МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ В ЕКОНОМІЦІ»

Першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 Кібербезпека
галузі знань 12 Інформаційні технології

Кваліфікація: ступінь вищої освіти «бакалавр»
спеціальність «Кібербезпека»

спеціалізація «Безпека інформаційних і комунікаційних систем в економіці»

Нова редакція

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ КНТЕУ
Голова вченої ради
_____/А.А. Мазаракі/
(протокол № 3 від «28» 11 2018 р.)

Освітня програма вводиться в дію з 1.12 2018 р.
Ректор_____/А.А. Мазаракі/
(наказ № 461 від «1» 12 2018 р.)

Київ 2018 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

Погоджено
Перший проректор
з науково-педагогічної роботи
_____ Н. В. Притульська
23.11 2018 р.

Погоджено
Проректор
з науково-педагогічної роботи
_____ С. Л. Шаповал
22.11 2018 р.

Погоджено
Начальник навчального відділу
КНТЕУ
_____ К. В. Мостика
21.11 2018 р.

Погоджено
Начальник навчально-методичного
відділу КНТЕУ
_____ Т. В. Божко
21.11 2018 р.

Погоджено
Завідувач кафедри програмної
інженерії та інформаційних
систем
_____ О. В. Криворучко
12.11 2018 р.

Погоджено
Представник РСС
_____ Антоневич М. Є.
13.11 2018 р.

Погоджено
Заступник директора Центра
Сертифікаційного навчання
ТОВ «ПРОКОМ»
_____ Столярчук І. А.
15.11 2018 р.

Погоджено
Начальник Департаменту кіберполіції
Національної поліції України,
кандидат юридичних наук
_____ Демедюк С. В.
19.11 2018 р.

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Пашорін Валерій Іванович – к.т.н., професор кафедри бойового застосування та навігації, керівник освітньої програми;
2. Харченко Олександр Анатолійович – декан факультету обліку, аудиту і інформаційних систем, к.т.н, доц.;
3. Криворучко Олена Володимирівна – завідувач кафедри програмної інженерії та інформаційних систем, д.т.н., проф.;
4. Цензура Микола Олександрович – к.т.н., доцент кафедри інформаційних систем та мереж;
5. Чубаєвський Віталій Іванович – заступник директора Департаменту кіберполіції Національної поліції України, к.політ.н.;
6. Щетініна Олена Костянтинівна – завідувач кафедри вищої та прикладної математики, д.ф-м.н., проф.;
7. Шестак Ярослав Іванович – директор головного центру інформаційних технологій КНТЕУ;
8. Десятко Альона Миколаївна – асистент кафедри програмної інженерії та інформаційних систем.

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Демедюк Сергій Васильович – начальник Департаменту кіберполіції Національної поліції України, кандидат юридичних наук, м. Київ;
2. Столярчук Ірина Аркадіївна – заступник директора Центра Сертифікаційного навчання ТОВ «ПРОКОМ» м. Київ.

1. Профіль освітньої програми зі спеціальності 125 «Кібербезпека» (за спеціалізацією «Безпека інформаційних і комунікаційних систем в економіці»)

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Київський національний торговельно-економічний університет Кафедра програмної інженерії та інформаційних систем
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Кваліфікація ступінь вищої освіти «бакалавр» спеціальність «Кібербезпека» спеціалізація «Безпека інформаційних і комунікаційних систем в економіці»
Офіційна назва освітньої програми	«Безпека інформаційних і комунікаційних систем в економіці»
Тип диплому та обсяг освітньої програми	Перший (бакалаврський), одиничний 240 кредитів ЄКТС Термін навчання – 3 роки 10 місяців
Наявність акредитації	–
Цикл/рівень	FQ for EHEA – перший цикл, НРК України – 7 рівень, EQF for LLL – 6 рівень
Передумови	Повна загальна середня освіта, початковий рівень вищої освіти
Мова(и) викладання	Українська мова
Термін дії освітньої програми	До наступного планового оновлення
Інтернет - адреса постійного розміщення опису освітньої програми	https://www.knteu.kiev.ua/
2 - Мета освітньої програми	
Формування сучасної системи професійних знань і навичок у сфері безпеки інформаційних і комунікаційних систем підприємства (організації). Формування особистості, здатної на основі набутих інтегральних, загальних (інструментальних, міжособистісних, системних) та фахових компетентностей успішно працювати у сфері IT-технологій забезпечення безпеки інформаційних і комунікаційних систем підприємства організації.	
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань 12 «Інформаційні технології» Спеціальність 125 «Кібербезпека» Спеціалізація «Безпека інформаційних і комунікаційних систем в економіці» Дисципліни циклу: обов'язкові компоненти: загальної підготовки – 84%; професійної підготовки – 72%; вибіркові компоненти: загальної підготовки – 31,5%; професійної підготовки – 30%; практичної підготовки – 22,5%.

