

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ
СИСТЕМ В ЕКОНОМІЦІ» / «SECURITY OF INFORMATION AND
COMMUNICATION SYSTEMS IN THE ECONOMY»**

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

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

**ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ ДТЕУ**

Голова вченої ради

_____ /Анатолій МАЗАРАКІ/

(протокол № ____ від «__» _____ 2023 р.)

Освітня програма вводиться в дію з _____ 2023 р.

Ректор _____ / Анатолій МАЗАРАКІ /

(наказ № ____ від «__» _____ 2023 р.)

Київ 2023 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Погоджено

Перший проректор
з науково-педагогічної роботи

_____ **Наталія ПРИТУЛЬСЬКА**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Проректор
з наукової роботи

_____ **Світлана МЕЛЬНИЧЕНКО**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Начальник навчального відділу
ДТЕУ

_____ **Сергій КАМІНСЬКИЙ**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Начальник навчально-методичного
відділу ДТЕУ

_____ **Тетяна. БОЖКО**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Декан факультету
інформаційних технологій

_____ **Олександр ХАРЧЕНКО**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Завідувач кафедри інженерії
програмного забезпечення та
кібербезпеки

_____ **Олена КРИВОРУЧКО**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Керівник групи забезпечення
спеціальності ДТЕУ

_____ **Тетяна САВЧЕНКО**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Гарант освітньої програми
ДТЕУ

_____ **Тетяна ЖИРОВА**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Заступник Міністра оборони
України

_____ **Олег ГАЙДУК**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Заступник директора
ТОВ «IT-biz solutions»

_____ **Сергій ЧОРНОУС**
(підпис) (ім'я, прізвище)
_____ 2023 р.

Погоджено

Представник РСС факультету

_____ **Антон. КУШКА**
(підпис) (ім'я, прізвище)
_____ 2023 р.

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Жирова Тетяна Олександрівна – доцент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ (гарант), к.пед.н.;
2. Власенко Лідія Олександрівна – доцент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ, к.т.н., доцент;
3. Савченко Тетяна Віталіївна – доцент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ, к.т.н., доцент;
4. Харченко Олександр Анатолійович – декан факультету інформаційних технологій ДТЕУ, к.т.н., доцент;
5. Криворучко Олена Володимирівна – завідувач кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ, д.т.н., професор;
6. Палагута Катерина Олексіївна – доцент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ, к.ек.н.;
7. Десятко Альона Миколаївна – доцент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ, PhD;
8. Тищенко Дмитро Олександрович – доцент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ, к.ек.н.;
9. Зверев Володимир Павлович – доцент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ, заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління забезпечення діяльності Національного координаційного центру кібербезпеки Апарату РНБО України, к.т.н., с.н.с.;
10. Костюк Юлія Володимирівна – асистент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ;
11. Хорольська Карина Вікторівна асистент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ;
12. Чернишова Дарина Дмитрівна асистент кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ;
13. Екштейн Валерія Віталіївна – студентка факультету інформаційних технологій, 2 курсу, 12 групи, спеціальність «Кібербезпека»;
14. Збіцька Катерина Олександрівна – студентка факультету інформаційних технологій, 4 курсу, 13 групи, спеціальність «Кібербезпека».

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Чорноус Сергій Миколайович – заступник директора ТОВ «IT-biz solutions» м. Київ;
2. Гайдук Олег Васильович – заступник Міністра оборони України

1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем в економіці» зі спеціальності 125 «Кібербезпека та захист інформації»

1 - Загальна інформація	
Повна назва закладу вищої освіти 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 бакалавр спеціальність «Кібербезпека та захист інформації»
Офіційна назва освітньої програми	«Безпека інформаційних і комунікаційних систем в економіці»
Відповідність стандарту вищої освіти МОН України	Відповідає СВО МОН України затвердженого наказом від 04.10.2018 р. № 1074
Тип диплому та обсяг освітньої програми	Перший (бакалаврський), одиничний 240 кредитів ЄКТС Термін навчання – 3 роки 10 місяців
Наявність акредитації	2022 р
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-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://knute.edu.ua
2 - Мета освітньої програми	
<p>Формування сучасної системи професійних знань і навичок у сфері безпеки інформаційних і комунікаційних систем підприємства (організації), <i>зокрема в економіці</i>.</p> <p>Формування особистості, здатної на основі набутих інтегральної, загальних та фахових компетентностей успішно працювати у сфері ІТ-технологій, забезпечення безпеки інформаційних і комунікаційних систем підприємства (організації), <i>зокрема в економіці</i>.</p>	

