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

УХВАЛЕНО
Рішенням Вченої ради
Харківського національного
економічного університету
імені Семена Кузнеця
від 24.06.2026 р. протокол № 8

ВВЕДЕНО В ДІЮ
Наказом ректора Харківського
національного економічного університету
імені Семена Кузнеця
від 24.06.2026 р. № 197

Тетяна ШТАЛЬ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

РІВЕНЬ ВИЩОЇ ОСВІТИ	**Другий (магістерський)**
СТУПІНЬ ВИЩОЇ ОСВІТИ	**Магістр**
ГАЛУЗЬ ЗНАНЬ	**F Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**F5 Кібербезпека та захист інформації**

Харків, 2026

ПРЕАМБУЛА

Робоча група освітньо-професійної програми «Кібербезпека»:

Тютюник Вадим Володимирович, професор кафедри кібербезпеки та інформаційних технологій, доктор технічних наук, професор, гарант освітньої програми.

Алексєєв Володимир Олегович, професор кафедри кібербезпеки та інформаційних технологій, доктор технічних наук, професор.

Поляков Андрій Олександрович, доцент кафедри інформаційних систем, кандидат технічних наук, доцент.

Муржа Дмитро Юрійович, випускник освітньої програми.

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

Розглянуто на засіданні кафедри кібербезпеки та інформаційних технологій, протокол № 14 від 13.05.2026 року.

Розглянуто вченою радою навчально-наукового інституту інформаційних технологій, протокол № 11 від 23.06.2026 р.

ОП розроблена/оновлена на підставі:

1. Законодавчих та нормативних актів: Законів України «Про освіту», «Про вищу освіту», Національної рамки кваліфікації, Національного класифікатору України.
2. Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.
3. Аналізу ринку праці, з урахуванням регіонального контексту.
4. Вивчення вітчизняного та зарубіжного досвіду.
5. Пропозицій роботодавців.
6. Рекомендації після процедур акредитації освітньої програми Національним агентством із забезпечення якості вищої освіти, протокол № 24 (41) від 15 грудня 2020 року.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузі знань	F Інформаційні технології
Спеціальності	F5 Кібербезпека та захист інформації
Спеціалізація	-
Освітня програма	Кібербезпека / Cybersecurity
Форми здобуття освіти, обсяг освітньої програми в кредитах ЄКТС та розрахункові строки виконання освітньої програми	очна (денна) форма – 90 кредитів, один рік 4 місяці
Наявність акредитації	Сертифікат про акредитацію освітньої програми НАЗЯВО № 18572, дійсний до 31.12.2027 р.
Мова(и) навчання / оцінювання	Українська
Структурний підрозділ відповідальний за ОП	Кафедра кібербезпеки та інформаційних технологій https://www.kafcbit.hneu.edu.ua/
Вимоги до зарахування	Для успішного засвоєння освітньої програми магістра вступники повинні мати вищу освіту першого (бакалаврського) рівня або другого (магістерського) рівня або освітньо-кваліфікаційний рівень спеціаліста та здібності до оволодіння знаннями, уміннями й навичками в галузі інформаційних технологій за спеціальністю кібербезпека та захист інформації. Правила та строки прийому на навчання розміщенні на сайті ХНЕУ ім. С. Кузнеця за посиланням https://pk.hneu.edu.ua/normatyvni-dokumenty/.
Обмеження щодо форм навчання	Денна, заочна, дистанційна, дуальна
Освітня кваліфікація	Магістр з кібербезпеки
Кваліфікація(-ї) професійна(-і)	Відсутня
Кваліфікація в дипломі	Ступінь вищої освіти – Магістр Спеціальність F5 Кібербезпека та захист інформації 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	-
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.
Силабуси освітні компонентів	https://hneu.edu.ua/informatsijnyj-paket-magistr-kiberbezpeka-2026

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	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. 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 F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ ОПП 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: професійна комунікація	3	Залік
ОК2	Сучасні методи децентралізованого розподілу та криптографічного захисту даних	3	Залік
ОК3	Основи моделювання та наукових досліджень в галузі кібербезпеки та захисту інформації	4	Залік
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК1	МАГ-МАЙНОР	5	Залік
ВК2	МАГ-МАЙНОР	5	Залік
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК4	Управління інформаційною безпекою, ризиками та кіберінцидентами	4	Залік
ОК5	Розширена мережева та хмарна безпека	5	Екзамен
ОК6	Безпечне програмування	5	Екзамен
ОК7	Тестування на проникнення та етичний хакінг	5	Екзамен
ОК8	Стандарти, аудит та моніторинг інформаційної безпеки	5	Залік
ОК9	Курсова робота: проєктування та впровадження систем інформаційної та	1	Курсова робота

