МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ 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

галузі знань 12 Інформаційні технології

Кваліфікація: ступінь вищої освіти магістр

спеціальність «Безпека систем електронних комунікацій в економіці»

спеціалізація «Безпека систем електронних комунікацій в економіці»

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ КНТЕУ
Голова вченої ради
_____ /А. А. Мазаракі/
(протокол № __ від "___"_____ 2021 р.)

Освітня програма вводиться в дію з _____2022 р.
Ректор_____ /А. А. Мазаракі/
(наказ № __ від "___"_____ 2021 р.)

Київ 2021

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми КНТЕУ

Погоджено
Перший проректор з науково-педагогічної роботи
(посада)
_____ _Н.В. Притульська__
(підпис) (ініціали, прізвище)
_____ 20_____

Погоджено
Проректор з наукової роботи
(посада)
_____ С.В. Мельниченко___
(підпис) (ініціали, прізвище)
_____ 20_____

Погоджено
Начальник навчального відділу КНТЕУ

_____ _С.І. Камінський_
(підпис) (ініціали, прізвище)
_____ 20_____

Погоджено
Начальник навчально-методичного відділу КНТЕУ

_____ _Т.В. Божко_
(підпис) (ініціали, прізвище)
_____ 20_____

Погоджено
Декан факультету інформаційних технологій_КНТЕУ
(назва факультету)

_____ _О.А. Харченко____
(підпис) (ініціали, прізвище)
_____ 20_____

Погоджено
Завідувач кафедри _інженерії ПЗ та кібербезпеки_КНТЕУ
(назва кафедри)

_____ _О.В. Криворучко_
(підпис) (ініціали, прізвище)
_____ 20_____

Погоджено
Керівник групи забезпечення спеціальності КНТЕУ
_____ В.І. Пашорін_
(підпис) (ініціали, прізвище)
_____ 20_____

Погоджено
Гарант освітньої програми КНТЕУ

_____ _В.І. Пашорін _
(підпис) (ініціали, прізвище)
_____ 20_____

Погоджено
Керівник управління інформаційної безпеки Апарату РНБО України
_____ __ В.П. Звєрєв___
(підпис) (ініціали, прізвище)
_____ 202__р.____

Погоджено
Заступник директора ТОВ «IT-biz solutions»
_____ ___С.М. Чорноус__
(підпис) (ініціали, прізвище)
_____ 202___р.____

Погоджено
Представник РСС факультету

_____ _____
(підпис) (ініціали, прізвище)

_____ 20_____

ПЕРЕДМОВА

Розроблено робочою групою в складі:

1. Пашорін Валерій Іванович – професор, к.т.н., професор кафедри інженерії програмного забезпечення та кібербезпеки, гарант освітньої програми;
2. Криворучко Олена Володимирівна – професор, д.т.н., завідувач кафедри інженерії програмного забезпечення та кібербезпеки;
3. Токар Володимир Володимирович – професор, доктор економічних наук, професор кафедри інжтенерії програмного забезпечення та кібербезпеки, гарант освітньої програми;
4. Сашньова Маряна Василівна – к.т.н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
5. Савченко Тетяна Віталіївна – к.т.н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
6. Харченко Олександр Анатолійович – к.т.н, доцент, декан факультету інформаційних технологій;
7. Десятко Альона Миколаївна – PhD, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
8. Котенко Наталія Олексіївна – к.пед.н. доцент кафедри інженерії програмного забезпечення та кібербезпеки;
9. Жирова Тетяна Олександрівна - к.пед.н. доцент кафедри інженерії програмного забезпечення та кібербезпеки;
10. Чубаєвський Віталій Іванович – заступник директора Департаменту інформаційно-аналітичної підтримки Національної поліції України, к.політ.н., доц;
11. Демедюк Сергій Васильович – заступник Секретаря Ради національної безпеки і оборони України, генерал поліції 3-го рангу, доцент кафедри інженерії програмного забезпечення та кібербезпеки;
12. Лахно Валерій Анатолійович – д.т.н, проф., завідувач кафедри комп'ютерних систем, мереж та кібербезпеки національного університету біоресурсів та природокористування України
13. Лукова-Чуйко Наталія Вікторівна – д.т.н., проф., завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
14. Бойко Тарас Віталійович – студент факультету інформаційних технологій, 2 курсу, 11 групи, спеціальність «Кібербезпека».
15. Чудік Михайло – студент факультету інформаційних технологій, 2 курсу, 6м групи, спеціальність «Інженерія програмного забезпечення».

