МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «ТЕХНІЧНІ СИСТЕМИ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ»

другого (магістерського) рівня вищої освіти (ПРОЄКТ)

Галузь знань **F «Інформаційні технології»**

Спеціальність **F5 «Кібербезпека та захист інформації»**

Кваліфікація: **«Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою технічні системи інформаційного та кібернетичного захисту»**

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Протокол № ___ від _____ 2026 р.

Наказ № _____ від _____ 2026 р.

Ректор _____ Володимир ШУЛЬГА

Освітня програма вводиться в дію з 01 вересня 2025 р.

Київ 2026

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

спеціальність	F5 «Кібербезпека та захист інформації»
галузь знань	F «Інформаційні технології»
рівень вищої освіти	другий (магістерський)
кваліфікація	Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою технічні системи інформаційного та кібернетичного захисту

1. Перший проректор _____ Олександр КОРЧЕНКО

2. Проректор з навчальної роботи _____ Артур ГУДМАНЯН

3. Начальник навчально-методичного відділу _____ Вадим ВЛАСЕНКО

4. Вчена рада Навчально-наукового інституту кібербезпеки та захисту інформації

Протокол № ____ від «____» _____ 2026 р.

Голова вченої ради ННІКБЗІ _____ Євгенія ІВАНЧЕНКО

Кафедра технічних систем кіберзахисту

Протокол № ___ від «___» _____ 2026 р.

Завідувач кафедри

Технічних систем кіберзахисту _____ Олександр ТУРОВСЬКИЙ

Голова студентської ради ННІ КБЗІ _____ Марія СІПАЙЛОВА

Рецензії від зовнішніх стейкхолдерів:

1. Департамент поліції охорони Національної поліції України;
2. ТОВ «ЛУЧ»;
3. ТОВ «ДЕФЕНДІКО»

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Гарант освітньої програми Туровський Олександр Леонідович	доктор технічних наук, професор, завідуючий кафедрою Технічних систем кіберзахисту
Члени робочої групи: Котенко Андрій Миколайович	кандидат технічних наук, доцент, доцент кафедри Технічних систем кіберзахисту
Пепа Юрій Володимирович	кандидат технічних наук, доцент, професор кафедри Технічних систем кіберзахисту
Шуклін Герман Вікторович **(представники роботодавців)**	кандидат технічних наук, доцент, заступник директора ТОВ «ЛУЧ»
Курчинська Поліна Валеріївна **(здобувач вищої освіти)**	Студент 5 курсу спеціальності F5 – кібербезпека та захист інформації

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Оновлено відповідно до наказу №1547 від 29 жовтня 2024 року «Про внесення змін до стандарту вищої освіти зі спеціальності «Кібербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти.

Оновлення освітньої програми розроблено відповідно до: наказу Міністерства освіти і науки України від 13.06. 2024 р. № 842; статті 101 Закону України «Про військовий обов'язок і військову службу» (визначено проводити базову загальновійськову підготовку громадян України у закладах вищої освіти всіх форм власності у порядку, визначеному Кабінетом Міністрів України); підпункту 7 пункту 2 розділу II Закону України від 11 квітня 2024 року № 3633-IX «Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку» (базова загально-військова підготовка, визначена статтею 101 Закону України «Про військовий обов'язок і військову службу», розпочинається з 1 вересня 2025 року); Постанови Кабінету Міністрів України від 21 червня 2024 р. № 734 (затверджено Порядок проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських); пропозицій та побажань стейкголдерів (здобувачів вищої освіти, науковопедагогічних працівників, випускників, роботодавців, громадської організації) та з урахуванням тенденцій розвитку спеціальності, ринку праці, галузевого контексту, а також досвіду аналогічних вітчизняних та іноземних освітніх програм. 2026 р. пропозицій та побажань стейкголдерів (здобувачів вищої освіти, науковопедагогічних працівників, випускників, роботодавців, громадської організації) та з урахуванням тенденцій розвитку спеціальності, ринку праці, галузевого контексту, а також досвіду аналогічних вітчизняних та іноземних освітніх програм.

Затверджено рішенням кафедри Технічних систем кіберзахисту,
(назва кафедри)
Протокол № ____ від «___» _____ 2026 р.

Введено в дію наказом ректора № _____ від _____ 2026 року.

