459

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

«ЗАТВЕРДЖУЮ»
Ректор
_____ Л.В.Губерський
«__» _____ 2018 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

Рівень вищої освіти: перший

на здобуття освітнього ступеню: бакалавр
за спеціальністю 125 «Кібербезпека»
галузі знань 12 «Інформаційні технології»

Розглянуто та затверджено
на засіданні Вченої ради
від «25» червня 2018 р.
протокол № 12

Введено в дію наказом ректора від
«12» 02 2019 р. за № 144-32

Київ 2018 р.

ПЕРЕДМОВА

1.Внесено кафедрою кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Розроблено робочою групою у складі:

Прізвище, ім'я, по батькові керівника та членів проектної групи	Найме-нування посади (для суміс-ників– місце основної роботи, наймену-вання посади)	Найменування закладу, який закінчив викладач, (рік закінчення, спеціальність, кваліфікація згідно з документом про вищу освіту)	Науковий ступінь, шифр і найменування наукової спеціальності, тема дисертації, вчене звання, за якою кафедрою (спеціальністю) присвоєно	Стаж науково-педагогічної та/або наукової роботи	Інформація про наукову діяльність (основні публікації за напрямом, науково-дослідна робота, участь у конференціях і семінарах, робота з аспірантами та докторантами, керівництво науковою роботою студентів)	Відомості про підвищення кваліфікації викладача (найменування закладу, вид документа, тема, дата видачі)
Керівник проектної групи **Браіловський Микола Миколайович**	Доцент кафедри кібербезпеки та захисту інформації	*Закінчив*: Українська державна академія зв'язку ім. О.С. Попова в 1994 році диплом: КГ № 005170 від 13 червня 1994 р. *спеціальність* радіозв'язок радіомовлення та телебачення *кваліфікація спеціаліста*: інженер радіозв'язку радіомовлен-	Кандидат технічних наук, 05.13.21 – системизахистуінформації, Диплом ДК №020523, від 8. 10. 2003 р. тема дисертації: «Методи та засобизахистуінформації в каналах автоматизованих систем управління повітряним рухом»,	21,5 років	Загальна кількість робіт – 129; з них: **Наукові публікації** **Статті** 1. Браіловський М.М., Погребна Т.В., Пташок О.В. «Мережі VPN та проблеми їх захисту». Телекомунікаційні та інформаційні технології №1, Київ: ДУТ, 2014.-с.76-81. 2. Браіловський М.М., Погребна Т.В., Пташок О.В. «Основні вимоги до побудови та безпеки мереж наступного покоління». Телекомунікаційні та інформаційні технології №2, Київ: ДУТ, 2014.-с.41-49. 3. Браіловський М.М., Хорошко О.В. «Жизнестойкость систем защиты информационного пространства» Телекомунікаційні та інформаційні технології №4, Київ: ДУТ, 2014.-с.41-49. 4. Браиловский Н.Н., Иванченко Е.В., Хорошко В.А. «Диагностика систем защиты информационного пространства» Захист інформації. Спеціальний випуск 2014. – с.59-67. 5. Браиловский Н.Н., Зыбин С.В., Хорошко В.А. «Модели управления в системах обеспечения информационной безопасности государства» Інформатика та математичні методи в моделюванні. – Одеса. – ОНПУ, Т.4. – № 4. – 2014. – с.304-311. 6. Браиловский Н.Н., Хорошко В.А. «Оптимизация характеристик сложных систем по критерию живучести» Науковий журнал	підвищення кваліфікації (стажування) в Національна Академія державного управління при Президентові України, Інститут підвищення кваліфікації керівних кадрів, свідоцтво про підвищення кваліфікації 12 СПВ № 132384 від 16.10.2015 р.

		ня та телебачення	доцент кафедри засобів захисту інформації 02ДЦ № 002476 від 21.10.2004 р		«Інформаційна безпека» №1(13), №2(14) – Луганськ: видавництво СНУ ім. В.Даля, 2014. – с. 17-22 7. Браіловський М.М., Козелков С.В., Коршун Н.В. «Математична модель розповсюдження шкідливого програмного забезпечення на комутуючих пристроях інформаційних систем» Телекомунікаційні та інформаційні технології №2, Київ: ДУТ, 2016.-с.5-10. 8. Браіловський М.М., Козелков С.В., Коршун Н.В «Оптимізація вибору параметрів якості системи захисту інформації в каналах зв'язку». Зв'язок №3(121), 2016, Київ: ДУТ,-с.58-60. 9. Браіловський М.М., Толюпа С.В., Самохвалов Ю.Я.. Пасивно-активний метод супроводження повітряних цілей із штучно заниженою площею віддзеркалення Харьков: ХНУРЭ № 2, 2017. ст. 98-106. 10. Браіловський М.М Толюпа С.В.. Синергетичні методи оптимізації характеристик складних систем за критерієм живучості К.: Вісник Інженерної академії України №1, 2017.ст. 47-52 11. Браиловский Н.Н. Баранник В.В., Мусиенко А.П. Кластиризация блоков аэрофотоснимков в двухпризнаковом структурном пространстве на основе метода к-средних в системеобработкиинформации «Радиоэлектроника и информатика», Харьков: ХНУРЭ № 2, 2017. ст. 46-54. 12. С.В. Толюпа, М.М. Браіловський. Синергетичні методи оптимізації характеристик складних систем за критерієм живучості. Вісник інженерної академії України. №1. – 2017. с. 208 – 213. 13. Толюпа С.В., Самохвалов Ю.Я., Браиловський Н.Н. Пасивно-активний метод супроводження повітряних цілей зі штучно зниженою площею віддзеркалення. Радіоелектроніка і інформатика. ХНУРЕ. №1. 2017р. – с. 89-97. 14. Toliupa. S. V, Nakonechny. V. S, Brailovskyi. N. N, BuildingCyber-Security Systems of Information Networks Based on Intellectual Technologies // Scientific&practical cybersecurity journal (SPCSJ) №1. [Electronicjournal]. URL: http://journal.scsa.ge/issues/ 2017/09/432 **Конференції** 1. Браіловський М.М. Прогнозування рівня захищеності інформаційних ресурсів держави. Семінар при Вчені раді НАН України «Технічні засоби захисту інформації» на 2015 2. Браіловський М.М. «Шляхи підвищення захищеності мереж за рахунок збільшення функціональної стійкості» Наукові доповіді та тези учасників науково-технічної конференції 12-13 березня 2015 «Інформаційна безпека України», Київського національного університету ім.. Тараса Шевченка. – К.; 2015. Стр.86-87.	

