55

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В ЕКОНОМІЦІ»/ «SECURITY OF ELECTRONIC COMMUNICATIONS SYSTEMS IN THE ECONOMY»

Другого (магістерського) рівня вищої освіти
за спеціальністю 125 Кібербезпека та захист інформації
галузі знань 12 Інформаційні технології

Кваліфікація: ступінь вищої освіти магістр
спеціальність «Кібербезпека та захист інформації»

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ ДТЕУ
Голова вченої ради
_____ /АнатолійМАЗАРАКІ
(протокол № 5 від «21» грудня 2023 р.)

Освітня програма вводиться в дію з 01.09 2024 р.
Ректор_____ /Анатолій МАЗАРАКІ
(наказ № 607 від «21» грудня 2023 р.)

Київ 2023

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми ДТЕУ

Погоджено
Перший проректор з науково-педагогічної роботи
(посада)
_____ Наталія ПРИТУЛЬСЬКА
(підпис) (ім'я, прізвище)
19. 12. 2023 р.

Погоджено
Проректор з науково-педагогічної роботи та міжнародних зв'язків
(посада)
_____ Анжеліка ГЕРАСИМЕНКО
(підпис) (ім'я, прізвище)
19.12 2023 р.

Погоджено
Начальник навчального відділу ДТЕУ
(посада)
_____ Сергій КАМІНСЬКИЙ
(підпис) (ім'я, прізвище)
18. 12. 2023 р.

Погоджено
Начальник навчально-методичного відділу ДТЕУ
(посада)
_____ Тетяна БОЖКО
(підпис) (ім'я, прізвище)
19. 12. 2023 р.

Погоджено
Декан факультету інформаційних технологій ДТЕУ
(посада)
_____ Олександр ХАРЧЕНКО
(підпис) (ім'я, прізвище)
04. 12. 2023 р.

Погоджено
Завідувач кафедри інженерії ПЗ та кібербезпеки ДТЕУ
(посада)
_____ Олена КРИВОРУЧКО
(підпис) (ім'я, прізвище)
04. 12 2023 р.

Погоджено
Керівник групи забезпечення спеціальності ДТЕУ
_____ Тетяна САВЧЕНКО
(підпис) (ім'я, прізвище)
04. 12. 2023 р.

Погоджено
Гарант освітньої програми ДТЕУ
_____ Тетяна САВЧЕНКО
(підпис) (ім'я, прізвище)
04. 12. 2023 р.

Погоджено
Керівник управління інформаційної безпеки Апарату РНБО України
_____ Володимир ЗВЄРЄВ
(підпис) (ім'я, прізвище)
05. 12. 2023 р.

Погоджено
Заступник директора ТОВ «IT-biz solutions»
_____ Сергій ЧОРНОУС
(підпис) (ім'я, прізвище)
07. 12 2023 р.

Погоджено
Представник РСС факультету
_____ Олександра ІГНАТОВИЧ
(підпис) (ім'я, прізвище)
04. 12 2023 р.

РЕЦЕНЗІЯ

на освітньо-професійну програму
«Безпека систем електронних комунікацій в економіці»
другого (магістерського) рівня вищої освіти
за спеціальністю 125 «Кібербезпека та захист інформації»
галузі знань 12 «Інформаційні технології»

Представлена на рецензування освітньо-професійна програма «Безпека систем електронних комунікацій в економіці» направлена на підготовку висококваліфікованих, конкурентоспроможних фахівців, здатних розв'язувати професійні задачі, пов'язані з системами електронних комунікацій, зокрема в економіці.

Програма передбачає підготовку професіоналів, здатних: моделювати та прогнозувати можливі кібервпливи на суб'єкти господарювання економіки держави та фізичних осіб; проводити аудит систем електронних комунікацій суб'єктів господарювання; застосовувати нормативні документи та стандарти в розробці заходів по захисту систем електронних комунікацій суб'єктів господарювання економіки держави.

Структурно-логічна схема освітньої програми є збалансованою та відображає логіку здійснення освітнього процесу, а також зв'язки між освітніми компонентами, що забезпечують системність у досягненні визначених цілей навчання. Позитивною рисою освітньої програми є також залучення до складу групи розробників не лише адміністративного складу та науково-педагогічних працівників університету, а й стейкхолдерів з числа роботодавців та здобувачів вищої освіти.

Професійні компетентності мають як практичний, так і науковий зміст і можуть бути використані в професійній діяльності майбутніх фахівців. Тенденції розвитку ринку праці показують, що вказані в ОПП цілі дозволяють здобувачам вищої освіти бути конкурентоспроможними на ринку праці.

