**ПРОЄКТ**

**Освітньо-професійна програма**

Відгуки, зауваження й пропозиції просимо надсилати гарантові освітньо-професійної програми до 1 квітня 2026 року.

Гарант програми к.т.н., доц. Кільдішев В.Й., v.y_kildishev@suitt.edu.ua

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Державний університет інтелектуальних технологій і зв'язку**

# ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

## «Кібербезпека та захист інформації»

## «Cybersecurity and information protection»

| | |
|---|---|
| **Рівень вищої освіти** | Другий (магістерський) |
| **Ступінь вищої освіти** | Магістр |
| **Галузь знань** | F Інформаційні технології |
| **Спеціальність** | F5 Кібербезпека та захист інформації |
| **Освітня кваліфікація** | Магістр з кібербезпеки та захисту інформації |
| **Інформація про внесення змін** | Друга редакція |

**ЗАТВЕРДЖЕНО**
Вченою радою Державного університету інтелектуальних технологій і зв'язку
(протокол від ___ _____ 2026 р. № )

Освітньо-професійна програма вводиться в дію з ___ _____ 2026 р.
Ректор
_____Олександр НАЗАРЕНКО
(наказ від ___ _____ 2026 р. № _____)

**Одеса 2026**

# ЛИСТ ПОГОДЖЕННЯ

**змін до освітньо-професійної програми**
**«Кібербезпека та захист інформації»**
**зі спеціальності F5 Кібербезпека та захист інформації**
**за другим (магістерським) рівнем вищої освіти**

**ВНЕСЕНО**
Кафедрою кібербезпеки та
технічного захисту інформації
Протокол від «10» березня 2026 р. № 9
Завідувач кафедри Володимир КОРЧИНСЬКИЙ

**ПОГОДЖЕНО**
Декан факультету інформаційних технологій
та кібербезпеки
___ березня 2026 р. Євген ВАСІЛІУ

**ПОГОДЖЕНО**
Начальник відділу ліцензування та акредитації
___ березня 2026 р. Юлія ШТОВБА

**ПОГОДЖЕНО**
Начальник навчального відділу
___ березня 2026 р. Світлана КІЙКО

**РЕКОМЕНДОВАНО**
до розгляду на Вченій раді ДУІТЗ рішенням спільного засідання Комісії з питань внутрішнього забезпечення якості та Навчально-методичної ради
(Протокол від 08 квітня 2026 р. № 3)

Голова Комісії з питань внутрішнього забезпечення якості Олег ГРАБОВСЬКИЙ

Голова Навчально-методичної ради Світлана ХАДЖИРАДЄВА

# ПЕРЕДМОВА

Освітньо-професійна програма «Кібербезпека та захист інформації» підготовки здобувачів вищої освіти другого (магістерського) рівня за спеціальністю F5 Кібербезпека та захист інформації, галузі знань F Інформаційні технології розроблена відповідно до Закону України «Про вищу освіту» №1556-VII від 01.07.2014 р.; Стандарту вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти, затвердженого Наказом МОН України № 332 від 18.03.2021; Наказу МОН України № 1734 від 31.12.2025 «Про затвердження Методичних рекомендацій щодо відповідності освітніх програм спеціальностям, за якими здійснюється підготовка здобувачів вищої освіти, та деталізованим галузям Міжнародної стандартної класифікації освіти ISCED-F 2013»; враховує вимоги Професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022.

1. **Внесено:** кафедрою кібербезпеки та технічного захисту інформації.
2. **Розроблено робочою групою у складі:**
   ***Керівник робочої групи (гарант освітньої програми):***
   Кільдішев Віталій Йосипович, д.т.н., доц., доцент каф. кібербезпеки та технічного захисту інформації
   ***Члени робочої групи:***
   - Василіу Євген Вікторович, д.т.н., проф., проф. каф. Кібербезпеки та технічного захисту інформації;
   - Рябуха О.М., к.т.н., ст. викл. каф. Кібербезпеки та технічного захисту інформації.