Орієнтація освітньої програми	Програма орієнтована на освітньо-професійний та прикладний напрямок підготовки.
Основний фокус освітньої програми та спеціалізації	Спеціальна. Вища освіта за спеціальністю 125 «Кібербезпека» в галузі інформаційних технологій. Здатність організовувати та підтримувати комплекс заходів щодо забезпечення безпеки інформаційних систем та мереж підприємства (організації), з урахуванням їхньої юридичної та економічної обґрунтованості, технічної реалізації, запобігання можливих зовнішніх впливів, ймовірних загроз і застосування технологій захисту інформації. Ключові слова: безпека інформаційних та телекомунікаційних систем; криптографічні методи захисту інформації; теорія чисел; безпека операційних систем та мереж.
Особливості програми	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення ІБ, інформаційних технологій захисту інформації в інформаційно-комунікаційних системах підприємства, технологій збереження даних в єдиному інформаційному просторі та впровадженню функцій протидій кіберзлочинності.
4 - Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT). Може займати наступні посади: – менеджер (управитель) систем з інформаційної безпеки (1495); – – помічник керівника іншого основного підрозділу; – фахівець (сфера захисту інформації); – фахівець із організації інформаційної безпеки (3439); – фахівець з режиму секретності; – інспектор з організації захисту секретної інформації; – аналітик систем забезпечення кібербезпеки; – фахівець з організації та проведення тестування на проникнення.
Подальше навчання	Навчання за програмою підготовки магістра 8 рівня НРК України, другого циклу FQ-EHEA та 7 рівня EQF-LLL.
5 - Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, самонавчання, навчання через лабораторну практику. проблемні, інтерактивні, проектні, інформаційно-комп'ютерні, саморозвиваючі, колективні та інтегративні, контекстні технології навчання.
Оцінювання	**Види контролю:** – за рівнями: самоконтроль, контроль на рівні викладача, контроль на рівні завідувача кафедри, контроль на рівні деканату, контроль на рівні директора, атестація; **Форми контролю:** усне та письмове опитування, тестування, презентація наукової роботи, захист курсових робіт. Поточний контроль, підсумковий контроль – екзамени та заліки, захист випускної кваліфікаційної роботи.

6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	**КЗ 1.** Здатність застосовувати знання у практичних ситуаціях. **КЗ 2**. Знання та розуміння предметної області та розуміння професії. **КЗ 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **КЗ 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **КЗ 5.** Здатність до пошуку, оброблення та аналізу інформації. **КЗ 6.** Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. **КЗ 7.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. **КЗ 8.** *Базові знання з основ економіки та підприємницької діяльності.*
Фахові компетентності (КФ)	**КФ 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **КФ 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. **КФ 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **КФ 4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. **КФ 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. **КФ 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **КФ 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

	КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **КФ 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. **КФ 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. **КФ 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **КФ 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. ***КФ 13.*** *Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення із забезпечення кібербезпеки.* ***КФ 14.*** *Здатність здійснювати управління ризиками інформаційної та кібербезпеки.*
7 - Програмні результати навчання	
	1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **2.** Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. **3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **4.** Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. **5.** Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. **6.** Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. **7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. **8.** Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. **9.** Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. **10.** Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. **11.** Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. **12.** Розробляти моделі загроз та порушника.

