МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ОСВІТНЬО-НАУКОВА ПРОГРАМА

КІБЕРБЕЗПЕКА

третього (освітньо-наукового) рівня вищої освіти
(оновлена)

Спеціальність: 125 Кібербезпека та захист інформації

Галузь знань: 12 Інформаційні технології

Кваліфікація: Доктор філософії з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Протокол № 10 від 01 квітня 2024 р.
Наказ № 64 від 01 квітня 2024 р.

Ректор _____ Володимир ТОЛУБКО

Освітня програма вводиться в дію з 01 вересня 2024 р.

Київ-2024

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬОЇ ПРОГРАМИ
ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

спеціальність	125 Кібербезпека та захист інформації
галузь знань	12 Інформаційні технології
рівень вищої освіти	третій (освітньо-науковий)
кваліфікація	доктор філософії з кібербезпеки та захисту інформації

1. Проректор з навчально-виховної роботи Вадим ВЛАСЕНКО
2. Проректор з навчально-виховної та наукової роботи Любов БЕРКМАН
3. Директор Навчально-методичного центру Ірина СРІБНА
4. Вчена рада Навчально-наукового інституту Захисту інформації

Протокол № 8 від 18 березня 2024 р.

Голова Вченої Ради ННІЗІ Віталій САВЧЕНКО

5. Кафедра Інформаційної та кібернетичної безпеки

Протокол № 8 від 05 березня 2024 р.

Завідувач кафедри Інформаційної та кібернетичної безпеки Галина ГАЙДУР

Рецензії від зовнішніх стейкхолдерів (фірм-партнерів):

1. Товариство з обмеженою відповідальністю «СІТОН ГРУП».
2. Товариство з обмеженою відповідальністю «Смартс».
3. Товариство з обмеженою відповідальністю «Луч».

ПЕРЕДМОВА

Розроблено робочою групою складі:

Гарант освітньої програми –

Савченко Віталій Анатолійович – доктор технічних наук, професор, директор Навчально-наукового інституту захисту інформації.

Члени робочої групи:

Гайдур Галина Іванівна – доктор технічних наук, професор, завідувач кафедри Інформаційної та кібернетичної безпеки.

Кузнецов Олександр Олександрович – доктор технічних наук, професор, професор кафедри Інформаційної та кібернетичної безпеки.

Ахрамович Володимир Миколайович – доктор технічних наук, професор, професор кафедри Систем інформаційного та кібернетичного захисту.

Марченко Віталій Вікторович – доктор філософії, доцент кафедри Інформаційної та кібернетичної безпеки.

Запорожченко Михайло Михайлович – аспірант кафедри Управління інформаційною та кібернетичною безпекою.

Приньов Сергій Миколайович – т.в.о. директора ТОВ «СІТОН ГРУП».

ВІДОМОСТІ ПРО ПЕРЕГЛЯД ОСВІТНЬОЇ ПРОГРАМИ

Освітньо-наукова програма переглянута та оновлена у зв'язку зі зміною назви Університету та у відповідності до:

- Закону України від 16.12.2020 № 1089-IX «Про електронні комунікації»;
- постанови Кабінету Міністрів України від 16.12.2022 № 1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»;
- рекомендацій акредитаційних комісій Університету,
- пропозицій роботодавців;
- побажань здобувачів вищої освіти.

1. **Профіль освітньо-наукової програми**

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний університет інформаційно-комунікаційних технологій, Навчально-науковий інститут захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Доктор філософії Освітня кваліфікація – Доктор філософії з кібербезпеки та захисту інформації
Офіційна назва освітньо-наукової програми	Освітньо-наукова програма «Кібербезпека»
Тип диплому та обсяг освітньо-наукової програми	Диплом доктора філософії, одиничний Обсяг освітньої програми - 60 кредитів ЄКТС; термін навчання 1 рік денної форми навчання та 1 рік заочної форми навчання
Наявність акредитації	Умовна акредитація
Цикл/рівень	НРК України – 8 рівень/ доктор філософії, QF-EHEA – третій цикл, EQF-LLL – 8 рівень
Передумови	наявність освітнього ступеня «магістр» або освітньо-кваліфікаційного рівня «спеціаліст» за спеціальністю 125 Кібербезпека та захист інформації (дозволяється вступ на ОНП з інших галузей знань за умови складання додаткового іспиту за спеціальністю за спеціальністю 125 Кібербезпека та захист інформації
Мова(и) викладання	українська, англійська
Термін дії освітньо-наукової програми	Програма впроваджена вперше з 01.09.2016 року і діє до затвердження державного стандарту
Інтернет - адреса постійного розміщення опису освітньо-наукової програми	http://www.dut.edu.ua/ua/1822-osvitno-profesiyni-programi-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

2 – Мета освітньо-наукової програми	
Здобуття теоретичних знань, умінь, навичок та інших компетентностей із захисту інформації та організації інформаційної безпеки на об'єктах інформаційної діяльності, достатніх для продукування нових ідей, розв'язання комплексних проблем у галузі професійної та/або дослідницько-інноваційної діяльності, оволодіння методологією наукової та педагогічної діяльності, а також проведення власного наукового дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.	
3 – Характеристика освітньо-наукової програми	
Предметна область, напрям (галузь знань, спеціальність)	*Галузь знань*: 12 Інформаційні технології *Спеціальність*: 125 Кібербезпека та захист інформації *Об'єкти професійної діяльності*: – об'єкти інформатизації, включаючи комп'ютерні, інформаційні, інформаційно-аналітичні системи, мережі електронних комунікацій, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. *Цілі навчання*: підготовка науковців, здатних розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики з питань 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; – сучасного програмно-апаратного забезпечення

