК.12	Здатність вибору захищених хмарних платформ та сервісів, безпечного розгортання на них, інтегрування, адміністрування і супроводу інформаційних систем.
	СК.13	Здатність оформляти отримані робочі результати у вигляді презентацій, звітів.
	СК.14	Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення.
	СК.15	Здатність здійснювати вибір, захист, розгортати, інтегрувати, діагностувати, адмініструвати, експлуатувати комп'ютерні системи та мережі, мережеві ресурси, елементи та складові інтернету речей, сервіси та інфраструктуру організації.
	СК.16	Здатність створювати, впроваджувати, адмініструвати та здійснювати захист баз даних і знань з використанням сучасних методів, технологій та систем керування базами даних.
	СК.17	Здатність застосовувати методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу в умовах супроводження та експлуатації програмних систем і комплексів.
7 – Програмні результати навчання		
РН.01	Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	
РН.02	Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	
РН.03	Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.	
РН.04	Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	
РН.05	Аналізувати, аргументувати, приймати рішення при розв'язанні спеціалізованих задач і практичних завдань у професійній діяльності, відповідати за прийняті рішення.	

PH.06	Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
PH.07	Застосовувати і адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
PH.08	Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
PH.09	Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
PH.10	Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
PH.11	Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації.
PH.12	Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
PH.13	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 в цілому.
PH.14	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.
PH.15	Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
PH.16	Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
PH.17	Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
PH.18	Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
PH.19	Розуміти сутність, правові засади та складові національного спротиву, демонструвати готовність до захисту національних інтересів, незалежності та територіальної цілісності України, зокрема шляхом протидії кіберзагрозам та інформаційно-психологічним операціям у сфері кібербезпеки.

8 – Ресурсне забезпечення реалізації програми

<p style="text-align: center;">Кадрове забезпечення</p>	<p>Освітній процес освітньо-професійної програми «Кібербезпека та захист інформації» спеціальності F5 Кібербезпека та захист інформації забезпечений педагогічними працівниками, необхідними для реалізації освітньої програми.</p> <p>Кожний освітній компонент освітньо-професійної програми «Кібербезпека та захист інформації» забезпечений педагогічними працівниками з урахуванням їх освітньої кваліфікації. Відповідність кваліфікації визначається спеціальністю згідно з документом про вищу освіту, науковий ступінь, або досвідом практичної роботи за відповідним фахом не менше п'яти років.</p> <p>Усі педагогічні працівники, що забезпечують освітньо-професійну програму відповідають профілю і напрямку дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. В процесі організації освітнього процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи та постійно підвищують рівень професійної компетентності.</p> <p>З метою підвищення фахового рівня всі педагогічні працівники у встановлені законодавством терміни, проходять підвищення кваліфікації.</p>
<p style="text-align: center;">Матеріально-технічне забезпечення</p>	<p>Навчальні приміщення дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньо-професійною програмою «Кібербезпека та захист інформації», оскільки мають достатню кількість комп'ютеризованих та спеціалізованих робочих місць та обладнанні необхідними сучасними технічними засобами.</p>
<p style="text-align: center;">Інформаційне та навчально-методичне забезпечення</p>	<p>Інформаційне: забезпеченість бібліотеки підручниками і посібниками, фаховими періодичними виданнями відповідного профілю; наявність офіційного вебсайту та електронних ресурсів дисциплін.</p> <p>Навчально-методичне:</p> <ul style="list-style-type: none"> - освітньо-професійна програма (ОПП); - навчальний план; - робочий навчальний план; - робочі програми освітніх компонент; - програми проходження практики; - методичні вказівки, тематика курсових робіт; - завдання для самостійної роботи студентів та методичні рекомендації щодо їх виконання; - засоби діагностики і контролю якості навчання (питання до заліків, питання до іспитів, пакети комплексних контрольних робіт (ККР) перевірки знань з дисциплін, критерії оцінки знань і умінь студентів.