	кібербезпеки		
ОК10	Комплексний тренінг	3	Звіт
ОК11	Переддипломна практика	12	Звіт
ОК12	Кваліфікаційна робота	15	Кваліфікаційна робота
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК3	МЕЙДЖОР 1	5	Екзамен
ВК4	МЕЙДЖОР 2	5	Екзамен
ВК5	МЕЙДЖОР 3	5	Екзамен

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ

Вибіркова складова навчального плану освітньої програми складається з: МАГ-МАЙНОРІВ, що студенти обирають з пулу вибіркових дисциплін університету та МЕЙДЖОРІВ, що обираються з пулу вибіркових дисциплін спеціальності (освітньої програми).

МАГ-МАЙНОР – умовна назва вибіркових навчальних дисциплін підготовки освітнього ступеня магістр (МАЙНОР для магістрів). Сутність МАГ-МАЙНОРів полягає у вільному виборі навчальних дисциплін таких напрямків, які відображають інтереси здобувачів вищої освіти, їх вподобання та плани на майбутнє працевлаштування. МАГ-МАЙНОР є обов’язковою складовою освітніх програм

Обсяг дисципліни МАГ-МАЙНОР – складає 5 кредитів ЄКТС. Формою підсумкового контролю є залік. Загальний обсяг дисциплін маг-майнорів складає 10 кредитів ЄКТС.

Здобувачі вищої освіти очної (денної) форми навчання обирають по одній дисципліні в 1 та 2 семестрі на першому році навчання.

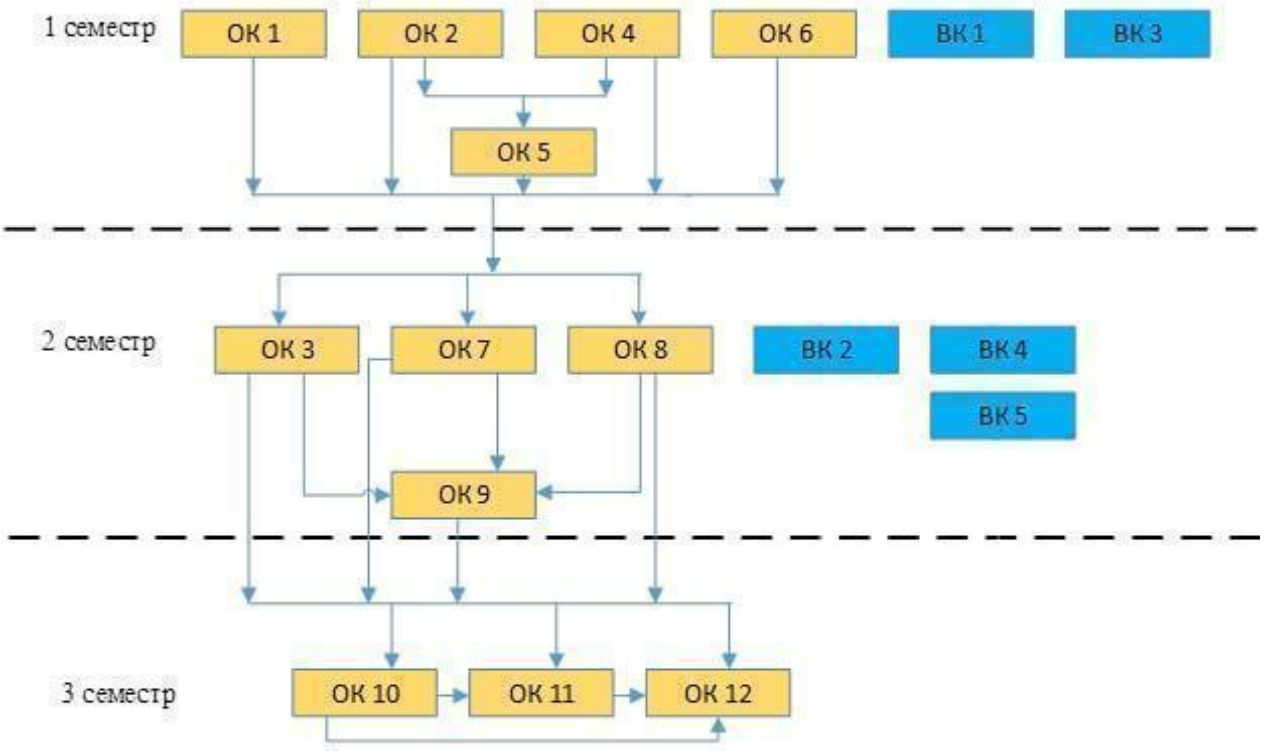
Здобувачі вищої освіти заочної форми навчання обирають 2 дисципліни на 1 році навчання.

