МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«Ужгородський національний університет»

ЗАТВЕРДЖЕНО
Протокол Вченої ради
ДВНЗ «Ужгородський національний університет»
31.03 2022 р. № 3

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»

другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

кваліфікація: Магістр з кібербезпеки

УВЕДЕНО В ДІЮ
Наказ ректора ДВНЗ
«Ужгородський національний університет»
01.04 2022 р. № 116/01-04

Ужгород 2022

АРКУШ ПОГОДЖЕННЯ

освітньо-професійної програми

«Системи технічного захисту інформації, автоматизація її обробки»

1. **Ректор** Володимир СМОЛАНКА

01.01. 2022 р.

2. **Гарант освітньо-професійної програми** Наталія ПОПОВИЧ

20.01. 2022 р.

3. **Декан фізичного факультету** Володимир ЛАЗУР

20.01. 2022 р.

4. **Керівник робочої групи** Наталія ПОПОВИЧ

20.01. 2022 р.

5. **Начальник навчальної частини** Анатолій ШТИМАК

28.03. 2022 р.

ПЕРЕДМОВА

Освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки» підготовки здобувачів другого (магістерського) рівня вищої освіти спеціальності 125 Кібербезпека 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. Програма відповідає другому (магістерському) рівню вищої освіти та сьомому кваліфікаційному рівню за Національною рамкою кваліфікації.

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ у складі:

1. РІЗАК Василь Михайлович, доктор фіз.-мат. наук, професор, завідувач кафедри твердо тільної електроніки та інформаційної безпеки ДВНЗ «УжНУ».
2. ПОПОВИЧ Наталія Іванівна, кандидат фіз.-мат. наук, доцент кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ «УжНУ» (гарант освітньо-професійної програми, керівник робочої групи).
3. ПИНЗЕНИК Василь Павлович, кандидат фіз.-мат. наук, доцент кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ «УжНУ».
3. ПЕТРУШКО Ірина Антонінівна, кандидат фіз.-мат. наук, доцент кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ «УжНУ».
4. ЧЕРЕПОВ Олександр Сергійович, здобувач вищої освіти.

ЗОВНІШНІЙ СТЕЙКХОЛДЕР: САМОХВАЛОВ Михайло Прокопович, керівник ТОВ «СПЕЦТЕЛЕКОМ».

1. Профіль освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки»

Розділ 1. 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	Магістр. Магістр з кібербезпеки.
Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Системи технічного захисту інформації, автоматизація її обробки
Тип диплому та обсяг освітньопрофесійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік і 4 місяці (денна форма навчання)
Наявність акредитації	Рішення Акредитаційної комісії від 3.07.2017 р.; сертифікат серія НД № 0789904. Термін дії сертифікату до 01.07.2022 р.
Цикл/рівень	7 рівень Національної рамки кваліфікацій України (НРК), другий цикл Європейського простору вищої освіти (FQEHEA), 7 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL).
Передумови	Наявність першого (бакалаврського) рівня вищої освіти. Можливість навчання за перехресним вступом. Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями, передбачає перевірку володіння особою компетентностями та результатами навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти. Умови вступу визначаються «Правилами прийому до Ужгородського національного університету».
Мова(и) викладання	Українська
Термін дії освітньої програми	До чергового перегляду відповідно до терміну сертифікації.
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.uzhnu.edu.ua/uk/infocentre/15068

Розділ 2. Мета освітньо-професійної програми	
Метою освітньої програми є підготовка фахівців, які володіють знаннями, вміннями та навичками розробляти, використовувати і впроваджувати технології інформаційної та/або кібербезпеки, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки; набуття компетентностей із застосування методів дослідження і проектування систем та комплексів забезпечення інформаційної та кібербезпеки.	
Розділ 3. Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	12 Інформаційні технології, 125 Кібербезпека, Обов'язкові навчальні дисципліни – 67 кредитів ЄКТС – 74,4% від загального обсягу ОП. Цикл дисциплін загальної підготовки - 13 кредитів ЄКТС, 390 год, в тому числі дисципліни вільного вибору студента - 7 кредитів ЄКТС, 210 год.); Цикл дисциплін професійної підготовки – 77 кредитів ЄКТС, 2310 год., в тому числі дисципліни вільного вибору студента – 16 кредитів ЄКТС, 480 год.)
Орієнтація освітньої програми	Освітньо-професійна програма орієнтована на отримання студентами необхідних знань, умінь та навичок для здійснення професійної діяльності з кібербезпеки, зокрема у галузі технічного захисту інформації,а також на розвиток здатності розв'язувати складні задачі і вирішувати проблеми у галузі професійної діяльності.
Основний фокус освітньої програми	Загальна вища освіта другого (магістерського) рівня в галузі інформаційної та кібербезпеки за спеціальністю 125 Кібербезпека Акцентована на розвиток здатності розв'язувати складні задачі і проблеми кібербезпеки, зокрема технічного захисту інформації, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог Ключові слова: кібербезпека, технічний захист інформації захист від несанкціонованого доступу.
Особливості програми	Програма передбачає вивчення: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки;