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 зі спеціальності 121 «Інженерія програмного забезпечення» (за спеціалізацією «Інженерія програмного забезпечення»)

1 – Загальна інформація	
Повна назва ЗВО та структурного підрозділу	Київський національний 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» спеціалізація «Безпека систем електронних комунікацій в економіці»
Офіційна назва освітньої програми	«Безпека систем електронних комунікацій в економіці»
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра
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», 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 (галузь знань, спеціальність, спеціалізація (за наявності**))**	Галузь знань 12 «Інформаційні технології» Спеціальність 125 «Кібербезпека» Спеціалізація «Безпека систем електронних комунікацій в економіці»
Орієнтація освітньої програми	Програма орієнтована на освітньо-професійний та прикладний напрямок підготовки
Основний фокус освітньої програми та спеціалізації	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 економіки держави; 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: 1495 Менеджери (управителі) систем з інформаційної безпеки; 1210.1 Керівник підприємства (установи, організації) (сфера захисту інформації); 2149.2 Професіонал із організації інформаційної безпеки ; Професіонал із організації захисту інформації з обмеженим доступом; 3439 Фахівець із організації інформаційної безпеки; Фахівець з режиму секретності; Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки; Інспектор з організації захисту секретної інформації. Випускник може обіймати інші посади відповідно до професійних назв робіт, що характеризуються спеціальними (фаховими) компетентностями.
Подальше навчання	Навчання за програмами: третього освітнього (освітньо-наукового) рівня, першого наукового ступеня
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	«Положення про організацію освітнього процесу студентів» «Положення про оцінювання результатів навчання студентів і аспірантів». Письмові екзамени, практика, есе, презентації, тестування, захист лабораторних робіт, захист індивідуальних робіт, захист випускної 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 (ЗК)	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).
Спеціальні (фахові, предметні) компетентності (СК)	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.
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.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Проектна група: 2 доктора; 2 кандидата наук. Всі розробники є 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 не рідше ніж 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 навчання MOODLE та середовище MS Office 365 забезпечує самостійну та індивідуальну роботу студентів.
9 – Академічна мобільність	
Національна кредитна мобільність	Організація кредитної мобільності Проект компанія «ЕПАМ СИСТЕМЗ», ДП «Український інститут інтелектуальної власності», Центр сертифікованого навчання «Проком», освітня компанія «Пірсон Ед`юкейшн», Корпорація «Парус», група компаній «BGS », ТОВ «IT-biz solutions», Національний координаційний центр кібербезпеки РНБО України, громадська спілка «КіберКовчер».
Міжнародна кредитна мобільність	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.