	інформаційно-комунікаційних технологій. *Методи, методики та технології*: загальнонаукові методи пізнання та дослідницької діяльності; методи математичного аналізу, моделювання та синтезу систем і об'єктів; методики і технології визначення та аналізу ризиків інформаційної і кібербезпеки державних та приватних установ; методи, моделі та засоби кіберзахисту інформації; інформаційно-комунікаційні технології презентації результатів досліджень; методи та методики викладацької діяльності вищої школи. *Інструменти та обладнання*: засоби, прилади та комплекси для моделювання об'єктів та систем; програмні, апаратні та програмно-апаратні комплекси, що використовуються для вирішення задач інформаційної та кібербезпеки; комп'ютеризовані системи у навчальній та викладацький діяльності.
Орієнтація освітньо-наукової програми	Освітньо-наукова. 100% обсягу освітньо-наукової програми спрямовано на забезпечення загальних та спеціальних (фахових компетентностей за спеціальністю 125 Кібербезпека та захист інформації). Програма носить науково-прикладний характер, спрямована на забезпечення потреб ринку праці у сфері дослідження та вирішення наукових проблем щодо захисту інформації, організації та забезпечення інформаційної та кібербезпеки в мережах електронних комунікацій та на об'єктах інформаційної діяльності.
Основний фокус освітньо-наукової програми	Дослідження в області науки та практики захисту інформації, організації та забезпечення кібербезпеки інформаційно-комунікаційних систем, безпеки на об'єктах інформаційної діяльності. Ключові слова: ІНФОРМАЦІЯ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ЗАХИЩЕНІСТЬ, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ.
Особливості програми	**Стиль навчання:** поєднання репродуктивного та творчого стилів навчання як взаємодоповнюючих з домінуючим творчим компонентом; емоційно-ціннісний стиль навчання з поєднанням емоційно-імпровізаційного та емоційно-методичного стилів; проблемно-орієнтовані лекційні курси, семінари, групові та індивідуальні консультації, самопідготовка у бібліотеці та мережі Інтернет. **Методика навчання:** узгодження декількох навчальних технологій –

	інформаційної, моделюючої, розвивальної та активізуючої технологій, технології виробничого, випереджаючого та дистанційного навчання; інтерактивне співробітництво з науковим керівником, колегами із наукової групи та науково-педагогічними працівниками університету. **Організація навчального процесу:** формування і дотримання дослідницького портфоліо.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Доктор філософії з кібербезпеки та захисту інформації здатен обіймати посади в дослідницьких групах в університетах та наукових установах інформаційно-комунікаційної галузі (наукові дослідження і сфера управління), у промисловості та комерції. Самостійне працевлаштування. Доктор філософії з кібербезпеки (випускник) здатний виконувати професійні роботи за Державним класифікатором професій ДК 003: 2010: **Основна:** 2131.1 Науковий співробітник (обчислювальні системи) **Додаткова:** 2139.1 Науковий співробітник (галузь обчислень) 2144.1 Науковий співробітник (електроніка, комунікації) 2310.2 Викладач вищого навчального закладу 2310.1 Доцент
Подальше навчання	Навчання впродовж життя для вдосконалення у науковій та інших діяльностях (наприклад, освітня діяльність). Отримання наукового ступеня доктора наук (за наявності диплому доктора філософії) за цією ж галуззю знань або суміжною (що узгоджується з отриманим дипломом доктора філософії).
5 – Викладання та оцінювання	
Викладання та навчання	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 на практиці. Основними способами передачі змісту освітньо-наукової програми є проведення лекцій, практичних, лабораторних та індивідуальних занять, консультацій, розв'язання ситуативних завдань, тестування, презентацій, педагогічна практика.

Оцінювання	Усні та письмові екзамени, заліки, наукові звіти із оцінюванням досягнутого, усні презентації, поточний контроль, публікації результатів досліджень. Написання та привселюдний захист наукових досягнень, виконаних у формі кваліфікаційної (дисертаційної) роботи.

	6- Програмні компетентності
Інтегральна компетентність	Здатність розв'язувати комплексні проблеми в галузі кібербезпеки, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.
Загальні компетентності (ЗК)	**ЗК-1. Уміння критичної самооцінки** – здатність визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним. **ЗК-2. Навички творчого спілкування** – здатність спілкуватися результативно в усній і письмовій формах з фахівцями та нефахівцями, здатність спілкуватися другою мовою. **ЗК-3. Знання інформаційних технологій** – здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах. **ЗК-4. Навички керування проектами** – здатність демонструвати своєчасність та спланованість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проектами. **ЗК-5. Уміння підтримати інших** – здатність допомагати через викладання, наставництво та наочні приклади (демонстрацію). **ЗК-6. Уміння працювати етично** – здатність визначати, поважати та керувати етичними, культурними та іншими питаннями, пов'язаними з наявністю тих чи інших відмінностей. **ЗК-7. Навички підприємництва** – здатність визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт. **ЗК-8. Уміння командної роботи** – знання про стимули та бар'єри в ефективній командній роботі, вміння виявляти, ставити та вирішувати проблеми.
Фахові компетентності (ФК)	**ФК-1. Інтегративна компетентність** – здатність до інтеграції знань, умінь і навичок та їх ефективного використання в умовах швидкої адаптації організацій