Вважаю, що освітньо-професійна програма «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» є своєчасною та перспективною, а також відповідає актуальним запитам сьогодення ти вимогам стандартів ІТ.

Заст. керівника служби з питань
інформаційної безпеки та кібербезпеки –
керівник управління інформаційної безпеки
Апарату РНБО України, дійсний член
Української академії кібербезпеки,
к.т.н., с.н.с. *В.П. Звєрєв*

РЕЦЕНЗІЯ
на освітньо-професійну програму
«Безпека систем електронних комунікацій в економіці»
другого (магістерського) рівня вищої освіти
за спеціальністю 125 Кібербезпека та захист інформації
галузі знань 12 Інформаційні технології

Подана на рецензування Державним торговельно-економічним університетом освітня програма «Безпека систем електронних комунікацій в економіці» розроблена у відповідності до стандарту другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології та орієнтована на освітньо-професійний та прикладний напрямок підготовки фахівців.

Програма спрямована на поєднання практики та науки щодо організації, розробки та експлуатації комплексних складових кіберпростору з метою забезпечення інформаційної безпеки суб'єктів господарювання економіки держави з урахуванням можливих зовнішніх кібервпливів, ймовірних загроз і рівня розвитку технологій захисту систем електронних комунікацій.

Представлена ОПП логічно структурована. Загальний обсяг програми складає 90 кредитів ЄКТС та включає всі види аудиторної та самостійної роботи здобувачів, практики та час, що відводиться для контролю якості засвоєння студентами освітніх компонент програми.

До реалізації освітньої програми залучаються науково-педагогічні працівники з науковими ступенями та вченими званнями, а також висококваліфіковані спеціалісти та фахівці-практики. Єдиний цифровий простір ДТЕУ поєднує всі підрозділи, що направлені на формування індивідуальної освітньої траєкторії здобувачі вищої освіти.

Програмні результати навчання освітньої програми корелюють із складовими професійної компетентності, які формують фундаментальні знання та фахові навички, а загальні компетентності забезпечують розвиток soft skills та сприяють формуванню високих моральних і ділових якостей, здатності до фахового розвитку та самовдосконалення.

Вважаю, що освітньо-професійна програма «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти є актуальною, відповідає вимогам вищої школи та ринку праці та може бути рекомендована для впровадження в навчальний процес.

Заступник директора
ТОВ «IT-biz solutions» С.М. Чорноус

ПЕРЕДМОВА

Розроблено робочою групою в складі:

1. Савченко Тетяна Віталіївна – к.т.н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки, гарант освітньої програми;
2. Криворучко Олена Володимирівна – д.т.н., професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки;
3. Токар Володимир Володимирович – д.е.н., професор, професор кафедри інженерії програмного забезпечення та кібербезпеки;
4. Власенко Лідія Олександрівна – к.т.н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
5. Харченко Олександр Анатолійович – к.т.н, доцент, декан факультету інформаційних технологій;
6. Десятко Альона Миколаївна – PhD, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
7. Котенко Наталія Олексіївна – к.пед.н. доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
8. Жирова Тетяна Олександрівна – к.пед.н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
9. Чубаєвський Віталій Іванович – д.е.н., доцент, начальник Управління виявлення та розшуку активів центрального апарату Агентства з Розшуку та Менеджменту Активів;
10. Лахно Валерій Анатолійович – д.т.н, проф., завідувач кафедри комп'ютерних систем, мереж та кібербезпеки національного університету біоресурсів та природокористування України;
11. Хохлачова Юлія Євгеніївна - к.т.н., доцент, професор кафедри безпеки інформаційних технологій Національного авіаційного університету
12. Шаяхметова Олександра Русланівна – студентка факультету інформаційних технологій, 2 курсу, 7м групи, спеціальність «Кібербезпека».
13. Збіцька Катерина Олександрівна – студентка факультету інформаційних технологій, 1 курсу, 9м групи, спеціальність «Кібербезпека та захист інформації».

Рецензії-відгуки зовнішніх стейкголдерів:

1. Звєрєв Володимир Павлович – заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату РНБО України, кандидат технічних наук, старший науковий співробітник;
2. Чорноус Сергій Миколайович – заступник директора ТОВ «IT-biz solutions».