	– теорії, моделей та принципів управління доступом до інформаційних ресурсів; – методів та засобів оцінювання захищеності інформації; – методів та засобів технічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – автоматизованих систем та комплексів технічного захисту інформації..
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 2149.2 Професіонал із організації захисту інформації з обмеженим доступом 2149.2 Професіонал із організації інформаційної безпеки Професіонал може займати первинні посади: – Інженер з організації та управління діяльності служб інформаційної безпеки; – Інженер-проектувальник комплексних систем захисту інформації; – Інженер з експлуатації систем захисту інформації, – Професіонал із організації захисту інформації з обмеженим доступом, – Викладач вищого навчального закладу та ін.
Подальше навчання	Можливість продовження навчання за програмою 8 рівня Національної рамки кваліфікацій України (третього (освітньо-наукового) рівня вищої освіти). Набуття додаткових кваліфікацій в системі післядипломної освіти.
Розділ 5. Викладання та оцінювання	
Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Студенто-центроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуально творчий підхід. Практико-орієнтоване навчання через різні види практик у лабораторіях,на підприємствах, установах та організаціях різних форм власності на підставі договорів про проходження практики. Виконання практичних та лабораторних робіт. Дистанційне навчання шляхом проведення занять з використанням чат-технологій; он-лайн лекцій, конференцій, семінарів, ділових ігор, лабораторних робіт, практикумів та інших форм

	навчальної діяльності за допомогою засобів комунікації з використанням мультимедійних комплексів та веб-технологій.
Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання усіх видів аудиторної та позааудиторної навчальної діяльності студентів, спрямовані на опанування навчального навантаження з освітньої програми: поточні контроль та оцінювання, поетапний, модульний, підсумковий контроль; екзамени; заліки, презентації, диференційований залік з науково-дослідної, виробничої та переддипломної практик, курсова робота, 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
Розділ 6. Програмні компетентності	
Інтегральна компетентність	ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	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 спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів господарської діяльності).
Фахові компетентності	КФ1. 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. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування; інтегрувати,

	аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. КФ4. 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. КФ5. Здатність до дослідження, системного аналізу та забезпечення неперервності 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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. 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. КФ8. 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. КФ9. 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. КФ10. 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. КФ11. Здатність здійснювати ліцензування, атестацію та сертифікацію засобів та систем захисту інформації на об’єктах інформаційної діяльності. КФ12. Здатність розробляти проектну документацію, програми та методики випробувань, налаштування та супровід комплексів захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури.
Розділ 7. Програмні результати навчання	
ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово, для представлення й обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	
ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	
ПРН3. Провадити дослідницьку та/або інноваційну діяльність у сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	
ПРН4. Розробляти, застосовувати, інтегрувати, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі у сфері інформаційної безпеки та/або кібербезпеки.	
ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі нових результатів досліджень інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	
ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	
ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	
ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби захисту інформації та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	
ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	

ПРН10. Забезпечувати неперервність бізнес/операційних процесів, виявляти вразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури контролю та розслідування, а також надавати рекомендації щодо попередження кіберінцидентів в цілому.
ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби технічного та криптографічного 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.
ПРН14. Розробляти, супроводжувати й аналізувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
ПРН15. Зрозуміло і однозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують, до персоналу, партнерів та інших осіб.
ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних й непередбачуваних ситуаціях, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень
ПРН17. 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.
ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом щодо інформаційної безпеки та/або кібербезпеки.
ПРН19. Обирати, аналізувати і розробляти типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти із захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
ПРН20. Ставити складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки та вирішувати їх із врахуванням вимог вітчизняних та світових стандартів та кращих практик.
ПРН21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати придатні для цього методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
ПРН23. 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.	
ПРН24. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.	
ПРН25. Здійснювати оцінювання захищеності інформації, яка циркулює на об'єкті інформаційної діяльності; аналізувати стан безпеки комп'ютерних систем та мереж.	
ПРН26. Використовувати методи та засоби виявлення і пошуку закладних пристроїв.	
ПРН27. Аналізувати захищеність території та приміщень об'єкта інформаційної діяльності, технічних засобів і враховувати можливий спектр загроз та їх наслідки для сервісів систем забезпечення інформаційної та кібернетичної безпеки.	
Розділ 8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Склад робочої групи освітньої програми, професорсько-викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на другому (магістерському) рівні вищої освіти. Професорсько-викладацький склад проходить стажування згідно Положення про підвищення кваліфікації https://www.uzhnu.edu.ua/uk/infocentre/get/5950
Матеріально-технічне забезпечення	Забезпеченість приміщеннями для проведення аудиторних лекційних, практичних та лабораторних занять, комп'ютерними робочими місцями та відповідними програмними засобами, мультимедійним обладнанням та оргтехнікою дозволяє здійснювати якісну підготовку фахівців за ОПП. Усі комп'ютерні робочі місця під'єднані до локальної мережі та надають відкритий доступ до глобальної Інтернет-мережі. Навчальні лабораторії оснащені устаткуванням для технічного захисту інформації (системи відеоспостереження, засоби для виявлення закладних пристроїв, засоби мережевого захисту). Усі приміщення відповідають будівельним і санітарним нормам. Наявна вся необхідна соціально-побутова інфраструктура Для забезпечення безперешкодного доступу до приміщень ДВНЗ «Ужгородський національний університет» для осіб з інвалідністю та інших маломобільних груп населення встановлено пандуси та кнопки виклику.

