

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	Перший (бакалаврський)
Ступінь вищої освіти	Бакалавр
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Освітня кваліфікація	Бакалавр з кібербезпеки
Інформація про внесення змін	Друга редакція

ЗАТВЕРДЖЕНО

Вченою радою Державного університету
інтелектуальних технологій і зв'язку
(Протокол від 10 квітня 2026 р. № 3)

Освітньо-професійна програма вводиться в
дію з 01 вересня 2026 р.

Наказ про введення в дію від 10 квітня 2026 р.

№ 01-02-02

Ректор

Олександр НАЗАРЕНКО



ЛИСТ ПОГОДЖЕННЯ

змін до освітньо-професійної програми
«Кібербезпека та захист інформації»
зі спеціальності F5 Кібербезпека та захист інформації
за першим (бакалаврським) 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

20 березня 2026 р.



Євген ВАСІЛІУ

ПОГОДЖЕНО

Начальник відділу ліцензування та акредитації

20 березня 2026 р.



Юлія ШТОВБА

ПОГОДЖЕНО

Начальник навчального відділу

20 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» є нормативним документом, який регламентує нормативні, компетентнісні, кваліфікаційні, організаційні, навчальні та методичні вимоги з підготовки здобувачів першого (бакалаврського) рівня вищої освіти зі спеціальності F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології.

1. Внесено: кафедрою кібербезпеки та технічного захисту інформації.

2. Розроблено робочою групою у складі:

Керівник робочої групи (гарант освітньої програми):

Васіліу Євген Вікторович, доктор технічних наук, професор, декан факультету інформаційних технологій та кібербезпеки Державного університету інтелектуальних технологій і зв'язку.

Члени робочої групи:

Корчинський Володимир Вікторович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та технічного захисту інформації;

Онацький Олексій Віталійович, кандидат технічних наук, доцент кафедри кібербезпеки та технічного захисту.

3. Рецензії-відгуки зовнішніх стейкхолдерів:

Корченко О.Г., президент громадської організації «Асоціація спеціалістів кібербезпеки»;

Ткаченко О.В., заступник Генерального директора товариство з обмеженою відповідальністю «Консалтингова компанія СІДКОН»;

Барановський С.В., директор департаменту інформаційних систем та систем безпеки товариство з обмеженою відповідальністю «Роберт Бош ЛТД».

Освітньо-професійну програму «Кібербезпека та захист інформації» розроблено відповідно до:

Законів України: «Про освіту» (від 05 вересня 2017 року № 2145-VIII; в редакції від 01.01.2026 р. № 4695-IX); «Про вищу освіту» (від 01 липня 2014 року № 1556-VII; в редакції від 11.03.2026 р.), «Про наукову і науково-технічну діяльність» від 26 листопада 2015 року № 848-VIII (в редакції від 22.03.2026 р. № 4794-IX);

Постанов Кабінету Міністрів України: «Про затвердження ліцензійних умов провадження освітньої діяльності» (від 30 грудня 2015 р. № 1187; в редакції від 31.10.2023 р. № 1134); «Про затвердження Національної рамки кваліфікацій» (від 23 листопада 2011 р. № 1341; в редакції від 05.02.2026 р. № 159); «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» (від 30 серпня 2024 р. № 1021);

Наказів Міністерства освіти і науки України: «Про затвердження Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти» (від 15 травня 2024 р. № 686); «Про внесення змін до деяких стандартів вищої освіти» (від 13 червня 2024 р. № 842); «Про внесення змін до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти» (від 29 жовтня 2024 р. № 1547); «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 та описів предметних областей спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» (від 31 грудня 2025 р. № 1734);

Додаток до листа Міністерства освіти і науки України «Про примірний зразок освітньо-професійної програми для першого (бакалаврського) та другого (магістерського) рівнів вищої освіти» (від 28 квітня 2017 р. № 1/9-239);

Стандарту вищої освіти України першого (бакалаврського) рівня вищої освіти ступеня «бакалавр» галузь знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації (про внесення змін до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547);

Статуту Державного університету інтелектуальних технологій і зв'язку (затвердженого наказом Міністерства освіти і науки України від 20 листопада 2023 № 1433) та інших нормативних документів ДУІТЗ (<https://suitt.edu.ua/polozhennia>).

