МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД

«Ужгородський національний університет»

ЗАТВЕРДЖЕНО
Протокол Вченої ради
ДВНЗ «Ужгородський національний університет»
07. 03. 2024 р. № 3

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

кваліфікація: Магістр з кібербезпеки та захисту інформації

УВЕДЕНО В ДІЮ
Наказ ректора ДВНЗ «Ужгородський національний університет»
18. 03. 2024 р. №229/01-04

Ужгород - 2024

АРКУШ ПОГОДЖЕННЯ
освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»

1. **Ректор** **Володимир СМОЛАНКА**

07.02. 2024 р.

2. **Гарант освітньо-професійної програми** **Василь РІЗАК**

21.02. 2024 р.

3. **Декан фізичного факультету** **Володимир ЛАЗУР**

21.02. 2024 р.

4. **Керівник робочої групи** **Василь РІЗАК**

21.02. 2024 р.

5. **Начальник навчальної частини** **Анатолій ШТИМАК**

27.03. 2024 р.

ПЕРЕДМОВА

Освітньо-професійна програма "Безпека інформаційнцх і комунікаційних систем» підготовки здобувачів другого (магістерського) рівня вищої освіти спеціальності 125 Кібербезпека та захист інформації розроблена згідно з вимогами Закону України «Про вищу освіту» та у відповідності до стандарту вищої освіти, затвердженого й уведеного в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332, із врахуванням професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку України 25 листопада 2022 року № 715. Програма відповідає другому (магістерському) рівню вищої освіти та сьомому кваліфікаційному рівню за Національною рамкою кваліфікації.

Розроблено робочою групою освітньо-професійної програми у складі:

Гарант освітньої програми: Різак Василь Михайлович, доктор фіз.-мат. наук, професор, завідувач кафедри твердотільної елекгроніки та інформаційної безпеки ДВНЗ «Ужгородський національний університет».

Члени робочої групи:

1. Пагіря Михайло Михайлович, доктор фіз.-мат. наук, професор кафедри твердотільної електроніки та інформаційної безпеки
2. Пригара Михайло Петрович, кандидат техн. наук, доцент кафедри технології машинобудування
3. Чобаль Олександр Ілліч, кандидат фіз.-мат. наук, доцент кафедри твердотільної електроніки та інформаційної безпеки
4. Маркевич Петро Вікторович, начальник Управління Державної служби спеціального зв'язку та захисту інформації України в Закарпатській області.
5. Старцев Андрій Олександрович, здобувач другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації.

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Корченко Олександр Григорович, завідувач кафедри безпеки інформаційних технологій НАУ, Заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, доктор технічних наук (05.13.21–Системи захисту інформації), професор.
2. Танчинець Михайло Михайлович, начальник відділу протидії кіберзлочинам в Закарпатській області Департаменту кіберполіції Національної поліції України.

Профіль освітньої програми
«Безпека інформаційних і комунікаційних систем» за спеціальністю
125 Кібербезпека та захист інформації

Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Державний вищий навчальний заклад «Ужгородський національний університет» Фізичний факультет Кафедра твердотільної електроніки та інформаційної безпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти: магістр. Освітня кваліфікація: магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС. Термін навчання 1 рік і 4 місяців.
Наявність акредитації	НАЗЯВО. Сертифікат про акредитацію освітньої програми № 6529 від 14.12.2023 р. Строк дії сертифікату до 01.07.2029 р.
Цикл/рівень	Національна рамка кваліфікацій України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень.
Передумови	Наявність першого (бакалаврського) рівня вищої освіти (або ОКР спеціаліста). Умови вступу визначаються «Правилами прийому до Ужгородського національного університету»
Мова(и) викладання	Українська
Термін дії освітньої програми	До чергового перегляду відповідно до терміну дії сертифіката про акредитацію
Інтернет-адреса постійного розміщення опису освітньої програми	https://www.uzhnu.edu.ua/uk/infocentre/15068
Мета освітньої програми	
Навчання та підготовка фахівців, які мають знання, вміння та навички щодо впровадження та застосування сучасних технологій кібербезпеки, а також розробки технологій і засобів захисту інформації та проектування систем й комплексів забезпечення кібербезпеки; фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.	

Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація(за наявності)	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації
Орієнтація освітньої програми	Освітньо-професійна програма орієнтована на підготовку фахівців, здатних розв'язувати складні задачі і проблеми у галузі професійної діяльності, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
Основний фокус освітньої програми	Загальна вища освіта другого (магістерського) рівня за спеціальністю 125 Кібербезпека та захист інформації. Акцентована на розвиток здатності розв'язувати складні задачі і проблеми кібербезпеки, зокрема безпеки інформаційних та комунікаційних систем, що передбачає проведення досліджень та/або здійснення інновацій. Рекомендовані дисципліни професійно-практичної підготовки спрямовані на формування комплексного підходу до безпеки інформаційно-комунікаційних систем та кіберзахисту критичної інфраструктури. КЛЮЧОВІ СЛОВА: кібербезпека, захист інформації, інформаційно-комунікаційні системи, розподілені системи, криптографічний захист інформації, кіберінциденти, критична інфраструктура
Особливості програми	Освітня програма передбачає: - узагальнення професійних навиків та знань, отриманих здобувачами першого рівня вищої освіти в сфері кібербезпеки та формування комплексного підходу до безпеки інформаційно - комунікаційних систем та кіберзахисту критичної інфраструктури; - орієнтованість змісту обов'язкових та вибіркових компонент на професійний стандарт "Фахівець сфери захисту інформації" та передові досягнення в IT- галузі. - поглиблене розуміння здобувачами принципів та особливостей функціонування розподілених інформаційно-комунікаційних систем, в тому числі і в критичній інфраструктурі. - залучення до викладацької діяльності керівників та професіоналів різних суб'єктів

	національної системи кібербезпеки та представників ІТ-бізнесу. Освітня програма забезпечує підготовку професіоналів, здатних: - організовувати і підтримувати комплекс заходів щодо забезпечення інформаційної та/або кібербезпеки; - забезпечувати функціонування об'єктів критичної інфраструктури, державних установ та органів місцевого самоврядування у контексті регіонального транскордонного співробітництва та умовах ризику стороннього кібернетичного впливу; - надавати консультативні послуги і технічну допомогу з питань технічного, криптографічного захисту інформації та кіберзахисту; - забезпечувати захищеність інформаційних і комунікаційних систем транскордонної та регіональної інфраструктури.
Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Магістри з кібербезпеки та захисту інформації, які здобули освіту за даною ОПП, є фахівцями у сфері безпеки інформаційних технологій, захисту комп'ютерних систем та мереж, організації захисту інформації, інформаційної та кібербезпеки. Випускники можуть займати посади згідно до Національного класифікатору професій ДК 003:2010 (із змінами) відповідно до Професійних стандартів, затверджених Адміністрацією Держспецзв'язку України.
Подальше навчання	Випускник другого магістерського рівня вищої освіти освітньої програми " Безпека інформаційних і комунікаційних систем" може продовжити навчання за програмою третього (освітньо- наукового) рівня вищої освіти для отримання наукового ступеня доктора філософії. Навчання за перехресним вступом, а також отримання додаткової післядипломної освіти.
Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та лабораторні заняття, самонавчання, проектно-орієнтоване навчання, консультації із науково-педагогічними

	співробітниками, проведення наукових досліджень, підготовка кваліфікаційної роботи. Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуально-творчий підхід, навчання через науково-дослідну та переддипломну практики.
Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної навчальної діяльності, спрямовані на опанування навчального навантаження з освітньої програми: поточні контроль та оцінювання, поетапний, модульний, підсумковий контроль; екзамени; заліки, презентації, диференційований залік з науково-дослідної та переддипломної практик, кваліфікаційна робота із захистом в ЕК. Проміжкове та підсумкове оцінювання знань відбувається на засадах студентоорієнтованого особистісного підходу з використанням сучасних методик та практик. Оцінювання знань здобувачів вищої освіти відбувається згідно з Положенням про організацію освітнього процесу в Державному вищому навчальному закладі «Ужгородський національний університет» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357) , Положенням про порядок та методику проведення семестрових (курсових) екзаменів і заліків в Ужгородському національному університеті (**https://www.uzhnu.edu.ua/uk/infocentre/get/5952**), Положенням про атестацію здобувачів вищої освіти та екзаменаційну комісію у Державному вищому навчальному закладі «Ужгородський національний університет» (https://www.uzhnu.edu.ua/uk/infocentre/get/11070) з дотриманням норм академічної доброчесності відповідно до Положення про академічну доброчесність в Ужгородському національному університеті (**https://www.uzhnu.edu.ua/uk/infocentre/get/12223**). Перезарахування кредитів відбувається на основі Положення про визнання (перезарахування) кредитів ЄКТС для учасників