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій, Навчально-науковий інститут кібербезпеки та захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Освітня кваліфікація – Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою технічні системи інформаційного та кібернетичного захисту
Офіційна назва освітньої програми	Освітньо-професійна програма «Технічні системи інформаційного та кібернетичного захисту»
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний Обсяг освітньої програми-90 кредитів ЄКТС; термін навчання 1 рік 5 місяців.
Наявність акредитації	Сертифікат про акредитацію УД №11007045, до 01.07.2025
Цикл/рівень	НРК України – 7 рівень/ Магістр, QF-EHEA- другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра або магістра іншої спеціальності
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	Вводиться в дію з 01.09.2025 року
Інтернет - адреса постійного розміщення опису освітньої програми	http://www.dut.edu.ua/ua/1823-osvitno-profesiyni-programi-kafedra-sistem-informaciynogo-ta-kibernetichnogo-zahistu
2 – Мета освітньої програми	
Метою магістерської програми є підготовка висококваліфікованих фахівців магістрів з кібербезпеки та захисту інформації за освітньо-професійною програмою технічні системи інформаційного та кібернетичного захисту , які здатні проводити наукові дослідження, здійснювати професійну діяльність у системі державних та комерційних підприємств пов'язаної з наданням послуг щодо захисту інформації на об'єктах інформаційної діяльності, здійснювати апробацію та практичне впровадження наукових результатів, які володіють інноваційними компетентностями, необхідними для ефективного захисту інформації на об'єктах інформаційної діяльності, і здатні вирішувати практичні та науково-дослідні завдання.	

Набуті компетентності можуть бути застосовані в дослідницьких, управлінських, освітніх, підприємницьких та інших дисциплінарно-професійних полях.	
3 – Характеристика освітньої програми	
Опис предметної області	**Об'єкт діяльності:** засоби технічного захисту інформації на об'єктах інформаційної діяльності; засоби забезпечення захисту інформації при її створенні, при її обробці, при її передачі, при її зберіганні, при її знищенні, та при її візуалізації, та при інших процесах, що відображають інформаційні потоки. **Цілі навчання:** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері технічного захисту інформації. **Теоретичний зміст предметної області:** поєднання фундаментальних основ математики і фізики, синергетики з прикладними аспектами fuzzy – технологій, системного аналізу, моделювання складних систем, задач оптимізації, теорії випадкових процесів, включаючи теорію ризиків, захисту інформації криптографічними та технічними засобами, та інших галузевих підходів, які використовуються в проблематиці захисту інформації. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформації та інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформації. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення,

	автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту інформації у автоматизованих та інформаційних системах. Комплекси та пристрої захисту мовної інформації, захисту інформації від витоку через побічні електромагнітні випромінювання та наведення. Обладнання для пошуку та локалізації закладних пристроїв прихованого зняття інформації. Методи і моделі теорії управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітня-професійна програма носить прикладний характер, спрямована на забезпечення потреб ринку праці і яка є базовою для мобільної адаптації при змінах, які постійно відбуваються в IT галузі.
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта та професійна підготовка в галузі F – «Інформаційні технології» за спеціальністю F5 – «Кібербезпека та захист інформації». Акцент на впровадженні інноваційних методів та технологій в процесі технічного захисту інформації на об'єктах інформаційної діяльності. *Ключові слова*: СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АВТОМАТИЗАЦІЯ ТА ОБРОБКА ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ
Особливості програми	Програма реалізується науковими групами та передбачає застосування широкого кола загальнонаукових і спеціальних аналітичних методів, принципів і прийомів наукових досліджень, з врахуванням сучасного світового досвіду в сфері технічного захисту інформації. Передбачено проведення лекційних курсів, семінарських та практичних занять, тренінгів, з залученням фахівців з захисту інформації з обмеженим доступом та інформаційної безпеки, а також самостійної науково-дослідної роботи. ***В програму впроваджені результати проекту Європейського союзу Tempus №544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR «Освіта експертів наступного покоління в галузі кібербезпеки: нова програма магістерської програми ЄС».***