**4 . Рецензії – відгуки зовнішніх стейкхолдерів:**

1. Громадське об'єднання «Асоціація спеціалістів кібербезпеки», президент ГО Корченко О.Г.
2. ТОВ «КОБІ СС», директор Вихристюк О.А.
3. ТОВ «Роберт Бош ЛТД», Директор департаменту інформаційних систем та систем безпеки Барановський С.В.

## 1. Профіль освітньої-професійної програми «Кібербезпека та захист інформації» зі спеціальності F5 «Кібербезпека та захист інформації»

| 1 – Загальна інформація | |
|---|---|
| **Повна назва закладу вищої освіти та структурного підрозділу** | Державний університет інтелектуальних технологій і зв'язку<br>Факультет Інформаційних технологій та кібербезпеки<br>Кафедра Кібербезпеки та технічного захисту інформації |
| **Ступінь вищої освіти та назва кваліфікації мовою оригіналу** | Магістр<br>Магістр з кібербезпеки та захисту інформації |
| **Офіційна назва освітньої програми** | Кібербезпека та захист інформації |
| **Тип диплому та обсяг освітньої програми** | Диплом магістра, одиничний, 90 кредитів ЄКТС,<br>термін навчання 1 рік 4 місяці |
| **Наявність акредитації** | Термін дії сертифіката про акредитацію освітньої програми закінчився |
| **Цикл/рівень** | НРК України – 7 рівень, QF-EHEA – другий цикл, EQF-LLL – 7 рівень |
| **Передумови** | Особа має право здобувати ступінь магістра за умови наявності в неї ступеня бакалавра |
| **Мова(и) викладання** | Українська |
| **Термін дії освітньої програми** | До повного завершення періоду навчання або наступного оновлення програми |
| **Інтернет-адреса постійного розміщення опису освітньої програми** | https://suitt.edu.ua/prohramy-osvity/ |
| **2 – Мета освітньої програми** | |
| Підготовка професіоналів, здатних забезпечувати захищеність інформації, що обробляється та передається в інформаційно-комунікаційних системах, від несанкціонованих дій з інформацією, витоку технічними каналами та спеціальних впливів на засоби обробки інформації. | |

| 3 - Характеристика освітньої програми | |
|---|---|
| **Предметна область (галузь знань, спеціальність, спеціалізація (за наявності)** | *Галузь знань:* F Інформаційні технології<br>*Спеціальність:* F5 Кібербезпека та захист інформації |
| **Об’єкт (об’єкти) вивчення та/або діяльності** | Наукові та інженерні основи технологій кібербезпеки та захисту інформації, технології, методи, моделі та засоби інформаційної та кібербезпеки, процеси управління кібербезпекою та захистом інформації, безпека інформаційних ресурсів, систем та технологій, штучного інтелекту, об'єктів інформаційної діяльності та критичної інфраструктури. |
| **Теоретичний зміст предметної області** | Теорії, поняття, концепції, принципи захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, безпеки інформаційних систем та технологій, забезпечення своєчасного виявлення, запобігання і нейтралізації цільових (змішаних) атак, об’єктів інформаційної діяльності та критичної інфраструктури у кіберпросторі. |
| **Методи, методики та технології** | Методи, методики та технології, дослідження, моделювання, аналізу та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів, розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації у кіберпросторі, виявлення, аналізу кіберінцидентів і протидії ним, запобігання і нейтралізації реальних і потенційних загроз інформаційним ресурсам, об’єктам інформаційної діяльності та критичної інфраструктури, створення, супроводження та забезпечення ефективного функціонування систем захисту інформації, дослідження та вдосконалення процесів обробки та захисту інформаційних ресурсів. |
| **Інструменти та обладнання** | Прикладне та спеціалізоване програмне забезпечення, мережне устаткування, апаратне забезпечення, засоби та пристрої захисту інформації. |