					3. Браіловський М.М. «Напрямки забезпечення функціональної стійкості систем захисту сучасних телекомунікаційних систем» Матеріали міжнародної науково-технічної конференції Сучасні інформаційно-комунікаційні технології. Том IV Сучасні технології інформаційної безпеки 17-20 листопада 2015. – К.; ДУТ, 2015. – стр. 76-78. 4. Белоус И.Ю., Орленко В.С. «Методика создания жизнеспособных центров обработки данных» доповідей VIII міжнародної науково-практичної конференції «Проблеми та перспективи розвитку IT-індустії», 28-29 квітня 2016 р. – Х.: ХНЕУ імені Семена Кузнеця, 2016. – стр. 50-51. 5. Заіка Г.О., Браіловський М.М. Раціональність використання інформаційно-аналітичних систем як інструменту безпеки підприємства. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”: Збірник матеріалів доповідей та тез; м. Київ, 23-24 березня 2017 р.; Київський національний університет імені Тараса Шевченка / - К.: ВЦП «Київський університет», 2017. 86-88 ст. 6. Браіловський М.М. Методология создания индикатора кибербезопасности объекта “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”: Збірник матеріалів доповідей та тез; м. Київ, 23-24 березня 2017 р.; Київський національний університет імені Тараса Шевченка / - К.: ВЦП «Київський університет», 2017. 135-138 ст. 7. Браіловський М.М., Зибін С.В. Підходи до створення захищених віртуалізованих сховищ даних VI Міжнародна науково-практична конференція (I Міжнародний симпозіум) ПРАКТИЧНЕ ЗАСТОСУВАННЯ НЕЛІНІЙНИХ ДИНАМІЧНИХ СИСТЕМ В ІНФОКУМУНІКАЦІЯХ 9-11 листопада 2017 р. Чернівці, Україна ст. 66 8. Браіловський М.М., Зибін С.В Критерії захищеності інформації при оцінці ефективності СППР IV Міжнародна науково-практична конференція Інформаційні технології та взаємодії 8-10 листопада 2017 р. Київ, Україна ст. 213-214.	
Члени проектної групи **Оксіюк Олександр Глібович**	Завідувач кафедри кібербез-пеки та захисту інформа-ції	Військова ордена Леніна Червонознаме нна академія зв’язку ім. С.М. Будьонного,	Доктор технічних наук, 05.13.06 -Інформаційні технології;тема закрита. Диплом ДД № 000918	28 років	*Наукові статті:* 1. Оксіюк О.Г. Перспективи розвитку застосування інтелектуальних навчальних систем / Вялкова В.І.//Збірник наукових праць. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України. - Київ., 2013. - №64. – С.25-32 2. Оксіюк О.Г. Архітектура і етапи функціонування систем підтримки прийняття рішень/ Вялкова В.І., Міщенко В.О., Шелемін З.К.// Збірник наукових праць. Інститут проблем моделювання в	1.«CiscoNetworkingAcademy», УКРТЕЛЕКОМ, філія «Центр післядипломної освіти», 04.10.2013, CCNA Exploration: Accessing the WAN, сертифікат.

		1987 р., спеціальність - інженерна систем та засобів зв'язку, кваліфікація - офіцер-організатор експлуатації озброєння Диплом ПВ №566957 від 25.07.1987р.	від 17.05.2012р. Професор кафедри кібербезпеки та захисту інформації. Атестат професора 12 ПР №011090 від 15.12.2015р.		енергетиці ім. Г.Є. Пухова Національної академії наук України. Київ., 2013. - №65. - С. 54-60 3. Оксіюк О.Г. Анализ подходов к управлению скоростью передачи видеопотока / ДвухглавовД.Э. ,Твердохлеб В.В. //Сучасна спеціальна техніка. – Харків., 2014. – №2.- С.17-19 4. Оксіюк О.Г. Выбор технических средств распределенной системы поддержки принятия решений/ В.І. Вялкова //[Электронный ресурс] – электрон.текстов. дан. – Режим доступа: http://moit.vivt.ru/wp-content/uploads/2014/01/Vyalkova_3_13_1.pdf. –. 5. ОксіюкО.Г. «Conceptualapproachforknowledgemodellinginthesystemofdistancetraining»/S. Rajba, V.Vialkova, O. Pastuch.//ZeszytynaukowewyższejszkołyfinansówiprawawBielsku-Białej. – 2013, No4.-P.100-108. 6. Оксіюк О.Г. Анализ сетевых технологий на базе беспроводных сетей/Шестак Я.В.// Науковий збірник «Інформаційна безпека», Східноукраїнський національний університет ім. Володимира Даля №2 (14), 2014, с.175-185 7. Оксіюк О.Г. Спосіб підвищення завадостійкості каналів радіозв'язкудля мобільних мереж нового покоління / Сайко В.Г., Бреславський В.А., Лисенко Д.О.// «Зв`язок», № 4 – 2015., ДУТ м. Київ, – С. 52-57 8. ОксіюкО.Г. ChoiceofReasonableVariantofSygnalandCodeConstructionsforMultiraysRadioChannels/ТолюпаС.В., Лукова-ЧуйкоН.В.// 2015 SecondInternationalScientific-PracticalConferenceProblemsofInfocommunications. ScienceandTechnology. IEEE PIC S&T 2015 м. Харьків., С.269-271 9. Оксіюк О.Г. Аналіз современных методик и методов проведения оценки защищенности информационных систем/Шестак Я.В.// Наукові записки Українського науково-дослідного інституту зв'язку. М. Київ, №4(38).,с.17-23, 2015 10. Оксіюк О.Г. Особливості забезпечення захисту інформації в системах управління навчанням// Збірник наукових праць ВІКНУ імені Тараса Шевченка, м. Київ, №49. 2015р. С.208-213 11. Оксіюк О.Г. Модель оптимізації семантичної мережі/ Системи управління, навігації та зв'язку. м.Київ., ДУТ, №1, 2015р.,С.24-31 12. Оксіюк О.Г. Параметричний синтез експертних навчальних систем// Вісник інженерної академії України. м. Київ, №3. 2015р, С. 166-170	

