МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Державний університет інтелектуальних технологій і зв'язку

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека та захист інформації»

«*Cybersecurity and information protection*»

№ 2-13-29

Рівень вищої освіти	Перший (бакалаврський)
Ступінь вищої освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня кваліфікація	Бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО
Вченою радою Державного університету інтелектуальних технологій і зв'язку
(протокол від 10 липня 2023 р. № 4)

Освітньо-професійна програма (*оновлена*) вводиться в дію з 01 вересня 2023 р.
Ректор _____ Олександр НАЗАРЕНКО
(наказ від 10 липня 2023 р. № 01-02-125)

Одеса 2023

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми
«Кібербезпека та захист інформації»
зі спеціальності 125 Кібербезпека та захист інформації
за першим (бакалаврським) рівнем вищої освіти

ВНЕСЕНО
Кафедрою кібербезпеки та технічного захисту інформації
Протокол № 10 від 26 травня 2023 р.

Завідувач кафедри Володимир КОРЧИНСЬКИЙ

ПОГОДЖЕНО
Декан факультету Інформаційних технологій та кібербезпеки
01 березня 2023 р. Євген ВАСІЛІУ

ПОГОДЖЕНО
Начальник відділу ліцензування та акредитації
12 червня 2023 р. Юлія ШТОВБА

ПОГОДЖЕНО
Навчально-методичною радою Державного університету інтелектуальних технологій і зв'язку
Протокол від 15 червня 2023 р. № 6

Голова Анатолій ЛОЖКОВСЬКИЙ

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 галузі знань 12 Інформаційні технології зі спеціальності 125 Кібербезпека та захист інформації.

1. Внесено: кафедрою кібербезпеки та технічного захисту інформації.

2. Затверджено та надано чинності рішенням ученої ради Державного університету інтелектуальних технологій і зв'язку, протокол від 10 липня 2023 р. № 4.

3. Розроблено робочою групою у складі:

Керівник робочої групи (гарант освітньої програми):

Онацький Олексій Віталійович, доцент, кандидат технічних наук, доцент кафедри кібербезпеки та технічного захисту Державного університету інтелектуальних технологій і зв'язку.

Члени робочої групи:

– Басов Віктор Євгенович, доцент, кандидат технічних наук, доцент кафедри кібербезпеки та технічного захисту;

– Лімарь Ігор Валерійович, старший викладач, кандидат технічних наук, старший викладач кафедри кібербезпеки та технічного захисту.

4. Рецензії-відгуки зовнішніх стейкхолдерів:

Корченко О.Г. - президент ГО Асоціація спеціалістів кібербезпеки;

Ткаченко О.В. - заступник Генерального директора ТОВ «Консалтингова компанія СІДКОН»;

Барановський С.В. - Директор департаменту інформаційних систем та систем безпеки ТОВ «Роберт Бош ЛТД».

Освітньо-професійну програму розроблено відповідно до:

Законів України «Про вищу освіту» (від 01 липня 2014 р. № 1556-VII; в редакції від 26 лютого 2021 р.) і «Про освіту» (від 05 вересня 2017 р. № 2145-VIII; в редакції від 01 січня 2021 р.);

Постанов Кабінету Міністрів України: «Про затвердження ліцензійних умов провадження освітньої діяльності» (від 30 грудня 2015 р. № 1187; в редакції від 03 травня 2020 р. № 180); «Про затвердження Національної рамки кваліфікацій» (23 листопада 2011 р. № 1341; в редакції від 5 червня 2020 р. № 519); «Про особливості запровадження переліку знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти (від 29 квітня 2015 р. № 266; із змінами, внесеними згідно з наказом МОН від 06 листопада 2015 р. № 1151);

Листом Міністерства освіти і науки України № 1/9-239 від 28 квітня 2017 р. (Примірний зразок освітньо-професійної програми для першого (бакалаврського) та другого (магістерського) рівнів);

Стандарту вищої освіти України першого (бакалаврського) рівня вищої освіти ступеня «бакалавр» галузь знань 12 Інформаційні технології за спеціальність 125 Кібербезпека (затверджено та введено в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074).

