МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

УХВАЛЕНО
Рішенням вченої ради
Харківського національного
економічного університету імені
Семена Кузнеця
від 25.05.2022 р. протокол № 4

ВВЕДЕНО В ДІЮ
Наказом ректора Харківського
національного економічного університету
імені Семена Кузнеця
від 25.05.2022 р. № 123

Володимир ПОНОМАРЕНКО

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

РІВЕНЬ ВИЩОЇ ОСВІТИ	**Другий (магістерський)**
СТУПІНЬ ВИЩОЇ ОСВІТИ	**Магістр**
ГАЛУЗЬ ЗНАНЬ	**12 Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**125 Кібербезпека**

Харків, 2022

ПРЕАМБУЛА

Робоча група освітньої програми:

Семенов Сергій Геннадійович, професор кафедри кібербезпеки та інформаційних технологій, доктор технічних наук, професор – гарант освітньої програми;

Солодовник Ганна Валеріївна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук, доцент.

Долгова Наталія Геннадіївна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук.

Муржа Дмитро Юрійович, здобувач вищої освіти.

Гриньов Денис Валерійович, керівник освітніх університетських програм міжнародної IT-компанії EPAM Systems Inc. в східній Україні

Розглянуто на засіданні кафедри кібербезпеки та інформаційних технологій, протокол № 15 , від 16.05.2022 р.

Розглянуто вченою радою факультету інформаційних технологій, протокол № 6, від 17.05.2022 р.

ОП оновлено на підставі:

1. Законодавчих та нормативних актів: Законів України «Про освіту», «Про вищу освіту», Національної рамки кваліфікації, Національного класифікатору України: Класифікатор професій (ДК 003:2010).
2. Стандарту вищої освіти 125 «Кібербезпека» другого (магістерського) рівня вищої освіти затвердженого Наказом Міністерства освіти та науки України № 332 від 18.03.2021.
3. Аналізу ринку праці, з урахуванням регіонального контексту.
4. Вивчення вітчизняного та зарубіжного досвіду.
5. Пропозицій роботодавців.
6. Рекомендації після процедур акредитації. Рішення НА від 15.12.2020, протокол № 24.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузі знань	12 Інформаційні технології
Спеціальності	125 Кібербезпека
Освітня програма (укр. та англ. мовою)	Кібербезпека / Cybersecurity
Форми здобуття освіти, обсяг освітньої програми в кредитах ЄКТС та терміни навчання	очна (денна) форма – 90 кредитів, один рік 4 місяці; заочна форма – 90 кредитів, один рік 4 місяці.
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти; сертифікат про акредитацію – № 957 від 18.12.2020 р.; термін дії акредитації – до 01.07.2026 р.
Мова(и) навчання / оцінювання	українська / англійська
Структурний підрозділ відповідальний за ОП	Кафедра кібербезпеки та інформаційних технологій
Вимоги до зарахування	Для успішного засвоєння освітньої програми абітурієнти повинні мати вищу освіту першого (бакалаврського) рівня та здібності до оволодіння знаннями, уміннями й навичками у галузі інформаційних технологій за спеціальністю кібербезпека. Правила та строки прийому розміщені на сайті ХНЕУ ім. С. Кузнеця за посиланням https://www.hneu.edu.ua/normatyvni-dokumenty/
Обмеження щодо форм навчання	Відсутні
Освітня кваліфікація	Магістр з кібербезпеки
Кваліфікація(-ї) професійна(-і)	Відсутня
Кваліфікація в дипломі	Ступінь вищої освіти − Магістр Спеціальність – 125 Кібербезпека Освітня програма – Кібербезпека
Мета освітньої програми	розвиток у здобувачів професійних, творчих, інтелектуальних здібностей щодо оволодіння методологією наукової діяльності та забезпечення здобувачам підготовки у вигляді знань, умінь та навичок для розв’язання задач в галузі кібербезпеки.
Фокус та особливості (унікальність) програми	**Фокус:** Формування компетенцій щодо**:** розробки та верифікації безпечних програмно-технічних засобів,