					13. Оксіюк О.Г. Методика розрахунку часу затримки інформації в інформаційно-комунікаційних мережах// Вісник Черкаського державного технологічного університету. м. Черкаси, №3, 2015р., С. 34-42 *Наукові конференції:* 14. Прийняття рішень про розподіл інвестицій у захист інформації на основі результатів моніторингу інцидентів інформаційної безпеки/Матеріали Всеукраїнської науково-практичної конференції «В.М. Глушков – піонер кібернетики» - К.: Вид-во «Політехніка», 2014. – 206-208 15. Пошук оптимального рішення в задачах інформаційної безпеки із врахуванням дій нападу/Актуальні проблеми забезпечення інформаційної безпеки держави: Матеріали науково-технічної конференції: 18 грудня 2014 року. – Київ: ДУТ, С.112-113 16.Обнаружение компьютерных атак на основе анализа данных мониторинга несколькими способами/Інформаційна безпека України: Зб. Нук. Доп. науково-технічної конференції; м. Київ, 12-13 березня 2015 р. КНУ ім. Тараса Шевченка С.150-153 17. Розробка комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах/Перспективні напрями захисту інформації: матеріали першої всеукр. Наук.-пр. конференції, м. Одеса 7-9 вересня 2015р.:ОНАЗ, 2015. С.69-73	
Бабенко Тетяна Василівна	Професор кафедри кібербезпеки та захисту інформації	Дніпропетровський хіміко-технологічний інститут. Спеціальність «Хімічна технологія в'яжучих матеріалів» Кваліфікація: інженер-хімік технолог.1992р. Диплом РВ № 824317 від 17.06.1992р.	Доктор технічних наук, 05.13.07 – «Автоматизація процесів керування». Тема докторської дисертації: «Методи і моделі штучного інтелекту в АСУТП керамічного виробництва». Диплом ДД №007055	19 років	*Навчальні посібники, підручники, монографії:* 1. Бабенко Т.В., Гулак Г.М., Сушко С.О., Фомичова Л.Я. «Криптологія у прикладах, текстах і задачах» для студентів галузі знань 1701 "Інформаційна безпека" // Навчальний посібник. – Д.: Національний гірничий університет, 2013. – 318 с. (гриф МОН). 2. Бабенко Т.В., Корнєєв М.В, Кручінін О.В., Тимофєєв Д.С. "Методичні рекомендації до підготовки та захисту дипломної роботи (проекту) для студентів галузі знань 1701 "Інформаційна безпека" та спеціальності 125 "Кібербезпека"" // Методична розробка. – Д.: Національний гірничий університет, 2016. – 44 с. 3. Бабенко Т.В.,Конспект лекцій в електронному вигляді з дисципліни "Технологія створення та застосування систем захисту інформаційно-комунікаційних систем" // Конспект лекцій – Д.: Національний гірничий університет, 2016. – 216 с. 4. Бабенко Т.В.,Конспект лекцій в електронному вигляді з дисципліни "Інформаційно-комунікаційні системи" // Конспект лекцій – Д.: Національний гірничий університет, 2016. –381 с. *Наукові статті:*	Підвищення кваліфікації у Державному ВНЗ «Національний гірничий університет» з 05.01.2015 р. до 04.07.2015 р. Свідоцтво 12СПК 810047, видане 06.07.2015 р.

			від 03.12.2008р. Професор за кафедрою “Безпеки інформації та телекомунікацій” Атестат професора 12ПР №008558 від 28 березня 2013р.		1. Бабенко Т.В. Дослідження ентропії мережевого трафіка як індикатора DDOS-атак // Науковий Вісник Національного гірничого університету. - 2013. - №2 (134). - С. 86-89. 2. Бабенко Т.В., Третяк О.М., Кручінін О.В., Тимофєєв Д.С. Проблеми захисту освітніх електронних інформаційних ресурсів // Науковий Вісник Національного гірничого університету. - 2012. - №5 (131). - С. 101-105. *Тези:* 1. Герасименок А.В., Бабенко Т.В. Применение интеллектуальных систем информационной безопасности для повышения защищённости АС управления вузом // Тези доповідей VI науково-практичної конференції студентів, аспірантів, молодих вчених. Інформаційні технології. Безпека та зв'язок (3 квітня 2014р.) Державний ВНЗ “НГУ”. - Дніпропетровськ, 2014. - С. 39-40. 2. Герасименок А.В., Бабенко Т.В. Анализ уровня защищённости автоматизированных систем управления автомобилями и рекомендации по его повышению // Тези доповідей VI науково-практичної конференції студентів, аспірантів, молодих вчених. Інформаційні технології. Безпека та зв'язок (3 квітня 2014р.) Державний ВНЗ “НГУ”. - Дніпропетровськ, - 2014. - С. 40-42. 3. Дашко Д.О., Бабенко Т.В., Аналіз сучасного стану систем водопостачання України // Тези доповідей VI науково-практичної конференції студентів, аспірантів, молодих вчених. Інформаційні технології. Безпека та зв'язок (3 квітня 2014р.) Державний ВНЗ “НГУ”. - Дніпропетровськ, - 2014. - С. 42-44. 4. Гвоздакова В.Г., Бабенко Т.В. Ідентифікація мережевих аномалій на базі нейроних мереж з самоорганізацією // Тези доповідей VII науково-практичної конференції студентів, аспірантів, молодих вчених. Інформаційні технології. Безпека та зв'язок Державний ВНЗ “НГУ”. - Дніпропетровськ, - 2016. - С. 8-9. 5. Кондрашов А.С., Бабенко Т.В. Генерации речеподобной помехи // Тези доповідей VI науково-практичної конференції студентів, аспірантів, молодих вчених. Інформаційні технології. Безпека та зв'язокДержавний ВНЗ “НГУ”. - Дніпропетровськ, - 2016. - С. 11-13. 6. Малик О.І., Бабенко Т.В. Применение нейросетевых систем для оценки параметров безопасности интернет-ориентированных систем // Тези доповідей VI науково-практичної конференції студентів, аспірантів, молодих вчених. Інформаційні технології. Безпека та зв'язок Державний ВНЗ “НГУ”. - Дніпропетровськ, - 2016. - С. 14-15.	

					Має статус академічного консультанта ISACA - організації з розробки методологій та стандартів в галузі управління, аудиту і безпеки інформаційних технологій. 7. Бабенко Т.В., Гречко В.В. Визначення інформативних ознак мережевого трафіка // II Науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”, Київ, 23 березня 2017, стор. 62. 8. Бабенко Т.В., Ковальва Ю.В. Забезпечення кібербезпеки об’єктів енергетичної інфраструктури // II Науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”, Київ, 23 березня 2017, стор. 121. 9. Бабенко Т.В., Рабченюк С.І. Кіберзахист об’єктів критичної інфраструктури // II Науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”, Київ, 23 березня 2017, стор. 168. 10. Бабенко Т.В., Савчук В.В. Ідентифікація аномалій мережевого трафіка // II Науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”, Київ, 23 березня 2017, стор. 181. 11. Бабенко Т.В., Романова А.С. Questionsofcybersecurityofcriticalinfrastructuresofdifferentcountries // II Науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”, Київ, 23 березня 2017, стор. 347. 12. Бабенко Т.В., Толюпа С.В., Ковалюва Ю.В. Моделі ідентифікації мережевих аномалій на основі карти самоорганізації // VII Міжнародна науково-практична конференція “ITSEC”, Київ 16-18 травня 2017, стр. 102-106. 13. Бабенко Т.В., Гречко В.В. Визначення інформативних ознак мережевого трафіка // Вісник інженерної академії наук 2017. - №1. - С. 82-89 фахове видання. 14. Бабенко Т.В., Толюпа С.В., Пархоменко І.І Themethodofformingandsignalprocessingaimedatimprovingstealsandenergyefficiently // 2th IEEE International Sientific-Practical Conference AICT-2017 June 24-27, 2017 paper 83 Іноземне видання. 15. Бабенко Т.В., Serhii Toliupa, AlexanderTrush TheBuildingof a Security Strategy Basedonthe Model of Game Management // 4th IEEE InternationalSientific-PracticalConferenceProblemsofInfocomunicationsSienceandTechnology PIC S&T-2017 October 10-13, 2017 paper 16. Іноземне видання.	