	до вимог зовнішнього середовищ, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської та інноваційної діяльності в інформаційній та безпековій сфері тощо. **ФК-2. Соціально-психологічна компетентність** (емоційні, перцептивні, концептуальні, поведінкові) – здатність особистості орієнтуватися у різних життєвих ситуаціях, ефективно працювати в умовах ринкової економіки; уміння реалізувати стратегії і плани; здатність до розуміння поведінки людей, мотивації та організації їх спільної діяльності тощо. **ФК-3. Організаційно-комунікативна компетентність** (у специфічних сферах управлінської діяльності) – здатність до лідерства та новаторської діяльності, до формування високого рівня комунікативної культури; здатність переконувати оточуючих, стверджувати свою позицію; володіння державною мовою, грамотним усним та писемним діловим мовленням, ораторським мистецтвом, професійним етикетом, а також навичками публічної презентації результатів роботи, вміннями обирати відповідні форми і методи презентації; володіння іноземними мовами, уміння правильно розмовляти та писати різними комунікативними стилями, а саме неофіційним, офіційним та науковим тощо. **ФК-4. Професійна компетентність** – стан теоретичної та практичної підготовленості, що забезпечує ефективність вирішення професійних проблем і типових професійних завдань; стан володіння інформаційними технологіями та технологіями захисту інформації; здатність до удосконалення та впровадження у практику інновацій у сфері інформаційної та кібербезпеки; ступінь використання наукової літератури та інших джерел інформації для реалізації інноваційних технологій; здатність до здійснення ефективного пошуку та структурування інформації, до кваліфікованої роботи з різними ІР тощо. **ФК-5. Загальнонаукова компетентність** – здатність до накопичення професійних вмінь та навичок (діагностування й інтерпретування ситуацій, планування та здійснення наукових досліджень, викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційних технологій та захисту інформації); здатність до генерування нових знань з теорії захисту інформації та інформаційної

	безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; здатність до застосування нових знань у професійній діяльності (проектній, винахідницькій та раціоналізаторській роботі) тощо. **ФК-6. Політехнічна компетентність** – знання загальних (методологічних, історичних, економічних, ергономічних тощо) питань безпекової сфери, принципів дії і будови основних функціональних органів інформаційних систем; здатність до оволодіння спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та без пековими технологіями; здатність до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації. **ФК-7. Інженерна компетентність** – здатність до виробничо-технологічної діяльності (розробки та впровадження інноваційних технологій інформаційної безпеки, вибору технології ІБ, устаткування та засобів, використання інформаційних технологій; розробки програм і методик випробувань систем інформаційної та кібербезпеки); здатність до організаційно-управлінської діяльності (організації процесу створення та надання інфокомунікаційних послуг); здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо. **ФК-8. Ділова компетентність** – здатність і готовність здійснювати ефективну професійну діяльність у відповідній галузі, надавати інфокомунікаційні послуги та послуги безпеки; здатність до планування й реалізації заходів із захисту інформації в ІКС, створення та забезпечення функціонування систем інформаційної та кібербезпеки; здатність до формування правильних висновків, оперативного приймання та реалізації нестандартних рішень тощо.
7 – Програмні результати навчання	
Програмні результати навчання (ПРН)	**ПРН-1. Уміти** формувати і аргументовано відстоювати власну позицію з різних проблем філософії науки та методології наукового пізнання. **ПРН-2. Уміти** визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним.

	ПРН-3. Уміти вести дискусії і полеміки, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовою. **ПРН-4. Уміти читати** оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію. **ПРН-5. Уміти розробляти** логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень. **ПРН-6. Уміти здійснювати** бібліографічний пошук і відбір літературних джерел, складати їх бібліографічний опис. **ПРН-7. Уміти** моделювати структуру наукового дослідження, формулювати мету, об'єкт, предмет та наукові задачі, упорядковувати та систематизувати результати дослідження, обґрунтовувати їх достовірність та проводити їх апробацію. **ПРН-8. Уміти обґрунтовувати** та формулювати висновки щодо проведених наукових досліджень та рекомендації щодо їх наукового і практичного використання. **ПРН-9. Володіти вмінням** робити наукові доповіді щодо захисту результатів дослідження, аргументувати і захищати теоретичну позицію на основі емпіричної роботи. **ПРН-10. Уміти узагальнювати** і критично оцінювати результати, отримані вітчизняними і зарубіжними дослідниками. **ПРН-11. Уміти характеризувати** основні елементи системи та змісту вищої освіти в Україні, приймати рішення щодо критеріїв якості навчання та діагностики знань. **ПРН-12. Уміти визначати** основні параметри інформаційних ресурсів наукового дослідження (навчального процесу), планувати структуру, зміст та процес організації його проведення (лекцій, практично-семінарських занять). **ПРН-13. Уміти** виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією. **ПРН-14. Володіти навиками** роботи із