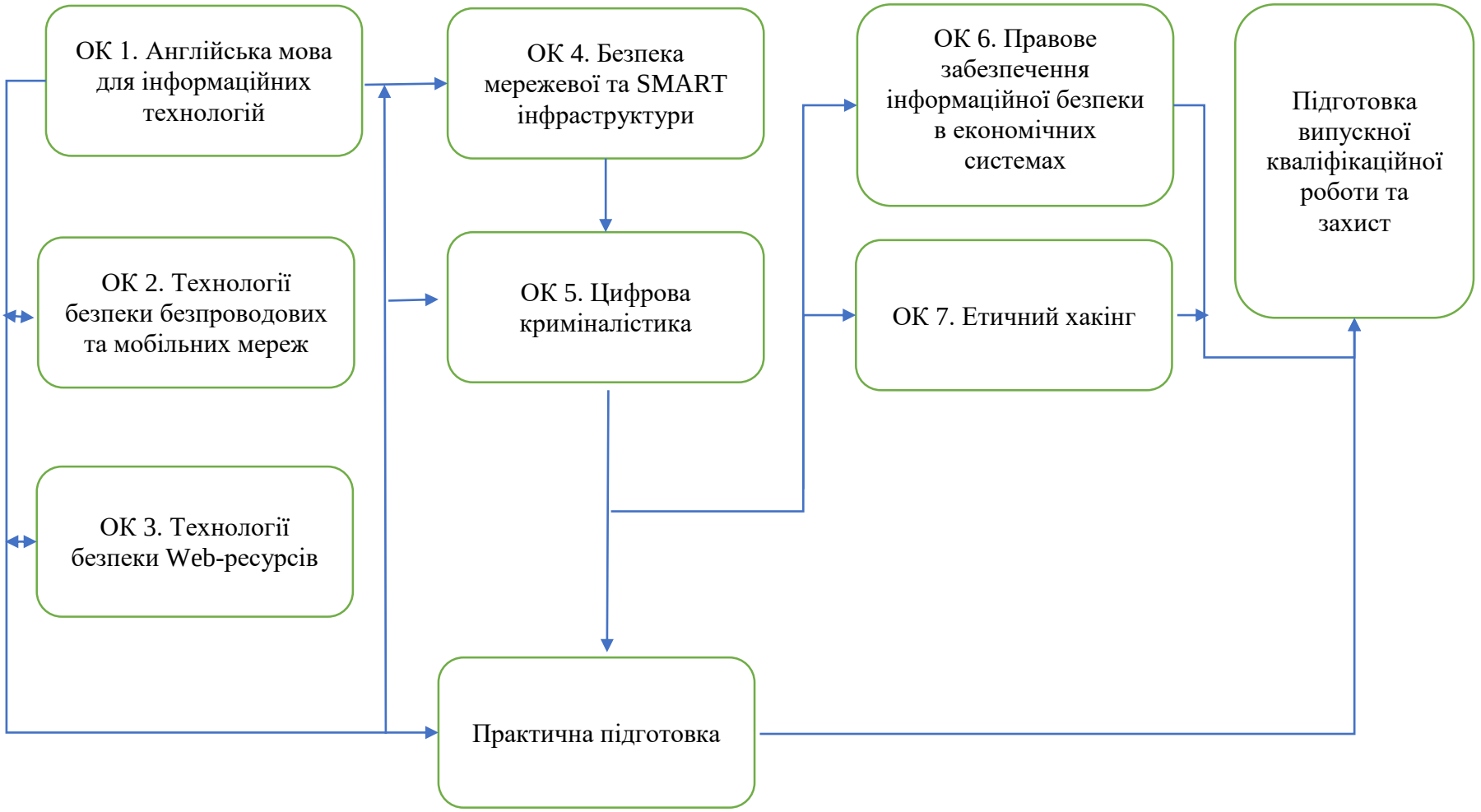
2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційний екзамен, випускна кваліфікаційна робота)	Кількість кредитів
1	2	3
Обов'язкові компоненти ОП		
ОК 1.	Англійська мова інформаційних технологій	6
ОК 2.	Технології безпеки безпроводових та мобільних мереж	6
ОК 3.	Технології безпеки Web-ресурсів	6
ОК 4.	Безпека мережевої та SMART інфраструктури	7,5
ОК 5.	Цифрова криміналістика	7,5
ОК 6.	Правове забезпечення інформаційної безпеки в економічних системах	6
ОК 7.	Етичний хакінг	6
Загальний обсяг обов'язкових компонент:		**45**
Вибіркові компоненти ОП		
ВК 1	Адміністрування та захист сховищ даних	6
ВК 2.	Безпека мобільних додатків	6
ВК 3.	Безпека технологій інтернету речей	6
ВК 4.	Біометричні технології аутентифікації в інформаційних системах	6
ВК 5.	Інструментальні засоби бізнес-аналітики	
ВК 6.	Інтелектуальна власність	6
ВК 7.	Інформаційні технології у системі забезпечення економічної безпеки держави	6
ВК 8.	IT-право	
ВК 9.	Комерційна розвідка та внутрішня безпека на підприємстві	6
ВК 10.	Психологія адаптації	6
ВК 11.	Психологія бізнесу	6
ВК 12.	Стохастичні методи в економіці	6
ВК 13.	Технології аналізу даних	6
ВК 14.	Філософія особистості	6
ВК 15.	Функціональне та логічне програмування	6
Загальний обсяг вибіркових компонент:		24
Практична підготовка		
Практична підготовка		9
Атестація		
Підготовка випускної кваліфікаційної роботи та захист		12
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