| | |
|---|---|
| **Орієнтація освітньої програми** | Освітньо-професійна |
| **Основний фокус освітньої програми** | Підготовка професіоналів, здатних до інноваційної та науково-дослідницької діяльності при дослідженні, проектуванні, модернізації, впровадженні та експлуатації сучасних систем та технологій кібербезпеки та захисту інформації; підготовка до виконання основних трудових функцій за професією «Фахівець сфери захисту інформації», код 2139.2.<br>*Ключові слова*: кібернетична безпека, інформаційна безпека, системи і технології інформаційної та кібербезпеки, комплексні системи безпеки; безпека об'єктів критичної інфраструктури; криптографічний захист інформації; технічний захист інформації. |
| **Особливості програми** | Розроблена з урахуванням міжнародних стандартів, рекомендацій та практик щодо студентоцентрованого навчання.<br>Розроблена з врахуванням основних трудових функцій та професійних компетентностей професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022.<br>Передбачає ґрунтовну фундаментальну підготовку у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити науково-дослідну та інноваційну діяльність і працювати з наукоємними технологіями кібербезпеки та захисту інформації.<br>Враховує особливості розвитку спеціальності та ринку праці шляхом залучення роботодавців, як зовнішніх аудиторів навчальних програм з метою підтвердження їхньої релевантності.<br>Орієнтована на партнерство із вітчизняними та закордонними закладами освіти та науки, приватним сектором, науковцями та практиками, передбачає участь у міжнародних програмах з метою підвищення якості освіти.<br>Передбачає дуальну освіту. |
| **4 – Придатність випускників до працевлаштування та подальшого навчання** | |
| **Придатність до працевлаштування** | Види економічної діяльності згідно з Національним класифікатором України ДК 009:2010 «Класифікація видів |

| | |
|---|---|
| | економічної діяльності»:<br>Секція J, розділ 62, група 62.0 – Комп'ютерне програмування, консультування та пов'язана з ними діяльність; розділ 63, група 63.9 – Надання інших інформаційних послуг.<br>Секція M, розділ 71, група 71.2 – Технічні випробування та дослідження; розділ 74, група 74.9 – Інша професійна, наукова та технічна діяльність.<br>Види професійної діяльності згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»:<br>Розділ 2 – Професіонали, Клас 213 – Професіонали в галузі обчислень (комп'ютеризації), підклас 2139 – Професіонали в інших галузях обчислень (комп'ютеризації). |
| **Подальше навчання** | Можливість навчання на третьому (освітньо-науковому) рівні вищої освіти (НРК України – 8, рівень QF-EHEA – третій цикл, EQF-LLL – 8 рівень). |
| **5 – Викладання та оцінювання** | |
| **Викладання та навчання** | Проблемно-орієнтоване та студентоцентроване навчання із запровадженням в освітній процес індивідуальної траєкторії навчання та забезпеченням принципів академічної свободи.<br>Комбінація лекцій, мультимедійних лекцій, семінарів, дослідницьких практичних занять, виконання проектів (в тому числі командних), участь у конкурсах та хакатонах, самонавчання.<br>На захист кваліфікаційних робіт (проектів) запрошуються представники компаній-стейкхолдерів.<br>Методи навчання і викладання базуються на принципах свободи слова і творчості, застосування проектних методів роботи, поширення знань та інформації, поєднанні навчання, досліджень та виконання навчальних проектів під час освітнього процесу. |
| **Оцінювання** | Оцінювання знань студентів здійснюється у відповідності до Положення про оцінювання знань студентів ДУІТЗ.<br>Екзамени, заліки, захист звіту з практики, захист курсових робіт (проектів), публічний захист кваліфікаційної роботи.<br>Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, |

| | |
|---|---|
| | незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F) |
| **6 – Програмні компетентності (ПК)** | |
| **Інтегральна компетентність** | Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. |
| **Загальні компетентності (ЗК)** | ЗК-1. Здатність застосовувати знання у практичних ситуаціях.<br>ЗК-2. Здатність проводити дослідження на відповідному рівні.<br>ЗК-3. Здатність до абстрактного мислення, аналізу та синтезу.<br>ЗК-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.<br>ЗК-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).<br>ЗК-6. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. |
| **Спеціальні (фахові, предметні) компетентності (СК)** | СК-1. 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.<br>СК-2. 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.<br>СК-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.<br>СК-4. 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.<br>СК-5. 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.<br>СК-6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.<br>СК-7. 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.<br>СК-8. 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.<br>СК-9. 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.<br>СК-10. 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.<br>СК-11. Здатність розробляти та впроваджувати комплексну систему захисту інформації, що протидіє багатьом різним |

| | |
|---|---|
| | за природою загрозам (кібератаки з боку інсайдерів та хакерів, злам програм, віруси, перехоплення трафіку, помилки тощо).<br>СК-12. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж.<br>СК-13. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.<br>СК-14. Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації.<br>СК-15. Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки.<br>СК-16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.<br>СК-17. Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації. |
| **7 – Програмні результати навчання (ПРН)** | |
| ПРН-1. 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.<br>Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.<br>ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.<br>ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.<br>ПРН5. 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. | |