**1. Профіль освітньо-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 Кафедра кібербезпеки та технічного захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Перший (бакалаврський) Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека та захист інформації
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС
Наявність акредитації	Сертифікат про акредитацію спеціальності УД 16021201 дійсний до 31.12.2027
Цикл/рівень	НРК України – 6 рівень, EQF-LLL – 6 рівень, FQ-EHEA – перший цикл
Передумови	Наявність повної загальної середньої освіти, освітньо-кваліфікаційного рівня молодшого спеціаліста, освітньо-професійного ступеня фахового молодшого бакалавра, освітнього ступеня бакалавра
Мова(и) викладання	Українська
Термін дії освітньої програми	До повного завершення періоду навчання та акредитації
Інтернет-адреса постійного розміщення опису освітньої програм	https://suitt.edu.ua/
2 – Мета освітньої програми	
Підготовка фахівців з кібербезпеки та захисту інформації, здатних розв'язувати спеціалізовані професійні завдання із застосуванням наукових засад та інженерних принципів кібербезпеки, сучасних технологій, методів, моделей і засобів захисту інформації, процесів управління кібербезпекою, а також забезпечувати безпеку об'єктів інформаційної діяльності, критичної інфраструктури.	

3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань F Інформаційні технології 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 програма має прикладну (професійну) орієнтацію. Вона спрямована на підготовку висококваліфікованих фахівців, здатних ефективно виконувати спеціалізовані завдання у сфері кібербезпеки та захисту інформації. Зміст програми забезпечує оптимальне поєднання фундаментальних теоретичних знань із практичними навичками. Програма враховує актуальні потреби ринку праці, відповідає вимогам Національної рамки кваліфікацій та галузевих професійних стандартів, а професійно спрямовані

	дисципліни формують у здобувачів комплексні компетентності, необхідні для успішного старту кар'єри.
Основний фокус освітньої програми й спеціалізації	Акцент робиться на формуванні та розвитку професійних компетентностей, щодо: захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури; застосування теоретичних засад, методичних положень та організаційно-практичних інструментів у межах спеціальності; використання сучасних методик забезпечення кібербезпеки, включаючи виявлення та протидію кіберінцидентам, захист інформаційних ресурсів та управління процесами кібербезпеки. <i>Ключові слова:</i> кібербезпека, кіберзагроза, кіберінцидент, кіберзахист, захист інформації, об'єкт інформаційної діяльності, критична інфраструктура, криптографічний захист, комплексні системи захисту інформації, технічні канали витоку інформації, несанкціонований доступ, технічний захист інформації, управління кібербезпекою.
Особливості програми	Програма розроблена з урахуванням професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку від 25.11.2022 № 715. Програма включає низку дисциплін, спрямованих на розвиток універсальних компетентностей (soft skills) здобувачів. Обов'язкова виробнича практика забезпечує підготовку фахівця в реальному середовищі майбутньої професійної діяльності. До викладацької діяльності залучаються керівники та фахівці, які працюють у системі професійної освіти, на підприємствах галузі інформаційних технологій, а також представники бізнесу. Це забезпечує передачу передового досвіду, висвітлення в навчальному процесі останніх досягнень науки і техніки, а також ознайомлення з сучасними практиками управління. Передбачено можливості для академічної мобільності, міжнародної співпраці та участі в молодіжних обмінах.
4 – Придатність випускників до працевлаштування й подальшого навчання	
Придатність до працевлаштування	Випускник є придатним для працевлаштування на підприємствах, в організаціях та установах, на яких обробляється інформація з обмеженим доступом, що займаються розробкою та супроводом програмного забезпечення захисту інформації і відповідно до Національного класифікатора України: Класифікатор професій (ДК 003:2010) займати первинну посаду за