3 - Характеристика освітньої програми

<p>Предметна область</p>	<p><i>Об'єкти професійної діяльності випускників:</i></p> <ul style="list-style-type: none"> – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. <p><i>Цілі навчання</i> підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.</p> <p><i>Теоретичний зміст предметної області</i></p> <p><i>Знання</i></p> <ul style="list-style-type: none"> – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. <p><i>Методи, методика та технології:</i></p> <p>Методи, методика, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки.</p> <p><i>Інструменти та обладнання:</i></p> <ul style="list-style-type: none"> – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
<p>Орієнтація освітньої програми</p>	<p>Освітньо-професійна. Спрямована на підготовку фахівців, що поєднують фундаментальні математичні, інформаційні та економічні положення з практичними навичками роботи у сфері кібербезпеки та інформаційних технологій, застосовуючи алгоритми, методи і технології розробки програмного забезпечення та криптографічні методи захисту інформації.</p>

Основний фокус освітньої програми та спеціалізації	<p>Спеціальна. Вища освіта за спеціальністю 125 «Кібербезпека та захист інформації» в галузі інформаційних технологій. Здатність організувати 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.</p> <p>Ключові слова: безпека інформаційних та телекомунікаційних систем; криптографічні методи захисту інформації; теорія чисел; безпека операційних систем та мереж.</p>
Особливості програми	<p>Програма створює наступний ланцюг: завдання, знання, вміння, здатності, професійна активність, професійний контекст, робоча зона, інтереси, професійні стилі, професійні цінності, суміжні професії, заробітна платня. Для розкриття сутності перелічених складових використовується модульний принцип.</p> <p>Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення ІБ, інформаційних технологій захисту інформації в інформаційно-комунікаційних системах підприємства, зокрема в економіці, технологій збереження даних в єдиному інформаційному просторі та впровадженню функцій протидії кіберзлочинності.</p>
4 - Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	<p>Фахівець може займати первинні посади (за Класифікатором професій України ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки.</p> <p>International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).</p> <p>Може займати наступні посади:</p> <ul style="list-style-type: none"> – менеджер (управитель) систем з інформаційної безпеки (1495); – фахівець із організації інформаційної безпеки (3439); – фахівець (сфера захисту інформації); – фахівець з режиму секретності; – інспектор з організації захисту секретної інформації; – аналітик систем забезпечення кібербезпеки; – фахівець з організації та проведення тестування на проникнення.
Подальше навчання	<p>Навчання за програмою підготовки магістра 7 рівня НРК України, другого циклу FQ-EHEA та 7 рівня EQF-LLL.</p>
5 - Викладання та оцінювання	
Викладання та навчання	<p>Студентоцентроване навчання, самонавчання, навчання через лабораторну практику. проблемні, інтерактивні, проектні, інформаційно-комп'ютерні, саморозвиваючі, колективні та інтегративні, контекстні технології навчання.</p>

Оцінювання	<p>Оцінювання здійснюється відповідно до «Положення про оцінювання результатів навчання студентів і аспірантів» та «Положення про організацію освітнього процесу студентів».</p> <p>Види контролю: за рівнями: самоконтроль, контроль на рівні викладача, контроль на рівні завідувача кафедри, контроль на рівні деканату, контроль на рівні директора, атестація;</p> <p>Форми контролю: усне та письмове опитування, тестування, презентація наукової роботи, захист курсових робіт.</p> <p>Поточний контроль, підсумковий контроль – екзамени та єдиний державний кваліфікаційний іспит.</p>
6 - Програмні компетентності	
Інтегральна компетентність	<p>Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, зокрема в економіці, що характеризується комплексністю та неповною визначеністю умов.</p>
Загальні компетентності (КЗ)	<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>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.</p> <p>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.</p> <p>КЗ 8. Базові знання з основ економіки та підприємницької діяльності.</p>