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН12. 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.
ПРН13. 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.
ПРН14. 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.
ПРН15. 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.
ПРН16. 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.
ПРН17. 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.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
ПРН19. 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.
ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
ПРН22. 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.
ПРН23. 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.
ПРН24. Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.
ПРН25. Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації.
ПРН26. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності.
ПРН27. Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації.
ПРН28. Здійснювати моніторинг та аудит загроз для інформації, що озвучується.
ПРН29. Використовувати інструменти та технології безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах
ПРН30. Проводити сканування вразливостей і розпізнання вразливостей в ІКС і системах безпеки.
ПРН31. Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.

| | |
|---|---|
| ПРН32. Складати програму та методику атестації комплексу технічного захисту інформації (ТЗІ).<br>ПРН33. Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в інформаційно-комунікаційних системах в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ.<br>ПРН34. Приймати участь в організації та навчанні (підвищенні кваліфікації) працівників структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань. | |
| **8 – Ресурсне забезпечення реалізації програми** | |
| **Кадрове забезпечення** | Кадрове забезпечення відповідає кадровим вимогам щодо провадження освітньої діяльності для другого (магістерського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності.<br>Реалізація програми забезпечується кадрами високої кваліфікації, які мають значний досвід навчально-методичної, науково-дослідної та практичної роботи, є визнаними професіоналами за фахом.<br>До реалізації програми злучається не менше 50% науково-педагогічних працівників, які мають науковий ступінь та/або вчене звання, не менше 25% мають науковий ступінь доктора наук або вчене звання професора.<br>Система професійного розвитку викладачів реалізується через співпрацю з декількома провідними компаніями у сфері кібербезпеки/інформаційної безпеки.<br>До освітнього процесу залучаються роботодавці сфери захисту інформації та професіонали-практики в цій сфері. |
| **Матеріально-технічне забезпечення** | Матеріально-технічне забезпечення відповідає технологічним вимогам щодо провадження освітньої діяльності для другого (магістерського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності.<br>Реалізація програми забезпечується:<br>- приміщеннями для проведення навчальних занять та контрольних заходів;<br>- мультимедійним обладнанням для одночасного використання в навчальних аудиторіях;<br>- наявністю соціально-побутової інфраструктури, в тому числі бібліотеки з читальним залом та гуртожитків; |

| | |
|---|---|
| | - комп'ютерними робочими місцями, лабораторіями, обладнанням, устаткуванням, доступом до кіберполігонів, доступом до Інтернету та інформаційних ресурсів, необхідних для навчання, викладацької та наукової діяльності. |
| **Інформаційне та навчально-методичне забезпечення** | Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого освітній програмі профілю, в тому числі в електронному вигляді.<br>Наявність безоплатного доступу викладачів і здобувачів вищої освіти до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю.<br>Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня / освітньо-наукова / видавнича / атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація).<br>Наявність електронного ресурсу закладу освіти, який містить матеріали, необхідні для навчання, викладацької та наукової діяльності. |
| **9 – Академічна мобільність** | |
| **Національна кредитна мобільність** | На загальних підставах в межах України.<br>На основі двосторонніх договорів між Державним університетом інтелектуальних технологій і зв'язку та закладами вищої освіти України. |
| **Міжнародна кредитна мобільність** | В рамках програми ЄС Еразмус+ на основі двосторонніх договорів між Державним університетом інтелектуальних технологій і зв'язку та навчальними закладами зарубіжних країн-партнерів. |
| **Навчання іноземних здобувачів вищої освіти** | Українською мовою при навчанні у спільних академічних групах з україномовними здобувачами ВО. |