	13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. **14**. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. **15.** Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. **16.** Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. **17.** Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. **18.** Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. **19.** Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. **20.** Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. **21.** Вирішувати задачі забезпечення та супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **22.** Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки. **23.** Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **24.** Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). **25.** Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. **26.** Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

	27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. **28.** Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. **29.** Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. **30.** Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. **31.** Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. **32.** Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. **33.** Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. **34.** Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. **35.** Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки. **36.** Виявляти небезпечні сигнали технічних засобів. **37.** Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. **38.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. **39.** Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. **40.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. **41.** Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. **42.** Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

	43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів. **44.** Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. **45.** Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. **46.** Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. **47.** Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. **48.** Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. **49.** Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. **50.** Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). **51.** Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. **52.** Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. **53.** Вирішувати задачі аналізу програмного коду на наявність можливих загроз. **54.** Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ***55.*** *Аналізувати економічну ефективність заходів інформаційної безпеки.* ***56.*** *Застосувати знання методів техніко-економічного аналізу й обґрунтування проєктних рішень.*
8 - Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Проектна група: 4 кандидати наук. Всі розробники є штатними співробітниками Київського національного торговельно-економічного університету До реалізації програми залучаються науково-педагогічні працівники з науковими ступенями та/або вченими званнями, а також висококваліфіковані спеціалісти. З метою підвищення фахового рівня всі науково-педагогічні працівники один раз на п'ять років проходять стажування.

Матеріально-технічне забезпечення	Використання лабораторій, комп'ютерних та спеціалізованих аудиторій КНТЕУ
Інформаційне та навчально-методичне забезпечення	Діюча система дистанційного невчання MOODLE та середовище MS Officce 365 забезпечує самостійну та індивідуальну роботу студентів
9 - Академічна мобільність	
Національна кредитна мобільність	Організація кредитної мобільності (окрім 1-го курсу) бакалаврів. Проект компанія «EPAM Systems Україна», ДП «Український інститут інтелектуальної власності», Центр сертифікованого навчання «Проком», освітня компанія «Пірсон Ед`юкейшн», корпорація «Парус», група компаній «BGS Solutions».
Міжнародна кредитна мобільність	Організація кредитної мобільності (окрім 1-го курсу) бакалаврів. Проект Університет Парі Ест Кретей (м. Париж, Франція), Бізнес-школа «Ауденсія» (м. Нант, Франція, Університет Гренобль Альпи (м. Гренобль, Франція). Університет Центрального Ланкаширу (м. Престон, Великобританія), Університет Хоенхайм (м. Штутгарт, Німеччина).
Навчання іноземних здобувачів вищої освіти	Передбачено.

2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
1. Обов'язкові компоненти ОП			
1.1 Цикл загальної підготовки			
ОК 1.	Лінійна алгебра та аналітична геометрія	6	екзамен
ОК 2.	Іноземна мова за професійним спрямуванням	24	екзамен
ОК 3.	Правознавство	6	екзамен
ОК 4.	Математичний аналіз	6	екзамен
ОК 5.	Комп'ютерна дискретна математика	6	екзамен
ОК 6.	Безпека життя	6	екзамен
ОК 7.	Філософія	6	екзамен
ОК 8.	Економіка підприємства	6	екзамен
ОК 9.	Теорія ймовірності та математична статистика	6	екзамен
ОК 10.	Теорія чисел	6	екзамен
ОК 11.	Правове забезпечення інформаційної безпеки держави	6	екзамен
	Фізичне виховання		залік
1.2 Цикл професійної підготовки			
ОК 12.	Алгоритмізація та програмування	12	екзамен
ОК 13.	Об'єктно-орієнтоване програмування	12	екзамен
ОК 13.1	Курсова робота з об'єктно-орієнтованого програмування		
ОК 14.	Архітектура комп'ютера	6	екзамен
ОК 15.	Операційні системи	6	екзамен
ОК 16.	Архітектура та проектування програмного забезпечення	6	екзамен
ОК 17.	Безпека інформаційних систем та мереж	6	екзамен
ОК 17.1	Курсова робота з безпеки інформаційних систем та мереж		
ОК 18.	Організація комп'ютерних мереж	6	екзамен