1. Профіль освітньої програми «Безпека систем електронних комунікацій в економіці» зі спеціальності 125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва ЗВО та структурного підрозділу	Державний торговельно-економічний університет, Факультет інформаційних технологій, Кафедра інженерії програмного забезпечення та кібербезпеки.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти магістр спеціальність «Кібербезпека та захист інформації»
Офіційна назва освітньої програми	«Безпека систем електронних комунікацій в економіці»
Відповідність стандарту вищої освіти МОН України	Відповідає СВО МОН України
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС
Наявність акредитації	Сертифікат про акредитацію ОПП, виданий НАЗЯВО, № 6526 від 14.12.2023 р. до 12.12.2024 р.
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Для здобуття освітнього рівня «магістр» зі спеціальності 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» можуть вступати особи, які здобули освітній рівень «бакалавр». Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти.
Мова(и) викладання	Українська
Термін дії освітньої програми	1 рік 4 місяці
Інтернет-адреса постійного розміщення опису освітньої програми	https://knute.edu.ua
2 – Мета освітньої програми	
Забезпечити здобувачам вищої освіти другого (магістерського) рівня фундаментальну підготовку за спеціальністю 125 «Кібербезпека та захист інформації», що є достатньою для вирішення задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки в галузі економіки.	

3 - Характеристика освітньої програми	
Предметна область	**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 (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; системи управління інформаційною безпекою та/або кібербезпекою; 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 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. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.

Орієнтація освітньої програми	Програма орієнтована на освітньо-професійний та прикладний напрямок підготовки. Акцент програми зроблений на формуванні фахівця, що здатний розв'язувати професійні задачі, пов'язані з системами електронних комунікацій, зокрема в економіці.
Основний фокус освітньої програми	Освітньо-професійний. Програма спрямована на поєднання практики та науки, щодо організації, розробки та експлуатації комплексних складових кіберпростору з метою забезпечення інформаційної безпеки суб'єктів господарювання економіки держави з урахуванням можливих зовнішніх кібервпливів, ймовірних загроз і рівня розвитку технологій захисту систем електронних комунікацій. Ключові слова: технології безпеки безпроводових та мобільних мереж, технології безпеки Web-ресурсів, тестування на проникнення, вразливість системи, система управління інформаційною безпекою суб'єкту господарювання, правове забезпечення інформаційної безпеки в економічних системах, економічна безпека держави.
Особливості програми	Програма передбачає підготовку професіоналів, здатних: моделювати та прогнозувати можливі кібервпливи на суб'єкти господарювання економіки держави та фізичних осіб; проводити аудит систем електронних комунікацій суб'єктів господарювання; застосовувати нормативні документи та стандарти в розробці заходів по захисту систем електронних комунікацій суб'єктів господарювання економіки держави.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець спроможний виконувати професійні роботи і займати посади, визначені Національним класифікатором України «Класифікатор професій ДК 003:2010», зокрема: Збирання, оброблення, аналізування та поширення результатів оцінювання кіберзагроз/сигналів попередження. Дослідження, аналіз та участь у реагуванні на кіберінцеденти в кіберпросторі що відповідають професійному стандарту «Аналітик з безпеки інформаційно-телекомунікаційних систем» (завтверджений 25.11.22р. Наказ Адміністрації Держспецзв'язку № 715)
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
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	Оцінювання навчальних досягнень студентів здійснюється на основі: «Положення про організацію освітнього процесу студентів»; «Положення про оцінювання результатів навчання студентів і аспірантів у ДТЕУ». За 100-бальною шкалою. Письмові екзамени, практична підготовка, презентації, тестування, захист лабораторних робіт, захист індивідуальних проєктів, захист кваліфікаційної роботи.

6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (КЗ)	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). *КЗ-6. Здатність діяти соціально відповідально та громадсько свідомо.* *КЗ-7. Здатність до адаптації та дії у новій ситуації.* *КЗ-8. Здатність до вибору стратегії спілкування, працювати в команді.* *КЗ-9. Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.*
Фахові компетентності (КФ)	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. *КФ11. Здатність аналізувати електронні комунікаційні мережі та протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, зокрема в економіці.* *КФ12. Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області.* *КФ13. Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки.*
7 – Програмні результати навчання	
	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. Приймати обґрунтовані рішення та вживати відповідних технічних та організаційних заходів для забезпечення безпеки електронних комунікаційних мереж та послуг з метою гарантування цілісності власних електронних комунікаційних мереж, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до електронних комунікаційних мереж.* *РН25. Виконувати обов'язки внутрішнього консультанта/радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації.* *РН26. Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу).* *РН27. Проводити сканування систем безпеки інформаційних ресурсів на вразливості.* *РН28. Застосовувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності.*