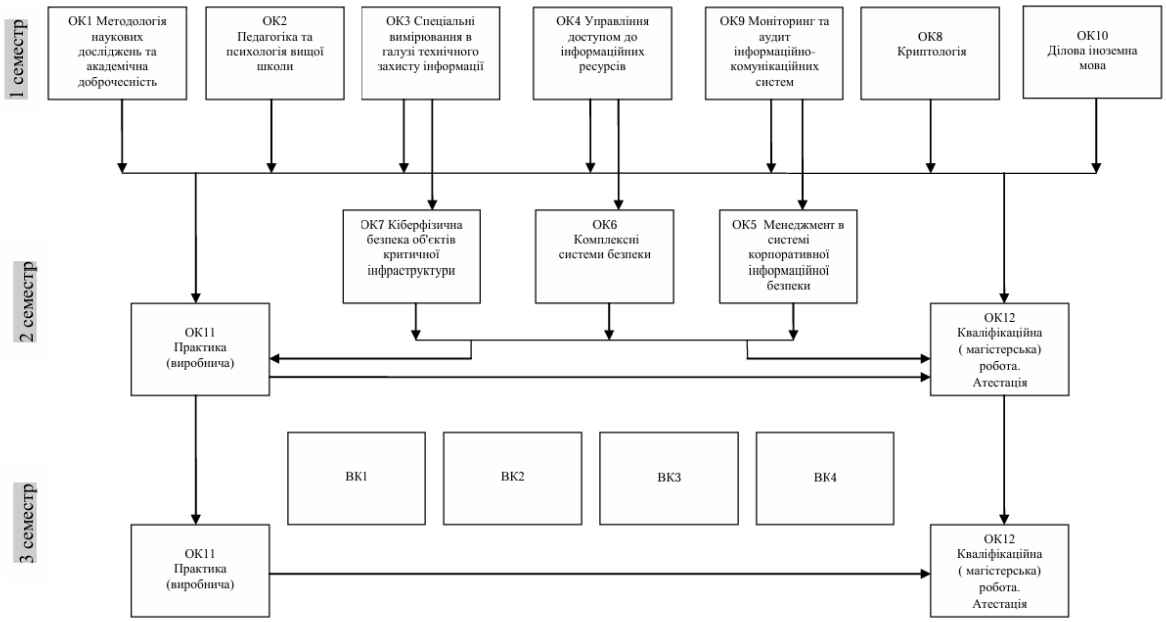
## 2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

### 2.1 Перелік освітніх компонентів освітньо-професійної програми

| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів ECTS | Форма підсумкового контролю |
|---|---|---|---|
| **ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ (ОК)** | | | |
| ОК1 | Методологія наукових досліджень та академічна доброчесність | 4 | Залік |
| ОК2 | Педагогіка та психологія вищої школи | 5 | Екзамен |
| ОК3 | Спеціальні вимірювання в галузі технічного захисту інформації | 4 | Екзамен |
| ОК4 | Управління доступом до інформаційних ресурсів | 4 | Екзамен |
| ОК5 | Менеджмент в системі корпоративної інформаційної безпеки | 5 | Екзамен, КР |
| ОК6 | Комплексні системи безпеки | 4 | Залік |
| ОК7 | Кіберфізична безпека об'єктів критичної інфраструктури | 4 | Екзамен |
| ОК8 | Криптологія | 4 | Екзамен |
| ОК9 | Моніторинг та аудит інформаційно-комунікаційних систем | 5 | Екзамен |
| ОК 10 | Ділова іноземна мова | 4 | Екзамен |
| ОК11 | Практика (виробнича) | 15 | Залік |
| ОК12 | Кваліфікаційна ( магістерська) робота. Атестація | 8 | Публічний захист |
| **Загальний обсяг обов'язкових компонентів** | | **66 кредитів 1980 акад. годин** | 9 екзаменів, 3 заліки |
| **Загальний обсяг вибіркових компонентів** *(4 дисципліни по 6 кредитів ЄКТС)* | | **24 кредитів 720 акад. годин** | 4 заліки |
| **Усього** | | **90 кредитів ЄКТС 2700 акад. годин** | |