	програм академічної мобільності у Державному вищому навчальному закладі «Ужгородський національний університет» (**https://www.uzhnu.edu.ua/uk/infocentre/get/20131**). Процедура оцінювання здобувачів вищої освіти також враховує результати неформальної освіти згідно Положення про порядок визнання Державному вищому навчальному закладі «Ужгородський національний університет» результатів навчання, здобутих у неформальній освіті (**https://www.uzhnu.edu.ua/uk/infocentre/get/22966**). Наявна чітка процедура розгляду апеляцій здобувачів вищої освіти, яка описана в Положенні про порядок застосування заходів з врегулювання конфліктів та спорів (суперечок) у діяльності співробітників та здобувачів вищої освіти Державного вищого навчального закладу «Ужгородський національний університет» (**https://www.uzhnu.edu.ua/uk/infocentre/get/22964**) та Положенні про порядок оскарження результатів (апеляція) оцінювання в Державному вищому навчальному закладі «Ужгородський національний університет» (https://www.uzhnu.edu.ua/uk/infocentre/get/22967)
Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність діяти соціально відповідально та громадсько свідомо. КЗ-6. Здатність спілкуватися з представниками інших професійних груп різного рівня (з

	експертами з інших галузей знань/видів економічної діяльності).
Загальні компетентності (ЗК) згідно професійного стандарту «Фахівець сфери захисту інформації»	ЗК.01. Здатність діяти соціально відповідально та громадсько свідомо. ЗК.02. Здатність застосовувати знання у практичних ситуаціях, розв'язувати завдання/задачі та практичні проблеми у професійній діяльності. ЗК.03. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК.04. Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим. ЗК.05. Здатність до адаптації та дії в новій ситуації. ЗК.06. Здатність до вибору стратегії спілкування, працювати в команді. ЗК.07. Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.
Фахові компетентності (ФК)	ФК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою

	організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. ФК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ФК8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Професійні компетентності (за трудовою дією або групою трудових дій) згідно професійного стандарту «Фахівець сфери захисту інформації»	Б4. Здатність проводити оцінку відповідності (державну експертизу) засобів криптографічного захисту інформації. Д1. Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації. Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо систем технічного та криптографічного захисту інформації. Е1. Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки. Е2. Здатність взаємодіяти із керівництвом і фахівцями технологічних та інших підрозділів підприємства/організації з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту. Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень. Е4. Здатність надавати консультативні послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту.
Програмні результати навчання	
Результати навчання (РН)	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної

	безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики

	інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18.Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту,

	розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. РН24. Володіти методиками аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно-комунікаційних системах. РН25. Надавати консультативні послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту.
Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та

	вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають Ліцензійним умовам провадження освітньої діяльності на другому (магістерському) рівні вищої освіти. Склад групи освітньої програми, професорсько-викладацький склад, що задіяний до викладання навчальних дисциплін постійно проходять стажування та підвищення кваліфікації, що відповідає Положенню про підвищення кваліфікації та стажування педагогічних та науково-педагогічних працівників ДВНЗ "УжНУ" . https://www.uzhnu.edu.ua/uk/infocentre/get/5950.
Матеріально-технічне забезпечення	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, лабораторіями, мультимедійним обладнанням, устаткуванням, контрольно- вимірювальними приладами необхідними для виконання навчальних планів. Засоби обчислювальної техніки з прикладним та спеціалізованим програмним забезпеченням, спеціальні радіовимірювальні пристрої, засоби технічного захисту інформації, спеціалізовані апаратно-програмні комплекси. Наявна вся необхідна соціально-побутова інфраструктура. Для проведення практичних і лабораторних робіт, інформаційного пошуку та обробки результатів наявний кіберполігон кафедри ТЕІБ та спеціалізовані комп'ютерні класи факультету з необхідним програмним забезпеченням та необмежено відкритим доступом до Інтернет-мережі. Також на основі Меморандуму про співпрацю з ДССЗЗІ України студенти можуть пройти навчання в навчальному центрі UA30 та вдосконалити свої навички, відпрацьовуючи сценарії реагування на кібератаки на спеціальних тренажерах.
Інформаційне та навчально- методичне забезпечення	– офіційний веб-сайт http://www.uzhnu.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти;