1. Профіль освітньо-професійної програми «Кібербезпека та захист інформації» зі спеціальності 125 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. Обсяг освітньої програми бакалавра: – на базі повної загальної середньої освіти становить 240 кредитів ЄКТС; – на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати кредити ЄКТС, отримані в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста), обсягом не більше ніж 120 кредитів ЄКТС. Термін навчання 3 роки 10 місяців.
Наявність акредитації	Сертифікат акредитації напряму 6.170102 – Системи технічного захисту інформації НД-ІІ № 1679594 від 21.06.2016. Термін дії до 01.07.2026 р.
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, здатних розробляти і використовувати технології інформаційної безпеки, з правом подальшої професійної діяльності у системі державних та комерційних підприємств, пов'язаної з надання послуг щодо захисту інформації на об'єктах інформаційної діяльності.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності)).	Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека та захист інформації *Об'єкти професійної діяльності випускників:* – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-комунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. *Цілі навчання:* – підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. *Теоретичний зміст предметної області (знання):* – 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. *Методи, методики та технології:* – методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки. *Інструменти та обладнання:*

	– системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна програма. Професійно-орієнтовані дисципліни забезпечують базові знання з усіх базових технологій інформаційної та/або кібербезпеки.
Основний фокус освітньої програми й спеціалізації.	Акцент робиться на формуванні та розвитку професійних компетентностей, щодо захисту інформації на об'єктах інформаційної діяльності; вивченні теоретичних та методичних положень, організаційних та практичних інструментів зі спеціальності кібербезпеки; методики та технології забезпечення безпеки інформації. *Ключові слова*: кібербезпека, захист інформації, криптографічний захист, безпека розробки додатків, комп'ютерні мережі, архітектура безпеки, керування доступом, безпека хмарних технологій, фізична безпека.
Особливості програми	Програма розроблена з урахуванням міжнародних стандартів, рекомендацій та практик, зокрема, з урахуванням змісту програм підготовки до іспиту для отримання міжнародних сертифікатів в галузі інформаційної безпеки (Certified Information Systems Security Professional – CISSP). Програма містить декілька окремих дисциплін для здобуття студентами soft skills, зокрема, передбачено більш 20 кредит для вивчення іноземної мови. Програма передбачає обов'язкове професійне навчання з метою отримання майбутнім фахівцем кваліфікації фахівця з кібербезпеки та захисту інформації в інформаційних і комунікаційних системах. Передбачена практика, з метою забезпечення умов підготовки фахівця в реальному середовищі майбутньої професійної діяльності. Залучаються до викладацької діяльності керівники та професіонали, які працюють в системі професійної освіти та на виробництві в галузі захисту інформації, а також представники бізнесу, з метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу. Реалізація процесного підходу при конструюванні змісту професійно-орієнтованих навчальних дисциплін. Рекомендується реалізація студентської мобільності, академічної співпраці та молодіжних обмінів.

4 – Придатність випускників до працевлаштування й подальшого навчання	
Придатність до працевлаштування	Випускник є придатним для працевлаштування на підприємствах, в організаціях та установах, на яких обробляєтеся 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: – 3439 – фахівець з режиму секретності; – 3439 – фахівець із організації захисту інформації з обмеженим доступом; – 3439 – фахівець із організації інформаційної безпеки.
Подальше навчання	Можливість продовження навчання 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	Викладання проводиться у вигляді: лекцій, семінарських, практичних занять робіт. Передбачена самостійна робота на основі підручників і конспектів, консультації з викладачем, електронне навчання за окремими освітніми компонентами, виконання проектів (в тому числі командних), електронне навчання в системі Moodle, самонавчання. Система методів навчання базується на принципах цілеспрямованості, бінарності – активної безпосередньої участі викладача і студента. До навчального процесу з фахових дисциплін запрошуються гостьові спікери (представники роботодавців), забезпечується наставництво під час проходження практики та в ході виконання курсових проектів.
Оцінювання	Усне та письмове опитування; тестовий контроль; захист індивідуальних та курсових робіт; доповіді на семінарських заняттях, презентації, заліки, екзамени, підсумкова атестація – атестаційний іспит, кваліфікаційна робота (дипломна робота). Модульно-рейтингова система оцінювання. Відповідність підсумкових рейтингових оцінок у балах оцінкам за національною шкалою і шкалою ECTS:

	Оцінка за 100-баловою	Оцінка за національною	Оцінка за шкалою
	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 (ПК)	
Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. 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. 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.
Спеціальні (фахові, предметні) компетентності (КФ)	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 та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей

	інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. 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.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. 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.
7 – Програмні результати навчання (ПРН)	
ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних	

проблем у професійній діяльності, оцінювати їхню ефективність.
ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
ПРН 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.
ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки.
ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
ПРН 12. Розробляти моделі загроз та порушника.
ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН 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.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних.

ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
ПРН 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.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 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).
ПРН 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.
ПРН 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.
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 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.
ПРН 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.
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації.
ПРН 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.
ПРН 36. Виявляти небезпечні сигнали технічних засобів.
ПРН 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.
ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
ПРН 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.
ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
ПРН 49. Забезпечувати належне функціонування системи моніторингу

інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	
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, а також співпраці з Агентством США з міжнародного розвитку (USAID) за проектом «Кібербезпека Критично Важливої Інфраструктури України».
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; також у

	рамках проекту «Кібербезпека Критично Важливої Інфраструктури України» Агентством USAID забезпечується безкоштовний доступ для студентів до кіберполігону RangeForce. Соціальна-побутова інфраструктура: бібліотека, зокрема і читальна зала; два 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/library; https://suitt.edu.ua/naukometrichni-bazi-danih; https://metod.suitt.edu.ua). 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 до навчальних дисциплін; програми та методичних матеріалів до практичної підготовки, методичні матеріали до виконання кваліфікаційних робіт. Наявність доступу до української науково-освітньої мережі «УРАН», підключення до Європейської мережі науки і освіти «GEANT».

9 – Академічна мобільність	
Національна кредитна мобільність	У межах реалізації освітньо-професійної програми здобувачам першого (бакалаврського) рівня вищої освіти зі спеціальності 125 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-pryjomu.

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 підсумк. контролю
1	2	3	4
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ (ОК)			
ОК-1	Ділова українська мова	4	залік
ОК-2	Історія українського державотворення	4	залік
ОК-3	Політологія та право	4	залік
ОК-4	Вища математика	10	екзамен
ОК-5	Іноземна мова (англійська, німецька, французька)	7	екзамен
ОК-6	Фізика	8	екзамен
ОК-7	Філософія	4	залік
ОК-8	Безпека життєдіяльності та охорона праці	3	залік
ОК-9	Введення до фаху	4	залік
ОК-10	Основи алгоритмізації та програмування	4	екзамен
ОК-11	Іноземна фахова мова	15	екзамен
ОК-12	Комп'ютерні технології	10	екзамен
ОК-13	Технології програмування	4	екзамен
ОК-14	Основи телекомунікацій та комп'ютерні мережі	9	екзамен
ОК-15	Теоретичні основи передавання та захисту інформації	5	залік
ОК-16	Законодавство в області інформаційної безпеки	6	залік
ОК-17	Забезпечення безпеки телекомунікацій	10	екзамен
ОК-18	Архітектура та моделі безпеки	5	залік
ОК-19	Керування доступом в системах безпеки	5	екзамен
ОК-20	Безпека розробки та підтримка додатків	5	екзамен
ОК-21	Методи та засоби захисту інформації	10	екзамен
ОК-22	Криптографічний захист інформації	9	екзамен
ОК-23	Безпека і експлуатація мережевих і хмарних технологій	3	екзамен
ОК-24	Неперервність бізнесу та відновлення після аварії	4	залік
ОК-25	Комплексні системи захисту інформації: проектування, впровадження та супровід	6	екзамен
ОК-26	Проведення розслідування інцидентів інформаційної безпеки	3	екзамен
ОК-27	Керування ризиками інформаційної безпеки	3	екзамен
ОК28	Практика (виробнича)	4	екзамен
ОК29	Практика (переддипломна)	3	екзамен
ОК30	Кваліфікаційна (бакалаврська) робота. Атестація	9	публічний захист
Загальний обсяг Обов'язкових компонент		**180 кредитів ЄКТС 5400 акад. год.**	**10 заліків 21 екзаменів**
Загальний обсяг Вибіркових компонент (10 дисциплін)		**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	ОК1/4 ОК2 /4 ОК3/4 ОК4 /3 ОК5 /3 ОК6 /4 ОК9/4 ОК10/4	ОК4 /3 ОК5 /4 ОК6 /4 ОК7 /4 ОК8 /3	ОК4 /4 ОК11 /6 ОК12 /6 ОК13 /4 ОК14 /4	ОК11 /6 ОК12 /4 ОК14 /5 ОК15 /5 ОК17 /4	ОК16 /6 ОК17 /6	ОК18 /5 ОК19 /5 ОК20 /5 ОК21 /5	ОК21 /5 ОК22 /6 ОК23 /3 ОК24/4 ОК25 /3 ОК26 /3	ОК11 /3 ОК22 /3 ОК25 /3 ОК27 /3
		ВК1/6 ВК2/6	ВК3/6	ВК4/6	ВК5/6 ВК6/6 ВК7/6	ВК8/6	ВК9/6	ВК10/6
Практична підготовка						ОК28/4		ОК29 /3
Кваліфікаційна робота								ОК30 /8
Атестація								ОК30 /1
Кількість кредитів ЄКТС	**30**	**30**	**30**	**30**	**30**	**30**	**30**	**30**