## 2.2. Структурно-логічна схема освітньо-професійної програми

| Складові програми | Таймінг навчання протягом 1 року 4 місяців (за семестрами) | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| **Обов'язкові та вибіркові компоненти теоретичної підготовки** | ОК1/4<br>ОК2/5<br>ОК3/4<br>ОК4/4<br>ОК8/4<br>ОК9/5<br>ОК10/4 | ОК5/5<br>ОК6/4<br>ОК7/4 | ВК1/6<br>ВК2/6<br>ВК3/6<br>ВК4/6 |
| | | | |
| **Практична підготовка** | | ОК11/12 | ОК11/3 |
| **Кваліфікаційна (магістерська) робота. Атестація** | | ОК12/5 | ОК12/3 |
| **Кількість кредитів ЄКТС** | **30** | **30** | **30** |



## 3. Форми атестації здобувачів вищої освіти

Випускна атестація здобувачів вищої освіти за освітньою програмою спеціальності F5 «Кібербезпека та захист інформації» проводиться у формі публічного захисту кваліфікаційної роботи та завершується видачею документа встановленого зразка про присудження ступеня магістра із присвоєнням кваліфікації: Магістр кібербезпеки та захисту інформації. Кваліфікаційна робота має передбачати розв'язання складної спеціалізованої задачі або практичної проблеми в галузі інформаційних технологій і характеризується комплексністю та невизначеністю умов.

У кваліфікаційній роботі не може бути академічного плагіату та фальсифікації. Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти, його структурного підрозділу або у репозитарії закладу вищої освіти.

## 3. Матриця відповідності компетентностей обов'язковим компонентам освітньої програми

| | Загальні компетентності (ЗК) | | | | | | | Спеціальні (фахові) компетентності (СК) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| ОК1 | + | + | + | | | + | | + | | | | | | | | | | | | | | | | |
| ОК2 | + | + | + | | + | | | | | | | | | | | | + | | | | | | | |
| ОК3 | + | + | | | | | | | + | + | | | | | + | | | | | + | | | | + |
| ОК4 | + | | | + | | | | | | | + | | + | | | | | | | + | | | | |
| ОК5 | + | | + | | | | | | + | | + | + | | + | | | | | + | | | + | + | |
| ОК6 | + | + | + | | | | | + | + | + | | | | | | | | + | | | | | + | + |
| ОК7 | + | + | + | | + | | | | + | + | + | + | | | + | | | | | | | | + | |
| ОК8 | + | + | + | | | | | | | + | | | | | + | | | | | | | + | | |
| ОК9 | + | + | + | + | | | | | | | | | | | | + | | | | | + | + | | |
| ОК10 | + | | | | + | | | | | + | | | | | | | | | | | | | | |
| ОК11 | + | | | + | + | | | + | + | | | | | | | | + | | + | | | | + | |
| ОК12 | + | + | + | + | + | | | + | + | + | | | | | | | + | | + | + | | | | |

## 4. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

| | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 | ОК10 | ОК11 | ОК12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ПРН1 | + | + | | | | | | | | + | | + |
| ПРН2 | + | | | + | + | + | + | + | | | + | + |
| ПРН3 | + | | | | | + | + | + | | + | | + |
| ПРН4 | | | | + | | + | + | + | | | | + |
| ПРН5 | | | | | + | + | | + | | | | + |
| ПРН6 | | | + | | | + | + | | | | | |
| ПРН7 | | | + | + | + | + | + | + | + | | | + |
| ПРН8 | | | | + | | + | + | | | | | + |
| ПРН9 | | | | | + | | | | | | | |
| ПРН10 | | | | | + | | | | | | | |
| ПРН11 | | | | + | | | | | | | | |
| ПРН12 | | | | + | | | | | | | | |
| ПРН13 | | | + | | | + | + | + | | | | |
| ПРН14 | | | | | | | | | + | | | |
| ПРН15 | | | | | | | | | | | + | |
| ПРН16 | | | | | + | | | | | | | |
| ПРН17 | | + | | | | | | | | | + | + |
| ПРН18 | | + | | | | | | | | | | |
| ПРН19 | + | | | | + | | | | | | | + |
| ПРН20 | + | | | | | | | | | | | + |
| ПРН21 | | | | | | | | + | | | | |
| ПРН22 | + | | | | | | | | | | | + |
| ПРН23 | | | | + | | | | + | | | + | + |
| ПРН24 | | | | | + | | | | | | | |
| ПРН25 | | | | + | | | | | | | | |
| ПРН26 | | | + | | | | + | | | | | |
| ПРН27 | | | | | | | | | + | | | |
| ПРН28 | | | | | | | | | + | | | |
| ПРН29 | | | | | | | | | + | | | |
| ПРН30 | | | | | | | | | + | | | |
| ПРН31 | | | | | | | | | + | | | |
| ПРН32 | | | + | | | | | | | | | |
| ПРН33 | | | + | | | | | | | | | |
| ПРН34 | | | | | | | | | | | + | |