	категоріями: 2139.2 Фахівець сфери захисту інформації; 2139.2 Фахівець з підтримки інфраструктури кіберзахисту; 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки); 2139.2 Фахівець з реагування на інциденти кібербезпеки; 3439 Фахівець із організації захисту інформації з обмеженим доступом.																					
Академічні права випускників	Мають право на здобуття освіти за програмою другого (магістерського) рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти. Отримання другої вищої освіти (за наявності диплому бакалавра) за цією ж галуззю знань або суміжною (що узгоджується з отриманим дипломом бакалавра).																					
5 – Викладання й оцінювання																						
Викладання й навчання	Здобувачоцентроване, проблемно-орієнтоване навчання і самонавчання, комунікативно-діяльнісний та технологічний підходи. Використовуються інтерактивні, дослідницькі, проєктні та проблемні методи навчання, що сприяють розвитку критичного мислення та практичних навичок. Викладання проводиться у таких формах: лекції, практичні та семінарські заняття, лабораторні роботи, тренінгова підготовка та бізнес-симуляція, майстер-класи від практиків галузі; курсові роботи та індивідуальні завдання; практика; виконання кваліфікаційної роботи.																					
Оцінювання	Екзамени, заліки, захист звіту з практик, захист курсових робіт (проєктів), публічний захист кваліфікаційної роботи. Оцінювання навчальних досягнень здобувачів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F). <table><tr><td>Оцінка за 100-бальною</td><td>Оцінка за національною</td><td>шкалою Оцінка за</td></tr><tr><td>90 – 100</td><td>відмінно</td><td>A</td></tr><tr><td>82 – 89</td><td rowspan="2">добре</td><td>B</td></tr><tr><td>74 – 81</td><td>C</td></tr><tr><td>64 – 73</td><td rowspan="2">задовільно</td><td>D</td></tr><tr><td>60 – 63</td><td>E</td></tr><tr><td>35 – 59</td><td rowspan="2">незадовільно</td><td>FX</td></tr><tr><td>0 – 34</td><td>F</td></tr></table>	Оцінка за 100-бальною	Оцінка за національною	шкалою Оцінка за	90 – 100	відмінно	A	82 – 89	добре	B	74 – 81	C	64 – 73	задовільно	D	60 – 63	E	35 – 59	незадовільно	FX	0 – 34	F
Оцінка за 100-бальною	Оцінка за національною	шкалою Оцінка за																				
90 – 100	відмінно	A																				
82 – 89	добре	B																				
74 – 81		C																				
64 – 73	задовільно	D																				
60 – 63		E																				
35 – 59	незадовільно	FX																				
0 – 34		F																				
6 – Програмні компетентності																						
Інтегральна компетентність (ІК)	Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.																					

Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою як усно. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6. 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. ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, 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. ЗК9. Здатність до національного спротиву.
Спеціальні (фахові, предметні) компетентності (СК)	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки інформаційної та захисту інформації. СК4. Здатність забезпечувати захист інформації інформаційних та інформаційно-телекомунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та

	технічних засобів і методів, процедур, практичних прийомів тощо). СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
Професійні компетентності з урахуванням професійного стандарту «Фахівець сфери захисту інформації»	
Професійні компетентності (А, Д) з професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022. А1. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації. А2. Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз. А3. Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах. А5. Здатність виконувати передпроектні роботи щодо систем та комплексів захисту інформації. А7. Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах. А8. Здатність адмініструвати системи, мережі та системи безпеки інформації. А10. Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності. Д1. Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації.	
7 – Програмні результати навчання (ПРН)	
ПРН-1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	

ПРН-2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

ПРН-3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

ПРН-4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН-5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН-6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН-7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

ПРН-8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

ПРН-9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

ПРН-10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

ПРН-11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

ПРН-12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

ПРН-13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

ПРН-14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

ПРН-15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з

метою оперативного відновлення функціонування інформаційної системи.

ПРН-16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

ПРН-17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

ПРН-18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

ПРН-19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

ПРН-20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

ПРН-21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

**Уміння та навички з урахуванням професійного стандарту
«Фахівець сфери захисту інформації»**

A1.У1. Визначати (формулювати) потреби щодо захисту інформації, що обробляється в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників).

A1.У3. Визначати (формулювати) потреби до кібербезпеки в електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників).

A1.У5. Здійснювати попередню оцінку достатності потреб і вимог користувачів (замовників) для забезпечення необхідного рівня захисту інформації та кіберзахисту.

A1.У7. Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки.

A2.У2. Виявляти загрози для інформації, що озвучується на об'єктах інформаційної діяльності (обґрунтовувати можливість створення певних технічних каналів витоку інформації, що озвучується на конкретному об'єкті інформаційної діяльності).

A2.У3. Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості комп'ютерної системи (систем) для розробки профілю безпеки.

A2.У4. Оцінювати та аналізувати ризики безпеки інформації та кібербезпеки.

A2.У5. Розробляти модель загроз для інформації від несанкціонованих дій

та модель порушника інформації.

A3.U2. Ураховувати методи управління мережевими системами при обґрунтуванні концепції безпеки інформації.

A3.U3. Ураховувати методи управління ризиками при обґрунтуванні концепції безпеки інформації.