Пархоменко Іван Іванович	Доцент кафедри кібербезпеки та захисту інформації	*Закінчив*: Український державний університет харчових технологій в 1996 році ЛМ № 000377 від 20 червня 1996 р. *спеціальність* автоматизація технологічних процесів та виробництв *кваліфікація спеціаліста*: інженер з автоматизація	Кандидат технічних наук ДК №015285 від 3 липня 2002 р. *шифр і назва наукової спеціальності:* 05.13.07 «Автоматизація технологічних процесів» *тема дисертації*: «Автоматизована система управління ділянкою очищення дифузійного соку на базі нечіткої логіки» доцент 12ДЦ №017184 від 21 червня 2007 р. *вчене звання за якою кафедрою присвоєно:* доцент кафедри комп'ютеризованих систем захисту інформації	19,5 років	Загальна кількість робіт – 127; з них: *Наукові статті:* 1) Пархоменко І.І., Воскобойніков А.О., "Організація захищеної передачі даних в системі Web-сервер - клієнт" / Вісник інженерної академії України випуск №1 – 2014. – С. 116-120. 2) Пархоменко І.І., Завацький С.М., " Застосування засобів моніторингу інформаційної безпеки в корпоративній мережі" / Вісник інженерної академії України випуск №1 – 2015. – С. 142-145 3) Пархоменко І.І., Бондаренко Л.Л., " Лінгвістична стеганографія та сучасні програмні засоби стеганографічного захисту інформації" / Вісник інженерної академії України випуск №2 – 2015. – С. 81-85 4) Пархоменко І.І., Чоботок А.Ю. "Загрози інформаційної безпеки в стільникових мережах стандарту lte з інтегрованми фемтосотами" /Вісник інженерної академії України випуск №2 – 2015. – С. 93-97 5) S.V. Toliupa, I.I. Parkhomenko "Methodology of selecting optimal parameters of OFDM- SCC in conditions of selective stopping in radio path"/ Science and Education a New Dimension. Natural and Technical Sciences, III(8), Issue: 73, BUDAPEST -2015. С. 85-88. 6) Toliupa S., Parkhomenko I. Data protection with intellectual support of organizational and technical and operational management. Радіотехніка та телекомунікації. Львів. НУ "Львівська політехніка". №3 – 2016. с. 121 – 130. 7) Toliupa S., Parkhomenko I. The development of a process planning model of rational modular composition of the information protection systems. Проблеми телекомунікацій. Харьків. ХНУРЕ. №3 – 2016. с. 56 – 64. 8) Пархоменко І.І., Кузнєцов К.Ю., "Порівняльний аналіз алгоритмів асиметричного шифрування" / Вісник інженерної академії України випуск №3 – 2016. – С.89-95 9) Пархоменко І.І., Галкін В.В. "Способи захисту каналів корпоративних мереж на базі VPN-рішень"/Науково-технічний журнал «Сучасний захист інформації» №4 – 2016. – С. 64-69 10) Пархоменко І.І., Баран Д.М. "Способи та механізми захисту інформаційних ресурсів на мобільних пристроях"" / Вісник інженерної академії України випуск №1 – 2017. – С. 81-85 11) Toliupa S., Babenko T., Parkhomenko I. "The method of forming and signal processing aimed at improving steals and energy efficiently" / 2nd IEEE International Conference AICT-2017 paper 83 12)Пархоменко І.І., Галкін В.В. «Способи захисту каналів корпоративних мереж на базі апаратно-програмних засобів» / Вісник інженерної академії України випуск №2 – 2017. – С. 81-85	підвищення кваліфікації (стажування) в навчально-науковому інституті комп'ютерних інформаційних технологій на кафедру комп'ютеризованих систем захисту інформації термін проходження з 20 вересня 2017 по 20 грудня 2017 Сертифікат №03.02/2724 від 20.12.2017 р.

					13) Пархоменко І.І., Кузнєцов К.Ю. «Захист електронних повідомлень за допомогою криптозасобів з відкритим ключем» / Вісник інженерної академії України випуск №2 – 2017. – С. 86-91 14) Толюпа С.В., Пархоменко І.І., Коноваленко А.Д. 72 «Аналіз вразливостей локальних бездротових мереж та способи їх захисту від можливих атак» / Вісник інженерної академії України випуск №3 – 2017. – С. 72-76 *Наукові конференції:* 1) Пархоменко І.І., Бондаренко Л.Л. "Спільне використання криптографічних та стеганографічних методів для передачі прихованої інформації" // II Міжнародна науково-практична конференція «Інформаційні технології та взаємодії – 3- 5 листопада 2015, тези доповідей, Київ 2015. ст. 53-54 2) Пархоменко І.І., Папуша А.В.. "Проблеми уразливості і засоби захисту в мережах LTE" // II Міжнародна науково-практична конференція «Інформаційні технології та взаємодії – 3- 5 листопада 2015, тези доповідей, Київ 2015. ст. 55-56 3) Пархоменко І.І., Столяр Д. В. «Захист інформаційних потоків у глобальних бездротових мережах на базі стандарту GSM» // Матеріали Міжнародної науково-технічної конференції "Сучасні інформаційно-телекомунікаційні технології" Том IV «Сучасні технології інформаційної безпеки» 17–20 листопада 2015 р., тези доповідей, Київ 2015, ст.. 134-136 4) Толюпа С.В., Пархоменко І.І. «Адаптивний вибір значень параметрів OFDM-сигналу, оптимальних за критерієм максимуму показника енергетичної ефективності» // Матеріали Міжнародної науково-технічної конференції "Сучасні інформаційно-телекомунікаційні технології" Том IV «Сучасні технології інформаційної безпеки» 17–20 листопада 2015 р., тези доповідей, Київ 2015, ст.. 149-151 5) Толюпа С.В., Пархоменко И.И., «Повышение эффективности управления сетями нового поколения на основе применения интеллектуальных технологий» // Труды II Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика», Алматы, Казакстан, 3-4 декабря, 2015 года I том, ст.. 271-275 6) Пархоменко І.І., Радченко З.І. «Захист глобальних бездротових мереж третього покоління» // Інформаційні технології в економіці, менеджменті і бізнесі. Проблеми науки, практики і освіти: XXI міжнародна науково-практична конференція 27 листопада 2015 р., : тези доповідей. – К: 2015. - С. 86-88.	