	– необмежений доступ до мережі Інтернет; – фонди та електронних каталогів наукової бібліотеки ДВНЗ «УжНУ», а також до електронного репозитарію ДВНЗ «УжНУ» (https://dspace.uzhnu.edu.ua/jspui/) де містяться навчально-методичні матеріали з дисциплін навчального плану; – наукова бібліотека, читальні зали; – навчальні і робочі плани; – графіки навчального процесу; –дидактичні матеріали для самостійної та індивідуальної роботи студентів з дисциплін, програми практик; – методичні вказівки щодо виконання кваліфікаційних робіт; – віртуальне навчальне середовище Moodle (https://e-learn.uzhnu.edu.ua/.
Академічна мобільність	
Національна кредитна мобільність	Академічна мобільність студентів здійснюється на основі двосторонніх угод, укладених між ДВНЗ «Ужгородським національним університетом» та закладами вищої освіти України.
Міжнародна кредитна мобільність	Відповідно до Положення про академічну мобільність студентів у ДВНЗ «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/21269 , встановлено загальний порядок організації академічної мобільності студентів. Здійснюється згідно програми міжнародної академічної мобільності «Еразмус +».
Навчання іноземних здобувачів вищої освіти	До ДВНЗ «УжНУ» приймаються іноземні громадяни, а також особи без громадянства, які проживають на території України на законних підставах. Особливості вступу та навчання визначаються Положенням про навчання іноземних громадян у ДВНЗ «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/9378

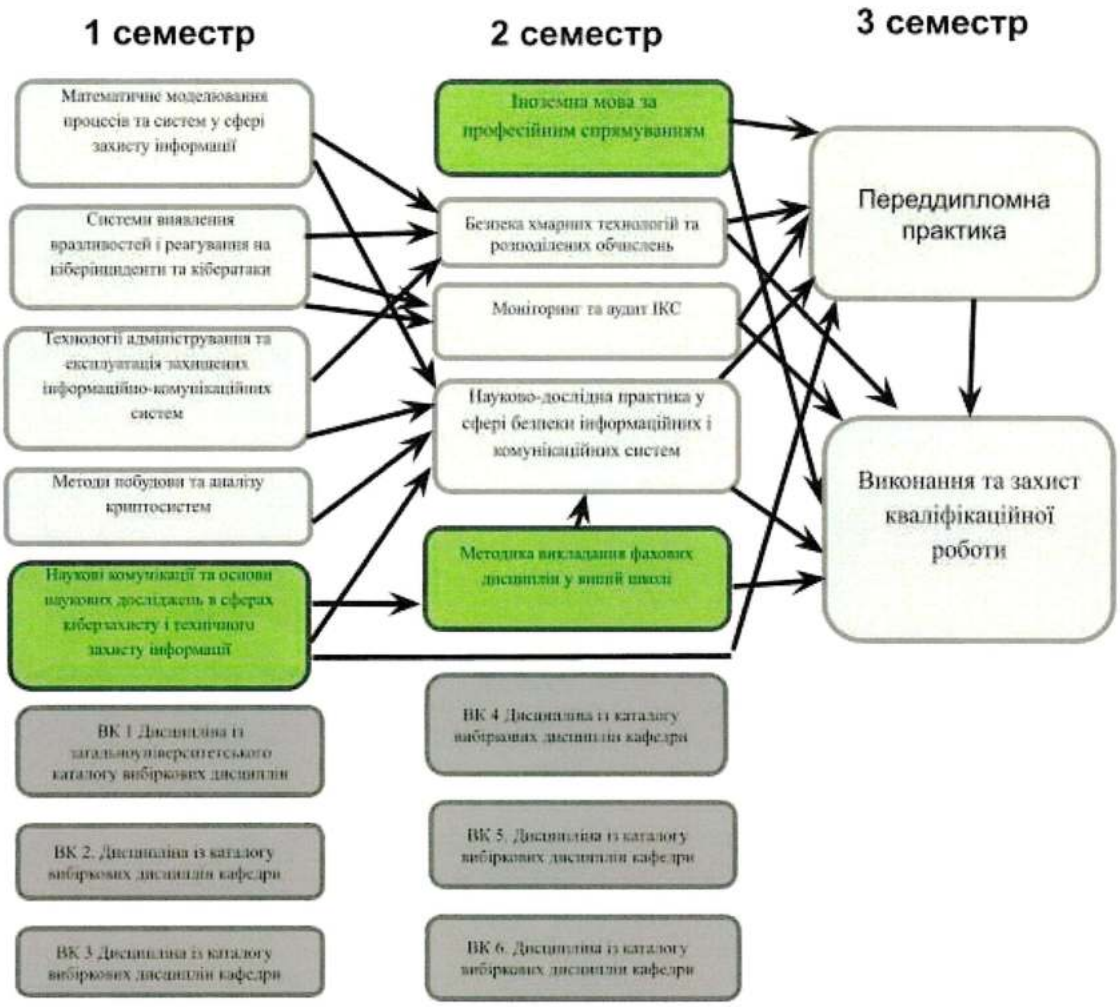
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
Цикл загальної підготовки			
ОК 1	Іноземна мова за професійним спрямуванням	3	Залік
ОК 2	Методика викладання фахових дисциплін у вищій школі	3	Залік
ОК 3	Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	3	Іспит
Цикл професійної підготовки			
ОК 4	Методи побудови та аналізу криптосистем	4	Іспит
ОК 5	Математичне моделювання процесів та систем у сфері захисту інформації	4	Іспит
ОК 6	Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	4	Іспит
ОК 7	Безпека хмарних технологій та розподілених обчислень	4	Іспит
ОК 8	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	4	Іспит
ОК 9	Моніторинг та аудит інформаційно-комунікаційних систем	3,5	Іспит
ОК 10	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	4,5	Диференційований залік
ОК 11	Переддипломна практика	10,5	Диференційований залік
ОК 12	Виконання та захист кваліфікаційної роботи магістра	19,5	Захист
Загальний обсяг обов'язкових компонент:		**67 Кредитів**	