A3.U5. Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам і потребам.

A5.U1. Здійснювати категоріювання об'єктів інформаційної діяльності (об'єктів електронно-обчислювальної техніки).

A5.U2. Здійснювати обстеження середовищ функціонування автоматизованих систем.

A5.U3. Здійснювати обстеження об'єктів інформаційної діяльності.

A5.U4. Розробляти моделі загроз для інформації.

A7.U7. Активізувати (налаштовувати) програмні механізми захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах (програмні фільтри, антивірусні програми, антишпигунське програмне забезпечення).

A8.U3. Здійснювати системне адміністрування операційних систем і спеціалізованих прикладних програм кіберзахисту та захисту інформації, систем (антивірусне програмне забезпечення, засоби аудиту та відновлення) та пристроїв віртуальних приватних мереж (VPN), включаючи інсталяції, налаштування, обслуговування, резервне копіювання і відновлення.

A8.U4. Здійснювати адміністрування серверів.

A10.U2. Здійснювати виявлення (брати участь у виявленні) закладних пристроїв на об'єктах інформаційної діяльності.

D1.U1. Аналізувати систему нормативних документів (нормативну базу) системи технічного та криптографічного захисту інформації України.

D1.U2. Виявляти, ставити та вирішувати проблемні питання щодо системи нормативних документів (нормативної бази) системи технічного та криптографічного захисту інформації України.

D1.U3. Проводити системний аналіз світових практик, стандартів із захисту інформації.

D2.U3. Впроваджувати нормативні документи системи технічного та криптографічного захисту інформації.

D2.U4. Здійснювати актуалізацію нормативних документів системи технічного та криптографічного захисту інформації.

8 – Ресурсне забезпечення реалізації програми

Кадрове забезпечення

Кадрове забезпечення відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності для першого рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності (залучення роботодавців до організації та реалізації освітнього процесу; залучення до аудиторних занять професіоналів

	практиків, експертів галузі). Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. Реалізована система професійного розвитку викладачів, у тому числі у вигляді співпраці з провідними компаніями галузі інформаційної та/або кібербезпеки.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення дозволяє повністю забезпечити освітній процес протягом всього циклу підготовки за освітньою програмою. Реалізація освітньо-професійної програми забезпечується: – приміщеннями для проведення навчальних занять та контрольних заходів; – мультимедійним обладнанням для одночасного використання в навчальних аудиторіях; – комп'ютерними робочими місцями, спеціалізованими лабораторіями, обладнанням, устаткуванням, доступом до Інтернету та інформаційних ресурсів, необхідних для навчання, викладацької та наукової діяльності. Соціальна-побутова інфраструктура: бібліотека, зокрема і читальна зала; пункти харчування; актова зала; спортивна зала. Стан приміщень засвідчено санітарно-технічними паспортами, що відповідають існуючим нормативним актам.
Інформаційне й навчально-методичне забезпечення	Інформаційне та навчально-методичне забезпечення освітньої програми відповідає ліцензійним вимогам, має актуальний і змістовний контент. Інформаційне забезпечення освітньої програми здійснюється бібліотекою, репозитарієм та онлайн ресурсами (https://suitt.edu.ua/biblioteka; https://metod.suitt.edu.ua; https://suitt.edu.ua/naukometrychni-bazy-danykh). Забезпеченість бібліотеки вітчизняними та іноземними періодичними фаховими виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді є достатньою для ефективної реалізації освітньої програми. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. Наявність офіційного веб-сайту Університету (https://suitt.edu.ua), на якому розміщено основну інформацію про його діяльність (структура; ліцензії; сертифікати про акредитацію; освітня, наукова, міжнародна, організаційна діяльність; структурні