## 6. Характеристика системи внутрішнього забезпечення якості підготовки здобувачів другого (магістерського) рівня вищої освіти

Принципи та процедури забезпечення якості підготовки здобувачів другого (магістерського) рівня вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» відповідають вимогам положень «Про внутрішнє забезпечення якості освітньої діяльності та якості вищої освіти в ДУІТЗ», «Про організацію освітнього процесу в ДУІТЗ», «Про оцінювання знань здобувачів вищої освіти в ДУІТЗ», «Про забезпечення академічної доброчесності та етики в ДУІТЗ» тощо, контролюються структурними підрозділами (деканат, кафедра, лабораторія якості, навчально-методичний відділ та ін.) та відповідними колегіальними органами ДУІТЗ, зокрема: Вчена рада, Навчально-методична рада, Комісія з питань етики та академічної доброчесності та ін.

Система внутрішнього забезпечення якості вищої освіти на освітньо-професійній програмі «Кібербезпека та захист інформації» передбачає такі процедури і заходи:

***Моніторинг та періодичний перегляд освітньої програми.*** Моніторинг освітньо-професійної програми «Кібербезпека та захист інформації» здійснюється на підставі аналізу і порівняння результатів поточного та підсумкового оцінювання здобувачів вищої освіти, виконання ними навчальних завдань самостійної навчальної і науково-дослідної роботи. Коригування змісту робочих програм навчальних дисциплін, програм практик, завдань для самостійної роботи і питань, що виносяться на підсумкове оцінювання, здійснюється кафедрами щорічно. Результати самооцінювання освітньої програми обговорюються на засіданні випускової кафедри із запрошення стейкхолдерів та інших зацікавлених осіб. Перегляд освітньої програми проводиться щонайменше один раз протягом повного курсу навчання. Пропозиції щодо її оновлення (об'єктивні зміни інфраструктурного, кадрового, інших ресурсних умов, перегляд навчального навантаження, кількості кредитів, змісту освітніх компонентів тощо) відображаються у документах відповідних структурних підрозділів і виносяться на розгляд вченої ради ДУІТЗ.

***Оцінювання здобувачів вищої освіти, науково-педагогічних та педагогічних працівників ДУІТЗ та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті або на інформаційних стендах.*** Оцінювання навчальних досягнень здобувачів освіти в межах освітньо-професійної програми «Кібербезпека та захист інформації» здійснюється за 100-бальною шкалою ЄКТС та національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, не зараховано). Система оцінювання результатів навчання здобувачів вищої освіти включає поточний, підсумковий семестровий контроль та атестацію. Щорічно результати оцінювання якості

навчання здобувачів вищої освіти обговорюються на засіданнях випускових кафедр, вченої ради ДУІТЗ та оприлюднюються на офіційному веб-сайті ДУІТЗ.

Оцінювання науково-педагогічних та педагогічних працівників, які входять до групи забезпечення освітньої програми, здійснюють кафедри, лабораторія якості та студентська рада через опитування/анкетування здобувачів вищої освіти, а також звітування викладачів за результатами навчальної, методичної, наукової та організаційної діяльності. Обговорення результатів щорічного оцінювання науково-педагогічних та педагогічних працівників відбувається на засіданні вченої ради ДУІТЗ.