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту випускної кваліфікаційної роботи.
Вимоги до випускної 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.

4.1. 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
КЗ-1.	+	+	+	+	+	+	+
КЗ-2.	+		+			+	+
КЗ-3.		+			+	+	
КЗ-4.		+		+	+		+
КЗ-5.	+		+	+	+	+	+
КФ1.	+	+	+	+		+	+
КФ2.	+	+		+	+	+	+
КФ3.		+	+			+	+
КФ4.		+		+		+	
КФ5.		+	+		+		
КФ6.		+		+			
КФ7.			+	+	+		+
КФ8.		+				+	
КФ9.		+		+	+		+
КФ10.	+		+	+		+	

4.2. Матриця відповідності програмних компетентностей вибірковим компонентам освітньої програми

Компоненти / Компетентності	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15
КЗ-1.	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
КЗ-2.	+			+	+		+			+	+			+	+
КЗ-3.	+	+	+	+						+	+				+
КЗ-4.		+		+			+					+		+	
КЗ-5.	+	+	+	+	+	+	+	+	+	+	+	+			
КФ1.		+		+		+							+		+
КФ2.	+		+	+	+									+	
КФ3.	+			+			+								
КФ4.		+		+					+						
КФ5.		+	+	+								+			
КФ6.	+			+									+		
КФ7.		+		+											
КФ8.	+						+							+	
КФ9.			+		+										
КФ10.	+								+						

5.1. 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
РН1	+				+	+	
РН2		+		+			
РН3			+		+	+	
РН4		+			+		+
РН5	+	+		+		+	
РН6		+	+		+		+
РН7	+	+		+			+
РН8		+			+	+	
РН9			+			+	
РН10		+			+		
РН11			+			+	
РН12			+			+	+
РН13		+			+		
РН14		+	+				
РН15	+		+		+		
РН16		+		+			
РН17			+	+		+	
РН18			+		+	+	
РН19		+		+			
РН20			+		+	+	
РН21			+			+	
РН22	+		+		+		+
РН23	+	+				+	+

5.2. Матриця забезпечення програмних результатів навчання відповідними вибірковими компонентами освітньої програми

Компоненти / Програмні результати навчання	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15
РН01	+	+		+	+	+	+	+		+	+	+		+	
РН02			+	+					+				+		+
РН03				+					+			+			
РН04	+			+	+										+
РН05				+					+				+		
РН06		+		+					+						
РН07	+		+	+		+						+			
РН08				+						+					
РН09			+	+											
РН10	+		+	+					+						
РН11					+										
РН12				+			+						+		
РН13			+												
РН14			+												
РН15	+			+											
РН16				+					+						+
РН17				+											
РН18			+												
РН19				+											
РН20		+		+											
РН21				+											
РН22				+											
РН23		+		+			+					+		+	+

Аркуш реєстрації змін

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