					7) Пархоменко І.І., Батюк О.А. «Методи захисту локальних бездротових мереж» // ІІ Міжнародна науково-практична конференція «Проблеми та перспективи розвитку енергетики, електротехнологій, та автоматики в АПК» 17-18 грудня 2015 р., : тези доповідей. – К: 2015. - С. 8-11. 8) Толюпа С.В., Пархоменко І.І. «Застосування методів теорії декомпозиції для формування системи показників якості безпеки інформаційних систем» // ІІ Міжнародна науково-технічна конференція «Актуальні проблеми розвитку науки і техніки» 20 грудня 2015 р., збірник тез, Київ 2015, ст.. 36-38 9) I.I.Parkhomenko, D.G.Kodlubovskyi. Steganography in information security // П'ята міжнароднанауково-практична конференція "Інфокомунікації – сучасність та майбутнє", том 3. – 2015. – с. 121-122. 10) I.I.Parkhomenko, D.G.Kodlubovskyi. Main objectives of steganography // Науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем"– 10-11 березня, 2016.– с. 11. 11) Пархоменко І.І., Кузнецов К.Ю., «Аналіз алгоритмів електронно-цифрового підпису при передачі інформації» // Науково-Практична Конференція. Проблеми кібербезпеки інформаційно-телекомунікаційних систем – К., 2016. – С.47 12) Пархоменко І.І., Галкін В.В., «Захист транзакцій в каналах корпоративних мереж за допомогою VPN-технологій»// IV Міжнародна науково-практична конференція. Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні 23 – 24 червня 2016. – К., 2016. – С. 53 -54 13) Пархоменко І.І., Брухаль Я.Л. «Методи захисту ресурсів домену локальної мережі організації» // ІІІ Міжнародна науково-практична конференція «Інформаційні технології та взаємодії», 8- 10 листопада 2016, тези доповідей, Київ 2016. ст. 195-196 14) Пархоменко І.І., Сич І.Г. «Методи стеганографічного приховування інформації в інформаційно-комунікаційних системах» // IV Міжнародна науково-практична конференція « Проблеми та перспективи розвитку енергетики, електротехнологій, та автоматики в АПК» 21-22 листопада 2016 р., : тези доповідей. – К: 2016. - С. 162-163. 15) Толюпа С.В., Пархоменко І.І. «Многоуровневые иерархические модели систем защиты информации» // Матеріали ІІ Міжнародної науково-практичної конференції "Тенденції розвитку корвергентних мереж: рішення пост: NGN, 4G, 5G ". 17-18 листопада 2016 року – м. Київ. ДУТ. – 2016р., с.111-114	

					16) Толюпа С.В., Пархоменко І.І. «Аналіз сучасних систем виявлення вторгнень як засобу боротьби з ботнет-кодом» // Матеріали V Міжнародної науково-практичної конференції «Фізико-технічні проблеми передавання, обробки та зберігання інформації в інфокомунікаційних системах» - 3-5 листопада 2016, тези доповідей, Чернівці 2016. ст. 223-225. 17) Пархоменко І.І. «Кібернетична безпека інтернет речей» // II Науково-Практична Конференція. Проблеми кібербезпеки інформаційно-телекомунікаційних систем – К., 2017. – С. 103-107 18) Пархоменко І.І., Баран Д.М. "Методи витоку даних з мобільних пристроїв" // X Міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні системи" – 16-17 травня 2017 року, тези доповідей, Київ 2017 ст. 264-265 19) Пархоменко І.І., Юшко З.І. "Захист глобальних мереж на базі технології LTE" // X Міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні системи" – 16-17 травня 2017 року, тези доповідей, Київ 2017 ст. 266-267	
Лукова-Чуйко Наталія Вікторівна	Доцент кафедри кібербез-пеки та захисту інформа-ції	Київський національний університет імені Тараса Шевченка, 2006 р., спеціальність - математика, кваліфікація - магістр математики. Диплом КВ №29239570 від 21.06.2006р.	Кандидат фізико-математичних наук 01.01.04-геомет-рія та топологія, «Функції на тривимірних многовидах». Диплом ДК №060875 від 1.07.2010р. Доцент кафедри кібербезпеки та захисту інформації. Атестат доцента 12ДЦ №044834 від 15 грудня 2015 р.	8 років	*Підручники, монографії:* 1.Системний аналіз та прийняття рішень в інформаційній безпеці: Підручник (у співавторстві) –К.: ДУТ, 2015. 2. Інформаційні та кібернетичні простори: проблеми безпеки, методи та засоби боротьби: Посібник (у співавторстві) – К.: ДУТ-КНУ, 2016. Рекомендовано МОН України. 3. Method sofself-diagnosis of telecommunication networks based on flexible structure softest connections //Collection of materials of International Scientific Conference «Complex Systems Security Management – 2015». –Liptovský Mikuláš, Slovakiya, - 2015. – P. 215 – 220. 4. Vulnerability Analysis for Dynamic Investment Management //Science and Education a New Dimension: Natural and Technical Sciences, III(6), I SSUE 54,2015.– P.42-46 5. Choiceof Reasonable Variant of Signal and Code Constructions for Multirays Radio Channels// Second International Scientific-Practical Conference Problems of Infocommunications. Science and Technology. - IEEE PIC S&T 2015 - P. 269 – 271 6. Математична модель взаємовідносин загроз та комплексних систем захисту інформації// Вісник інженерної академії України. м. Київ, № 3, 2015– С. 131-135 7. Minimalfunctions on 3-manifold with boundary//Proc. Intern. Geom. Center. – 2015. – Т 8 (3), 2015– С. 6-12	СПК №301868, від 29 травня 2015 року Вінницький національний технічний університет, Центр інформаційних технологій і захисту інформації, «Оцінювання захищеності інформації. Виявлення закладних пристроїв»

					8. Application game theory in constructing the mathematical model of threatsand complex systems of information security//International Scientific and Practical Conference “WORLDSCIENCE”. — ISSN 2413-1032.–№ 4(4), Vol.4.,2015.– P. 12-15 *Наукові конференції:* 9. Визначення оптимального варіанту побудови комплексних систем захисту інформації // Об’єднані наукою: перспективи міждисциплінарних досліджень: Матер. круглого столу: 10-11 листопада 2014 . – Київ, 2014. – С. 32-35 10. Застосування теорії нечітких множин для формалізації задачі оцінки рівня захищеності інформації// Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави»: Зб. мат. наук.-практ. конф. студ., асп., викл. та науковців – 18 грудня, Київ, ДУТ, 2014. – С. 5 11. Методи оцінки рівня захисту інформації на основі застосування Fuzzi-технологій//Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави»: Зб. мат. наук.-практ. конф. студ., асп., викл. та науковців – 18 грудня, Київ, ДУТ, 2014. – С. 3 12. Моделювання оптимальних систем захисту інформації// Науково-технічна конференція «Інформаційна безпека держави»: Наукові доповіді учасників науково-технічної конференції – 12 – 13 березня, Київ, КНУ імені Т. Шевченка, 2015. – С. 119-120 13. Модель функціонування системи підтримки прийняття рішень//Матеріали Восьмої науково-практичної конференції “Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення з урахуванням досвіду АТО”, 29 жовтня 2015 р., ВІТІ ДУТ, м. Київ 14.AutomatedUnifiedSecurityAnalyticsSystemforDetectingandIdentifyingThreatstotheCriticalInfrastructures //Матеріали II Міжнародної науково-практичної конференції “Інформаційні технології та взаємодії”, 3-5 листопада 2015 р., м. Київ 15. Decision making process in information security based on vulnerability analysis // Науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем», 10-11 березня 2016 р., м. Київ	