	спеціалізованими системами криптохзахисту та криптоаналізу, управляти змінами при роботі з існуючими системами криптографічного захисту. **ПРН-15. Уміти** орієнтуватися у сучасних концепціях і моделях, методах та засобах управління інцидентами інформаційної безпеки. **ПРН-16. Уміти** розробляти та проектувати нові, вдосконалювати існуючі системи управління інформаційною безпекою. **ПРН-17. Уміти** підтримувати комплексні системи інформаційної та кібербезпеки в стані, необхідному для вирішення завдань захисту інформації. **ПРН-18. Уміти** аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів. **ПРН-19. Уміти** проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів й застосовувати їх на практиці. **ПРН-20. Уміти** визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, уразливостях мережевих та Web-ресурсів. **ПРН-21. Уміти** аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. **ПРН-22. Уміти** розробляти та впроваджувати дослідницькі проекти в галузі знань «Інформаційні технології» спеціальності «Кібербезпека та захист інформації» для забезпечення безпеки мережевої інфраструктури. **ПРН-23. Бути здатним** генерувати нові знання з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки. **ПРН-24. Уміти** здійснювати науково-технічне супроводження заходів з формування і коригування програмних комплексів забезпечення безпеки та захисту інформації на об'єктах інформаційної діяльності. **ПРН-25. Уміти** визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної

	діяльності. **ПРН-26. Уміти** використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів. **ПРН-27. Бути здатним** оволодіти спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпековими технологіями. **ПРН-28. Бути здатним** до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації. **ПРН-29. Уміти розробляти та впроваджувати** раціональні технології інформаційної безпеки, програми і методики випробувань систем інформаційної та кібербезпеки **ПРН-30. Бути здатним** до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо. **ПРН-31. Уміти** проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності. **ПРН-32. Уміти** обґрунтовувати раціональні шляхи щодо захисту інформації на об'єктах інформаційної діяльності та інформації, що циркулює в ІТ системах та мережах.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Група забезпечення спеціальності 125 Кібербезпека та захист інформації сформована у відповідності до Ліцензійних вимог
Матеріально-технічне забезпечення	Теоретичні заняття проводяться в сучасних комп'ютерних класах та спеціалізованих лабораторіях, які оснащені спеціалізованими апаратно-програмними засобами. Для проведення досліджень, практичних та лабораторних занять з метою формування професійних компетентностей зі спеціальності 125 Кібербезпека та захист інформації використовуються 6 спеціалізованих лабораторій, які оснащенні сучасними комп'ютерами, програмно-апаратними комплексами та мультимедійними системами, а саме:

	НАВЧАЛЬНА ЛАБОРАТОРІЯ АКАДЕМІЧНИЙ ЦЕНТР КОМПЕТЕНЦІЙ IBM «КІБЕРПОЛІГОН» Лабораторія призначена для проведення практичних занять з використанням програмно-апаратних комплексів: IBM QRadar SIEM, IBM i2 Analyze Notebook Premium, Tenable Nessus Professional. Дозволяє відпрацьовувати навички роботи у Центрі забезпечення кібербезпеки (Security Operation Center) з використанням технологій моніторингу, виявлення, аналізу та реагування на кіберінциденти в корпоративних інформаційних системах. НАВЧАЛЬНА ЛАБОРАТОРІЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ НА БАЗІ ТЕХНОЛОГІЙ «АВТОР» Лабораторія використовується для вивчення спеціалізованих засобів криптографічного захисту на базі продуктів компанії АВТОР – партнера кафедри Інформаційної та кібернетичної безпеки. Крім того, у лабораторії проводяться тренінги з використанням криптографічних засобів захисту інформації в інформаційно-комунікаційних системах, віртуальних приватних мереж VPN, електронного цифрового підпису та інфраструктури відкритих ключів. Дозволяє вивчати та застосовувати програмно-технічний комплекс «Центр сертифікації ключів», засоби криптографічного захисту IP-шифратор CryptoIP-448, електронні ключі “SecureToken-337, програмний IP-шифратор «CryptoIP-VPN Client», безконтактні кард-рідери КР-382, USB. НАВЧАЛЬНА ЛАБОРАТОРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ CISCO Лабораторія призначена для вивчення технологій мережевої безпеки CISCO, проведення тренінгів з впровадження технології HoneyPot щодо протидії кібератакам зловмисників на корпоративні інформаційні системи та сертифікаційних курсів від партнера кафедри Інформаційної та кібернетичної безпеки – компанії CISCO: Introduction to Cybersecurity, CCNA Security, CCNA Cybersecurity Operations. НАВЧАЛЬНА ЛАБОРАТОРІЯ ЦЕНТР УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ (SECURITY OPERATION CENTER) Лабораторія призначена для проведення занять з питань аналізу, обробки та аудиту інформаційної безпеки за допомогою SIEM-систем та програмних сканерів типу Nessus та Kali Linux. Крім того, дозволяє

	вивчати методи управління ризиками на основі методологій CRAMM, OCTAVE та RiskWatch у відповідності до вимог міжнародних стандартів з інформаційної та кібербезпеки. Дозволяє працювати з програмними засобами підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority 1.0). НАВЧАЛЬНА ЛАБОРАТОРІЯ ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ «HIKVISION» – забезпечує проведення практичних занять та досліджень з питань контролю та управління доступом, використання автономних біометричних терміналів, мережевих контролерів, програмно-апаратного комплексу системи відеоспостереження HikVision. Обладнана автоматизованим комплексом відеоспо-стереження та охорони об'єктів інформаційної діяльності (Harbor), програмно-апаратними комплексами контролю доступу (HikVision), сповіщувачами інфрачервоними (SRP 600) та магніто-контактними (СОМК-10). Дозволяє вивчати питання застосування програмних комплексів захисту інформації («Лоза», «Гриф», «Рубіж»). НАВЧАЛЬНА ЛАБОРАТОРІЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «PIAC» – 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 (Piac-2ГС, ГШ 1000, «Беркут»). Крім того, у лабораторії досліджуються питання 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	Всі дисципліни навчального плану забезпечені інформаційними та навчально-методичними матеріалами, засобами системи дистанційного навчання Moodle у т.ч. доступом до електронної бібліотеки Державного університету інформаційно-комунікаційних технологій.