	підрозділи та їх склад; правила прийому, контактна інформація і т. ін.). Наявність в Університеті електронного ресурсу, що містить 100% навчально-методичних матеріалів з дисциплін навчального плану освітньо-професійної програми. Наявність авторських розробок науково-педагогічних працівників, які долучені до групи забезпечення освітньо-професійної програми. Навчально-методичне забезпечення освітньо-професійної програми складається з: навчального плану, силабусів навчальних дисциплін, робочих програм навчальних дисциплін; навчально-методичних матеріалів; програми та методичних матеріалів до практичної підготовки, методичні матеріали до виконання кваліфікаційних робіт.
9 – Академічна мобільність	
Національна кредитна мобільність	У межах реалізації освітньо-професійної програми здобувачам першого (бакалаврського) рівня вищої освіти зі спеціальності F5 Кібербезпека та захист інформації надається можливість скористатися освітніми пропозиціями вітчизняних Університетів-партнерів, з якими ДУІТЗ підписано відповідні меморандуми та угоди про академічну мобільність. Визначення результатів навчання за програмами кредитної мобільності здійснюється на основі узгоджених з університетами-партнерами навчальних планів та/або їх окремих частин (кредитних модулів, навчальних дисциплін) та на основі Європейської кредитної трансферно-накопичувальної системи.
Міжнародна кредитна мобільність	Міжнародна кредитна мобільність здійснюється відповідно до нормативно-правових документів з цієї діяльності з міжнародними Університетами-партнерами та стейкхолдерами проектів і програм технічної допомоги Україні, наказів ректора тощо, за такими напрямками: програми обміну, подвійного диплому, стипендіальні програми, програми стажування/практики, проектна діяльність і т. ін.
Навчання іноземних здобувачів вищої освіти	Прийом на навчання іноземних здобувачів здійснюється за «Правилами прийому на навчання для здобуття вищої освіти в Державному університеті інтелектуальних технологій і зв'язку» https://suitt.edu.ua/pravyla-priyomu.

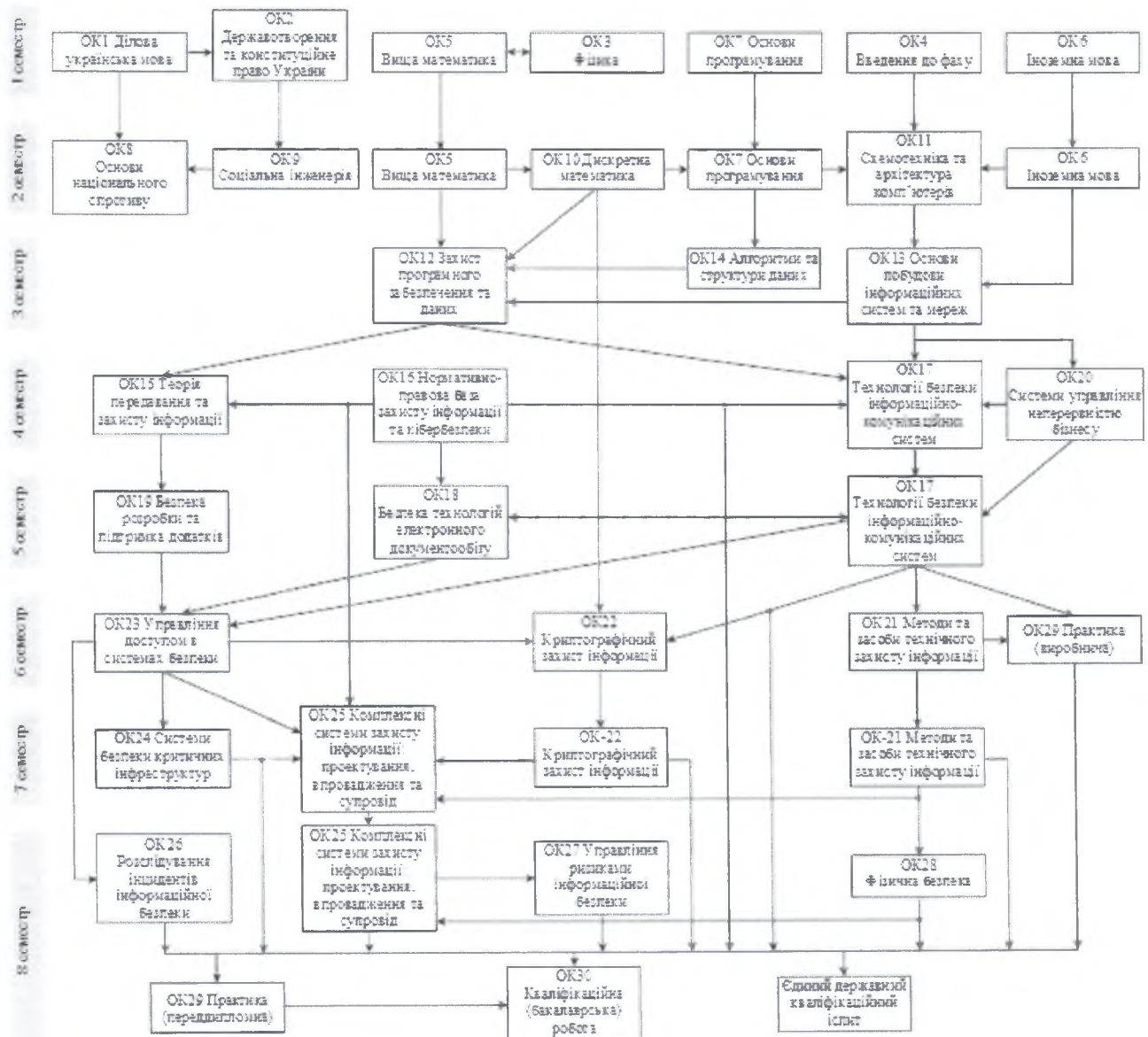
**2. Перелік компонент освітньо-професійної програми
«Кібербезпека та захист інформації»
та їх логічна послідовність**