згідно М № 503

ОК 19.	Бази даних	6	екзамен
ОК 20.	Криптографічні методи захисту інформації	6	екзамен
ОК 21.	Безпека телекомунікаційних мереж	6	екзамен
Загальний обсяг обов'язкових компонент:		156	
2. Вибіркові компоненти ОП			
2.1. Цикл загальної підготовки			
ВБ 1.1	Історія економіки та економічної думки	6	екзамен
ВБ 1.2.	Історія України	6	екзамен
ВБ 1.3.	Історія української культури	6	екзамен
ВБ 2.1.	Українська мова (за професійним спрямуванням)	6	екзамен
ВБ 2.2.	Світова культура	6	екзамен
ВБ 3.1.	Інженерна та комп'ютерна графіка	6	екзамен
ВБ 3.2.	Фізика	6	екзамен
ВБ 3.3.	Електротехніка	6	екзамен
ВБ 4.1.	Договірне право	6	екзамен
ВБ 4.2.	Інформаційне право	6	екзамен
ВБ 5.1.	Психологія безпеки	7,5	екзамен
ВБ 5.2.	Інженерна психологія та психологія праці	7,5	екзамен
2.2. Цикл професійної підготовки			
ВБ 6.1.	Технологія Java	6	екзамен
ВБ 6.2.	Людино-машинна взаємодія	6	екзамен
ВБ 6.3.	WEB-дизайн і WEB-програмування	6	екзамен
ВБ 7.1.	Безпека операційних систем	6	екзамен
ВБ 7.2.	Експертні системи	6	екзамен
ВБ 7.3.	Штучний інтелект	6	екзамен
ВБ 8.1.	Безпека систем баз даних	6	екзамен
ВБ 8.2.	Методи і засоби передачі даних	6	екзамен
ВБ 8.3.	Безпека програмного забезпечення	6	екзамен
ВБ 9.1.	Менеджмент проектів програмного забезпечення	6	екзамен
ВБ 9.2.	Управління проектами інформатизації	6	екзамен
ВБ 9.3.	Економіка і організація інформаційного бізнесу	6	екзамен
ВБ 10.1.	Моделювання та аналіз програмного забезпечення	6	екзамен