9 – Академічна мобільність	
Національна кредитна мобільність	Наявність двосторонніх договорів між Державним університетом інформаційно-комунікаційних технологій та закладами вищої освіти України забезпечує національну кредитну мобільність
Міжнародна кредитна мобільність	Зміст освітньо-наукової програми відповідає стандартам вищої освіти, що дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці
Навчання іноземних здобувачів вищої освіти	Передбачає навчання іноземців та осіб без громадянства після акредитації освітньо-наукової програми

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

2.1. Зміст підготовки за освітньо-науковою програмою, компетентності та результатами навчання

№ п.п.	Дисципліна	Шифр	Компетентність	Результат навчання
1. Цикл обов'язкових компонент освітньо-наукової програми				
1.1. Оволодіння загальнонауковими (філософськими) компетентностями, спрямованими на формування системного наукового світогляду, професійної етики та загального культурного кругозору				
1.	Філософські проблеми наукового пізнання	ОК11.1.1.01	ЗК1, ЗК5, ЗК6	ПРН1, ПРН2, ПРН3, ПРН9, ПРН10
2.	Основи наукових досліджень та організація науки	ОК11.1.1.02	ФК1, ФК5, ФК7	ПРН5, ПРН6, ПРН7, ПРН8, ПРН10, ПРН12, ПРН13, ПРН29
1.2. Набуття універсальних навичок дослідника				
3.	Патентознавство та авторське право	ОК11.1.2.01	ЗК4, ЗК7	ПРН3, ПРН6, ПРН10, ПРН24
4.	Сучасні методи викладання у вищій школі	ОК11.1.2.02	ФК2, ФК3	ПРН1, ПРН11, ПРН13, ПРН28
5.	Науково-педагогічна практика	ОК11.1.2.03	ФК3, ФК4, ФК8	ПРН1, ПРН9, ПРН11, ПРН28
1.3. Здобуття мовних компетентностей				
6.	Англійська мова наукового спрямування *	ОК11.1.3.01	ЗК2, ЗК3, ЗК8, ФК3	ПРН3, ПРН4, ПРН10, ПРН13
1.4. Здобуття глибинних знань зі спеціальності				
7.	Методологія наукових досліджень у кібербезпеці	ОК11.1.4.01	ФК3, ФК4, ФК5, ФК6, ФК7	ПРН14, ПРН18, ПРН19, ПРН20, ПРН22, ПРН23, ПРН26, ПРН27, ПРН30
8.	Теоретичні та практичні проблеми технічного захисту інформації	ОК11.1.4.02	ФК1, ФК4, ФК5, ФК6, ФК7	ПРН5, ПРН13, ПРН17, ПРН21, ПРН24, ПРН25, ПРН31, ПРН32
9.	Сучасні методи управління інформаційною та кібербезпекою	ОК11.1.4.03	ФК1, ФК2, ФК6, ФК7, ФК8	ПРН12, ПРН15, ПРН16, ПРН21, ПРН25, ПРН28, ПРН29, ПРН30
2. Цикл вибіркових компонент освітньо-наукової програми				
10.	*Дисципліна 1***			
11.	*Дисципліна 2***			
12.	*Дисципліна 3***			
13.	*Дисципліна 4***			
14.	*Дисципліна 5***			

** Дисципліна «Іноземна мова» для підготовки іноземців та осіб без громадянства замінюється на дисципліну «Українська мова як іноземна».*

*** Дисципліни вільного вибору обираються аспірантами самостійно на початку навчального року з Каталогу вибіркових освітніх компонентів, при цьому загальний обсяг таких дисциплін повинен складати 15 кредитів ЄКТС.*

2.2. Перелік компонент освітньо-наукової програми

Код н/д	Компоненти освітньо-наукової програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти освітньо-наукової програми			
ОК11.1.1.01	Філософські проблеми наукового пізнання	3	Залік
ОК11.1.1.02	Основи наукових досліджень та організація науки	3	Залік
ОК11.1.2.01	Патентознавство та авторське право	3	Залік
ОК11.1.2.02	Сучасні методи викладання у вищій школі	3	Залік
ОК11.1.2.03	Науково-педагогічна практика	6	Залік
ОК11.1.3.01	Англійська мова наукового спрямування *	15	Іспит
ОК11.1.4.01	Методологія наукових досліджень у кібербезпеці	4	Іспит
ОК11.1.4.02	Теоретичні та практичні проблеми технічного захисту інформації	4	Іспит
ОК11.1.4.03	Сучасні методи управління інформаційною та кібербезпекою	4	Іспит
Загальний обсяг обов'язкових компонент:		**45**	
Вибіркові компоненти освітньо-наукової програми			
	*Дисципліна 1***	15	Залік
	*Дисципліна 2***		Залік
	*Дисципліна 3***		Залік
	*Дисципліна 4***		Залік
	*Дисципліна 5***		Залік
Загальний обсяг вибіркових компонент:		**15**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ		**60**	