2.1. Перелік освітніх компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю
1	2	3	4
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ (ОК)			
OK1	Ділова українська мова	4	екзамен
OK2	Державотворення та конституційне право України	5	екзамен
OK3	Фізика	6	екзамен
OK4	Введення до фаху	4	екзамен
OK5	Вища математика	8	екзамен
OK6	Іноземна мова	8	екзамен
OK7	Основи програмування	7	екзамен
OK8	Основи національного спротиву	5	екзамен
OK9	Соціальна інженерія	4	залік
OK10	Дискретна математика	4	екзамен
OK11	Схемотехніка та архітектура комп'ютерів	5	залік
OK12	Захист програмного забезпечення та даних	6	екзамен
OK13	Основи побудови інформаційних систем та мереж	6	екзамен
OK14	Алгоритми та структури даних	6	екзамен
OK15	Теорія передавання та захисту інформації	5	екзамен, КР
OK16	Нормативно-правова база захисту інформації та кібербезпеки	4	екзамен
OK17	Технології безпеки інформаційно-комунікаційних систем	11	екзамен, КР
OK18	Безпека технологій електронного документообігу	6	екзамен
OK19	Безпека розробки та підтримка додатків	6	екзамен
OK20	Системи управління неперервністю бізнесу	4	екзамен
OK21	Методи та засоби технічного захисту інформації	9	екзамен, КР
OK22	Криптографічний захист інформації	11	екзамен, КР
OK23	Управління доступом в системах безпеки	4	екзамен
OK24	Системи безпеки критичних інфраструктур	4	екзамен
OK25	Комплексні системи захисту інформації: проектування, впровадження та супровід	6	екзамен
OK26	Розслідування інцидентів інформаційної безпеки	4	екзамен
OK27	Управління ризиками інформаційної безпеки	4	екзамен
OK28	Фізична безпека	6	екзамен, КР
OK29	Практика (виробнича, переддипломна)	10	екзамен
OK30	Кваліфікаційна (бакалаврська) робота. Атестація	8	публічний захист
Загальний обсяг Обов'язкових компонент		180 кредитів ЄКТС 5400 акад. год.	2 заліки 28 екзамени
Загальний обсяг Вибіркових компонентів (60 кредитів ЄКТС, з них: 10 кредитів ЄКТС – обов'язкова вибіркова дисципліна «Базова загальновійськова підготовка»)		60 кредитів ЄКТС 1800 акад. год.	10 заліків
Усього:		240 кредитів ЄКТС 7200 акад. год.	

2.2. Структурно-логічна схема освітньо-професійної програми

Складові програми	Таймінг навчання протягом 3 років 10 місяців (за семестрами)							
	1	2	3	4	5	6	7	8
Обов'язкові та вибіркові компоненти теоретичної підготовки	OK1/4 OK2/5 OK3/6 OK4/4 OK5/3 OK6/4 OK7/4	OK5/4 OK6/4 OK7/4 OK8/5 OK9/4 OK10/4 OK11/5	OK12/6 OK13/6 OK14/6	OK15/5 OK16/4 OK17/5 OK20/4	OK17/6 OK18/6 OK19/6	OK21/4 OK22/4 OK23/4	OK21/5 OK22/4 OK24/4 OK25/3 OK26/4 OK27/4	OK22/3 OK25/3 OK28/6
Практична підготовка			BK1/6 BK2/6	BK3.1/3 BK3.2/7 BK4/2	BK5/6 BK6/6	BK7/6 BK8/6	BK9/6	BK10/6
Кваліфікаційна робота						OK29/6		OK29/4
Кількість кредитів ЄКТС	30	30	30	30	30	30	30	30