***Підвищення кваліфікації науково-педагогічних працівників.*** Підвищення кваліфікації науково-педагогічних та педагогічних працівників, які забезпечують освітньо-професійну програму «Кібербезпека та захист інформації» здійснюється відповідно до «Положення про порядок підвищення кваліфікації науково-педагогічних та педагогічних працівників ДУІТЗ». Основними видами підвищення кваліфікації є стажування, воркшопи, тренінги тощо. Контроль за впровадженням результатів підвищення кваліфікації в освітній процес здійснюється на рівні кафедр.

***Наявність необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів вищої освіти, за освітньою програмою.*** Для реалізації освітньо-професійної програми «Кібербезпека та захист інформації» розроблено навчально-методичні комплекси з усіх обов'язкових та вибіркових компонентів, підготовлено методичні рекомендації з написання кваліфікаційної (магістерської) роботи, наскрізну програму практики, завдання для самостійної роботи здобувачів вищої освіти, які розміщенні в системі Moodle на платформі e-Learning ДУІТЗ. Інформаційне забезпечення освітньої програми здійснюється бібліотекою, та відповідними онлайн ресурсами (https://suitt.edu.ua/library; https://suitt.edu.ua/ naukometrichni-bazi-danih; https://metod.suitt.edu.ua).

За випусковою кафедрою, яка забезпечує реалізацію освітньо-професійної програми «Кібербезпека та захист інформації», закріплено спеціально обладнані приміщення, де крім навчальних аудиторій в наявності є три лабораторії: «Кібербезпеки», «Технічних засобів охорони та захисту інформації», «Проєктна лабораторія KobiSoftware».

***Публічність інформації про освітню програму, ступені освіти та кваліфікації.*** На офіційному веб-сайті ДУІТЗ (https://suitt.edu.ua) розміщено усю актуальну інформацію про освітньо-професійну програму «Кібербезпека та захист інформації», зокрема про право здійснювати освітню діяльність у сфері вищої освіти, інформація про освітню програму, навчальний план, силабуси, вимоги та програма вступних випробувань (https://suitt.edu.ua /prohramy-vyprobuvan), правила прийому іноземних громадян тощо.

***Система академічної доброчесності, запобігання та виявлення академічного плагіату у наукових працях працівників ЗВО і здобувачів вищої освіти.*** Система академічної доброчесності ґрунтується на вимогах «Положення про забезпечення академічної доброчесності та етики в ДУІТЗ». Питання академічної доброчесності контролюються структурними підрозділами (деканат факультету Інформаційних технологій та кібербезпеки, кафедра кібербезпеки та технічного захисту інформації, лабораторія якості, науково-виробничий центр науково-технічної інформації та міжнародних програм та ін.) та відповідними колегіальними органами ДУІТЗ, зокрема комісія з питань етики та академічної доброчесності. Діяльність комісії регламентована «Положення про комісію з питань етики та академічної доброчесності в ДУІТЗ».

## 7. Перелік нормативних документів, на яких базується освітня програма

1. Закон України «Про вищу освіту» від 01.07.2014 № 1556-VII.
2. Постанова КМУ від 23.11.2011 р. № 1341 «Про затвердження національної рамки кваліфікацій».
3. Постанова КМУ від 30.09.2024 р. № 1021 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти».
4. Класифікація видів економічної діяльності: ДК 009:2010. (Національний класифікатор України).
5. Класифікатор професій ДК 003:2010. (Національний класифікатор України).
6. Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності».
7. Стандарт вищої освіти України за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затверджений Наказом МОН України від 18.03.2021 № 332.
8. Професійний стандарт «Фахівець сфери захисту інформації», затверджений наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022.
9. Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти, затверджене Наказом Міністерства освіти і науки України від 15.05.2024, № 686.
10. Наказ МОН України № 1734 від 31.12.2025 «Про затвердження Методичних рекомендацій щодо відповідності освітніх програм спеціальностям, за якими здійснюється підготовка здобувачів вищої освіти, та деталізованим галузям Міжнародної стандартної класифікації освіти ISCED-F 2013».
11. Положення про організацію освітнього процесу в ДУІТЗ від 29.05.2025.

12. Положення про освітні програми ДУІТЗ від 29.05.2025.

Гарант освітньої програми  Віталій КІЛЬДІШЕВ