	адміністрування та керування локальними, глобальними комп'ютерними мережами інтерфейсами та протоколами взаємодії їх компонентів, що направлені на виявлення їх вразливостей і підвищення інформаційної безпеки (DevSecOps); управління інформаційними процесами, технологіями, методами, способами та інструментами; процедурами та засобами стандартизації, сертифікації та підтримки життєвого циклу вказаних програмно-технічних засобів; розробки методів та способів опрацювання інформації (у тому числі стеганографічних та стеганофонічних), математичних моделей та технологій обчислювальних процесів, в тому числі високопродуктивних, паралельних, розподілених, мобільних, архітектура та організація функціонування відповідних програмно-технічних засобів. **Особливості:** Особливістю освітньої програми є її орієнтованість на сучасні моделі та методи створення безпечної операційної структури та діяльності для розробки та впровадження програмного забезпечення (DevSecOps), та їх застосування для розв'язання задач кібербезпеки.
Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів правової діяльності та менеджменту (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного, стеганографічного та технічного захисту інформації, теорії ризиків та інших

	міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення (кіберполігон), автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Академічна мобільність	Польсько-українська програма обміну та двох дипломів для підготовки магістрів за спеціальністю "Кібербезпека" з Університетом у Бєльсько-Бялій (м. Бельсько-Бяла, Польща).
Академічні права	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
Професійні права	Професійні права магістра – робота за фахом відповідно до кваліфікації «магістр з кібербезпеки». Магістр з кібербезпеки може займати посади на підприємствах, установах, організаціях незалежно від форми власності, ІТ-компаніях та стартапах, органах державної влади і місцевого самоврядування.
Працевлаштування випускників	Випускники можуть працювати за такими професіями (згідно з Національним класифікатором професій ДК 003:2010): 3439 фахівець із організації інформаційної безпеки; 2149.2 - професіонал із організації інформаційної безпеки; 2149.2 - професіонал із організації захисту інформації з обмеженим доступом.

ІІ – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА

Інтегральна компетентність	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 економічної 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, а також 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 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. 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.

З метою забезпечення кореляції визначених компетентностей з класифікацією компетентностей НРК використовується матриця відповідності визначених компетентностей та дескрипторів НРК, яка є інформаційним додатком (**Таблиця 1 Пояснювальної записки**).

ІІІ – НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА СПЕЦІАЛЬНІСТЮ 125 КІБЕРБЕЗПЕКА

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. Аналізувати, розробляти і супроводжувати інфраструктуру та стек застосунків у безперервному потоці змін Agile DevSecOps.

РН25. Досліджувати, обґрунтовувати вибір та застосовувати платформи та інструменти, що використовуються для реалізації підходу DevSecOps.

РН26. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби стеганографічного та стеганофонічного 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.