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою технічні системи інформаційного та кібернетичного захисту (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010: **Основна :** **2149.2** – Професіонал із організації захисту інформації з обмеженим доступом **2310.2** – Викладач закладу вищої освіти **Допоміжна**: **2149.2** – Професіонал із організації інформаційної безпеки **3439** – Фахівець із організації захисту інформації з обмеженим доступом
Академічні права випускників	Можливість продовжити освіту за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі дорослої освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання і викладання. Викладання проводиться державною мовою. Іноземною мовою (англійською) проводиться викладання окремих дисциплін, які формують професійні компетентності. Викладання спрямовано на засвоєння знань, умінь і навичок для подальшого застосування у практиці, яке доповнюється практичними складовими компаніями партнерами. Основними способами передачі змісту освітньої програми є проведення лекцій, практичних, лабораторних і індивідуальних занять, консультацій, розв'язання ситуативних завдань, тестування, презентацій, змістовні кейси від партнерів кафедри науково-дослідна, науково-педагогічна переддипломна практики
Оцінювання	Види контролю: вхідний, поточний, рубіжний (модульний, тематичний) та підсумковий контроль. Оцінювання сформованих компетенцій проводиться під час контрольних заходів, які передбачені цією освітньою програмою та зазначені у навчальному плані. Критерії оцінювання знань, умінь та навичок здобувачів вищої освіти розроблені у відповідності до чинного

	законодавства та затверджені у «Положенні про організацію освітнього процесу у Державному університеті телекомунікацій». Також, з метою отримання додаткових балів в межах дисциплін зараховуються здобуті студентами сертифікати відомих компаній за тематикою дисциплін.
6- Програмні компетенції	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/ або інноваційного характеру у сфері інформаційного та кібернетичного захисту та/або кібербезпеки.
Загальні компетентності (КЗ)	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). КЗ6. Вміння визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ7. Вміння виявляти, ставити та вирішувати проблеми. КЗ8. Вміння розробляти математичні моделі завдань забезпечення інформаційної безпеки та захисту інформації. КЗ9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. КЗ10. Здатність застосовувати кращі практики у професійній діяльності. КЗ11. Здатність проявляти толерантність та повагу до культурної різноманітності.

Фахові компетентності спеціальності (КФ)	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на

	об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. КФ11. Здатність створювати методики ліцензування, атестації та сертифікації у сфері захисту інформації на об'єктах інформаційної діяльності. КФ12. Здатність розробляти технічну документацію для проведення тестування, налагоджування та допоміжних заходів щодо функціонування та експлуатації систем захисту інформації на об'єктах інформаційної діяльності.
7 – Програмні результати навчання	
	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

	РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

	РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень

	щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики. РН25. Розділяти складові, які відносяться до інформаційної безпеки та захисту інформації на об'єктах інформаційної діяльності. РН26. Створювати систему допуску учасників інформаційної діяльності з обмеженим допуском у відповідності з поточною політикою інформаційного та кібернетичного захисту і з урахуванням чинного законодавства. РН27. Організовувати гнучку адаптацію пропускної системи на підприємстві або організації з урахуванням поточних змін, пов'язаних з розвитком інформаційних технологій. РН28. Виявляти пристрої несанкціонованого зняття інформації на об'єктах інформаційної діяльності.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, залучені до реалізації освітньої складової освітньо-професійної програми є штатними співробітниками Державного університету телекомунікацій, мають підтверджений рівень наукової і професійної активності. Група забезпечення спеціальності F5 Кібербезпека та захист інформації, сформована з числа науково-педагогічних працівників Державного університету інформаційно-комунікаційних технологій. Кількісний та якісний склад групи відповідають Ліцензійним вимогам
Матеріально-технічне забезпечення	Для проведення практичних та лабораторних занять з метою формування спеціальних компетентностей зі спеціальності F5 Кібербезпека та захист інформації спеціалізації Технічні системи інформаційного та кібернетичного захисту використовуються спеціалізовані лабораторії університету, які оснащені сучасними комп’ютерами, програмно-апаратними комплексами та спеціалізованим обладнанням. НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАСОБІВ КОНТРОЛЮ