МЕЙДЖОР - дисципліна, що обирається здобувачем вищої освіти другого (магістерського) рівня вищої освіти з пулу спеціальності та/або освітньої програми. Призначена для формування індивідуальної освітньої траєкторії та забезпечує можливості здобувачу вищої освіти поглибити професійні знання в межах обраної спеціальності та/або освітньої програми та/або здобути додаткові не фахові компетентності.

Формою підсумкового контролю є іспит. Загальний обсяг МЕЙДЖОРІВ складає 15 кредитів ЄКТС.

Вибіркові навчальні дисципліни не формують результати навчання, що передбачені стандартом вищої освіти для відповідного рівня, але можуть поглиблювати певні з них та розвивати софтскілс. Здобувачі вищої освіти заочної форми навчання обирають в якості мейджорів 3 дисципліни на 1 році навчання залежно від спеціальності (освітньої програми).

4.3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ОСВІТНЬОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА» ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ



V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи. Атестація здійснюється екзаменаційною комісією відповідно до вимог стандарту вищої освіти після виконання здобувачем вищої освіти навчального плану у формі публічного захисту кваліфікаційної роботи магістра за спеціальністю F5 Кібербезпека та захист інформації. До атестації допускаються здобувачі вищої освіти, які виконали всі вимоги освітньої програми та навчального плану.
Вимоги до кваліфікаційної роботи	ХНЕУ ім. С. Кузнеця розробляє та затверджує: Положення про атестацію здобувачів вищої освіти ХНЕУ ім. С. Кузнеця; Регламент перевірки на унікальність академічних текстів здобувачів вищої освіти та науково-педагогічних працівників ХНЕУ ім. С. Кузнеця навчально-методичним відділом. Кафедрою кібербезпеки та інформаційних технологій затверджуються нормативи унікальності текстів кваліфікаційних робіт. Кваліфікаційна робота має розв’язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення дослідження та /або здійснення інновацій. Кваліфікаційна робота – це навчально-наукова робота здобувача вищої освіти, яка виконується на завершальному етапі здобуття кваліфікації магістра для встановлення відповідності отриманих здобувачами вищої освіти результатів навчання (компетентностей) вимогам стандартів вищої освіти.

	Вона є кваліфікаційним документом, на підставі якого Екзаменаційна комісія визначає рівень теоретичної підготовки випускника, його готовність до самостійної роботи за фахом і приймає рішення щодо присвоєння відповідної кваліфікації та видачі документа про вищу освіту. Атестація осіб, які здобувають ступінь магістра, здійснюється ЕК, до складу якої можуть включатися представники роботодавців та їх об'єднань. Атестація здійснюється відкрито і публічно. У кваліфікаційній роботі не новинна містити академічнино плагіату, фабрикації, фальсифікації. Кваліфікаційні роботи допущені до захисту на кафедрі мають бути підписані кваліфікованим електронним підписом здобувача вищої освіти, оприлюднені до їх захисту у машинозчитувальному форматі, на постійній основі, з наданням вільного доступу до них без проходження автентифікації та з дотриманням інших вимог, визначених законодавством, зокрема положенням про Національний репозитарій академічних текстів, затвердженим Кабінетом Міністрів України.
Вимоги до публічного захисту	У процесі публічного захисту кандидат на присвоєння магістерського ступеня повинен показати уміння чітко і впевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь здобувача вищої освіти повинна супроводжуватися презентаційними матеріалами, призначеними для загального перегляду. Ухвалення екзаменаційною комісією рішення про присудження ступеня магістра з кібербезпеки та видачу диплома магістра за результатами атестації здобувача вищої освіти оголошується після оформлення в установленому порядку протоколів засідань екзаменаційної комісії.