IV. СТРУКТУРА ОСВІТНЬОЇ ПРОГРАМИ ПІДГОТОВКИ МАГІСТРІВ

4.1. СТРУКТУРА ПРОГРАМИ ТА ОСВІТНІ КОМПОНЕНТИ

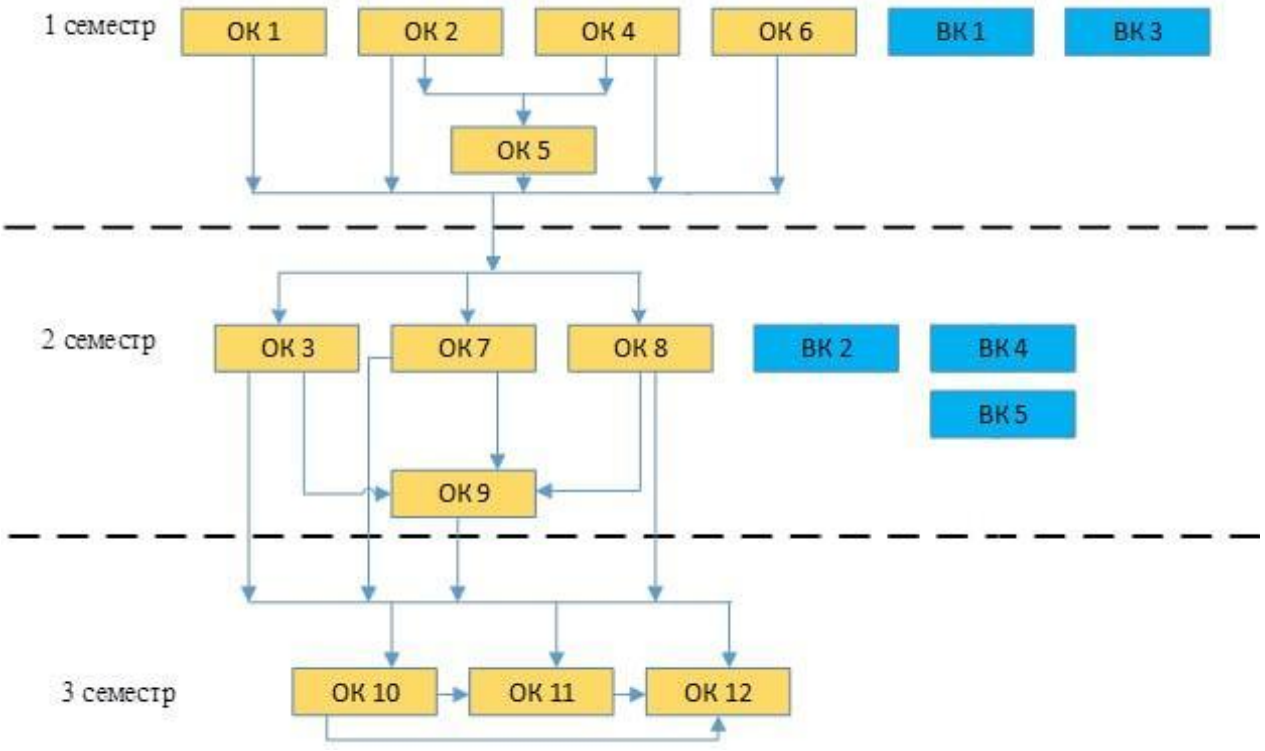
№	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Структура, %
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	10	11,1
2	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	10	11,1
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
3	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	55	61,1
4	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	15	16,7
	ЗАГАЛЬНА КІЛЬКІСТЬ :	***90***	***100%***
	в тому числі: вибіркова складова	25	27,8%

Код ОК	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Форми підсумкового контролю
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК1	ІНОЗЕМНА МОВА ЗА ПРОФЕСІЙНИМ СПРЯМУВАННЯМ	3	залік
ОК2	СУЧАСНІ МЕТОДИ ДЕЦЕНТРАЛІЗОВАНОГО РОЗПОДІЛУ ДАНИХ	3	залік
ОК3	ОСНОВИ НАУКОВИХ ДОСЛІДЖЕНЬ ТА НАУКОВО-ПЕДАГОГІЧНА ДІЯЛЬНІСТЬ В ГАЛУЗІ КІБЕРБЕЗПЕКИ	4	залік
	ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ		
ВК 1	МАГ-МАЙНОР	5	залік
ВК 2	МАГ-МАЙНОР	5	залік
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК 4	ТЕОРІЯ РИЗИКІВ В КІБЕРБЕЗПЕЦІ	4	залік
ОК 5	РОЗШИРЕНА МЕРЕЖЕВА ТА ХМАРНА БЕЗПЕКА	5	екзамен
ОК 6	БЕЗПЕЧНЕ ПРОГРАМУВАННЯ	5	екзамен
ОК 7	ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ	5	екзамен
ОК 8	СТАНДАРТИЗАЦІЯ ТА СЕРТИФІКАЦІЯ КІБЕРНЕТИЧНОЇ ДІЯЛЬНОСТІ	5	залік
ОК 9	КУРСОВА РОБОТА	1	курсова робота
ОК 10	КОМПЛЕКСНИЙ ТРЕНІНГ	3	звіт
ОК 11	ПЕРЕДДИПЛОМНА ПРАКТИКА	12	звіт
ОК 12	ДИПЛОМНА РОБОТА	15	дипломна робота
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК 3	МЕЙДЖОР 1	5	екзамен
ВК 4	МЕЙДЖОР 2	5	екзамен
ВК 5	МЕЙДЖОР 3	5	екзамен

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ

Студентам надається можливість вільного вибору навчальних дисциплін. Обрані дисципліни увійдуть до індивідуального навчального плану кожного студента, а результати навчання будуть відображені у додатку до диплому. Принцип вільного вибору дає змогу кожному студенту вивчати навчальні дисципліни, які відображають індивідуальні вподобання, інтереси та плани на майбутнє працевлаштування. Реєстрація на вибіркову складову освітньо-професійної програми підготовки відбувається на підставі форми-заяви, що заповнюється та подається до відповідного деканату. Вибіркова складова складається з двох дисциплін МАГ-МАЙНОР (розвивають та формують загальні результати навчання). Маг-майнори обираються з загального пулу дисциплін ХНЕУ ім. С. Кузнеця. А також три дисципліни МЕЙДЖОРИ (поглиблюють професійні компетентності та результати навчання), обираються з пулу спеціальності/ освітньої програми.