	ДОСТУПУ – забезпечує проведення практичних занять з питань контролю та управління доступом, використання автономних біометричних терміналів, мережевих контролерів, програмно-апаратних комплексів систем відеоспостереження HikVision та Ajax. НАВЧАЛЬНА ЛАБОРАТОРІЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «РІАС» – забезпечує проведення практичних занять з питань технічного захисту конфіденційної інформації на об'єктах інформаційної діяльності від витоку акустичним, віброакустичним та електромагнітним каналами з використанням широкосмугових генераторів акустичного та електромагнітного шуму, забезпечення вивчення порядку застосування пошукового програмно-апаратного комплексу DigiSkan EX; методів виявлення випромінювань за допомогою індикаторів поля типу PROTEKT; порядку застосування скануючих приймачів AR 8200, IC-R5, IC-R2500 та локатора нелінійностей NR-900 EM.
Інформаційне та навчально-методичне забезпечення	Інформація про освітню програму, її освітні компоненти та вимоги до осіб, які можуть здобувати вищу освіту за цією програмою розміщена на офіційному сайті Державного університету інформаційно-комунікаційних технологій. Усі освітні компоненти освітньої програми забезпечені навчально-методичними матеріалами, є у вільному доступі у якості ресурсів бібліотеки, електронної бібліотеки університету та системи дистанційного навчання Moodle
9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між ДУІКТ та вищими навчальними закладами України забезпечує національну кредитну мобільність
Міжнародна кредитна мобільність	Зміст навчання відповідає світовим освітнім стандартам, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці
Навчання іноземних здобувачів вищої освіти	Дозволяє можливість навчання іноземним громадянам

2. Перелік компонент освітньо-професійної / наукової програми та їх логічна послідовність

2.1. Зміст підготовки за освітньою програмою компетентності та результатами навчання

№ п.п.	Дисципліна	Код н/д	Компетентність	Результат навчання
Цикл дисциплін загальної підготовки				
1.	Захист професійної діяльності в галузі	ОК1	К31, К34, К35, К36	РН2, РН17
2.	Педагогіка та психологія у вищій школі	ОК2	К33, К34, К35, К36, К37, К38, К39, К310, К311, КФ10	РН2, РН17, РН18
3.	Організація проведення наукових досліджень	ОК3	К31, К32, К34, К35, К37, К38, К39, К310, КФ3	РН3, РН17, РН19, РН20, РН23, РН24
4.	Науково-технічний переклад	ОК4	К31, К32, К34, К35, КФ2	РН1, РН2, РН17, РН20, РН23
Цикл дисциплін професійної підготовки				
1.	Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	ОК5	К31, К32, К34, К35, КФ2, КФ3, КФ8, КФ11, КФ12	РН1,РН3, РН7, РН10, РН13, РН16, РН19, РН20, РН24, РН26, РН28
2.	Стандарти кібербезпеки та захисту конфіденційної інформації	ОК6	К31, К33, К39, КФ2, КФ6, КФ9, КФ11, КФ12	РН1,РН7, РН8, РН14, РН17, РН26, РН27
3.	Технологія створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності	ОК7	К31, К32, К33, К34, КФ1, КФ2, КФ3, КФ4, КФ5, КФ6, КФ7, КФ8, КФ9, КФ11, КФ12	РН1, РН2, РН3, РН4, РН5, РН6, РН7, РН8, РН10, РН11, РН12, РН13, РН15, РН19, РН21, РН22, РН26, РН27, РН28
4.	Теорія захисту інформаційних ресурсів обмеженого доступу	ОК8	К31, К34, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10, КФ12	РН2, РН3, РН4, РН5, РН6, РН7, РН8, РН9, РН10, РН11, РН12, РН13, РН15, РН16, РН17, РН20, РН22, РН25
5.	Радіомоніторинг і радіопротидія на об'єктах інформаційної діяльності	ОК9	К31, К32, К33, К34, КФ1, КФ3, КФ5, КФ6, КФ7, КФ9, КФ11	РН3, РН4, РН7, РН8, РН11, РН15, РН18, РН22, РН25