зміни НН 1488 ВВ 2.5 Логіка 6 екзамен

Зміни наказ №041

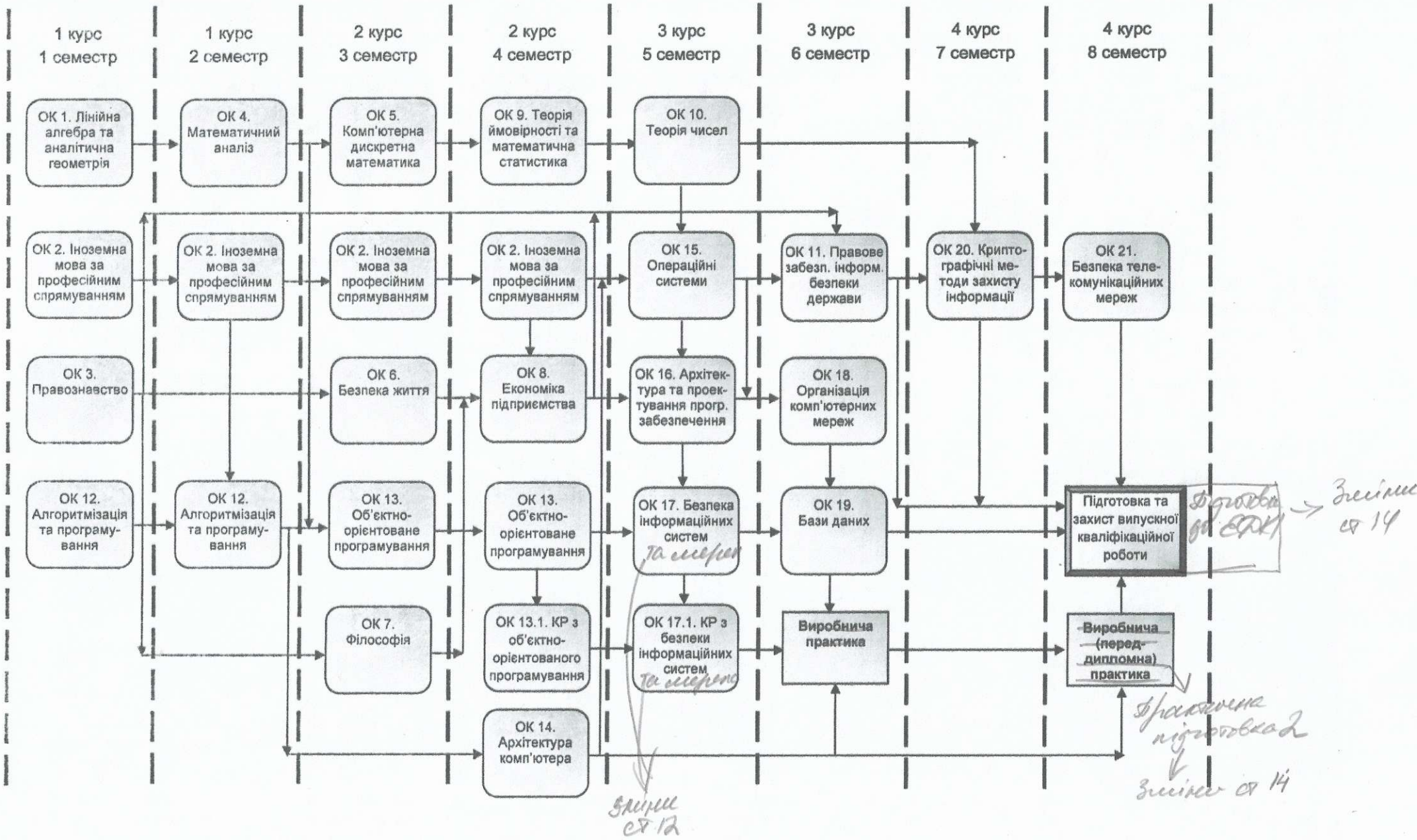
ВБ 10.2.	Моделювання ~~економічних~~ бізнес процесів	6	екзамен
Загальний обсяг вибіркових компонент:		61,5	
3. Практична підготовка			
Виробнича практика		6	залік
~~Виробнича (переддипломна) практика~~ практичне підготовка		6	залік
4. Атестація			
~~Підготовка випускної кваліфікаційної роботи~~		10,5	захист
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГАМИ		240	

Зміни наказ №132

Підготовка до ВКР та захист 4,5 захист

Підготовка до СДКІ 3 екзамен

2.2. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Атестація випускників здійснюється у формі публічного захисту випускної кваліфікаційної роботи.

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за стандартом вищої освіти.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Випускна кваліфікаційна робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки, *зокрема в економіці.*

Випускна кваліфікаційна робота має бути перевірена на плагіат.

Випускна кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу КНТЕУ або його підрозділу, або у репозитарії закладу вищої освіти.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 2.1	ВБ 2.2	ВБ 3.1	ВБ 3.2	ВБ 3.3	ВБ 4.1	ВБ 4.2	ВБ 5.1	ВБ 5.2	ВБ 6.1	ВБ 6.2	ВБ 6.3	ВБ 7.1	ВБ 7.2	ВБ 7.3	ВБ 8.1	ВБ 8.2	ВБ 8.3	ВБ 9.1	ВБ 9.2	ВБ 9.3	ВБ 10.1	ВБ 10.2
КЗ 1	+	+		+	+			+	+	+		+	+	+	+	+	+	+	+	+	+	+					+	+	+	+	+	+	+		+	+	+	+	+	+		+		+	+	+	+
КЗ 2													+	+		+		+		+	+							+	+						+						+		+			+	+
КЗ 3		+																							+											+											
КЗ 4															+	+	+		+	+							+									+		+	+	+	+		+	+	+	+	+	+
КЗ 5	+			+	+	+			+	+		+			+		+	+	+			+													+		+	+	+	+	+	+	+	+	+	+	+
КЗ 6			+			+					+												+	+		+				+	+	+	+														
КЗ 7			+				+	+			+												+	+		+								+													
КЗ 8								+																																								
КФ 1			+			+					+																			+	+	+	+														
КФ 2												+	+								+																+	+		+					+	+
КФ 3														+							+																										
КФ 4																	+																		+							+	+	+		
КФ 5															+		+		+		+																+			+		+					
КФ 6																		+			+																										
КФ 7											+																																					
КФ 8																	+				+																+	+		+			+	+		
КФ 9																	+				+																										
КФ 10																				+																											
КФ 11																+					+																									+	+
КФ 12															+		+	+	+																		+	+	+	+		+					
КФ 13												+																																				
КФ 14								+														+																										