9 – Академічна мобільність	
Національна кредитна мобільність	<p>Двосторонні угоди між Відокремленим структурним підрозділом «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича» та іншими закладами фахової передвищої освіти України про академічну мобільність.</p> <p>URL: https://college.chnu.edu.ua/koledzh/akademichna-mobilnist/</p>
Міжнародна кредитна мобільність	<p>Кредити, отримані в закладах освіти інших країн, можуть зараховуватися відповідно до довідки про академічну мобільність, а також за умов відповідності їх набутим компетентностям, що регламентується <u>Положенням про академічну мобільність у Відокремленому структурному підрозділі «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича»</u>.</p>
Навчання іноземних здобувачів вищої освіти	Не передбачає

2. Перелік компонентів освітньо-професійної/наукової програми та їх логічна послідовність

2.1. Перелік компонентів освітньо-професійної програми «Кібербезпека та захист інформації»

Код О/К	Освітні компоненти освітньо-професійної програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційний іспит)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК.01	Історія України	4,0	Іспит
ОК.02	Соціологія	3,0	Залік
ОК.03	Економічна теорія	3,0	Залік
ОК.04	Основи національного спротиву	3,0	Залік
ОК.05	Основи правознавства	3,0	Залік
ОК.06	Іноземна мова за професійним спрямуванням	14,0	Іспит
ОК.07	Українська мова за професійним спрямуванням	2,0	Залік
ОК.08	Громадське здоров'я	2,0	Залік
ОК.09	Фізичне виховання	7,0	Залік
ОК.10	Інформаційний пошук у кібербезпеці	3,0	Залік
ОК.11	Комп'ютерне проєктування	3,0	Залік
ОК.12	Теорія ймовірностей і математична статистика	3,0	Іспит
ОК.13	Фізика	7,0	Іспит
ОК.14	Алгоритмізація та програмування	9,0	Іспит
ОК.15	Об'єктно орієнтоване програмування	6,0	Іспит
ОК.16	Спеціалізовані мови програмування	6,0	Іспит
ОК.17	Вища математика	6,0	Залік
ОК.18	Комп'ютерна дискретна математика	3,0	Залік
ОК.19	Комп'ютерні мережі	6,0	Іспит
ОК.20	Основи теорії інформації та кодування	4,0	Іспит
ОК.21	Теорія електричних та магнітних кіл	3,0	Залік
ОК.22	Комп'ютерна схемотехніка та архітектура комп'ютерів	4,0	Іспит
ОК.23	Операційні системи	4,0	Іспит

ОК.24	Методи та засоби захисту інформації	4,0	Іспит
ОК.25	Сигнали і процеси в системах захисту інформації	3,0	Залік
ОК.26	Основи криптографії	4,0	Іспит
ОК.27	Організація та безпека баз даних	3,0	Залік
ОК.28	Технічний захист інформації	4,0	Залік
ОК.29	Основи кібербезпеки та захист інформації	5,0	Іспит
ОК.30	Технології інтернету речей та їх захист (IoT)	3,0	Залік
ОК.31	Курсова робота (3 курс)	3,0	Захист
ОК.32	Курсова робота (4 курс)	3,0	Захист
ОК.33	Кваліфікаційний іспит	1,0	Іспит
Практична підготовка			
ОК.34	Навчальна практика з інформаційної безпеки (4 сем., 2 тижні)	3,0	Залік
ОК.35	Навчальна практика (5 сем., 2 тижні)	3,0	Залік
ОК.36	Виробнича практика (6 сем., 4 тижні)	6,0	Іспит
ОК.37	Виробнича практика (8 сем., 6 тижнів)	9,0	Іспит
Загальний обсяг обов’язкових освітніх компонентів:		162,0	
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК.01	Вибіркова освітня компонента	3,0	Залік
ВК.02	Вибіркова освітня компонента	3,0	Залік
ВК.03	Вибіркова освітня компонента	3,0	Залік
ВК.04	Вибіркова освітня компонента	3,0	Залік
ВК.05	Вибіркова освітня компонента	3,0	Залік
ВК.06	Вибіркова освітня компонента	3,0	Залік
Загальний обсяг вибірових освітніх компонентів:		18,0	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		180	

Відповідно до Пункту 17 Статті 54 Закону України «Про фахову передвищу освіту» здобувачу фахової передвищої освіти гарантовано право участі у формуванні індивідуального навчального плану, вибір навчальних дисциплін у межах, передбачених відповідною освітньо-професійною програмою та навчальним планом, в обсязі, що становить не менше 10 відсотків (18 кредитів ЄКТС) загальної кількості кредитів ЄКТС, передбачених для освітньо-професійної програми «Кібербезпека та захист інформації».