При розробці проекту освітньої програми враховані вимоги: Стандарту вищої освіти України з підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
“Кібербезпека”
“CyberSecurity”
зі спеціальності 125 “Кібербезпека”
125 “CyberSecurity”

1 – Загальна інформація	
Ступінь вищої освіти та назва кваліфікації	ступінь вищої освіти: бакалавр спеціальність: 125 - кібербезпека освітня програма: кібербезпека Obtainedqualification: BachelorDegree Program Subject Area: Cybersecirity Program: Cybersecurity
Мова(и) навчання і оцінювання	українська, Ukraine
Обсяг освітньої програми	240 кредитів ЄКТС, 4 роки (при вступі на базі ОКР «молодший спеціаліст», ОР «молодший бакалавр» за умови перерахування до 60 кредитів – 180 кредитів ЄКТС, 3 роки)
Тип програми	Освітньо-професійна
Повна назва закладу вищої освіти, а також структурного підрозділу у якому здійснюється навчання	Київський національний університет імені Тараса Шевченка, Україна ***Taras Shevchenko National University of Kyiv, Ukraine*** Факультет інформаційних технологій ***Faculty of Information Technology***
Назва закладу вищої освіти який бере участь у забезпеченні програми (заповнюється для програм подвійного і спільного дипломування)	-
Офіційна назва освітньої програми, ступінь вищої освіти та назва кваліфікації ВНЗ-партнера мовою оригіналу (заповнюється для програм подвійного і спільного дипломування)	-
Наявність акредитації	Сертифікат про акредитацію серія УД № 11001454 від 20 червня 2018 року
Цикл/рівень програми	НРК України – 7 рівень, FQ-EHEA – перший цикл, EQFLLL – 6
Передумови	Атестат про середню освіту. Диплом «молодшого спеціаліста» або «молодшого бакалавра» при вступі на скорочену форму навчання відповідно до вимог правил прийому до Університету
Форма навчання	денна
Термін дії освітньої програми	5 років
Інтернет-адреса постійного розміщення опису освітньої програми	http://fit.univ.kiev.ua/

2 – Мета освітньої програми	
Мета програми (з врахуванням рівня кваліфікації)	Підготовка фахівців здатних розв'язувати спеціалізовані задачі і практичні проблеми у галузі інформаційної безпеки та використовувати і впроваджувати технології інформаційної та/або кібербезпеки
3 - Характеристика освітньої програми	
Предметна область (галузь знань / спеціальність / спеціалізація програми)	12 Інформаційні технології 125 Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна академічна
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта за спеціальністю «Кібербезпека». Ключові слова: захист інформації, кіберпростір, кібератаки, система захисту, проектування комплексних систем захисту, захист програмного забезпечення, сервіси безпеки.
Особливості програми	Включає обов'язкові виробничі практики.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Робочі місця в компаніях, підприємствах приватного та державного сектору в сфері забезпечення інформаційної та кібернетичної безпеки Фахівець із організації інформаційної безпеки.
Подальше навчання	Можливість продовжити навчання за освітньо-професійною або освітньо-науковою програмою ступеня магістр
5 – Викладання та оцінювання	
Викладання та навчання	Загальний стиль навчання – завдання-орієнтований. Лекції, практичні заняття, лабораторні роботи в невеликих групах, самостійна робота на основі підручників та конспектів, консультації із викладачами. Під час останнього семестру навчання половина часу відводиться на написання бакалаврської кваліфікаційної роботи (дипломної), яка презентується та обговорюється за участю викладачів та одногрупників.
Оцінювання	Письмові та усні іспити, лабораторні звіти, усні презентації, поточний контроль, заліки, диференційовані заліки, захист бакалаврської роботи
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю, неповною та визначеністю умов
Загальні компетентності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

	ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації. ЗК 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; ЗК 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.
Фахові компетентності спеціальності (ФК)	ФК 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. ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

	ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам.
7 – Програмні результати навчання	
Програмні результати навчання	**ПР1 -** застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; **ПР2 -** аналізувати, аргументувати, приймати рішення при розв'язанні спеціалізованих задач та практичних проблем у професійній діяльності, що характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; **ПР3 -** діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, в тому числі міжнародних в галузі інформаційної та /або кібербезпеки; **ПР4 -** виконувати аналіз та декомпозицію ІТС; **ПР5 -** виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; **ПР6 -** розробляти моделі загроз та порушника; **ПР7 -** аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; **ПР8 -** забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, архітектур та моделей захисту електронних інформаційних ресурсів; **ПР9 -** забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів руйнуючих кодів в ІТС; **ПР10 -** вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів

	і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки; **ПР11** - забезпечувати процеси захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих); **ПР12** - аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; **ПР13** - вирішувати задачі управління процесами відновлення штатного функціонування ІТС; **ПР14** - 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; **ПР15** - виявляти небезпечні сигнали технічних засобів; **ПР16** - вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації **ПР17** - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; **ПР18** - проводити атестацію (спираючись на облік та обстеження) режимних територій, приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; **ПР19** - забезпечувати безперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур **ПР20** - впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки, застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів **ПР21**застосовувати політики, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; **ПР22** - здійснювати аналіз ризиків обробки інформації в ІТС; **ПР23–**застосовувати методи та засоби криптографічного захисту інформації; **ПР24** - виконувати впровадження та підтримку систем виявлення вторгнень

	ПР25 - використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІТС. **ПР26 -** забезпечувати належне функціонування системи моніторингу та програмних і програмно-апаратних комплексів виявлення вторгнень; **ПР27 -** вирішувати задачі аналізу програмного коду на наявність можливих вразливостей.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	До викладання професійно-орієнтованих дисциплін освітньої програми «Кібербезпека» залучаються, фахівців служби безпеки України та державної служби спеціального зв'язку та захисту інформації
Специфічні характеристики матеріально-технічного забезпечення	Проведення занять здійснюється із застосуванням комп'ютерних засобів та програмного забезпечення HashCalle, Virtualbox, dtopbox, а також спеціалізованого обладнання для виявлення каналів витоку інформації, та для проведення спеціалізованих досліджень
Специфічні характеристики інформаційного та навчально-методичного забезпечення	Все необхідне інформаційне та навчально-методичне забезпечення розміщується в електронному вигляді на хмарних ресурсах, що забезпечує дистанційний доступ до інформації.
9 – Академічна мобільність	
Національна кредитна мобільність	-
Міжнародна кредитна мобільність	-
Навчання іноземних здобувачів вищої освіти	На загальних умовах.