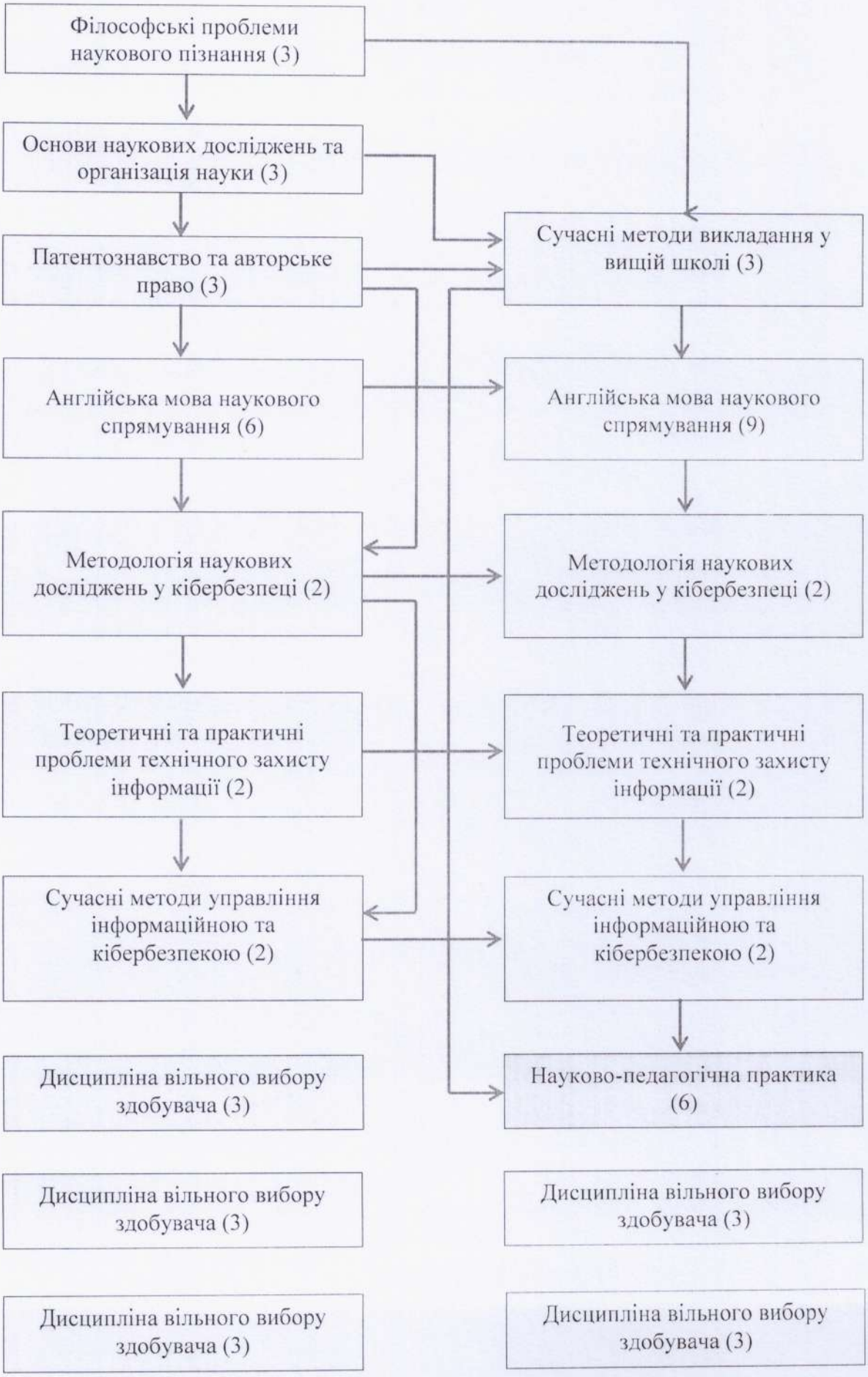
** Дисципліна «Іноземна мова» для підготовки іноземців та осіб без громадянства замінюється на дисципліну «Українська мова як іноземна».*

*** Дисципліни вільного вибору обираються аспірантами самостійно на початку навчального року з Каталогу вибіркових освітніх компонентів, при цьому загальний обсяг таких дисциплін повинен складати 15 кредитів ЄКТС.*

2.3. Структурно-логічна схема освітньо-наукової програми (частина 1)

Цикл	I курс				Всього	
	1 семестр		2 семестр		Кр.	%
Здобуття глибинних знань зі спеціальності	Методологія наукових досліджень у кібербезпеці	2	Методологія наукових досліджень у кібербезпеці	2		
	Теоретичні та практичні проблеми технічного захисту інформації	2	Теоретичні та практичні проблеми технічного захисту інформації	2		
	Сучасні методи управління інформаційною та кібербезпекою	2	Сучасні методи управління інформаційною та кібербезпекою	2		
	Всього	***6***	***Всього***	***6***	**12**	**20%**
Оволодіння загальнонауковими (філософськими) компетентностями	Філософські проблеми наукового пізнання	3				
	Основи наукових досліджень та організація науки	3				
	Всього	***6***	***Всього***	***0***	**6**	**10%**
Набуття універсальних навичок дослідника	Патентознавство та авторське право	3	Сучасні методи викладання у вищій школі	3		
			Науково-педагогічна практика	6		
	Всього	***3***	***Всього***	***9***	**12**	**20%**
Здобуття мовних компетентностей	Англійська мова наукового спрямування	6	Англійська мова наукового спрямування	9		
	Всього	***6***	***Всього***	***9***	**15**	**25%**
Цикл вибіркових компонент	*Дисципліна 1*	3	*Дисципліна 4*	3		
	Дисципліна 2	3	*Дисципліна 5*	3		
	Дисципліна 3	3				
	Всього	***9***	***Всього***	***6***	**15**	**25%**
	Всього за I курс	***30***		***30***	**60**	**100%**