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».

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. Перевірка наукових праць науково-педагогічних працівників Університету та здобувачів вищої освіти здійснюється за допомогою інтернетсервісів на основі відкритих інтернет-ресурсів та системи StrikePlagiarism.com, що діє на підставі Ліцензійного Договору про надання права користування антиплагіатним програмним забезпеченням. Нормативними документами в ХНЕУ ім. С.Кузнеця щодо регламентації є такі докумени: 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; Політика використання штучного інтелекту в освітньому процесі та наукових дослідженнях. Використання ШІ-інструментів у навчанні та дослідженнях дозволене як допоміжний засіб за умови обов'язкового декларування їх застосування та критичної оцінки отриманих результатів. Неприйнятним є видавання ШІ-контенту за власний, використання ШІ під час контрольних заходів без дозволу, а також застосування ШІ для маніпуляцій та фальсифікацій. Кваліфікаційні роботи (дипломні роботи / проєкти), підписуються кваліфікованим електронним підписом, оприлюднюються до їх захисту у машинозчитувальному форматі, на постійній основі, з наданням вільного доступу до них без проходження автентифікації та з дотриманням інших вимог.

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					ОК1, ОК10										ОК1 , ОК10
РН 2	ОК3, ОК5	ОК3, ОК9	ОК3, ОК5			ОК3, ОК5				ОК3, ОК4					
РН 3		ОК3, ОК12	ОК3, ОК9			ОК3, ОК9		ОК3, ОК9		ОК3, ОК9		ОК3, ОК9			ОК3, ОК9
РН 4	ОК2, ОК3, ОК5	ОК3, ОК9	ОК2, ОК3			ОК2, ОК3, ОК5		ОК2, ОК5				ОК5, ОК7	ОК2, ОК3		
РН 5	ОК3, ОК5	ОК3, ОК12	ОК3, ОК8	ОК8, ОК10		ОК3, ОК5	ОК3, ОК8	ОК5, ОК6	ОК4, ОК8	ОК4, ОК8		ОК5, ОК7		ОК4, ОК8	ОК3, ОК8
РН 6			ОК7, ОК8	ОК7, ОК8				ОК5, ОК7	ОК4, ОК8	ОК4, ОК8	ОК4, ОК8	ОК7, ОК8		ОК7, ОК8	
РН 7				ОК4, ОК8	ОК4, ОК8		ОК4, ОК8, ОК10		ОК4, ОК8, ОК10					ОК4, ОК8	
РН 8	ОК5, ОК9					ОК5, ОК6		ОК5, ОК9, ОК11					ОК2, ОК5		
РН 9				ОК4, ОК8	ОК4, ОК8		ОК4, ОК8		ОК4, ОК8, ОК10	ОК4, ОК8	ОК4, ОК8, ОК10			ОК4, ОК8	
РН 10	ОК4, ОК8		ОК4, ОК8	ОК4, ОК8			ОК4, ОК8		ОК4, ОК8	ОК4, ОК8,	ОК4, ОК8	ОК4, ОК8		ОК4, ОК8	

Програмні результати навчання	Компетентності														
	Загальні					Спеціальні (фахові)									
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10
										ОК10					
РН 11				ОК4, ОК8			ОК4, ОК8		ОК4, ОК8, ОК10	ОК4, ОК8	ОК4, ОК8, ОК10			ОК4, ОК8	
РН 12				ОК4, ОК7				ОК4, ОК7	ОК4, ОК10			ОК4, ОК7, ОК10			
РН 13	ОК2, ОК9			ОК2, ОК9		ОК2, ОК5		ОК2, ОК9, ОК11					ОК2, ОК9, ОК11		
РН 14			ОК8, ОК10	ОК8, ОК10			ОК8, ОК10		ОК8, ОК10	ОК8, ОК10	ОК8, ОК10	ОК8, ОК10		ОК8, ОК10, ОК12	
РН 15					ОК1, ОК12										ОК1, ОК12
РН 16	ОК4, ОК10	ОК9, ОК12	ОК4, ОК10	ОК4, ОК10	ОК10, ОК12	ОК9, ОК10	ОК4, ОК10		ОК4, ОК10	ОК4, ОК10		ОК4, ОК10		ОК4, ОК10	ОК10, ОК12
РН 17					ОК1, ОК3										ОК1, ОК3
РН 18					ОК4, ОК11				ОК4, ОК11						ОК4, ОК11
РН 19	ОК6, ОК7	ОК7, ОК9	ОК7, ОК9	ОК7, ОК10		ОК5, ОК6, ОК7		ОК5, ОК7		ОК7, ОК10		ОК7, ОК10	ОК2, ОК5	ОК7, ОК10	
РН 20	ОК9, ОК12	ОК9, ОК12	ОК9, ОК12	ОК9, ОК12		ОК9, ОК12	ОК8, ОК12	ОК9, ОК12	ОК9, ОК12	ОК9, ОК12	ОК9, ОК12	ОК9, ОК12	ОК9, ОК12	ОК9, ОК12	ОК9, ОК12