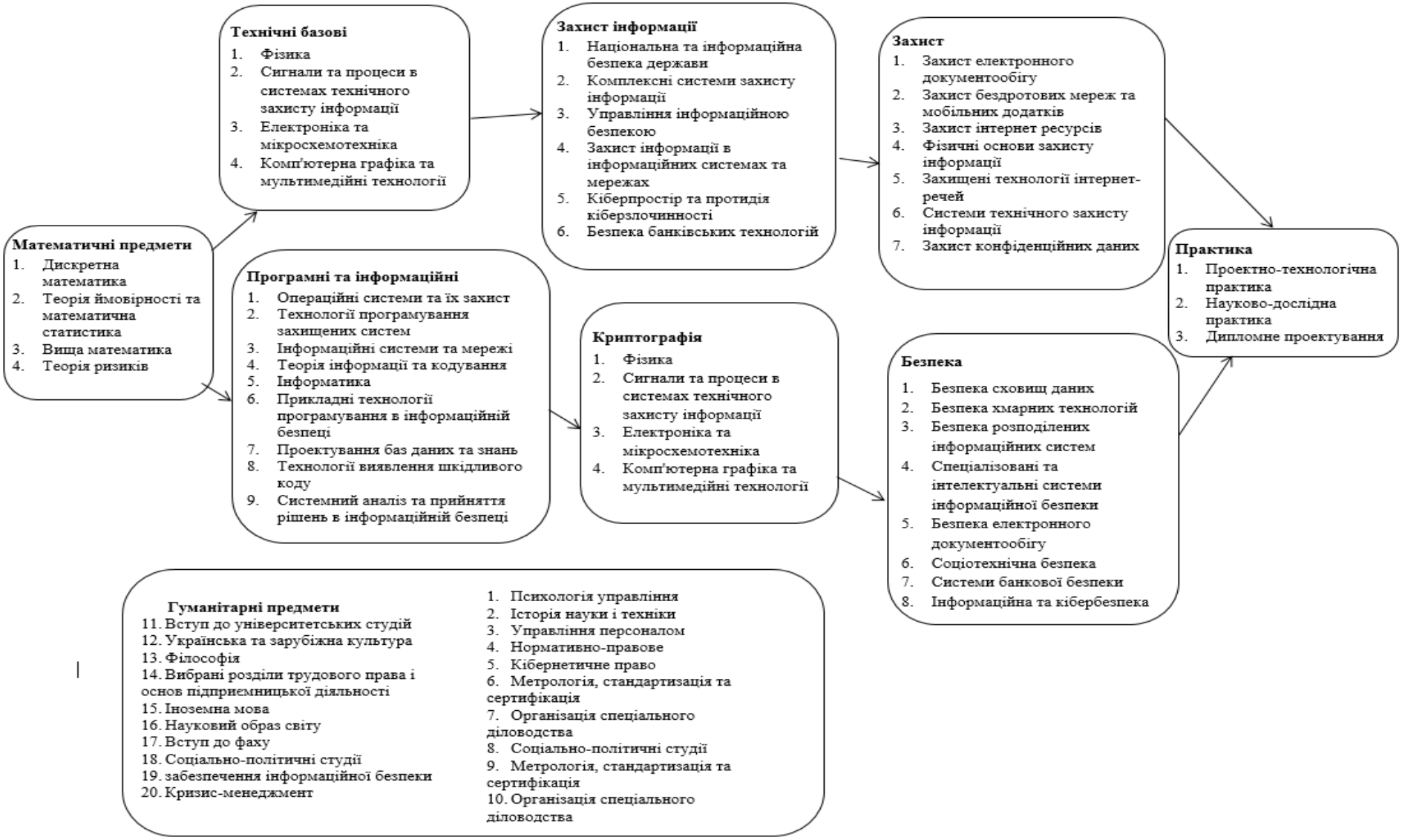
2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Вступ до університетських студій	2	залік
ОК 2.	Українська та зарубіжна культура	3	залік
ОК 3.	Філософія	4	іспит
ОК 4	Дискретна математика	4	залік
ОК 5.	Теорія ймовірності та математична статистика	4	іспит
ОК 6.	Фізика	6	іспит
ОК 7.	Національна та інформаційна безпека держави	8	залік
ОК 8.	Операційні системи та їх захист	5	залік
ОК 9.	Технології програмування захищених систем	6	іспит
ОК 10.	Сигнали та процеси в системах технічного захисту інформації	8	іспит
ОК 11.	Електроніка та мікросхемотехніка	6	іспит
ОК 12.	Архітектура комп'ютерних систем	4	іспит
ОК 13.	Інформаційні системи та мережі	8	іспит
ОК 14.	Теорія інформації та кодування	6	залік
ОК 15.	Криптографічні системи захисту інформації	10	іспит
ОК 16.	Комплексні системи захисту інформації	9	іспит
ОК 17.	Вибрані розділи трудового права і основ підприємницької діяльності	3	залік
ОК 18.	Управління інформаційною безпекою	6	іспит
ОК 19.	Захист інформації в інформаційних системах та мережах	9	іспит
ОК 20.	Кіберпростір та протидія кіберзлочинності	6	залік
ОК 21.	Проектно-технологічна практика	4	диференційований залік
ОК 22.	Науково-дослідна практика	4	диференційований залік
ОК 23.	Іноземна мова	15	іспит
ОК 24.	Вища математика	10	іспит
ОК 25.	Науковий образ світу	3	залік
ОК 26	Комп'ютерна графіка та мультимедійні технології	3	залік
ОК 27	Інформатика	7	іспит
ОК 28	Вступ до фаху	3	іспит
ОК 29	Безпека банківських технологій	4	залік
ОК 30	Дипломне проектування	8	захист
ОК 31	Соціально-політичні студії	2	залік
З агальний обсяг обов'язкових компонент:		180	
Вибіркові компоненти ОП			
Вибірковий блок 1 Безпека інформаційних і комунікаційних систем			
ВБ 1.1.	Безпека сховищ даних	4	залік