Структурно-логічна схема освітньо-наукової програми (частина 2)



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація докторів філософії із кібербезпеки здійснюється у формі публічного захисту дисертаційної роботи на спеціалізованій вченій раді після успішного складання іспитів і заліків освітньої складової програми.
Вимоги до кваліфікаційної роботи	Дисертація на здобуття наукового ступеня є кваліфікаційною науковою працею, виконаною особисто здобувачем у вигляді спеціально підготовленого рукопису або опублікованої монографії. Підготовлена до захисту дисертація повинна містити висунуті здобувачем науково обґрунтовані теоретичні або експериментальні результати а також характеризуватися єдністю змісту і свідчити про особистий внесок здобувача в науку у галузі інформаційної та кібербезпеки. Робота має бути перевірена на плагіат відповідно до «Кодексу академічної доброчесності Державного університету інформаційно-комунікаційних технологій» та оприлюднена у репозитарії Університету.

4. Матриця відповідності програмних компетентностей компонентам освітньо-наукової програми

	ОК11.1.1.01	ОК11.1.1.02	ОК11.1.2.01	ОК11.1.2.02	ОК11.1.2.03	ОК11.1.3.01	ОК11.1.4.01	ОК11.1.4.02	ОК11.1.4.03
ЗК 1	•								
ЗК 2						•			
ЗК 3						•			
ЗК 4			•						
ЗК 5	•								
ЗК 6	•								
ЗК 7			•						
ЗК 8						•			
ФК 1		•						•	•
ФК 2				•					•
ФК 3				•	•	•	•		
ФК 4					•		•	•	
ФК 5		•					•	•	
ФК 6							•	•	•
ФК 7		•					•	•	•
ФК 8					•				•

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-наукової програми

	ОК11.1.1.01	ОК11.1.1.02	ОК11.1.2.01	ОК11.1.2.02	ОК11.1.2.03	ОК11.1.3.01	ОК11.1.4.01	ОК11.1.4.02	ОК11.1.4.03
ПРН 1	•			•	•				
ПРН 2	•								
ПРН 3	•		•			•			
ПРН 4						•			
ПРН 5		•						•	
ПРН 6		•	•						
ПРН 7		•							
ПРН 8		•							
ПРН 9	•				•				
ПРН 10	•	•	•			•			
ПРН 11				•	•				
ПРН 12		•							•
ПРН 13		•		•		•		•	
ПРН 14							•		
ПРН 15									•
ПРН 16									•
ПРН 17								•	
ПРН 18							•		
ПРН 19							•		
ПРН 20							•		
ПРН 21								•	•
ПРН 22							•		
ПРН 23							•		
ПРН 24			•					•	
ПРН 25								•	•
ПРН 26							•		
ПРН 27							•		
ПРН 28				•	•				•
ПРН 29		•							•
ПРН 30							•		•
ПРН 31								•	
ПРН 32								•	

Гарант освітньо-наукової програми
Директор Навчально-наукового інституту захисту інформації
Державного університету інформаційно-комунікаційних технологій
доктор технічних наук, професор **В.А. Савченко**

РЕЦЕНЗІЯ-ВІДГУК
на оновлену Освітньо-наукову програму «Кібербезпека»
підготовки докторів філософії третього (освітньо-
наукового) рівня вищої освіти за спеціальністю
125 Кібербезпека та захист інформації

Оновлена освітня програма «Кібербезпека» на третьому рівні підготовки докторів філософії в Державному університеті інформаційно-комунікаційних технологій спрямована на підготовку аспірантів з урахуванням поточних вимог. Основна мета – розвиток у сучасного спеціаліста здатності розв'язувати інноваційні наукові завдання. Оновлена програма враховує тенденції розвитку інформаційних технологій, стан безпеки критичних об'єктів державної інфраструктури та сучасні підходи до кібербезпеки та захисту інформації.

Програма зосереджена на трьох основних аспектах кібербезпеки та захисту інформації: мережевій безпеці, технічних системах захисту інформації та управлінні в цій сфері. Для досягнення цієї мети у програмі впроваджені три ключові дисципліни з фокусом на проблематику кожного напрямку, що сприяє розвитку у студентів навичок постановки завдань та пошуку їх рішень. Зміст цих дисциплін базується на огляді передових досягнень науки, сучасних методах вирішення проблем з використанням передових технологій, таких як хмарні обчислення, штучний інтелект та автоматизація технологічних процесів.

Позитивним аспектом оновленої освітньо-наукової програми є те, що вона розвиває не лише професійні, а й загальні наукові, дослідницькі та мовні компетенції, що сприяє інтеграції студентів у світове освітнє середовище.