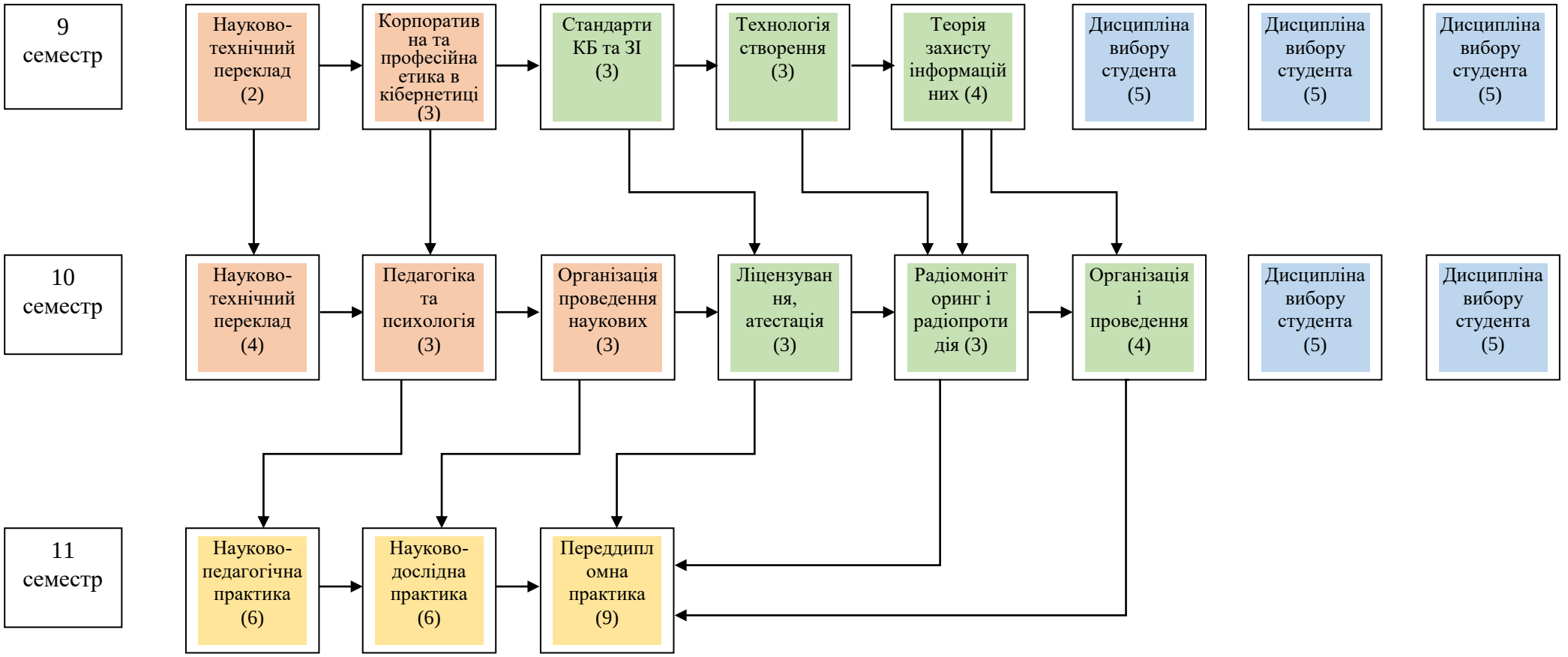
6.	Організація і проведення спеціальних досліджень на об'єкті інформаційної діяльності	ОК19	К31, К32, К33, К34, КФ2, КФ3, КФ6, КФ11	РН7, РН8, РН10, РН11, РН12, РН14, РН15, РН16, РН18, РН20, РН28
7.	Науково-педагогічна практика	ОК11	К31, К34, К36, К37, К38, К39, К310, К311, КФ10	РН1, РН2, РН15, РН17, РН18
8.	Науково-дослідна практика	ОК12	К31, К32, К33, К34, КФ1, КФ2, КФ3, КФ6, КФ7, КФ8	РН3, РН4, РН5, РН8, РН11, РН12, РН13, РН17, РН19, РН20, РН21, РН22, РН23
9.	Переддипломна практика	ОК13	К31, К32, К33, К34, КФ1, КФ2, КФ6, КФ7, КФ8	РН3, РН4, РН5, РН8, РН10, РН11, РН12, РН13, РН17, РН19, РН20, РН22, РН23
10.	Підготовка кваліфікаційної роботи, підсумкова атестація	ОК14	К31, К32, К33, К34, КФ1, КФ2, КФ3, КФ6, КФ7, КФ9	РН3, РН4, РН5, РН8, РН10, РН11, РН12, РН13, РН17, РН19, РН20, РН21, РН22, РН23
Дисципліни вільного вибору студента				
1.	Дисципліни вільного вибору студента			
2.	Дисципліни вільного вибору студента			
3.	Дисципліни вільного вибору студента			
4.	Дисципліни вільного вибору студента			
5.	Дисципліни вільного вибору студента			