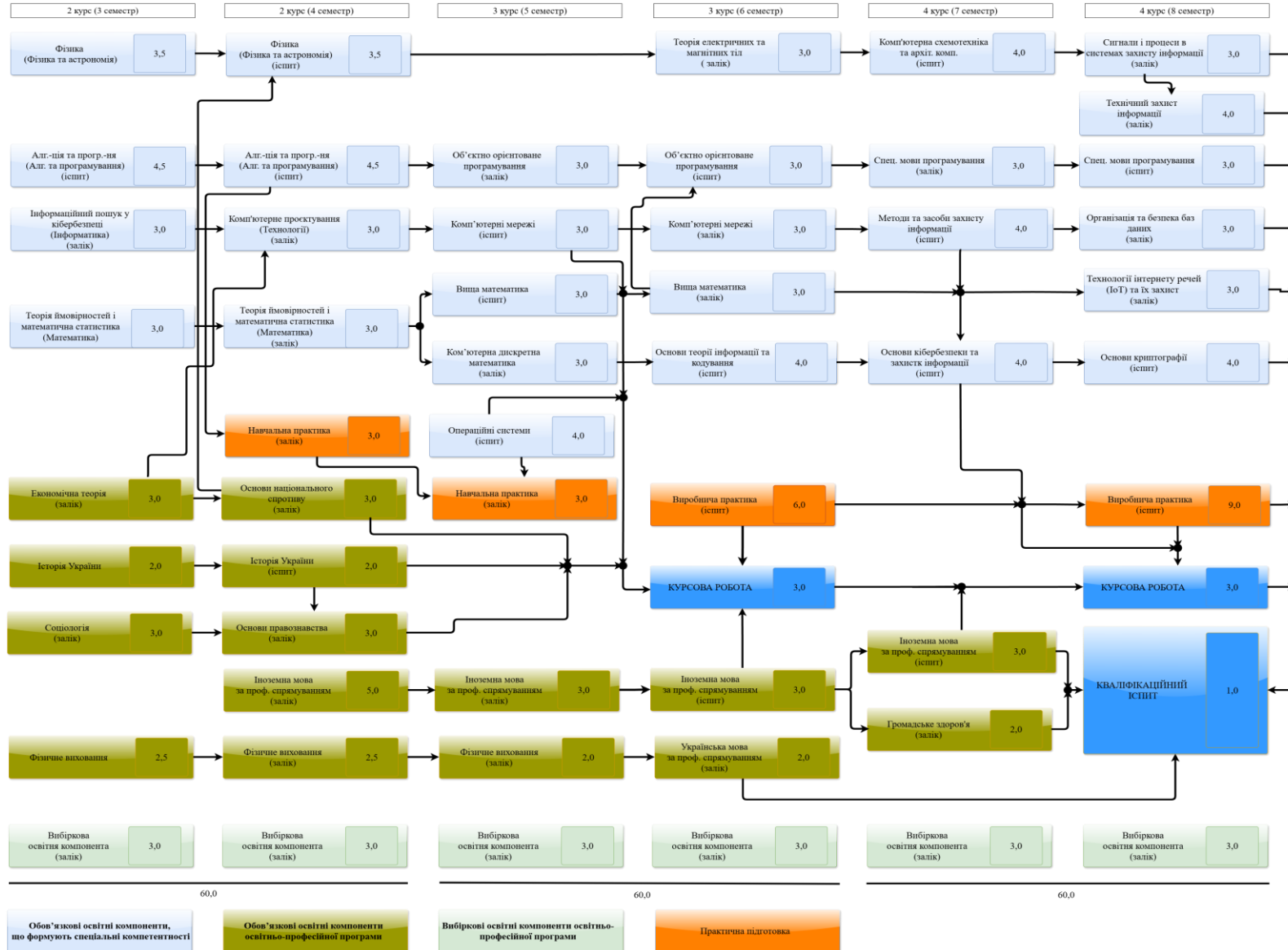
Здобувачі освіти мають можливість обирати дисципліни з переліку вибірових компонентів із [загального каталогу вибірових дисциплін ВСП «Фаховий коледж ЧНУ»](#) чи [каталогу загальноуніверситетських вибірових дисциплін Чернівецького національного університету імені Юрія Федьковича](#) а також з [каталогу вибірових дисциплін, що формується випускаючою цикловою комісією](#). Такий підхід до вибору сприяє індивідуалізації освітньої траєкторії та поглибленню професійних компетентностей. Перелік дисциплін, із якого здобувачі освіти здійснюватимуть вільний вибір, формується цикловими комісіями ВСП «Фаховий коледж ЧНУ» на кожний новий навчальний рік та доводиться до відома студентів. Вибір проводиться відповідно до [Положення «Про порядок реалізації студентами Відокремленого структурного підрозділу «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича» права на вільний вибір навчальних дисциплін»](#).