3. Форми атестації здобувачів вищої освіти

Атестація здобувачів освітньої програми «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації проводиться у формі єдиного державного кваліфікаційного іспиту, затвердженого постановою Кабінету Міністрів України від 19 травня 2021 р. № 497 «Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту» (в редакції від 06.09.2024 № 1024) пункту 3 Порядку, а також захисту кваліфікаційної (бакалаврської) роботи й завершується видачою документа встановленого зразка про присудження йому освітнього ступеня «бакалавр» із присвоєнням кваліфікації: Бакалавр із кібербезпеки за спеціальністю F5 Кібербезпека та захист інформації. Атестація здійснюється відкрито і публічно. Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.

Вимоги до кваліфікаційної (бакалаврської) роботи. Кваліфікаційна (бакалаврська) робота здобувача першого (бакалаврського) рівня вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації є самостійним розгорнутим дослідженням, що відображає інтегральну компетентність здобувача та підбиває підсумки набутих ним програмних результатів навчання з обов'язкових компонентів, передбачених навчальним планом. Кваліфікаційна робота має передбачати розв'язання спеціалізованого завдання або практичної проблеми у галузі інформаційної та/або кібербезпеки. Виконання кваліфікаційної роботи має за мету систематизувати, закріпити та розширити теоретичні знання та практичні навички зі спеціальності, розвинути творчі здібності та вміння здобувача повною мірою застосувати свої знання для вирішення технічних, проектних і організаційних задач у галузі кібербезпеки та захисту інформації. Випускна кваліфікаційна робота має продемонструвати здатність випускника виконувати актуальні завдання спеціальності та вміння використовувати надбані компетентності та результати навчання, логічно, на підставі проведених досліджень обґрунтувати проектні рішення, робити аргументовані висновки та формулювати конкретні пропозиції та рекомендації щодо виконаного завдання. Вимоги до змісту, обсягу й структури кваліфікаційної роботи визначаються закладом вищої освіти.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	Загальні компетентності										Спеціальні (фахові) компетентності											Професійні компетентності стандарту «Фахівець сфери захисту інформації»											
	1	2	3	4	5	6	7	8	9		1	2	3	4	5	6	7	8	9	10		A1	A2	A3	A5	A7	A8	A10	Д1	Д2			
OK1	+		+																														
OK2	+					+		+																									
OK3	+	+																															
OK4	+	+										+					+																
OK5	+																																
OK6	+			+																													
OK7	+				+																												
OK8									+																								
OK9	+		+																														
OK10	+																																
OK11	+				+																												
OK12	+	+			+													+			+												
OK13	+	+			+							+		+	+					+		+											
OK14	+				+																												
OK15	+	+			+							+									+												
OK16	+	+			+						+					+															+	+	
OK17	+	+		+								+	+		+	+		+			+	+			+	+				+	+		
OK18	+	+									+	+						+					+							+			
OK19	+	+			+									+	+		+			+		+											
OK20	+	+			+									+							+		+										
OK21	+	+			+							+				+			+			+					+	+	+	+	+	+	
OK22	+	+			+						+			+				+													+	+	
OK23	+	+			+							+					+						+										
OK24	+	+			+							+		+		+				+		+	+										
OK25	+	+			+						+			+	+				+			+	+		+								
OK26	+	+			+						+	+		+								+	+										
OK27	+	+			+						+										+		+	+									
OK28	+	+			+						+	+								+													
OK29	+	+			+						+	+					+		+			+	+	+	+	+	+	+	+	+	+	+	
OK30	+	+	+		+						+	+				+				+		+	+	+	+	+	+	+	+	+	+	+	

5. Матриця забезпечення результатів навчання відповідними компонентами освітньо-професійної програми

[illegible]