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. Здобувачі освіти отримують − необмежений доступ до мережі Інтернет; − доступ до фондів та електронних каталогів наукової бібліотеки ДВНЗ «УжНУ», а також до електронного репозитарію ДВНЗ «УжНУ» (https://dspace.uzhnu.edu.ua/jspui/); − наукова бібліотека, читальні зали; − віртуальне навчальне середовище Moodle (https://elearn.uzhnu.edu.ua/); − веб-сайт фізичного факультету за адресою https://www.uzhnu.edu.ua/uk/cat/faculty-fphysics , де міститься інформація про організацію навчального процесу; − навчальні і робочі навчальні плани; − графіки навчального процесу; − навчально-методичні комплекси дисциплін; − дидактичні матеріали для самостійної та індивідуальної роботи студентів з дисциплін, програми практик; − методичні вказівки щодо виконання кваліфікаційних робіт.
Розділ 9. Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність забезпечується на основі двосторонніх угод, укладених між ДВНЗ «Ужгородський національний університет» та вітчизняними закладами вищої освіти.
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	Можливе навчання іноземних громадян та осіб 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.

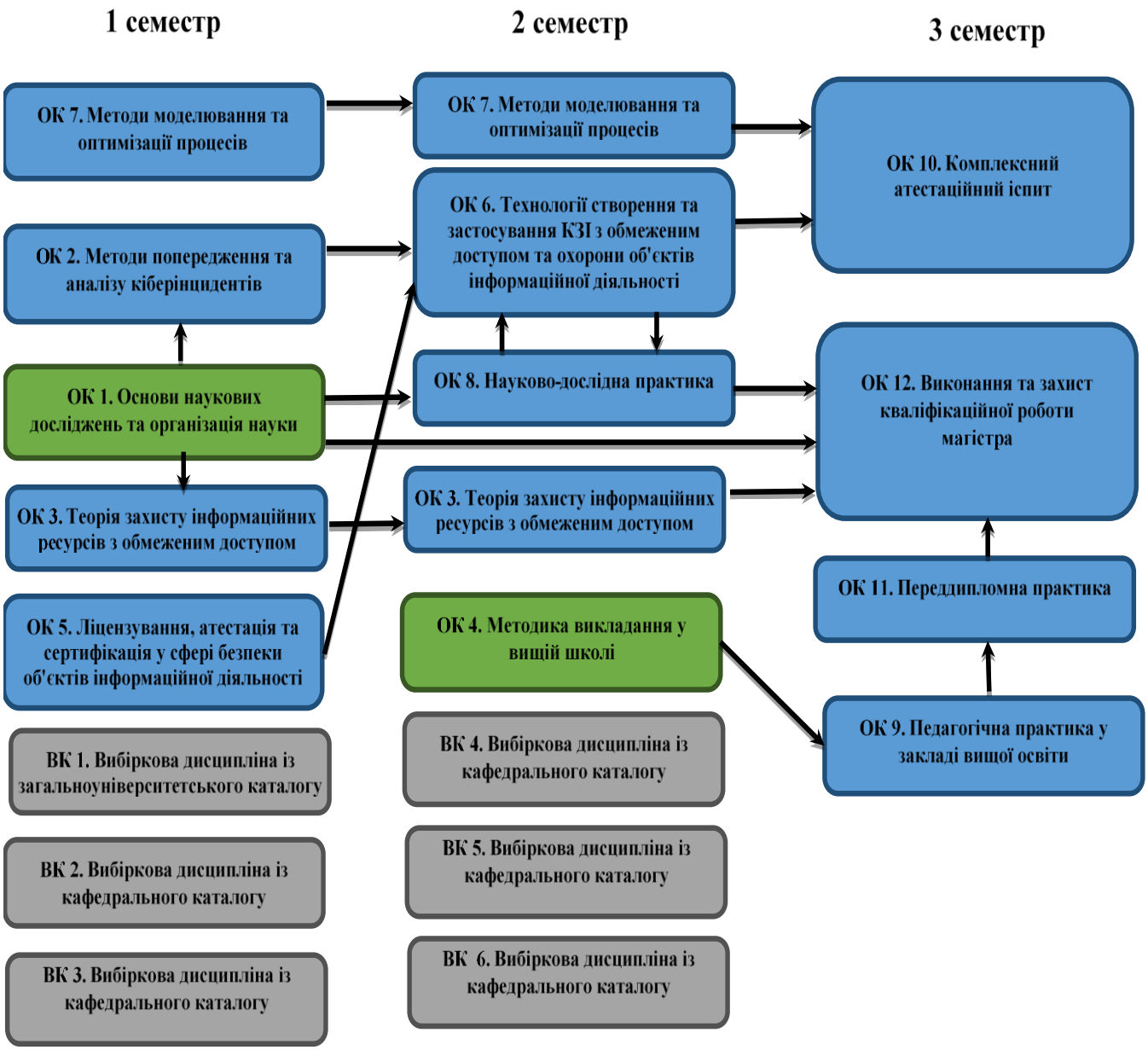
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