4.3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ



V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. 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.
Вимоги до публічного захисту	У процесі публічного захисту кандидат на присвоєння магістерського ступеня повинен показати уміння чітко і упевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь здобувача вищої освіти повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду.

VI. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Вимоги до системи внутрішнього забезпечення якості в Університеті розроблені на підставі Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG), статті 16 Закону України "Про вищу освіту", Стандарту вищої освіти за спеціальністю 125 Кібербезпека другий (магістерський) рівень вищої освіти.

Політика щодо забезпечення якості вищої освіти	Основні принципи внутрішнього забезпечення якості освіти у ХНЕУ ім. С. Кузнеця: відповідальності; відповідності; адекватності; автономності; вимірюваності; академічної культури; відкритості. Основні процедури внутрішнього забезпечення якості освіти в ХНЕУ ім. С. Кузнеця: формалізація політики якості, стратегічних цілей, завдань постійного поліпшення якості; забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації; забезпечення дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої освіти; підготовка та проведення маркетингово-моніторингових та соціально-психологічних досліджень для визначення потреб ринку праці, вимог стейкхолдерів вищої освіти, якості надання освітніх послуг і задоволеності якістю освітньої діяльності та якістю освіти; залучення стейкхолдерів вищої освіти (здобувачів вищої освіти, роботодавців, представників академічної

	спільноти тощо) до прийняття рішень за напрямами внутрішнього забезпечення якості; зовнішнє оцінювання якості діяльності ХНЕУ ім. С. Кузнеця за результатами участі в національних та міжнародних рейтингах вищих навчальних закладів, виконання Ліцензійних вимог, акредитації. Напрями: розроблення, затвердження, моніторинг та періодичний перегляд освітніх програм; забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; забезпечення студентоцентрованого навчання, викладання та оцінювання здобувачів вищої освіти; забезпечення наявності необхідних ресурсів для організації освітнього процесу; забезпечення наявності інформаційних систем для ефективного управління освітнім процесом.
Забезпечення якості розроблення, затвердження, моніторингу, перегляду та оновлення освітніх програм	Моніторинг та періодичний перегляд освітніх програм здійснюється згідно з діючими нормативними актами в ХНЕУ ім. С. Кузнеця. Перегляд освітніх програм здійснюється на основі аналізу задоволення освітніх потреб здобувачів вищої освіти: можливості побудови індивідуальної траєкторії навчання, дотримання академічних свобод в освітньому процесі, задоволеності якістю освітньої програми, тощо; роботодавців: якості формування загальних та фахових компетентностей, актуальних та соціальних навичок (soft skills); інших стейкхолдерів. Для перегляду освітніх програм використовуються: онлайн опитування, проведення дослідження фокус-групи, аналіз документів, аналіз ситуації, самооцінка робочою групою відповідно до вимог щодо структури та змісту освітньої програми. Періодичність перегляду освітніх програм здійснюється: а) щорічно за результатами моніторингу; б) після завершення освітньої програми здобувачами вищої освіти, в) в разі зміни н законодавчої та нормативної бази.
Забезпечення зарахування, досягнення, визнання та атестація здобувачів	Оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених в Університеті процедур згідно з нормативними актами. Щорічне оцінювання здобувачів освіти здійснюється відповідно до визначених освітньою програмою форм контролю; порядку оцінювання результатів навчання, що висвітлюється в робочих програмах навчальних дисциплін, робочих планах (технологічних картах) навчальних дисциплін, силабусах навчальних дисциплін; обліку результатів навчання, який ведеться з використанням програмного забезпечення корпоративної інформаційної системи управління (електронний журнал) та інформаційного середовища Персональної навчальної системи (ПНС) Університету. Оприлюднення результатів успішності, оцінювання результатів навчання відбувається через звіт «Інформація про поточну успішність та відвідування занять за навчальними дисциплінами