<p>Фахові компетентності (КФ)</p>	<p>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.</p> <p>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>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.).</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>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.</p> <p>КФ 13. Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення із забезпечення кібербезпеки.</p> <p>КФ 14. Здатність здійснювати управління ризиками інформаційної та кібербезпеки.</p>
--	---

7 - Програмні результати навчання

1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
2. Організувати 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 часткої 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 проектних рішень.*

8 - Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	<p>Проектна група: 3 доктора наук та 6 кандидати наук.</p> <p>Всі розробники є співробітниками Державного торговельно-економічного університету.</p> <p>До реалізації програми залучаються науково-педагогічні працівники з науковими ступенями та/або вченими званнями, а також висококваліфіковані спеціалісти.</p> <p>З метою підвищення фахового рівня всі науково-педагогічні працівники один раз на п'ять років проходять стажування.</p>
Матеріально-технічне забезпечення	<p>Основу матеріально-технічного забезпечення складають спеціалізовані комп'ютерні лабораторії із сучасними апаратними та програмними ресурсами, що забезпечують якісну підготовку бакалаврів за освітньою програмою «Безпека інформаційних і комунікаційних систем в економіці».</p>
Інформаційне та навчально-методичне забезпечення	<p>Діюча система дистанційного навчання MOODLE та середовище MS Office 365 забезпечує самостійну та індивідуальну роботу студентів.</p>
9 - Академічна мобільність	
Національна кредитна мобільність	<p>Організація кредитної мобільності (окрім 1-го курсу) студентів, які здобувають освітній ступінь бакалавра. Проект компанія «ЕРАМ Systems Україна», ДП «Український інститут інтелектуальної власності», Центр сертифікованого навчання «Проком», освітня компанія «Пірсон Ед`юкейшн»,</p>
Міжнародна кредитна мобільність	<p>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).</p>
Навчання іноземних здобувачів вищої освіти	<p>Умови та особливості освітньої програми в контексті навчання іноземних громадян: знання української мови на рівні не нижче B1.</p>