ВБ 1.2.	Нормативно-правове забезпечення інформаційної безпеки	4	залік
ВБ 1.3.	Технології виявлення шкідливого коду	6	іспит
ВБ 1.4.	Захист електронного документообігу	6	іспит
ВБ 1.5.	Захист бездротових мереж та мобільних додатків	6	залік
ВБ 1.6.	Безпека хмарних технологій	6	іспит
ВБ 1.7.	Прикладні технології програмування в інформаційній безпеці	6	іспит
ВБ 1.8	Безпека розподілених інформаційних систем	6	іспит
		44	
Вибірковий блок 2 Управління інформаційною безпекою			
ВБ 2.1.	Захист інтернет ресурсів	4	залік
ВБ 2.2.	Проектування баз даних та знань	4	іспит
ВБ 2.3.	Фізичні основи захисту інформації	6	іспит
ВБ 2.4.	Теорія ризиків	6	іспит
ВБ 2.5	Захищені технології інтернет-речей	6	залік
ВБ 2.6	Стеганографія	6	залік
ВБ 2.7	Системи технічного захисту інформації	6	іспит
ВБ 2.8	Системний аналіз та прийняття рішень в інформаційній безпеці	6	іспит
		44	
Вибірковий блок за переліком 1 (студент обирає 1 дисципліну)			
ВБ 3.1	Кризис-менеджмент	4	залік
ВБ 3.2	Спеціалізовані та інтелектуальні системи інформаційної безпеки	4	залік
ВБ 3.3	Інфраструктура відкритих ключів	4	залік
ВБ 3.4	Психологія управління	4	залік
Вибірковий блок за переліком 2 (студент обирає 1 дисципліну)			
ВБ 4.1	Кібернетичне право	4	іспит
ВБ 4.2	Захист конфіденційних даних	4	іспит
ВБ 4.3	Історія науки і техніки	4	іспит
ВБ 4.4	Безпека електронного документообігу	4	іспит
Вибірковий блок за переліком 3 (студент обирає 1 дисципліну)			
ВБ 5.1	Соціотехнічна безпека	4	іспит
ВБ 5.2	Системи банкової безпеки	4	іспит
ВБ 5.3	Управління персоналом	4	іспит
ВБ 5.4	Інформаційна та кібербезпека сучасного підприємства	4	іспит
Вибірковий блок за переліком 4 (студент обирає 1 дисципліну)			
ВБ 6.1	Метрологія, стандартизація та сертифікація	4	іспит
ВБ 6.2	Стандарти інформаційної безпеки	4	іспит
ВБ 6.3	Квантова криптологія	4	іспит
ВБ 6.4	Організація спеціального діловодства	4	іспит
Загальний обсяг вибіркових компонент:		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

Структурно-логічна схема



ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників освітньої програми спеціальності № 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної бакалаврської роботи (проекту) та завершується видачою документу про присудження йому ступеня бакалавра з присвоєнням кваліфікації - бакалавр кібербезпеки.

Випускна кваліфікаційна робота повинна продемонструвати виконання студентом навчального плану підготовки фахівця з кібербезпеки і бути результатом закінченого дослідження, що має внутрішню єдність і свідчити про те, що її автор спроможний самостійно їх проводити та складається з пояснювальної записки до дипломної роботи і демонстраційного матеріалу для доповіді перед екзаменаційною комісією.

Кваліфікаційний проект (робота) має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційний проект (робота) має бути перевірений на плагіат.

При атестації перевіряється: програмні результати навчання, зокрема вміння: аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, відповідати за прийняті рішення; розробляти моделі загроз та порушника; вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.

Атестація здійснюється відкрито і публічно.

4. Матриця відповідності програмних компетенцій компонентам освітньої програми

	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	ОК31
ЗК1				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	
ЗК2				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+		+	+	+	+	+	
ЗК3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК4								+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+			+	+	+	+	
ЗК5	+						+		+					+			+			+	+	+			+	+	+	+	+	+	+
ЗК6																	+				+	+								+	+
ЗК7		+																							+					+	
ФК1							+						+				+	+			+	+						+		+	
ФК2								+	+	+	+	+	+	+	+	+		+	+		+	+								+	
ФК3									+										+		+	+								+	
ФК4																	+	+			+	+								+	
ФК5									+	+	+					+			+		+	+								+	
ФК6																		+			+	+								+	
ФК7							+			+	+					+		+	+		+	+		+						+	
ФК8																		+			+	+								+	
ФК9									+	+	+							+	+		+	+							+	+	
ФК10										+	+				+						+	+								+	
ФК11																		+			+	+								+	
ФК12								+	+	+	+							+			+	+								+	

Продовження таблиці

	ВБ 1.1.	ВБ 1.2.	ВБ 1.3.	ВБ 1.4.	ВБ 1.5.	ВБ 1.6.	ВБ 1.7.	ВБ 1.8.	ВБ 2.1.	ВБ 2.2.	ВБ 2.3.	ВБ 2.4.	ВБ 2.5.	ВБ 2.6.	ВБ 2.7.	ВБ 2.8.
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

ЗК3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК5		+				+		+	+			+	+			
ЗК6		+														
ЗК7																
ФК1		+														
ФК2					+			+	+	+	+		+	+	+	+
ФК3	+			+	+										+	
ФК4																
ФК5	+				+						+				+	
ФК6																
ФК7		+			+						+				+	
ФК8																
ФК9	+		+	+	+						+				+	
ФК10				+							+					
ФК11	+		+													
ФК12											+	+				+

Продовження таблиці

	ВБ 3.1.	**ВБ 3.2.**	**ВБ 3.3.**	**ВБ 3.4.**	**ВБ 4.1.**	**ВБ 4.2.**	**ВБ 4.3.**	**ВБ 4.4.**	**ВБ 5.1.**	**ВБ 5.2.**	**ВБ 5.3.**	**ВБ 5.4.**	**ВБ 6.1.**	**ВБ 6.2.**	**ВБ 6.3.**	**ВБ 6.4.**
ЗК1	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+
ЗК2		+	+	+	+	+		+	+	+	+	+	+	+	+	+
ЗК3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК4		+	+	+	+	+		+	+	+	+	+	+	+	+	+
ЗК5				+	+		+			+		+				
ЗК6					+											
ЗК7				+			+									
ФК1	+				+							+	+	+		+
ФК2		+										+			+	

ФК3		+				+		+																				
ФК4																				+								
ФК5																				+								
ФК6																												
ФК7		+			+				+		+																	+
ФК8																												+
ФК9		+				+		+	+	+	+	+																
ФК10						+		+																		+		
ФК11																												
ФК12									+																			

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідним компонентам освітньої програми

	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**	**ОК 30**	**ОК 31**
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									+												+	+								+	

Продовження таблиці

	ВБ 1.1.	**ВБ 1.2.**	**ВБ 1.3.**	**ВБ 1.4.**	**ВБ 1.5.**	**ВБ 1.6.**	**ВБ 1.7.**	**ВБ 1.8.**	**ВБ 2.1.**	**ВБ 2.2.**	**ВБ 2.3.**	**ВБ 2.4.**	**ВБ 2.5.**	**ВБ 2.6.**	**ВБ 2.7.**	**ВБ 2.8.**
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			+		+		+		+				+			

Продовження таблиці

	ВБ 3.1.	**ВБ 3.2.**	**ВБ 3.3.**	**ВБ 3.4.**	**ВБ 4.1.**	**ВБ 4.2.**	**ВБ 4.3.**	**ВБ 4.4.**	**ВБ 5.1.**	**ВБ 5.2.**	**ВБ 5.3.**	**ВБ 5.4.**	**ВБ 6.1.**	**ВБ 6.2.**	**ВБ 6.3.**	**ВБ 6.4.**
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																