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

Гарант ОП *підписано* **Вадим ТЮТЮНИК**

ЛИСТ ПОГОДЖЕННЯ
Освітньо-професійної програми «Кібербезпека»

Назва структурного / функціонального підрозділу / посадова особа	**Підпис**
1. Навчально-методичний відділ	
2. Відділ забезпечення якості освіти	
3. Завідувач випускової кафедри	
4. Проректор з навчально-методичної роботи	

uken Uniwersytet Komisji Edukacji Narodowej w Krakowie

РЕЦЕНЗІЯ
на освітньо-професійну програму «Кібербезпека»
другого (магістерського) рівня вищої освіти
за спеціальністю F5 - Кібербезпека
галузі знань F - Інформаційні технології
Харківського національного економічного університету ім. Семена Кузнеця

Останнім часом спостерігається стрімкий ріст застосування інформаційних технологій та комп'ютерних систем в різних сферах людської діяльності. Сучасні цифрові засоби стають все складнішими, розширюється коло задач, для яких вони застосовуються. Особливої актуальності зараз набули комп'ютерні системи, що призначені для обробки фінансових транзакцій та даних економічного змісту. Важливим елементом, що супроводжують процес обробки таких критично важливих даних є система забезпечення інформаційної безпеки. Ці системи відрізняються високими вимогами та складністю щодо функцій, змісту та архітектури побудови. Саме тому актуальність підготовки фахівців з кібербезпеки дослідницького рівня є актульним завданням.

Метою поданої на рецензію освітньо-професійної програми (ОПП) є підготовка висококваліфікованих фахівців, здатних застосовувати набуті теоретичні та практичні знання, уміння та навики для розв'язання задачі дослідницького та/або інноваційного характеру та викликів професійної діяльності у сфері інформаційної та/або кібербезпеки. ОПП фокусується на особливостях:

- проектування верифікації програмно-технічних засобів, розробки програмного забезпечення комп'ютерних систем універсального та спеціального призначення, адміністрування та керування локальними, глобальними комп'ютерними мережами, інтерфейсами та протоколами взаємодії їх компонентів, що спрямовані 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;
- розробка методів та способів опрацювання інформації (включно стеганографічних та стеганофонічних), математичних моделей та технологій обчислювальних процесів, зокрема високопродуктивних, паралельних, розподілених, мобільних, а також архітектури та організації функціонування відповідних програмно-технічних засобів.

ОПП містить перелік навчальних компонентів та опис їх логічних зв'язків, матрицю забезпечення результатів навчання компонентами ОПП, визначення форми атестації здобувачів. Це дозволяє зробити висновок про зміст навчання за ОПП.

На наш погляд ОПП «Кібербезпека» другого (магістерського) рівня вищої освіти за спеціальністю F5-Кібербезпека галузі знань F-Інформаційні технології Харківського національного економічного університету ім. Семена Кузнеця є актуальною, відповідає вимогам підготовки здобувана вищої освіти рівня магістр.