2.2. Розподіл змісту освітньо-професійної програми за групами компонентів

№ за\п	Цикл підготовки	Обсяг навчального навантаження (кредитів ECTS, %)	
		Кредити ECTS	відсотки від обсягу кредитів
1.	Загальний обсяг обов'язкових компонент	162,0	90,00
2.	Загальний обсяг вибірових компонент	18,0	10,00
3.	Загальний обсяг освітньо-професійної програми	180	100

2.3. Структурно-логічна схема

ОП «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»



3. Форма атестації здобувачів фахової передвищої освіти

Атестація здобувачів фахової передвищої освіти освітньо-професійної програми **«Кібербезпека та захист інформації»** спеціальності **F5 Кібербезпека та захист інформації** проводиться у вигляді кваліфікаційного іспиту.

Кваліфікаційний іспит спрямований на перевірку досягнень результатів навчання, визначених освітньо-професійною програмою «Кібербезпека та захист інформації». До складання кваліфікаційного іспиту допускаються здобувачі освіти, які виконали всі вимоги індивідуального навчального плану студента. Кваліфікаційний іспит проводиться у повній відповідності до програми атестації.

Атестацію здійснює екзаменаційна комісія. Відокремлений структурний підрозділ «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича» на підставі рішення екзаменаційної комісії присуджує особі, яка продемонструвала відповідність результатів навчання вимогам освітньо-професійної програми «Кібербезпека та захист інформації», освітньо-професійний ступінь фахового молодшого бакалавра та присвоює освітню кваліфікацію – **фаховий молодший бакалавр із кібербезпеки та захисту інформації**. Особі, яка успішно виконала освітньо-професійну програму, видають диплом фахового молодшого бакалавра. Атестація здійснюється відкрито і публічно.

4. Вимоги до системи внутрішнього забезпечення якості фахової передвищої освіти

Концептуальні засади системи внутрішнього забезпечення якості освіти, процедури розробки, затвердження, моніторингу та періодичного перегляду освітньо-професійної програми «Кібербезпека та захист інформації» передбачено Положенням про систему внутрішнього забезпечення якості освітньої діяльності та якості фахової передвищої освіти у Відокремленому структурному підрозділі «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича».

5. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компетен- тності	Освітні компоненти																																						
	ОК.01	ОК.02	ОК.03	ОК.04	ОК.05	ОК.06	ОК.07	ОК.08	ОК.09	ОК.10	ОК.11	ОК.12	ОК.13	ОК.14	ОК.15	ОК.16	ОК.17	ОК.18	ОК.19	ОК.20	ОК.21	ОК.22	ОК.23	ОК.24	ОК.25	ОК.26	ОК.27	ОК.28	ОК.29	ОК.30	ОК.31	ОК.32	ОК.33	ОК.34	ОК.35	ОК.36	ОК.37		
ЗК.01		+	+							+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК.02			+	+	+					+	+		+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК.03						+	+																									+	+	+					
ЗК.04		+	+	+	+	+	+	+		+	+		+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК.05	+	+		+	+																+				+				+	+									
ЗК.06	+	+			+					+												+							+	+									
ЗК.07										+	+		+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК.08	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК.09										+	+									+				+				+											
ЗК.10	+	+			+					+																		+	+	+		+	+	+	+	+	+	+	+
ЗК.11	+	+		+					+																					+			+	+	+	+	+	+	+
ЗК.12							+																										+	+	+	+	+	+	+
СК.01				+	+					+															+	+	+		+	+		+	+	+	+	+	+	+	+
СК.02				+															+					+			+	+	+	+									
СК.03			+							+																		+	+	+	+								
СК.04										+									+	+				+			+	+		+	+								
СК.05														+	+	+						+										+	+	+	+	+	+	+	+
СК.06										+					+	+			+	+				+			+		+	+	+	+	+	+	+	+	+	+	+
СК.07																								+	+	+		+	+		+	+		+	+	+	+	+	+
СК.08				+															+					+	+			+	+		+	+	+	+	+	+	+	+	+
СК.09				+															+		+	+		+	+			+			+	+	+	+	+	+	+	+	+
СК.10																+			+					+				+	+		+	+	+	+	+	+	+	+	+
СК.11														+	+	+							+									+	+	+	+	+	+	+	+
СК.12															+	+			+								+					+	+	+	+	+	+	+	+
СК.13									+					+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
СК.14										+			+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
СК.15																			+			+	+	+				+	+	+									
СК.16															+	+							+				+				+	+	+	+	+	+	+	+	+
СК.17															+	+							+	+			+		+	+	+	+							