Доступ до передової матеріально-технічної бази та кваліфікованих науково-педагогічних кадрів в Державному університеті інформаційно-комунікаційних технологій гарантує високий рівень знань, умінь та навичок у випускників. Аспіранти мають можливість користуватися спеціалізованими лабораторіями, класами та, за необхідності, матеріальною базою компаній-партнерів, серед яких є відомі світові лідери IT-індустрії, такі як IBM, Cisco, Hewlett Packard, Eset та інші.

Таким чином, науковий та методичний рівень Освітньо-наукової програми «Кібербезпека» за спеціальністю 125 Кібербезпека та захист інформації підтверджують здатність Державного університету інформаційно-комунікаційних технологій забезпечити високу якість підготовки фахівців освітньої кваліфікації «Доктор філософії з кібербезпеки та захисту інформації».

Генеральний директор ТОВ «Луч» Євген ЧЕМЕС

РЕЦЕНЗІЯ-ВІДГУК
на оновлену Освітньо-наукову програму «Кібербезпека»
третього (освітньо-наукового) рівня вищої освіти з
підготовки докторів філософії за спеціальністю
125 Кібербезпека та захист інформації

Розвиток інформаційних технологій в сучасному суспільстві стає ключовим фактором у всіх галузях діяльності. Організації та підприємства потребують значної кількості кваліфікованих ІТ-фахівців, зокрема тих, хто спеціалізується на кібербезпеці та захисті інформації, включаючи фахівців з науковим ступенем.

Освітньо-наукова програма "Кібербезпека" для підготовки докторів філософії, що розроблена в Державному університеті інформаційно-комунікаційних технологій, ґрунтується на сучасних світових наукових підходах. Ця програма становить логічне продовження навчання бакалаврів та магістрів університету. Вона була оновлена відповідно до поточних вимог на ринку праці у сфері Кібербезпеки та захисту інформації.

Основною особливістю цієї програми є включення трьох основних напрямків кібербезпеки та захисту інформації: безпека інформаційно-комунікаційних систем, технічний захист інформації та управління в сфері кібербезпеки. Програма розглядає ці напрямки з точки зору розв'язання проблем та методології їх вирішення. Кожен напрямок підтримується окремою дисципліною, яка призначена для навчання студентів знаходити раціональні рішення для сучасних практичних проблем, формулювати наукові завдання та розробляти методики їх вирішення.

Практична реалізація освітнього компонента цієї програми здійснюється на потужній навчально-технічній базі Державного університету інформаційно-комунікаційних технологій, яка включає в себе спеціалізовані лабораторії для дослідження окремих аспектів кібербезпеки та захисту інформації. Крім цього, освітньо-наукову програму забезпечують висококваліфіковані науково-педагогічні працівники, які мають великий досвід для її впровадження.

Науковий та методичний рівень освітньо-наукової програми "Кібербезпека", потужна навчально-технічна база і досвідчений колектив науково-педагогічних працівників Державного університету інформаційно-комунікаційних технологій підтверджують здатність університету ефективно підготовлювати фахівців з освітньою кваліфікацією "Доктор філософії з кібербезпеки та захисту інформації".

Директор ТОВ «Смартс» Едуард ГРІНБЕРГ

РЕЦЕНЗІЯ-ВІДГУК
на Освітньо-наукову програму «Кібербезпека» підготовки докторів філософії третього (освітньо-наукового) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації

У сучасному світі розвиток інформаційних технологій відіграє вирішальну роль у всіх сферах суспільства. Ефективне функціонування організацій та підприємств неможливе без значної кількості висококваліфікованих ІТ-фахівців, зокрема в галузі кібербезпеки та захисту інформації, серед яких особливу роль відіграють ті, хто має вчений ступінь.

Освітньо-наукова програма "Кібербезпека" для підготовки докторів філософії в Державному університеті інформаційно-комунікаційних технологій базується на сучасних світових наукових підходах. Підготовка аспірантів у цій програмі є послідовним кроком після навчання бакалаврів та магістрів. Програма була оновлена відповідно до сучасних вимог та зміни назви спеціальності.

Основною особливістю цієї програми є включення трьох основних напрямків кібербезпеки та захисту інформації: безпека інформаційно-комунікаційних систем, технічний захист інформації та управління в сфері кібербезпеки. Програма розглядає ці напрямки з точки зору вирішення проблем та методології їх вирішення. Кожен напрямок підтримується окремою дисципліною, яка має навчити студентів знаходити раціональні рішення для сучасних практичних проблем, формулювати наукові завдання та розробляти методики їх вирішення.

Практична реалізація освітнього компоненту цієї програми здійснюється на потужній навчально-технічній базі Державного університету інформаційно-комунікаційних технологій, яка включає спеціалізовані лабораторії для дослідження окремих аспектів кібербезпеки та захисту інформації. Крім цього, освітньо-наукову програму забезпечують висококваліфіковані науково-педагогічні працівники, які мають достатній досвід для її реалізації.

Науковий рівень Освітньо-наукової програми «Кібербезпека», потужна навчальна матеріально-технічна база та досвідчений колектив науково-педагогічних працівників Державного університету інформаційно-комунікаційних технологій підтверджують здатність університету якісно готувати фахівців з освітньою кваліфікацією «Доктор філософії кібербезпеки та захисту інформації».

Т.в.о. директора
ТОВ «СІТОН ГРУП» Сергій ПРИНЬОВ