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 та професійної підготовки**			
ОК 1	Основи наукових досліджень та організація науки	3	Залік
ОК 2	Виявлення та попередження кіберінцидентів	3.5	Іспит
ОК 3	Теорія захисту інформаційних ресурсів з обмеженим доступом	6.5	Іспит, диференційований залік
ОК 4	Методика викладання у вищій школі	3	Залік
ОК 5	Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	4.5	Іспит
ОК 6	Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності	4	Іспит
ОК 7	Методи моделювання та оптимізації процесів	9.5	Іспит
ОК 8	Науково-дослідна практика (2 тижні)	3	Диференційований залік
ОК 9	Педагогічна практика у закладі вищої освіти (2 тижні)	3	Диференційований залік
ОК 10	Комплексний атестаційний іспит	1.5	Екзамен
ОК 11	Переддипломна практика (6 тижнів)	9	Диференційований залік
ОК 12	Виконання та захист кваліфікаційної роботи магістра	16.5	Захист
Загальний обсяг обов`язкових компонент:		**67 Кредитів**	

Вибіркові компоненти ОП **Цикл загальної підготовки та професійної підготовки**			
ВК 1	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
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



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 Кібербезпека здійснюється у формі комплексного іспиту та публічного захисту кваліфікаційної роботи магістра й завершується видачею документа встановленого зразка про присудження ступеня магістра із присвоєнням кваліфікації: Магістр з кібербезпеки.

Кваліфікаційна робота передбачає розв’язання наукової або науково-технічної задачі у галузі інформаційної безпеки та/або кібербезпеки, повинна бути самостійною логічно завершеною науково-дослідною роботою. Кваліфікаційна робота не повинна містити академічного плагіату, в тому числі некоректних текстових запозичень, фабрикації, фальсифікації.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12
КЗ-1								+	+		+	
КЗ-2	+							+				
КЗ-3		+	+				+				+	+
КЗ-4					+	+						+
КЗ-5				+					+	+		
КФ-1	+		+			+	+	+			+	
КФ-2					+	+		+				+
КФ-3						+		+				
КФ-4		+	+						+			
КФ-5		+	+									
КФ-6			+			+						
КФ-7	+	+										
КФ-8			+			+						
КФ-9		+			+							
КФ-10				+					+			
КФ-11					+	+				+		
КФ-12					+	+				+		+

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12
ПРН 1		+							+			
ПРН 2	+							+			+	+
ПРН 3	+							+				
ПРН 4						+	+					
ПРН 5			+	+						+		
ПРН 6				+		+		+				+
ПРН 7					+	+				+	+	+
ПРН 8						+		+			+	
ПРН 9		+	+									
ПРН 10		+	+									
ПРН 11		+	+						+			
ПРН 12		+						+	+			
ПРН 13		+				+					+	+
ПРН 14					+	+						
ПРН 15				+					+	+		+
ПРН 16		+			+		+		+			+
ПРН 17		+		+				+				
ПРН 18				+					+			
ПРН 19							+	+				
ПРН 20	+							+			+	+
ПРН 21	+						+					
ПРН 22	+		+								+	
ПРН 23		+	+								+	+
ПРН 24			+		+							
ПРН 25		+			+							
ПРН 26					+	+						
ПРН 27					+	+				+		