6. Матриця забезпечення результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

Програмні результати навчання	Освітні компоненти																																						
	ОК.01	ОК.02	ОК.03	ОК.04	ОК.05	ОК.06	ОК.07	ОК.08	ОК.09	ОК.10	ОК.11	ОК.12	ОК.13	ОК.14	ОК.15	ОК.16	ОК.17	ОК.18	ОК.19	ОК.20	ОК.21	ОК.22	ОК.23	ОК.24	ОК.25	ОК.26	ОК.27	ОК.28	ОК.29	ОК.30	ОК.31	ОК.32	ОК.33	ОК.34	ОК.35	ОК.36	ОК.37		
PH.01	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
PH.02						+				+	+			+	+	+				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
PH.03	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
PH.04			+							+	+			+	+	+												+	+	+	+	+	+	+	+	+	+	+	+
PH.05										+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
PH.06				+						+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
PH.07										+		+	+				+	+		+	+	+		+	+	+		+			+	+	+	+	+	+	+	+	
PH.08												+	+				+	+		+	+	+			+			+			+	+	+	+	+	+	+	+	+
PH.09				+	+															+				+			+		+	+									+
PH.10											+									+				+	+	+	+	+	+	+								+	
PH.11			+		+											+											+		+	+									+
PH.12					+					+	+			+	+	+			+	+			+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+
PH.13											+			+	+	+							+				+	+	+	+	+	+	+	+	+	+	+	+	+
PH.14																							+	+	+			+	+		+	+	+	+	+	+	+	+	+
PH.15				+						+														+				+	+			+	+	+	+	+	+	+	+
PH.16																+						+	+					+	+			+	+	+	+	+	+	+	+
PH.17																				+					+		+	+	+			+	+	+	+	+	+	+	+
PH.18																				+					+		+	+	+			+	+	+	+	+	+	+	+
PH.19	+	+		+	+																			+					+			+	+	+	+	+	+	+	+

ВІДОМОСТІ
про членів робочої (проектної) групи ОПП «Кібербезпека та захист інформації»,
спеціальності **F5 Кібербезпека та захист інформації**

Керівник робочої (проектної) групи	
Ім'я, по батькові, ПРИЗВИЩЕ	Гресь Олександр Володимирович
Найменування посади	Викладач (за суміщенням), доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича
Найменування закладу, який закінчив (рік закінчення, спеціальність, кваліфікація згідно з документом про вищу освіту)	Чернівецький національний університет імені Юрія Федьковича, 2008, спеціальність «Захист інформації з обмеженим доступом та автоматизація її обробки», кваліфікація – магістр інформаційної безпеки
Кваліфікаційна категорія, пед. звання, науковий ступінь, вчене звання	Спеціаліст вищої категорії, кандидат технічних наук (спеціальність 05.13.21 – Системи захисту інформації), доцент
Педагогічний стаж (повних років)	15 років
Підвищення кваліфікації за фахом (найменування закладу)	<p>1. Підвищення кваліфікації молодих вчених та викладачів закладів вищої освіти Тема: «Нові горизонти зростання сучасного викладача-науковця» – 30 год. (1 кредит ЄКТС). Свідоцтво про підвищення кваліфікації ПК-РМВ № 99/2025 від «11» квітня 2025 р.</p> <p>2. Підвищення кваліфікації на платформі Prometheus “Академічна доброчесність: онлайн курс для викладачів” – 60 год. (2 кредити ECTS). Сертифікат від 12.12.2024 р.</p> <p>3. Lublin University of Technology, “Lubelska Politechnica”, Poland. Traineeship: “New knowledge in the development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring”, 180 hours / 6 credits ECTS, Certificate № 3-2023-ChNU, 06-05-2023.</p>