3. Форми атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Кібербезпека та захист інформації» зі спеціальності 125 «Кібербезпека та захист інформації» проводиться у формі захисту кваліфікаційної (бакалаврської) роботи й завершується видачою документа встановленого зразка про присудження йому освітнього ступеня «бакалавр» із присвоєнням кваліфікації: Бакалавр із кібербезпеки за спеціальністю 125 Кібербезпека та захист інформації. Атестація здійснюється відкрито і публічно.

Вимоги до кваліфікаційної (бакалаврської) роботи. Кваліфікаційна (бакалаврська) робота здобувача першого (бакалаврського) рівня вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» зі спеціальності 125 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 організаційно економічних задач у галузі інформаційної та/або кібербезпеки.

Випускова 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 (КЗ)								Спеціальні (фахові) компетентності (КФ)											
	1	2	3	4	5	6	7		1	2	3	4	5	6	7	8	9	10	11	12
ОК1	+		+		+				+											
ОК2	+				+	+	+													
ОК3					+	+	+													
ОК4										+					+			+		
ОК5	+		+		+				+											
ОК6	+	+									+									
ОК7										+					+			+		
ОК8	+			+							+		+	+	+		+	+		
ОК9	+			+									+			+	+			+
ОК10	+				+	+	+													
ОК11	+		+		+				+											
ОК12		+		+	+	+	+		+											
ОК13		+								+	+		+	+					+	
ОК14		+		+						+			+		+					+
ОК15	+	+		+	+									+				+		+
ОК16		+		+						+	+	+	+	+	+				+	+
ОК17	+	+			+				+	+		+	+		+		+		+	
ОК18	+	+		+							+		+		+			+		
ОК19	+	+		+						+	+		+	+			+		+	+
ОК20	+	+		+	+		+			+			+	+			+	+		
ОК21	+			+	+				+		+		+		+					
ОК22	+	+		+								+	+			+	+		+	+
ОК23	+	+		+	+		+			+	+	+	+	+			+	+	+	+
ОК24		+		+							+			+	+					+
ОК25	+			+	+				+		+		+		+					
ОК26	+	+		+	+	+	+						+							
ОК27	+	+		+			+				+	+			+			+		+
ОК28	+	+		+	+		+			+	+	+	+	+		+	+	+	+	+
ОК29	+		+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	+
ОК30	+	+	+	+	+	+	+		+	+	+	+				+	+	+	+	+

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

	Програмні результати навчання (ПРН)																										
	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
ОК1	+	+																								+	
ОК2			+																								
ОК3			+																								
ОК4	+																									+	
ОК5	+												+													+	
ОК6			+						+				+														
ОК7	+												+													+	
ОК8			+						+																		
ОК9	+								+				+													+	
ОК10	+												+													+	
ОК11	+												+													+	
ОК12	+																									+	
ОК13	+		+						+																	+	
ОК14									+				+														
ОК15			+												+				+	+							
ОК16		+	+	+	+	+		+		+		+		+	+	+	+	+	+	+	+	+	+	+			
ОК17				+						+		+	+	+	+						+	+					
ОК18									+		+		+				+										
ОК19			+		+		+			+			+	+	+		+	+	+	+		+	+	+			
ОК20	+																									+	
ОК21		+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+
ОК22					+	+	+	+		+					+	+		+	+	+							
ОК23				+	+								+													+	
ОК24			+		+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ОК25		+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+
ОК26			+	+	+	+		+				+	+	+	+	+	+	+	+	+	+	+	+	+	+		
ОК27			+		+		+		+						+			+					+	+			
ОК28			+	+		+	+																				
ОК29			+	+		+	+	+	+	+			+	+							+	+			+		
ОК30			+	+		+	+	+	+	+		+	+	+			+	+			+	+			+		