	Уміння та навички з урахуванням стандарту «Фахівець сфери захисту інформації»																							
	A1. У1	A1. У3	A1. У5	A1. У7	A2. У2	A2. У3	A2. У4	A2. У5	A3. У2	A3. У3	A3. У5	A5. У1	A5. У2	A5. У3	A5. У4	A7. У7	A8. У3	A8. У4	A10. У2	Д1. У1	Д1. У2	Д1. У3	Д2. У3	Д2. У4
OK1																								
OK2																								
OK3																								
OK4	+	+																		+				
OK5																								
OK6																								
OK7																								
OK8																								
OK9																								
OK10																								
OK11																								
OK12	+	+		+																				
OK13	+	+																						
OK14																								
OK15	+			+																				
OK16																				+	+	+	+	+
OK17	+					+										+	+	+				+	+	
OK18	+			+																+		+		
OK19				+																				
OK20				+					+	+														
OK21					+														+			+	+	
OK22																				+			+	+
OK23									+		+													
OK24			+				+																	
OK25	+							+				+	+	+	+									
OK26						+	+			+														
OK27						+	+			+														
OK28			+	+																		+		
OK29	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
OK30	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

6. Характеристика системи внутрішнього забезпечення якості підготовки здобувачів першого (бакалаврського) рівня вищої освіти

Принципи та процедури забезпечення якості підготовки здобувачів першого (бакалаврського) 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 вебсайті 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 (бакалаврської) роботи, наскрізну програму практики, завдання для самостійної роботи здобувачів вищої освіти, які розміщені в системі Moodle на платформі e-Learning ДУІТЗ (<https://e-learning2.suitt.edu.ua>). Інформаційне забезпечення освітньої програми здійснюється бібліотекою, та відповідними онлайн ресурсами (<https://suitt.edu.ua/biblioteka>; <https://suitt.edu.ua/naukometrychni-bazy-danykh>; <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 дві лабораторії: «Кібербезпеки», «Технічних засобів охорони та захисту інформації».

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 липня 2014 року № 1556-VII (в редакції від 11.03.2026 р. № 4702-IX).
URL: <https://zakon.rada.gov.ua/laws/show/1556-18#Text>
2. Закон України «Про наукову і науково-технічну діяльність» від 26 листопада 2015 року № 848-VIII (в редакції від 22.03.2026 р. № 4794-IX).
URL: <https://zakon.rada.gov.ua/laws/show/848-19#Text>
3. Закон України «Про освіту» від 05 вересня 2017 року № 2145-VIII (в редакції від 01.01.2026 р. № 4695-IX).
URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text>
4. Наказ Міністерства освіти і науки України «Про затвердження Вимог до міждисциплінарних освітніх (наукових) програм» від 01.02.2021 № 128 (в редакції від 21.03.2025 р. № 482).
URL: <https://zakon.rada.gov.ua/laws/show/z0454-21#Text>
5. Наказ Міністерства освіти і науки України «Про затвердження Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти» від 15 травня 2024 року № 686.
URL: <https://zakon.rada.gov.ua/laws/show/z1013-24#Text>
6. Національний класифікатор України: «Класифікатор професій» ДК 003:2010 (в редакції від 13.12.2024).
URL: <https://zakon.rada.gov.ua/rada/show/va327609-10#Text>.

7. Положення про організацію освітнього процесу в ДУІТЗ, введеного в дію наказом ректора від 29.05.2025 № 01-02-102.
URL: <https://suitt.edu.ua/polozhennia/>
8. Постанова Кабінету Міністрів України «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» від 30 серпня 2024 року № 1021.
URL: <https://zakon.rada.gov.ua/laws/show/1021-2024-%D0%BF#Text>
9. Постанова Кабінету Міністрів України «Про затвердження ліцензійних умов провадження освітньої діяльності» від 30 грудня 2015 року № 1187 (в редакції від 31.10.2023 р. № 1134).
URL: <https://zakon.rada.gov.ua/laws/show/1187-2015-%D0%BF#Text>
10. Постанова Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій» від 23 листопада 2011 року № 1341 (в редакції від 05.02.2026 р. № 159).
URL: <https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text>
11. Постанова Кабінету Міністрів України «Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційною іспиту» від 19 травня 2021 року № 497.
URL: <https://ips.ligazakon.net/document/KP210497>
12. Наказ Адміністрації Держспецзв'язку професійний стандарт «Фахівець сфери захисту інформації» від 25 листопада 2022 року № 715.
URL: https://register.nqa.gov.ua/uploads/0/439-profesijnij_standart_fahivec_sferi_zahistu_informacii.pdf
13. Наказ Міністерства освіти і науки України «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 та описів предметних областей спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 31 грудня 2025 р. № 1734.
URL: https://register.nqa.gov.ua/uploads/0/439-profesijnij_standart_fahivec_sferi_zahistu_informacii.pdf

Гарант освітньої програми



Євген ВАСІЛІУ