Вибіркові компоненти ОП			
Цикл загальної підготовки			
ВК 1	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
Цикл професійної підготовки			
ВК 2	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК 3	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК 4	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК 5	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВК 6	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
Загальний обсяг вибіркових компонент		**23 кредити**	
Загальний обсяг освітньої програми		**90 кредитів**	

2.2. Структурно-логічна схема ОП



2.3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 Кібербезпека та захист інформації проводиться у формі захисту кваліфікаційної роботи магістра з видачею документа встановленого зразка про присудження ступеня магістра із присвоєнням кваліфікації: Магістр з кібербезпеки та захисту інформації, за умови успішного захисту кваліфікаційної роботи.

Захист кваліфікаційної (магістерської) роботи відбувається як публічна презентація. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

2.4. Матриця відповідності компетентностей (КЗ, КФ) компонентам освітньої програми (ОК)

Компетентності	Обов'язкові компоненти освітньої програми											
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12
КЗ-1	+	+	+	+	+	+	+	+	+	+	+	+
КЗ-2				+			+			+	+	+
КЗ-3		+	+	+	+		+	+		+	+	+
КЗ-4			+		+	+	+		+	+	+	+
КЗ-5	+	+	+			+	+	+		+	+	+
КЗ-6	+	+	+	+	+			+	+	+	+	+
КФ-1			+	+	+	+	+	+		+	+	+
КФ-2						+	+			+	+	+
КФ -3				+		+	+	+		+	+	+
КФ -4				+		+			+			
КФ -5			+	+	+		+	+	+	+	+	+
КФ -6			+		+	+	+	+		+		
КФ -7				+		+				+	+	+
КФ -8			+	+		+		+		+	+	+
КФ -9			+	+	+				+			
КФ-10	+	+		+						+	+	+

Матриця відповідності загальних та професійних компетентностей фахівця сфери захисту інформації (за професійним стандартом) компонентам освітньої програми (ОК)

Компетентності	Обов'язкові компоненти освітньої програми											
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12
ЗК.01		+	+	+	+	+	+	+		+	+	+
ЗК.02	+	+	+	+	+	+	+	+	+	+	+	+
ЗК.03		+			+			+	+	+	+	+
ЗК.04	+	+	+	+	+			+		+	+	+
ЗК.05	+	+	+	+	+	+	+	+		+	+	+
ЗК.06	+	+		+	+				+	+	+	+
ЗК.07	+	+		+			+		+	+	+	+
Б4				+	+					+	+	+
Д1			+	+	+	+	+			+	+	+
Д2			+	+	+		+	+	+	+	+	+
Е1				+			+		+	+	+	+
Е2		+		+		+	+	+		+	+	+
Е3	+	+	+	+			+	+		+	+	+
Е4			+	+	+	+		+	+	+	+	+

2.5. Матриця забезпечення результатів навчання (РН) відповідними компонентами освітньої програми (ОК)

Результати навчання	Обов'язкові компоненти освітньої програм											
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12
РН1	+	+								+	+	
РН2			+	+			+	+				
РН3			+	+	+			+		+	+	+
РН4			+	+	+		+	+				
РН5		+	+	+			+	+		+	+	+
РН6				+	+		+	+	+	+	+	+
РН7			+	+		+	+					
РН8				+		+	+	+	+			
РН9				+	+	+			+			
РН10			+	+					+			
РН11			+	+			+	+		+	+	+
РН12				+			+					
РН13			+	+	+			+				
РН14				+		+			+		+	+
РН15		+		+				+	+	+	+	+
РН16			+		+	+		+	+	+	+	+
РН17	+	+										
РН18	+	+				+			+			
РН19			+	+					+	+	+	+
РН20			+	+				+		+	+	+
РН21				+	+			+			+	+
РН22			+	+	+		+	+				
РН23				+		+	+	+	+	+	+	+
РН24					+		+	+	+	+	+	+
РН25			+			+			+	+	+	+