2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент ОП

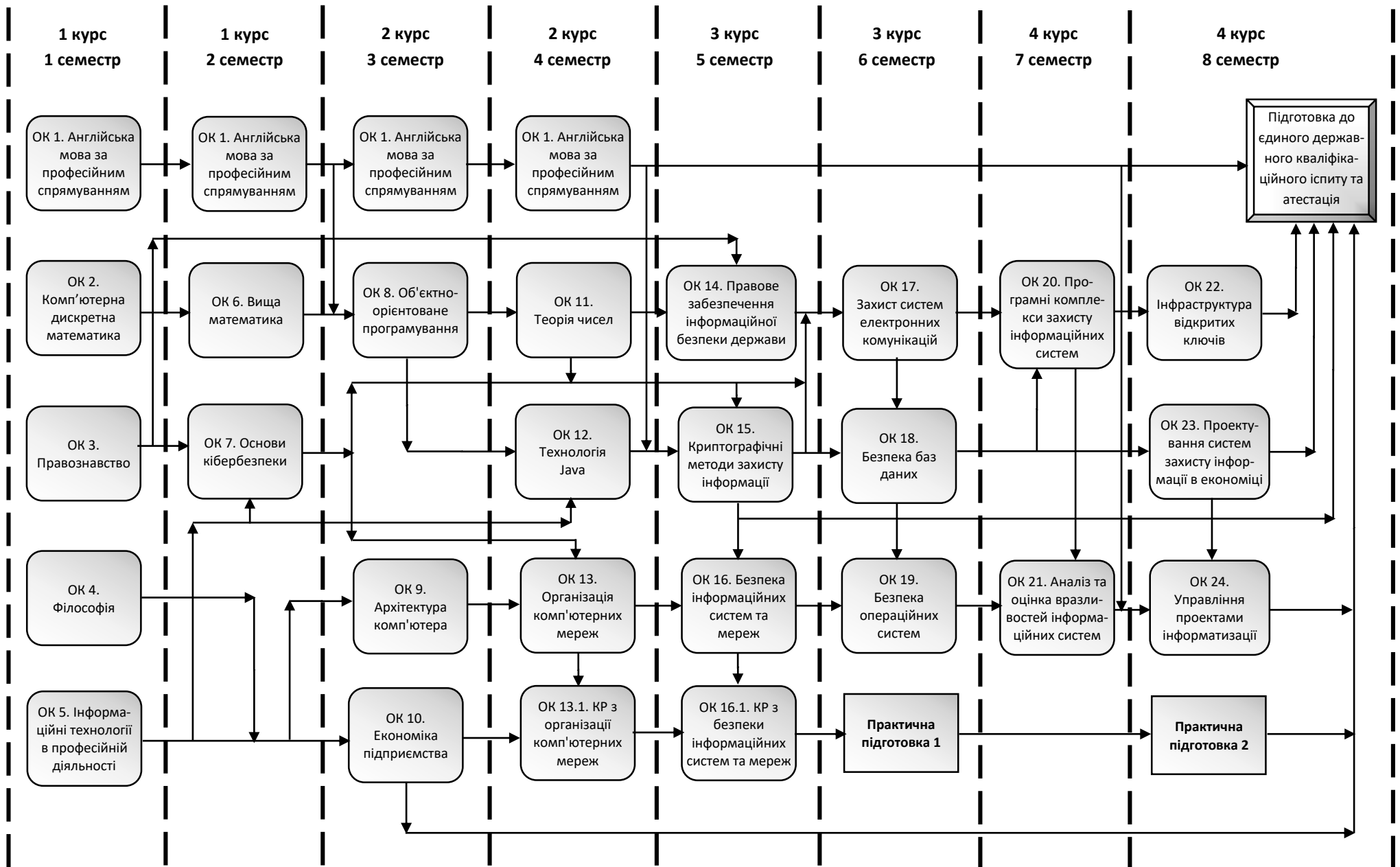
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів
1	2	3
Обов'язкові компоненти ОП		
ОК 1.	Англійська мова за професійним спрямуванням	24
ОК 2.	Комп'ютерна дискретна математика	6
ОК 3.	Правознавство	6
ОК 4.	Філософія	6
ОК 5.	Інформаційні технології в професійній діяльності	6
ОК 6.	Вища математика	6
ОК 7.	Соціотехнічна безпека	6
ОК 8.	Об'єктно-орієнтоване програмування	6
ОК 9.	Архітектура комп'ютера	6
ОК 10.	Економіка підприємства	6
ОК 11.	Теорія чисел	6
ОК 12.	Технологія Java	6
ОК 13.	Організація комп'ютерних мереж	6
ОК 13.1.	Курсова робота з організації комп'ютерних мереж	
ОК 14.	Правове забезпечення інформаційної безпеки держави	6
ОК 15.	Криптографічні методи захисту інформації	6
ОК 16.	Безпека інформаційних систем та мереж	6
ОК 16.1.	Курсова робота з безпеки інформаційних систем та мереж	
ОК 17.	Захист систем електронних комунікацій	6
ОК 18.	Безпека баз даних	6
ОК 19.	Безпека операційних систем	6
ОК 20.	Програмні комплекси захисту інформаційних систем	6
ОК 21.	Аналіз та оцінка вразливостей інформаційних систем	6
ОК 22.	Інфраструктура відкритих ключів	7,5
ОК 23.	Проектування систем захисту інформації в економіці	7,5
ОК 24.	Управління проектами інформатизації	6
Загальний обсяг обов'язкових компонент:		165