	Програмні результати навчання (ПРН)																										
	28	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
ОК1																											
ОК2																											+
ОК3																											+
ОК4																											
ОК5																											
ОК6	+						+				+										+	+				
ОК7																											
ОК8	+						+				+																
ОК9							+																				
ОК10											+																
ОК11																											
ОК12																											
ОК13	+						+				+																
ОК14																											
ОК15										+																	
ОК16	+	+	+	+		+		+		+		+	+	+	+	+	+	+	+	+	+	+					
ОК17		+						+		+	+	+	+						+	+							
ОК18							+		+		+				+												
ОК19	+		+		+			+				+	+		+	+	+	+		+	+	+					
ОК20																										+	
ОК21	+	+	+			+		+	+	+	+	+	+	+	+	+				+	+	+	+		+	+	
ОК22			+	+	+	+		+					+	+		+	+	+									
ОК23																											
ОК24	+		+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+					
ОК25	+	+	+			+		+	+	+	+	+	+	+	+	+				+	+	+	+		+	+	
ОК26	+	+	+	+		+				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ОК27	+		+		+		+				+		+			+					+	+					
ОК28	+	+		+	+																						
ОК29	+	+		+	+	+	+			+	+								+	+							
ОК30	+	+		+	+	+	+		+	+	+			+	+				+	+			+				

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

Система внутрішнього забезпечення якості вищої освіти в Державному університеті інтелектуальних технологій і зв'язку складається з таких процедур і заходів, передбачених Законом України «Про вищу освіту»:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів першого (бакалаврського) рівня вищої світи, науково-педагогічних працівників ЗВО та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ЗВО або на інформаційних стендах;

4) забезпечення підвищення кваліфікації науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів першого рівня вищої освіти, за освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників ЗВО і здобувачів першого (бакалаврського) рівня вищої освіти.

7. Перелік нормативних документів, на яких базується освітня програма

1. Закон України «Про вищу освіту». http://zakon.rada.gov.ua/laws/show/1556-18.
2. Закон України «Про освіту». https://zakon.rada.gov.ua/laws/show/2145-19.
3. Національна рамка кваліфікацій. Додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341 (в редакції 02.07.2020). https://zakon.rada.gov.ua/laws/show/1341-2011-п.#Text
4. Постанова Кабінету Міністрів України від 29.04.2015 № 266 "Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти" (редакція від 11.02.2017 р.). https://zakon.rada.gov.ua/laws/show/266-2015-п#Text
5. Постанова КМУ № 579 “Про затвердження Положення про порядок реалізації права на академічну мобільність” від 12 серпня 2015 року. https://zakon.rada.gov.ua/laws/show/579-2015-п.#Text
6. Національний класифікатор України: "Класифікатор професій" ДК 003:2010", затверджений наказом Держспоживстандарту від 28.07.2010 р. (редакція від 01.03.2015 р.). https://zakon.rada.gov.ua/rada/show/va327609-10/ed20150301.

7. Положення про організацію освітнього процесу в ДУІТЗ. Введено в дію наказом ректора від 13.07.2022 р. № 01-02-126. https://suitt.edu.ua/polozennja-duitz/

8. Наказ Міністерства освіти і науки України від «01» червня 2016 р. № 600 (у редакції наказу Міністерства освіти і науки України від 01.10.2019 р. № 1254) «Про внесення змін до методичних рекомендацій щодо розроблення стандартів вищої освіти». http://edu-mns.org.ua/img/news/8635/NakMON_1254_19.pdf.

9. Положення про розроблення, затвердження, моніторинг та перегляд освітніх програм в ДУІТЗ. Введено в дію наказом ректора від 13.07.2022 р. № 01-02-126. https://suitt.edu.ua/polozennja-duitz/

10. Положення про систему внутрішнього забезпечення якості вищої освіти та освітньої діяльності в ДУІТЗ. Введено в дію наказом ректора від 13.07.2022 р. № 01-02-126. https://suitt.edu.ua/polozennja-duitz/

11. Положення про академічну мобільність здобувачів вищої у Державному університеті інтелектуальних технологій і зв'язку. Введено в дію наказом ректора від 10.02.2023 № 01-02-22 https://suitt.edu.ua/polozennja-duitz/

Гарант освітньої програми Олексій ОНАЦЬКИЙ