	семестру» (сайт Університету) та на сайті Персональних навчальних систем. Оцінювання здобувачів вищої освіти здійснюється на основі 100-бальної накопичувальної бально-рейтингової системи.
Забезпечення якості студентоцентрованого навчання, викладання та оцінювання	Планування, розподіл та надання навчальних ресурсів і забезпечення підтримки здобувачів вищої освіти враховують їх потреби та принципи студентоцентрованого навчання. Внутрішнє забезпечення якості вищої освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а здобувачі вищої освіти поінформовані про їх наявність.
Забезпечення якості науково-педагогічних працівників	Щорічне рейтингове оцінювання діяльності науково-педагогічних працівників, кафедр і факультетів Університету здійснюється за рахунок використання механізмів оцінювання та самооцінювання результативності науково-педагогічної діяльності, її спрямованості на пріоритети розвитку національної системи вищої освіти, стратегії розвитку Університету, особистісного професійного розвитку науково-педагогічних працівників. Підсумки рейтингового оцінювання підводяться за результатами діяльності, досягнутими протягом навчального року. Оприлюднення результатів щорічного оцінювання науково-педагогічних працівників, кафедр та факультетів відбувається на засіданні вченої ради Університету.
Ресурсне забезпечення освітнього процесу (навчальні ресурси та підтримка здобувачів вищої освіти)	Заклад вищої освіти забезпечує освітній процес необхідними та доступними ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснює відповідну підтримку здобувачів вищої освіти. Організаційно-методична підтримка самостійної роботи здобувачів вищої освіти полягає у розробці методичних, дидактичних, інструктивних матеріалів, наданні можливості формувати, закріплювати, поглиблювати й систематизувати отримані під час аудиторних занять знання та вміння, здійснювати самопідготовку й самоконтроль опанування освітньої-професійної програми та реалізується через Персональну навчальну систему ХНЕУ ім. С. Кузнеця.
Інформаційне забезпечення (інформаційний менеджмент)	З метою управління освітнім процесом розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну систему управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної кампанії, планування та організацію освітнього процесу; доступ до навчальних ресурсів; облік та аналіз успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; управління кадрами та ін.

Публічність інформації про освітні програми, освітню, наукову діяльність	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація за освітньо-професійною програмою публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних здобувачів вищої освіти, випускників, інших стейкхолдерів і громадськості. Публічною є інформація про освітню діяльність за спеціальністю включаючи критерії відбору на навчання; заплановані результати навчання за цією програмою; процедури навчання, викладання та оцінювання, що використовуються тощо.
Забезпечення академічної доброчесності	Забезпечення запобігання та виявлення академічного плагіату у наукових працях працівників закладу вищої освіти та здобувачів вищої освіти реалізується через політику, стандарти і процедури дотримання академічної доброчесності, регулюється такими документами ХНЕУ ім. С. Кузнеця: Кодекс академічної доброчесності; Кодекс професійної етики та організаційної культури працівників і здобувачів вищої освіти ХНЕУ ім. С. Кузнеця; Положення про комісію з питань академічної доброчесності ХНЕУ ім. С. Кузнеця. Перевірка наукових праць науково-педагогічних працівників Університету та здобувачів вищої освіти здійснюється за допомогою інтернет-сервісів на основі відкритих інтернет-ресурсів та системи StrikePlagiarism.com, що діє на підставі Ліцензійного Договору про надання права користування антиплагіатним програмним забезпеченням.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Матриця відповідності визначених Стандартом (за наявності) компетентностей дескрипторам НРК та матриця відповідності визначених Стандартом результатів навчання та компетентностей представлені в Таблицях 1 і 2.