Професор кафедри комп'ютерної інженерії та кібербезпеки
Університет комісії Національної світи в Кракові (Польща)

д.т.н. Анна КОРЧЕНКО

Pełnomocnik Rektora
ds. Rozwoju Dyscypliny
Informatyka Techniczna i Telekomunikacja

dr hab. Serhii Semenov

РЕЦЕНЗІЯ
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ
«КІБЕРБЕЗПЕКА»
ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ
ЗА СПЕЦІАЛЬНІСТЮ *«F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»*
«ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ
ім.. СЕМЕНА КУЗНЕЦЯ»

Компанія EPAM є найбільшою та найвідомішою IT-компанією України. Вона впевнено очолює різні рейтинги за кількістю та якістю фахівців, які співпрацюють з компанією (понад 14 тис. фахівців). В той же час, в останні роки спостерігається тренд збільшення кількості та складності проектів, до яких долучаються фахівці компанії, що в свою чергу збільшує попит компанії на підготовку якісних фахівців. Рішення цього завдання компанія бачить у активній співпраці з навчальними закладами. З цього погляду підготовка якісних фахівців-магістрів на кафедрі кібербезпеки та інформаційних технологій Харківського Національного Економічного Університету ім. Семена Кузнеця є актуальним завданням, що потребує тісної співпраці університету та компанії.

Можливості кафедри кібербезпеки та інформаційних технологій Харківського Національного Економічного Університету ім. Семена Кузнеця у підготовці якісних фахівців підкреслюються наявністю висококваліфікованого викладацького складу, серед яких можливо окремо виділити:

7 викладачів, що мають фаховий досвід співробітництва з провідними IT-компаніями або стартапами;

10 викладачів, що пройшли стажування у провідних IT-компаніях, та отримали відповідні сертифікати;

2 викладачів є сертифікованими фахівцями таких компаній як Microsoft, Google, Cisco, Oracle, AWS.

Харківський Національний Економічний Університет ім. Семена Кузнеця має відповідний досвід, розуміння культури інновацій, потужний кадровий потенціал та матеріально-технічну базу для виконання завдання підготовки IT-фахівців за обраним фокусом.

Проаналізувавши структуру програми та освітні компоненти, можна відзначити таке:

структура програми відповідає вимогам стандарту освіти у рамках спеціальності «F5 Кібербезпека та захист інформації;

структурно-логічна схема підготовки здобувачів вищої освіти пройшла спільну верифікацію представниками кафедри та спеціалістами компанії EPAM, що зафіксовано у відповідному протоколі засідання кафедри;

крім основних, стандартних форм навчання (лекції, практичні та лабораторні роботи, самостійна робота та ін.) у структурі програми передбачені інноваційні форми навчання, такі як самостійне та групове проектне навчання, комплексний

тренінг, ІТ-марафон.

Позитивною стороною освітньо-професійної програми є те що її розробка виконувалась співробітниками університету у співпраці з фахівцями компанії та ІТ-співтовариства:

зміст робочих програм та силабусів навчальних компонент «Безпечне програмування», «Розширена мережева та хмарна безпека» було верифіковано фахівцями компанії ЕРАМ, що зафіксовано у протоколі засідання кафедри;

побажання фахівців компанії щодо структурної та змістовної складових ОПП враховані та реалізовані у відповідних пунктах 4.1 та 4.3.

Висновки:

Зважаючи на позитивний досвід університету у підготовці фахівців, серед яких декілька осіб на поточний момент співпрацюють з компанією ЕРАМ та спираючись на результати рецензування вважаємо, що освітньо-професійна програма «КІБЕРБЕЗПЕКА» другого (магістерського) рівня вищої освіти за спеціальністю «F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ» ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ ім. СЕМЕНА КУЗНЕЦЯ відповідає сучасним вимогам підготовки ІТ-фахівців та рекомендується до продовження терміну акредитації.

Заступник генерального директора
ТОВ "ЕПАМ СИСТЕМЗ" Надія БАБЕЙКО

Громадська спілка "Харківський
кластер інформаційних технологій"
вул.Громадянська 11/13,
м.Харків, 61057 Україна
+38 (050) 658-88-46
olga.shapoval@it-kharkiv.com
www.it-kharkiv.com

Рецензія

на освітньо-професійну програму «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти в Харківському національному економічному університеті імені Семена Кузнеця

У сучасних умовах інформаційна безпека є критично важливою для національної стійкості України, яка щоденно протистоїть масштабним кібератакам і технологічним загрозам. Освітньо-професійна програма «Кібербезпека» другого (магістерського) рівня вищої освіти в Харківському національному економічному університеті імені Семена Кузнеця створена саме для формування висококваліфікованих фахівців, здатних захищати критичну інформаційну інфраструктуру держави та бізнесу. Її структура та зміст враховують як фундаментальні теоретичні засади, так і сучасні практичні інструменти – від управління кібербезпекою та мережевого захисту до етичного хакінгу та тестування на проникнення, що гарантує готовність випускників ефективно протистояти реальним загрозам.