1	2	3
Вибіркові компоненти ОП		
ВК 1.	Алгоритми та структури даних	6
ВК 2.	Архітектура та проектування програмного забезпечення	6
ВК 3.	Безпека життя	6
ВК 4.	Дипломатичний та діловий протокол та етикет	6
ВК 5.	Договірне право	6
ВК 6.	Експертні системи	6
ВК 7.	Електронний документообіг	6
ВК 8.	Інформаційні війни	6
ВК 9.	Інвестиційне право	6
ВК 10.	Інструментальні засоби бізнес-аналітики	6
ВК 11.	Інформаційне право	6
ВК 12.	Історія України	6
ВК 13.	Історія української культури	6
ВК 14.	Комп'ютерна графіка та візуалізація даних	6
ВК 15.	Логіка	6
ВК 16.	Людино-машинна взаємодія	6
ВК 17.	Математичне програмування	6
ВК 18.	Менеджмент проектів програмного забезпечення	6
ВК 19.	Методи і засоби передачі даних	6
ВК 20.	Міжнародна економіка	6
ВК 21.	Моделі і структури даних	6
ВК 22.	Моделювання економічних процесів	6
ВК 23.	Моделювання та аналіз програмного забезпечення	6
ВК 24.	Національні інтереси у світовій геополітиці та геоekonomіці	6
ВК 25.	Основи програмування	6
ВК 26.	Політологія	6
ВК 27.	Право ЄС	6
ВК 28.	Програмування Інтернет	6
ВК 29.	Проектування та адміністрування інформаційних систем	6
ВК 30.	Психологія безпеки	6
ВК 31.	Психологія праці та інженерна психологія	6
ВК 32.	Психологія управління	6

1	2	3
ВК 33.	Психологія	6
ВК 34.	Релігієзнавство	6
ВК 35.	Світова культура	6
ВК 36.	Технологія аналізу даних	6
ВК 37.	Технологія розробки та тестування програмного забезпечення	6
ВК 38.	Технологія створення стартапу	6
ВК 39.	Українська мова (за професійним спрямуванням)	6
ВК 40.	Штучний інтелект	6
ВК 41.	WEB-дизайн і WEB-програмування	6
ВК 43.	Фізика	6
Загальний обсяг вибіркових компонент:		60
Практична підготовка		
Практична підготовка 1		6
Практична підготовка 2		6
Разом		12
Атестація		
Підготовка до єдиного державного кваліфікаційного іспиту та атестація		3
Разом		3
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240

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 єдиного державного кваліфікаційного іспиту.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

**4.1. Матриця відповідності програмних компетентностей
обов'язковим компонентам освітньої програми**

Компо- ненти/ Компе- тентності	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	ОК 22	ОК 23	ОК 24
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										+											+			

4.2. Матриця відповідності програмних компетентностей вибірковим компонентам освітньої програми

Компоненти/ Компетентності	БК 1	БК 2	БК 3	БК 4	БК 5	БК 6	БК 7	БК 8	БК 9	БК 10	БК 11	БК 12	БК 13	БК 14	БК 15	БК 16	БК 17	БК 18	БК 19	БК 20	БК 21	БК 22	БК 23	БК 24	БК 25	БК 26	БК 27	БК 28	БК 29	БК 30	БК 31	БК 32	БК 33	БК 34	БК 35	БК 36	БК 37	БК 38	БК 39	БК 40	БК 41	БК 42							
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								+																																									

**5.1. 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	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	ОК 22	ОК 23	ОК 24
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																+	+		+		+			+

**5.1. Матриця забезпечення програмних результатів навчання
відповідними обов'язковими компонентами освітньої програми (продовження)**

Компоненти/ Програмні результати навчання	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	ОК 22	ОК 23	ОК 24
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					+																			+

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	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29	ВК 30	ВК 31	ВК 32	ВК 33	ВК 34	ВК 35	ВК 36	ВК 37	ВК 38	ВК 39	ВК 40	ВК 41	ВК 42									
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																			+			+																													

**5.2. Матриця забезпечення програмних результатів навчання
відповідними вибілковими компонентами освітньої програми (продовження)**

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	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24	ВК 25	ВК 26	ВК 27	ВК 28	ВК 29	ВК 30	ВК 31	ВК 32	ВК 33	ВК 34	ВК 35	ВК 36	ВК 37	ВК 38	ВК 39	ВК 40	ВК 41	ВК 42												
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