Таблиця 1

Матриця відповідності визначених Стандартом компетентностей результатів навчання дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень **Зн2** Критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
Загальні компетентності				
КЗ1	Зн1, Зн2	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1, Зн2	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн2	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн2	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1, Зн2	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ4	Зн1, Зн2	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1, Зн2	Ум1, Ум2	К1	АВ1, АВ2
КФ6	Зн1	Ум1, Ум2	К1	АВ1
КФ7	Зн1	Ум1, Ум2	К1	АВ1
КФ8	Зн1	Ум1, Ум2	К1	АВ1
КФ9	Зн1	Ум1, Ум2	К1	АВ1
КФ10	Зн2	Ум1, Ум2, Ум3	К1	АВ1, АВ2

Таблиця 2

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

Програмні результати навчання	**Компетентності**														
	Загальні					**Спеціальні (фахові)**									
	КЗ1	**КЗ2**	**КЗ3**	**КЗ4**	**КЗ5**	**КФ1**	**КФ2**	**КФ3**	**КФ4**	**КФ5**	**КФ6**	**КФ7**	**КФ8**	**КФ9**	**КФ10**
РН 1	ОК8		ОК3	ОК8	ОК1	ОК3	ОК8								
РН 2		ОК3	ОК3	ОК4		ОК3	ОК4	ОК6		ОК4					ОК3
РН 3	ОК3					ОК5		ОК5	ОК5		ОК5		ОК5	ОК5	
РН 4	ОК9 ОК10 ОК11	ОК10 ОК12	ОК7	ОК10	ОК11 ОК12	ОК6 ОК9	ОК6 ОК12			ОК12				ОК12	ОК11
РН 5			ОК2	ОК4	ОК3		ОК4			ОК4	ОК2				
РН 6	ОК7			ОК7		ОК6 ОК7	ОК6	ОК2		ОК12	ОК7	ОК7		ОК12	
РН 7	ОК9 ОК10	ОК10 ОК12	ОК3	ОК10	ОК11 ОК12	ОК9	ОК12			ОК12				ОК12	ОК11
РН 8	ОК9 ОК10	ОК10 ОК12		ОК10	ОК11 ОК12	ОК9	ОК12	ОК10		ОК12				ОК12	ОК11
РН 9	ОК2 ОК4	ОК2 ОК4	ОК2 ОК4	ОК4					ОК11					ОК12	ОК11
РН 10	ОК3		ОК3	ОК4		ОК7	ОК4			ОК4	ОК7	ОК7		ОК12	
РН 11	ОК3		ОК3	ОК4		ОК7		ОК5	ОК5		ОК7 ОК5	ОК7	ОК5	ОК5	ОК11
РН 12	ОК3		ОК3	ОК4				ОК5	ОК5		ОК5		ОК5	ОК5	ОК11
РН 13	ОК9 ОК10	ОК10 ОК12	ОК3	ОК10		ОК9					ОК5		ОК5	ОК5 ОК12	ОК11

Програмні результати навчання	Компетентності														
	Загальні					Спеціальні (фахові)									
	КЗ1	**КЗ2**	**КЗ3**	**КЗ4**	**КЗ5**	**КФ1**	**КФ2**	**КФ3**	**КФ4**	**КФ5**	**КФ6**	**КФ7**	**КФ8**	**КФ9**	**КФ10**
РН 14	ОК2		ОК2	ОК2		ОК7			ОК7		ОК7 ОК2	ОК7		ОК7	ОК7
РН 15				ОК2	ОК1										ОК3
РН 16	ОК3	ОК3	ОК3	ОК3		ОК7		ОК7	ОК7	ОК7	ОК7	ОК7		ОК12	ОК11
РН 17								ОК11	ОК11	ОК12				ОК12	ОК11
РН 18	ОК11	ОК3	ОК3	ОК3	ОК3 ОК11				ОК11						ОК11
РН 19	ОК3			ОК3	ОК3	ОК11 ОК12	ОК11 ОК12	ОК11 ОК12	ОК11 ОК12		ОК11 ОК12	ОК11 ОК12	ОК11 ОК12	ОК11 ОК12	
РН 20	ОК8	ОК3	ОК3	ОК2	ОК3	ОК8	ОК8	ОК8							
РН 21	ОК2	ОК2		ОК2		ОК9	ОК12	ОК9 ОК10 ОК11	ОК11	ОК12		ОК9 ОК10 ОК11	ОК9 ОК10 ОК11	ОК12	ОК11
РН 22		ОК3 ОК12	ОК3	ОК3	ОК3 ОК12	ОК12	ОК12	ОК12		ОК12				ОК12	
РН 23	ОК11	ОК12	ОК3	ОК4	ОК11 ОК12	ОК6	ОК12 ОК6	ОК11	ОК11	ОК12 ОК4	ОК12	ОК12	ОК12	ОК12	ОК11
РН 24									ОК2, ОК5			ОК2			
РН 25						ОК2								ОК2	
РН 26								ОК5	ОК5		ОК5		ОК5		