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	До реалізації програми залучаються науково-педагогічні працівники з науковими ступенями та/або вченими званнями, а також висококваліфіковані спеціалісти та фахівці-практики.
Матеріально-технічне забезпечення	Використання лабораторій, комп'ютерних та спеціалізованих аудиторій, бібліотеки та інфраструктури ДТЕУ вцілому.
Інформаційне та навчально-методичне забезпечення	Єдиний цифровий простір Університету поєднує всі підрозділи, які направлені на формування індивідуальної траєкторії здобувача вищої освіти. Діюча система дистанційного навчання MOODLE та середовище MS 365 забезпечує самостійну та індивідуальну роботу студентів.
9 – Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність здійснюється відповідно до укладених договорів про академічну мобільність
Міжнародна кредитна мобільність	Міжнародна кредитна мобільність реалізується за рахунок укладання договорів про міжнародну академічну мобільність (Еразмус+), про подвійне дипломування, про тривалі міжнародні проєкти, які передбачають навчання студентів, видачу подвійного диплому, тощо.
Навчання іноземних здобувачів вищої освіти	Передбачено, за умови обов'язкового знання української мови на рівні не нижче В1.

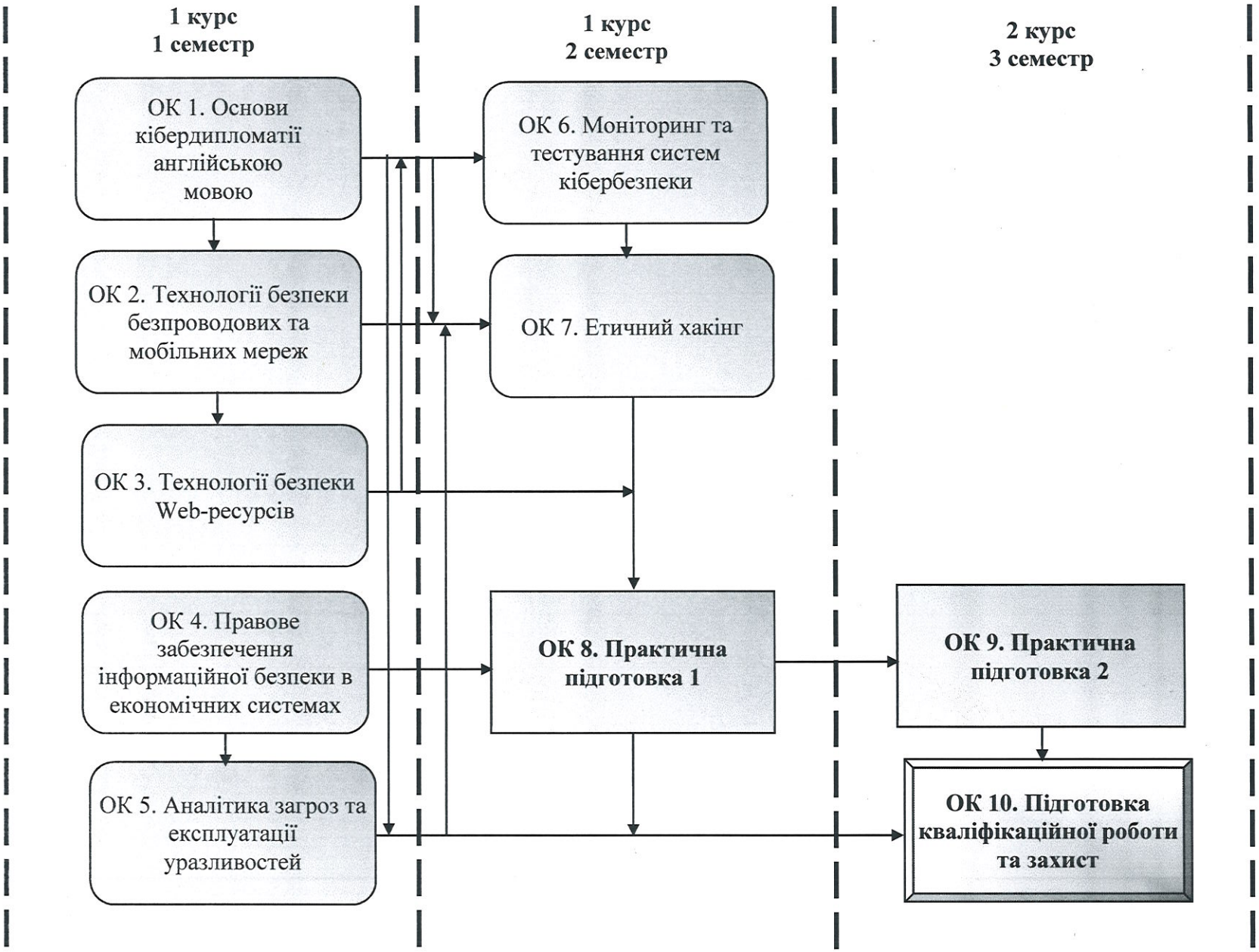
2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційний екзамен, випускна кваліфікаційна робота)	Кількість кредитів
1	2	3
Обов'язкові компоненти ОП		
ОК 1.	Основи кібердипломатії англійською мовою	6
ОК 2.	Технології безпеки безпроводових та мобільних мереж	6
ОК 3.	Технології безпеки Web-ресурсів	6
ОК 4.	Правове забезпечення інформаційної безпеки в економічних системах	6
ОК 5.	Аналіз загроз та експлуатації уразливостей	6
ОК 6.	Моніторинг та тестування систем кібербезпеки	6
ОК 7.	Етичний хакінг	6
ОК 8.	Практична підготовка 1	12
ОК 9.	Практична підготовка 2	3
ОК 10.	Підготовка кваліфікаційної роботи та захист	9
Загальний обсяг обов'язкових компонент:		**66**
Вибіркові компоненти ОП		
ВК 1	UI/UX дизайн англійською мовою	6
ВК 2.	Адміністрування та захист сховищ даних	6
ВК 3.	Безпека мобільних додатків	6
ВК 4.	Безпека технологій інтернету речей	6
ВК 5.	Біометричні технології аутентифікації в інформаційних системах	6
ВК 6.	Інструментальні засоби бізнес-аналітики	6
ВК 7.	Інтелектуальна власність	6
ВК 8.	Інформаційні технології у системі забезпечення економічної безпеки держави	6
ВК 9.	IT-право	6
ВК 10.	Правове регулювання безпеки підприємницької діяльності	6
ВК 11.	Психологія адаптації	6
ВК 12.	Психологія бізнесу	6
ВК 13.	Стохастичні методи в економіці	6
ВК 14.	Технології аналізу даних	6
ВК 15.	Філософія особистості	6
ВК 16.	Функціональне та логічне програмування	6
Загальний обсяг вибіркових компонент:		**24**
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**