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 2.1	ВБ 2.2	ВБ 3.1	ВБ 3.2	ВБ 3.3	ВБ 4.1	ВБ 4.2	ВБ 5.1	ВБ 5.2	ВБ 6.1	ВБ 6.2	ВБ 6.3	ВБ 7.1	ВБ 7.2	ВБ 7.3	ВБ 8.1	ВБ 8.2	ВБ 8.3	ВБ 9.1	ВБ 9.2	ВБ 9.3	ВБ 10.1	ВБ 10.2
1		+																							+																						
2	+			+	+				+	+													+			+																+	+	+		
3							+			+			+									+	+	+		+	+						+									+			+	+
4							+			+													+																				+	+	+	+
5												+	+											+									+	+					+				+				
6						+																+																									
7			+			+					+																		+	+																
8			+			+					+																		+	+																
9			+								+														+					+	+	+														
10										+		+		+									+																	+					+	
11												+		+										+										+	+									+	+		
12																		+																												+	+
13																		+																	+								+			+	
14														+	+	+	+		+		+																+			+		+				+	
15														+		+											+									+					+					
16															+		+		+		+								+	+						+			+		+		+	+		
17															+	+	+		+		+															+			+		+				+	
18														+		+												+	+																	
19															+		+		+		+															+			+	+	+					
20														+	+		+		+		+															+			+	+	+				+	
21													+		+		+		+		+				+									+			+			+		+	+				
22									+																																		+	+	+		
23																					+											+						+	+							
24																	+																										+	+	+		
25						+																										+	+													
26																		+														+						+	+							
27															+		+		+		+															+			+		+					
28															+		+		+		+															+			+		+	+	+	+		+

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 2.1	ВБ 2.2	ВБ 3.1	ВБ 3.2	ВБ 3.3	ВБ 4.1	ВБ 4.2	ВБ 5.1	ВБ 5.2	ВБ 6.1	ВБ 6.2	ВБ 6.3	ВБ 7.1	ВБ 7.2	ВБ 7.3	ВБ 8.1	ВБ 8.2	ВБ 8.3	ВБ 9.1	ВБ 9.2	ВБ 9.3	ВБ 10.1	ВБ 10.2
29																					+																	+	+								
30																					+																	+	+								
31																	+																								+						
32																	+																					+	+								
33										+													+																				+	+	+		
34															+		+		+		+																+			+		+					
35																					+																	+	+								
36																	+																								+	+					
37															+		+		+		+																+			+							
38																					+																										
39						+					+																																				
40											+																																				
41																			+														+							+			+	+	+		
42																	+																														
43											+																			+	+																
44																				+																							+	+	+		
45											+																																+	+	+		
46												+																										+	+								
47																				+																											+
48																		+		+																											+
49																					+																						+	+	+		
50														+		+																															
51														+																								+	+								
52																					+																										
53																+																						+	+								
54			+				+																							+	+	+	+														
55								+																																							
56												+																																			

Аркуш реєстрації змін

№ пор.	Дата	Пункти, до яких вносяться зміни	Ініціатор зміни	Прізвище, ініціали особи, що відповідає за внесення змін	Підпис
1.	11.05 2018	2.1. ВК 2.3. згідно Н №[illegible]	група забезпечення	[illegible] В.І.	
2.	25.11 2019	2.2. ВК10.1 згідно Н № 4021	група забезпечення	Криворученко О.В	
3.	05.02 2021	2.1. ОК17, ОК21 згідно Н № 503	група забезпечення	Десятко Д.М.	
4.	07.06 2021	2.1. „Практична підготовка" згідно Н №311	група забезпечення	Савченко Т.В.	
5.	08.07 2021	2.1. „Атестація" згідно Н № 1598	група забезп.	Десятко Д.М.	