Гарант ОП *підписано* **Сергій СЕМЕНОВ**

ЛИСТ ПОГОДЖЕННЯ
освітньої програми «КІБЕРБЕЗПЕКА»

Назва структурного / функціонального підрозділу / посадова особа	**Дата, підпис**
1. Навчальний відділ	
2. Керівник відділу забезпечення якості освіти та інноваційного розвитку	
3. Завідувач кафедри кібербезпеки та інформаційних технологій	
4. Проректор з навчально-методичної роботи	

РЕЦЕНЗІЯ-ВІДГУК

на магістерську освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету імені Семена Кузнеця

Сьогодні, у часи цифрового суспільства, вплив інформаційно-комунікаційних технологій на життя людини зростає у геометричній прогресії – виникають нові загрози і нові виклики. Саме тому особливої актуальності дедалі більше набуває поняття «кібербезпека». Якісна підготовка здобувачів вищої освіти в сфері кібербезпеки на теперішній час для України є важливим завданням. Вони покликані захищати ресурси (інформації, комп'ютерів, серверів, підприємств, приватних осіб), а також дані на етапі їх обміну та збереження.

Харківський національний економічний університет імені Семена Кузнеця в цьому питанні має досвід, потужний кадровий потенціал та матеріально-технічну базу для виконання поставленого завдання. Рецензована магістерська освітньо-професійна програма «Кібербезпека» розроблена проектною групою працівників кафедри кібербезпеки та інформаційних технологій після консультацій із науковцями, потенційними роботодавцями, які підтвердили потребу підготовки фахівців цієї спеціальності. В освітньо-професійній програмі визначені програмні компетентності виходячи із видів і завдань діяльності кіберзахисту. Вони розподілені на загальні та фахові компетентності, найбільш відповідні для запропонованої програми. Фахові компетентності носять практичний характер і можуть бути використані у професійній діяльності майбутніх фахівців. Навчальний план підготовки магістрів освітньо-професійної програми «Кібербезпека» повністю відповідає завданням освітньої професійної програми. Послідовність вивчення дисциплін, план та графік навчального процесу, перелік та обсяг нормативних та вибіркових дисциплін відповідають структурно-логічній схемі підготовки здобувачів вищої освіти за спеціальністю 125 «Кібербезпека» і покликані сприяти забезпеченню відповідності програмних результатів навчання запитам потенційних роботодавців (стейкхолдерів).

ТОВ «ДОСЛІДНИЦЬКО-ТЕХНІЧНИЙ
ОСВІТНІЙ ЦЕНТР «ВОЛЬТ» Богдан ВОРОБЙОВ

РЕЦЕНЗІЯ-ВІДГУК

на магістерську освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету імені Семена Кузнеця

Робота сучасних фахівців в різних сферах діяльності, незалежно від посад, які вони обіймають, так, або інакше пов'язана з використанням інформаційних систем. Забезпечення надійної, безперебійної роботи таких інформаційних систем життєво необхідне як на загальнодержавному рівні, так і в умовах повсякденної діяльності окремих підприємств, установ, бізнес компаній, тощо. Не менш важливою функціональною складовою є захист інформації в інформаційних системах від спотворення, викрадення, або несанкціонованого використання. Підтримка та реалізація таких функції є прерогативою фахівців з кібербезпеки, роль яких посилюється, стає дедалі більш актуальною з розвитком високотехнологічного та інформатизованого суспільства.

В магістерській освітньо-професійній програмі «Кібербезпека» наголошено на актуальних потребах та основних напрямках розвитку щодо забезпечення кібербезпеки. В освітньо-професійній програмі визначені основні програмні компетентності, які передбачають підготовку фахівців у сфері кібербезпеки. Навчальний план підготовки бакалаврів освітньо-професійної програми «Кібербезпека» відповідає завданням магістерської освітньої професійної програми. Фахові компетентності, що передбачені у програмі та результати навчання забезпечують високий рівень професійної підготовки випускників, сприяють широкому діапазону їх професійної діяльності та високій конкурентоспроможності на ринку праці.