Члени робочої (проектної) групи	
Ім'я, по батькові, ПРИЗВИЩЕ	Рождественська Маргарита Григорівна
Найменування посади	Викладач (за суміщенням), доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича
Найменування закладу, який закінчив (рік закінчення, спеціальність, кваліфікація згідно з документом про вищу освіту)	<p>1. Чернівецький державний університет імені Юрія Федьковича, 1992, спеціальність «Радіотехніка», кваліфікація – радіоінженер;</p> <p>2. Харківський національний університет внутрішніх справ, 2025, спеціальність «Кібербезпека та захист інформації», кваліфікація – магістр з кібербезпеки та захисту інформації.</p>
Кваліфікаційна категорія, педагогічне звання, науковий ступінь, вчене звання	Спеціаліст вищої категорії, кандидат фізико-математичних наук (спеціальність 01.04.10 – фізика напівпровідників і діелектриків), доцент
Педагогічний стаж (повних років)	27 років
Підвищення кваліфікації за фахом (найменування закладу)	<p>1. 07.07.2025 – 28.08.2025. Курс SoftServe Academy Tech Summer for Educators: Big Data Edition. Сертифікат RB № 26455/2025 від 28.08.2025 р. 60 год. / 2 кред.</p> <p>2. 27.01.2025 – 09.02.2025. Чернівецький національний університет імені Юрія Федьковича. Програма підвищення кваліфікації науково-пед. працівників ЗВО «Розвиток професійно-особистісного потенціалу викладача ЗВО: психолого-педагогічні, дослідницькі, цифрові компетентності». Сертифікат ПК-НПП-022025 № 130 від 10.02.2025 р. 90 год. / 3 кред.</p> <p>3. 07.03.2024 – 02.04.2024. Курс SoftServe Academy CLOUD ENVIRONMENT CONFIGURATION AND SECURITY (Налаштування та безпека хмарних середовищ). Сертифікат OV № 17561/2024 від 02.04.2024 р. 120 год. / 4 кред.</p>

Ім'я, по батькові, ПРИЗВИЩЕ	Косован Григорій Васильович
Найменування посади	Викладач (за суміщенням), асистент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича
Найменування закладу, який закінчив (рік закінчення, спеціальність, кваліфікація згідно з документом про вищу освіту)	Чернівецький національний університет імені Юрія Федьковича, 2008, спеціальність «Захист інформації з обмеженим доступом та автоматизація її обробки», кваліфікація – магістр інформаційної безпеки
Кваліфікаційна категорія, педагогічне звання, науковий ступінь, вчене звання	Спеціаліст вищої категорії, кандидат технічних наук (спеціальність 05.13.21 – Системи захисту інформації)
Педагогічний стаж (повних років)	12 років
Підвищення кваліфікації за фахом (найменування закладу)	<p>1. Підвищення кваліфікації (стажування) в Чернівецькому національному університеті імені Юрія Федьковича (м. Чернівці, Україна), 2024 р., свідоцтво ПК-РМВ № 52/2024 – 30 год.</p> <p>2. Підвищення кваліфікації (стажування) в Тернопільському національному технічному університеті імені Івана Пулюя (м. Тернопіль, Україна), 2021 р., свідоцтво ПК № 5408102/001738-21 – 180 год.</p>
Ім'я, по батькові, ПРИЗВИЩЕ	Ташук Роман Юрійович
Найменування посади	Викладач
Найменування закладу, який закінчив (рік закінчення, спеціальність, кваліфікація згідно з документом про вищу освіту)	Чернівецький національний університет імені Юрія Федьковича, 2019, спеціальність «Фізика та астрономія», кваліфікація - магістр фізики та астрономії
Кваліфікаційна категорія, педагогічне звання, науковий ступінь, вчене звання	Спеціаліст вищої категорії, доктор філософії (спеціальність 104 Фізика та астрономія)
Педагогічний стаж (повних років)	2 роки

<p>Підвищення кваліфікації за фахом (найменування закладу)</p>	<ol style="list-style-type: none"> 1. Магістрант 1-го року навчання за ОПП «Кибербезпека» спеціальності F5 Кибербезпека та захист інформації Чернівецького національного університету імені Юрія Федьковича, індивідуальний навчальний план здобувача освіти, 2025 р., 30 кредитів ЄКТС; 2. Сертифікат підвищення кваліфікації з курсу «Небайдужі: базові емоційні потреби та соціальна взаємодія», платформа Prpmetheus, № c93f69983ff24b0c967d75cabcc92fсе, 30.01.2024 р., 15 годин (0,5 кредитів ЄКТС); 3. Захист наукової дисертації та здобуття ступеня доктора філософії з спеціальності 104 Фізика та астрономія, 11 грудня 2023 р., Диплом Н23 №001703.
--	--