Програма охоплює весь спектр необхідних тем. Особливу увагу привертає поєднання теоретичної підготовки з практичними завданнями: робота з кіберполігоном, виконання курсових проєктів і проходження переддипломної практики у реальних ІТ-підрозділах створюють умови, що максимально наближені до тих, з якими доводиться стикатися фахівцям під час щоденної роботи над забезпеченням інформаційного захисту.

Важливо відзначити, що програма передбачає достатні можливості для формування індивідуальної траєкторії навчання здобувача освіти. Наявність маг-майнорів і мейджорів дозволяє студентам самостійно формувати траєкторію з урахуванням актуальних потреб роботодавців та власних кар'єрних цілей. Цей підхід сприяє гнучкості й адаптивності випускників, які залежно від обраних курсів можуть поглиблювати знання у сфері хмарної

безпеки, розробки безпечного програмного забезпечення чи аналітики кіберзагроз.

Крім того, програма робить акцент на інтеграції безпеки у життєвий цикл проєкту. Студенти отримують навички автоматизованого тестування та моніторингу загроз. Такий підхід відповідає світовим трендам і дозволяє майбутнім фахівцям відразу долучатися до робочих процесів у провідних IT-компаніях і стартапах.

Водночас для підвищення конкурентоспроможності випускників пропонується розширити компоненти програми шляхом проходження курсів із машинного навчання та аналітики кіберзагроз, де студенти вивчатимуть алгоритми обробки великих обсягів логів та поведінковий аналіз інцидентів. Додаткову цінність матиме впровадження практичних занять із безпеки контейнерів і мікросервісів, а також поглиблених модулів із цифрової криміналістики й реагування на інциденти, під час яких магістранти навчаться збирати докази та проводити розслідування складних атак.

Узагальнюючи, можна констатувати, що «Кібербезпека» в ХНЕУ ім. С.Кузнеця має міцний фундамент і відповідає запитам роботодавців. Програма здатна підготувати фахівців із широким спектром компетенцій, але шлях до її вдосконалення лежить через доповнення сучасними темами аналітики та управління безпекою у хмарних і контейнерних середовищах, а також поглиблення дисциплін із цифрової криміналістики. Впровадження цих доповнень зробить програму ще привабливішою для студентів і дозволить їм

відповідати найвищим професійним стандартам світового IT-ринку.

Виконавчий директор
ГС «Харківський кластер
інформаційних технологій» Ольга ШАПОВАЛ

2026 рік

РЕЦЕНЗІЯ
на освітньо-професійну програму «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти в Харківському національному економічному університеті ім. С. Кузнеця

Програма демонструє системний підхід до формування професійних компетентностей у сфері кібербезпеки. Структура навчального плану збалансована: поєднує фундаментальні теоретичні дисципліни, сучасні прикладні курси, практику та науково-дослідну складову. Програма відповідає вимогам часу — орієнтується на захист критичної інфраструктури, розвиток DevSecOps, тестування на проникнення, етичний хакінг, безпечне програмування. Це формує у випускника комплексне бачення галузі.

Сильними сторонами програми є: сучасність та актуальність дисциплін; практична спрямованість із включенням практики, тренінгів та дипломної роботи; гнучкість вибору освітніх компонентів; якісне забезпечення процесу через чітко прописані компетентності, результати навчання та використання механізмів академічної доброчесності.

У рекомендаційному порядку можна звернути увагу на посилення інтеграції практичних кейсів і симуляцій інцидентів, оновлення курсів відповідно до динаміки загроз, додавання невеликих блоків міждисциплінарного характеру (зокрема, щодо нормативної бази та процедур поводження з цифровими доказами), а також розширення співпраці з практиками галузі через гостьові лекції та воркшопи.

Загалом, освітньо-професійна програма «Кібербезпека» відповідає сучасним викликам та здатна забезпечити високу якість підготовки фахівців. Вона формує у випускників як глибокі теоретичні знання, так і практичні навички, необхідні для роботи в IT-індустрії, державному секторі чи дослідницьких структурах. Запропоновані доповнення є рекомендаційними та спрямовані лише на посилення практичної складової і міждисциплінарності, не змінюючи основної концепції програми.

Начальник Управління протидії кіберзлочинам
в Харківській області
Департаменту кіберполіції НПУ **Валерій БЕРЕЗА**