Магістерська освітньо-професійна програма «Кібербезпека», що складена та запропонована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, дозволяє забезпечити сучасну та якісну фахову підготовку магістрів за спеціальністю 125 «Кібербезпека». Освітньо-професійна програма містить в собі усі необхідні структурні та змістові складові, відображає сучасні вимоги до підготовки фахівців у сфері кібербезпеки і відповідає запитам практичного використання.

Голова департаменту ІТ комунікацій
ПП "ВКФ "Харківінтелком" Олеся КИРИЧЕНКО

University
of Bielsko-Biala

РЕЦЕНЗІЯ
на освітньо-наукову програму "КІБЕРБЕЗПЕКА"(CYBERSECURITY)
другого (освітньо-наукового) рівня вищої освіти
спеціальності 125 "КІБЕРБЕЗПЕКА" (CYBERSECURITY)

Місія та стратегічна мета рецензованої освітньо-наукової програми Харківського національного економічного університету ім. С. Кузнеця (ХНЕУ ім. С. Кузнеця) полягають в прагненні виховувати студентів на найвищому рівні, забезпечуючи їм умови для повноцінного інтелектуального розвитку та участі у різних формах наукового та культурного життя ХНЕУ ім. С. Кузнеця та інших вітчизняних і закордонних університетів, підготовляючи студентів до компетентного та свідомого функціонування в суспільстві, що динамічно розвивається та ґрунтується на знаннях. Бачення ХНЕУ ім. С. Кузнеця зводиться до забезпечення того, щоб кожен випускник здобував освіту відповідно до сучасних вимог та очікувався роботодавцями на ринку праці. Вищезазначені припущення реалізуються для досягнення наступних стратегічних цілей:

• якісна освіта на основі наукового та дослідницького досвіду;

• проведення навчального процесу, спрямованого на виховання студентів у дусі поваги до прав та гідності людини, національних почуттів та філософської толерантності, відповідальності та надійності у виконанні своїх службових обов'язків, набуття здатності постійно розвивати власну особистість та критичне мислення;

• вдосконалення навчального процесу з метою задоволення потреб ринку праці шляхом співпраці з органами місцевого самоврядування та промисловістю.

Концепція навчання студентів у галузі кібербезпеки тісно пов'язана з головною стратегічною метою факультету, а саме: постійний освітній та науковий розвиток, що передбачає високу якість та культуру освіти та досліджень, за підтримки ефективної системи управління з повною повагою до академічних цінностей та традицій.

Основою навчального процесу є відповідна послідовність навчальних дисциплін як базової, так і вибіркової складових. Визначені результати навчання вимагають активного використання раніше набутих навичок, знань та компетентностей. Форми занять визначені в плані навчального процесу. У освітньо-науковій програмі переважну більшість занять спрямовано на здобуття приктичних навиків. Інтелектуальні вміння студентів перевіряються під час лабораторних занять. У цьому випадку виявлення, аналіз, формулювання припущень та вибір інструменту для розв'язання поставлених задач значною мірою є результатом самостійної роботи студентів та вимагають їх активної участі. У той же час компетентності з англійської мови розвиваються у формі семестрового мовного курсу, індивідуальної роботи в рамках інших дисциплін з використанням англомовної літератури та документації. Завершення навчання складається з переддипломної практики та процесу дипломного проєктування, під час яких студенти дізнаються про методологію виконання та написання дипломного проєкту як з точки зору редагування, так і з застосуванням методів та інструментів дослідження. Під час занять студенти вчаться співпрацювати в групі, представляти та захищати результати своєї роботи.

Слід зазначити, що рецензованна освітньо-наукова програма розроблялася спільно з нашим Університетом, що дозволяє здійснювати спільне навчання за спеціальністю «Кібербезпека», а її рівень відповідає вимогам, які ставляться у цій галузі в Євросоюзі.

UNIVERSITY OF BIELSKO-BIALA
DEPARTMENT OF COMPUTER SCIENCE
AND AUTOMATICS
2 Willowa St, Bielsko-Biala, 43-309 Poland
tel. 33 827 92 64

PROXY of RECTOR
for Eastern Europe
Prof. D.Sc. Mikolaj Karpinski