Для всіх компонентів освітньої програми формою підсумкового контролю є екзамен.

2.2. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі публічного захисту 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.

4. Матриця відповідності програмних компетентностей обов'язковим компонентам освітньої програми

Компоненти / Компетентності	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10
КЗ-1.	+	+	+	+	+	+	+	+	+	+
КЗ-2.		+	+	+	+		+			+
КЗ-3.	+				+	+	+			+
КЗ-4.			+		+	+		+	+	
КЗ-5.	+	+		+	+		+			
КЗ-6.	+			+	+		+			
КЗ-7.	+			+	+			+	+	
КЗ-8.	+			+				+	+	
КЗ-9.	+							+	+	+
КФ1.		+	+	+	+	+	+	+	+	+
КФ2.	+	+	+	+		+	+	+	+	+
КФ3.		+		+	+	+	+	+	+	+
КФ4.	+	+		+			+	+	+	+
КФ5.	+	+	+		+		+	+	+	+
КФ6.			+					+	+	+
КФ7.			+					+	+	+
КФ8.								+	+	+
КФ9.		+				+	+	+	+	+
КФ10.	+			+			+	+	+	+
КФ11.		+				+		+	+	+
КФ12.	+	+	+	+		+	+	+	+	+
КФ13.		+	+			+	+	+	+	+

5. Матриця забезпечення програмних результатів навчання відповідними обов'язковими компонентами освітньої програми

Компоненти / Програмні результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10
РН1	+	+		+			+	+	+	+
РН2	+	+					+	+	+	+
РН3	+						+	+	+	+
РН4		+	+				+	+	+	+
РН5	+			+	+	+		+	+	+
РН6			+	+	+	+		+	+	+
РН7	+		+	+				+	+	+
РН8		+					+	+	+	+
РН9		+					+	+	+	+
РН10		+	+		+		+	+	+	+
РН11		+	+				+	+	+	+
РН12			+	+				+	+	+
РН13		+					+	+	+	+
РН14				+		+		+	+	+
РН15	+	+	+		+	+	+	+	+	+
РН16	+		+					+	+	+
РН17	+	+		+			+	+	+	+
РН18	+						+	+	+	+
РН19			+					+	+	+
РН20		+					+	+	+	+
РН21								+	+	+
РН22			+	+				+	+	+
РН23			+		+	+		+	+	+
РН24		+						+	+	+
РН25	+	+	+	+			+	+	+	+
РН26	+			+				+	+	+
РН27		+	+				+	+	+	+
РН28		+	+				+	+	+	+

Аркуш реєстрації змін

№ пор.	Дата	Пункти, до яких вносяться зміни	Ініціатор зміни	Прізвище, ініціали особи, що відповідає за внесення змін	Підпис