2.2. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
Цикл загальної підготовки			
ОК1	Корпоративна та професійна етика в кібернетиці	3	Іспит
ОК2	Педагогіка та психологія у вищій школі	3	Залік
ОК3	Організація проведення наукових досліджень	3	Залік
ОК4	Науково-технічний переклад	6	Залік, Іспит

Цикл професійної та практичної підготовки			
ОК5	Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	3	Залік
ОК6	Автоматизація обробки інформації з обмеженим доступом	3	Залік
ОК7	Технологія створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності	3	Іспит
ОК8	Теорія захисту інформаційних ресурсів обмеженого доступу	4	Іспит
ОК9	Радіомоніторинг і радіопротидія на об'єктах інформаційної діяльності	3	Залік
ОК10	Організація і проведення спеціальних досліджень на об'єкті інформаційної діяльності	4	Іспит
ОК11	Науково-педагогічна практика	6	Залік
ОК12	Науково-дослідна практика	6	Залік
ОК13	Переддипломна практика	9	Залік
ОК14	Підготовка кваліфікаційної роботи, підсумкова атестація	9	
Загальний обсяг обов'язкових компонент:		**65**	
Вибіркові компоненти ОП			
ВК1	Дисципліни вільного вибору студента	5	Залік
ВК1	Дисципліни вільного вибору студента	5	Залік
ВК1	Дисципліни вільного вибору студента	5	Залік
ВК1	Дисципліни вільного вибору студента	5	Залік
ВК1	Дисципліни вільного вибору студента	5	Залік
Загальний обсяг вибіркових компонент:		**25**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

2.3. Структурно-логічна схема ОП



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки та технічного захисту інформації передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації згідно «Положення про запобігання академічному плагіату у Державному університеті інформаційно-комунікаційних технологій» Атестація здійснюється відкрито і гласно.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14
КЗ 1	•		•	•	•	•	•	•	•	•	•	•	•	•
КЗ 2			•	•	•		•		•	•		•	•	•
КЗ 3		•				•	•		•	•		•	•	•
КЗ 4	•	•	•	•			•	•	•	•	•	•	•	•
КЗ 5	•	•	•	•										
КЗ 6	•	•									•			
КЗ 7		•	•								•			
КЗ 8		•	•								•			
КЗ 9		•	•			•					•			
КЗ 10		•	•								•			
КЗ 11		•									•			
КФ 1						•	•	•	•			•	•	•
КФ 2				•	•	•	•	•		•		•	•	•
КФ 3			•		•		•	•	•	•		•		•
КФ 4					•		•							
КФ 5							•	•	•					
КФ 6						•	•	•	•	•		•	•	•
КФ 7							•	•	•			•	•	•
КФ 8					•		•	•				•	•	
КФ 9						•	•	•	•					•
КФ 10		•						•			•			
КФ 11						•	•		•	•				
КФ 12						•	•	•						

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14
РН1				•	•	•	•				•			
РН2	•	•		•			•	•			•			
РН3			•		•		•	•	•			•	•	•
РН4							•	•	•			•	•	•
РН5							•	•				•	•	•
РН6							•	•						
РН7					•	•	•	•	•	•				
РН8							•	•	•	•		•	•	•
РН9								•						
РН10					•		•	•		•			•	•
РН11							•	•	•	•		•	•	•
РН12							•	•		•		•	•	•
РН13					•	•	•	•				•	•	•
РН14						•				•				
РН15							•	•	•	•	•			
РН16					•			•		•				
РН17	•	•	•	•		•		•			•	•	•	•
РН18		•							•	•	•			
РН19			•		•		•					•	•	•
РН20			•	•	•			•		•		•	•	•
РН21							•					•		•
РН22							•	•	•			•	•	•
РН23			•	•								•	•	•
РН24			•		•									
РН25								•	•					
РН26					•	•	•							
РН27						•	•							
РН28					•		•			•				

Гарант освітньої програми
Завідувач кафедри Технічних систем кіберзахисту
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій
доктор технічних наук, професор

Олександр ТУРОВСЬКИЙ